Is That Real? Identification and Assessment of the Counterfeiting Threat for U.S. Banknotes

Committee on Technologies to Deter Currency Counterfeiting, National Research Council

ISBN: 0-309-65784-9, 74 pages, 8 1/2 x 11, (2006)

Is That Real?

Identification and Assessment of the Counterfeiting Threat for U.S. Banknotes

Committee on Technologies to Deter Currency Counterfeiting
Board on Manufacturing and Engineering Design
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

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 competences and with regard for appropriate balance.

This study was supported by Contract No. TEP-05-0002 between the National Academy of Sciences and the U.S. Department of the Treasury, Bureau of Engraving and Printing. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number 0-309-10124-7

Available in limited quantities from:

Board on Manufacturing and Engineering Design
500 Fifth Street, N.W.
Washington, DC 20001
bmed@nas.edu
http://www.nationalacademies.edu/bmed

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and 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. Ralph J. Cicerone 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. Wm. A. Wulf 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. Harvey V. Fineberg 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. Ralph J. Cicerone and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON TECHNOLOGIES TO DETER CURRENCY COUNTERFEITING

ROBERT E. SCHAFRIK, *Chair,* GE Aviation
MARTIN A. CRIMP, Michigan State University
CHARLES B. DUKE, Xerox Innovation Group
ALAN H. GOLDSTEIN, Alfred University
ELIZABETH A. HOLM, Sandia National Laboratories
PRADEEP K. KHOSLA, Carnegie Mellon University
CAROLYN R. MERCER, NASA Glenn Research Center
STEPHEN M. POLLOCK, University of Michigan
ARTHUR J. RAGAUSKAS, Georgia Institute of Technology
JOHN A. ROGERS, University of Illinois at Urbana-Champaign
BARTON RUBENSTEIN, Rubenstein Studios
MICHAEL A. SMITH, France Telecom
GARY K. STARKWEATHER, Microsoft (retired)
DENNIS J. TREVOR, OFS Laboratories

Staff

TONI MARECHAUX, Study Director (until February 2006)
MICHAEL MOLONEY, Senior Program Officer (Study Director from February 2006)
MARTA VORNBROCK, Research Associate
TERI THOROWGOOD, Administrative Coordinator
LAURA TOTH, Senior Project Assistant

Preface

The U.S. Department of the Treasury, through the Bureau of Engraving and Printing (BEP), manufactures security documents—including banknotes, Treasury securities, identification cards, naturalization certificates, and other special documents—for the United States. One of the key missions of the bureau is the design and printing of U.S. banknotes, also known as Federal Reserve notes (FRNs).

The BEP has the fundamental responsibility for producing currency that is easily recognized as U.S. banknotes and is respected around the world. To that end, notes must contain a combination of elements that serve a variety of purposes. These features must allow users to distinguish the denomination of notes and also to authenticate them as real. Therefore, the features of notes must be difficult for counterfeiters to duplicate using the same processes the bureau employs, and also be difficult for counterfeiters to simulate through alternate processes. The features and their arrangement must allow the general public to distinguish counterfeit from genuine notes quickly and consistently.

While resistance to counterfeiting is vital, another important aspect of banknotes is that they are a manufactured product used daily by millions of people around the world. Therefore, on each of the billions of notes produced each year, features must be reproduced reliably. Notes must also be durable during normal use and able to survive folding, crumpling, and occasional laundering. Their design should be aesthetically pleasing, and finally, as with any manufactured product, they should be cost-effective to produce.

Historically, the BEP has been very attuned to the threat of counterfeiting. Indeed, the bureau was established during the Civil War as a key element in the national strategy to reduce the volume of counterfeit currency flooding the Union. In recent years, the bureau has recognized that modern information technology could lead to entirely new types of counterfeiting threats, and over the past two decades, it has asked the National Research Council (NRC) to carry out several studies to assess and characterize these evolving threats.[1] The BEP has since initiated a series of currency design changes aimed at reducing the vulnerability of U.S. banknotes to counterfeiting.

In response to a new request from the BEP, the NRC appointed the Committee on Technologies to Deter Currency Counterfeiting. Appendix A presents biosketches of the committee members. The committee is tasked to aid the BEP in identifying and evaluating significant emerging counterfeiting threats against Federal Reserve notes, as well as to assess technologically feasible counterfeit-deterrent

[1]The following reports have been issued by the NRC in response to these requests: Advanced Reprographic Systems: Counterfeiting Threat Assessment and Deterrent Measures (1985); Counterfeit Threats and Deterrent Measures (1987); and Counterfeit Deterrent Features for the Next-Generation Currency Design (1993).

features for potential use in future design changes. The specific objective of this effort is to provide the bureau with up-to-date information on the factors that will allow it to produce designs to enhance the security of notes to the greatest extent possible, taking into account identified current and emerging counterfeiting threats. Specifically the committee is undertaking the tasks specified in the following statement of task:

Primary Tasks:

1. Identify technologies, both existing and emerging, that pose the most significant counterfeiting threats to Federal Reserve notes (FRNs). Threats known today include digital methods of producing images, desktop scanners, digital cameras, color printers, digital imaging software, and digital pre-press and printing equipment. The evaluation should include existing emerging threats to FRN features used by the general public to authenticate currency, as well as features used in vending, ATM's, retail sorters, the gaming industry and other automated currency processing.
2. Identify features, materials, and technologies to deter counterfeiting of FRNs, and assess their relative effectiveness. The study should include the identification, analysis, evaluation, and ranking by effectiveness of technologies that may deter the counterfeiting of FRNs and that could be incorporated into U.S. banknotes in the longer term (more than 5 years). The evaluations of technologies should include the following criteria:
    a. Effectiveness in deterring the counterfeiting of FRNs (i.e., difficulty in duplicating or simulating FRNs using existing or emerging commercially available materials and processes);
    b. Promoting visual authentication (i.e., technologies that are visually distinctive and obvious to the untrained observer, as well as noticeable, understandable, and easily used by the general public as a method of visually authenticating FRNs in a variety of lighting conditions);
    c. Uniqueness and aesthetics (i.e., novel or strikingly different from existing features used to deter counterfeiting of high security documents, and aesthetically pleasing in the design of FRNs).
3. Identify potential costs, including material costs, equipment costs, and the costs of processing banknotes for the Federal Reserve System and third-party users of FRNs, including transportation, storage/handling, and eventual disposal. Feature evaluation should evaluate the implications of implementing proposed materials, technologies, or features on the BEP's FRN manufacturing operations, including the following:
    a. Evaluation of the merits of exploiting the three-dimensional character of a banknote. Development of a new class of deterrents based on compositional changes of the substrate [the surface or material on which printing is done], incorporating new materials in a variety of new innovative ways, or incorporating optical or auditory security elements into the substrate.
    b. Evaluation of alternative banknote substrates relative to each other, and the potential of blending various substrates with other substrates—including standard banknote paper to create a hybrid that expands value as a counterfeit deterrent or new security feature. Include substrates already used for banknotes world-wide, as well as potential materials not yet in use, but that may have significant potential benefits.

Secondary Task (not required, but to be completed if time and funds allow)

4. Identify, including analysis, evaluation and ranking of the effectiveness of technologies that could be incorporated into FRNs in the long term (more than 5 years) for denominating or authenticating by the blind, for forensic analysis, and for third-party machine denominating or authenticating (e.g., point of sale), including estimated costs of implementation.

This first report of the study assesses the counterfeiting threats to FRNs resulting from new technology as specified in Task 1 of the committee's charge. The committee's second report will take into account these threats while evaluating new banknote features as requested in Tasks 2, 3, and 4.

