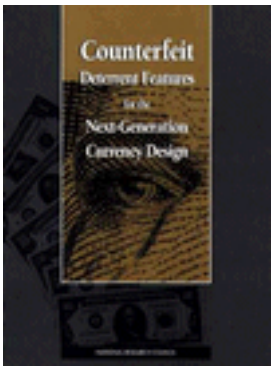

Counterfeit Deterrent Features for the Next-Generation Currency Design

Committee on Next-Generation Currency Design, Commission on Engineering and Technical Systems, National Research Council

ISBN: 0-309-56279-1, 144 pages, 8.5 x 11, (1993)

COUNTERFEIT DETERRENT FEATURES FOR THE NEXT-GENERATION CURRENCY DESIGN

Committee on Next-Generation Currency Design
National Materials Advisory Board
Commission on Engineering and Technical Systems
National Research Council

Publication NMAB-472

National Academy Press
1993

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competencies and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

The National Academy of Sciences is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The National Academy of Engineering was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Robert M. White is president of the National Academy of Engineering.

The Institute of Medicine was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth I. Shine is President of the Institute of Medicine.

The National Research Council was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. Robert M. White are chairman and vice chairman, respectively, of the National Research Council.

This study by the National Materials Advisory Board was conducted under Contract No. TEP-92-58(N) with the U.S. Treasury Department, Bureau of Engraving and Printing.

Library of Congress Catalog Card Number 93-87390
International Standard Book Number 0-309-05028-6

Available in limited supply from:
National Materials Advisory Board
2101 Constitution Ave, NW - Rm. HA 262
Washington, DC 20418
Additional copies available for sale from:

National Academy Press 2101 Constitution Ave, NW P.O. Box 285 Washington, DC 20055 1-800-624-6242 202-334-3313 (in Washington metropolitan area)

B-273
Printed in the United States of America.

COMMITTEE ON NEXT-GENERATION CURRENCY DESIGN

GLENN T. SINCERBOX Chair, IBM Research Division, Almaden Research Center, San Jose, California
STEVEN ANDRIOLE, Drexel University, Philadelphia, Pennsylvania
NORBERT S. BAER, New York University, New York, New York
DONALD BAUDER, Sandia National Laboratory (Retired), Albuquerque, New Mexico
MITCHELL J. FEIGENBAUM, Rockefeller University, New York, New York
JOSEPH GAYNOR, Innovative Technology Associates, Ventura, California
STEVEN M. GEORGE, University of Colorado, Boulder
ANNETTE B. JAFFE, Apple Computer, Inc., Santa Clara, California
MICHAEL MORRIS, University of Rochester, Rochester, New York
KURT NASSAU, AT&T Bell Laboratories (retired); Nassau Consultants, Lebanon, New Jersey
ROBERT R. SHANNON, University of Arizona, Tucson
RODNEY SHAW, Consultant, Pittsford, New York

Liaison Representative

SARA CHURCH, Department of the Treasury, Bureau of Engraving and Printing, Washington, D.C.

National Materials Advisory Board

ROBERT E. SCHAFRIK, Director
ROBERT SPRAGUE, Consultant
JANICE M. PRISCO, Administrative Assistant, Project Assistant

ACKNOWLEDGMENTS

The committee is grateful to the many individuals who presented invited briefings on specific technical areas relevant to the production of banknotes, details of particular counterfeit deterrence features, reprographic technology, and the detection of counterfeit bills.

The committee acknowledges the following *industry* representatives:

Barney Barnes, Mars Electronics International: low technology bill validators

Haim Bretler, Director General, SICPA Holdings SA, Switzerland: overview of optical variable ink technology

Tim Crane, Crane & Co.: counterfeit deterrence features in banknote paper

Jim Farrand, James River Corp: overview of innovative security paper

Tom Gazda, Arthur D. Little: market survey on color reprographic equipment

John Haslop, Thomas DeLaRue Corp: counterfeit deterrence features used in world currency, and issues in designing secure banknotes

Bill Jumper and Bruce Radl, Ektron: input scanners and currency inspection methods

Mike Ott, IA Corporation: sensors for high speed Federal Reserve Board equipment

Bill Patton, General Electric Aerospace: engineering considerations of radar reflective paper

Roger Phillips, Flex Products: optically variable pigments

Jim Tsujita, Canon Corporation: counterfeit deterrent features built into copiers and printers

The committee acknowledges the following *government* and *Federal Reserve System* representatives (members of the New Currency Design Task Force are noted by an *):

James Brown* and Craig Einsel, U.S. Secret Service: counterfeiting experience in the U.S. and in foreign countries

Len Buckley, Bureau of Engraving and Printing: banknote designing and engraving

Jon Cameron*, Federal Reserve Board: how the Federal Reserve System operates

John Collins, Bureau of Engraving and Printing: counterfeit deterrent research

Tom Ferguson,* Bureau of Engraving and Printing: role of this study assisting the New Currency Design Task Force in evaluation of counterfeit deterrence methods

Mark Hepfinger, U.S. Army Natick R&D Center: dyes and pigments

Dan Littman, Federal Reserve System, Bank of Cleveland: survey of advanced counterfeit deterrence features

James Reese,* Federal Reserve Bank, Richmond: importance of secure currency

John Stoides,* Currency Technology Office, Federal Reserve System: advances in instrumental methods used by the Federal Reserve Banks to screen banknotes

Robert Stone,* Bureau of Engraving and Printing: issues related to counterfeit deterrent features

The committee is particularly grateful to the Bureau of Engraving and Printing's liaison representative, Dr. Sara Church,* Office of Advanced Counterfeit Deterrence for her active participation at all data gathering meetings and for providing valuable supporting materials and data for the committee's use.

Finally, the committee acknowledges the support of Dr. Robert Schafrik, the senior staff officer at the National Materials Advisory Board (who also assumed the responsibilities first as acting director then director of the board during the course of this study); Dr. Bob Sprague, who provided very able insight and help during the preparation of the report; and Ms. Janice M. Prisco, who provided much appreciated assistance and administrative support throughout the course of the study.

PREFACE

The Department of Treasury's Bureau of Engraving and Printing (BEP) has designed, engraved, and produced U.S. banknotes since 1862. (The BEP has produced all U.S. currency since October 1, 1877.) Having begun with only six employees and borrowed equipment to print $1 and $2 treasury demand notes, the BEP has evolved into a major industrial operation. The BEP now employs 2,300 people who work around the clock. At any given time, as much as $200 million may be in production. In 1991 the Federal Reserve System ordered 7 billion banknotes (all denominations) from the BEP. The 1994 order may be as high as 9.3 billion banknotes.

An important part of the Department of Treasury's mission is the deterrence of counterfeiting. As new and improved reprographic methods have come into use, the Department of Treasury has made changes to banknotes to enhance their resistance to counterfeiting. Specific legislation is not required for a change in the design of currency, since the Secretary of the Treasury is empowered by law to issue paper money in a suitable form (12 U.S.C. 418). But realistically, any change to the design of the currency would not be made without a period of public debate; it is hoped that this report will add value to the debate.

In 1992, the Department of Treasury requested that the National Research Council, through its National Materials Advisory Board, analyze and recommend overt counterfeit deterrence features that could be incorporated into a redesign of U.S. banknotes. Previous studies by the board had assessed counterfeit deterrence features at a time when a major redesign was not undertaken (NRC, 1985, 1987). The major conclusions and recommendations from these studies are summarized in Appendix A. It should be noted that the security thread, implemented in the Series 1990 U.S. banknotes, was one of the recommendations in these reports. This change was the subject of Congressional Hearings (House of Representatives. 1985).

As a matter of historical interest, one of the first studies undertaken by the National Academy of Sciences after its formation in 1863 concerned counterfeit deterrence. The Secretary of the Treasury, in August 1863, requested that the Academy provide advice on ways to eliminate the counterfeiting of greenbacks (Cochrane, 1978). The Committee on Prevention of Counterfeiting was formed and its first confidential report was presented directly to the secretary on January 7, 1864. Until it was disbanded several years later, after counterfeiting ceased to be a problem, the committee analyzed different methods being suggested to reduce counterfeiting.

The major objectives of the current study were to:

- analyze and recommend new overt (e.g., readily visible and recognizable to the general public) counterfeit deterrence features that can be incorporated into U.S. currency in the short term, intermediate term, and long term; and

- assess technological directions of future reprographic techniques that could be used for counterfeiting by "casual" and "professional" counterfeiters.

A committee (of 12 members) with expertise in advanced reprographic technology, chemistry, color, optical science and engineering, paper, physics, security marking, and systems engineering was formed. The committee met six times between June 1992 and June 1993. Invited presentations by experts from industry and government provided data relevant to the production and inspection of banknotes, advanced reprographic technology, and advanced counterfeit deterrence features and methods.

The report reviews and assesses a number of possible counterfeit deterrent features. Conclusions and recommendations are presented to assist the U.S. Treasury Department in developing the design of the next-generation currency, and in ensuring that U.S. currency remains secure well into the next century. Due to the fact that some readers may not be familiar with many of the technical terms used, a glossary is provided at the end of the report for their convenience.

Any comments or suggestions that readers of this report wish to make can be sent via Internet electronic mail to nmab@nas.edu or by fax to the National Materials Advisory Board at (202) 334-3718.

Glenn Sincerbox, Chair
Committee on Next-Generation Currency Design

REFERENCES

Cochrane, R. C. 1978. The National Academy of Sciences: The First Hundred Years, 1863–1963. Washington, D.C.: National Academy Press.

House of Representatives. 1985. Hearing on the Currency Design Act. First Session on H.R. 48. June 18, 1985. Subcommittee on Consumer Affairs and Coinage Committee on Banking, Finance, and Urban Affairs. Serial No. 99-27. Washington, D.C.: U.S. Government Printing Office.

National Research Council (NRC). 1985. Advanced Reprographic Systems: Counterfeiting Threat and Deterrent Measures(U). National Materials Advisory Board. Washington, D.C.: National Academy Press.

National Research Council (NRC). 1987. Counterfeit Threats and Deterrent Measures. National Materials Advisory Board. Washington, D.C.: National Academy of Press.

TABLE OF CONTENTS

TABLES AND FIGURES

TABLES

FIGURES

EXECUTIVE SUMMARY

PROBLEM DEFINITIONS

Highly sophisticated and technologically advanced reprographic systems are no longer the tools of the skilled technician but are widely available to, and accepted by, the general public. Ease of use and versatility, facilitated by user-friendly control panels, permit an unskilled user to make faithful, full-color reproductions of any document. Reproduction quality, ease of access, and relative freedom from discovery combine to create an atmosphere within which many individuals may experiment with the replication of U.S. banknotes: committing the so-called crime of opportunity. To the dedicated semiprofessional or professional counterfeiter, these reprographic machines are turnkey systems that can be purchased on the open market. They are easily installed and permit limited mass production. Law enforcement agencies could be overwhelmed by these counterfeits, since traceability to the source would be very difficult. The quality of the reproduction can be very high, not solely dependent on the skill of the counterfeiter. Even if the total monetary value of counterfeits grows at a modest rate, widespread counterfeiting capability could reduce public confidence in U.S. currency.

Traditional counterfeiting deterrents, such as unique high-quality paper, fine-line engravings and high-pressure (intaglio) printing, were adequate in the past to restrict counterfeiting to the dedicated craftsman with access to a printing press; these have kept counterfeiting to a reasonably manageable level in the United States. However, with the advent of advanced reprographic systems, these methods are no longer sufficient. Indeed, samples provided by the U.S. Secret Service, made on a commercially available color copier, were very impressive and, in the committee's estimation, would have no trouble in passing all but the most demanding visual inspection. Modern deterrents are required that possess a highly visible means of authentication that is difficult to reproduce and is readily observable by an individual unaided, or using low-cost, relatively unobtrusive devices. This latter requirement is important because of the perceived reluctance of the public to appear obvious in the inspection of a banknote.[1] The intent is to make the attempted forgery so obviously different from a genuine note that it is either readily recognized and intercepted at the first pass, or, even better, the counterfeiter decides that it is not good enough to risk passing.

[1]Close inspection of credit cards and checks by point-of-sale personnel is accepted as a matter of course; the committee's opinion is that close scrutiny of banknotes would become acceptable as well if it were done rapidly with few false rejections.

Redesign of the U.S. banknotes is required to accommodate additional counterfeit-deterrent features. The extent of the design changes will depend upon the additional features selected, and which current ones are removed. Changes to banknote design are subject to several constraints. First, the size of the notes should not be changed in a manner that would prevent co-circulation of old and new notes and continued use of vending machines, automated teller machines, change machines, and Federal Reserve Bank sorting and authentication sensors and equipment. Design modifications to the note should not reduce circulation life or produce environmental hazards, either in manufacture, during circulation, or at the time of disposal. Finally, the evaluation of changes must include consideration of the manufacturing capability and cost.

The U.S. Bureau of Engraving and Printing (BEP) is among the world's largest printers of banknotes, and it has a history of introducing innovations in printing equipment. This tradition should certainly be continued as plans are made for time-phasing the introduction of advanced deterrent features. Incorporation of some desirable features may lead to the need for future additional modernization of production equipment and facilities. For example, new intaglio presses would be required to greatly improve the front-to-back registration, and offset printing of some features would be needed if high-resolution lines or dots are required.

MAJOR FINDINGS

U.S. banknotes remain very important to the economy of the United States, and to many foreign countries, as the U.S. dollar is a *de facto* world currency. Thus, the security of U.S. currency is interwoven with the economic well-being of the United States and the U.S. currency's stature in the world.

The conclusions and recommendations presented in the previous National Materials Advisory Board reports, are as relevant today as they were 6 years ago (NRC, 1985, 1987). The potential magnitude of the threat today is at least as great as was projected in those reports and could grow at a faster rate, perhaps geometrically. The print resolution of color copiers and printers will continue to improve and will soon challenge the resolution capabilities of present-day intaglio printing. Therefore, small-size intaglio printed characters or letters (microprinting) introduced on series 1990 banknotes will provide only temporary counterfeiting deterrence. Color reprographics technology continues to advance rapidly. It exhibits exceptional color quality and resolution and is starting to permeate all segments of the market, from business to home. Market growth is proceeding at a fast pace, and many companies are manufacturing color copiers and printers; the resulting competitive pressures are driving unit cost down. Placement of new non-impact color copier and printer systems in 1995 is expected to exceed 2 million units in the United States, and a similar number is expected for the rest of the world.

Widespread availability of advanced reprographic systems and their relative ease of use present an environment for occasional, casual counterfeiting. These systems also provide a convenient base technology for the more professional counterfeiters so that they need onlyconcentrate on simulating the deterrent features and not on the printing process itself. Sophisticated and inexpensive image-processing software is available that can be coupled with

high-resolution scanners and color printers to provide an opportunity for an advanced amateur, such as a computer hacker, to experiment with counterfeiting in relative privacy. These individuals will not only view the task as a challenge but may share their techniques and results over computer networks.

At the present time, the total value of counterfeit notes that enter circulation each year in the United States is relatively small compared with that of all of the currency in circulation. In 1991, the Federal Reserve System handled $265 billion worth of U.S. banknotes. In that same year, $15.1 million in counterfeit notes were passed in the United States. In addition, the Secret Service seized $87 million in counterfeit notes before they entered circulation. Most of these counterfeit notes (90 percent) were produced using a lithographic process; this requires considerable skill, specialized equipment, and special supplies obtainable from a limited number of suppliers (Brown, 1993a).

The amount of counterfeit notes produced using non-impact reprographic technology (i.e., copiers, scanners, and computer printers) is presently small in contrast to that produced by lithographic processes that use specialized equipment. The 1992 data indicates that counterfeits produced using non-impact reprographic technology accounted for $6 million to $8 million of the total amount; these types of counterfeits have been doubling for the past three years (Brown and Einsel, 1992). The most recent 1993 counterfeiting data indicates a dramatic increase in casual counterfeiting using ink-jet technology (Brown, 1993b). These reprographic methods are pernicious, because they do not provide the Secret Service with leads through which the production source can be traced.

The counterfeiting of U.S. currency overseas is also a problem. Interpol, an international police organization composed of 169 member countries, rarely encounters counterfeit notes of currencies that have incorporated sophisticated security features. Most of the counterfeit cases they are investigating deal with U.S. banknotes (87.6 percent; Kendall, 1993). In 1991, $50 million in counterfeit U.S. notes were detected overseas. While part of the overseas problem can be attributed to unfamiliarity with U.S. currency (although this is by no means proven to be true), it may be due primarily to the relative ease with which U.S. currency can be counterfeited compared with the currency of other industrialized countries, most of whom have recently redesigned their currency. Also, U.S. currency is widely accepted throughout the world, making it a prime target for international counterfeiters.

In line with the assessment of the Committee on Next-Generation Currency that these will be the primary methods for counterfeiting in the future, the rate of growth of notes created using color reprographic equipment is growing geometrically. An illustration of how large the problem could become is to assume that the rate of counterfeiting with non-impact reprographic equipment doubles every year until year 2000, as it has since 1989. With this assumption, the present day value of counterfeit currency could grow to $1.6 billion to $2 billion in the year 2000. Obviously, such a large amount of counterfeiting would cause severe problems for the economy. Appropriate actions can, and undoubtedly will, be taken long before counterfeiting becomes a problem of such proportions.

The combination of creative simulation by the counterfeiter and inattentiveness of the general public has permitted some very poor counterfeits to enter circulation. While they are eventually detected and removed with machine-based authentication systems, these are virtually untraceable if made by a copier or printer. Many other nations regularly change their currency designs, oftentimes to add advanced deterrent features. Some of these features are candidates for use on U.S. currency. Information regarding the effectiveness and durability of these features, derived from actual circulation experience, would be highly useful in judging their value as deterrents and suitability for use. At present, however, very little specific information appears to be shared among countries regarding effectiveness, cost, and durability of particular features.

The distinctive feel of U. S. banknotes this is imparted by a combination of intaglio printing and unique paper substrate continues to serve as an important method for banknote authentication by individuals who handle money on a regular basis. The security thread introduced in series 1990 banknotes will be effective once it is present in most U.S. banknotes,[2] and the public becomes more aware of it. There are a number of additional deterrents now being considered for incorporation in U.S. banknotes. A systematic method is required to compare the advantages, limitations, and costs of each.

FEATURE-ASSESSMENT CONSIDERATIONS

Over the course of this study, technical information about numerous deterrent features was gathered from vendors, expert witnesses, the BEP, the Federal Reserve Board, and the Secret Service. This information ranged from conceptual proposals with little or no supporting data to prototypes with extensive test results. A limited amount of data were also available for features already in use on the currency of other countries.

An extensive list of features was generated that represents a wide variety of technologies. Many candidates were based on a common theme. They were considered as a generic class unless a specific implementation exhibited highly advantageous characteristics.

The overall effectiveness of an individual feature was determined by two primary considerations: resistance against technical threat and technical success probability.

Resistance against technical threat assumes success in deploying the deterrent and is a measure of the feature's value as a counterfeit deterrent. This category is subdivided in the four subcategories: (1) visual and tactile recognizability, (2) inherent resistance to copying, (3) resistance to simulation, and (4) ease of machine readability.

Technical Success Probability is a measure of the risk of incorporating a feature into a banknote. This category is also subdivided into four subcategories to identify the primary areas of consideration. These are (1) availability and manufacturability, (2) change to recurring production costs, (3) durability, and (4) capital cost of new or modified production tooling.

[2]The security thread was present in about half the U.S. $50 and $100 banknotes in mid 1993.

Environmental considerations, in manufacture as well as disposal, were discussed where appropriate but not included as specific factors, as the majority of features did not appear to present a hazard. The selection of deterrent features by the BEP for eventual use should include such an evaluation.

The two categories with their eight subcategories form the cornerstone of the committee's evaluation by helping identify the relative strengths and weaknesses of each feature. Some caveats are in order. First, the subfactors are not equally weighted; depending on the threat scenario, some would be more important than others. For example, visual and tactile recognizability is much more important than machine readability when considering detection by the person on the street, whereas the opposite is true when considering machine validation. In a similar manner, the inherent resistance to copying addresses all levels of counterfeiter expertise, from unskilled to highly skilled, while the resistance to simulation targets those individuals willing to perform at least one additional step (the serious hackers and professionals) and will likely discourage the casual counterfeiter as well.

The committee did not expect that any single feature would rank first in all categories, and none did. Hence, the committee thought it was important to understand the intent (target) of each deterrent. In order to provide a multifaceted system of deterrents, consideration should be given to deploying multiple features that complement each other. A well-designed set would address issues of visibility and recognizability under different viewing conditions; require different methods and skills for simulation; and, generally, require too many additional process steps for anyone but the dedicated professional to attempt. Some caution is required, however. The use of too many features could overwhelm the public and thereby reduce the overall effectiveness of the deterrents.

CONCLUSIONS

The increased availability of advanced color copiers and systems composed of a computer-scanner, and printer makes widespread counterfeiting of U.S. banknotes a real and substantial threat. Ready access and ease of use could lead to abuse by “casual” counterfeiters. Copiers certainly pose a significant threat, but the most important threat in the foreseeable future, in the judgment of the Committee on Next-Generation Currency Design, is color scanner-computer-printer systems, aided by the continuing evolution of more-sophisticated image-processing software. These systems also provide additional opportunities for professional counterfeiters.

The system of deterrence used today has been very efficient, as measured by the relatively low rate of counterfeiting in the United States. The combination of a unique paper substrate, security thread (introduced starting in Series 1990 banknotes), fine-line engraved portraits, and intaglio printing has played an important role in this deterrence. The system should not, however, be assumed effective against future threats.

Features that defeat the casual counterfeiter do not necessarily work effectively against professional counterfeiters. Casual, opportunistic counterfeiters do not have the skills,

resources, or determination to defeat sophisticated individual deterrents or combinations of them, whereas professional counterfeiters do have these skills and the resources to simulate or duplicate any single deterrent, and probably most combinations, given sufficient time. Certain combinations of features, rather than features acting alone, offer robust potential for defeating the casual counterfeiter and slowing down the professional. In the committee's opinion, the set of deterrent features need not be the same on all denominations of banknotes. For example, more sophisticated features may be used on the $100 banknote than on a $5 (or $1) note[3].

Many of the candidate deterrent features are effective within a particular set of conditions. For example, diffraction-based optically variable devices, such as holograms or kinegrams, while effective on rigid substrates such as credit cards, at present lack durability on a flexible substrate. Also, these features, though effective against casual counterfeiters, can be easily simulated by even semiprofessional counterfeiters. Metallized or specular reflecting features also offer deterrent protection against casual copying. As with the diffraction-based features, however, there are a number of durability issues. Color-shifting inks, on the other hand, have been shown to be more durable than diffraction-based features and are also effective against the casual counterfeiter if the public is willing to carefully manipulate the banknote to observe the color change. (They are in widespread use in foreign currency, stamps, and other security documents.)

Innovative covert deterrence concepts, such as unique three-dimensional random pattern generation combined with encryption of the pattern, are highly resistant to counterfeiting and effective against all levels of counterfeiting expertise. But they would not at present be a first line of defense, as they require machine sensing, and such devices are not yet available at most points of sale. The first generation of local, built-in intelligence for copiers and scanners, which prohibits banknote reproduction, does not appear to be a universally promising first line of defense either; as presently implemented, these systems store a limited number of banknote designs, and the controller can probably be circumvented by those who are electronically proficient. Also, there are many copiers, scanners, and printers that do not offer this feature.

It appears to the committee that the public in the United States, for a variety of reasons, does not aggressively examine its banknotes and report counterfeits. But it is not obvious to the committee what incentives could improve the situation. (The degree of inspection is probably correlated to experience in finding a counterfeit note.) An appropriately designed reward system may provide more of an incentive for people and businesses to report counterfeit notes. Personnel employed at points of sale who regularly handle cash, are a crucial line of defense (as are vending machines). The committee's opinion is that the casual counterfeiter would be significantly deterred if relatively simple, speedy, and inexpensive point-of-sale devices were commercially available and commonly used to authenticate banknotes. Such devices would detect one or more deterrent features incorporated in the note.

[3]This policy may already be in place. For example, the BEP has not announced plans to incorporate the security thread into the $1 note.

The use of color alone as a deterrent offers little protection against today's advanced copying technology. However, color used in combination with other features can provide enhanced visibility of deterrents and thus aid the general public in identifying counterfeits. Color can also be used to differentiate between different denominations.

It appears technically feasible to incorporate a low-cost application-specific integrated circuit in all color printers and copiers to encode the machine serial number on all output pages in a way that is not obvious. Assuming that such a circuit were tamper proof, it would allow forensic analysis of the copy to identify the owner of the machine that produced the counterfeit. It also would provide law enforcement authorities with the means to determine the volume of counterfeit produced from a particular source. Once the public became aware of this capability, it would serve as an excellent deterrent against casual counterfeiting (Canon, 1990).

Currently, there is no clear association between some of the banknote testing specifications applied by the BEP and the real-world use of currency. This leads to a concern that potentially effective counterfeiting deterrents may be erroneously eliminated from consideration.

A long-term deterrent strategy must anticipate and lead the evolution of reprographic systems and the level of expertise of the counterfeiting community. Technological progress in non-impact printing will continue to be driven by market forces in a never-ending quest for better accuracy and quality, and it is imperative that the Department of Treasury be informed of developments in ample time to respond to future threats. In a similar fashion, there is a considerable amount of basic research being conducted in the academic and industrial community that could have relevance for future counterfeit deterrence. However, the link between this research and the BEP's long-term needs would not normally be made in a timely way unless specific mechanisms were put in place.

RECOMMENDATIONS

Although there are many new features that can be used to deter counterfeiters, the BEP should continue to utilize fine-line engraving, intaglio printing on high-quality pale-tinted paper, and the security thread as methods of deterrence against “classical” printing technologies and present-day reprographics. Future banknote designs should also incorporate additional visible features to serve as deterrents against counterfeiting and as a means for rapid visual authentication. If analysis shows it is cost effective to do so, some of these overt features could be incorporated into a banknote and their existence not publicly disclosed until they are needed to thwart a new counterfeiting threat.

The BEP should implement a system of complementary features on each banknote that create added complexity for simulation by all levels of counterfeiters. They should not, however, constrain their design by a requirement that the same set of counterfeit deterrence features be on all denominations of bills. And although multiple features rather than a single dominant feature should be present on each banknote, the number of announced features

should not be so great that it overwhelms the user or does not allow space for future feature incorporation.

The BEP should redesign U. S. banknotes to include at least some of the features recommended below, making such changes in appearance as are necessary to produce a new series of notes that effectively and efficiently incorporates these advanced counterfeiting deterrents. The recommended features (discussed in detail in a subsequent chapter) fall into three categories: near term, intermediate term, and long term. Within the categories, the deterrent features are not prioritized because of insufficient data relating to implementation issues and the realization that no single feature is adequate protection from even casual counterfeiting.

The committee recommends (listed in alphabetical order) incorporation of at least some of the following visible features in the near term:

- color-shifting inks for printing;
- moiré (alias-generating) line structures, with color added as necessary to enhance the effect;
- security-thread modifications e.g., location or width based on the denomination;
- variable-size dot patterns, with color added to enhance the effect; and
- localized watermarks.

Incorporation of at least some of the following features, requiring inexpensive visual aids for detection at the point of sale, are recommended for the intermediate term:

- infrared inks for printing;
- optically active coated fibers and particles embedded in the substrate; and
- photoluminescent inks for printing.

Longer-term plans for advanced deterrents should include additional development and understanding of the following features:

- diffraction-based holograms and related devices;
- embedded zero-order diffraction gratings;
- laminated paper substrates with selected features;
- metallic or specular woven security features;
- optical fibers embedded in the substrate; and
- random pattern encryption methods.

For the far term, the BEP should continually assess fundamental advances in the chemical, applied physical, and biological sciences for developments that are applicable to innovative deterrent features. Assessment of research in psycho-physics would also be pertinent since a better understanding of how people perceive visible features may provide insight into the selection of the “best” features.

Before any new counterfeit-deterrent feature is implemented, it should be evaluated by adversary-analysis experts to determine how readily it can be defeated. This process would be aided by having a means to quickly produce currency with appropriate design changes.

There are other aspects of a counterfeit deterrent strategy that should be developed along with incorporating new features in banknotes. To begin with, counterfeit-detection education should be emphasized for point-of-sale persons as a priority, and it should be available for the public at large. Potential incentives that would encourage the public to turn in counterfeits should be closely studied to determine which would be effective and not subject

to abuse.

Industry should be encouraged to develop effective point-of-sale aids to assist in banknote authentication. Efforts that will lead to a high degree of authentication, particularly for the higher denomination bills, should be continued.

The Department of Treasury should investigate the cost effectiveness of requiring source identification (e.g., machine serial numbers) to be embedded in images produced by new copier and printer systems that are capable of producing quality color counterfeit banknotes. If it is determined to be cost effective, appropriate U.S. legislation requiring source identification should be encouraged. In addition, the Department of Treasury should strongly encourage the use of sensors built into color copier and printer systems that can recognize and inhibit banknote copying. For this approach to be most effective, a unique, feature with a high signal-to-noise ratio currency should be identified, developed, and applied universally to currency, possibly in conjunction with other nations. The application of this technology to lower-end systems, such as ink-jet printers, should be analyzed. Many of these printers do not now contain the sophisticated electronics necessary to implement this technology, and thus the inclusion of such technology would have a major cost impact. Also, it is unclear how easily these systems can be defeated by a determined, knowledgeable computer "hacker."

To stay ahead of the evolving counterfeiting threats, the Department of Treasury (perhaps led by the BEP) should establish a multiphased program of identifying and evaluating advancements in relevant technologies. Understanding the technological progress in non-impact printing technologies, and which counterfeiting techniques and methods are being employed, would help the Department of Treasury anticipate advances in the sophistication level of counterfeiters so that the type and timing of counterfeit deterrents could be planned accordingly. Appropriate mechanisms to accomplish this can take the form of advisory panels, committees, workshops, and briefings.

In order to link the science and technology research community with BEP needs, the same mechanisms suggested above for keeping up to date with reprographic technology would be appropriate. However, this is such a wide-ranging area that more in-depth preparatory work would be necessary. In order to make maximum use of information about scientific and technological advances in all relevant areas, there should be internal Department of Treasury technical activity to ensure comprehension and proper interpretation of these research reports.

The BEP should continue to reevaluate its current materials, process specifications, and tests against actual use requirements, taking into account that different use requirements may apply to different bill denominations. Correlation should be made between the different failure modes of currency experienced in practice and the suite of specification tests performed by the BEP.

Long-range systematic planning for incorporation of features should be instituted as a regular part of the mission within the Department of Treasury.

Finally, the Department of Treasury should continuously gather data from other nations as to the effectiveness and durability of features such as color-shifting inks and holograms that have been incorporated into their currency.

REFERENCES

Brown, J. 1993a. Presentation by Special Agent James Brown, U.S. Secret Service, to the Committee on Next-Generation Currency Design. June 15, 1993.

Brown, J. 1993b. Personal communication from Special Agent James Brown, U.S. Secret Service. September 1993.

Brown, J., and C. Einsel. 1992. Comments by Special Agent James Brown and Special Agent Craig Einsel, U.S. Secret Service, to the Committee on Next-Generation Currency Design. June 15–16, 1992; September 1–2, 1992; and October 21–22, 1992.

Canon. 1990. Apparatus for Image Reading or Processing. European Patent Application EP 382,549. August 16, 1990.

Kendall, R. E. 1993. Letter from R. E. Kendall, Secretary General, Interpol, to the Committee on Next-Generation Currency Design. April 5, 1993.

National Research Council (NRC). 1985. Advanced Reprographic Systems: Counterfeiting Threat Assessment and Deterrent Measures(U). National Materials Advisory Board. Washington, D.C.: National Academy Press.

National Research Council (NRC). 1987. Counterfeit Threats and Deterrent Measures. National Materials Advisory Board. Washington, D.C.: National Academy Press.

1

INTRODUCTION

A nation's ability to print money to enhance trade and commerce is critical to its sovereignty. It is difficult to imagine a modern economy functioning smoothly without conducting some financial transactions with paper money. At this juncture, achieving a “cashless” society appears to be a very long-term prospect[1]. It has been estimated that there are approximately 50 billion banknotes (all currencies) in circulation worldwide (Murphy, 1992). The U.S. Bureau of Engraving and Printing (BEP), one of the world's largest printer of banknotes, produces 7 to 9 billion banknotes per year worth over $80 billion for the Federal Reserve System; about 93 percent of these new notes replace those that are destroyed, and the remainder are used to satisfy the increased demand. During 1991, the Federal Reserve System handled 13.6 billion banknotes that had a total value of $265 billion (Cameron and Stoides, 1992).

The earliest paper money is reported to have appeared in China's Sichuan Province at the end the tenth century. Its use is attributed by some to the difficulty that mercantile traders experienced in handling large quantities of coins. Marco Polo is generally credited with introducing the concept of paper money to the West, presumably as a consequence of his travels to China at the end of the thirteenth century. Although different countries adopted various implementations of paper money, they all shared an important, common characteristic: the currency had intrinsic value payable to the bearer of the note. Since these notes were not registered to any individual, their anonymity was quickly recognized by counterfeiters as providing a lucrative target: a problem that persists to this day.

In order to reduce counterfeiting, early societies exacted severe penalties for forgery. Chinese notes of the early Ming dynasty (1368-1644) carried this warning: Whoever forges notes or circulates counterfeit notes shall be beheaded. Whoever reports and apprehends a counterfeiter shall receive a reward of 250 silver tael and the counterfeiter's entire property (Kranister, 1988). Forgery was a hanging offense in England from 1697 to 1832. During this period, approximately 600 counterfeiters were condemned to death, but even this threat of severe punishment did not eliminate counterfeiting[2].

[1]The New Directions Committee of the Institute of Electrical and Electronics Engineers cites achieving a cashless society as one of the grand challenges for electrotechnology (IEEE, 1993).

[2]Interestingly, the penalty was eased after the public became outraged at the Bank of England's lackadaisical approach to producing a note that was resistant to counterfeiting.

Thus, forgery has been a threat for centuries. The old axiom is still true: What one man can do, another can copy. Throughout history, people have received and passed money without detailed examination. Counterfeiters have exploited this behavior by realizing that they do not have to make an exact copy, but only one good enough to pass once.