During the course of this study, the committee's deliberations also highlighted the perhaps greater threat of counterfeiting that may be perpetrated through cybercrimes relating to electronic funds transfer and digital currency. Considering these threats is clearly beyond the scope of this study, but the committee strongly believes that this equally if not more important subject should be examined further in the future.

The members of the committee appointed for this study have expertise encompassing a broad range of disciplines and fields, including systems engineering, materials science and engineering, analog and digital imaging and printing, optics, computer software and hardware engineering, decision analysis and operations research, paper science, biomaterials, optical materials, and art.

The committee met a total of three times: on May 23-24, 2005, and July 21-22, 2005, in Washington, D.C., and on October 10-11, 2005, in Woods Hole, Massachusetts. The first two meetings included sessions open to the public; the third was devoted to the preparation of the report.

The committee is grateful to the following individuals, who presented invited briefings on specific areas relevant to the management, design, and production of banknotes; security features; and machine verification of banknotes: Sara Church of the Bank of Canada, Peter Crean of the Xerox Corporation, John Haslop of De La Rue, Annette Jaffe of Jaffe Consulting, James Jonza of 3M Corporation, and Ely Sachs of the Massachusetts Institute of Technology.

The committee is also particularly grateful to the following government personnel who took the time to share their perspectives with the committee: Lenore Clark, Lisa DiNunzio, Larry Felix, Tom Ferguson, Goutam Gupta, Kalyan Maitra, and Robert Stone of the Bureau of Engraving and Printing; Eugenie Foster from the Federal Reserve Board; and Lorelei Pagano of the U.S. Secret Service.

Supplementing the committee meetings, a number of site visits were conducted in order for members to gain an appreciation of banknote production, counterfeit detection, and verification equipment. The committee thanks these organizations and companies for making their personnel, facilities, and time available:

- Bureau of Engraving and Printing, Washington, D.C.;
- U.S. Secret Service, Washington, D.C.;
- Crane and Company, Dalton, Massachusetts; and
- Cummins-Allison Corporation, Mount Prospect, Illinois.

The framework used in this study to describe the counterfeiting threat considers four activities: the production, stockpiling, passing, and circulation of counterfeit notes. It also considers five classes of counterfeiters who carry out these activities, each of which employs the four activities differently. The counterfeiters are classified as primitive, hobbyist, petty criminal, professional counterfeiter, and state-sponsored counterfeiter. Both the effectiveness of new features and the implications for new production and security feature technology are highly specific to the counterfeiting activity, the class of counterfeiter, and likely detection mechanisms.

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report: Sara E. Church, Bank of Canada; David R. Clarke, University of California, Santa Barbara; Amy Crook, Not Dead Yet Studios;

Jill Culler, U.S. Patent and Trademark Office; Martin A. Hubbe, North Carolina State University; Ronald S. Indeck, Washington University; Edward H. Kaplan, Yale School of Management; Shayla Key Parker, Lawyers' Committee for Civil Rights Under Law; Johannes Schaede, KBA-GIORISA; and Mark Willner, 3DTL, Inc.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Anthony J. DeMaria, Coherent-DEOS, LLC. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Finally, the committee acknowledges the support from the staff members of the National Research Council, including Laura Toth, Marta Vornbrock, Teri Thorowgood, Michael Moloney, and Toni Marechaux.

Robert E. Schafrik, *Chair*
Committee on Technologies to Deter
Currency Counterfeiting

Contents

Tables, Figures, and Box

TABLES

FIGURES

BOX

Summary

The deterrence of currency counterfeiting is an important element of U.S. public policy because of the need to maintain confidence in the nation's currency in the United States and around the world. During the past 20 years, a counterfeiting threat has emerged with the evolution of new reprographic technology and the related emergence of a new class of counterfeiters: nonprofessional, independent individuals with limited, if any, traditional counterfeiting skills. These "casual counterfeiters" took advantage of the increased availability of advanced color copiers and color scanner-computer-printer systems during the mid-1980s. To deter counterfeiting, the Bureau of Engraving and Printing (BEP) of the U.S. Department of the Treasury began adding new features to banknotes and implemented changes in U.S. banknote design to stay a step or two ahead of this threat.

A proactive counterfeit-deterrence strategy, which includes not only continual updating of banknote features but also public education and vigorous law enforcement, has had clear results: U.S. banknotes have one of the lowest counterfeiting rates of any major currency.[1] Currently, approximately $720 billion in U.S. banknotes is in worldwide circulation. This amount is increasing by about 6.5 percent per year.[2] The rate of counterfeiting of U.S. banknotes is estimated at 5 counterfeits per million notes circulating in 2002. The number of counterfeit $100 notes is estimated at 30 counterfeits per million.[3]

In response to a request from the BEP to the National Research Council (NRC), this report identifies technologies, both existing and emerging, that pose the most significant counterfeiting threats to U.S. banknotes, also known as Federal Reserve notes (FRNs). A second report from the NRC's Committee on Technologies to Deter Currency Counterfeiting will identify future possible banknote features, materials, and technologies that could be employed to deter counterfeiting in future versions of FRNs while remaining cognizant of the threats described in this first report.

CURRENT CURRENCY FEATURES

Security features that maintain the "look and feel" of historical U.S. banknotes are key elements of today's Federal Reserve notes. These features are described in Appendix B of the report. New features—

[1] R. Judson and R. Porter. 2003. Estimating the Worldwide Volume of Counterfeit U.S. Currency: Data and Extrapolation. Report by the Federal Division of Monetary Affairs. Washington, D.C.: Board of Governors of the Federal Reserve System. The paper has two main conclusions: first, the stock of counterfeits in the world as a whole is likely on the order of 1 or fewer per 10,000 in both piece and value terms; second, losses to the U.S. public from the most commonly used note, the $20 note, are relatively small, and are minuscule when only counterfeit notes of reasonable quality are considered.

[2] E. Foster, Federal Reserve Board. 2005. Presentation to this committee, May 24.

[3] J. Haslop, De La Rue. 2005. Presentation to this committee, July 21.

including security strips, watermarks, embedded fibers, color-shifting ink, and microprinting, fine-line printing, and color printing—provide means for counterfeit deterrence and authentication as well as presenting difficulties for nonauthorized sources attempting to replicate the notes.

The security features in current use are highly durable, low cost, odorless, and environmentally sound. Many of the features are detectable by the unaided eye. The unique look and feel of the substrate itself is an important part of the FRN's recognizability.

Machine readers for currency mostly make use of FRN features that are different from those used by human cash handlers. The use of machine readers is increasing worldwide, and because the machine-readable features of currency sometimes change as currency design evolves, the design of these machines must be changed with each currency design change. It is possible that this kind of evolutionary cycle might provide a window of opportunity for astute counterfeiters. Additionally, the orientation of features may not necessarily work optimally with high-speed machine feeders, which can limit the machine's functionality, or in accommodating the visually impaired.

CLASSIFICATION OF COUNTERFEITERS AND A SYSTEMS APPROACH TO THE COUNTERFEITING THREAT

While carrying out this study the committee found it helpful to classify counterfeiters into five categories:

- *Primitive counterfeiters*—who do not use digital technology, but create counterfeits using little more than manual artistry to modify a piece of currency in order to increase its value and obtain financial gain;
- *Hobbyists*—who counterfeit occasionally and use typical desktop computer equipment and available crafting supplies, sometimes in creative ways;
- *Petty criminals*—who counterfeit in a dedicated manner and actively invest in specialized computer equipment and materials;
- *Professional counterfeiters*—who focus the efforts of a large group of people on the sophisticated production and distribution of counterfeits; and
- *State-sponsored counterfeiters*—who may use the very same high-precision equipment that the government uses to manufacture notes.

Looking at the counterfeiting threat as a system may reveal approaches or combinations of approaches that may be more effective than focusing only on one step in the process. For example, while much attention may be given to preventing the production of a counterfeit note, attention can also be paid to preventing its casual circulation.

Although U.S. currency has a low rate of counterfeiting, it is in the national interest to remain vigilant about preserving the actual and perceived security of U.S. currency. Today, domestic counterfeiting—dominated by the first four classes of counterfeiters—focuses on the $20 note and is primarily a for-profit enterprise. Foreign counterfeiting—primarily primitive, professional, and state-sponsored—currently centers on the $100 note and may be engaged in to generate revenue as well as to support other illegal activities. It is possible, however, that several trends, including the following, will affect this balance:

- Lower-cost, higher-performance image-printing equipment;
- Improved global purchasing access—which could allow counterfeiters to find and purchase specialized materials or surplus printing machinery more easily; and
- Improved communication that facilitates information sharing among counterfeiters—which may include access to expertly processed image files, leads on sources for specialty raw

materials, ideas for ways to simulate features, and connections to a distribution network for counterfeit products.

These trends enable a professional counterfeiter to expand operations dramatically with minimal cost; they may also allow a petty criminal to enter the realm of the professional without previous connections to the underworld. For example, wide distribution of counterfeit notes may be possible through communication within an Internet-based community.

The counterfeiting threat may be described by a systems model with four components. Counterfeit notes flow down the system from production through stockpiling to passing and circulation. Counterfeit deterrence focuses on disrupting or preventing each of these components. Thus, a comprehensive response to counterfeiting must include ways to do the following:

- Prevent or deter production, through the use of technology blockers and note features that are difficult to simulate;
- Empty counterfeit stockpiles, through law enforcement programs;
- Disrupt passing of counterfeit currency, by means of public education and machine authentication of currency; and
- Remove counterfeits from continued circulation, through the identification of counterfeit currency by individuals and by special methods within the banking system.

Banknote features are important elements of counterfeiting deterrence at each stage of this system. Because each class of counterfeiter engages in the four components differently, the impact of different deterrence efforts will vary among the counterfeiting classes; however, each effort fulfills an important role in preserving the security of U.S. currency.

COUNTERFEITING TECHNOLOGY TRENDS

A number of features for digital imaging tools expected to be introduced in the next 5 years would allow the casual counterfeiter to achieve what only a specialist can do today.

Image-Acquisition Technology

Digital images that appear on FRNs can be acquired using art software, digital cameras (including cell phone cameras), and a variety of digital scanning equipment. Current technology encompasses a variety of devices offering very cost-effective capture of images with adequate quality. In the future, improvements in consumer-grade scanners are possible, but they will not overcome the limitations on counterfeiting presented by substrate quality and the printing processes used to produce FRNs. Expected significant improvements in digital photography will enable the ordinary user to obtain results of the quality that professional counterfeiters can produce today.

Image-Processing Technology

Digital image processing of FRN images can be done using a wide variety of software tools, ranging in cost from free to inexpensive to very expensive. Current capabilities with such software are highly dependent on the skill of the user. In the future, substantial improvements in automation are expected to help the ordinary user process images like an expert. These improvements may include automatic contrast and brightness enhancement, optimal unsharp masking, and color balancing, and they could extend to many other areas. Significant increases in processing speed and automation capabilities may enable a user with little or no training to optimize images with high bit depth. Automated capabilities such as line-width

control, uniform image appearance, and color balance would enable an ordinary user to easily obtain an optical image that is very faithful to the original.

Image-Printing Technology

The capability needed to print captured and processed images is the limiting step in the counterfeiting process at the present time. Current printers for home use, primarily thermal ink-jet printers, offer very-low-cost image printing. Other types of ink-jet printers and electrophotographic printer technologies produce counterfeits that can be passed, even though no counterfeits produced with such equipment are currently able to withstand minimal scrutiny by a trained money handler. Thermal printing and digital photography are available but are not specifically useful for printing counterfeit notes; however, they are useful for simulating specific features.

In the future, the capabilities of electrophotographic printers will continue to advance in terms of image quality, image maintenance, and color quality. While fine lines and small details may be possible to reproduce through the use of smaller toner particles than are available today, the introduction of particles smaller than 4 to 5 micrometers is unlikely because of environmental and performance factors. A more useful improvement in electrographic printers for counterfeiters would be an improvement in gray-scale printing. Having even four levels of gray compared with the option for on-or-off imaging of most current products could provide significant advantages in image appearance.

Ink-jet printers will continue to improve, but it is unlikely that droplet volumes will fall appreciably below 1 picoliter. Improvement in the number and design of ink nozzles is also expected to increase the print speed, but more importantly, would also allow for the use of inks with the same color but differing density, thus improving both color and gray-scale image printing. Variable droplet size and placement, combined with new ink formulations and innovative curing cycles, may also help impart texture to the note or could enable printing of optically variable features.

An important class of printers consists of copiers, or devices that only scan and print an image. This class includes commercial copiers, but also stand-alone multifunction devices that may act as printers, scanners, and fax machines on the home desktop. When these are used only to scan and copy, they may bypass the image-acquisition and processing steps.

IMPLICATIONS OF DIGITAL IMAGING TRENDS

A range of excellent, reliable, and cost-effective digital printers for consumer use are available today at very affordable prices. Innovation and skilled engineering have resulted in this progress, and while innovation will continue, some physical limits may dominate the possible improvements in image quality.

Image-capture, processing, and reproduction technologies, both current and predicted, pose a significant threat to the security of Federal Reserve notes—particularly because the security of FRNs depends on the casual viewing of two-dimensional printed features in reflected light. Emerging technologies are targeted at dramatic improvements in desktop capabilities. These improvements will continue to limit the ability of any two-dimensional printed image to deter widespread counterfeiting successfully. The committee concludes that images involving other classes of features—images viewed in transmitted light, light-reflecting features, or other complex optical features—offer a substantial challenge to primitive and hobbyist counterfeiters and a costly barrier to petty and professional criminal counterfeiters.

An obvious consideration for the future is the goal of incorporating in image-processing software the ability to disable in all digital tools the processing of image patterns that are unique to currency. Because digital printing devices depend on software, the potential to disable the devices to keep them from reproducing these identified patterns is also a pertinent issue. Whereas simple copy protection may deter an opportunistic counterfeiter, the growing availability of online “hacks” means that a criminal with intent will not be deterred. A more sophisticated approach would be to add features to banknotes that

intentionally frustrate image-capture capabilities or that generate unwanted patterns when scanned and processed images are printed. Some successful features on currency today are optical features that cannot be directly captured by present-day input scanners but can be seen by the human eye.

CONCLUSIONS

The advent of new materials and fabrication technologies and image-analysis tools, and especially the existence of the Internet—which allows communication of the results of the use of these technologies and tools—have changed the world of secure documents. To keep ahead of counterfeiters, continuous assessment is needed of the development of technologies and of the viability of various deterrents in practice.

The greatest threat from counterfeiting in the future will arise from the growth in low-cost, high-performance image-printing equipment. This equipment is used today primarily by hobbyists, the most casual of counterfeiters. As the cost of imaging equipment goes down and print quality goes up, the use of this type of equipment by hobbyists will expand. The same equipment will enable expanded operations by petty criminals, and it may make counterfeiting more lucrative for professionals as well. The trend means that the protection against counterfeiting afforded by a two-dimensional printed image casually viewed in reflected light is highly diminished.