Governments know that if the public could readily recognize fakes, counterfeiting would become very risky and unprofitable. This line of reasoning has led to the incorporation of security features in banknotes. Banknote producers have used a variety of methods that include unique, complex methods of printing not generally commercially used; unique materials, such as watermarked paper, not available to the general public; distinctive images, designs, and patterns developed by artisans, which are easily recognizable but difficult to duplicate; and public education regarding recognition of genuine notes.

It is instructive to examine how the United States solved the most severe counterfeiting problem in its history. The U.S. Civil War of 1861-1865 represented a peak period for American forgers[3]. It has been estimated that about one-third of the paper money in circulation in 1863 was fake. This caused significant erosion of confidence in the federal government. A key factor leading to this problem was the approximately 1,600 state and private banks with the authority to design and issue notes independently. In 1863, Congress standardized American banknotes by instituting a single national currency. However, counterfeiting continued relatively unabated. As a result, President Lincoln established the Secret Service in 1865 as a law enforcement agency dedicated to the elimination of banknote forgery. The Secret Service was very successful in forming investigative units that tracked down and prosecuted counterfeiters. Consequently, faith in American money was quickly restored.

This success story was aided by two critical elements: (1) only a few counterfeiters accounted for the preponderance of the problem; and (2) counterfeiting required specialized skills, equipment, and materials that could be traced. At the same time, counterfeit-deterrence features were being added to the banknotes to make them more difficult to copy. For instance, in 1861 green ink was first used for printing American banknotes in order to counter the threat posed by the cameras of that age that only used black-and-white film (Kranister, 1988) Also, in 1869 the U.S. Treasury began printing paper money on a controlled, high-quality watermarked paper that featured wide vertical bands of dark blue jute fibers embedded in the paper substrate.

In 1879, the paper specification was changed to “pure linen stock, with continuous colored (red and blue) silk lines or threads running parallel to each other from top to bottom of each cell. . . in addition colored (red and blue) silk fibers were introduced into the pulp” (BEP, 1963). These bands of colored threads were determined to be a sufficient deterrent, the watermark was eliminated.

No significant changes in distinctive features of U.S. banknotes were made until the introduction of redesigned notes in 1929. The size of the note was reduced by 25 percent,

[3]From an earlier point in U.S. history, the well-known cliché “Not Worth a Continental” was the result of widespread counterfeiting of currency issued by the Continental Congress, which was greatly encouraged by the British.

resulting in significant cost savings. The localized silk threads were discontinued and replaced with small, distributed red and blue fibers. The planning for these changes had started 20 years earlier, in 1909. An important feature was the standardization of a particular portrait each denomination banknote to prevent counterfeiters from easily "upping" the value of a note by only changing the denomination. There were many differences of opinion to resolve in the process, such as selection of the portraits, the denominations they would be used for, colors for overprinting on the faces, the color of the back, and so on.

The design of American banknotes has not undergone major changes since 1929. Since that time, the U.S. dollar has become a *de facto* worldwide currency. Also with the advent of advanced imaging and printing methods, the dollar's resistance to counterfeiting has begun to decrease. Changes to U.S. currency which were introduced as late as 1991, attempted to forestall a major redesign of the dollar while providing additional security against the newer threats[4]. At the present time, the number of counterfeit bills produced using the new color copiers and printers is still small, but the rate has been doubling for the past three years. This has set the stage for a close examination of the design and materials used in U.S. banknotes so that a future crisis can be avoided[5].

There are many possible deterrent features that could be employed. Some of these features are already in use in other countries and could be incorporated in U.S. currency very quickly; some could be ready for incorporation within a relatively short time; and others require further development effort and thus would not be available for some time. The critical issue is: Which features should be added to provide increased counterfeit deterrence for the next 5 to 10 years? In order to address this question properly, the following factors must be taken into account:

- What counterfeiting scenarios are likely to be employed in the foreseeable future?
- Which counterfeit deterrent features have the most promise, based on technical considerations?
- What unchangeable constraints and design limitations are imposed by the currency manufacturing and distribution system?
- What is a reasonable trade-off between security and added cost?

This report addresses these issues and makes a number of recommendations concerning the strengthening of U.S. banknotes against counterfeiting.

[4]These changes were the security thread and microprinting around the portrait.

[5]It might be observed that the forecasted primary threat (many casual counterfeiters employing readily available equipment and supplies) is the inverse of the two critical elements that helped the Secret Service successfully halt counterfeiting after the Civil War (few counterfeiters using specialized equipment and supplies).

REFERENCES

Cameron, J., and J. Stoides. 1992. Presentation by J. Cameron and J. Stoides, Federal Reserve System, to the Committee on Next-Generation Currency Design. June 15, 1992.

Krevsky, Seymour. 1993. President's Message. Engineering Management Newsletter 4(3), July. Pg. 1. New York: IEEE Engineering Management Society of the IEEE.

Kranister, W. 1988. The Moneymakers International. Cambridge, England: Black Bear Publishing, Limited.

Murphy, C. 1992. A license to print money. Atlantic 169(6): 26-18.

2

U.S. BANKNOTE COUNTERFEITING THREATS

There is increasing concern about a new counterfeiting threat enabled by continuing significant advancements in color non-impact printing and related technologies. Beginning in 1983, a number of studies were sponsored by the BEP and the Federal Reserve Board to examine this emerging threat (Arthur D. Little, Inc., 1986; Batelle Columbus Laboratories, 1982; NRC, 1985; Price Waterhouse, 1983; Sheldrick and Pickett, 1985; Sheldrick et al., 1983). All concluded that the increasing availability of very capable color copiers and printers, at lower and lower prices, posed a very serious threat to U.S. currency and that more effective anticounterfeiting measures would soon be required to maintain a reasonable degree of deterrence.

The primary purpose of this chapter is to update these prior threat assessments, taking into account changes that have occurred over the course of the six years since the last National Mateials Advisory Board study. Projections of the availability and accessibility of advanced non-impact color printing technology and general technical trends are presented, and the most important threats are identified. (Appendix B describes advancements in non-impact printing technologies in greater detail.) Various classes of counterfeiters are explained, along with the general types of deterrents required to neutralize them. The last two chapters of this report then provide specific recommendations and suggested strategies that respond to the threat assessments discussed in this chapter.

COUNTERFEITING TRENDS

In 1991, $17.1 million in counterfeit notes—25 percent of the counterfeits produced in the U.S.—were reported to have entered the commercial mainstream in the United States. Those that were not culled out along the way were removed by the Federal Reserve System, where they were identified using covert features and highly effective sensors. Another $87 million in counterfeit banknotes was seized by the Secret Service before entering circulation. According to the Secret Service, counterfeiting is increasing by 4–6 percent each year. The latest data for fiscal year 1993 (October 1992 through September 1993) indicate that $20 million in counterfeit banknotes entered the commercial mainstream in the United States (Brown, 1993a). In addition, during that fiscal year, $121 million in counterfeit U.S. notes was seized worldwide at the production source (i.e., before they entered circulation (Brown, 1993a).

Currently, 90 percent of counterfeit banknotes are produced in the United States lithographic methods, and this is also true of counterfeits made outside the United States (Brown, 1992). This type of counterfeiting is usually performed by a professional, since it requires skill, as well as specialized equipment and supplies. These counterfeiters must produce large enough quantities of counterfeit notes to recover their investment in time and effort. Typically, the number of notes printed have been large enough to permit the Secret Service to trace the source and seize the bogus notes.

The total value of counterfeits produced by color copiers and printers is small now, on the order of several million dollars, but it has been doubling every year since 1989 (Brown and Einsel, 1992). The increasing counterfeiting rate plus the rapidly increasing number of color copier and printer placements over the next few years (discussed later in this chapter) are major reasons that the government is concerned about the integrity of U.S. currency and is actively engaged in a deterrence program. In 1990, $1 million in counterfeit banknotes were produced by office machine copiers. In 1991, this doubled to $2 million, and in 1992 the amount increased to $6-8 million.

The fastest growing fraction is being made by ink-jet technology (Brown, 1993b). Ink jet printers make up the largest color printer population. For the 9-month period from October 1, 1992, to June 30, 1993, the U.S. Secret Service has observed a dramatic increase in ink-jet counterfeits. Prior to this time, only a few notes were produced using ink jet copiers or printers. But during this period, the number "exploded" to 205 geographically dispersed occurrences in separate, apparently unrelated cases. They accounted for 2,283 notes, with a face value of over $66,000. The low number and value of the notes indicate that most of them can be attributed to casual counterfeiters. Table 2-1 shows the distribution of occurrences by denomination. The $20 note was the one most frequently counterfeited.

Table 2-1. Counterfeits Produced by Ink-Jet Technology, October 1992 through June 1993

Denomination	Separate Occurrences[a] (Cases)	Total Number of Notes Passed	Average Number of Notes Passed Per Occurrence
$1.00	2	2	1
$5.00	8	80	10
$10.00	29	253	9
$20.00	115	1524	13
$50.00	20	157	8
$100.00	31	244	8

[a] An occurrence is a set of identical counterfeit notes.

Figure 2-1 shows the distribution of the counterfeiting instances for $20 notes. Even though the overall average is 13 notes per occurrence, it is clear that most of the cases involved the passing of only a few counterfeit notes. For example, there were 23 instances in which only a single note was passed and 18 instances in which only two notes were passed. The horizonal axis of this graph is truncated at 25 $20 notes per case. In addition, there was one case of each of the following quantities being passed: 32, 34, 45, 50, 52, 86, 137, and 432. These larger quantities are less indicative of activity by a casual counterfeiter and more indicative of a petty counterfeiter (these different classes of counterfeiters will be discussed later in the chapter).

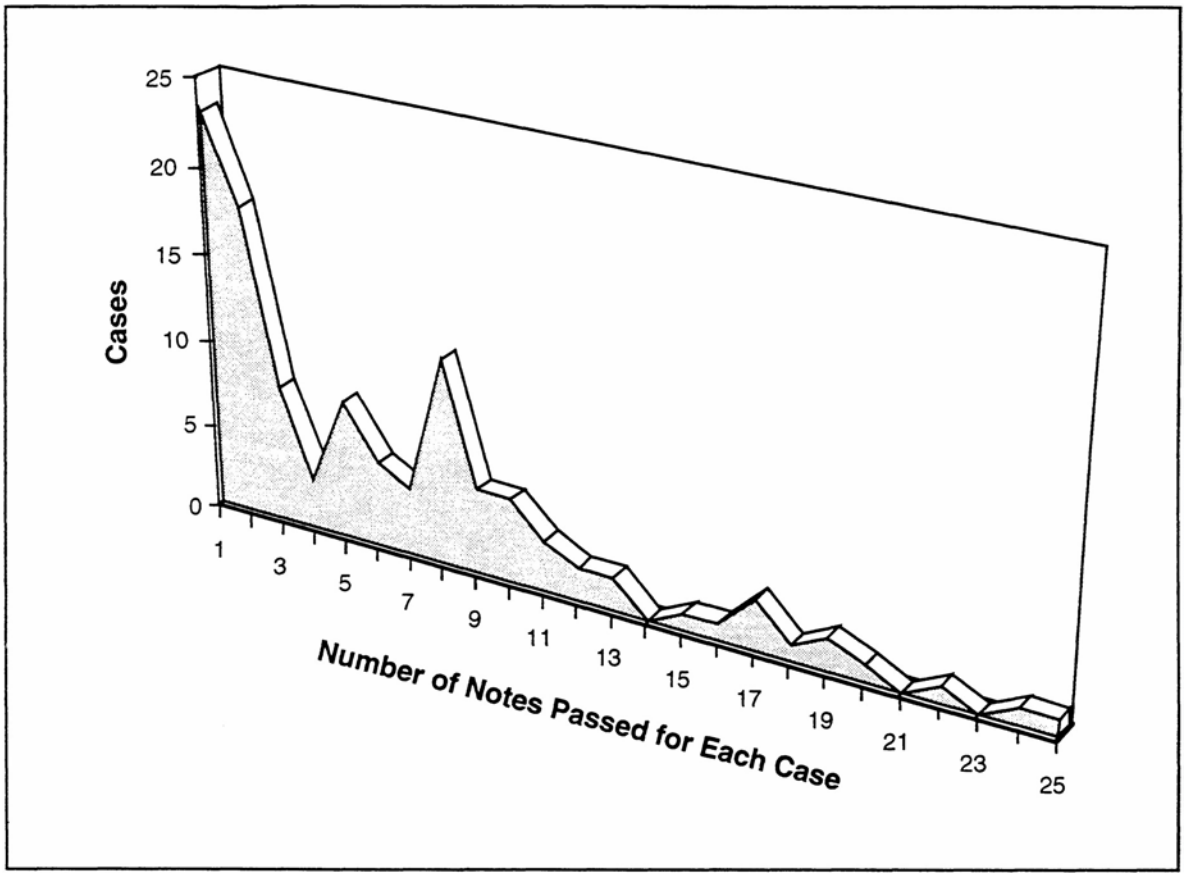

FIGURE 2-1 Cases of counterfeiting $20 notes using ink jet technology.
Source: US Secret Service Data, Sept 1, 1992-June 30, 1993

The counterfeiting of U.S. currency overseas is also a problem. Interpol, an international police organization composed of 169 member countries, rarely encounters counterfeit notes of currencies that have incorporated sophisticated security features. Most of the counterfeit

cases they are investigating deal with U.S. banknotes (87.6 percent; Kendall, 1993). In 1991, $30.7 million in counterfeit U.S. notes were reportedly detected overseas. However, these data are not comprehensive, since there is, at present, no system in place worldwide that reports all incidents of counterfeiting to the U.S. Secret Service; thus the overseas counterfeiting problem may be greater than the figures mentioned in this report indicate. While part of the overseas problem can be attributed to unfamiliarity with U.S. currency (although this is by no means proven to be true), it may be due primarily to the relative ease with which U.S. currency can be counterfeited compared with the currency of other industrialized countries, most of whom have recently redesigned their currency. Moreover, U.S. currency is widely accepted throughout the world, making it a prime target for international counterfeiters. As one measure of the problem, U.S. travelers are beginning to experience difficulty in exchanging U.S. currency overseas. For instance, many Japanese banks are very relunctant to accept $100 U.S. banknotes due to their concern about counterfeit notes (Japan Times, 1993).

Also, not all acts of counterfeiting are solely motivated by profit; state-sponsored counterfeiting can be done to embarrass or lessen the influence of another country in world affairs, or wage economic warfare (Kranister, 1988). The United States is not immune to such attacks by such counterfeiters who possess essentially unlimited resources.

ASSESSMENT OF THE TECHNICAL THREAT

To date, most printing and copying in the office or home has been text oriented. Since text can relay its information content in low-cost black-and-white or low-cost impact printers, non-impact color printers are not currently dominant. However, the advent of high-resolution color monitors in the office and the requirements of presentation graphics have helped create the growing demand for color printers and copiers in the office that can reproduce high-quality color images. The committee envisions that desktop color printers will become one of the fastest growing areas in the domain of reprographic technology during the next decade. In order to satisfy the emerging demand, increasingly sophisticated and capable color copiers, scanners, and printers are being developed and sold worldwide by more and more companies[1]. As usual, selling price varies inversely with volume and competition. Consequently, placements of systems that can scan originals and produce color reproductions are growing rapidly. They are being purchased not only for businesses but also by individuals for home use. Thus, rather powerful “counterfeiting” equipment is becoming commercially available at readily affordable prices. All indications point to a low cost desktop color system (less than $5,000) being available by 1995 and becoming cheaper and more widely placed by the turn of the century. Historically, key counterfeit-deterrent features were selected because they were difficult to

[1]Advanced, color non-impact reprographic technology has been used in niche applications, such as for proofing and final color copy by the graphics art industry, but these costly systems, on the order of $100,000, have not been widely available.

reproduce. However, modern imaging and printing technology is making such rapid advances that many deterrent features will come under severe challenge. For instance, in the past, the art of a craftsman has been used to make fine-line engravings that are then printed using a high-pressure printing technique (intaglio printing) to provide realistic portrayals of shadow, highlight, and detail. These images could only be approximated by any other process. However, advanced reprographic equipment has sufficiently fine resolution detail and color fidelity to very closely simulate the appearance of intaglio images and many other visible security features. The proliferation of printers and scanners is making it much easier to do quick, quality reproduction in the office environment.

Equipment

Electrophotography, electrostatics, ink jet, and thermal transfer are the four technologies on which virtually all color copiers and printers are based. There are recent indications that reasonable quality color can also be produced using magnetic toners; thus, magnetic printing technology is a fifth relevant technology. At this time, most of the color copiers are based on electrophotography, because it is the only technology that permits direct optical input, that is, the use of a photoconductive image-sensing element. Computer scanners use a similar technology to digitize an image. All the other types of printers respond to electronic input directly, so there is no light-sensing component.

Ink-jet and thermal-transfer copiers are available and are attractive, because the process is less complex than electrophotography and less expensive. However, at the present time, the output quality from those types of copiers is generally not as high as from the other technologies. But the technology is advancing. For example, the new top-of-the-line thermal transfer copiers provide very good color images.

The front and back of a note could be scanned and recorded on floppy or rigid magnetic disks and the disks themselves circulated among counterfeiters. Converting this digital information to color copying is then simple using ink-jet or thermal-transfer printers attached to a microcomputer.

For the professional counterfeiter, two approaches to high-speed color printing appear to be gathering considerable momentum. In one, a floppy disk containing the requisite color image information is used to make lithographic printing plates (Bruno, 1993). Electrophotography, electrostatics, and other processes permit easy, rapid, inexpensive production of such plates (Bruno, 1993). In the other, the aforementioned non-impact printing processes are being modified and improved to permit printing at speeds of 300 ft/min and higher (McMillian, 1993). Such high rates have already been demonstrated in black and white with the electrophotographic, electrostatic, ink-jet, and magnetic technologies. Color electronic printers operating at even higher speeds are beginning to become available.

Thus, potential counterfeiters have a wide choice of equipment. The high-speed and most-sophisticated machines are the most expensive. However, anyone with a personal computer can now purchase a reasonably good computer scanner for a few hundred dollars and a basic ink-jet or thermal-transfer printer for $1,000 or less.

General Technical Trends

Perhaps the most significant technical trend is the continuing improvement in print quality. Every new product reproduces finer detail (600 dots per inch is rapidly becoming the present standard) along with more of the original color gamut (Sutherland, 1993). Tonal range, once considered to be very limited, is no longer a problem[2].

Another important trend is the increased ease of use, reliability, and reproducibility of the equipment. Most new machines require virtually no skill to operate correctly, since embedded sensors linked to sophisticated control systems ensure reproducible results. The machines are also essentially maintenance free, only requiring simple replenishment of supplies.

Most color copiers are not now designed for two-sided printing. Copiers capable of printing on two-sides are beginning to appear on the market, but they are not designed for accurate front-to-back registration[3]. However, there does not appear to be a technical barrier to eventual incorporation of the registration techniques used in lithography or gravure printing if the marketplace demands it.

Unit Placements and Selling Prices

When the previous National Materials Advisory Board studies were performed during the period 1985 to 1987, there was very limited market information on advanced copiers and printers. In 1985, only two companies offered color copiers (Ling, 1986). Both were based on electrophotographic technology and were very expensive, costing more than $40,000. Although color was available in many lower-cost ink-jet and thermal printers, it had not yet become popular. Within one year, two more companies introduced color copiers that were also based on electrophotographic technology; prices were somewhat below those of the first copiers. By 1987, five companies were known to be developing photographic-quality color electrophotographic printers, and three others were working on low-cost color copiers. The target selling price was $10,000-$15,000 (Ling, 1986). Projections for 1992 included much higher resolution, better print quality, and greater reliability.

In the intervening years since 1987, there have been formal studies of the non-impact-printer color market. Accordingly, there is now more accurate information about units placed,

[2]It is now possible to reproduce as many as 256 color tones in electrophotographic and electrostatic printers and 100 or more in ink-jet and thermal-transfer printers.

[3]Recently available two-sided color copiers include the Canon 550, Afga's chromapress, and Indigo; the last two copiers are electronic printers.

average selling prices, etc., as well as with market trends. Following are averages of projections from three independent sources of market data plus information available to individuals on this committee (Hard Copy Observer 111, 1993; Prechowski, 1993; Testan, 1992).

One measure of market size and growth rate is the number of competitors. In 1992, there were 21 companies manufacturing color copiers and printers. In that same year, there were approximately 30,000 color copiers in use in the United States. Worldwide figures for color copiers and printers are about twice those cited for the United States. U.S. unit placements in 1992 were about 11,000 and are expected to have an annual growth rate of at least 26 percent through 1996. It is estimated that there could be 110,000 color copiers in use in the United States by 1966 (Testan, 1993). About 70 percent of these are forecasted to be electrophotographic. These projections are graphically depicted in Figure 2-2. The estimated number of color copies to be made in the United States in 1994 is about 2 billion, a large increase from the 500,000 copies produced in 1989.

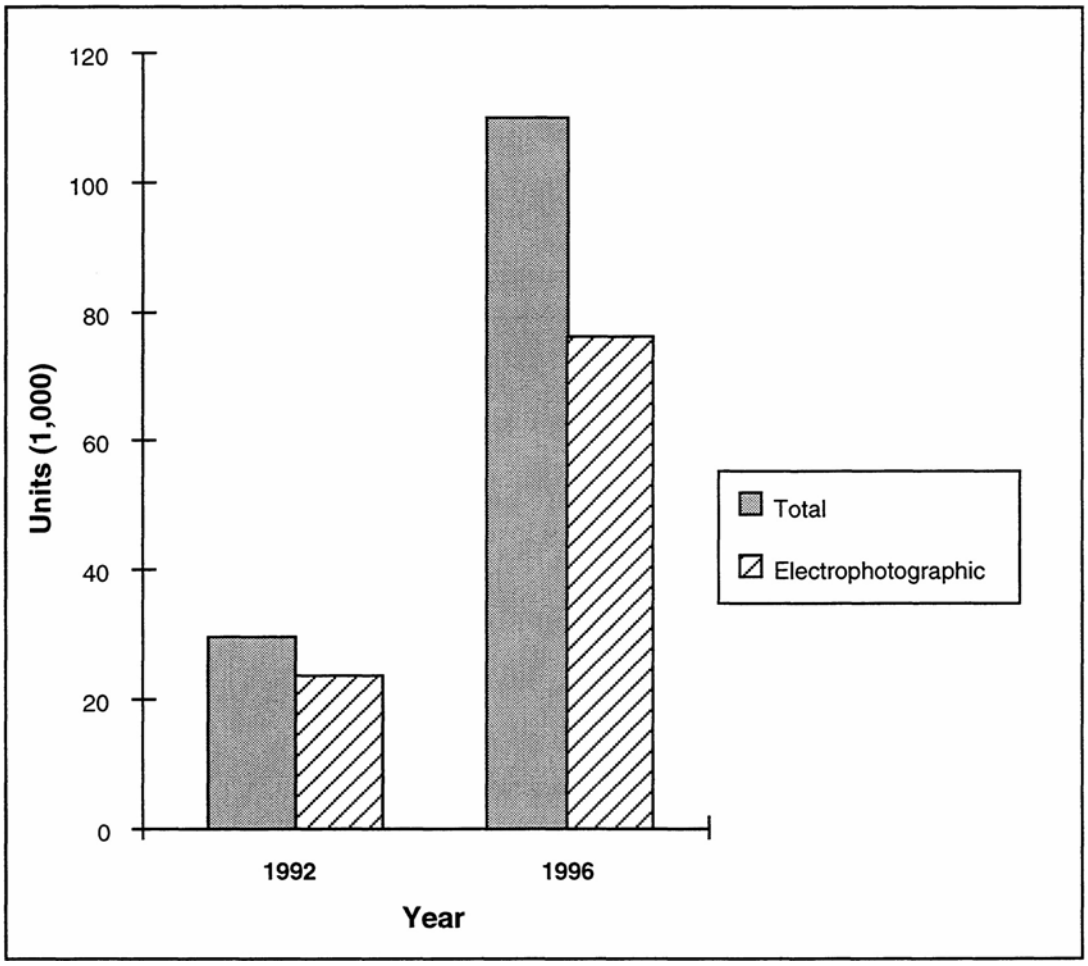

FIGURE 2-2 Trend in color copier year placements.

The average selling price of electrophotographic units was $36,000 in 1987. There is now a color electrophotographic copier on the market that sells for $13,500, and further price reductions can be anticipated (Gazda, 1992). A color laser printer suitable for use in small offices and homes for the output from personal computers has just been announced at a list price of $12,500. Additional manufacturers are expected to introduce similar products later in 1993 and early in 1994.

Non-electrophotographic copiers will be much less expensive. Present prices of color inkjet and thermal-transfer units are on the order of $9,000 to $10,000. Reductions to $5,000 to $7,000 are anticipated over the next year or two. An ink-jet printer has been announced for less that $5,000 (Testan, 1991).

One of the conclusions of the former National Materials Advisory Board studies (see Appendix A) was that color printers constituted a much greater counterfeiting threat than color copiers, because the cost is much lower, and they are part of personal computer systems that are themselves inexpensive and ubiquitous. Current information has strongly reinforced that earlier conclusion. Thirteen companies offer color printers; only three of them also manufacture color copiers. U.S. unit placements of non-impact color printers totaled 121,000 in 1991, (Testan, 1993), (compared with 953,000 impact printers; i.e., 9-pin and 24-pin dot-matrix printers). The placements of non-impact color printers are projected to increase to 644,000 in 1993 and to approach 2.5 million units by 1995. This placement trend, depicted in Figure 2-3, is indicative of an estimated annual growth rate over the next 3 to 5 years of 58 percent (Testan, 1993). The estimated 1995 cost of these printers is summarized in Table 2-2

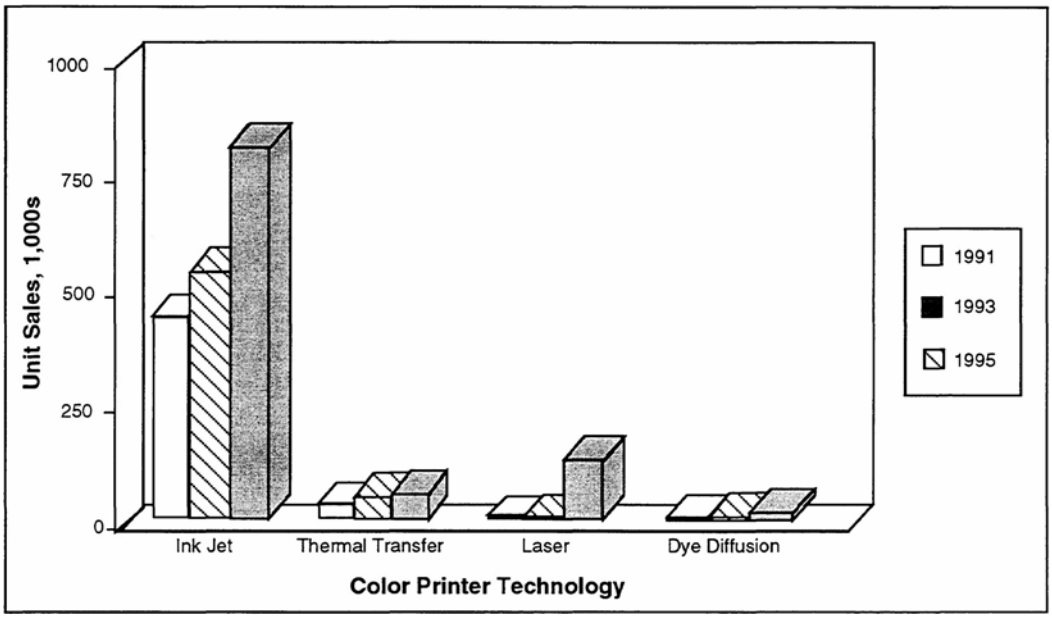

FIGURE 2-3 Trend in non-impact color printer placements.

(Testan, 91). Due to favorable performance and price, ink-jet printers could make up as much as 95 percent of the new printer placements by 1995 (Gazda, 1992; Testan, 1993).

Table 2-2 Estimated 1995 Non-Impact Color Printer Costs

Printer Technology	**Estimated 1995 Cost**
Ink Jet	$1,000 or less
Thermal Transfer	$3,000
Laser	$4,000 to $5,000

Thus, by 1995, there will be on the order of 4.9 million color printers associated with personal computers (many of which will have peripheral scanning devices) in the United States, and 4 million worldwide. Such systems will be extremely capable of reproducing a banknote.

Summary of the Technical Threat

The greatest technical threat to the printed currency of the United States is the result of

- dramatic improvements in non-impact color reprographic equipment that have enabled very good color copies to be made and that allow the machines to function with only simple periodic replenishment of supplies;
- competitive pricing that has allowed the average user to buy equipment that only the specialist had access to before (permiting the creation, editing, communication, production, and reproduction of color images for almost any users); and
- advances in technology that have pushed reprographic hardware resolution to limits only dreamed of a few years ago (e.g., 600 dpi in monochrome is the de facto standard in 1993, with gains to 1200 dpi in the future).

While color printing and reproduction is becoming a multibillion dollar business, it is reducing the security of printed documents, such as banknotes. Looking into the future, it does not appear that there will be an immediate push for resolutions to go beyond 600 dpi in mass market use because that level of resolution is ample for the applications. The rapid improvements in ink-jet printers, which will become even less inexpensive but more capable, will most likely lead to the ink-jet printer becoming the predominante printer employed by the casual counterfeiter using a computer. Color copiers and printers using electrophotography will have wide placements in offices and will be the preferred method at first.

The professional counterfeiter already has a wide array of non-impact printing methods to choose from and will soon join in the electronic revolution as better technology becomes widely available at lower cost.

TYPES OF COUNTERFEITERS AND REQUIRED GENERAL DETERRENTS

Counterfeiters can be considered to fall into three classes. The first group is composed of individuals who are not normally considered hardened criminals. The second group commits crimes but has limited skills and resources (e.g., petty criminals). Finally, there are the professional counterfeiters possessing considerable skills and resources. This latest group may, at times, be aided and abetted by governments pursuing economic sabotage against, or embarrassment of, another country.

Class I: Opportunistic Counterfeiters

There appears to be convincing evidence that counterfeiting is not necessarily the sole province of hardened criminals. For example, there is related experience regarding the making of illegal reproductions of intellectual property items that are protected by copyrights (e.g., computer software, audio-recordings, etc.) when the danger of being caught is remote and the task is easy (OTA, 1986). A 1988 survey by the Office of Technology Assessment found that 40 percent of a nationally representative sample of Americans over the age of 10 had tape recorded music during the past year aided by advancements in recording technology that have made it very easy to inexpensively produce high quality copies in the home (OTA, 1986). (The increased use of digital representations for music, and video, is expected to continue this trend since nearly perfect copies can be made.) The Office of Technology Assessment estimates that there are more than 1 billion instances per year of unallowed copying of audio recordings. Most of these copies are for personal use, not for sale, so the analogy to counterfeiting is far from perfect. But, it does indicate that many people will violate the law if there is a compelling reason, the means to do it, and little chance of apprehension.

A conclusion reached by former Committees of the National Materials Advisory Board, (NRC, 1985) resulting from considerable inquiry, was that some individuals, generally not considered to be inveterate criminals, would produce counterfeit currency if:

- the opportunity presented itself;
- the probability of being caught was perceived to be small;
- the need for temporary funds was great; and
- it was viewed as a benign crime.

Two typical potential scenarios considered were

1. A worker in a relatively sophisticated office has access to color copiers and printers. Such a person might have an sudden need for several hundred dollars. At the end of a workday, that person could be tempted to see how easily currency could be reproduced. If the result is a close duplicate of the original, that individual might try the bill in a money changing machine or attempt to pass it. If the attempt is successful, that person might become an occasional counterfeiter with no consistent pattern, making apprehension very difficult.
2. The same type of person described above could have a home computer equipped with a scanner, a disk drive, a color monitor, and a color printer and be relatively free to experiment in privacy. By 1995, such a system might be purchased for about $2,500.

Another scenario of concern is that casual counterfeiting could become the "in thing" to do, such as around college campuses. Persons with more technical knowledge than a casual counterfeiter, but not necessarily "criminals," could try counterfeiting for the challenge; such a group, known as "hackers," could present a particularly formidable law enforcement problem. Hackers, within the definition applied by the committee, are a technologically knowledgeable group motivated more by the challenge, than by pure criminal intent (which is not to suggest that they are not criminals if they break the law).

The probability of the U.S. Secret Service catching random, infrequent counterfeiters is small at the present time for a number of reasons. First, the general public and proprietors of small businesses usually accept currency without carefully inspecting it. U.S. Secret Service experience indicates that even very poor reproductions are accepted, at times, even in broad daylight. There is also a disincentive for the public to closely inspect currency, because discovery of a counterfeit note leads to a monetary loss when the bogus bill is surrendered to the Secret Service as required by law. Machines that change $10 and $20 bills for lower denomination currency present a low-risk target for counterfeiters, because they will either accept the bogus bill or unobtrusively return it to the counterfeiter.

Based on these scenarios and the behavioral assumptions, the most effective deterrents against casual or opportunistic (Class I) counterfeiters, except for hackers, would be those that result in copies that are obviously different from bona fide currency, and not passable without substantial additional effort being required to correct the errors. Such deterrents could be present in the currency itself or could be built into the scanning or copying equipment.

Class II: Petty Counterfeiters

These individuals are committed to a life of crime. They may be skilled, but they do not have access to significant resources. These semiprofessionals would be intent on counterfeiting and willing to exert considerable effort to produce generally acceptable reproductions. Available deterrents would be effective if they were not easily simulated or reproduced and if the features were targeted against the different means of copying that could be employed, including photography and offset printing. It also appears advisable to include a deterrent feature that can be readily detected by a money changing machine. Thus, multiple deterrents will enhance the probability of discouraging these types of counterfeiters and will improve the chances of apprehension by law enforcement. These deterrents would also be effective against the hackers discussed above.

Class III: Professional Counterfeiters

These individuals usually work in groups and may, in the extreme cases, have access to equipment similar to that of the BEP. This class of counterfeiters includes state-sponsored efforts in which the available resources can be considered infinite. It is assumed that such organizations, given sufficient time and resources, could detect and simulate or reproduce any and all visible deterrents. Furthermore, they can print in large quantities.