The second most pressing threat related to counterfeiting in the future—and the more insidious one—involves what can be done as a result of improved communication available via the Internet. Counterfeiters today can easily search online for raw materials and surplus high-quality printing equipment. This search capability, coupled with the ability to purchase these materials and equipment from global sources via the Internet, accounts for an important and growing threat.

Information itself is also a precious commodity for the counterfeiter. The information shared across the globe today may include ideas for simulating currency features, novel concepts for combining processes to create a better counterfeit, or expertly processed image files. Successful information sharing may also create new distribution networks for counterfeits. Such network-coordinated distribution would require law enforcement to be at least equally well networked in order to discover and stop it.

The committee concludes that reliance on the current printed image used on U.S. banknotes is not sufficient. New digital technologies combine to create the opportunity for rapid growth in counterfeiting. However, the underlying reasons why people choose to counterfeit are more difficult to understand.[4] Economic drivers, the effectiveness of laws and their enforcement, and ethical motives all play a role. All of these threats—technological, legal, and cultural—will provide an ongoing challenge to the entire monetary system.

[4]M. Naim. 2005. Illicit. New York: Doubleday. The author expressed his opinion this way: "Most of all, I was baffled by how an inherently economic phenomenon was customarily treated with moral denunciations and law enforcement remedies." P. 10.

1

Background and Overview

One necessary attribute of a modern nation is its ability to sustain an economic system among its global partners. A vital aspect of any financial system is the means of settling financial transactions quickly and fairly. This aspect of statehood directly touches every citizen. In this context, the soundness of a country's financial system is critically important to its citizens.

THE EVOLUTION OF MONEY

The use of money to facilitate financial transactions evolved during the early history of humankind. To alleviate the awkward nature of barter, primitive forms of money, such as shells and teeth, came to be used. Well before the invention of coins, societies engaged in banking and finance which reached a level of sophistication that can be compared to today's standards.

The physical representation of money over the centuries remained important. As the level of technology advanced, various cast metal forms were used for money because of the value of the metal, but also because the forms were difficult to make and to reproduce. Coins eventually became the common form of money that was minted, and the expansion of the Persian, Roman, and Ottoman empires broadened the use of coins. Banknotes were introduced originally in China, and later in Europe. Whereas gold and silver coins held intrinsic value, these paper notes represented value held elsewhere.[1]

The transformation from paper currency to electronic forms of money is clearly the latest chapter in the saga of the evolution of money in terms of both monetary value and number of transactions. Indeed, one of the major developments of the past two decades has been the rise of electronic funds transfer and digital currency. Global financial and banking networks now constitute one of the pillars on which the global economy rests; the value of the transactions handled by these networks dwarfs the cash economies of the world.[2]

Despite the pervasive use of electronic money, however, the modern world is still far from being a cashless society. Regardless of their lack of intrinsic value, banknotes have proven to be ubiquitous and highly popular for a number of reasons:

- *Access*. Many people do not have credit cards or checking accounts and only use cash transactions.

[1]Counterfeiting of currency has existed in the United States from its birth. For some brief notes on the history of counterfeiting in the United States, see http://www.secretservice.gov/counterfeit.shtml. Accessed March 2006.

[2]National Research Council. 2005. Network Science. Washington, D.C.: The National Academies Press.

- *Anonymity*. Cash purchases preserve privacy and anonymity; many consider privacy one of the basic rights of a U.S. citizen.
- *Convenience*. Cash enables rapid, low-technology sales transactions. Such transactions can take place without access to machine authentication or even electricity.
- *Acceptability*. Banknotes can serve as a universally accepted medium of exchange. The U.S. banknote is well accepted throughout the world because people understand that it is backed by confidence in U.S. economic power; and, as a stable currency, it provides a measure of protection against inflation for people in countries with unstable currencies.

THE INEVITABILITY OF COUNTERFEITING

Counterfeiting has existed almost as long as there has been money. Counterfeit coins, for example, have always been an interesting aspect of history both in the study of numismatics and in the larger world of currency. Though counterfeiting is predominantly a criminal activity, it has also been used by a number of countries as a weapon of war. Today, counterfeiting is thought to be used by terrorists as one of the means to finance their operations.

For many reasons then, nations have a strong obligation to protect the integrity of their banknotes against attempts to make illegal copies. The deterrence of counterfeiting is an important element of public policy that is required to maintain confidence in a nation's currency both domestically and internationally. Because any original banknote can be duplicated, provided the materials, equipment, and expertise are accessible, responsible states endeavor to use materials and techniques that are not generally available and that present as many obstacles as possible to would-be counterfeiters.

In the United States, the U.S. Department of the Treasury's Bureau of Engraving and Printing (BEP) and the U.S. Secret Service were established to combat pervasive counterfeiting during the Civil War. At that time, it was estimated that one-third to one-half of the currency in circulation was counterfeit. Today, counterfeit U.S. notes are estimated at less than a hundredth of 1 percent of the currency in circulation. According to the Department of the Treasury, "the value of counterfeits in circulation is most likely around $70 million, or fewer than one in 10,000 notes, with about 60 percent of these held overseas. The upper bound is estimated to be about $170 million, or about 2.8 in 10,000 notes."[3]

For hundreds of years, counterfeiting required considerable artistic and technical skill, as well as substantial resources. Until recently, the primary counterfeiting threat arose from organized professional criminals and, in a few instances, from hostile states. These types of counterfeiters were relatively large enterprises that presented multiple opportunities for tracking by law enforcement. Because the production of realistic copies of a sophisticated banknote was quite an expensive proposition, the quality of the counterfeits oftentimes was not high, enabling the public to spot forgeries readily.

This scenario began to change during the 1980s with the advent of advanced reprographic systems and the accessibility of highly capable and inexpensive graphics software tools running on readily available workstations and desktop computers. Counterfeiting of this type is not intended to duplicate the processes used to make genuine banknotes, but instead simulates the result with much less expensive equipment. This type of counterfeiting no longer required artisans to engrave intaglio plates, nor did it require a large investment. Advances have put the technical means to counterfeit in the hands of ordinary people who, if they so choose, can manufacture a few counterfeits on an irregular basis with little fear of apprehension.

At the request of the Bureau of Engraving and Printing, the National Research Council has undertaken several studies during the past 20 years to evaluate the emerging threat posed by advanced

[3]U.S. Department of the Treasury. 2003. The Use and Counterfeiting of United States Currency Abroad, Part 2. The second report to the Congress by the Secretary of the Treasury, in consultation with the Advanced Counterfeit Deterrence Steering Committee, pursuant to Section 807 of Public Law 104-132, p. 68. Available at http://www.federalreserve.gov/boarddocs/rptcongress/counterfeit2003.pdf. Accessed April 2006.

reprographic technology. Some general conclusions regarding the changing threat from three of the resulting reports are as follows:

- 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.[4]
- 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.[5]
- Rapid developments in reprographic technology could give rise to an unacceptable level of counterfeiting activity by making high-quality reprographic systems widely available.[6]
- 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 . . . 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.[7]

These studies identified potential counterfeiting threats posed by technologies that primarily replicate the visual appearance of banknotes. Until recently, most casual counterfeiters have focused on reproducing the visual appearance of a banknote while using primitive methods to replicate other features, such as the banknote's tactile properties. However, emerging technology is being extended beyond the image-reproduction capability to the capacity for simulating or duplicating tactile and other nonvisual features. Also, new consumer products in crafting supplies, automotive touch-up paints, and nail polish are a few of the tools, along with new technologies, that can provide the counterfeiter with ways to replicate both the look and feel of the U.S. banknote.

Counterfeit currency has impacts that can be considered on several levels—fiscal, personal, and psychological. While passing a counterfeit penny slug might be considered harmless, an incontrovertible fact is that no one wants to receive a counterfeit banknote.

Laws of the United States and of nearly every country prohibit the spending or possession of counterfeits and require the reporting of the receipt of a counterfeit banknote. Reported counterfeits always produce a direct monetary loss to those who receive them because the fake bills must be surrendered to authorities without compensation. With no compensation incentive, a pattern of complacency may have emerged, with many people and businesses willingly absorbing the monetary loss of the value of the counterfeit rather than taking the trouble to report it. Many would choose to avoid what could be an intrusive and time-consuming interaction with authorities. The potential awkwardness of reporting a genuine note as a fake is also present. For these reasons, it is conceivable that counterfeiting is currently an underreported crime in the United States.

The counterfeiting threat is constantly evolving, and new participants, methods, and effects are emerging.[8] Undoubtedly the greatest modern threat is the counterfeiting of electronic forms of money and

[4]National Research Council. 1985. Advanced Reprographic Systems: Counterfeiting Threat Assessment and Deterrent Measures. Washington D.C.: National Academy Press.

[5]National Research Council, 1985. See note 4.

[6]National Research Council. 1987. Counterfeit Threats and Deterrent Measures. Washington D.C.: National Academy Press.

[7]National Research Council. 1993. Counterfeit Deterrent Features for the Next-Generation Currency Design. Washington, D.C.: National Academy Press.

[8]M. Naim. 2005. Illicit. New York: Doubleday.

its use for criminal purposes.[9] While this is an urgent and strategic issue for modern law enforcement, it is not the focus of this report, which addresses the counterfeiting of physical currency, specifically, U.S. Federal Reserve notes (FRNs).

An effective defense against counterfeiting requires an examination of technological advancements that can be employed by potential counterfeiters. It is clear that distributed, low-volume, casual counterfeiting poses a significant challenge to law enforcement. Indeed, much of the BEP's rationale for upgrading the security features in U.S. banknotes has been based in the countering of this threat. The resulting proactive analysis has significantly influenced the design changes and incorporation of additional security features in U.S. banknotes during the past 20 years. Educating the general public with respect to the new security elements used in the redesign of banknotes and encouraging the use of simple but relatively accurate authentication tests have also become more important.

THE NEED FOR A SYSTEMS APPROACH

A U.S. banknote is one of the most respected items in our culture, yet it can also be one of the most mistreated. No other item of such value is routinely folded, crumpled, soiled, laundered, and otherwise ill-treated throughout its useful life. To survive this challenge, U.S. banknotes must meet daunting physical requirements. They must be manufactured reliably in large quantities and must be durable over time. In addition, their features must allow authentication, indicate their denomination, and deter their counterfeiting.

Advances in reprographic technologies have driven the addition of specific counterfeit-deterrent features, which have been adopted without compromising current banknote recognition and respect.[10] In the last decades of the 20th century, digital reprography—especially color copiers, desktop computers, and color printers—emerged as a serious counterfeiting threat. The ubiquitousness of home computers meant that casual computer users could now more easily make high-quality banknote simulations. It was this trend that led to the major redesign of U.S. banknotes. Since the mid-1980s, digital image-acquisition, image-processing, and image-printing technologies have grown steadily in their effect on FRN counterfeiting. Digitally produced counterfeits have increased from less than 1 percent in 1995 to roughly 40 percent today.[11]

The $1 bill was first issued as a Federal Reserve note in 1929, and its design has remained essentially unchanged since then. The $2 notes in use today were introduced in 1976, and their design has remained unchanged as well. The $5, $10, $20, $50, and $100 bills were redesigned beginning in 1990 to include several new security features that vary depending on the denomination. Most notable among the features added to FRNs are the introduction of offset printing (of colors other than green and black), color-shifting ink, watermarks, and colored threads. (Appendix B describes these features.) These features have been added while retaining the characteristic, highly recognizable appearance of U.S. currency. However, it is becoming increasingly easy and common to acquire and process the digital two-dimensional image features that are meant to be observed in reflected light. The capabilities of the technology are quickly approaching the point at which such features will no longer produce a significant barrier even to casual counterfeiting.

These developments make necessary a regular assessment of the current state and near-term outlook for these technologies and of the threats that they may pose in terms of providing capabilities for creating

[9]B. Grow. 2006. Gold rush. Business Week 3966:68-69.

[10]The process began with the New Currency Design Task Force, which comprised representatives of the U.S. Department of the Treasury, the Federal Reserve System, the U.S. Secret Service, and the Bureau of Engraving and Printing (BEP). The Task Force made its recommendations to the Advanced Counterfeit Deterrence Steering Committee, also composed of representatives of the Treasury Department, Federal Reserve, Secret Service, and BEP. On the basis of *Counterfeit Deterrent Features for the Next-Generation Currency Design*, a comprehensive study by the National Research Council (NRC) issued in 1993, the Steering Committee then made recommendations for the new design and security features to the Secretary of the Treasury, who has the statutory authority to approve such changes.

[11]L. Pagano, U.S. Secret Service. 2005. Presentation to this committee, May 24.

counterfeit FRNs. These trends also imply that more elaborate optical and substrate features will need to be incorporated in the FRNs of the future to stay ahead of counterfeiters. The increase in digital counterfeits has also increased the availability of point-of-use machine detection of counterfeits. This may someday be a viable means to detect both counterfeit notes and their sources in an era of greater and more widespread use of digital image technology.

Understanding and addressing the growing complexity of technologies used to produce, to verify, and to counterfeit FRNs requires a systems model. Such a model would permit a synthetic view of the application of new technology not only in the creation of counterfeit notes but also in their detection, their removal from circulation, and the identification of their sources.

THE EFFECTIVENESS OF FEATURES ON U.S. BANKNOTES

In the same way that "$" is a global symbol for "money," U.S. currency is considered to be a worldwide symbol of security and integrity. The unique combination of design, paper and inks, and printing technology make a U.S. banknote one of the most recognized symbols worldwide. Maintaining this symbol and what it stands for is among the duties of the Bureau of Engraving and Printing. In the early history of the United States, the design of paper currency changed many times. Since 1928, however, changes in the design have preserved the overall architecture of U.S. currency; that is, all U.S. currency in circulation has the same size and feel, and the same historical figures and national symbols remain the same for each denomination. Appendix B describes the features on current U.S. notes, instituted in part to deter the creation of counterfeit notes. It is noteworthy that while many changes have been instituted there has been no recall or demonetization of U.S. currency already in circulation.

The effectiveness of a banknote feature depends on the specific nature of a note's use. Examples of different types of use include the following: two individuals wishing to complete a sale; a variety of machines designed to accept, disperse, or count banknotes; visually impaired individuals engaged in a transaction involving currency with machines or people; a foreign government official contemplating the circulation of U.S. banknotes in the local economy; and, finally, a counterfeiter intent on breaking the law. Banknote design is complicated by this wide variety of uses: a given feature on a banknote may aid just one or many of them. The wide range in types of use for FRNs is complicated further by the fact that these transactions may take place anywhere on the globe under a wide range of ambient lighting conditions.

For any feature to be effective, it must work for the duration of the life of the note. A variety of durability tests are conducted by the BEP to ensure that banknotes have a reasonable circulation life. Tests include repeated crumpling and folding, soiling and occasional laundering of notes, as well as tests of their wet tensile strength, lightfastness, and chemical resistance to a variety of fluids. Interestingly, the durability of banknotes is itself a security feature. Experts report that counterfeit notes are often identified by their poor and uneven wear.[12]

Visual and Tactile Effectiveness

The most striking visual feature of an FRN is the portrait on the front of the note. It is the largest single feature, and because it is a human face, many people find it easy to recognize small changes in its proportions or coloring.