Defeating this class of criminals requires the incorporation of a suite of covert and overt deterrents. In addition, the deterrents or their combinations must be changed at intervals frequent enough to make counterfeiting a large and difficult job. At least one of the deterrents must permit its presence or absence to be sensed in money changing machines. This deterrent may have to be changed from time to time, along with the sensor.

The Principal Threat

Although the semi-professional and professional types of counterfeiters are best able to defeat counterfeit deterrents, the committee does not think that they constitute the greatest threat to U.S. currency. In general, they produce such large volumes of bogus notes, purchase such special equipment and supplies, and involve such a large number of people that the U.S. Secret Service can normally find enough leads to track them down.

The greatest threat to U.S. currency, in the committee's judgment, is the Class I counterfeiter; that is, the casual, opportunistic type. This class would leave no traceable pattern, and the sources would be so numerous and so widely distributed as to make them virtually impossible to track. Accordingly, one of the main objectives of a currency redesign effort should be to defeat the Class I counterfeiter.

Of almost equal importance is the need to make counterfeiting extraordinarily difficult for the petty criminal (Class II) and the hacker, who are willing to exert considerable effort (but with limited resources and equipment) to make reasonable reproductions of U.S. currency.

REFERENCES

Arthur D. Little, Inc. 1986. Assessment of New Technologies Applicable to Image Generation and Reproduction Needs of BEP. BEP-85-28 (N). Cambridge, Mass.: Arthur D. Little, Inc.

Batelle Columbus Laboratories. 1982. Assessment of the Timing and Nature of the Threat to Counterfeiting U.S. Currency. Final Report to the Board of Directors of the Federal Reserve System, Contract 3975. Columbus, Ohio: Battelle Columbus Laboratories.

Brown, J. 1992. Personal communication from Special Agent James Brown, U.S. Secret Service. June 15, 1992.

Brown, J. 1993a. Personal communication from Special Agent James Brown, U.S. Secret Service. October 8, 1993.

Brown, J. 1993b. Personal communication from Special Agent James Brown, U.S. Secret Service. September 1993.

Brown, J., and C. Einsel. 1992. Comments by Special Agent James Brown and Special Agent Craig Einsel, U.S. Secret Service, to the Committee on Next-Generation Currency Design. June 15–16, 1992, and October 21–22,1992.

Bruno, M. H. 1993. The printers new role in digital printing. The IS&T Reporter 7(3):1–4.

Gazda, T. 1992. Presentation by T. Gazda, Arthur D. Little, Inc., to the Committee on Next-Generation Currency Design. September 1992.

Hard Copy Observer III. 1993. QHS beats rivals to punch with first office color laser. C. Le Cohpte, Ed., No. 6 (June): Pg. 30-34.

Japan Times. 1993. Bogus Bills, Strong Yen Lead to Limits on Exchanges. Business Notes. October 8, 1993. 11.

Kendall, R. E. 1993. Letter from R. E. Kendall, Secretary General, Interpol, to the Committee on Next-Generation Currency Design. April 5, 1993.

Kranister, W. 1988. Governments as Counterfeiters. Pp. 62–64 in The Moneymakers International. Cambridge, England: Black Bear Publishing.

Ling, G. 1986. Verbal presentation on review of xerographic color copying and printing as a preview of future requirements. Conference on Color Hard Copy. Monterey, California, June 15–17, 1986. Boston, Mass: Institute for Graphic Communications. .

McMillian, T. 1993. (Verbal Communication) The promise of portable color. Computer graphics world. September 1993. p. 30.

National Research Council (NRC). 1985. Advanced Reprographic Systems: Counterfeiting Threat Assessment and Deterrent Measures(U). National Materials Advisory Board. Wash.: D.C.: National Academy Press.

Piechowski, R., ed. Print Business Register. No 8 (April 19): Pp.1-4. Vol. 8. News Item p.4.

Price Waterhouse. 1983. Implications of Increased Counterfeiting. Final Report to the Bureau of Engraving and Printing, Contract No. TEP-85-80. Washington, D.C.: Price Waterhouse.

Sheldrick, J. E., and G. E. Pickett. 1985. Summary of Battelle Research Related to Counterfeit Deterrence for the Board of Governors of the Federal Reserve. Presented to the U.S. Currency Study Committee, National Academy of Sciences, January 3, 1985.

Sheldrick, J.E., J. D. Robbins, R. Cooper, G. E. Pickett, and J. H. Lindhold 1983. The Impact of Emerging Technologies on Counterfeiting U.S. Currency. Final Report to the Board of Governors of the Federal Reserve System, Contract 3975. Columbus, Ohio: Battelle Columbus Laboratories.

Sutherland, D. 1993. Kodak tackles the color calibration curve. Computer Graphics World. Vol. 8 (April) 84.

Testan, P. 1992. Overview of Color Non-Impact Printer Market. Proceedings of Eighth International Congress on Advances in Non-Impact Printing Technologies. Pg 1-3. Springfield, Va.: Society for Imaging Science and Technology, .

Testan, P. 1991. Personal communication.

Testan, P. 1993. Personal communication October.

OTA. 1986. Intellectual Property Rights in an Age of Electronics and Informations. OTA-CIT-302. U.S. Congress, Office of Technology Assessment. Melbourne, FL: Kreiger Publishing Co.

3

ASSESSMENT METHODOLOGY FORCOUNTERFEIT-DETERRENCE FEATURES

REQUIREMENTS

The U.S. government must identify those features and combinations of favorably interacting features most likely to reduce the threat of counterfeiting in a cost-effective manner. The general requirements suggest that: (1) the authentic feature(s) should be obvious to the public, and a copy should be obviously different from the authentic feature; (2) the cost-effectiveness of the features must be determined early in the process of planning for banknote design changes; and (3) the features must be nontoxic and nonhazardous.

It appears imperative that more than a "representative" list of features be examined; what is necessary is a careful assessment of all individual and combined features likely to reduce the counterfeiting threat for "reasonable" investments.

The key to such an assessment lies in giving operational meaning to terms like "reduce" and "reasonable." The Committee on Next-Generation Currency agrees with the prior National Materials Advisory Board study in concluding that color copiers and printers used by casual counterfeiters constitute the greatest near-term threat of counterfeiting (NRC, 1985). "Reduced" risk was therefore focused upon, but not limited to, reduction of this threat.

"Reasonable" investment was benchmarked by determining the cost of the security thread used in today's higher value notes. This cost of $0.013 per note was used by the committee as reasonable for any proposed deterrent features. As reference point, the cost for printing banknotes in 1991 totaled $30 per thousand notes—that is, 3 cents each- (Federal Reserve System, 1991).

The committee agreed that the width and thickness dimensions of the banknote could not practically be changed without causing a major change in the infrastructure supporting the handling of cash. However, it would be possible to vary the length by denomination, up to the present standard length.

THE "PERFECT" VISIBLE FEATURE

The ideal counterfeit-deterrence feature can be described as having the following characteristics (Church and Littman, 1992):

- extremely difficult to duplicate;
- easily recognized by the general public (readily visible with little manipulation);
- durable (passes all BEP evaluation standards and is visible even after considerable wear);

- can be machine readable;
- easy to produce at low cost;
- acceptable to the public (aesthetically pleasing); and
- nontoxic and nonhazardous.

While the "perfect" feature was not identified, the committee decided that the most realistic feature (or combination of features) is one that reduces the threat of counterfeiting more cost effectively than any other individual feature (or combination of features). The committee believes that nearly all currently incorporated, as well as candidate, individual features can be at least simulated, and in many cases duplicated, by a dedicated professional counterfeiter. Therefore, the individual features were evaluated for the purpose of identifying advantages, limitations, and issues so that they could later be appropriately combined into a set of mutually reinforcing features.

TIME FRAME FOR POTENTIAL INCORPORATION

The committee was interested in features that realistically meet the above criteria and could be implemented successfully within 2 to 5 years. If a feature could be incorporated readily with little additional development work, it was judged as a *near-term* opportunity. If some additional development was required, such as time to prepare a specification, perform durability tests, etc., it was judged *an intermediate term* opportunity (i.e., closer to 5 years than to 2 years for incorporation). If a feature was assessed as probably being unable to be implemented within 5 years, it was considered for implementation in the *longer term.*

EVALUATION STRATEGY

The evaluation of many different features was complex and multidimensional. There are many candidate features, and nearly every feature can have several variations. There are also a variety of threats that must be addressed (see Chapter 2), and there are inevitable questions about a particular feature's technological feasibility, cost, and deterrent effectiveness.

An approach that could yield insight into the trade-offs involved when comparing the relative potential of different features was necessary. It was also essential to have a mechanism by which the relative benefits and limitations of features to counter various counterfeiting threats could be cataloged and assessed on a continuing basis. Such mechanism would allow for evaluation criteria to be changed as technology, threats, costs, and other conditions evolved.

Importantly, a framework was needed to assist in formulating specific strategies to thwart counterfeiting using consistent, measurable, and defensible criteria. Since no single feature by itself is ideal, one strategy for determining the final suite of features would be to select combinations of features that are mutually reinforcing. (This issue is discussed further in Chapter 5.) These and other objectives motivated the committee to adopt a structured approach to add discipline to the evaluation process.

A structured methodology that would help organize, track, and document the evaluation process was selected. The methodology-multi-attribute utility assessment—has been used for a variety of similar evaluation problems and is widely known in the operations-research and decision-analysis worlds. This criteria-based approach to problem-solving in general, and to technology assessment in particular, has often proven effective.

The essence of the methodology is the identification of a set of requirements that may be stated initially in vague or general terms, the conversion of the requirements into indicators or criteria, the weighing of criteria in terms of their relative importance, and the scoring (or ranking) of the alternatives with reference to the criteria.

EVALUATION FRAMEWORK

The committee first developed two categories of evaluation criteria. These were *resistance against the threat* and *technical success probability.* They formed the basis from which a deterrence merit could be assigned to deterrent features, taking into account the incorporation potential. These major rating categories were subdivided into the four subcategories described in *Table 3-1 and Table 3-2*. Individual features were first rated according

Table 3-1 Resistance Against the Threat

FACTOR	DESCRIPTION
Visual and Tactile Recognizability	An assessment of the ease with which a U.S. citizen (who typically does not closely examine a banknote) could readily recognize the feature in normal ambient illumination unaided, or aided with a simple, inexpensive device.
Inherent Resistance to Copying	The “strength” of a deterrent feature, from basic principle considerations, to resist duplication by available or soon-to-be-available reprographic methods. Takes into account how far into the future a feature is expected to be effective, given anticipated advancements in the threat.
Resistance to Simulation	The ease with which a “good enough” copy of the feature can be made to fool the typical nonexpert.
Ease of Machine Readability	An assessment of how easily the feature can be authenticated using instrumental aids that could be readily available.

to the criteria in Table 3-1, *resistance against the threat.* A feature's evaluation was scored as *"high," "medium,"* or *"low,"* depending on how well the committee expected it to perform from an understanding of the basic physical mechanisms involved.

If a deterrent feature rated high for some categories, but low in others, the committee assessed whether the low rating could be improved by further development effort or if it was due to an inherent limitation. If development seemed feasible, then research opportunities were identified.

If a fundamental limit was involved, a determination was made regarding any potential role the feature might play in complementing another feature. If the committee could not determine such a role, the feature was not considered further. However, if the committee felt that a feature might have a future role, the evaluation proceeded to the consideration of factors in Table Table 3-2, which includes availability and manufacturability, recurring cost, durability, and capital cost. If any of the data needed for these categories were not available, that aspect of a feature was rated unknown; this meant that additional time and effort would be required to "fill in" the missing blanks. Thus, features with "unknowns" were not considered for near-term implementation but were considered for longer time frames.

Table 3-2 Technical Success Probability

FACTOR	DESCRIPTION
Availability and Manufacturability	A measure of how readily the feature can be obtained for incorporation in U.S. currency. Included is a consideration that a feature's availability should be tightly controlled and monitored so that it does not become publicly available.
Change in Recurring Cost	An assessment of the additional recurring cost required to incorporate the feature, using the current banknote with a security thread as the baseline.
Durability	Expectation that the feature can continue to serve as a viable deterrent as it undergoes wear while in circulation.
Capital Cost	An assessment of the amount of additional equipment that the BEP will have to purchase to produce the feature.

Two of the subcategories in Table 3-2 deal with cost. Figure 3-1 shows the BEP's current distribution of cost for printing banknotes (Church and Littmen, 1992). Material and capital equipment account for 37 percent of the cost.

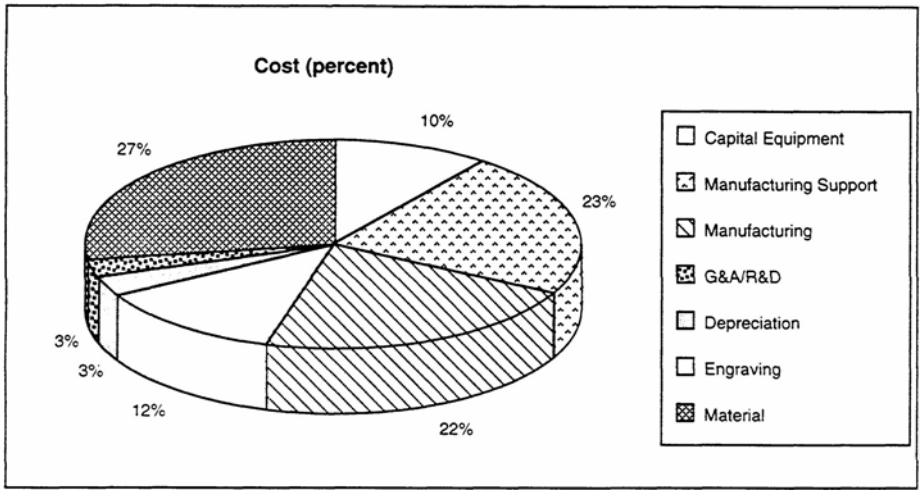

FIGURE 3.1 Distribution of BEP currency printing cost.

The committee organized the currently used and candidate deterrent features into the following groups: substrate-based, design-based, ink-based, post-printing, and other. The ratings of individual features within categories were then compared, and all obvious differences were examined to ensure that features were rated uniformly.

The committee analysis of deterrent features recommended for BEP banknote incorporation was not prioritized. This is due to two factors: (1) a lack of sufficiently detailed analysis of incorporation difficulty (an activity that logically emanates from, rather than precedes, this study) and (2) a realization that no single feature is adequate protection from even casual counterfeiting.

REFERENCES

Church, S., and D. Littman. 1992. Presentation by Sara Church, Bureau of Engraving and Printing, and Dan Littman, Federal Reserve System, to the Committee on Next-Generation Currency Design. October 21, 1992.

Federal Reserve System. 1991. A Comprehensive Assessment of U.S. Currency Quality, Age, & Cost Relationships, Washington, D.C.

National Research Council (NRC). 1985. Advanced Reprographic Systems: Counterfeiting Threat Assessment and Deterrent Measures(U). National Materials Advisory Board. Wash. D.C.: National Academy Press.

BIBLIOGRAPHY

Edwards, 1976. W. How to Use Multi-Attribute Utility Measurement for Social Decision Making. Los Angeles: University of Southern California.

Edwards, W. 1979. Multi-Attribute Utility Assessment. Beverly Hills, Calif.: Sage Publications.

Barclay, S., R. V. Brown, et al., 1977. Handbook for Decision Analysis. McLean, Va.: Decisions & Design, Inc.

Andriole, S. J., 1980. Handbook of Problem-Solving. Princeton, N.J.: Petrocelli Books, Inc.

Andriole, S. J., Ed. 1986. Microcomputer Decision Support Systems: Design, Implementation & Evaluation. Wellsey, Mass.: QED Information Sciences.

Adelman, L., 1992. Evaluating Decision Support and Expert Systems Technology. New York: John Wiley & Sons.

4

DESCRIPTION AND ASSESSMENT OF DETERRENT FEATURES

A number of features are now being used in U.S. currency to deter counterfeiting, and many additional ones are being considered for future use to respond to the projected threats. This chapter contains a description of and results from the committee's assessment of categories of counterfeit-deterrence features that represent a wide variety of technologies. In line with the objectives of this study, the emphasis is on those features that are visible to the unaided eye. But less obvious features that can be easily inspected using relatively inexpensive aids have also been included. The first section discusses the features that are currently incorporated in U.S. banknotes. The following section discusses candidate features, grouped by generic classes. The last section is a summary of the recommendations.

Discussion of two types of visible deterrent features is contained within this chapter: passive and active. A passive feature is one that is difficult to reproduce or simulate in its own right; if it is copied or simulated, the fake can be detected by examining the quality of the reproduction. An active feature may not be an obvious feature on a genuine note; however it interacts with the reprographic process in some way, resulting in an obvious indication on the duplication attempt. The security thread is an example of a passive feature; an aliasing pattern is an example of an active feature.

Within the discussion of each feature class is a description of the feature, its significant advantages and limitations, and the committee's assessment. The committee was guided by evaluation framework (presented in the previous chapter) in performing the assessment.

In some instances, a strong synergistic deterrent effect was found between features that were placed in different classes. Each class was assessed separately, but where appropriate the discussion points out the possible increase in effectiveness if one feature is used in conjunction with another. For instance, color by itself was not assessed to be a particularly effective deterrent; but the effectiveness of moiré patterns can be enhanced through the appropriate use of color. Suggested criteria for integrating multiple features are further discussed in the next chapter.

CURRENTLY USED OVERT U.S. COUNTERFEIT-DETERRENCE FEATURES

U.S. currency presently in circulation has a number of features that serve to deter counterfeiting. Some of the features can be authenticated at points of sale through unaided visual inspection by inspection using a low-power magnifier or similar simple device. Other features require relatively sophisticated instrumental aids and will not be discussed further. This report focuses on overt, visible features that serve as counterfeit deterrents.

Paper

U.S. currency is printed on a special paper composed of cotton and linen fibers with no wood fibers or starch. Stringent specifications describe the fiber configuration, thickness, weight, color, and reflectance to ensure uniformity and durability of the paper (BEP, 1991). It has a distinctive feel that is readily detectable by many people who handle large amounts of currency; they can easily identify counterfeits that are not printed on the appropriate paper. Many of the counterfeits are detected at points of transaction by having a wrong “feel.” This distinctive paper, in combination with intaglio printing, provides significant counterfeit deterrence at a moderate cost. The BEP requires strict control of currency paper to ensure that it is not available to potential counterfeiters. Unauthorized possession or control of this or similar paper is a criminal offense. While it is theoretically possible that counterfeiters could make paper that is identical to the U.S. currency paper, it would be a major effort, requiring significant technical expertise, equipment, and monetary resources.

Red and Blue Fibers

U.S. currency paper contains red and blue fibers that are added to the paper slurry and become randomly dispersed throughout the paper. These fibers are observable visually; however, it requires close inspection in good lighting to detect them. The fibers represent a deterrent to the professional counterfeiter who must add two colors to his palette for a high-quality forgery. However, the red and blue fibers can be simulated by drawing red and blue lines with a pen or pencil or, possibly, by printing them. Such simulations would most likely pass casual visual inspection but not careful inspection with a magnifier. The casual counterfeiter will most likely find the color copy reproduction of the fiber quite adequate. The red and blue fibers do not provide a high level of counterfeit deterrence for detection at points of sale, but they are relatively inexpensive. They could also be enhanced, as discussed in a later section.

Intaglio Printing and Fine-Line Engraving

The intricate designs used in existing U.S. banknotes represent a significant deterrent feature that is already in place. The variations in the fineness and depth of the line work,

which are produced by master engravers, give an intaglio-printed note its characteristic embossed or raised "feel" (Buckley, 1992). The variation of line width in a portrait or a sculptured border gives an appearance of gray-level and depth to the imagery that is very difficult to reproduce—most counterfeit notes simply do not look "right."

Intaglio is a complex printing process commonly used for printing high-security documents. The process starts with the fabrication of master printing plates containing the fine-line engraving, incised by hand by skilled engravers. The master plates are used to produce the production plates that are used in the printing presses. Intaglio printing presses require a specially formulated high-viscosity ink that is applied to the grooves in the plate. The plate is wiped to remove all of the ink except what is captured in the grooves. The plate is then pressed against the paper under a very high pressure (typically 7,500 to 15,000 psi) to transfer the ink and emboss the paper (Graminski, 1993a). The plates are wiped clean after each impression. (Generally, approximately 15 percent of the ink actually is transferred to the banknote. Graminski, 1993b). The remainder is removed during the wiping operations.)

The embossing effect and the thick layer of printed ink causes the printed lines to be raised, giving the notes a distinctive look and feel. This produces lifelike portraits that cannot be exactly duplicated in counterfeits made by other printing processes or by copiers and printers. Similarly, the complex, unbroken fine-line patterns in the borders of the notes and in the backgrounds of the portraits are not duplicated well by lower-resolution copiers or printers.

The intaglio printing process is used for the black print on the front side of the notes and the green print on the back side. The Treasury seal, Federal Reserve seal, and serial numbers are printed by a typographic or letterpress process. In a letterpress, the characters to be printed are formed by raised surfaces on the printing dies. A roller applies ink to these raised surfaces and then the die is pressed against the paper to transfer the ink.

Microscopic inspection reveals unique characteristics of intaglio and letterpress print that distinguish them from other types of print. For example, the high pressure applied to the ink when the printing plates are pressed against the paper during intaglio printing forces ink into the spaces between the paper fibers, beyond the edges of printed lines. In letterpress printing, the pressure between the plate and the paper tends to squeeze ink to the edges of the raised characters, leaving an obviously thicker layer of ink along the boundaries.

Figures 4-1 through Figures 4-3 contain a series of photomicrographs, taken at 11-power magnification, of the eye in the engraved portrait of Alexander Hamilton on a $10 banknote. Figures 4-1 is the image as printed by the BEP using the intaglio process. The distinctness of the lines and the bleeding of ink (or "feathering") along the fibers is evident. Figures 4-2 is a photomicrograph of the same area that has been photocopied. Note the loss of detail and the inability of the process to reproduce the sharp lines. The toner particles are clearly evident.

Figures 4-3 is a photomicrograph of the same area again, this time from a counterfeit note produced using the lithographic process. Again, the image is clearly different from the intaglio one. The raised border and loss of definition can be seen. The amount of detail is greater than that of the photocopies note, but less than that of the intaglio printed note. In addition, the tactile feel of U.S. currency is extremely difficult to exactly reproduce using other printing or duplication methods. The committee judges intaglio printing of fine-line engravings to be an effective deterrent, particularly if a low-power magnifier is used as an aide for detection.

FIGURE 4-1 Photomicrograph of intaglio printed image.

FIGURE 4-2 Photomicrograph of photocopied image.

Figure 4-3 Photomicrograph of lithographic printed image.

However, the intaglio printing equipment employed by the BEP has several limitations that prevent some potential deterrent features from being incorporated. For instance, those counterfeit-deterrence features that depend on accurate registration of printed features between the front and back sides of the note would not be possible to produce on the existing intaglio equipment, even assuming ideal conditions. The BEP prints currency in 32-note sheets. The green print forming the backs of the notes is printed first and allowed to dry. Then the black print for the front side is applied. The very high pressure produced by the printing plates tends to stretch the paper. This causes errors in registration between the front and back images, even if the sheets have been placed into the press very accurately. Exact registration would require simultaneous, or near simultaneous, printing of the front and back images.

As another example, the current BEP intaglio equipment is limited in its ability to print additional colors. Multiple colors can be printed by selective inking of the printing plates. However, only a restricted number of fountains are available in which to hold additional ink colors.

Serial Numbers

There are two serial numbers printed in the same green ink as the Treasury seal on the face of each note. No two notes of the same series, bank, and denomination have the same serial number. The Federal Reserve banks are designated by a letter and a corresponding numeral. The first character of the serial number is a letter that designates the Federal Reserve Bank and matches the letter in the Federal reserve seal. The corresponding numerical designation of the Federal Reserve Bank is printed in four locations on the face of each note.

The serial numbers and Federal Reserve Bank designators are faithfully copied on counterfeits made by copiers or electronic printers. A large number of copies of the same note, with the same serial number and bank designators, is subject to detection by alert point-of-sale or bank personnel. The serial numbers and bank designators are a more effective deterrent to the printing of notes on printing presses. The relationship among the features is not commonly known, although it is public information. Even professional counterfeiters are not aware of the simple relationship. But neither are personnel at points of transaction. Therefore, it is not normally used as a means of counterfeit detection. Making notes with different serial numbers complicates the printing process for the forger.

The denomination of each note is printed in intaglio in each corner on both sides of the notes and is spelled out in the lower border. It is also printed in black ink where it is overprinted with the green Treasury seal. The large number of denomination indicators is a deterrent to attempts to upgrade notes by simply altering the denomination numbers in the corners of the notes. Also, a distinctive portrait on the front of the note is associated with a particular denomination, as is a distinctive back. (This was one of the important changes made during the last major currency-redesign effort, which occurred in 1929.)

Security Thread

The BEP began incorporating a security thread in the Series 1990 banknotes. It was first introduced in the $100 notes and then subsequently in the $50, $20, and $10 notes. This thread is a thin metallized polyester strip 1.4 to 1.8 mm in width, and 10 to 15 μm in thickness (BEP, 1990). It is placed in the paper during its manufacture. It is located in the clear field between the border of the note and the Federal Reserve seal. The letters “USA” and the denomination of the note are printed on the thread. The thread is contained within the paper substrate so that it is not observable in reflected light and cannot be reproduced by the reflected light of copiers. The thread and its printing can be detected visually in transmitted light. A deliberate action (holding the note up to the light) is required for visual detection of the existence of the thread and especially to read the printing on it. It is the committee's opinion that at the present time, the public is not generally aware of this security feature or how to authenticate it. Therefore the security thread's deterrence potential has not yet been fully exploited.

The thread can be simulated to pass casual inspection by drawing, printing a white line with an opaque white ink, or pasting on a thin sheet of paper. It would be easy to simulate the printing on the thread using the latter approach. If the simulation was done first, followed by the banknote printing, the simulated thread would be more difficult to detect as a forgery.

Even though the security thread was not originally developed to be easily machine detectable, readers are available that can detect the existence and the location of a metallized thread; these readers can be fooled if the counterfeits contain a metal strip or wire in the appropriate location.

The security thread has been incorporated into 45 percent of the $100 and $50 notes in circulation worldwide; status for lower denominations are not available. It will be incorporated into $5 notes in 1994. When most of the notes in circulation have the security thread (estimated to be 1995) and the public is educated better about its existence and how to authenticate it, the security thread will be a reasonably effective counterfeit deterrent.

Microprinting

Concurrent with the introduction of the security thread in the Series 1990 banknotes, the words "THE UNITED STATES OF AMERICA" have been printed repeatedly around the portrait in a very fine line, 6 to 7 thousands of an inch wide. The print appears as a thin line to the naked eye, but the lettering can easily be read using a low-power magnifier. The resolution of most current copiers is not sufficient to copy this fine print, but equipment beginning to appear in the marketplace has sufficient resolution to copy it. The microprint is at the limit of resolution of the intaglio printing process; therefore, it will not be possible to use intaglio microprint to deter reproduction by higher-resolution copiers and printers.

Color

The light-green tint of authentic currency paper is difficult to reproduce and is one feature distinguishing this paper from commonly available paper. Since currency paper contains none of the fluorescent whiteners that are common in commercial papers, it will not fluoresce under an ultraviolet light. This provides a simple means of detecting suspicious notes, but is not a foolproof method. For example, genuine notes that have been washed might exhibit fluorescence due to whiteners present in laundry detergents.

Overall Assessment of Existing Visible Features

The existing counterfeit-deterrence features cannot be authenticated easily and unobtrusively by inexperienced and untrained personnel at points of sale.

- Detecting the unique feel of authentic currency paper requires experience in handling currency. But the feel of the paper changes with wear.
- The distinctness of intaglio printed images can be observed with a low-power magnifier, but this requires experience (and time) to do. And, the richness of the intaglio images becomes harder to discern as the banknotes wear in circulation.
- The simple relationship between the serial numbers and the Federal Reserve Bank indicators is not known by most cashiers. It does require a certain amount of concentration.

Most people do not pay particular attention to serial numbers and will rarely notice multiple bills with the same serial number.

- The red and blue fibers can be detected only with a very close inspection in good lighting.
- Reading the microprinting requires the use of a magnifier; but the advanced copiers and printers that are becoming widely available will be able to satisfactorily reproduce it.
- The polyester strip can be detected only by holding the note so it can be observed in transmitted light.

In summary intaglio printed fine-line engravings on a yellow-green tinted paper has been very effective in the past in allowing the general public to readily identify notes that “aren't right.” However, with the availability of high-quality color copiers and printers, these deterrents will become much less effective over time. As has happened before in history, the existing overt counterfeit-deterrence features of U.S. currency require upgrading to respond to new counterfeiting threats that are driven by advanced technology.

INNOVATIVE VISIBLE COUNTERFEIT-DETERRENCE FEATURES

A number of innovative counterfeit-deterrence features have been proposed for incorporation into U.S. currency. These features can be categorized as substrate-based, printed, multicolored, design-based, post-printed optically variable, and random pattern with encryption and as deterrents built into copiers and printers.

Substrate-Based Features

The use of a particular, high-quality paper substrate represents the first line of defense of U.S. currency. As currently produced for Series 1990 bills, the paper stock incorporates a number of security features, including a denominated metallized polyester security thread, red and blue fibers, and a distinctive tint. The physical properties, fiber composition, and surface treatment are closely specified and subjected to careful quality control. Substrate-based deterrent features cannot be exactly reproduced and are therefore particularly attractive deterrent features. A large number of additional substrate-based features have been suggested, and several of these are currently employed in foreign currencies. An assessment of the generic types of substrate-based features follows.

Laminated Substrates

The ability to produce currency paper by joining two half-thickness sheets with or without a very thin plastic interleaf provides many possibilities for the introduction of deterrent features to the substrate (James River, 1993). For example, designs, images, or text can be printed on what becomes the interior of the note. Such printed information would not be visible in reflected light but would be apparent on viewing in transmitted light. If a plastic interleaf is employed, transparencies could be introduced. In effect, then, the current features

of the security thread could be extended over the entire note. The sophisticated paper-making technology that is available to produce and join the half-thickness sheets makes this a potentially attractive deterrent.

The committee views the laminated substrate as a system capable of incorporating multiple security features. These systems in paper/paper, paper/plastic and plastic/plastic laminates have undergone substantial development and are in use for some security document applications (paper/paper) and, in one case for currency (plastic/plastic in Australia). The promise of this technology recommends a careful monitoring of the progress in their development and experience in various applications. The ability of the adhesive that joins the laminates to withstand intentional separation of the layers is a particular area of interest.

Skilled counterfeiters could probably readily simulate these laminates, as well as any of the features contained within the laminate. They would not be concerned with durability of the note, making the task much easier than that of the genuine paper maker. Paper splitting and re-bonding with glue is one possible simulation route; another would involve bonding two thin sheets of paper.

Plastic Substrates

As mentioned above, plastic can be substituted for paper as the substrate material, as has been done in Australia for its $10 note. Plastic provides a smoother surface for microprinting, and hence finer details can be printed. It also makes it relatively easy to introduce transparencies. The plastic may itself incorporate various additives and deterrent features. Some increase in substrate durability may be anticipated but there may be problems with heavy creasing in the bills leading to premature cracking (Haslop, 1993a).

There are a number of problems with using plastic substrates for a note. First, the feel of a plastic note would be substantially different from that of a paper note. It may be more difficult to develop a distinctive feel for a genuine plastic banknote, as has been done for the current paper ones. And thin plastic material is readily available and would be impossible to restrict. Also, plastic is currently more expensive than paper. Many of the security features associated with paper substrate (e.g., watermarks) are not possible with a fully plastic substrate. But similar features are possible; for example, a shadow image can be produced in the plastic coating that can have the same functionality as a watermark. it's also sensitive to the ink composition and printing parameters regarding durability issues such as ink adherence, temperature, and humidity effects.

Most of the benefits associated with a plastic substrate can be achieved with laminated paper structures, or innovative extensions to the current substrate material. All of the U.S. experience and testing procedures are based on the current substrate material. At this time, there does not appear to be a significant enough advantage to plastic substrates to overcome the cost of conversion.

Enhanced Security Thread

A security thread has been introduced in Series 1990 currency in denominations of $10 and higher. As currently specified, the threads do not fluoresce under ultraviolet illumination; they are not visible in reflected light but are clearly readable to the unaided eye in transmitted

light. The committee recommends that the position or width of the thread, which currently is essentially the same for all denominations, be varied by an obvious amount to permit denomination discrimination on the basis of position or width alone. In addition to their assistance to the casual viewer, such changes would assist in machine recognition.

A change in position would have to be carefully designed to avoid occlusion by another feature, such as a printed image. The center of the note should also be avoided, since that is where bills tend to be folded. As an alternative, the number of threads could be varied depending on the denomination. Both the wider thread and the incorporation of more than one thread raise concerns about creating weak zones in the substrate. Analysis would be required to determine if delamination and reduced note durability would result from these changes.

The committee was shown an example of a forged note with a simulated security thread, complete with microprinting. Though this note was not fully convincing, one cannot assume that the thread as currently employed will deter the dedicated professional counterfeiter. However, it is highly effective against the casual photocopy, which does not copy the thread.

Two enhancements to polyester security threads have been incorporated in foreign currencies. A windowed thread is used in British, German, Turkish, and Bahrainian currency, while Finnish notes use an imbedded thread with holographic printing (Haslop, 1993a). The current supplier of security paper to the BEP could implement a windowed thread following some development effort (Crane, 1993).

The security thread could be enhanced by combining it with other features. For example, if the thread were overprinted with characters using a photoluminescent ink, the characters could potentially be made to appear obvious on a reprographic copy. There are many potential combinations of other features that could be used to enhance the security thread. These should be studied for long-term implementation. The experiences of other countries in similarly enhancing their security threads should also be closely monitored.

Watermarks

Watermarks have been used in paper since handmade papers were produced in Italy at the end of the thirteenth century. It is estimated that some one million different watermarks were used before the introduction of machine-made papers in the nineteenth century. Watermarks have been widely employed for centuries as a means of marking high-value documents. For instance, authentication of rare prints and drawings often involves the study and identification of the watermarks contained in the substrate.