Each note also has one large, high-contrast numeral for use in low-light environments and by the visually impaired. However, this feature and others do not provide adequate differentiation for many visually impaired individuals and provide no method of differentiation for blind persons.[13,14]

[12]J. Haslop, De La Rue. 2005. Presentation to this committee, July 21.

[13]National Research Council. 1995. Currency Features for Visually Impaired People. Washington, D.C.: National Academy Press.

Overt visual features on U.S. banknotes are designed to require only direct visual inspection for authentication. They are also intended to be impossible to replicate using low-resolution computer technology. These include the watermarked images, embedded plastic security strips, and color-shifting ink. Each of these features is denomination-specific; the watermarks repeat the portrait on each denomination and the security strips are embedded in a different position and contain different text and graphics for each denomination.

Perhaps more important than the effectiveness of individual features is the effectiveness of the combination of features on the entire note. The placement of features and how they interact, however, is difficult to gauge. For example, printing over the many visual security features in the paper substrate may make them less effective. Crowding the note with too many features may result in users not noticing any of them.

The lack of comprehensive information on the effectiveness of individual features was striking. Specifically, a variety of systematic and well-designed statistical tests would be very useful in decision making regarding recent feature modification and implementation. A limited number of these are discussed here, and more are needed.

The BEP conducted a focus group study in 2001 and 2002 to determine how specific cash-handling audiences detect counterfeits in Series 1996 banknotes.[15] In the course of these focus group studies, the bureau interviewed a total of 1,423 people in six categories: consumers, bank tellers, cashiers, gaming industry employees, law enforcement officials, and teachers. It was found that 29 percent of the cash handlers interviewed had identified counterfeit notes; the major tip-off was that the note "looked suspicious," followed closely by the fact that it "felt suspicious." In order, the features that caused interviewees to look closer were these: color, waxy feel, paper feel, paper thickness, smudged ink, portrait quality, and security strip. Color is the first feature checked, according to the group interviewed, and color is now easily duplicated by commonly available computer technology. Thus, the new series of notes may be less secure because cash handlers might stop looking for other features if the color appears to be "correct."

The BEP focus group members reported that when they suspected a counterfeit, the features that they used for confirmation, in order, were these: watermark, pen to indicate starch content, security strip, feel, color-shifting ink, fine lines, and shading in the denomination number. The features that this focus group was most aware of were, in order: watermark, security strip, color-shifting ink, fine lines, and microprinting.

Although interesting and informative, focus group data are not as useful as those obtained in controlled studies, and self-reported usage of features should be interpreted with caution. In more controlled studies on U.S. currency, researchers have observed that "experiments indicate that people are good at detecting counterfeits, that inkjet counterfeits are easier to detect than offset counterfeits, and that counterfeits of the newly designed bills are easier to detect than counterfeits of the older series. The design improvement was greatest with the $100 bills and, to a lesser extent, $50 bills."[16]

A marked improvement was also noted in recognition of the copper-to-green color-shifting ink on the $20 and $50 notes versus the green-to-black ink on the $10 and $100 notes. However, a key observation made in the course of this study was that "judging the improvement of features was not the same as judging their absolute efficacy."[17] When asking participants in the study to look at single features on the notes, the researchers noticed a variation in perception between situations when the entire note was presented and when the rest of the note was masked and only a single feature was visible. Experience and focus were also noted as key discriminators.

---

[14]Information at http://www.ourmoneytoo.org/position.php refers to strategies of individuals and coalitions for improving this aspect of U.S. banknotes. Accessed March 2006.

[15]Summary of BEP focus groups conducted in 2001 and 2002.

[16]A.P. Hillstrom and I.H. Bernstein. 2002. Counterfeit detection for new and old currency designs. Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV, R.L. van Renesse (ed.), Vol. 4677, pp. 65-80.

[17] Hillstrom and Bernstein, 2002. See note 16.

Studies of banknote features on other nation's currencies have confirmed the importance of subjective considerations, including the consistency of the feature from note to note and the complexity of the overall design.[18,19] All of the studies cited observed that education plays a large role in recognition of a genuine note.

Machine Counting and Authentication

In addition to the visually and tactilely detectable features of FRNs—a key line of defense against the passing of counterfeit notes—several machine-readable features are useful for both authentication and denomination. Machine reading of banknotes is a new technology; it was virtually nonexistent 15 years ago, but now annually processes more than $64 billion in U.S. currency. The features of U.S. banknotes most used in current machine readers are the optical spectrum and image, magnetic inks, ultraviolet fluorescence, ultraviolet spectrum, and infrared ink pattern. Low-end readers may sense only a single feature, usually the infrared ink pattern; high-end readers may use 10 or more measurements to authenticate each note.

Four classes of machine readers are shown in Table 1-1. Each of these machines relies on different sets of banknote features:

- *Single-note denominators*. Commonly found in vending machines and change machines and at self-checkout stations, these typically use infrared, broad-wavelength optical, or magnetic sensors to detect denomination-specific features.
- *Single-note authenticators*. These typically include additional sensors to also detect ultraviolet and fluorescent patterns and to identify individual features.
- *Desktop counters*. These are used to sort and count large numbers of notes at high speeds, up to thousands of notes per minute. They typically employ broad-wavelength optical imaging, ultraviolet spectrum, and magnetic signals.
- *High-speed counter-sorters*. These require features that give a strong signal that is not highly position dependent; thus, neither the ultraviolet and infrared ink features nor the gamut of overt features are generally sensed. Large-scale counter-sorters, used typically by banks, casinos, and high-volume businesses, employ detection technologies similar to those of desktop counters.

Typically, manufacturers of machine readers report that low-quality counterfeits are identified by a low optical image quality, lack of magnetic and/or infrared ink, or incorrect paper fluorescence. High-quality counterfeits may require detailed magnetic signature sensing or ultraviolet spectrum sensing to be detected. Ninety percent of suspect notes are caught because they do not have an authentic magnetic pattern signature.

Most overt counterfeit-deterrent features are not used by machine readers because they are difficult to sense, locate, or verify. Features not used for machine authentication include color-shifting ink, cotton fibers, watermarks, security strips, and microprinting.

Typical machine readers use point sensors that scan a narrow strip near the center of the note as it moves through the reader; they do not scan the full width of the bill. To do so would require an array of point sensors, which would be cost-prohibitive, or a rastered sensor, which would be speed-prohibitive. In addition, the large data set collected by scanning the complete note would require too much time to analyze. Because point sensors are used, image-recognition schemes, which require scanning a large area,

[18]A.A. Andrade. 2004. Assessing the security of a hologram with the assistance of a multi-criteria decision analysis. Keesing Journal of Documents and Identity 9:10-14.

[19]R.M. Klein, S. Gadbois, and J.J. Christie. 2004. Perception and detection of counterfeit currency in Canada: Note quality, training and security features. Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques V, R.L. van Renesse (ed.), Vol. 5310, pp. 1-12.

TABLE 1-1 Banknote Features Used in Commercial Machine Authentication

Feature	Single-Note Denominator		Single-Note Authenticator	Desktop Counter	High-Speed Counter-Sorter
	Low-end	High-end			
Optical spectrum	—	X	X	X	X
Magnetic properties	—	X	X	X	X
Paper fluorescence	—	—	X	X	X
Fluorescent strip	—	—	X	X	X
Color-shifting inks	X	X	X	—	—

NOTE: Features not used in commercial machine authentication include the watermark, optically variable ink, security strip, microprinting, portrait, freedom symbols, intaglio printing, color, digital counterfeit deterrence system, metallic ink seals, and colored fibers.

are not practical. In addition, small, distinct features such as security strips, which occur in different locations on each denomination, may miss the sensor "window." Finally, features that move when a note is redesigned may move out of the sensor window.

In a high-speed counter, the signal strength from each note must be high enough to be sensed in 0.04 second. Several features can be useful for reading in this short time, including the magnetic ink signal, the pattern in infrared ink, and the ultraviolet spectrum and fluorescence of the paper. High color contrast, as in previous, all-intaglio note series, provides a strong optical signal; however, artistically smooth shadings and the addition of multiple colors and features cause the optical contrast to decrease. In addition, for the purposes of machine readers, the signal from a feature must be reliable. Overall color, which changes with use, is an example of an unreliable signal.

Machine readers feed notes in one of two directions. "Short-end-first" readers include nearly all single-note readers, as well as some large-scale counter-sorters. All other high-speed readers take notes "wide-end first." The advantage of short-end-first readers is that sensing the length of the bill provides more information and a higher signal. Wide-end-first readers have the advantage in speed because they read a shorter path per bill.

Certain features on current notes are easily read in either feed direction. These include the ultraviolet spectrum and fluorescence of the paper and the patterns in magnetic and optical ink in the printed image. An example of a feature that is not readable in both directions is the infrared ink pattern, which is a set of stripes parallel to the short edge of the note.[20] A short-end-first reader senses an on-off pattern as the counter moves along the note, whereas a wide-end-first reader cannot sense the stripe pattern, but only whether the sensor is or is not within a stripe.

CONCLUSIONS

Security features that maintain the "look and feel" of historical U.S. banknotes have been added to today's Federal Reserve notes. (Appendix B describes these features.) These new features—including security strips, watermarks, embedded fibers, color-shifting ink, and microprinting, fine-line printing, and color printing—provide means for counterfeit deterrence and authentication as well as presenting difficulties for nonauthorized sources attempting to replicate the notes.

[20]Cummins-Allison Corporation, Mount Prospect, Ill. 2005. Discussions during a subcommittee visit, October 7.

The security features in current use are highly durable, low-cost, odorless,[21] and environmentally sound. Many of the features are detectable by the unaided eye. The unique look and feel of the substrate itself is an important part of the FRN's recognizability, so printing over much of it may be counterproductive.

The use of machine readers for currency is increasing worldwide; the security features used by machine readers differ from those used by human cash handlers. Because the machine-readable features of currency are sometimes changed as currency design changes, the design of these machines must be changed with each currency design change, which may provide a window of opportunity for astute counterfeiters. Additionally, the orientation of features may not necessarily work optimally with high-speed machine feeders, which can limit the machine's functionality.

[21]It is interesting to note that banknotes are odorless once the ink has fully dried; however, some volatiles may be detected by scent in brand new notes.

2

Counterfeiting Technology Trends

Current digital technology has evolved over the past 20 years in a number of ways. Some of these were predicted, but many—especially the low cost for high quality—were difficult to foresee in the early days of photoreproduction. The digital technology revolution has had a profound effect on counterfeiting technology. Each of the three major steps involved in digital imaging technology is used in counterfeiting: (1) acquiring the image, (2) processing the image, and (3) printing the image.

Each of these three steps may be carried out in either binary or analog mode, there may sometimes be hybrid processes, and steps may be done in various combinations. Both binary and analog images have advantages and disadvantages. Producing images in binary systems requires patterning the image in such a way as to make it appear to have gradations; upon close inspection, these are dense on-and-off spatial patterns. Each pixel must be printed with either ink or no ink. Analog printing produces images with an array of elements that have different optical densities. Hybrid systems can draw from both paradigms, but the results tend toward the artistic rather than producing multiple images that are all closely identical.

IMAGE ACQUISITION

To replicate the Federal Reserve note (FRN) using digital technology, a counterfeiter must first transform an analog copy—a physical note, printed by the Bureau of Engraving and Printing (BEP)—into a digital format. This is also called image capture. A variety of low-cost, high-quality consumer-grade devices for image capture are available. Capture devices can also be custom-built by enterprising counterfeiters. Table 2-1 provides a summary of image-capture devices, their capabilities, and relative costs.

Scanners

U.S. currency is approximately 2.5 by 6.0 inches, which means that the scanned image of a U.S. banknote from a 2,500 pixel per inch (ppi) scanner would be about 6,250 by 15,000 pixels. This would result in an RGB (red, green, blue) file size of about 94 million pixels, which is well beyond the performance capabilities of a digital camera. A counterfeiter would have to piece together several images taken with a digital camera to use this method. However, this image size is well within the capabilities of even lower-priced home copiers and amateur flatbed scanners.

An artifact of the image-scanning system revolves around the fact that the majority of the printed features on FRNs are binary, meaning that at every pixel, ink is either deposited on the substrate or it is

TABLE 2-1 Capabilities of Digital Image Capture Devices

Capture Device	Resolution (pixels per inch)	Cost	Comments
Digital camera	Varies	Low to High	Limited number of total pixels available
Simple consumer-grade reflective flatbed scanner	2,500	Low	Ideal for counterfeiting owing to high quality and low cost
High-quality reflective flatbed scanner	2,500-4,000	Moderate	High quality with only slightly higher costs
Professional drum scanner	4,000-5,000	High	High cost presents barrier to entry
Artwork software	No limit	Free to Moderate	Time consuming and limited to use by experienced artists

not. This is characteristic of virtually all of today's high-quality printing processes.[1] An image sourced from an input scanner is usually retained, not in binary form, but in analog. This means that each pixel of the image is retained with more than 1 bit of information, usually at least 8 bits, or 256 levels of intensity. These levels are then sent to the image-processing software. When the image is prepared for printing, however, the bit depth is reduced again to 1 bit because most electronic printers are binary devices. Most often, because halftoning or similar techniques are used to generate the appearance of gray in the image that is printed, the sharp binary image is lost in the transition to analog and back again.

A scanning resolution of up to 4,000 to 5,000 pixels per inch is currently available on the best graphic arts scanners. These scanners are often referred to as copy-dot scanners because they attempt to copy all of the halftone dots in the original. Printing on currency paper, however, is difficult above 2,500 pixels per inch because of surface roughness. Thus, advances in image capture will not improve image acquisition for counterfeiting since that is at a practical limit already.

An exception to the binary nature of printing on the current U.S. banknote is the watermark. This is not strictly a binary image, and it is likely that analog image capture would do a better job than binary could in reproducing a watermark through printing.

Artwork Software

The process of visually inspecting currency and then re-creating it line by line using software illustration programs is a painfully slow process. However, this approach is also one in which great detail can be properly executed. Re-creating a design feature by feature may be more efficient, and programs such as Adobe Illustrator, Adobe Photoshop, Adobe Pagemaker, and Quark Xpress provide a rich set of tools with which to generate exceptionally high-quality images. In addition, these programs can leave the created or re-created data in a form that can allow "resolution-independent" printing options. This means that the quality of the output will be materially dependent on the quality of the printer.

This is generally not true of scanning or other pixel-by-pixel methods. Bitmap editing, or pixel-by-pixel editing, can be done using very inexpensive software such as Microsoft Paint, but it would take a tremendous investment in time and a good dose of eyestrain to generate a useful image this way. While illustration programs and software will improve over the next several years, the hard work of faithfully capturing a "squiggly" line bit by bit will be difficult to turn over to the machine. Using an illustration program in this manner is not unlike engraving the false duplicate by hand. Thus, while a software rendering of currency in a pixel-by-pixel fashion is a viable approach, it is likely to be uncommon. The labor content of such an approach is not expected to abate in the next 5 to 10 years.

[1]Photographic film and thermal dye printers are two exceptions in that they are analog rather than binary technology.