Watermarks may be introduced by bent wire devices in cylinder-mold paper machines, embossed in the wet paper with a dandy roll in a Fourdrinier paper machine, or impressed on the dried paper. Simulated watermarks may be printed on paper with fatty materials (Kühn, 1986).

The image in a watermark is formed by local variations in paper density becoming visible in transmitted light. The watermark may also be detected in transmitted light as a variation in the thickness of the paper. There are two types of watermarks. “Non-localized” ones that are placed in generalized locations throughout the substrate with no particular reference to other features; and “localized” or “registered” watermarks that are placed in a specific location

within a printed image.

Watermarks are widely used in selected denominations of most of the world's currency. They were used in U.S. currency from 1869 to 1879 as part of a campaign to halt widespread counterfeiting that developed during the Civil War. Though watermarks are highly resistant to copying, they are not easily observed under difficult lighting conditions and can be simulated. However, watermarks can be designed to make high-quality simulations difficult. Should different watermarks be used for different denominations, they would introduce an added deterrent against "raising," that is, bleaching a low domination bill and printing a higher denomination bill on the bleached substrate. The introduction of watermarks to U.S. currency was recommended in the previous National Materials Advisory Board report. The current supports committee supports that recommendation.

Tinted Substrates

A yellowish-green color tint is currently specified for all U.S. currency denominations. Such pale tints are difficult to reproduce accurately in most reprographic systems, are readily recognized, are easily machine read, and do not add to the cost of the paper. The use in U.S. currency of a pale tint that is difficult to reproduce serves as a visible deterrent. While the use of different tints for the several denominations and the general use of color, or selectively enhanced features in the unprinted stock, is discussed later in this chapter, it should be noted that tints can improve the effectiveness of other deterrent features. Tinted substrates are being used by many other countries, among them Mexico, Thailand, and Japan (Haslop, 1993a).

Paper Furnish Additives

The BEP has been offered a wide range of additives to the paper furnish that have the potential to increase the security of the paper substrate. Among them are planchettes, enhanced fibers, optical fibers, taggants, and particles with special properties. The enhancements for fibers and planchettes include: optically variable iridescence, dichroism, metamerism, microprinting, fluorescence, and phosphorescence. Since the quantities added would be very small (for example, the current BEP specification calls for 0.31 kg of red and blue fibers per 1,000 kilograms of fiber furnish), such additives offer low-cost deterrent possibilities. However, additives in these small quantities would be barely noticeable to the casual observer.

Fibers that are simply colored could be readily reproduced by high-quality copiers. Many other possible enhancements are discussed elsewhere in this chapter. The addition of small amounts of enhanced fibers (e.g., plastic optical fibers), or combinations of variously enhanced fibers, for example, may play a significant role in the random pattern/encryption concept, as discussed in a later section.

Fibers or particles that selectively emit or absorb light at the same wavelengths used for scanning or copying can produce obvious forgeries, because the copier or printer will yield spots or lines on the copy that are white, black, or unevenly colored. These are discussed below. A technical discussion of the chemical aspects of these features is present in the section, *Inks for Printed Features* later in this chapter.

Enhanced Fibers

The introduction of randomly distributed fibers with specific responses to ultraviolet, infrared, or visible radiation detectable with simple point of exchange devices (a bright pen-light would be adequate for optical fibers) would enhance the security of the paper substrate with little additional cost. Ultraviolet enhanced fibers are being incorporated by several countries, such as Brazil and Bahrain (Haslop, 1993a).

The nature of these enhancements makes such fibers virtually impossible to copy and difficult to simulate. It is their limited distribution, and in some cases nonvisible character, that makes them unsuitable for public deterrence as presently deployed. Both an increase in concentration and considerable education of the general public would be required to render them generally effective. They may, however, prove quite useful for point-of-sale devices, machine readability, and forgery detection sensors that could be built into copiers (see *Counterfeit Deterrence Incorporated in Copiers and Printers* later in this chapter).

The committee examined paper made with small lengths of plastic optical fibers added to the furnish. Resistance to copying and simulation would be very high, and the ease of recognition by examination with a simple pen light is impressive. The BEP printed some notes on this paper, using a hand-operated intaglio press (Church, 1993). There was some evidence of ink adherence problems in the area directly above some of the fibers. There was also a concern that the high pressure in the production presses might cause the fibers to crush. The committee believes that these are typical of problems encountered with any new development and may be readily overcome. No fundamental barrier to future progress is evident, and several avenues of research opportunity are possible. For instance, a smaller diameter plastic fiber could be tried. Therefore, the committee recommends the continued development of optical fibers as an enhancement of the counterfeit-deterrent feature of the paper substrate.

Planchettes

Planchettes are colored or reflective pieces of paper or plastic a few millimeters in diameter. They are added in the paper furnish during paper manufacture. They can be enhanced in the same manner as fibers and thus can be optically variable, luminescent, magnetic, iridescent, microprinted, etc. Iridescent planchettes are currently incorporated in the currency of several countries, such as Mexico (Haslop, 1993a). As with fiber additives, cost is not a significant factor. Significant deterrence to routine copying and simulation can be achieved, but many of the enhancements do not present visible deterrence. Some can, however, be easily observed with inexpensive aids, such as a “black” light for the ultraviolet dyed planchettes. The use of reflective planchettes will defeat simple copying, but simulation of the effect appears to be relatively easy. There is also some concern that planchettes could lead to durability problems if some material properties of the planchette (such as stiffness) are significantly different from that of the substrate or are inadequately bonded to the substrate.

Microtaggants™ and Microcapsules

Tiny fragments of a wide range of materials, typically color coded with well-defined chemical composition or specific microwave, ultraviolet, infrared, or other characteristics, may be added to the paper furnish. Microtaggants™ are color-coded, layered polymer particles. These particles are generally of dimensions such that they are not visible to an unaided eye. These types of features would be most effective for machine detection and forensic analysis. They may also prove useful in random encryption applications. A careful assessment of these particles must be conducted to ensure that they are nonhazardous and nontoxic.

Radar Reflectance

The introduction of radar reflective dipoles either randomly distributed in the paper or included in an enhanced security thread was considered as a machine-readable feature (Patton, 1993). Model calculations suggest that the concept is feasible, but an instrumental method operating at radar frequencies is required for authentication. Bekaert, Inc. makes stainless fibers that a French-British company, Arjomari-Wiggins, places in a special paper reportedly used for some high security documents. As an alternative approach, the dipoles could possibly be printed on the paper with metallic ink; this approach would require further study to assess the printing resolutions and methods required, long-term durability, etc. However, the committee is not aware of any currency development effort on this feature. Although producing the paper may not require much development effort, the radar detector will. The radar transmitter will probably have to be separated from the receiver (i.e., the banknote would be examined in transmission). Making a detector that would not be fooled by a simulation that glued wires of the proper length to the outside of the bill might be a considerable effort.

Color

Some Fundamentals

Color is a perception: we see color when a non-white distribution of light is detected by our eyes and interpreted by the brain. The eye has three sets of cone detectors, most sensitive in the blue, green, and red parts of the spectrum. The relative responses of these three sets of cones gives us our color perception (Evans, 1974; Hill, 1987). These responses depend strongly on the nature of the illumination, yet our eye-brain system can compensate for considerable color and huge intensity variations in the illumination with minimal change in the color perceived. What little change in perception does remain is called metamerism and can prove troublesome in subtle color matching. Another complication is produced by color perception defects. The most common defects are deuteranopia (“green blindness”) and deuteranamoly, where there is, respectively, an absence or limitation in the ability to distinguish red from green[1].

[1] Deuteranopia or deuteranamoly is present in 6 percent of males and 0.4 percent of females.

By itself, the memory for a specific color is relatively unreliable. Machine reading is preferred for precise identification. However, in proper illumination, when color standards are available for comparison, the eye is an excellent instrument. In the context of colored patterns, the eye is quite sensitive to anomalies and can detect an unusual pattern or color component relatively easily.

Appendix C contains additional background materials relating to the measurement of color and the physical and chemical causes of color.

Uses of Color in Banknotes

Color can serve many functions in banknotes, but it is not a great deterrent by itself[2]. It can provide general identification of the note, specific identification of the denomination[3], and counterfeit deterrence when used in conjunction with another feature and in machine-readable form. An example of color used for deterrence is the use of colored or colorless inks that fluoresce under ultraviolet illumination. Color features lend themselves to instrumental detection.

Color can be utilized several different ways in currency. It can be used to tint the paper itself in a uniform manner; as part of various paper additives such as fibers, threads, planchettes, and the like; in intaglio printed background and foreground designs; and in overprinting.

It is frequently assumed that the essentially two-color nature of U.S. banknotes (black with green overprinting on the face, green back) is dictated by tradition and that the U.S. public would be opposed to any change. The committee found no evidence for this point of view, and some anecdotal evidence indicates the contrary. A small but statistically valid public opinion survey could add needed data to this debate.

There are a number of possible ways in which color can be used effectively on U.S. banknotes. Full-color printing with multiple colors on both the face and back that are different for each denomination is one possibility. This would provide ready denomination recognition and additional counterfeit deterrence against the professional counterfeiter using lithographic equipment (currently the most prevalent method of counterfeiting), who would be forced to make many plates and skillfully maintain precise registration while using several different inks. But printing fully multicolored notes on the existing intaglio printing presses is not a short-term possibility, since the BEP has a restricted number of additional ink fountains available on the current intaglio press equipment with which to apply other colors.

Additional options present a limited use of color that could be incorporated almost immediately on existing equipment. Each denomination could use a different pale color tint in the paper, as described in a previous section. There is the possibility of employing the existing overprinting step, used to apply the seal and serial number, to print additional color

[2]This is more a tribute to the advancements in non-impact color printing than it is a failing of color.
[3]This is not currently used in U.S. currency but is widely used in the currencies of other countries.

for the face. For instance, the denominations could be overprinted in prominent size, using a different color for each denomination matched to the pale tint of the paper[4].

Yet another option is the incorporation of additional color involving an optically variable feature, with much stronger counterfeit deterrence (Brettler, 1992; Haslop, 1993a; Phillips, 1993). These features are described in a following section. Also, overprinting a detailed image, such as a seal, using a reflective metallic ink is possible. Metallic ink does not have to be carefull tilted in light and closely examined under close scrutiny, as do optically variable images, and would therefore be observed more frequently. But metallic ink by itself would not be difficult to simulate, so it must be used to print a detailed pattern. However, the durability of such a pattern would be expected to be poor, similar to that of the metallized holograms (which are described in a following section). As a variation of this option, metallic or ordinary colored or colorless inks that fluoresce in response to ultraviolet light could be used. This would take advantage of two very useful features, and could be easily checked by a cashier or bank teller equipped with an ultraviolet lamp. Such fluorescent inks are used in the currencies of several countries.

Finally, induced moiré and variable-sized dot patterns discussed elsewhere in this chapter are made more effective by being printed in color, using different spatial frequencies for the different primary colors. As a result, the moiré or variable sized dot patterns show up in a different tint juxtaposed against the background; the eye is particularly sensitive to such small changes in color.

Other Aspects of Color in Banknotes

Color combines well with the fine-line engraved intaglio printing with its subtle shading and precision registration. Color anomalies, poor registration, and the absence of the crispness of quality printing are readily detected even by the relatively untrained observer. There are specialized line designs that show abnormal patterns when reproduced on color copiers; this effect is enhanced when subtle color patterns are used (Haslop, 1993a). This is discussed in detail elsewhere in this report.

Several general principles should be followed in using color. First, colors and color combinations should be tasteful and aesthetically pleasing. Second, the color compatibilities and color distinctions should be acceptable in commonly encountered illuminations. Finally, the choice of colors should be made with due consideration for human color deficiencies, particularly the red-green discrimination defect, which is present in about three percent of the population.

Inks for Printed Features

U.S. currency is currently printed using intaglio techniques. Intaglio inks are typically dark powder pigments that are added to oils. The intaglio inks transferred from plate to paper

[4]In addition to the colors needed for the current six denominations ($1,5,10,20,50,100), it might also be desirable to be prepared for at least one additional color, in case the need arises for printing another denomination, such as a $2 bill or a denomination higher than the $100 bill.

display graphic relief with a thickness of approximately 20 μm. The thick intaglio ink provides a versatile medium to carry other inks or agents. Consequently, printed features on the currency provide many opportunities to incorporate anticounterfeiting measures. To meet the threat of color copiers, printed features are desired that can not easily be reproduced by copying technology. Besides the special images and patterns that can be printed, the optical and materials properties of the inks used to form the printed features are themselves potential anticounterfeiting vehicles.

A number of the dye and pigment substances, both colored and colorless, show photoexcitation; that is, they produce color by photoluminescence (fluorescence) when suitably excited (e.g., with ultraviolet light). For machine reading, the fluorescent emission does not need to be in the visible region.

The various specialty inks that have potential for deterrence include:

- color-shifting (optically variable) inks;
- metameric ink pairs;
- photochromic inks;
- photoluminescent inks;
- transparent or absorbing infrared inks; and
- reflective inks.

As a group, these inks have many different optical and materials properties. Overt features that produce optical effects to the naked eye in sunlight or incandescent light can be achieved by some of these inks. Other inks require external perturbation of light to produce visible indications. In addition, covert features that can only be monitored by an instrument can be incorporated by some of the inks.

Given the emphasis on readily visible and recognizable overt anticounterfeiting features, the color-shifting inks have the highest potential for successful deterrence in the near term of all the inks listed above. They possess many desirable optical characteristics that do not require any perturbations other than sunlight or incandescent light. They can be implemented easily by the BEP. And their manufacture requires a high-technology fabrication processes that would not be easy to replicate or simulate. In contrast, the metameric, photochromic, and photoluminescent ultraviolet and visible inks are active features that require either additional perturbations to realize their effects or special instruments to observe their special properties.

The transparent or absorbing infrared inks offer excellent covert features that would be desirable for machine readers. The reflective inks are analogous to metallic stripes or metallic films in their effect and will not be considered further in this section. Photochromic or photoluminescent inks could produce false colors on reproduced banknotes, thereby thwarting the counterfeiter before an attempt is made to pass the bogus notes. These inks would have to respond to the exposing light wavelengths and intensities used in copiers and scanners. To be effective though, these inks must undergo a relatively rapid noticeable color change in response to light stimulus. In the future, the committee envisions that nonlinear optical material could be developed with high enough sensitivity to respond to the intensity of infrared laser light used in copiers to produce short wavelength response in the visible region.

Color-shifting Inks

Color-shifting (optically variable) inks reflect various wavelengths in white light differently depending on the angle of incidence to the surface. An unaided eye will observe this effect as a color change as the viewing angle is changed. A color copier or scanner can copy a document only at one fixed angle relative to a document's surface. Therefore, a copier or scanner would record only one color of an image printed in an color-shifting ink, losing information about the reflectivity changes versus angle of incidence. Thus the color copied image will be obvious, since it will remain the same color regardless of the viewing angle.

These inks are composed of color-shifting thin-film flakes suspended in a mixture of regular ink. The thin flakes produce their unique optical effect because of optical interference of light reflected from two parallel interfaces as shown in Figures 4-4. The reflected light from the two parallel interfaces will either constructively or destructively interfere with itself depending on the optical path differences.

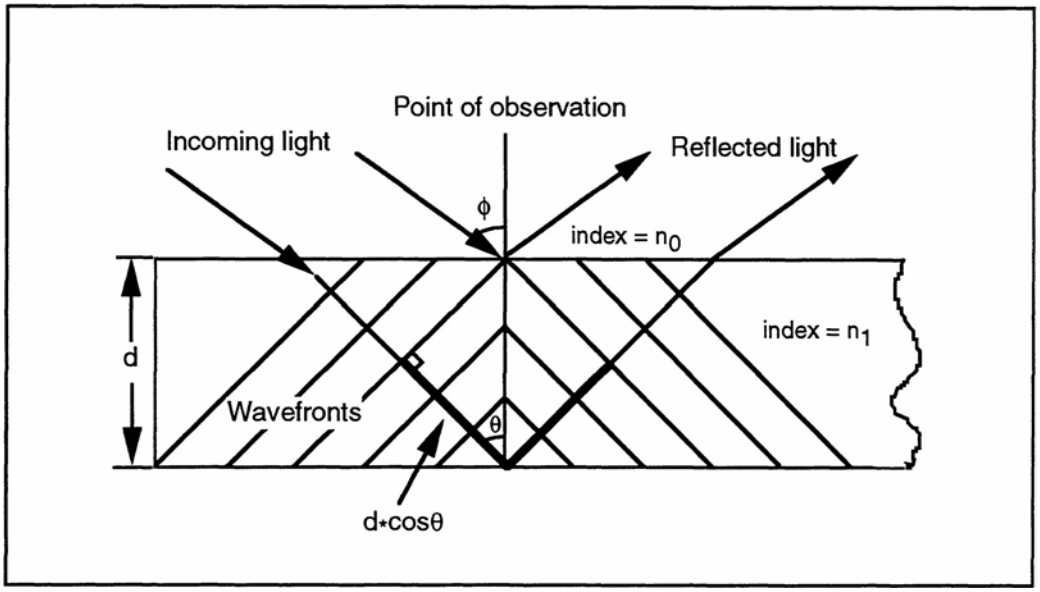

FIGURE 4-4 Color-shifting device principle of operation.

For a particular thickness of a thin film with two parallel interfaces, different wavelengths will constructively or destructively interfere at different angles. For example, the thin film may appear green at normal incidence and blue at 45° relative to the surface normal. The particular colors that are observed at normal incidence and at 45° relative to the surface normal will depend critically on the thin-film thickness. This thickness must be carefully controlled in the fabrication process and cannot be easily produced without expensive instrumentation.

The magnitude of the optical effect from the ink depends on the number density of thin-film flakes in the ink. The quality of the optical effect also depends on the precise orientation of the flakes on the surface of the ink. Physical forces cause the flakes to align parallel to the surface as shown in Figures 4-5. Without this preferential orientation, the optical effect would

be significantly degraded. The use of surfactants and functional groups on the thin-film flakes may further improve the optical effect. Figures 4-6 is a detailed cross-section of a typical thin film flake used as a pigment.

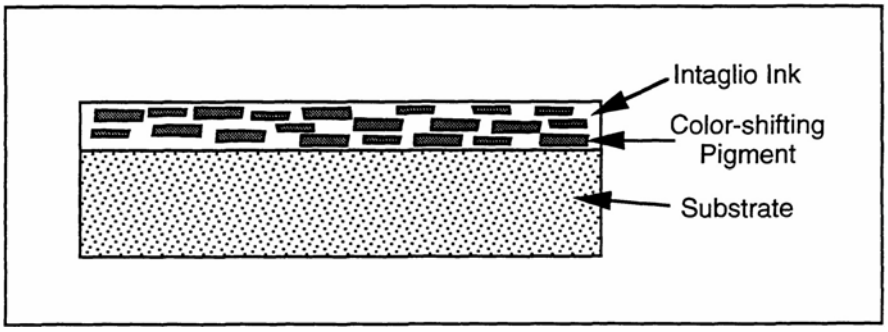

FIGURE 4-5 Color-shifting ink.

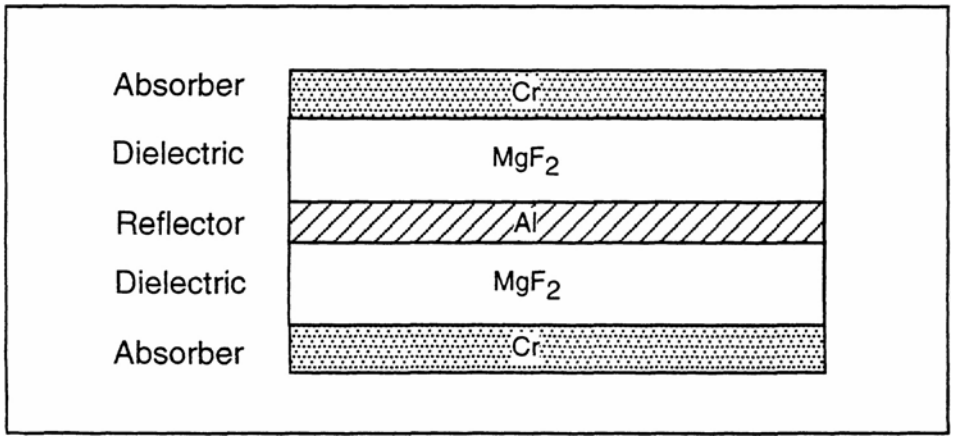

FIGURE 4-6 Cross-section of color-shifting pigment.

The intaglio inks with color-shifting thin-film flakes that are currently available produce a readily observed color change versus viewing angle under conditions of normal illumination[5]. The colors that are observed at normal incidence and 45° relative to the surface normal depend on the thin film thickness. In addition, dye or pigment filters can be added to the ink mixture to absorb particular light wavelengths. These absorbing dyes and pigments can further intensify and modify the observable color change of the ink versus viewing angle. With different combinations of flake thicknesses and dye or pigment filters, many color combinations are possible such as gold/green, green/magenta, green/blue, and green/black (Phillips, 1990, 1993). The committee's opinion is that the color changes, while noticeable (the committee thought that the last two pairs, of the four mentioned above, seemed to give the

[5]For example, OVI™ is a color-shifting intaglio ink available now from SICPA.

most noticeable color change, but this was a decidedly nonscientific sample), would be more effective if they were even more dramatic. The BEP should encourage the color-shifting ink manufacturers to continue to explore various combinations of dyes and optical flakes to intensify the optical interference effect.

A brief description of the fabrication process will illustrate the difficulty in reproducing color-shifting inks. Ultrathin films are initially deposited on a flexible planar substrate in high vacuum using electron-beam or sputtering-deposition techniques. The absorber/dielectric/reflector/dielectric/absorber structure is symmetrical, because the thin-film flakes can either be oriented up or down in the ink suspension. Typical materials used to obtain this multilayer structure are $Cr/MgF_2/Al/MgF_2/Cr$ or $Cr/SiO_2/Al/SiO_2/Cr$. Typical thicknesses for the layers are respectively 50 Å, 4,000 Å, 900 Å, 4,000 Å, 50 Å. The flexible planar substrate is dissolved and the thin film broken into flakes, 50 to 200 μm in diameter, which are then ultrasonically agitated to reduce the particle diameters to approximately 2 to 20 μm. Since the flakes are approximately 1 μm thick, they have a "pancake" structure with an aspect ratio that averages 10 to 1. Because typical printed ink thicknesses are between 5 to 30 μm this high aspect ratio helps align the flakes parallel to the surface of the ink.

The high-technology manufacturing process enhances the security of this ink, since the process is far beyond the capabilities of most (but not all) counterfeiters. Simulation is possible using inks that have metallic sheen. However, these inks do not change color. If the public is aware of the color change and knows how to observe it, and if the ink is used to print a design that is somewhat complex, simulation will be very difficult.

Macroscopic thin-film devices, such as interference films, can also produce excellent color-shifting effects. However, these large films are very susceptible to mechanical damage and they typically fail the "crumple" test. The small size of the thin-film flakes in the color-shifting ink precludes significant mechanical damage. They are already broken up and dispersed in the ink, and crumpling does not adversely affect their optical performance. The optical flakes are fairly chemically resistant, because they are composed of relatively stable metallic and dielectric materials. Moreover, they are embedded in the ink mixture, which protects them to some extent from chemical exposure.

The ink is compatible with intaglio and silk screen printing; it cannot, at this time, be applied using a lithographic or offset process. The cost of the ink is extremely high compared with the usual intaglio inks (two orders of magnitude more expensive), but it is not so expensive as to be impractical. However, since this is a new technology, the committee feels that with additional development effort, a significant reduction in the current cost of this ink may be possible.

Test banknotes printed with color-shifting ink have been subjected to the usual gamut of tests. The notes did not perform exceedingly well in the 24- acid soak or alkali soak tests, as was be expected (BEP, 1993). On the other hand, notes printed by other countries using color-shifting inks have not yet shown ink-related durability problems. A potentially fruitful area of research would be investigating ways to enhance the effect of the color shift. The concentration of the ink pigment, the size of the coated area, printing method, and the presence of a reference color can be optimized to enhance the effect. It was also demonstrated to the committee that having a reference color that does not shift color immediately adjacent to the image printed with color-shifting ink makes the color shift more dramatic. And, since

the color-shift effect does require manipulation by the observer relative to a light source, care must be taken in the design of the printed image to provide a large enough area that the effect can be readily discerned.

Many countries are beginning to apply these inks to print small images on their banknotes. Examples are the German 500 and 1,000 Deutschemark, the 50,000 Italian Lira, and the 10,000 Belgian Franc. Other countries are considering adopting color-shifting ink and may do so in the near future. Their experience should be closely monitored.

Color-shifting ink could be implemented fairly quickly by the BEP if the need arose, and hence is recommended by the committee as a feature for consideration in the short term. Additional research directed at enhancing the color shift should be encouraged.

Metameric, Photochromic, and Photoluminescent Inks

Whereas the effect of color-shifting inks can be seen in sunlight or incandescent light, other specialty inks display effects that require additional perturbations to obtain their unique signatures. Consequently, additional light sources or special viewing instruments are required to see their effects. Despite this disadvantage, these specialty inks can potentially be an effective measure against counterfeiting by color copiers or scanners. Most of these specialty inks are visible or ultraviolet inks.

Metameric ink pairs are designed to appear the same color under a particular illumination. When illuminated with a different light source, the metameric ink pair yields a different color. Metameric inks could have great utility if they induced a color change in the process of replication that subsequently produced a copy that did not accurately duplicate the original color. However, the previous evaluations of metameric inks have judged their color changes to be too subtle to be an effective deterrent. Since the last committee report, there is no new evidence to suggest that this situation has changed. Metameric inks must be judged an intriguing prospect for the future, and research developments should be monitored.

Photochromic inks have color properties that change as a function of light illumination. Well known examples of photochromic materials are the silver halides or spiro compounds found in sunglasses, which darken when exposed to bright light. The principle of photochromic inks is based on the photochemical conversion of the original compound to a photoproduct with different optical properties. For example, exposure to ultraviolet light can lead to molecular bond breakage and ring opening in various aromatic molecules, such as adamantane-2-spiro-naphtopyran. Upon ring opening, the light absorption properties will change, resulting in a change of ink color. After photochemical excitation, the photochromic inks revert back to the original state.

One drawback is that this excitation process is generally time consuming, reported to require seconds to minutes. However, faster response times have been recently reported for some experimental inks (Hepfinger, 1993). Fast reaction times and dramatic color change must be demonstrated before these photochromic materials can be seriously considered.

Another issue with photochromic inks is their long-term chemical stability. They are known to experience photochemical fatigue and will degrade with time. Even the best photochromic inks will degrade after several thousand photochemical conversion cycles, although the degradation rate may be a function of light intensity. The importance of this

stability for banknote applications must be further assessed, since banknotes would not be expected to be subjected to more than several copying attempts over their lifetime.

Photoluminescent inks display colors that are determined by both the absorption spectrum of the dye molecule and subsequent energy transfer in the excited dye molecule. If the energy transfer leads to the occupation of lower-lying electronic states, these states can relax to produce luminescence that is significantly red-shifted. Assuming that the initial excitation of the dye molecule was in the ultraviolet, this red-shifted light can mix with ambient light reflected in the visible to produce a composite color. Consequently, the color of the ink in the visible will depend on whether the photoluminescent ink is simultaneously excited in the ultraviolet spectral region.

Another feature of some photoluminescent inks is the lifetime of the luminescent dye molecules. The lower-lying electronic state may be "triplet" in nature, and its relaxation may require a spin-forbidden electronic transition in order to return to the "singlet" ground state. This spin-forbidden transition leads to a long phosphorescence lifetime of 10^{-3} to 10 seconds. Consequently, after the excitation source is removed, the ink will continue to luminescence for a period of time that can be detected either instrumentally or by the naked eye under ideal conditions or instrumentally. Other types of photoluminescent inks will undergo photochemical conversion to excited reaction products that have a different red-shifted emission spectrum. These inks are related to photochromic inks. The difference between photochromic and photoluminescent inks is that the effect of photoluminescent inks is observed in the altered emission spectra, whereas the effect of photochromic inks is observed in the altered absorption spectra.

Chemical and photochemical stability is a key issue with photoluminescent and photochromic inks. Recent work indicates that their chemical fragility can be improved by encasing photoluminescent molecules in small polymer fibers (Hepfinger, 1993). These small polymer fibers could then be incorporated in the ink. Although this technique remedies the chemical stability problem, the photochemical stability of the photoluminescent inks must also be surmounted. Additional research is required before the photoluminescent inks can be confidently deployed.

Photochromic and photoluminescent materials have great potential to be deterrents. Advancements in the field and the experiences of other countries that have implemented features using these materials, such as Japan, should be closely monitored.

Transparent or Absorbing Infrared Inks

In some instances of copying, infrared inks could potentially act as active features. The light emitted by the laser diodes, used in most printers and scanners to form a digital image, is in the range of 800-900 nm. Since many infrared inks absorb light at these wavelengths, the resulting image would be black where it obviously should not be this could be used to spell out a word to draw attention to the copy. For this concept to work, the absorption spectrum of the ink must fall within the emission wavelength of the laser diodes, and the laser illumination must be sufficiently intense.

Infrared inks are a potential source of covert anticounterfeiting features. Because they can not be duplicated by a color copier, they may provide an additional deterrent to augment

currency security. Their main drawback is that they are primarily not visible and normally require machine reading to detect their presence. Besides their use in anticounterfeiting efforts, the infrared inks would be extremely useful for machines that perform currency verification and denomination determination.

An advantage of infrared inks is that they can absorb very weakly in the visible wavelengths and very strongly in the infrared wavelength. Thus, they can not be observed by the naked eye, but can be detected by common infrared detectors. Most infrared dyes are based on a substituted phthalocyanine structure. This extended aromatic ring acts as an excellent antenna for infrared light. The precise details of the infrared light absorption are dictated by the various substituents attached to the extended aromatic ring. Depending on the substituents, the infrared dyes can absorb light in the range of 700-1100 nm. A comparison between typical dyes in the visible region and narrow and broad-band dyes in the near infrared is displayed in Figures 4-7.

This wavelength range is compatible with a variety of inexpensive infrared light emitters and detectors, so detection technology is readily available to exploit the signature of infrared dyes on currency[6]. For example, semiconductor lasers based on GaAlAs emit infrared laser light at wavelengths of 780-840 nm. These diodes are the same ones used in laser printers. Light-emitting diodes also used in electronic printers emit at about 900 nm as well. Common infrared light-emitting diodes also emit at 900 nm. These infrared wavelengths are also efficiently detected by inexpensive silicon photodiodes. Because of their large

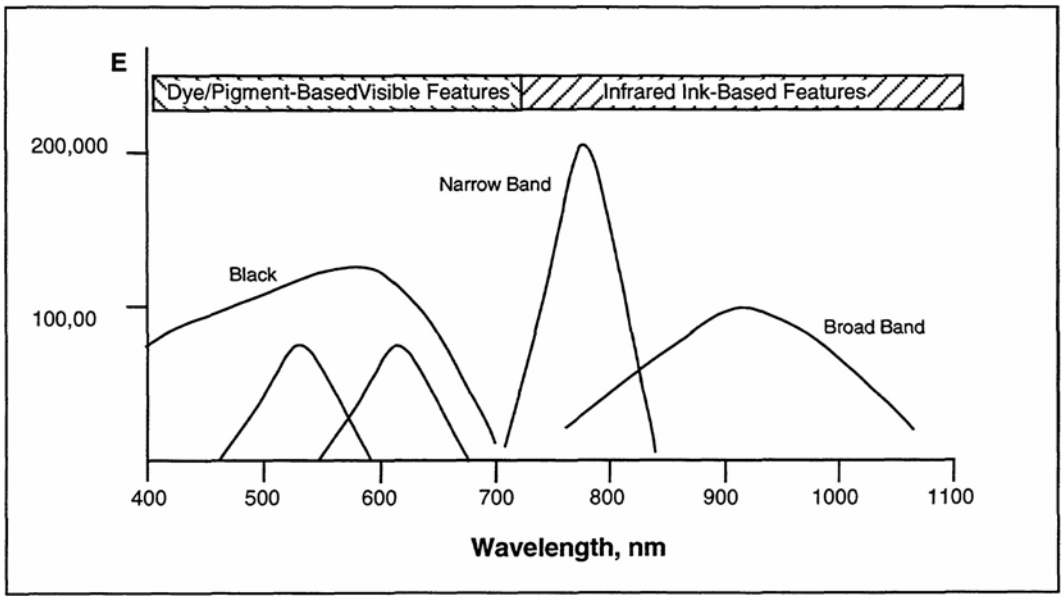

FIGURE 4-7 Infrared dye spectrum.

[6]The wavelength of visible light in 400-700 nm, and the infrared range begins above it, starting at 700 nm.

absorption coefficients, the presence of infrared inks could be easily detected by transmission measurements. But these absorption properties may make it difficult to record detailed pattern information.

The phthalocyanine infrared dyes are also well known for their excellent chemical properties. The phthalocyanines are nonpolar and not water soluble. They are also resistant to aqueous acids and bases and various organic solvents. These phthalocyanine infrared inks are known for their heat resistance. Moreover, in tests of photochemical stability, the phthalocyanine dyes were very robust[7]. These infrared dyes can potentially provide useful and reliable anticounterfeiting measures as both overt and covert deterrent features.

Design-Based Security Features

Design-based security features involve counterfeit-deterrent methods that can be incorporated into the printed banknote by modifying its design layout. In this section, several design-based features will be described together with an assessment of their effectiveness as a deterrents against counterfeits made using copier/ computer/ scanner systems. Each security feature is described in a separate section below. Design-based security features include: fine-line engraving, line work that induces moiré patterns when photocopied or digitized, variable-sized dot patterns, and latent images. In addition, the use of bar-code technology as a machine-readable, counterfeit-deterrent feature for banknote applications is discussed. Line patterns that produce moiré patterns or variable sized dot structures are examples of active deterrent features, since their presence on a genuine note may not be obvious but would be on a copied note.

Moiré-Inducing Line Structures

Current high-quality color photocopiers, and those that will be produced in the foreseeable future, are based on digital imaging technology. Computer work stations and their associated imaging peripherals (input scanners and printers) are also digital in nature. A digital image can appear to be a very faithful reproduction provided that the digital samples were taken sufficiently close together. However, if the image being digitized possesses spatial detail that is sufficiently fine, spurious patterns will be introduced into the reconstructed image; this effect is known as “aliasing” (Pratt, 1968)[8]. In the fields of printing and optics, aliasing errors are often referred to as moiré patterns. By using a properly designed pattern on the banknote, whose spatial frequency content is higher than the sampling frequency of digital photocopiers, scanners, and printers, a striking large-scale moiré pattern will be produced in the

[7]After exposure in a xenor fadeometer to the equivalent of about 4 months of daylight, the infrared absorption at 900 nm decreased only nominally (ICI Colours, Inc., 1993).

[8]Moiré patterns often look like ripples on the surface of water.

reconstructed image that immediately suggests the note is a counterfeit. (Note: these designs will not produce a moiré pattern if copied on the older analog copiers.) Appendix D contains additional technical discussion of the moiré effect.

An example of moiré patterns that are induced by digital sampling is shown in Figures 4-8 and Figures 4-9; this example was used in a presentation to the committee to illustrate the concept of induced moiré (Morris, 1992). Figures 4-8 contains a pattern known as a Fresnel zone plate (Longhurst, 1973). The fundamental spatial frequency of the grating pattern of Fresnel zone plates increases linearly as the radius increases from the center. The resulting image produced when this pattern is sampled using a digital scanner is shown in Figures 4-9. (Note that the resulting sampled image actually contains several moiré or "ripple-like" patterns.) The additional patterns are produced by commensurations between the various spatial harmonic frequencies of the zone plate and the sampling rate of the scanner.

A previous National Research Council report considered the use of moiré-generating patterns as a counterfeit-deterrent feature (NRC, 1987). The report considered the case in which two linear grating patterns were superimposed (or printed) with a small angular misalignment, giving rise to a low-frequency fringe pattern that is readily visible, while the individual gratings were of sufficiently high frequency so as to show no visible fringe pattern by themselves. In the proposed scheme, the presence of a visible moiré fringe pattern would then be used for authentication. It was noted that the printing resolution of the BEP exceeded the resolution capability of then available copiers and scanners. The committee reasoned that these systems would produce the low-frequency moiré fringe pattern but not the high-frequency grating pattern. Therefore, the visual effect of both the original and the photocopy

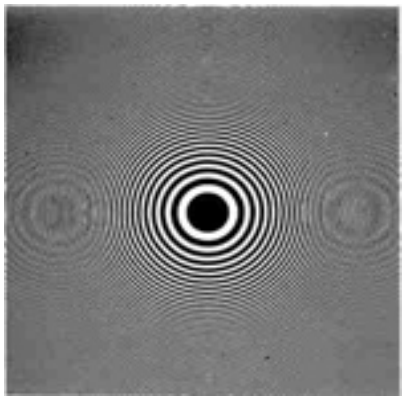

FIGURE 4-8 Fresnel zone plate pattern.

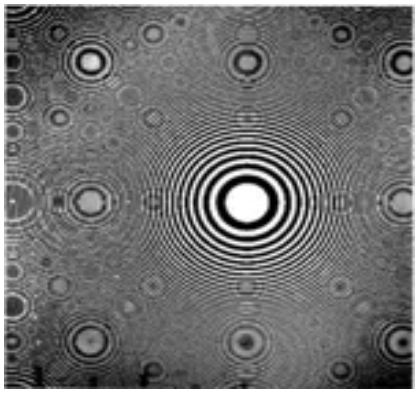

FIGURE 4-9 Digital image produced by a sampled Fresnel zone plate.

would be the same; hence, they concluded that this did not appear to be a viable deterrent method. While the committee addressed moiré patterns produced between two patterns printed on the note and reproduced by analog copiers, they apparently did not consider aliasing effects that will occur when high-frequency patterns are under-sampled by digital photocopiers and scanners.

Induced moiré (i.e., moiré patterns due to aliasing in a sampled image system) has been used as a counterfeit-deterrent feature in various forms since the late 1970s for document security (Wicker, 1991; Canadian Banknote Company, 1966; Kendrick and Jefferson, Ltd. 1988; Thomas De La Rue and Company, Ltd. 1985)[9].

Recently another method of using induced moiré for document security has been reported (Spannenburg, 1991). The formation of "alias" or moiré images was investigated using dot- and line-frequency modulation and screen-angle modulation. An example of a frequency-modulated image and a copy of this image made using a digital color copier are shown in Figures 4-10 and Figures 4-11 respectively (Spannenburg, 1991).

Researchers have also investigated "specialized line structures" that are invisible on the genuine document and clearly visible on the counterfeit, thereby confirming its invalidity (Thomas De La Rue and Company, Ltd., 1992).

FIGURE 4-10 Frequency-modulated image. (True original did not have any moiré.)

FIGURE 4-11 Copy of image made using a state-of-the-art color copier.
Source: Dr. Sijbrand Spannenburg, Manager MatheGraphics, The Netherlands.

The committee has found that concentric-circle patterns and zone plate patterns (Figure 4-8, Figure 4-9, and Figure D-1) are effective in defeating accurate reproductions. Due to the alias patterns

[9] Wicker, 1991, a follow-on patent that covers further extensions and embodiments of introduced moiré for document security, has also been granted.

generated, this approach should be capable of defeating digital systems operating with sample frequencies up to 1,800 dpi or more.

The committee suggests further development of another family of moiré-inducing patterns, referred to as space filling, self-similar patterns, by the BEP. A fractal-like pattern utilizing this concept is shown in Figures Figures 4-12 and Figures 4-13. Initial BEP experiments on this first-generation pattern utilizing an advanced color copier indicate that it will cause moiré at the appropriate combination of line spacing and line width. This pattern has the advantage that it naturally has built-in a range of modulation frequencies that will induce moiré over a wide range of copiers and scanners that have different spatial resolutions.

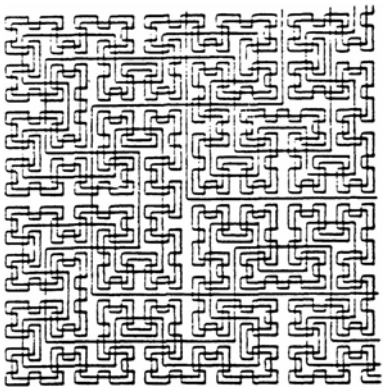

FIGURE 4-12 Space-filling pattern.

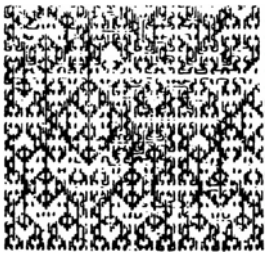

FIGURE 4-13 Moiré image of the pattern in Figures 4-12 that had been reduced (50 μm line width).

Interestingly, the moiré pattern occurred in color even though the original image was black and white. This indicates that the sampling registry was probably not the same for all the colors in the copier. In fact the latest approach in color copiers is to use color filter arrays in front of the imaging array; this automatically results in a different sampling registry for each color. Hence, it appears that induced moiré can be quite effective as a deterrent against color photocopiers, scanners, and printers.

To eliminate aliasing effects (i.e., to defeat this feature) the image must be optically "pre-filtered" prior to sampling in order to remove the high spatial frequency content. Optical pre-filtering can be accomplished by two different methods-defocusing the image or designing a special "low-pass" optical imaging system prior to sampling. Fortunately, the amount of image defocus that would be required to eliminate the moiré patterns destroys the fidelity of the entire image, and the design of the appropriate imaging optics prior to sampling is beyond the capabilities of the casual counterfeiter, whose tools consist of a photocopier or computer image processing work station. Likewise, to eliminate aliasing when printing one must utilize some type of "anti-aliasing" filter. Printer vendors are beginning to offer "anti-aliasing" filters implemented in software (Sensors, 1992). The committee recommends that the BEP monitor the status of "anti-alias" filter design, including devices that produce variable dot shapes and

sizes or an irregularly spaced raster, to minimize these effects. To date, these various resolution enhancements are somewhat limited and at best modestly decrease the visibility of the induced moiré patterns.

A casual counterfeiter would have a difficult time overcoming the moiré effect. The resultant copies would be obvious fakes due the moiré patterns that could not be easily reworked by hand or that were badly out of focus. The petty counterfeiters would likewise be stymied. However, the professional counterfeiters would not find this feature much of an obstacle, since they would have access to higher-resolution systems.

Given the above discussion, it is the committee's opinion that the induced moiré technique represents an effective and low-cost method to deter counterfeits produced by digital color photocopiers and digital scanning systems. In the long run however, manufacturers of high-quality copiers and scanners will probably incorporate optical anti-alaising filters to appropriately “blur” the sharp edges of line patterns to reduce the moiré effect.

Variable-Sized Dot Patterns

By using halftone methods, one can create the appearance of gray-scale images using binary printing techniques. With halftone printing a human observer will perceive two areas as having the same average shade of gray, even when one area is printed with a large number of small dots and the other area with a small number of larger dots. If the dots that make up one gray-scale area are selected to be below the resolution of reprographic systems and the adjacent areas are selected to contain resolvable dots, then the first area will be incorrectly reproduced. It will appear to the eye as a different shade of gray. In this way, a validation pattern, such as the word “VOID” in large letters, can be encoded that will appear upon reproduction. (Note that in digital image systems, such as high-quality photocopiers and computer work stations, a dot pattern that is finer than the resolution limit of the reprographic system is also likely to produce significant alias or moiré patterning.)

Color could enhance the effect of this deterrent. The dots could be printed in color, using a different dot size for each primary color, in close proximity (but not overlapping) so that the the eye would perceive the result as a dark color (e.g., near black). At least one of the primary color dots would be below the resolution limit of a targeted copier or scanner. The resultant copy would not contain all the colored dots, making it appear an obviously different color from the original.

Effectiveness of this deterrent requires that the printing resolution capability of the BEP stay ahead of that of reprographic technology. For example, for the foreseeable future, readily available copiers and printers will not exceed a resolution of 1,200 dpi. This resolution corresponds to a dot pattern with a dot diameter of 31.75 μm or 1.25 mils (this diameter includes the industry standard 50 percent overlap necessary to avoid jagged edges). This is below the practical resolution limit of intaglio printing. The high pressure of intaglio printing results in small dots being printed with feathered edges requiring fairly wide dot separations. In addition, the array of dots would not lie on a flat plane. Also, sufficient color fonts are not available on the BEP presses to print each size dot with a particular color. However, the necessary resolutions are well within the limits that can be achieved by offset printing.

Therefore, this feature will require an additional offset printing step to be effective against the high-resolution copiers and scanners. However, another possibility exists. A variable dot pattern could be incorporated in the banknote's design, and the pattern photo-etched into an engraving. The fine pattern would be at the limit of the intaglio printing process. Such a feature would be effective against the older copiers and scanners. If an offset printing step was added, the feature could be printed in finer detail. In this way, the feature could evolve over time without requiring a major design change.

The committee concludes that variable dot-pattern-generated gray-scale printing or “void” patterns can be an effective deterrent as long as the BEP's printing capability exceeds the resolution of new reprographic technologies. (A similar conclusion was reached in a previous report; NRC, 1987.) These features also lend themselves to continual improvement over time.

Latent Images

In the context of counterfeit-deterrent methods, the term “latent image” is used to refer to the method in which the variation surface-relief pattern of the ink obtained with the intaglio printing process is used to produce a different image when the image viewing angle is changed[10]. Normally, the latent image is observed at large angles with respect to the surface normal, that is, at near grazing incidence. Several countries currently utilize latent images in their currency.

It is the committee's opinion that the latent images can be difficult to see, even on new currency under good lighting conditions. Furthermore, the durability of a latent image is fairly low, as demonstrated by standard durability testing. For these reasons, latent images do appear to be as promising as other deterrent methods. The experiences in other countries should, however, be closely monitored.

See-Throughs

“See-throughs” refers to an area on the banknote in which the front and back images are printed in almost perfect registry. The image on the front is printed to complement the image on the back. These images may be in different colors. The design of the images is done so that any slight misalignment would be obvious when viewed in transmission, and hence would be an indication that the note was a counterfeit. Thus, the name “see-through.” The production of this feature requires a press that prints both sides of a note simultaneously so that the necessary high-precision registration is achievable. Such precision is not possible with the current intaglio press equipment installed at the BEP. Therefore, the implementation of such a feature would require a significant capital investment by the federal government. The value of the effectiveness of this feature would have to be closely analyzed before such expenditures were made. However, with the proper equipment, the printing of these features is inexpensive. Many countries are beginning to print such features. Their effectiveness in deterring counterfeiting should be closely monitored.

[10]This “latent image” is not the same as a photographic “latent image.”

Bar-Code Technology

Bar-code technology provides a reliable method to encode information about a given item in a convenient machine-readable format. Several bar-code formats have been developed. Conventional linear bar codes are widely used to represent product identification numbers; these are used to look up product information contained in a central data base, for example, the product description and price. Similarly, bar codes can represent the denomination and serial number of banknotes to provide a fast and reliable machine-readable method to sort (and potentially track) them (Storch and Van Haage, 1989). In fact, The Netherlands has adopted such a scheme for its banknotes.

Conventional linear bar codes are, however, limited in the amount of information that can be stored. To increase information capacity, two-dimensional bar codes have been devised for example, with stacked bar codes and matrix codes (Pavlidis et al., 1991; Pennisi, 1991). By increasing the information content, the two-dimensional codes offer the potential to create a "portable data file" that can be retrieved without the need to access a central data base.

With regard to counterfeit deterrence, by tracking and processing bar-coded serial numbers, unauthorized or duplicated notes could be detected. But there may be an appreciable cost associated with the information processing task of maintaining a data base of active currency serial numbers.

It has been proposed that the bar code include randomly selected information in a manner somewhat analogous to the random pattern/encryption concept described later in this section (Storch and Van Haage, 1989). The random information that is encoded might be associated with some particular physical characteristics of the note, for example, the orientation of fibers in the paper or the number of fluorescent microtaggants at a given location. A counterfeit could therefore be detected by comparing the encoded, randomly selected information with the actual physical characteristics of the note; this would, however, require a special machine reader to detect the physical characteristic in addition to the required bar-code scanner.

The general use of bar-code technology for U.S. currency is beyond the scope of this report that focuses on counterfeit deterrence. However, visible bar-codes can be copied as easily as any other printed feature. The counterfeit-deterrent aspects associated with bar codes arise from two aspects: the ability to match serial numbers against an external data base, and to encode random patterns. The practicality of the former has yet to be demonstrated, although it would seem that a major benefit is related to the tracking of currency; this feature would provide a technological solution to the possibilities offered by the individual serialization of each banknote. A detailed discussion of encryption of random patterns is presented in a subsequent section of this chapter.

Post-Printed Optically Variable Devices

Post-printed optically variable devices are those that are added after all other printing operations have been completed. They include diffraction-based devices-holograms, kinegrams, and pixelgrams; multiple diffraction gratings; thin-film devices; and hot-stamped metallic

security stripes (these stripes can also be applied by the paper manufacturer). The committee's description and analysis of the various devices are discussed below.

Diffraction-Based Holograms

Holograms are widely used as counterfeit-deterrent features for security documents and credit cards. The striking image that can be produced by a hologram provides a good overt security feature. By far, the largest application to date for hologram security devices has been for credit-card security.

A hologram is a recording of the interference pattern formed by two coherent beams of light–the picture beam and the reference beam (see Figure 4-14). When illuminated by the reference beam during readout, the hologram produces (or reconstructs) the picture beam. The picture beam can take on many different forms: a three-dimensional image, which posses depth information; a two-dimensional image, for example, a presidential portrait, a bar-code pattern for a machine-reading system; and so on.

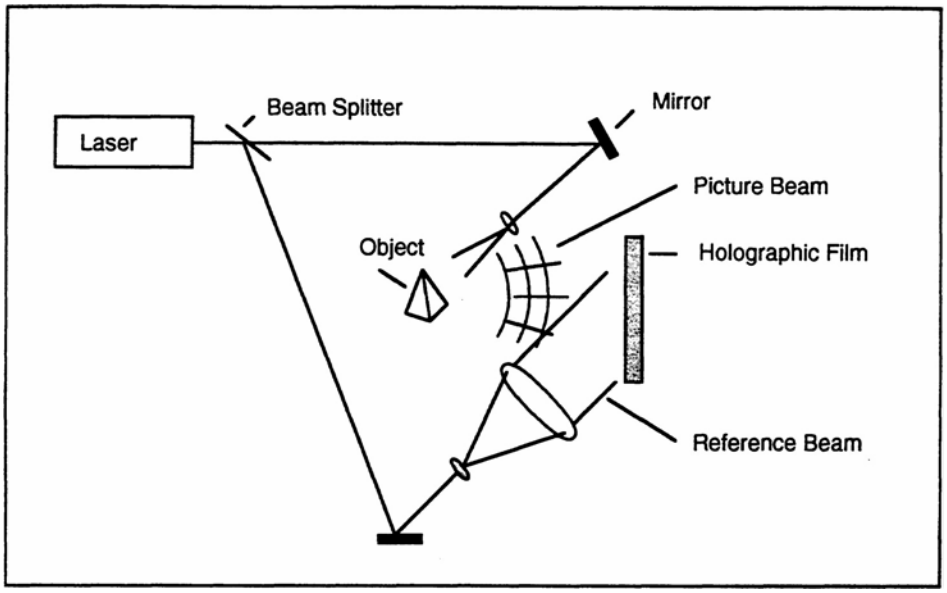

FIGURE 4-14 Optical setup for recording a hologram of an object.

A unique property of holography is that more than one image can be recorded and subsequently reconstructed from a given hologram. For example, when viewed at normal incidence, one might see the portrait of Andrew Jackson; however, when viewed at a different angle, one would see an image of printed text, for example, “$20.” Multiple-exposure holograms can also be used to produce image motion as the hologram is viewed at different angles.

Because a hologram possesses extremely fine structural features, it is essentially impossible to copy or duplicate reprographically with even the most sophisticated equipment; hence, it is an excellent deterrent for the casual counterfeiter. However, it is possible to replicate or simulate hologram security devices using more advanced technical methods. (See *Random Pattern/Encription Counterfeit Deterrence Concept.)*

The use of holograms for document security has been investigated extensively (American Bank Note Company, 1984; Battelle Columbus Laboratories, 1983, 1985, 1990; Bander, 1984; Church and Littman, 1991; Collins, 1986; Fagan, 1990, 1991; Martin, 1983). A major shortcoming is the hologram's lack of durability under even normal usage when placed on a flexible substrate. The image rather quickly becomes unrecognizable, making the job of a counterfeiter much easier, since a "worn" hologram is easy to simulate. The durability of holograms suffers from the wrinkling of the metallic film. If these devices were not metallized, but were instead placed in a "window" on the banknote for viewing in transmission, their durability might be significantly increased.

The BEP should continue to monitor the status of developments for these devices, and promising research directions should be encouraged. Experience in other countries the effectiveness and durability of holograms should be closely followed. These devices have potential for future consideration.

Diffraction-Based Kinegrams and Pixelgrams

In the recent literature two important variations of hologram technology for document security have been reported: the kinegram and the pixelgram. The kinegram, a patented device, was invented at Landis and Gyr. (Antes, 1983). The pixelgrarn, also a patented device, was invented at CSIRO in Australia (Lee, 1988, 1991). The salient features of these devices are summarized briefly below.

Both the kinegram and the pixelgram can be regarded as special types of surface-relief, computer-generated diffractive optical elements. The basic distinction between these two devices is that a kinegram is constructed using vector-addressing methods, whereas the construction of a pixelgram is based on a discrete-pixel (picture element) addressing scheme. The master element for both the kinegram and the pixelgram is typically generated using electron-beam lithography.

When designing a kinegram, one can vary the spacing, angle, and depth of the lines to produce the desired image reconstruction. These line features can also be varied at different spatial locations so that when the kinegram is rotated, the reconstructed image appears to move. For document security applications, the principal advantage offered by the kinegram is that the recording of the holographic master requires additional processing steps and more sophisticated equipment than those required for making a "simple" hologram. Because of the apparent motion, the image produced by a kinegram is both striking and unique; hence, its authenticity can be easily checked by the public.

Like the kinegram, the pixelgram is also capable of producing multiple high-resolution images. To make a pixelgram, one starts by digitizing the desired image into an array of $N \times M$ pixels using a high-quality color scanner-the larger the number of pixels one chooses, the higher the resolution of the resulting image. In the second step, each pixel of the image is

converted into a miniature diffracting grating. The lines of the diffraction grating are generally curved so as to produce a diffracted intensity that is proportional to the average intensity of the pixel associated with the original portrait image. The resulting grating structure is written onto a recording material using electron-beam lithography; this serves as the pixelgram "master" plate. A pixelgram master typically contains over 10 gigabytes of binary data, and it takes between 10 to 20 hours to write a 20-mm by 26-mm pixelgram. Available optical effects include a positive/negative flip; switch on/off effects; specific color flips; and movement effects.

Both the kinegram and pixelgram can be applied to bank notes quickly and at relatively low cost by using hot-stamping, foil-based techniques (Reinhart, 1991). However, the fastest current hot stamping equipment operates at about 3,000 sheets/hr, which is one-third the rate required by the BEP (Church, 1993), thus three such units would be required on the production floor, necessitating a major realignment of the equipment and production flow, plus additional production personnel.

Several countries have used these technologies on their bank notes. Finland and Austria have used the kinegram (Finland: 500 and 1,000 Mark notes; Austria: 5000 Shilling). Australia and Singapore have incorporated pixelgrams into commemorative banknotes (Australia: $10 note; Singapore: $50 note).

The kinegram and pixelgram technologies offer a number of excellent counterfeit-deterrent aspects for document security. Unfortunately, however, for U.S. banknote applications all of the hologram samples that have been tested to date have been deemed to have a severe limitation:*durability.* The holograms that have been tested have all failed, to various degrees, the BEP's tests for mechanical durability (abrasion, crumpling, etc.) and chemical durability (laundry detergent, bleach, dry-cleaning chemicals, etc.)[11] As is the case for holograms, the durability of kinegrams and pixelgrams suffers from the wrinkling of the metallic film. Their durability might be significantly increased if they were not metallized but were placed in a "window" for viewing in transmitted light.

The so-called "crumple test" is particularly detrimental to the integrity of the reconstructed holographic image (Church, 1992). To improve the fidelity of the holographic image after mechanical distortion (creasing, folding, or crumpling) of the banknote, a "multi-redundancy" hologram has been developed (Haslop, 1993b). The multi-redundancy hologram consists of a unique sub-image that has been replicated several times over the area of the reflective holographic foil. Since only a single sub-image is required to detect authenticity, not the full image produced by the holographic foil, the device exhibits improved resistance to mechanical distortions.

At the time of this report, data regarding the durability of the banknotes in circulation, that utilize holographic technology were not available. To assess properly the issue of durability, the BEP should seek information regarding the durability of circulated banknotes, particularly about recognizability, from the other countries currently utilizing holographic security devices and should correlate this information with the test procedures used at the

[11]See Bureau of Engraving and Printing Test Methods BEP-88-02, "Crumple Test;" BEP-88-04, "chemical Resistance;" and BEP-88-05, "Laundering."

BEP. Promising research directions should be encouraged, and the BEP should continue to monitor the status of developments for these devices, which have promise for the future.

Multiple-Diffraction Gratings

A diffraction grating is an optically variable device that consists of a series of finely spaced parallel grooves. Diffraction gratings can be formed on a wide variety of substrate materials, including metals, glass, polyesters, and polymers (or plastics). The optically variable nature of a diffraction grating is controlled by the selection of grating parameters-the groove spacing and the width, depth, and shape of the grooves-so as to produce a particular color and brightness in a specified viewing direction. By combining a collection of gratings (multiple diffraction gratings) with different grating parameters, one can create a detailed multicolor design pattern (lettering or other two-dimensional images). When the multiple diffraction grating is tilted to a different observation angle, both color shifts and design shifts can occur.

Multiple-diffraction-grating structures were investigated in detail in the 1980s by the BEP and several other countries, including Austria, Australia, Canada, the United Kingdom, and Switzerland. The research on multiple diffraction gratings for counterfeit deterrence was summarized in a BEP presentation (Church and Littman, 1991). They were found to be readily recognizable by the general public and cannot be reproduced on advanced reprographic equipment. However, they could be simulated by technically proficient counterfeiters with relatively simple materials. The durability of the devices was also rated low. They are susceptible to severe wear by abrasion, and cannot survive the BEP's crumple test. Australia is using a multiple diffraction grating in its commemorative $10 note; Singapore also is using a multiple-diffraction-grating in a commemorative note.

Thin-Film Interference Filters

A thin-film interference filter (TFIF) consists of one or more layers of vacuum-deposited inorganic materials formed on a substrate. The filter utilizes the wave nature of light to filter selectively a specific color or band of colors. Using TFIFs, it is possible to design a multilayer structure that exhibits a striking and distinctive color change when viewed from different angles, for example, green to gold, blue to red, etc (Berning and Phillips, 1987a,b; Dobrowolski et al., 1989; Phillips, 1990). Color-shifting inks, discussed earlier in this chapter, are a special case of TFIFs.

This variable color change cannot be produced by photocopying, photography, or other reprographic techniques. Furthermore, because one needs sophisticated vacuum-coating equipment, coating designs, and process control to make TFIFs, there are only a limited number of facilities in the world that are capable of making these filters, which further adds to document security. However, the notes must be manipulated correctly with respect to a light source to observe the color shift.

TFIFs can be based on either a dielectric-metal multilayer stack or an all-dielectric multilayer system, which can be affixed to the document using an adhesive. It was found that the performance of the dielectric-metal TFIFs in aging, mechanical, and chemical durability tests was worse than the all-dielectric designs (Dobrowolski et al., 1989). Furthermore, since the metal-dielectric TFIFs don't require as many layers as the all-dielectric designs, they are

somewhat easier to make; hence, they are more susceptible to attempted counterfeiting. If metals are used for one or more layers, their potential environmental effect should be analyzed.

Researchers have investigated TFIFs consisting of a metal reflector/dielectric/metal absorber structure (Berning and Phillips, 1987a,b). To overcome problems associated with the transfer of the TFIF to the document and to improve the performance of the TFIF with respect to mechanical wear and tear, the researchers found that by removing the multilayer coating from the polyester web, they could produce small flakes of TFIF, which could be used to make an optically variable pigment as a component in an color-shifting (optically variable) ink. Color-shifting inks, discussed earlier in this chapter, exhibit the same type of color shift with angle observed the large-area TFIFs but at a lower apparent intensity, since the optically variable pigment is suspended in ink. On the other hand, color-shifting inks are less sensitive than TFIFs to mechanical deformations, such as crumpling and folding.

The National Research Council of Canada determined that the preferred combination of multilayers were oxide (dielectric) films of ZrO_2 and SiO_2 (Dobrowolski et al., 1989). It reported that the films of these materials deposited by evaporation were rather porous and tended to age on exposure to air. However, the aging was found to be quite predictable and could be taken into consideration in the filter design. Measurements of dependence of the spectral performance of the dielectric multilayers with changes in temperature, humidity, mechanical wear and tear, and chemical attack were found to be acceptable for banknote applications. This type of TFIF is currently being used on the Canadian $50 and $100 notes. The Bank of Canada reports that its tests indicate that the optical effect of its thin-film security device can still be recognized after the note has been crumpled, washed, dry-cleaned, and scratched (Church and Littman, 1991). However, these films will not hold up to all of the BEP's exacting durability tests.

These devices have many of the advantages of the color-shifting inks. They are presently more expensive than the color-shifting inks, although the color change is more dramatic. They could be simulated by metallic film, but such a counterfeit would be easy to detect since it would not undergo the characteristic color change. The BEP should stay informed about the Canadian experience with TFIFs.

Hot-Stamped Security Stripe

Metallized, hot-stamped stripes, followed by an overprint step, can also be an effective counterfeit deterrent against photocopying. When a banknote containing a metallized security stripe (normally consisting of metallized segments) is copied, the photocopy turns black at the locations of the metallic segments due to specular reflection, and the overprinting on the original banknote is completely lost in the photocopied one. Furthermore, because of the overprinting, one cannot simply remove a given segment and place it at different locations, which makes it more difficult to produce “raised” notes. The security stripe can contain different regions, some functioning as a simple reflector and some functioning as an optically variable device. Stripe widths typically vary from 3 to 3 mm. Because of its small size, the security stripe is found to be more durable than large-area diffraction-based and thin-film devices described above. Mechanical durability of an optically variable device in the stripe is

increased because it is small, (Haslop, 1993a) and both the chemical and the mechanical durability of the stripe can be improved, because there is greater latitude in selecting materials that are more flexible and more resistant to chemical attack (Reinhart, 1991). This feature has potential for the long term, and the progress of its development should be monitored by the BEP.

Embedded Zero-Order Diffraction Gratings

Embedded zero-order diffraction gratings represent a new type of microstructure device that may prove to be useful as a counterfeit-deterrent feature. The optical characteristics are similar to those of a thin-film interference filter in that striking color shifts are produced as the structure is rotated or tilted. They consist of extremely fine, surface-relief grating structures embedded in a transparent plastic.

The structure and reflected spectrum of an embedded zero-order diffraction grating structure are shown in Figures 4-15. The reflection spectrum is sharply peaked due to the fact that the operation of the device depends on guided-mode resonances associated with the structure. The optical properties and applications of these structures are being investigated by a number of researchers (Gale, 1991; Gale et al., 1990; Norton et al., 1993; Wang et al., 1990). The design and fabrication of such structures are now possible due to recent advances in the theoretical understanding and computer modeling of light propagation in sub-wavelength structures and advances in microlithography. Because the operation of these devices depends on the fact that the submicron grating structure must be embedded in plastic and the refractive index of the plastic plays a key role in the design of the device, the possibility of copying these structures either mechanically or optically is highly unlikely.

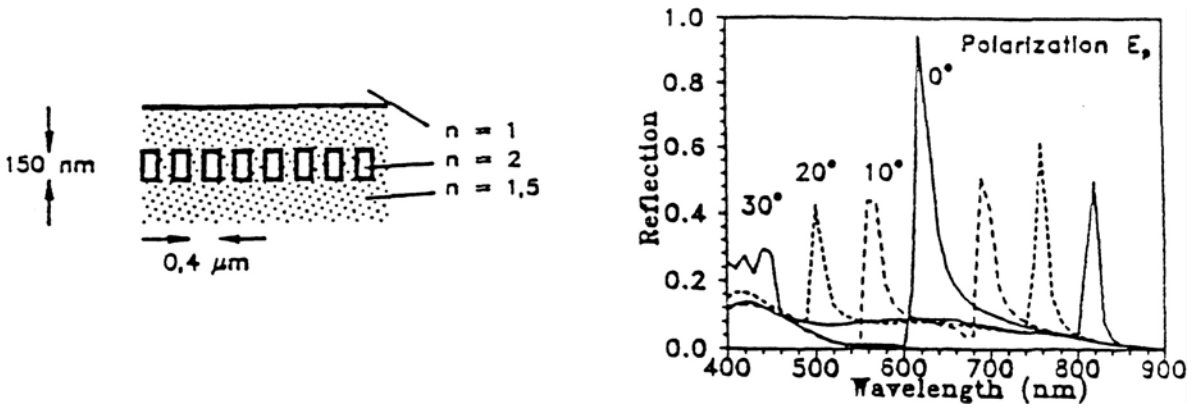

FIGURE 4-15 Structure and reflection spectrum of an embedded lamellar diffraction grating.
Source M.T. Gale, Zurich Switzerland, Diffraction Microstructures for Security Applications (Figure 2).

While the application of zero-order gratings as a counterfeit-deterrent feature requires significant further development, it appears promising. Therefore, the committee that the BEP monitor the progress that is being made in the development of these devices.

Random Pattern/Encryption Counterfeit-Deterrence Concept

Implementation Using Two Visible Features

This system has the potential to provide a very high degree of authentication of banknotes that even the determined professional counterfeiter cannot defeat. It does require the use of an automated reader. And leverages a significant amount of development that has been done for arms control verification purposes (Bauder, 1983; Graybeal and McFate, 1989).

This concept is based on tagging each banknote with a unique random three-dimensional pattern as an identifier. Since the unique identifier is three-dimensional, it cannot be reproduced by copiers or printers such as those discussed in this report or by other existing reprographic processes that produce only two-dimensional images. Since the unique identifier (fingerprint) is randomly generated, a counterfeiter cannot duplicate it even by employing the same process used to produce the original[12]. In order for this method to work for banknotes, three technical issues must be addressed: (1) selection of an appropriate three-dimensional random pattern, (2) encryption of the pattern in such a way that an authenticator can be printed directly on the banknote, and (3) implementation of a method to read the pattern and compare the results with the printed authenticator of the pattern (Church and Littman, 1991). The progress made to date in addresing these issues is summarized below.

The unique identifier can be drawn from the natural three-dimensional features of the paper such as the pattern of the fibers or features that are added to the paper during its manufacture. In a proof-of-concept demonstration for banknotes, short pieces of plastic optical fiber are added to the fiber-water slurry that forms the paper. The optical fibers become distributed randomly throughout the paper. The pattern in a defined area is read by passing the note under a light bar surrounded by an array of photodetectors. Whenever the end of an optical fiber is illuminated, the light transmitted to the other end is detected and its location recorded. The result is a pattern that is a function of the relative locations of the ends of the optical fibers. Other unique identifiers can be used; a choice among them would consider readability, cost, durability, and appearance.

The three-dimensional properties of the unique identifier are read with an imaging device to create a numerical description of the pattern. The description can be encrypted and printed on the note in bar code or other machine-readable pattern to serve as the authenticator. A note is authenticated using a device that reads the unique identifier pattern, reads and decrypts the authenticator, and compares the two; if they match, the note is authentic.

[12]By definition, it is impossible to predict the outcome of a random process; therefore, each pattern that is generated will be different.

A public key encryption method can be used (Hellman, 1979; Rivest et al., 1979). This method includes a decryption key and an encryption key that are different, and neither one can be derived from the other. For this application, the key required to decrypt the authenticator can be public knowledge. This allows authentication of notes by the public without fear that the secret encryption key would become available to potential counterfeiters who could then generate their own random unique identifiers and the related correct encrypted authenticators.

Fiber-optic patterns on currency have been read and authenticators have been printed at speeds up to 400 in/s (equivalent to more than 40 notes/s in a production application; Baird Corporation, 1989). By careful selection of the random pattern, it would be possible to provide a lower level of authentication at points of sale inexpensively, since special equipment would not be required. A higher level of authentication could be implemented at the Federal Reserve banks, and possibly other locations, using automated high-speed readers. For example, if the fiber-optic pattern described above were implemented, the existence of the fibers themselves could easily be detected visually at points of sale. Further inspection with a small light source (e.g., a pen light) would detect whether or not these fibers conduct light. The highest level of detection would require machine reading to compare the fingerprint (the specific unique pattern of the fibers) with the authenticator.

Initial readings of unique identifiers will differ from subsequent readings taken when notes are authenticated because of unavoidable variations in the location of the reader with respect to the note, variations in the readers, and changes in the pattern due to wear and tear. Methods have been developed that account for these variations and ensure low false-decision probabilities. These methods are described in Appendix E.

Efforts should continue to develop the random-pattern/encryption concept for possible future use in currency. It has the potential to provide a major increase in counterfeit deterrence.

Implementation Using One Visible and One Secret Feature

An alternative approach to implementing this concept would involve a visible and a secret feature. In this case, a unique visible feature, such as the serial number, could be subjected to a public key encryption algorithm as before. But the resulting pattern would be printed in a secret fashion. During authentication, the device would compare the unique overt feature with the covert encryption; if they match, the note would be accepted as genuine.

Such a system suffers from the fact that the visible feature selected is not a random three-dimensional pattern, and hence could be readily copied. The security of the method would then depend on the ability to keep the encrypted pattern secret and thus not able to be copied. The committee thinks that the covertly printed image could be detected by a determined professional. Because of this, the approach is not attractive.

Counterfeit Deterrence Incorporated in Copiers and Printers

The committee has concluded that color copiers and color printers operated by the casual counterfeiter present the greatest counterfeiting threat. (See Chapter 2 and Chapter 3.) One approach to discouraging such opportunistic counterfeiting involves making the equipment less "friendly" to use. Two strategies being pursued are for the equipment to recognize banknotes and fail to reproduce them and for each copy from a particular machine to print a covert, traceable code in the image area of the reproduction.

Currency Recognition System

One manufacturer of advanced color copiers has developed and installed in its latest copiers, a first-generation system to automatically identify an attempt to copy certain banknotes (Tsujita, 1993). If the equipment detects a forgery attempt, it prints a black or blank copy and can be programmed to then shut down until it is reset by a repairman.

The detailed implementation of this anti-forgery approach has, understandably, not been presented in full detail. It is, after all, a security measure, and complete disclosure would leave the system vulnerable to compromise. Since it is a technological solution to a human problem, the solution is not likely to be perfect. It could however be reasonably effective for some period of time, particularly against the threat posed by the casual counterfeiter. But eventually any purely technological solution is likely to be compromised through development of some countertechnology.

This forgery detection and prevention system is, in effect, an expert system that includes software and hardware components (Canon, 1990)[13]. The input information to the software is provided as a byproduct of the successive red, blue, green, and brightness scans. The scans provide a rough location of the position and orientation of the bill, followed by a refinement that includes the location and identification of important features on the bill. Statistical information is computed regarding the distribution of colors and feature sizes (possibly linked with color).

The example stated in the patent involves the detection of a specific Japanese banknote. The present system can reportedly store the data for four samples of each of eight different currencies; that is, 32 separate images. Therefore not all possible denominations of all possible currencies will be contained in the stored detection set. It is not known whether the samples stored in each machine are identical. Features have been included in the design of the electronics to prohibit operation of the copier if the forgery detection feature is disabled. However, a drawback for any technological approach to forgery detection is that once the rules are known, possible countermeasures can be developed to evade the detection algorithm.

[13]The patent describes the form scanning operations used to determine if a forgery is being attempted. The first scan detects the approximate position of the note. The second scan determines the exact position and oventation of the note. The third scan calculates the expected position of the seal using data from the previous scans, and then determines if the seal is present at that position. The fourth scan produces a black full overprint of the note image if the third scan concluded that a forging is being attempted.

There a number of unknowns. The committee does not know the extent to which this forgery detection process is successful. Reports are that it does work under a number ofunidentified conditions. (Legal considerations prohibited field testing of the feature by individual committee members.) This committee did not receive any information as to the efficiency of the process against simple countermeasures. Since the print engines in color copiers will also function as computer-driven output devices, it is not clear what degree of protection will be provided by the forgery detection feature in computer printers. Also, the degree to which the technology will be made available to other manufactures is not known.

The number of false alarm detections of currency will certainly become an issue. The cost of these machines is significant enough that no user will purchase a system that fails to copy any range of materials that "look like" but are not currency. Market forces will eliminate any feature that diminishes the usefulness of the copier. In addition, it is not known how well the feature can detect attempts to copy an already counterfeit (and thus not perfect) banknote.

In the opinion of the committee, the copier manufacturer is to be congratulated for this technological achievement. In the short term, the currency recognition feature will probably serve as a deterrent for the casual counterfeiter as a result of the knowledge about the anticounterfeiting feature. The committee, however, thinks that this feature will not be a long-term solution to the copying problem. Any well-defined technological detection scheme can probably be unwrapped by a technological solution. It is not likely to deter a technically knowledgeable, determined professional or casual "hacker" counterfeiter.

The present copy-protection scheme is a promising start. As electronics continue to grow cheaper and more capable, it is likely that more sophisticated schemes for recognizing attempts to copy currency will be made. Since the committee's concern is the U.S currency, it is interesting to note that good copying of the colors in the present currency are reported to be more difficult than that of some of the varicolored currency of other countries. Post-copying addition of simulations of such features as metallic or variable inks seems possible and can likely be done successfully. The use of metameric ink to "fool" the copier is not likely to be successful in the long run, as market forces will force development of techniques that are resistant to metameric problems in non-currency copying.

Consideration should be given to requiring the application of this technology to all advanced color copiers and printers, as other countries are considering. That depends, of course, on whether the patent holder is willing to license at least some aspects of the technology or if an alternative approach can be found that would be made widely available. Also, the addition of appropriate electronic components to *all* advanced color copiers and printers could increase the price of the low-end models significantly enough to be outside the range of the feasible.

The usefulness of this approach could be enhanced if many nations adopted the same unique feature on their banknotes that would trigger the currency recognition system. In addition to easy detection, such a feature should not require extensive pattern-matching algorithms to match-up scale, geometric orientation effects, etc. A fractal-based self-similar pattern, such as is shown in Figures 4-12, may be useful. The U.S. Treasury Department could take the lead in lead in defining the problem and securing international cooperation in this regard.

It is important to note that the color copier will fail to copy correctly such features as metallic inks, color-shifting inks, and holographic types of features. It is possible to consider machine detection schemes that are capable of discriminating such features on currency and detecting probable attempts to carry out forgeries. The result of a copy operation will be to record whatever optical image of the variable feature is presented through the copier which will necessarily be incomplete and readily detected.

Copier/Printer Identification System

A potentially important feature on some advanced copiers is the encryption of the machine serial number at several locations on all of the copied material. A microdot pattern is used to encode the machine number in every copy that is made. Detection and reading of this encoded microdot pattern require special techniques that must be implemented in the laboratory. The presence of a traceable origin of each copy will probably deter some copying and would make tracing the origin of copied currency possible[14].

Consideration should also be given to extending this technique to color printers, not just electophotographic printers (e.g., ink-jet printers). This may require the addition of additional pre-printing computational processing steps, resulting in a requirement for increased computational power. The cost effectiveness of such a requirement must be closely examined.

Features Used by Other Countries

During its deliberations, the committee considered more than forty types of features that were deemed either to offer an aid to detection of counterfeit currency or to act as a deterrent to counterfeiters. The debate had to take place mainly in the domain of the former, since there are relatively easy measures of success for detection—either in the public marketplace or by official government agencies—whereas it is more difficult to prove a negative in the domain of the latter (i.e., whether due to incorporation of any specific feature, counterfeits have not shown up in circulation).

Of the long list of special features (a described in detail throughout this report), all but about a dozen are already incorporated in world currencies, although some have been introduced only relatively recently (e.g., plastic substrates in Australia) or have been announced to be imminent (e.g. kinegrams in Australia now, in Switzerland in 1995). Thus, at first sight, it might appear that there is a considerable body of experience to draw from, but in actuality there are few quantitative facts. Obvious and intuitive special features such as holograms may have defeated color copiers and other forms of electronic printing but could be relatively easy for proficient counterfeiters to simulate otherwise. They may even be counterproductive in the sense that they may reduce the practical life of the note or focus attention on a single feature of the note. On the other hand, color-shifting inks—now used

[14]The committee realizes that other public policy issues will be raised by this capability. The perspective here is purely from the standpoint of counterfeit deterrence.

by many countries—are more subtle in appearance but defeat color copiers and at this stage would seem to be more difficult to counterfeit by other means. The trade-off would thus seem to favor color-shifting inks, but there are no readily available data to support this conclusion. The situation becomes further complicated by the classification into visible and hidden features. For example, Dutch currency has incorporated visible bar codes, whereas Great Britain uses these codes in hidden form, principally as an aid to the automatic sorting of notes by banks. Most "smart inks" are not obvious unless detected by means of an appropriate physical property, such as fluorescence, phosphorescence, iridescence, and magnetic properties. There are varying degrees of difficulty in copying or simulating these inks using existing technologies. The inks currently used by various countries, but again with little quantitative evidence of effectiveness.

The majority of features deemed attractive for special consideration by the committee have typically already been incorporated in one or more currency (or related documents). On the other hand, technical approaches that appear promising for future research and consideration (e.g., optical fibers in paper) have not yet been incorporated in any known currencies and so there is no practical experience on which to draw.

The overall conclusion is that whereas long lists can be drawn up of currencies incorporating a variety of smart features, there is very little evidence of quantitative effectiveness, or for that matter of sharing any practical experience between countries. Ironically, it is the existence of new emerging global communication technologies (electronic networks and output devices) that presents the opportunity for prospective counterfeiters and that may pose a much more serious problem as these technologies evolve. Just as a single, new high-quality color copier may cause simultaneous counterfeiting problems worldwide, the power of a collective deterrent strategy rather than ad hoc design changes by individual countries will probably become increasingly important.

A handful of nations print their own currency—these are typically the more economically advanced nations—while the remainder are served by a very small number of private printing companies. In that sense, there are only relatively few "independent" blocks of data/experience, and there are existing collaborations between some of these blocks in certain common currency matters. It is important to increase the degree of sharing of counterfeiting/deterrence information.

Other U.S. federal agencies are concerned with secure documents. These include the Postal Service (e.g., postal money orders), State Department (Passport Office), Agricultural Department (e.g., food stamps), and so on. Increased sharing of ideas and experience would be mutually beneficial. Thus it would seem there are obvious avenues for greater sharing of experience and for a collective approach to research in detection and deterrence in the future.

RECOMMENDATIONS

Although there are many new features that can be used to deter counterfeiters, the BEP should continue to utilize intaglio printing, the security thread, and the current substrate material as methods of deterrence against "classical" printing technologies and present day reprographics. In addition, future banknote designs should incorporate additional visible

features to serve as deterrents against counterfeiting and as a means for rapid visual authentication. If analysis shows it is cost-effective to do so, some of these visible features could be incorporated into a banknote and their existence not publicly disclosed until they are needed to thwart a new counterfeiting threat.

The BEP should implement a system of complementary features on each banknote that create added complexity for simulation by all levels of counterfeiters. They should not, however, constrain their design by a requirement that the same set of counterfeit-deterrence features be on all denominations of bills. And although multiple features rather than a single dominant feature should be present on each banknote, the number of announced features should not be so great that it overwhelms the user or does not allow space for future feature incorporation.

The BEP should carry out a redesign of U.S. banknotes to include the recommended features, making such changes in appearance as are necessary to produce a new series of notes that effectively and efficiently incorporates these advanced counterfeiting deterrents. By a wide margin, most banknotes in circulation are genuine. All things being equal, deterrent features that would cause a counterfeit note to look significantly different from a genuine note would probably be more useful to the average citizen than a feature that caused a genuine note to be authenticated upon detailed inspection. On the other hand, a specific machine-detectable feature incorporated in a genuine note would be more useful in a currency-authentication device.

The recommended features fall into three categories: near term, intermediate term, and long term. Within the categories, the deterrent features are not prioritized because of insufficient data relating to implementation issues and the realization that no single feature is adequate protection from even casual counterfeiting.

The committee recommends incorporation of at least some of the following visible features in the *near term:*

- color-shifting inks for printing;
- moiré (alias-generating) line structures, with color added as necessary to enhance the effect;
- security thread modifications—for example, location or width based on the denomination;
- variable-size dot patterns, with color added to enhance the effect; and
- localized watermarks.

Incorporation of at least some of the following features, requiring inexpensive visual aids for detection at the point-of-sale, are recommended for the *intermediate term:*

- infrared inks for printing;
- optically active coated fibers and particles embedded in the substrate; and
- photoluminescent inks for printing.

Longer-term plans for advanced deterrents (listed in alphabetical order) should include additional development and understanding of the following features:

- diffraction-based holograms and related devices;
- embedded zero-order diffraction gratings;
- laminated paper substrates with selected features;
- metallic or specular woven security features;

- optical fibers embedded in the substrate; and
- random pattern encryption methods.

For the *far term,* the BEP should continually assess fundamental advances in the chemical, applied physical, and biological sciences for developments that are applicable to innovative deterrent features. Assessment of research in psycho-physics would also be pertinent since a better understanding of how people perceive visible features may provide insight into the selection of the "best" features.

Before any new counterfeit-deterrent feature is implemented, it should be evaluated by adversary-analysis experts to determine how readily it can be defeated. This process would be aided by having a means to quickly produce currency with appropriate design changes.

There are other elements of a deterrent strategy that can be implemented. To begin with, counterfeit-detection education should be emphasized for point-of-sale persons as a priority, and then for the public at large. Potential incentives that would encourage the public to turn in counterfeits should be closely studied to determine which would be effective and not subject to abuse[15].

Industry should be encouraged to develop effective point-of-sale aids to assist in banknote authentication. Efforts that will lead to a high degree of authentication, particularly for the higher denomination bills, should be continued. These may involve synergistic combinations of visible and hidden covert features that could be related in some way, such as through a public key encryption system.

The Department of Treasury should encourage U.S. legislation to require source identification to be embedded in images produced by new copier and printer systems capable of producing color counterfeit banknotes. In addition, the department should strongly encourage the use of sensors built-into color copier/printer systems that can recognize and inhibit banknote copying. For this approach to be most effective, a unique, high signal-to-noise ratio feature universally applied to currency should be identified and developed, possibly in conjunction with other nations.

[15]The committee believes that counterfeiting should not be a "victimless" crime, since the fear of a loss does provide the public with some incentive to examine banknotes.

REFERENCES

American Bank Note Company. 1984. A Study of the Durability of a Holographic Device for Application to U.S. Currency. February 1984. New York: American Bank Note Company:

Antes, G. 1983. Document with Diffraction Grating. Australian patent abridgment, Au-B-19576/83.

Baird Corporation. 1989. Final Report on Random Label Counterfeit Deterrent, Phase I, Year 1. March 31, 1989. Submitted to Sandia National Laboratory. Albuquerque, N.M. Sandia National Laboratories.

Battelle Columbus Laboratories. 1983. The Impact of Emerging Imaging Technologies on Counterfeiting of U.S. Currency. Final Report to the Board of Governors of the Federal Reserve System. August 16. Columbus, Ohio: Battelle Columbus Laboratories.

Battelle Columbus Laboratories. 1985. Evaluation of Visual Counterfeiting Deterrent Features (VCDSs). Final Report to the Board of Governors of the Federal Reserve System. May 1985. Columbus, Ohio: Battelle Columbus Laboratories.

Battelle Columbus Laboratories. 1990. Identification of Candidate Security Features to Facilitate Machine Validation of U.S. Bank Notes. For Mars Electronics. March. Columbus, Ohio: Battelle Columbus Laboratories.

Bauder, D. W. 1983. An Anti-Counterfeiting Concept for Currency. Systems Research Report PTK-11990. Albuquerque, N.M.: Sandia National Laboratories.

Bander, D. W. 1984. Evaluation of Variable Device Labels for Currency. For the Bureau of Engraving and Printing. Albuquerque, N.M.: Sandia National Laboratories.

BEP. 1990. BEP Specification for Paper: Distinctive, with Security Threads. Specification P:DST-2d. July 31. Washington, D.C.: Bureau of Engraving and Printing, U.S. Department of the Treasury.

BEP. 1991. BEP Specification Change Notice for Paper: Distinctive. Specification P:D-1K. June 28, 1991. Dated March 19, 1991. Washington, D.C.: Bureau of Engraving and Engraving and Printing, U.S. Department of the Treasury.

Berning, P. H., and R. W. Phillips. 1987a. Thin Film Optically Variable Article and Method Having Gold to Green Color Shift with Angle and Method. U.S. Patent 4,705,300. November 10.

Berning, P. H., and R. W. Phillips. 1987b. Thin Film Optical Variable Article Having Substantial Color Shift with Angle and Method. U.S. Patent 4,705,356. November 10.

Brettler, H. 1992. Presentation by H. Brettler, Director General, SICPA, SA, Switzerland, to the Committee on Next-Generation Currency Design. October 22, 1992.

Buckley, L. 1992. Presentation by Len Buckley, Bureau of Engraving and Printing, to the Committee on Next-Generation Currency Design. October 21, 1992.

Canadian Banknote Company. 1966.U.K. patent 1,138,011. Improvements in Printed Matter for the Purpose of Rendering Counterfeiting More Difficult.

Canon, 1990. Apparatus for Image Readers or Processing. European patent application EP 382,549. August 16, 1990.

Church, S. 1992. Presentation by Sara Church, Bureau of Engraving and Printing, on durability tests for U.S. banknotes to the Committee on Next-Generation Currency Design. September 1992.

Church, S. 1993. Test results update, Bureau of Engraving and Printing, on durability tests for U.S. banknotes to the Committee on Next-Generation Currency Design. June.

Church, S. 1993. Personal communication from Sara Church, Bureau of Engraving and Printing. August 1993.

Church, S., and D. Littman. 1991. Machine Reading of Visual Counterfeit Deterrent Features and Summary of U.S. Research, 1980-1990. Four Nation Group on Advanced Counterfeit Deterrence, Ottawa, Canada. September 1991.

Collins, B. L. 1986. Visual Assessment of Holograms. For the Bureau of Engraving and Printing. Gaithersburg, Md.: National Bureau of Standards.

Crane, T. 1992. Presentation by Tim Crane, Crane & Co., to the Committee on Next-Generation Currency Design. October 22, 1992.

Crane, T. 1993. Personal communication from Tim Crane, Crane & Co. August 16, 1993.

Dobrowolski, J. A., F. C. Ho, and A. Waldorf. 1989. Research on thin film anticounterfeiting coatings at the National Research Council of Canada. Applied Optics 28: 2702-2717.

Evans, R. M. 1974. The Perception of Color. New York; John Wiley & Sons.

Fagan, W. F., Ed. 1990. SPIE Proceedings on Holographic Optical Security and Anticounterfeiting Systems. Vol. 1210 (January 1990). Bellingham, Wash.: SPIE-The International Society for Optical Engineering.

Fagan, W. F., Ed. 1991. SPIE Proceedings on Holographic Optical Security and Anticounterfeiting Systems. Proceedings of the Society of Photo-Optical Instrumentation Engineers. Vol. 1509 (March 1991). Bellingham, Wash. SPIE-The International Society for Optical Engineering>.

Farrand, J. 1993. Presentation by J. Farrand, James River Corporation, to the Committee on Next-Generation Currency Design. January 19, 1993.

Gale, M. T. 1991. Diffractive microstructures for security applications. Pp. 205–209 in Proceedings of the Third International Conference on Holographic Systems, Components and Applications, Edinburgh, September 16–18, 1991 (IEE Conf. Pub #342). Piscataway, N.J.: IEEE Press, .

Gale, M. T., K. Knop, and R. Morf. 1990. Zero-order diffractive microstructures for security applications. Pp. 83–89 in Proceedings of the International Society for Optical Engineering—SPIE 1210.

Graminski, E. L. 1993a. Personal communication from Edward L. Graminski, Bureau of Engraving and Printing Intaglio Research Institute, Bureau of Engraving and Printing. August 1993.

Graminski, E. L. 1993b. Personal communication from Edward L. Graminski, Bureau of Engraving and Printing Intaglio Research Institute, Bureau of Engraving and Printing. September 30, 1993.

Graybeal, S. N., and P. B. McFate. 1989. Getting out of the STARTing block. Scientific America 261(6):64–65.

Haslop, J. 1993a. Presentation by J. Haslop, Thomas De La Rue Company, to the Committee on Next-Generation Currency Design. June 1, 1993.

Haslop, J. 1993b. Presentation by J. Haslop, Thomas De La Rue Company, on international experience with counterfeit deterrence features to the Committee on Next-Generation Currency Design. March 1993.

Hellman, N. E. 1979. The mathematics of public key encryption. Scientific American 241,(2): 130-9.

Hepfinger, M. J. 1993. Presentation by M. J. Hepfinger, U.C. Army Natick RD&E Center to the Committee on Next-Generation Currency Design. January 19, 1993.

Hill, A. R. 1987. How we see color. Color Physics. Bradford, England: Society of Dyers and Colourists.

ICI Colours, Inc. 1993. Test results and private communication from ICI Colours, Inc. July 1993.

James River. U.S. Patent 5,128,182. 1993. Innovative Deterrence Features for Substrates.

Kendrick & Jefferson Ltd. 1988. UK Patent Application GB 2,224,240A Copy Protection of Muli-colour documents.

Kühn, H. 1986. Conservation and Restoration of Works of Art and Antiquities, Volume I. London: Butterworths.

Lee, R. A. 1988. Diffraction Grating. Australian Provisional Patent Application, PJ 2020.

Lee, R. A. 1991. Pixelgram: An application of electron beam lithography for the security printing industry. Pp. 48–54 in Holographic Optical Security Systems, W. F. Fagan, ed. Proceedings of the Society of Photo-Optical Instrumentation Engineers. Vol. 1509. Bellingham, Wash.: SPIE—The International Society for Optical Engineering.

Longhurst, R. S. 1973. Geometrical and Physical Optics. London: Longman London.

Martin, C. R. 1983. Final Report—Stages I through IV, Public Acceptance of Proposed Changes in United States Currency. For the Federal Reserve System. June 1983. Federal Reserve System.

Morris, G. M. 1992. Presentation by G. M. Morris to the Committee on Next-Generation Currency Design on aliasing in sampled data systems.

Norton, S. M., D. H. Raguin, and G. M. Morris. 1993. Effective medium theory approach to guided-mode resonances. Optical Society of America (OSA) Topical Meeting on Optical Design for Photonics, Palm Springs, California, March 22–24, 1993. Washington, D.C.: Optical Society of America.

National Research Council (NRC). 1987. Counterfeit Threats and Deterrent Measures. National Materials Advisory Board. Washington, D.C.: National Academy Press.

Patton. B. 1993. Presentation by Bill Patton, General Electric Aerospace, to the Committee on Next-Generation Currency Design. March 16, 1993.

Pavlidis, T., J. Swartz, and Y. P. Wang. 1991. Information encoding with two-dimensional bar codes. Computer 25(6): 18-28.

Pennisi, 1991. Bolder bar codes. Science 140:160-107.

Phillips, R. W. 1990. Optically variable films, pigments, and inks. Pp. 98–109 in Optical Thin Films III: New Development. Proceedings of the Society for Photo-Optical Instrumentation Engineers. Vol. 1323. Bellingham, Wash.: SPIE-The International Society for Optical Engineering.

Phillips, R. W. 1993. Presentation by R. Phillips, Flex Products, Inc., to the Committee on Next-Generation Currency Design. January 19, 1993.

Pratt, W. K. 1968. Introduction to Fourier Optics. New York: McGraw-Hill.

Reinhart, W. 1991. Advanced hot stamping foil based OVD technology: An overview about security applications. In Holographic Optical Security Systems, W. F. Fagan, Ed. Proceedings of the Society of Photo-Optical Instrumentation Engineers. Vol. 1509. Bellingham, Wash.: SPIE-The International Society for Optical Engineering.

Rivest, R. L., A. Shamir, and L. Adelman. 1979. A method for obtaining digital signatures and public key cryptosystems. ACM 26(1): 96-99. Cambridge, Mass. MIT Laboratory for Computer Science.

Sensor, 1992. Selecting anti-alias filters. Sensors 9(11): 14-23.

Spannenburg, S. 1991. Frequency modulation of printed gratings as a protection against copying. Pp. 88–104 in Holographic Optical Security Systems, W. F. Fagan, ed. Proceedings of the Society of Photo-Optical Instrumentation Engineers. Vol. 1509. Bellingham, Wash.: SPIE-The International Society for Optical Engineering.

Storch L., and E. van Haage. 1989. Information Transfer and Use, Particularly with Respect to Objects Such As Gambling Chips. U.S. Patent 4,814,589.

Thomas De La Rue and Company, Ltd. 1985. European Application EP 204,552A. Improvements in and relating to printed documents resistant to counterfeiting.

Thomas De La Rue and Company, Ltd. 1992. Colour Copiers 1970-1992. Eighth International Conference on Currency Counterfeiting and First International Conference on Fraudulent Travel Documents, April - May 1, 1992. Ottawa, Canada. International Criminal Police Organization (INTERPOL), Lyon, France.

Tsujita, J. 1993. Presentation by J. Tsujita, Cannon USA, to the Committee on Next-Generation Currency Design. March 16, 1993.

Wang, S. S., R. Magnusson, and J. S. Bagby. 1990. Guided-mode resonances in planar dielectric-layer diffraction gratings. Journal of the Optical Society of America 7(8): 1470-14F4.

Wicker, 1991. Counterfeit Protected Document. U.S. patent number 5,018,767. May 28, 1991.

BIBLIOGRAPHY

American Society for Testing and Materials (ASTM) Committee F-12 on Security Systems and Equipment, F1448 Guide for Selection of Security Technology for Protection Against Counterfeiting, Alteration, Diversion, Duplication, Simulation, and Substitution (CADDSS) of Products or Documents.

Becker, H., and F. Piper, 1992. Cypher Systems New York:, John Wiley & Sons, Inc.

Dobrowolski, J. A., F. C. Ho, and A. Waldorf, 1989. "Research on thin film anticounterfeiting coatings at the National Research Council of Canada. Applied Optics 28: 2702-2717.

Durbeck, R. C. and S. Sherr, editors. 1988. Hard Copy Output Devices. New York: Academic Press.

Fagan, W. F. Ed., 1991. Holographic Optical Security Systems. Bellingham, Wash.: SPIE-The International Society for Optical Engineering.

Fagan, W. F. Ed., SPIE Proceedings on Holographic Optical Security and Anticounterfeiting Systems. Systems on Vol. 1210, January 1990. Bellingham, Wash.: SPIE-The International Society for Optical Engineering.

Gross, A. 1970. Etching Engraving and Intaglio Printing. London: Oxford University Press

Kühn, H. 1986. Conservation and Restoration of Works of Art and Antiquities, Volume I. London: Butterworths.

MacAdam, D. L., Ed. 1993. Colorimetry—Fundamentals, Holographic Optical Security Systems. Bellingham, Wash.: SPIE-The International Society for Optical Engineering.

National Research Council (NRC). Counterfeit Threats and Deterrent Measures. 1987. National Materials Advisory Board. Washington, D.C.: National Academy Press.

National Research Council (NRC). 1985. Advanced Reprographic Systems: Counterfeiting Threat Assessment and Deterrent Measures(U), Wash. D.C.: National Academy Press.

Pavlidis, T., J. Swartz, and Y. P. Wang. 1992. Information encoding with two-dimensional bar codes," Computer 25(6): 18-28.

Phillips, R. W. 1990. Optically variable films, pigments, and inks. Pp. 98-109 in Optical Thin Films III: New Development. Proceedings of the Society for Photo-Optical Instrumentation Engineers. Vol. 1323. Bellingham, Wash.: SPIE-The International Society for Optical Engineering.

Proceedings of the International Conference on Security Documents for the 21st Century, April 1-3, 1987, San Diego, Calif. prepared by Oak Ridge National Laboratories, CONF-87040175, Contract DE-AC05-840R2140, Oak Ridge, Tennessee 37831.

Ross, J. and C. Romano. 1974. The Complete Intaglio Print. New York: The Free Press, MacMillan.

Schaffert, R. 1980. Electrophotography, Focal Press.

Schein, L. B., 1988. Electrophotography and Development Physics. New York: Springer-Verlag.

U.S. Treasury Department. 1991. Your Money Matters. Wash. D.C.: Bureau of Engraving and Printing.

5

COUNTERFEIT-DETERRENT STRATEGIES

A comprehensive counterfeit-deterrence program for U.S. banknotes must contain many elements to respond to the threats discussed throughout this report. This chapter summarizes those elements that can be used to formulate a comprehensive national strategy that can reduce future counterfeiting incidents of U.S. banknotes. Such a strategy entails far more than a one-time incorporation of a new set of counterfeit-deterrent features in banknotes. Required is a guiding philosophy that includes responding to emerging threats before they become a significant problem; identification, selection, and rapid incorporation of appropriate deterrent features; use of devices to aid authentication of banknotes (i.e., using more than visual inspection alone); public education and acceptance of the changes; implementation of appropriate law enforcement strategies; and continuing exchange of information with other countries of the world.

It is commonly accepted that at least half of the solution to a problem consists of the recognition of it, plus careful and complete definition of it. Thus, the increasing awareness by the U.S. government regarding the counterfeiting threat and its growing severity is the critical step toward the derivation of an effective, anticipatory, multifaceted, anticounterfeiting program.

The recently established anticounterfeiting task force composed of representatives from various agencies within the Department of Treasury (including the BEP, the Federal Reserve, and the Secret Service) is a very positive step. This task force will be far more credible and effective than any of the individual members acting alone.

RESEARCH AND DEVELOPMENT STRATEGIES

Technology Advancements

A long-term deterrent strategy must anticipate and lead the evolution of reprographic systems and the level of expertise of the counterfeiting community. Technological progress in nonimpacting printing will continue to be driven by many market forces in a never-ending quest for accuracy and quality, and it is imperative that the Department of Treasury be kept informed of developments in ample time to respond to a future threat. In the same manner, the skill level of counterfeiters will change as they attempt to improve their craft. Continuing information must be provided in these two areas.

Appropriate mechanisms for the Department of Treasury to stay up-to-date can include the use of advisory panels, committees, workshops, and briefings that address technological advances in reprographics and a continuing forensic evaluation of counterfeiting techniques and methods. In the latter case, knowing that a counterfeit has been created and its production eventually stopped is a reaction mode of operation and is the domain of the Secret Service; the Treasury Department along with the Federal Reserve Board should anticipate advances in the level of sophistication of the counterfeiter, adjust the type and timing of deterrent features accordingly, and perform in a proactive mode.

There is a considerable amount of scientific and technological work underway in university, industrial, and government research laboratories that could have relevance for future counterfeit deterrence. However, the link between these research results and the BEP's needs would not normally be made in a timely way unless the efforts were specifically geared to that end.

Cases in point are the many emerging photonic materials that can serve in the future as active deterrent features that is, they can make the counterfeit bill look outstandingly different. One class of candidates would be photo-induced charge-transfer complexes. These materials, of which there are a large number, change their light-absorption characteristics upon exposure to intense light. The mechanism involves the transfer of an electron from a "donor" molecule to an "acceptor" molecule when activated by photonic energy. For example, a copy of an image printed in an ink that contained such material would show a "color" (usually dark green, brown, or black) where there was none apparent in ambient light for the genuine banknote. Many of these reactions are completely reversible.

Another class of photonic materials that may some day be useful are those that exhibit nonlinear optical properties, such as some fullerene derivatives. They convert long wavelength light to shorter, more energetic wavelengths. These materials can be used to shift light wavelengths in interesting, and perhaps useful, ways, such as for light-frequency doubling with photo-emitting compounds. Nonlinear optical materials combined with reversible saturable absorbers (i.e., in which light transmission decreases as exposure increases) may also lead to very useful combinations of future features. These materials are not now suitable for use in banknotes, but further dramatic developments can radically change this assessment. There are many other such examples.

In the recent past, the counterfeiting-deterrence research and development program at the BEP has drawn primarily on external technical work, with little internal research. This balance may be shifting; the BEP recently announced the formation of the Security Technology Institute within the organization (Church, 1993). The breadth and quality of the investigations, procurements, and external research and development support of anticounterfeiting methods, techniques, and materials has improved considerably since the earlier National Materials Advisory Board studies. The committee strongly supports a more balanced approach between external and internal work, as long as the internal work does not duplicate external efforts. Internal research and development activities that included a

component of fundamental research would permit the BEP to become a "full-fledged" member of the technical community and be able to capitalize on pertinent scientific and technological advances.

The same mechanisms suggested above for keeping the Department of Treasury up-to-date with advancements in reprographic technology and counterfeiting methods (e.g., advisory panels, committees, workshops, and briefings) would be appropriate[1].However, more in-depth preparatory work would be required, since the amount and detail of information is immense. The benefit of such planned interactions would be a leveraging of the research already going on and increased awareness in the general research community regarding the needs for counterfeit-deterrent features.

Realistic Testing and Specifications

A program must be in place to continually devise and evaluate new deterrent features. An essential part of such a program would be the re-evaluation of the testing specifications and their relevance to real-world wear and tear in order to not preclude the use of some exceptionally effective features that may fail an overly demanding test. The current BEP efforts to examine the suitability of chemical resistance tests should be extended to other test specifications. Some consideration should also be given to learning how banknotes of different denominations are handled and determining if the durability requirements can be different for higher denomination banknotes.

Implementation of Changes

The BEP estimates that under normal circumstances when competitive contracting must be used, approximately 2 to 5 years are required from the time it decides to use a new deterrent feature until that deterrent appears in new currency (Sellers, 1993). (The time required for implementation can be considerably shorter if the changes can be implemented internally without the need for competitive contracting.) Approximately 1 to 2 years are required to develop the specifications, complete all the testing, and produce proofs. Up to 2 years may be required for the competitive contracting process, and 1 year for production incorporation. Additional time may be required if no offer fully meets the specification, if the proposed prices are too far above the estimated cost, etc. However, if the new feature is an upgrade to a current feature, then the process time can be shortened to about 1 year.

Thus, under normal circumstances a feature must be targeted at a counterfeiting threat well before the threat is fully realized. Counterfeiters will thus enjoy a period of time to learn

[1]One of the strongest recommendations of prior National Materials Advisory Board studies was the selection and use of a technical advisory group consisting of experts to serve as a "sounding board" and provide counsel, guidance, and direction to the development of advanced features.

how to simulate a feature. The security thread provides a case in point. The thread was targeted at counterfeiters who were using nonimpact printing reprographic technology. The existing supplier of currency paper originally expected to have the new paper available for the printing of the first notes with the new thread within 2 years of go-ahead. However, the introduction of the thread was delayed for a year since the supplier had difficulty in meeting all the specifications during production scale-up. Today, approximately 2 years after its introduction in Series 1990 $100 bills, only a few counterfeit notes with the security thread have been attempted. (Of course, the older notes without the thread are still legal tender.) Although these simulations would not withstand close examination, they have been successfully passed (Brown, 1993a)[2]. As banknotes containing the security thread become more prevalent, it is highly probable that professional counterfeiters will devote more effort to producing better simulations[3].

Methods must be developed to shorten the time required to produce redesigned banknotes once the decision to proceed has been made. As color printers and copiers become more prevalent and sophisticated, effectiveness lifetimes of deterrent features may decrease, making faster response critically important. Strategies could include conducting additional production risk assessment before the changes are finalized, expediting the contracting process, and establishing a timetable for periodic assessment and replacement of, addition to, or modification of counterfeit-deterrent features.

As part of a major currency redesign effort, some visible features could be incorporated in anticipation of future threats but not initially disclosed. These features could be “held in reserve” and disclosed as the currency comes under attack. This strategy may prevent counterfeiters from having advance notice of their presence and ample time to practice their simulation. Features could also be introduced that lend themselves to further improvements and upgrading as required, without the necessity for major design changes. Of course, too many changes within too short a time period would only serve to confuse the public, making the counterfeiters' job easier.

SELECTION OF COMBINATIONS OF FEATURES

There is no single visible deterrent feature that is readily recognizable, highly durable, impractical to counterfeit or simulate, available at low cost, and easy to produce. Indeed, if a single dominating feature were employed, the currency would tend to be less secure, since that feature would present a single target for the counterfeiter. Multiple features add complexity to the counterfeiter's task and increase the number of counterfeiting steps to the point that the casual counterfeiter would “give up”. A determined professional counterfeiter still may be

[2]A skilled counterfeiter using a lithographic printing over a pasted simulated “thread” successfully passed the new note 18 months after its introduction.

[3]The BEP estimates that about half the $20, $50, and $100 banknotes in circulation now (mid-1993) contain the security thread.

tempted, but the task should be sufficiently difficult that the risk of getting caught would be high. Therefore, a combination of features will be required to provide a high level of practical counterfeit deterrence.

In general, any single deterrent feature can be simulated or overcome if the counterfeiter is creative and willing to perform the necessary additional steps. For that matter, given sufficient time and effort, any combination of features can be simulated. These tasks would not necessarily require sophisticated technical expertise or particularly expensive equipment, since simulation need not be highly accurate. The general public appears to be reluctant to observe and confront, and hence the chances are good that a banknote will only undergo a cursory inspection at the first encounter. Once a counterfeit enters the monetary system, its point of origin generally becomes "fuzzy." Counterfeits produced with reprographic equipment are especially difficult to trace.

The most straightforward way to curb counterfeiting is at the source. A copier or computer printer can be prevented from copying a banknote by employing appropriate pattern recognition technology. The "print engine" can be taught to recognize a banknote and then refuse to operate properly until the offending print request is terminated or the equipment is reset. Such a capability would significantly discourage the casual, nontechnical counterfeiter. The effectiveness of such devices would be enhanced if a standard banknote feature, or small set of such features, was adopted by many countries; however such features must be unique to currency to preclude inadvertent disabling of the copier or printer.

Whereas the simulation of multiple deterrent features may not require expertise and sophisticated equipment, it does require an investment of time—a considerable investment if the simulations are done by hand, one at a time. The goal of a balanced system of deterrents, therefore, must be to make the process of overall simulation so time consuming that the counterfeiter is discouraged and abandons the task. This is accomplished by deploying a complementary set of features, each requiring a different simulation process. Each additional feature should address a potentially weak attribute of the existing set that is, it should add value to the overall system of deterrents. Such a defense in depth would address different reprographic technologies, different levels of counterfeiter expertise and tenacity, and the requirements of different viewing conditions for authentication. Care must be taken, however, that the overall visual effect remains balanced so that one deterrent does not dominate, lest the lesser deterrent not be carefully viewed. The combination of features must not produce an unpleasant appearance. (Examples of possible combinations are presented later in this chapter.)

The primary threat is the casual counterfeiter, defined in Chapter 2 as an individual who will attempt to use the output of a reprographics system directly without engaging in additional complicated steps needed to simulate deterrent features. Individual features that do not reproduce, or features that result in the copy appearing blatantly obvious, are therefore effective against this type of threat since an attempt will probably not be made to pass it. Any number of features that can not be easily copied or scanned satisfy this requirement; (e.g., color-shifting inks, holograms, watermarks, etc). Discouraging the hacker is more difficult and is best accomplished by having a larger number of deterrents, each requiring a different means and material for simulation. The goal here is one of attrition; overwhelm with so many tasks

that the counterfeiter eventually "gives up." With the semiprofessional, deterrents should be selected that are more difficult and expensive to simulate accurately. These individuals deal in much higher volumes than the casual counterfeiter and hacker, and their product must be of higher quality. They are more subject to the economics, time and cost, of the process. Very little can be done to stop the dedicated professional except the periodic addition of new features designed to introduce delays into the counterfeiter's "product" cycle.

As part of a system of features, the banknote substrate offers an important dimension for embedding features that are particularly useful and compatible with many other surface features. Security threads, watermarks, patterns, images, etc., may be incorporated with minimum disruption of the overall architecture. Visible only in transmission and not in reflection, they are immune to reproduction by copying or scanning means. Required is the allocation of a clear, unprinted area for viewing clarity.

In summary, the following general criteria can be considered for evaluating combinations of anticounterfeiting deterrents:

- all those that applied to individual deterrents (see Chapter 3);
- extent to which all three types of counterfeiters are expected to be deterred deterrence against specific counterfeiting methods e.g., color copiers/scanners /printers, photography, offset printing, etc., and deterrence against counterfeiting skill levels;
- synergistic relationships among the deterrents;
- range of sensors available for detecting the features, for either the manual or automated mode; and
- how easy it would be to add, replace, or upgrade one or more of the deterrent features.

Examples of possible feature combinations are

- color combined with variable-sized dot pattern or induced moiré;
- print with photoluminescent ink on security thread;
- laminated paper with watermarks on both halves to create a complex image; could also add various other transparent or low-optical-density deterrents in the same window;
- transparent (non-metallized) hologram, kinegram, pixelgram, or zero-order submicron diffraction grating in the same window as a watermark, induced moire line pattern, or variable-sized dot pattern.

Combinations of features that score high using the above criteria should be incorporated into test banknotes. These could then be subjected to adversarial analysis to determine their deterrent effectiveness and used to gauge public acceptability through mechanisms such as focus groups.

REACTIVE AND PROACTIVE STRATEGIES

Overt, visible deterrent features in a banknote that are very difficult to reproduce serve as the most obvious means of authentication. But every feature should be viewed as having a finite lifetime, since the threat will continue to evolve as reprographic technology continues to advance and the social environment changes. The rate of counterfeiting has been observed

to increase over time until changes are made. Counterfeiting using copiers and printers has been observed to be increasing at a geometric rate during the last 3 years. Therefore, additional features, or additional enforcement actions, will be needed to reverse the rate and cause it to fall back to a lower level. Not all features of interest will be ready for incorporation at the same time and hence should be planned to be phased-in over time, as needed.

Some deterrents may turn out to have a short lifespan. They may be introduced to combat a particular threat and become less effective against assault by newer equipment as reprographic systems improve. Microprint, for example, which was adequate to thwart low-resolution systems for a while, will become less effective as 400-dpi and 600-dpi systems come into wider usage. This example also indicates the benefit of not relying on a single deterrent feature.

Two general strategies that can lead to appropriate changes in currency design have been postulated. A *reactive strategy* is one in which no action is taken or new feature added until the counterfeiting rate reaches a relatively high level. This rate, the *threshold of tolerance,* is the point at which a change is made. However, a dramatic decrease in the extent of counterfeiting would also require the rapid withdrawal of the old, compromised currency from circulation. Case A in Figure 5-1 schematically depicts the reactive scenario. The counterfeiting rate increases to a high level at which time drastic action is taken, and the rate precipitously declines. It then begins to climb again as the counterfeiters respond to the new deterrent. In reality, the scenario would be much more complex than schematically indicated, so the figure is only notional. For instance, replacement of older-design currency would take considerable time. The counterfeiting rate would thus continue to climb for a while at a smaller rate, and it would not decline so sharply once the rate began to decrease.

Practical advantages of this strategy include the rapid coalescence of a consensus for change, and the high likelihood that sufficient resources will quickly be brought to bear to solve the problem. But the disadvantages are substantial. They include lost public confidence in the federal government and the prospect that the dramatic changes will be expensive and upsetting to a large portion of the public.

A*proactive strategy* to currency design is one in which new features are incorporated in anticipation of future threats, before a large increase in counterfeiting occurs. Relative to the reactive strategy, this approach employs a much lower *threshold of tolerance.*

It is schematically depicted as Case B in Figure 5-2. The potential increase in counterfeiting rate is the same as for Case A except that action is taken to reduce the rate much sooner. Therefore, the actual rate never gets very high, relatively speaking. As before, the curves are idealized simplifications; the actual situation would be more complicated.

The practical advantages of the proactive approach include the containment of small counterfeiting problems and the orderly transition to new currency designs. A principal disadvantage is the expected difficulty of achieving a consensus for a change, since the exact magnitude of the future threat cannot be precisely known. If the threat is perceived as being low, adequate resources for counterfeit deterrence might not be made available. Also, more changes to currency design would probably be made under this strategy.

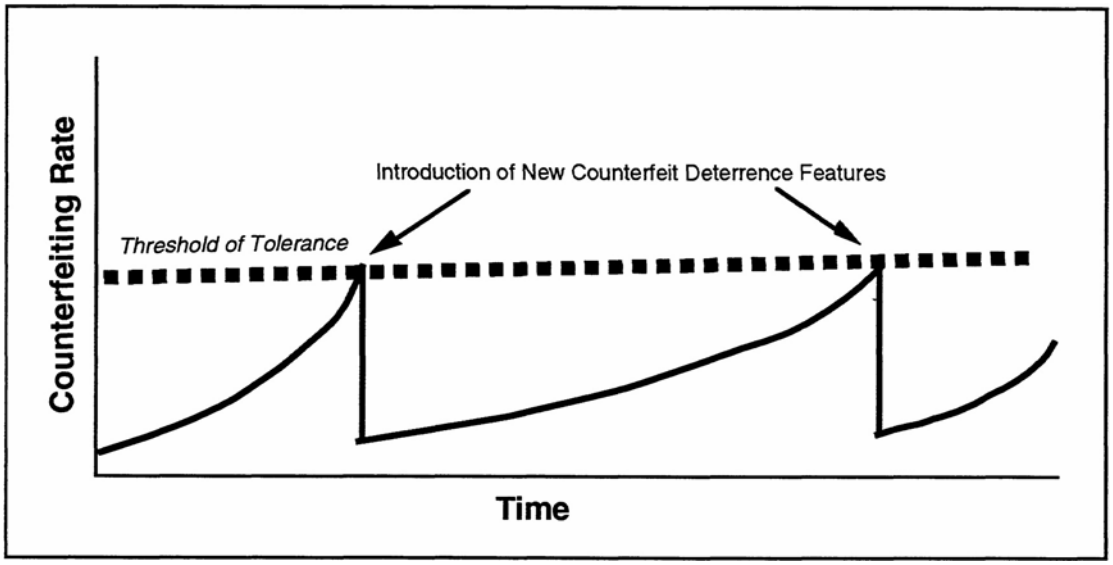

FIGURE 5-1 Case A: reactive strategy.

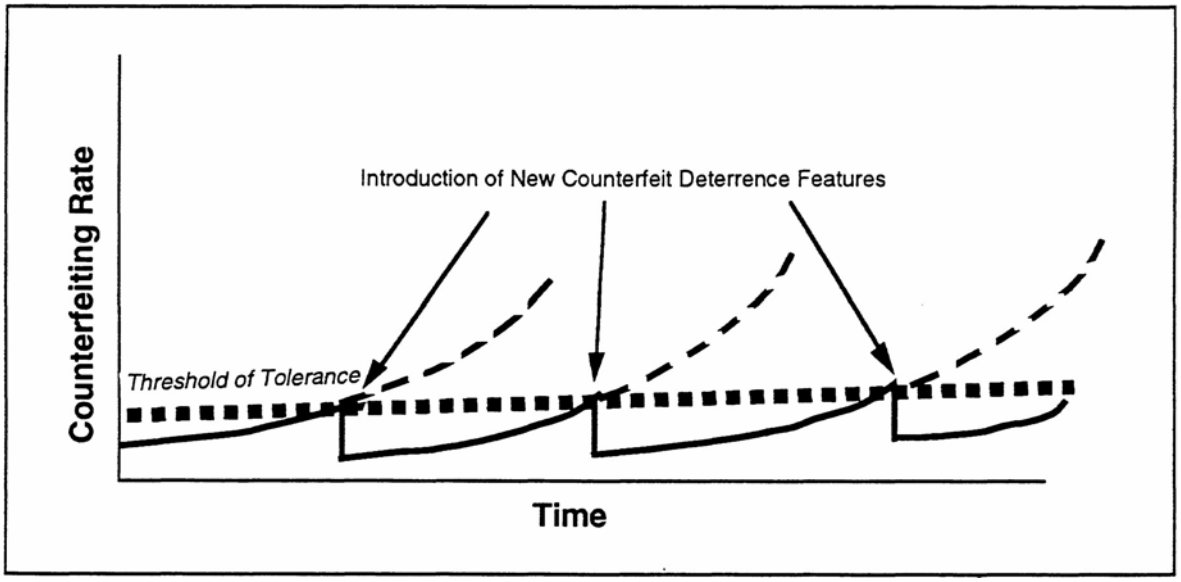

FIGURE 5-2 Case B: proactive strategy.

In both cases, the *threshold of tolerance* curve would be shifted upward depending on the policy employed regarding the rate of withdrawal of the older currency from circulation. Figure 5-3 depicts the average age of U.S. banknotes, based on recent Federal Reserve System data. The lower-denomination bills have a relatively short lifetime compared the higher denominations, but the higher denominations are those that present the most attractive counterfeiting targets. Therefore, phase-in of changes should start with large denomination bills.

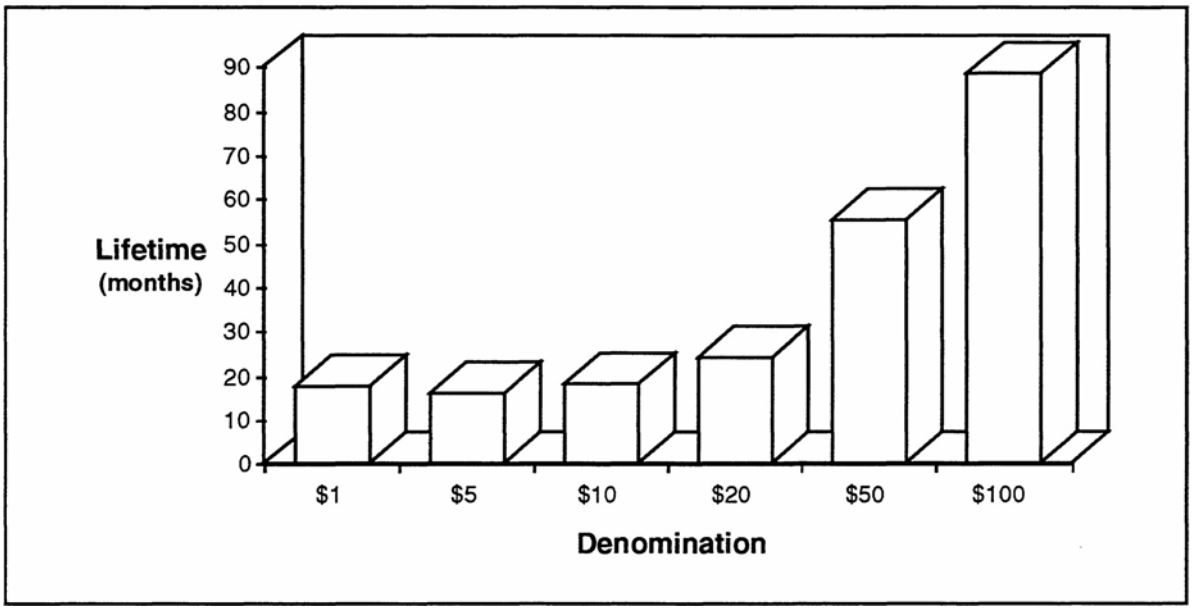

FIGURE 5-3 Average lifetimes of U.S. banknotes.

In line with this approach, phasing-in deterrents over time requires the adoption of a long-range plan that anticipates the deployment of a new deterrent with minimum overall design impact. Establishment of a base design should take into account the requirements of future additions so that the visual appearance of a banknote would not markedly change. An example would be a design that contains clear (unprinted) areas on both sides of a note for the eventual incorporation of a localized watermark. The general goal is to maintain design integrity and avoid a patchwork visual appearance.

An old visible deterrent, made obsolete by the latest technology, may still serve a purpose as it will continue to be useful against lower-level reprographic technologies. Also, its absence may be noted by a substantial portion of the public and be cause for false rejections. Discontinuance of a deterrent also presents the counterfeiter with a somewhat easier task, as it may eliminate extra steps required for simulating the feature. Upgrades or changes to a deterrent to render it more effective should be considered as a relatively fast and inexpensive option for improving security. One example, mentioned in the previous chapter, is the possibility of changing the location or width of the security thread, or the number of security threads, according to banknote denomination.

However, there may be a cost penalty associated with retaining a less-effective feature, and this must be weighed against the value of retention. Also, there is only so much "real estate" on the banknote; at some time, features will have to be removed to make room for newer ones.

VALIDATION/DETECTION DEVICES

In order to accelerate and standardize the authentication process, the use of low-cost, relatively unobtrusive devices should be considered, particularly at point-of-sale locations. Just as reading the magnetic stripe on a credit card is universally accepted as normal, devices that enhance the visibility of deterrent features may facilitate the detection of counterfeits, speed the process up, and overcome resistance to careful inspection. Simple means, such as illuminated panels at store registers to help view embedded substrate features, mounted 10-power magnifying glasses to view microfeatures, or a combination of the two to confirm front-to-back registration, are illustrative.

There appears to be a general reticence in the general public and point-of-sale personnel to hold currency up to the light for very careful scrutiny or to examine it under magnification. Therefore, deterrents easily discernible by casual, nearly effortless inspection would be more effective. However, the use of simple, fast authentication devices at point-of-sale locations would also be effective. The committee believes that if such devices were available, the public would accept them just as credit-card authentication is widely accepted.

Simple systems can also be envisioned to render visible simple hidden features, such as ultraviolet fluorescent inks, infrared absorbing inks, and embedded special fibers. More-sophisticated measurement systems can be devised that are more effective, using both overt and covert features, but these will have to be judged on the basis of the cost and reliability requirements. Authentication sensors at each point of sale should cost less than the systems used today to validate credit-card transactions but might be slower, since usually more than one banknote is offered for payment.

Authentication of credit cards has become commonplace and the delays more or less tolerated, because there is a general awareness that they may be stolen or otherwise used fraudulently. Because of this, delays are inevitable, and many merchants employ cash-only registers to help speed the check-out process. Authentication of banknotes should not seriously ompromise the flow of business, hence it is essential that personnel be well-trained, features be designed for ready authentication, and adequate support be commercially available.

Somewhat higher-cost sensor systems are suitable for use in vending and change machines for automatic validation. Many of the proposed innovative visual features can be detected with relatively simple optical systems, such as a light source, filters, and photodetectors. Development of a strategy for machine readability may provide the infrastructure and cost leverage for introducing greater levels of sophistication in point-of-sale devices.

PUBLIC EDUCATION AND ACCEPTANCE

By definition, an overt feature is one that can be seen in ambient light by a person with normal vision, with the unaided eye, or with a simple aid. But such a feature cannot be effective if the public is unaware of its existence. Since there is a wide variation in the vision capabilities within the human population, a concentrated effort should be made to define the appropriate metrics for what features can be seen in "ambient light" by a person with "normal vision."

The front line of defense comprises the point-of-sale and transaction personnel who handle currency as a part of their job. Thus, in order to be an effective counterfeit deterrent, visible features must be accepted and widely used by them. Acceptance embodies an understanding of the need (the magnitude of the threat), a confidence that the U.S. government has provided safeguards for the detection of counterfeits, and a visually pleasing appearance for the new banknote designs. Use implies that personnel know what to look for and that feature visibility is sufficient to allow ease of authentication and create minimum delays at the point of sale.

These requirements must be accomplished with a properly designed program of public information and education with emphasis on point-of-sale/transaction personnel. Care must be taken so as not to create a panic; the monetary system has not been flooded with counterfeit banknotes, and older banknote issues are not being recalled. At the same time, however, the public must be made aware that technological advances in copying, scanning, and printing have reached the point where there is indeed a threat that counterfeiting can become widespread.

LAW ENFORCEMENT CONSIDERATIONS

New law enforcement strategies to prevent counterfeiting at the source can be envisioned that respond to the diffuse threat posed by many casual counterfeiters who use readily available reprographic equipment to print a few counterfeit notes each. For example, the ability of law enforcement agents to track copied banknotes back to a specific copier would greatly assist forensic investigations of counterfeiting. Currently, there is no effective reward structure to provide incentives for the public's interception of a counterfeit note close to the initial distribution point. In fact, there is a disincentive to do so, since the finder of a counterfeit note must turn it in without receiving any offsetting compensation. On the other hand, if the compensation were set at too high a level, counterfeiting might then be viewed by the public as a victimless crime in which the government would sustain the loss. This would not assist law enforcement either; if the government made up the entire loss, there would be little incentive for the public to try to identify passers of bogus notes. This is an issue of major public policy. The public is apt to view casual counterfeiting as a small-time fraud that is not seriously harmful.

INFORMATION EXCHANGE

Virtually every country in the world now incorporates counterfeiting deterrents in its currency. Thus, there is a wealth of information being generated worldwide about the effectiveness of new features, feature durability, public acceptance, counterfeiting methods, and new features under development. A concerted effort should be mounted to open a pathway by which this information, in as quantitative a form as possible, can be shared to mutual advantage.

For example, the Japanese government has deterrent features built into its currency. Nonetheless, 280 lithographic printed counterfeit 10,000 yen notes (~ $89 each) were recently discovered in the Osaka region. The resulting counterfeiting "scare" led to the shut-down of thousands of ticketing and money-changing machines in the area. Japan's central bank is preparing to issue a new "copy-proof" currency (Brown, 1993b). The effectiveness of these changes in deterring counterfeiting would be of great interest to the Department of Treasury.

There is at present no focused effort to comprehensively record and assess all the incidents and means of counterfeiting U.S. banknotes in all countries of the world. An appropriate data collection system should be instituted so that the entire scope of the counterfeiting threat could be determined.

REFERENCES

Brown, J. 1993a. Discussion with Special Agent James Brown, U.S. Secret Service, at meeting of the Committee on Next-Generation Currency Design.

Brown, J. 1993b. Personal communication from Special Agent James Brown, U.S. Secret Service. August 1993.

Church, S. 1993. Personal communication from Sara Church, Bureau of Engraving and Printing. August 1993.

Sellers, J. 1993. Personal communication from Jennifer Sellers, Bureau of Engraving and Printing. September 1993.

APPENDIX A

CONCLUSIONS AND RECOMMENDATIONS FROM PREVIOUS NATIONAL MATERIALS ADVISORY BOARD REPORTS ON COUNTERFEIT DETERRENCE

- Conclusions and Recommendations from *Advanced Reprographic Systems: Counterfeiting Threat Assessment and Deterrent Measures,* NMAB 433-2 (NRC, 1985):

Conclusions

1. The potential threat to the United States currency from modern reprographic technology is great, due primarily to the expected increase in availability of high-quality color copier and scanner-printer combinations during the next five years.
2. A broadening of the counterfeiting base made possible by the availability of commercial reprographic equipment can pose an intractable enforcement problem and cause serious erosion of confidence in United States currency.
3. Timely action is needed if appropriate deterrent countermeasures to this threat are to be in place by the end of the decade.
4. The primary deterrent objectives are two-fold: (a) to discourage the growth of a new category of "casual" or "crime-of-opportunity" counterfeiters, and (b) to give the public a simple means of recognizing a reprographically attempted counterfeit. Both objectives can be achieved by use of deterrents that foil the use of advanced reprographic equipment at the source . . . .
5. Although the "crime-of-opportunity" counterfeiter will normally be defeated by a single deterrent of the above type, no one deterrent exists which can permanently thwart a determined, highly skilled professional counterfeiter. . . . any currency modification adopted should incorporate more than one type of deterrent, and the selected deterrents should be based on different technologies.
6. Since reprographic technologies—and consequently counterfeiting threats—continue to evolve, new deterrents may have to be considered at a later time. It is therefore important that currency modifications be initially designed to permit subsequent incorporation of additional deterrents without extensive redesign.
7. Advances in reprographic technologies require close monitoring and relevant research to develop alternative and improved deterrents . . . as needed.
8. Certain covert deterrents can have a very useful back-up role for verification and sorting. Other covert deterrents, as well as certain overt deterrents, could become even more useful as the economy moves towards automated currency transactions. . . .

Recommendations

1. Actions should be initiated at once to change the design of: United States currency.
2. For the near term, design changes should use a combination of "conventional" deterrent technologies.
3. The following deterrents are recommended for the initial change to protect the currency: security thread, localized watermark, and variable dot-pattern-generated gray-scale printing.
4. Design changes should be selected such that, if more advanced deterrents are necessary later, other deterrents can be added without substantial further alteration in design.
5. In the longer term, the following deterrents are also candidates for adoption if the present difficulties can be overcome by research: holograms, optically variable ink, diffraction gratings, multilayer paper, and other modifications of the substrate material.
6. Appreciable departures from traditional note design should not be ruled out in advance, lest the adoption of effective deterrents be thereby thwarted.
7. The currency modifications selected should take into account their potential for use in automatic change machines.
8. The development of inexpensive instrumental aids for counterfeit detection at points-of-sale, that take advantage of deterrents incorporated in the currency, should be encouraged.
9. Special emphasis should be given to the advantages associated with the control of substrate material.
10. Immediate consideration should be given to legal, procedural, sociological and law enforcement measures with the potential to deter reprographic counterfeiting.
11. Governmental research on both "low level" (overt) and "high level" (covert) counterfeiting deterrence and detection schemes, both in-house and contract, should be substantially increased.
12. An independent review process should be established to assess the effectiveness of any implemented design changes, as well as the impact of advancing technologies on the counterfeiting problem.

• Conclusions and Recommendations from *Counterfeit Threats and Deterrent Measures,* NMAB 433-3 (NRC, 1987):

Conclusions

1. Rapid developments in reprographic technology could give rise to an unacceptable level of counterfeiting activity by making high-quality reprographic systems widely available.
2. Incorporation of certain deterrents will require some modification of the design of the currency.
3. Once currency redesign is undertaken to foil advanced reprographics, it is prudent to incorporate more than a single new deterrent—preferably deterrents based on different physical principles. The probability is small that new technological developments will appear that can negate simultaneously the effect of different types of deterrents.
4. Types of deterrents recommended not only produce easily recognizable gross differences between counterfeit and genuine currency but also have the practical advantages of low cost as well as requiring little further development.
5. Exploitation of the three-dimensional nature of the substrate can produce a class of deterrents of singular power to foil counterfeiting by any means of reproduction.

Recommendations

1. Changes of U.S. currency design should be initiated at once to protect the U.S. public against the emergence of "crime-of-opportunity" counterfeiting as well as increased professional criminal counterfeiting that advanced reprographic methods could make possible.
2. Appreciable departures from traditional note design should not be ruled out *a priori,* lest the choice of counterfeiting deterrents be unnecessarily limited and the effectivenesss of the action thereby weakened.:
3. The new currency should incorporate a combination of deterrents based on different technologies.
4. The following deterrents are recommended for further development because they have characteristics compatible with use in currency and, in principle, can produce gross differences, easily recognizable by an untrained observer, between genuine and reprographically attempted counterfeit currency:

- Most effective are security threads, watermarks, and volume-related substrate modifications.
- Next in effectiveness are variable dot-pattern-generated gray-scale printing and complex design.
- Optically variable inks would be less effective still.

5. Special emphasis should be given to the most effective deterrents listed above because of the advantages inherent in the use of the three-dimensional properties of the substrate.

REFERENCES

National Research Council (NRC). 1985. Advanced Reprographic Systems: Counterfeiting Threat Assessment and Deterrent Measures(U). National Materials Advisory Board. Washington, D.C.: National Academy Press.

National Research Council (NRC). 1987. Counterfeit Threats and Deterrent Measures. National Materials Advisory Board. Washington, D.C.: National Academy Press.

APPENDIX B

ADVANCED NON-IMPACT COLOR REPROGRAPHIC TECHNOLOGIES

There are many technologies that are currently used in the non-impact printing industry. These will be briefly discussed in terms of their principle of operation, performance characteristics, strengths, limitations, and technical trends.

ELECTROPHOTOGRAPHY

Electrophotography, the leading non-impact technology, is widely used in copiers and printers, both monochrome and color. Devices using this technology, along with input scanners, are common in the modern workplace (Schaffert, 1980). They are used to copy, print, and reproduce almost any printed document.

The differences between copiers and printers are merging quite rapidly since both employ the same basic electrophotographic process to reproduce either printed or electronic data. A copier has been an analog device (copiers that convert the image into digital format are beginning to appear) that uses light to create a latent image of an entire original document on a photosensitive plate. The latent image is developed with toner using one of several electrophotographic developer techniques and is then transferred and fixed to paper. A printer, on the other hand, is not a stand alone device; it must be connected to a computer system or network. It relays the image information, in digital form, to the photosensitive member by use of a controllable light source, such as a laser, light-emitting diodes, light valves, or some other method of addressing many points using light. (The digital image information may have been generated by a computer scanner, by use of a software program, or by both.) The latent image is developed using the same choices of developer technology as for a copier.

Various methods can be used to develop the latent image. The objective of the development system is the delivery of electrostatically charged toner particles that partially neutralize the charged image to produce the printed image that is transferred to the paper. The types of development systems include dual component, monocomponent, non-magnetic monocomponent, and liquid (Hayes, 1991). These terms describe the composition of the development system, which vary in complexity and size (Jaffe and Burland, 1988).

In order to be able to produce the higher print quality that is required today, the size and uniformity of the toner must be optimized. In 1989, toner size was in the 10—15 μm range and was produced by a milling process that resulted in a wide, non-uniform distribution of both shape and size. As true resolution increases from today's standard 300 dots per inch (dpi) to 600 dpi,[1] toner size must become smaller and more uniform. Today's toner can be in the 9–12μm size, or smaller, for dry powders and from 1–2μm for liquid toner. New methods of producing toner can provide a very uniform spherical shape, allowing much crisper printed edges. In order to achieve the best color reproduction, both the average size and size distribution of toner particles must be controlled. The technological aspects of toner production are in place to support higher-quality levels of color electrophotography.

When copying or printing in full color, sequential passes must be made to lay down the subtractive primary colors of cyan, magenta, yellow, and black. This need for four separate development systems resulted in a physically large print engine in early models. Smaller-sized developers, such as nonmagnetic monocomponent or liquid ones, have led to process simplifications, smaller units, and cheaper, and more durable machines.

Many companies have patented or licensed basic print engine architectures that will lead to a new breed of smaller, cheaper, color copiers/printers. There are many configurations that can accomplish the sequential printing of the three primary colors plus black. One approach exposes and develops each color separately on the photoconductor. After the first color is toned, it is transferred to an intermediate member so the photoconductor can be cleaned and imaged with the next color, which is transferred on top of the first, and so on until all (four-color separation planes) have been completed. The finished image is then transferred to paper for a final fusing step. This method requires that the relationship between planes be maintained so the resulting image will be well registered. Since the intermediate member can be controlled both in position and material, this can be accomplished with great accuracy in both dry and liquid systems.

Another method uses the paper itself as the intermediate member. This method has more difficulty with registration, since the dimensional stability of most grades of paper is not very good or repeatable. Also, paper is abrasive and tends to wear the photoconductor excessively.

A simple method of developing the four planes would require that the photoconductor hold all four layers until the final transfer. But this is difficult to do in practice, because most development systems use direct contact with the photoconductor to develop the latent image, and contamination will occur on subsequent passes, because residual toner particles will be left from the previous passes. However, if development does not require direct contact with the photoconductor, the contamination problem can be controlled. This is possible with monocomponent and nonmagnetic monocomponent systems (Konica Corporation, 1992). This configuration is also being considered using liquid toner. These developments can lead to even smaller and simpler full-color copiers/printers.

[1]600 dpi is equal to dot diameters of 63.5 mm, allowing 50 percent overlap.

INK JET

Ink-jet technology has great potential for color printing (Jaffe et al., 1978, 1981). This potential was unrealized for some time due to the complexity of this technology and the unreliability of the nozzle system. As ink-jet technology progressed, the complexity of print heads has decreased and the reliability increased. Today there are many ink jet products on the market. The technology most widely used now is thermal ink-jet[2].

Ink-paper interactions are the key to controlling the quality of the print (Jaffe et al., 1979). The need for special paper to ensure dependable print quality has been an issue for ink-jet printers. Much of the work conducted in recent years has been aimed at overcoming this limitation. New ink formulations greatly improve the ink-paper interaction (and paper manufacturers are designing special papers for ink-jet printing) helping pave the way for ink jet printing to become a low-cost, highly capable technology for everyday color printing. The most important ink formulation developments are described below.

Water-based pigmented inks, in which the colorant is a normal printing ink pigment, have been patented (E.I. DuPont de Nemours and Company, 1998)[3]. They have stabilized emulsions that use water as a carrier fluid that can be readily jetted. The water is absorbed into the paper or evaporates, leaving the coloring agent on the paper surface.

A paper-insensitive approach uses an ink that is normally solid at room temperature but is jetted at elevated temperatures where it is liquid (Titerington and Jaeger, 1992). Another method uses solvent-based inks in a print head that incorporates piezoelectrically grooved channels; it can use an ink that is similar to regular printing.

Technology advancements looming on the horizon include the elimination of nozzles. Acoustic ink jet and electrostatic-pull ink jet accomplish this in different ways. Another advance has been the development of a cartridge containing both the ink and thermal drivers produced by photolithographic methods; these drives are so inexpensive that the cartridge is disposable.

In summary, ink-jet technology inherently is a less complex color system than technologies requiring sequential imaging of the same spot. Breakthroughs in ink technology have resulted in color ink-jet printers becoming available now for less than $1,000. Further improvements in cost and print quality are expected in the future.

THERMAL TRANSFER PRINTING

Thermal transfer printing is one of the technologies that is currently popular for color printing. Two ways are used to transfer color from a ribbon to paper. One implementation uses a colored wax that melts at a low temperature on a mylar base, and which transfers to

[2]As implemented by Hewlett Packard and Canon (Hewlett Packard Company, 1991).

[3]Implemented by Hewlett Packard in the 1200C printer.

paper when heated with a thermal print head. It requires a very smooth paper that can make intimate contact with the ribbon for good transfer properties. The other uses a dye diffusion process (sometimes erroneously called dye sublimation) that melts the ribbon base. Diffusion across the ribbon/paper boundary requires a special layer to trap the dye. The paper needed for this process looks very much like the stock on which photographs are printed. Because diffusion is difficult to localize, the transferred areas spread laterally, and sharp lines and text are difficult to reproduce. This limits the applications that can be covered using this technology.

Recently, work has been done to develop ribbons that transfer ink to plain paper. One approach is to change the rheology of the ink to be more flexible in transfer and able to conform to the morphology of plain paper (Abe and Kitamura, 1991). The other approach uses a coating that is applied to the paper before the color is transferred. This coating is on a ribbon, like the colored wax, and is applied with the same print head to the paper in the areas to be printed by the regular wax transfer ribbon. The printed areas are calculated by the printer. In this manner, each paper appears the same to the ribbon that follows. This method is already used in a commercially available printer.

MAGNETIC PRINTING

Magnetic printed has not progressed in the same manner as some of the more popular nonimpact printing technologies. The color printing capabilities have been projected, but it is difficult to produce pure colors from a toner that requires large amounts of dark magnetic material. Research on color-masked magnetic material has shown that it is theoretically feasible but not probable to make a commercially successful product in the foreseeable future.

ELECTROSTATIC PRINTING AND ELECTROSTATIC PRESSES

The area of electrostatic printing and presses is one that has taken a mature technology and applied it to new applications. Large-format color printing has served the engineering design market, but newer markets such as the graphic arts, outdoor advertising, and lithography for short runs have recently emerged (Hard Copy Observer III, 1993). Even though this technology is suited for color, most of the implementations have been in large-format machines (i.e., large-size and high-cost ones). These machines, which cost between $40,000 and $100,000, are probably not available for the casual user. They require maintenance and trained operators. Future progress could bring the technology to smaller and cheaper models, but with all the other technologies available for the lower end market, the committee does not think this is probable in the foreseeable future.

INPUT SCANNERS AND ELECTRONIC IMAGING SYSTEMS

This field is advancing very rapidly with new products appearing monthly. As demand for digital input increases, more and more ways to get data into computer systems will be implemented. Scanners and digital cameras are becoming more popular as their prices fall. High-quality scanners for color are already available for under $2,000, and, as generally occurs with electronic equipment, the prices will continue to decline, and function will increase (Imaging Magazine, 1992)[4]. It is evident that if a printed document can be seen in reflected light, it can usually be digitized.

IMAGE-PROCESSING SOFTWARE

Once an image is digitized, the manipulation of its pixels can begin. The lack of uniform standards and the difficulty of sending color information across various devices lack of uniform standards, are being addressed by the industry. The advent of many different input and output color devices has emphasized the need for software to manipulate the large amount of digital data dictated by color images. This field is rapidly growing, as evidenced by a conference covering only the data-manipulation segment of color transfer has been planned[5].

There are software programs that match colors, manipulate every pixel, and prepare color output for printing. Appropriate manipulation of the image can significantly improve the printed image. For example, each section can be optimally separated. Fine lines can be sharpened independently from the balancing of halftone areas. After the manipulation is complete, storage on one of the many available storage media allows the image to be available for reuse.

DIGITAL PRESS

Digital technology has been leading advances that allow easier and cheaper access to color printing in the conventional offset printing industry, just as it has done in office and home printing. The digital nature of this technology allows data from many input sources, such as scanners and computers, to be used. Some equipment manufacturers are now employing digital presses to receive digital data that can directly generate a plate for printing[6]. This capability

[4]Apple Computer Color Scanner and Hewlett Packard's Scanjet currently will do color at 300 dpi, and more expensive desktop models by Agva Gevaert and others are already doing 600 and 1,200 dpi.

[5]Color Imaging Conference: Transforms and Transportability of Color, November 7-11, 1993, Phoenix, Arizona. [Sponsored by IS&T and SID, Conference Chairs: Annette Jaffe, Apple, and Andras Yakators, Xerox.]

[6]Digital press manufacturers include Heidelberger and Presstek, as described in Uhrig and Williams (1993).

has dramatically decreased the time and cost of short-run color printing to the extent that it is economic to print in color in runs as small as 20 to 1,000 copies.

Recently, advanced color presses have been announced by several European-based companies. These products have the advantage of flexibility, and no plates or films as intermediates[7]. Although these machines cost more than $200,000 each, the development of the market for short-run color will insure faster and more competitive machines for the future.

DIGITAL PHOTOGRAPHY

The past has relied on standard photographic methods to produce input separations for printing work. But current technology has moved so rapidly that digital camera technology is now good enough for prepress work. The advantages of digital photography are many. Its versatility and extendibility will allow its importance to expand in the future. For example, the possible dynamic range is even wider than for conventional photography. The rapid turnaround that is inherent in this digital process gives a new perspective for the designing and publishing business. The charged coupled device (CCD) camera technology, which uses the same technology as flatbed scanner, is relatively mature, and new products are being introduced rapidly. This coupled with Photo Compact Disk (CD) technology, allows images to become part of any computer-based system[8]. It is expected to become a widespread source of available images for printing.

[7]Xeikon N.V., (Mortsel, Belgium) has announced a product based on conventional dry toner electrophotographic that prints 35 two-sided pages per minute at 600 dpi. Indigo (Rehovet, Israel) uses 800-dpi liquid toner technology in their product, the E Print 1000 (Color Business Report, 1993).

[8]Photo CD, introduced by Kodak, is basically a technology to store many scanned images on a single CD-ROM (compact disk-read-only memory) in a compressed format (see Stoy, 1993).

REFERENCES

Abe, T., and S. Kitamura. 1991. Relation between dynamic characteristics of thermo-fusible ink and print quality in thermal transfer printing. Journal of Imaging Technology 17:119–122.

Color Business Report. 1993. New products for Xeikon and Indigo re-define high speed color electrophotography. Color Business Report 3 (7):1.

E.I. DuPont de Nemours and Company. 1998. Aqueous Pigmented Inks for Ink Jet Printers. European Patent Application 0, 518, 225.

Etchells, R. D. 1993. Digital photography gets serious. Color Publishing 3(4):19–24.

Hard Copy Observer III. 1993. QHS beats rivals to punch with first office color laser. C. Le Cohpte, Ed., No. 6 (June) p. 1.

Hard Copy Observer. Indigo and Xeikon roll out fist high speed digital color presses. C. Le Conpte, Ed., No. 7, P.10.

Hayes, D. A. 1991. The evolution of color xerographic development systems. Journal of Imaging Technology 17:252–258.

Hewlett Packard Company. 1991. Method for Enhancing the Uniformity and Consistency of Dot Formation Produced by Color Ink Jet Printing. U.S. Patent 4,999,646. March 12, 1991.

Imaging Magazine. 1992. High speed scanner roundup and color scanner roundup. M. Neilson, Ed., Volume 9, pp. 39-630.

Jaffe, A. B., and D. Burland. 1988. Electrophotographic printing. Pp. 221-260 in. Output Hardcopy Devices. Boston, Mass.: Academic Press.

Jaffe, A. B., W. Crooks, and T. Niewegha. 1979. Materials parameter affecting the quality of color printing. Second International Conference on Business Graphics, Washington, D.C. Springfield, Va.: SPSE,

Jaffe, A. B., E. W. Luttman, and W. Crooks. 1981. High quality color printing with continuous “ink jet.” in The First International Congress on Non-Impact Printing Technologies, Venice, Italy. Springfield, Va., SPSE.

Konica Corporation. 1992. Color Image Forming Apparatus. U.S. Patent 5,162,821. November 10, 1992.

Schaffert, R. 1980. Electrophotography. New York, New York Focal Press.

Stoy, J. 1993. Photo CD: A practical guide. Color Publishing 3(4):10.

Titerington, D., and C. W. Jaeger. 1992. Design parameters for a phase change ink jet ink. Pg. 298 in Proceedings, Society for Imaging Science and Technology, Eighth International Conference on Advances in Non-Impact Printing. Springfield, Va,: IS&T.

U.S. Patent 5,115,277. Electrostatically Assisted Transfer Roller and Method for Directly Transferring Liquid Toner to a Print Medium. Hewlett-Packard Co. Camis Thomas (US). May 19, 1992.

U.S. Patent 4,879,568. Droplet Deposition Apparatus. AM International. Bartky W. Scott(US); Michaelis A. John(US); Paton Anthony D. (GB). November 7, 1989.

APPENDIX C

BACKGROUND ON COLOR

Color measurement[1] is most often performed using the Commission Internationale de l'Eclairage system, with values frequently given in terms of "x", "y", and "Y." Here, x and y are the coordinates on the chromaticity diagram or "color triangle," and Y is the intensity. Several other systems are used; interconversion is relatively simple and automatic in modern, computerized color-measuring instruments.

The Commission Internationale de l'Eclairage has also specified a number of standard illuminates, in particular "A," corresponding to a tungsten filament bulb with a color temperature of 2854K, "C" for noon sunlight, and "D_{65}" for daylight with a color temperature of 6500K. A last type of illumination, not standardized but important for currency, is the reddish candle or low-level incandescent tungsten filament light so often found in dimly lit surroundings.

Nine of the fifteen physical and chemical causes[2] that can cause a non-white distribution of light from non-color light have been used or could be used in currency:

1. Transition metal compounds as in pigments such as *chrome green,* where the colors are caused by light absorption at restricted energies, producing the excitation of unpaired electrons.
2. Organic compounds as in dyes and pigments such as in the dye *indigo,* where the colors derive from absorptions leading to excited electrons in extended conjugated organic molecules having alternating single and double bonds.
3. Charge transfer compounds as in the pigment *Prussian blue,* where electrons absorb energy in moving from one atom, ion, or group to another.
4. Metals as in reflective pigments such as those based on aluminum flakes, where light is totally absorbed into an electron band at the metal surface, but essentially all of it is immediately re-emitted in the metallic reflection.
5. Pure semiconductors as in some pigments such as *cadmium yellow,* where selected absorption of light is limited by an energy gap in the structure of the electron band, in which gap electrons cannot exist.
6. Refractive index differences as in transparent and translucent materials and in watermarks, where the refractive index depends on the physical nature of the substance, including its chemical composition, structure, and the strength of the bonding.

[1]Color measurement and related topics are well covered in Billmeyer and Saltzman, 1981, and in Hunt, 1987.
[2]Details of the 15 causes of color are given in Nassau, 1983.

7. Scattering as in opaque regions and in watermarks where opacity and scattering depend on the nature of the material and the size of the particles as well as on the refractive index of the medium surrounding them.
8. Interference as in optically variable pigments holograms, where the waves of light scattered by structured thin films or different parts of an object interfere with each other and either cancel or reinforce to produce patterns of colors from white light.
9. Diffraction as in diffraction gratings, where a similar result is produced by regular two- or three-dimensional geometrical arrays or structures that scatter and break up reflected or transmitted light into spectral arrays of color.

REFERENCES

Billmeyer, F. W., Jr., and M. Saltzman. 1981. Principles of Color Technology, 2nd ed. New York: John Wiley and Sons.
Hunt, R. W. G.. 1987. Measuring Color. New York, New York: John Wiley and Sons.
Nassau, K.. 1983. The Physics and Chemistry of Color. New York: John Wiley and Sons.

APPENDIX D

INDUCED MOIRE PATTERN BACKGROUND

Large-scale moiré patterns occur when two regularly repeating patterns with slightly different periods are superimposed. The spacing of the resulting moiré pattern is most striking when the frequencies are in the ratio of small integers.

A simple illustration of induced moiré can be seen using the concentric-circle pattern shown in Figure D-1. To observe an induced moiré pattern, place a pocket comb one to two inches above the concentric-circle pattern. In this example, the comb serves a sampling function which analogous to the sampling that occurs in digital imaging systems.

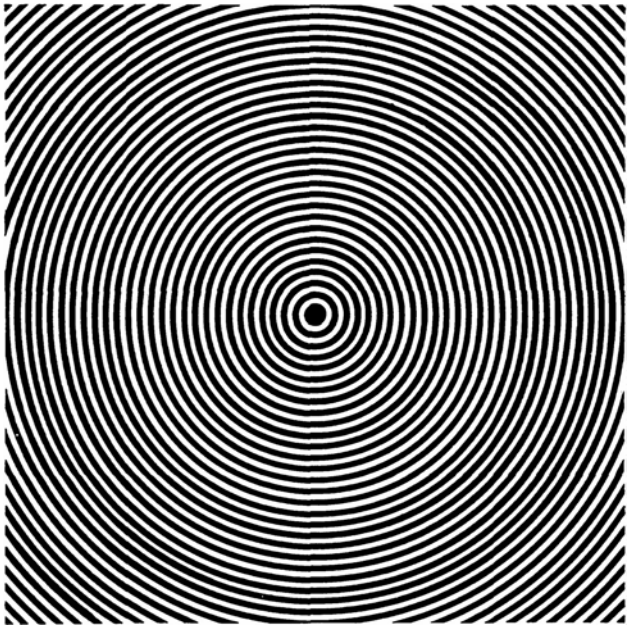

FIGURE D-1 Concentric-circle pattern.

The mathematical formulation of the moiré phenomenon can be done in several ways. A Fourier series representation can be made of the object and the sampling function in frequency space. The presence of a sampling function leads to the generation of aliased frequencies, which, when reconstructed, represent the moiré pattern. The same calculation can be performed in the spatial domain using discrete sampling. If there exists a certain ratio relationship between the period of an object and the sampling function, then false data (moiré pattern) will be generated that are fixed in space and related to the sampling ratio.

APPENDIX E

METHODS FOR AUTHENTICATION OF UNIQUE RANDOM PATTERNS

The random pattern/encryption concept as applied to currency uses random three-dimensional patterns as positive identifiers to distinguish authentic from counterfeit notes. The concept was originally developed to provide positive identification of specific items for intelligence and arms control applications; that us, once a particular missile was inspected and identified as missile that was allowed by the treaty, it was necessary to ensure that the exact same missile was the one found in a later inspection (Graybeal and McFate, 1989). This concept can be extended to provide a high degree of counterfeit deterrence for banknotes.

The identifier must initially be read and a description of it created that is stored for future reference. To authenticate the positive identifier, the same random pattern is read again and compared with the recorded description. If they match, authentication occurs.

In practice, initial and subsequent readings of an identifier will differ because of unavoidable variations in the location of the reader with respect to the pattern, variations in the sensors, resolution limits of the sensors, and changes in the pattern resulting from wear and tear. These differences could cause false decisions by judging that the patterns are the same when actually they are different (a false positive) or judging that the patterns are different when actually they are the same (false negative).

A number of methods have been developed and tested that take these errors into account and ensure very low probabilities of false decisions. These methods take advantage of the fact that it is not necessary for authentication purposes to exactly match the true pattern with that read subsequently. It is only necessary to distinguish between the distribution of correlation numbers of like patterns and the distribution of the correlation numbers of unlike patterns. If a large number of readings are taken of the same pattern and correlated with each other, random reading errors will cause variations in the correlation numbers. If the correlation numbers are plotted, they will approximate a normal distribution. The peak value and the standard deviation (spread) of the values will depend on the sources of error. Similarly, when a large number of unlike patterns are read and correlated, they will generate a different distribution with a peak at a lower value. If there is a complete separation between these curves, a threshold correlation value between the peaks can be selected such that all correlation numbers below that value result from correlation of unlike pattern descriptions and all correlation values above the threshold number result from correlation of like pattern descriptions. In the ideal case, there would never be a false decision. In practice, there will

rarely be complete separation between the curves. Also, it is theoretically possible that two randomly generated patterns, regardless of how complex they are, will be exactly the same. For complex patterns, this probability is infinestimally small.

The reading errors mentioned above increase the overlap between the curves. The result is that there is a chance of making a false decision. This has been the subject of considerable research and development, which has identified methods that account for these errors and ensure an acceptable probability false decision. In the application for arms control verification mentioned above, substantial effort was devoted to adversary analysis to ensure that the random patterns could not be counterfeited successfully and that both the false negatives and false positives resulting from correlations of pattern readings taken in the field would be less than one in a million.

A simple method for minimizing concerns regarding misalignment of the reader with the pattern on successive readings is to desensitize the spacial resolution of the pattern reading. This is done by placing the locations of the features that are read into bins (or cells) that are larger than the alignment errors. While this reduces the effective number of pattern features that are used for identification, with certain patterns there is still enough random information to result in acceptable false-decision probabilities if the alignment errors are not very large. This method proved to be successful in the proof-of-concept demonstration of the random pattern/encryption concept that was conducted for the Bureau of Engraving and Printing, and which used fiber-optic patterns (Kromer, 1987).

Various concepts were developed and tested that eliminate errors caused by variations in the alignment of the reader for certain patterns. The complex pattern reading is transformed into a series of coefficients. This results in a description of the pattern with respect to itself instead of with respect to an external reference frame. If the patterns are completely covered by the reader and no information outside of the pattern is read, the descriptions of the readings are the same regardless of the position of the reader. Comparison of the transform coefficients allows authentication of the pattern descriptions (Ahmed et al., 1986).

Another method developed to reduce the sensitivity to reading errors employs a computer program to shift the patterns with respect to each other and correlate them at each relative orientation. The maximum correlation-value occurs when the two patterns are registered correctly. This value is used for comparison with the threshold decision correlation value to indicate whether or not the pattern descriptions represent the same pattern.

A variation of this method shifts and correlates small areas of the patterns (instead of shifting the entire pattern on a trial and error basis) until a peak value is found for each area. This approach reduces the amount of computer manipulation of images and reduces the time required to determine the correct alignment of the pattern descriptions. The distance and direction that each area was shifted to get a peak correlation number is used to calculate how to shift the whole pattern with respect to the other pattern, both in translation and in rotation, to register them accurately. Then the complete patterns are correlated (Tolk, 1992).

Another approach compensates for errors in the reader location with respect to the pattern. It results in low false-decision probabilities even if a large portion of the unique identifier is missing because of wear and tear. This can be illustrated by two images made from a photograph of a unique identifier. The significant features of the pattern appear as transparent spots. The rest of the area is made opaque. The images are then overlaid. Consider

n locations on the transparency, with each location having probability *p* of being transparent. Then the expected number of transparent locations when the two transparencies are registered with each other is $N_R=np$

If the images are not registered with each other, the expected number of transparent locations is $N_{NR}=np^2$

Thus, the expected ratio *R* of matching transparencies in the registered position to the matching transparencies in the unregistered position is

$$R=\frac{N_r}{N_{NR}}=\frac{np}{np^2}=\frac{1}{p}$$

If damage to the pattern causes a loss of transparencies equal to *k* times the original number of transparencies, the expected number of matching patterns in the registered position of the patterns is $N_R=n\,(p\text{-}kp)$

The expected number of matching transparencies in the unregistered position is $N_{NR}=n\,(p\text{-}kp)\,p$

The expected ratio of matching transparencies in the registered position to the matching transparencies in the unregistered position then is

$$R=\frac{N_R}{N_{NR}}=\frac{n(p-kp)}{n(p-kp)\,p}=\frac{1}{p}$$

This result for the damaged pattern is the same ratio as that for the undamaged pattern. Thus, wear and tear of a pattern does not change the expected value of this ratio, although it does change the variance. If different random patterns that possess the same proportion of transparencies to opacities are overlaid, the expected number of matching transparencies is np^2 regardless of the registration. The criteria for deciding whether or not two readings are from the same pattern is based on the ratio of transparencies in the registered and unregistered orientations exceeding a chosen value (Bauder, 1983).

REFERENCES

Ahmed, N., R. Kruker, and D. Park. 1986. Authentication Scheme for Random Patterns Using Transforms. University of New Mexico memo to Don Bauder, Sandia National Laboratories. August.

Bauder, D. W. 1983. An Anti-Counterfeiting Concept for Currency. Systems Research Report PTK-11990. Albuquerque, N.M.: Sandia National Laboratories.

Graybeal, S. N., and P. B. McFate. 1989. Getting Out of the STARTing block. Scientific American 261(6)64–65.

Kromer, R. P. 1987. Demonstration of a Random Label Counterfeit Deterrence System (RLCDS) for Currency. Sandia National Laboratories. May 1, 1987. Unpublished.

Tolk, K. 1992. Reflective particle technology for identification of critical components. Institute of Nuclear Management, 33rd Annual Meeting Proceedings, July, 1992. Vol. 21pp.xxi., Northbrook, Ill.: American Materials Proceedings.

APPENDIX F

BIOGRAPHICAL SKETCHES OF COMMITTEE MEMBERS

GLENN T. SINCERBOX received the B.S. degree in physics from Rensselaer Polytechnic Institute in 1959 and the M.S. degree in physics from the University of Illinois in 1960. He continued graduate studies at the University of Illinois until 1962, when he joined IBM. He has been a member of the research staff at IBM's Almaden Research Center since 1972, where he has held several technical and managerial positions, including group manager of holographic optics, department manager of exploratory I/O studies, department manager of inspection science and technology, and department manager of optical storage heads. He is currently program manager of holographic storage systems and technology. His primary research contributions have been in the areas of holography, novel recording processes, and optical devices, with emphasis on their application to information storage, display, scanning, printing, and inspection. He has published and presented over 60 papers, 3 book chapters, holds 39 patents, and over 65 patent publications. He is the recipient of 15 IBM invention achievement awards and an IBM Outstanding Innovation Award. He is a Fellow of the Optical Society of America and has served on numerous society and conference committees. He was a member of the 1985-1987 NMAB studies on currency and counterfeiting.

STEVEN ANDRIOLE is Director of the Center for Multidisciplinary Information systems Engineering at Drexel University, where he is also professor of information studies and electrical and computer engineering. He was formerly the Director of ARPA's Cybernetic Technology Office and Chairman of the Department of Information Systems and Systems Engineering at George Mason University. He is also founder of International Information Systems, Inc. He received his Master and Ph.D degrees from the University of Maryland.

NORBERT S. BAER received his M.S. and Ph.D. from New York University in chemistry and environmental science. His research interests include the application of physicochemical methods to the examination and preservation of artistic and historical works. His professional activities include serving as editor and board member of various publications and authoring many technical works. In 1980 he chaired the National Materials Advisory Board Committee on Conservation of Historic Stone Buildings and Monuments, and since 1980 has chaired the National Archives Advisory Committee on Preservation. He is currently at New York University.

DONALD BAUDER received his B.S. from the University of Colorado in mechanical engineering. He retired from Sandia National Laboratory, where he spent more than 30 years. His expertise is in systems analysis and systems design. He was the originator of the Random Label Counterfeit Deterrence System for the Bureau of Engraving and Printing as a method to deter counterfeiting.

MITCHELL J. FEIGENBAUM received his B.S.E.E at City College of New York and his Ph.D. at the Massachusetts Institute of Technology in theoretical physics. He played a pivotal role in developing the field of fractals and chaos as applied to understanding non-linear systems. His research is on the discovery of metrically universal behaviors in dynamical systems. He is a member of the National Academy of Sciences. He is currently at Rockefeller University.

JOSEPH GAYNOR received his B.Ch.E. from Polytechnic Institute Brooklyn (now Polytechnic University) and a Ph.D. from Case Institute of Technology (now Case-Western Reserve University). His technical interests and expertise include areas such as imaging materials and processes, non-impact printing technologies, optical memory materials and processes, chemical processes, photochemistry (especially applications), and polymeric films and coatings. He was a member of the former NMAB committees (1984-1987) concerned with U.S. currency. He is President of Innovative Technologies Associates in Ventura, California.

STEVEN M. GEORGE received his B.S. in chemistry at Yale and his Ph.D. in chemistry from the University of California, Berkeley. His research interests are in understanding and evaluating surface effects. He is currently at the University of Colorado.

ANNETTE B. JAFFE received her B.A. in chemistry at Douglas College, her Ph.D. in physical chemistry at Yale University. Her postdoctoral work was at the University of Rochester. She is currently the principal scientist of hardcopy technology in the Imaging Products Division of Apple Computer, where she is responsible for the evaluation and recommendation of technologies appropriate for future products in printers, scanners, and imaging test tools.

MICHAEL MORRIS received his B.S. at the University of Oklahoma in engineering physics and his M.S. and Ph.D. in electrical engineering at the California Institute of Technology. He is an expert in diffractive optics and opto-electronic systems design. He is currently at the Institute of Optics at the University of Rochester.

KURT NASSAU received his B.S. from Bristol University and his Ph.D. from the University of Pittsburgh (both in physical chemistry). His research is in the growth of crystals and their physical and chemical properties; solid state and crystal chemistry and physics; crystallography; and laser, magnetic, piezoelectric, ferroelectric, and vitreous materials. He was with AT&T Bell Labs for 30 years before retiring as a distinguished scientist. He now does some consulting work.

ROBERT R. SHANNON received his B.S. and M.A. from the University of Rochester. He is an expert in applied optics and is well known for his practical approach to problems. He has both academic and industrial experience. For the past twenty-five years he has been a Professor at the University of Arizona, and, is a past director of the Optical Sciences Center. He is a member of the National Academy of Engineering and is currently Professor Emeritus at the University of Arizona.

RODNEY SHAW received his B.S. from Leeds University and his Ph.D. from Cambridge University, both in physics. He has both academic and industrial experience in advanced imaging concepts and applications. Currently, he is on an extended professional leave from Rochester Institute of Technology and consults in electronic imaging and digital printing.

GLOSSARY

TERM	DEFINITION
Aliasing	See Moiré Pattern.
BEP	Bureau of Engraving and Printing.
Black Light	See Ultraviolet.
Charge Transfer (CT)s	A color-producing mechanism in which the absorption of light produces the movement of one or more electrons from one atom in an ion to another.
Chromaticity Diagram	A three-dimensional array containing all the colors that can be perceived. A simplified two-dimensional section is usually known as the "color triangle."
Color	The perception in the eye-brain system produced by a non-white distribution of electromagnetic energy. See Appendix C.
Color-Shifting Inks	See Optically Variable Inks.
Covert Features	Security features that are hidden in the banknote and are not intended to be made public. Used by the Federal Reserve Bank for currency authentication and by law enforcement for forensic purposes.
Diffraction	The spreading of light at a sharp boundary. When diffraction occurs from periodic structures, it produces color by interference, as in the colors produced by a diffraction grating.
dpi	dots per inch
Electrophotography	An electrostatic image-forming process in which light, x-rays, or gamma rays form an electrostatic image on a pre-charged, photoconductive, insulating medium. The charged image areas attract and hold a fine powder called a toner, and the powder image is then transferred to paper and fused there by heat.
Electrostatics	The study of electric charges at rest, their electric fields, and potentials.
Embedded Features	Security features that are added during the papermaking process or inserted between laminated layers. They include threads, planchettes, fibers, microtaggants, microcapsules, and so on.
Enhanced Fibers	Fibers that respond to ultraviolet, infrared, or other excitations to give identifiable reactions and are added to paper as a security feature.
Fibers	Dyed fibers embedded in the paper as a security feature. See also Enhanced Fibers.
Fluorescence	See Luminescence.

Hologram	A structure that transmits or reflects light so that a three-dimensional image can be seen. This image appears to move as the viewing orientation is changed.
Hot Stamping	A process in which separate stripes, foils, or other features are applied to the surface of the substrate.
Infrared	Electromagnetic energy beyond the red end of the visible spectrum, that is, with wavelength longer than 700 μm. May be perceived as heat by the skin.
Infrared Inks	Inks containing dyes or pigments that absorb in the region 700 to 1,000 μm.
Ink-Jet Printing	A non-impact priting technique that uses electrostatic acceleration and deflection of ink particles emerging from nozzle to form characters on plain paper.
Intaglio Printing	Characters are formed as depressed areas on the printing plates. These are filled with ink, which is transferred to paper under pressure.
Interference	The constructive reinforcement or destructive cancellation when two beams of light interact. Thus, the beams reflected from the two surfaces of a soap bubble film can interfere to produce colors.
Iridescence	Those interference colors that show a change of color with orientation and are metallic-like in that they have a high reflectivity, as in multiple-layer interference filters on camera lenses.
Kinegram	A special type of surface-relief hologram.
Laminate(s)	A sheet of material made of one or more bonded layers.
Latent Image	See Void Pattern.
Letter Press Printing	Characters are formed by raised surfaces on the printing plates; a roller applies ink to these raised surfaces and the plate is pressed against the paper to transfer the ink.
Luminescence	The production of light when a substance is nonthermally activated as by ultraviolet, electricity, friction, chemically, etc. Also termed “fluorescence,” “photoluminescence,” “electroluminescence,” and so on. Also see Phosphorescence.
Magnetic Printing	Non-impact printing in which the ink contains magnetic particles that control the printing process.
Metamerism	When two different dyes or pigments match in color in one illumination but do not match in a different illumination.
Microcapsules	Small particles, not visible to the eye that are added to substrate and that respond to ultraviolet, infrared may be plastic particles or other excitations to give identifiable reactions.

Microprinting	Printing so small that it is not reproduced by machines with low dpi capability; usually only visible with magnification. Due to the fibrous nature of U. S. currency, there is a limit to the size of microprinting.
Microtaggants	See Microcapsules.
Moiré Pattern	A new pattern formed by the superpositioning of two patterns whose periodicities are not identical. This process is also called aliasing.
Multi-Diffraction Grating	A diffraction grating that produces a shift in the pattern seen on changing the viewing angle.
Non-impact Printer	A line printer in which the characters are produced electrically, electro-optically, or optically rather than mechanically.
Opacity	Nontransparency to light.
Optically Variable Device	Any feature that uses the color-shifting (optically variable) effect.
Optically Variable Inks	Inks that contain thin-film interference filter pigments that produce an iridescent reflection that changes color as the viewing angle is changed. Also known as “color-shifting” inks.
Optically Variable Pigment	The pigment portion of a color-shifting (optically variable) ink.
Overt Feature	A security feature that is visible or apparent without requiring special instruments. May require some instruction on how to observe it. The feature may be particularly visible on the genuine note (a passive visible feature) or may only show after a copy has been made.
Paper	The substrate used in printing currency, usually based on cotton and linen fibers rather than cellulose as in ordinary paper.
Paper Furnish	The fiber-water slurry from which the paper is made.
Phosphorescence	A slow luminescence, which lasts minutes to hours, usually produced in organic molecules and involving “forbidden” triplet to singlet transitions.
Photochromic Inks	Inks containing dyes or pigments that change color when exposed to ultraviolet or very intense visible light. They subsequently revert to their original color.
Photoluminescence	Luminescence produced by exposure to ultraviolet.
Pixelgram	A special type of surface-relief, computer-generated diffractive optical element, based on a discrete-pixel (picture element) addressing scheme.
Planchettes	Colored or reflective pieces of paper or plastic a few millimeters in diameter that are added during paper manufacture.
Scanner	Any device that examines an area or region point by point in a continuous systematic manner, repeatedly sweeping across until the entire area of the region is covered; an example is a flying spot scanner.

Security Thread	The thread present inside the paper used in currency printing. May carry the domination of the bill or may be fully metallized.
Substrate	The medium on which currency is printed. May be paper, plastic, or a laminated combination.
Thermal-Transfer Printing	A technique in which heat transfers a dye or a colored wax from a ribbon onto paper.
Thin-Film Interference Filters (TFIF)	Multiple-layer structures that produce color effects by interference.
Thread	See Security Thread.
Transparency	An image fixed on a clear base by means of a photographic, printing, chemical, or other process, especially adaptable for viewing by transmitted light. (Optics) The ability of a substance to transmit light of certain wavelengths.
Ultraviolet	Electromagnetic energy beyond the violet end of the visible spectrum, that is with wavelength less than 400 μm. Also called black light. May produce tanning of the skin and injure the eye.
Variable-Sized Dot Patterns	Printing with a combination of large and small halftone dots; the larger dots would be above the resolution limit of scanner or copier, while the smaller dots would be below it. The larger dots would be printed in a pattern, such as one spelling “VOID,” which would stand out on the copy, since the smaller dots would not be resolved. A typed “Void Patterns.”
Void Pattern	A security device consisting of a period structure as an overt but not visible feature. When copied on a machine with a different periodicity, the resulting moiré pattern displays the word “VOID” or some other message.
Watermark	A localized modification of the structure and opacity of a sheet of paper so that the pattern or design can be seen when the sheet is held to the light.