Image-Acquisition Implications

Image capture for the average consumer or user is at a high state of development. Flatbed input scanners costing a few hundred dollars or less can now scan at high quality, at reasonable speed, and with spatial pixel densities up to 3,000 pixels per inch or higher. This resolution is more than adequate to capture most printed material very well, especially with some post processing of the image to enhance fine features.

While there may be improvements in capture technology, such as increased bit depth of the image and larger tonal ranges, increasing the scanning density beyond an effective 4,000 pixels per inch is both impractical and unnecessary. Current flatbed scanners usually use a single silicon sensor chip that has sufficient sensors to cover the entire page image. This means that if one is scanning at 3,000 pixels per inch, the chip would need about 25,000 sensors to cover an image 8½ inches wide. Furthermore, the imaging lens must image the platen of the scanner at sufficient quality to permit the sensor density to be adequately utilized.

Image scanner design always presents a trade-off between speed and spatial resolution. The light sources used in most flatbed scanners are either special fluorescent lamps or light-emitting diodes, and the lens f-number, or ratio of focal length to optical aperture, must be such that it can adequately generate the required flux on the silicon sensors in the time required while maintaining the required image quality. This is often no easy task, but significant progress has been made in the past few years.

It thus appears that the quality available today for image acquisition may not improve greatly. Consider that improved scanning pixel density will not be needed for most applications and that increasing this density would require costly improvements in optics and storage. The profitability of flatbed scanners is not high enough to warrant large investments for specialty or niche applications. In addition, increasing the bit depth to 12 or 14 bits per pixel would significantly improve the quality of scanned continuous-tone material such as film or other analog images. However, because authentic currency is printed using a binary process, this would not improve the scanned image quality of banknotes.

Digital cameras will certainly continue to improve their quality levels, and performance-for-cost will significantly increase in the next few years. Cell phone cameras are becoming so ubiquitous and functional that an increase in quality will make them a serious threat. Today, digital cameras cannot provide the image quality of a flatbed scanner owing to many optical effects as well as to limited pixel density. Capturing the approximate appearance of security strips and watermarks, however, can be done quite well with either digital cameras or flatbed scanners.

The use of masking software, automated subroutines, and other such software shortcuts can greatly reduce the amount of work required of a determined counterfeiter. Less with hardware than with artistic design software, innovations are made and integrated into each generation of upgrades, making it easier for the skilled user to reproduce complex effects. In addition, software that seeks to reproduce the look and feel of traditional art materials has advanced by leaps and bounds in the past few years and continues to improve—intaglio being a traditional medium that can now be simulated more easily than ever.

In summary, innovations in flatbed scanners, artistic design software, and other methods for capturing images are not likely to be an area in which technology will further aid the counterfeiter in the next 5 or 10 years. Scan quality along with the capture of color features and other image characteristics is already adequate for many counterfeiting activities.

IMAGE PROCESSING

Once an image has been captured, it must undergo a number of processing steps before a good reproduction can be made. Some of these steps, listed below, would likely be used in preparing an image for high-quality reproduction. Of course, poorer-quality reproductions are possible without this additional effort.

- Removing scanning artifacts such as dust specks;
- Adjusting the brightness and contrast of the image;
- Performing color adjustments;
- Applying software filters to enhance edges and sharpen the image, often called unsharp masking; and
- Rotating of the image if it has been scanned at a small angle.[2]

Image-Processing Capabilities

One of the significant improvements in image processing has come about through generally available software. Packages such as Adobe Photoshop, Microsoft's Digital Image Pro, and others provide powerful tools for improving and enhancing digital images. Personal computer (PC) operating systems also are sold with image tools that can be accessed by the most casual users. The capabilities of the very low cost tools are expected to increase with new operating system releases. The growing demand for accessible digital photography tools makes image processing a very rich area of innovation that will be available to the counterfeiter. Additional tools available through online photo-sharing Web sites can easily—and anonymously—improve the reproduction of color images.

While image scanning is approaching practical cost limits, image processing has just begun its advance toward impressive automation and application capabilities.

Scanning of sharp lines such as those found in intaglio printing is a particular challenge. Often, the images of lines scanned at angles or lines that are wavy or that possess other artistic features will not necessarily reproduce with uniform thickness in an image. When printed, the lines can vary by a pixel or so, which can be quite obvious in certain circumstances. Often such lines need to be retouched to remove problematic artifacts. Software to perform this task automatically is under development; it would greatly reduce the labor cost of making high-quality images and eliminate the need for special skills.

To prepare an image for most digital printing, the scanned image needs to be converted to a binary format. The scanned image can be halftoned, as in conventional printing, or it can be made without halftone patterns using an on-off process often referred to as thresholding. While technologies are in development, it seems that the practicalities of binary printing processes will be limiting for some time.

Image-Processing Implications

Image processing will no doubt be an area of significant development in the next 5 or 10 years. The modern personal computer can now readily handle gigabyte-size images. A $20 bill captured at 4,000 pixels per inch, in color at 8 bits per image plane, is not a particularly large data file. A 2.5 by 6.0 inch FRN, at 4,000 pixels per inch, represents only 720 megabytes of disk storage space. This amount of data would have been considered immense only a few years ago; today, however, storing such an image costs only about 50 cents! Because capture quality is already at a high level of fidelity, image processing can be used to enhance the scanned image and can enable high-quality printing. However, most of the software available today, while having somewhat sophisticated automated tools, delivers the best results when it is in the hands of experienced users.

In the next 5 years, much of what occurs today in application software may be incorporated in the scanner or operating system. The growth of the digital imaging market will require that such capabilities be close to automatic. A few years ago, one could do a very good job of processing color film and prints at home. To do so required a darkroom, chemistry, some basic photoinstrumentation, and a lot of experience if it was to be done well. As is clear from any number of trends, the darkroom is now digital,

[2]This can be quite important in banknotes with features that rely on front-to-back registration. However, today's U.S. banknotes do not utilize such a feature.

and today's experienced digital imaging enthusiasts are constantly improving their skills. However, like their predecessors in chemical photography, most do not "mix their own chemicals"; they use what is commercially available. This is becoming easier; several products introduced in 2005 will automatically produce multiple versions of a color-corrected image, requiring the user simply to select the best image from a group.

Most users want to take a picture with their digital camera or scan an image with their scanner and then be able to print out a faithful reproduction of the original. While good images can be readily obtained today, faithful reproductions are not so easy or repeatable. Color-management tools are available in image-processing software and are intended to deliver good color reproduction. A skilled user will be able to match colors easily, and these tools are becoming accessible even to casual users.

Technology development will result in increasing automation in image processing in the next 5 to 10 years. Techniques such as automatic contrast adjustment, unsharp masking, line width control, and feature smoothing are all under development as automatic features. The driver for these changes is to make the user's experience as pleasant and simple as possible. Automatic comparison of the input and output image is currently available in some software packages. Significant improvement is expected in image reproduction because the market will demand it.

In 1981, SciTex provided a stunning image-processing system for graphic artists that cost approximately $1 million. Today, systems that dwarf SciTex system capabilities can be purchased along with their host PC for less than $2,000, a 500 times performance-for-cost improvement. There is no indication that we are nearing the limit of software or computing technology. The ability to use image-processing software to customize individual notes by changing the serial numbers, plate numbers, or other identifiers may enhance the ability to pass a counterfeit note.

IMAGE PRINTING

Image printing is the final step in digital reproduction except for finishing operations, which would include cutting, trimming, and the addition of simulated security elements. Electronic printing began more than 35 years ago with the invention of the laser printer. When the first laser printers were built, no one could have envisioned the quality levels that would be attainable today. The same can be said of early ink-jet printers which were interesting, but around the time of their invention they were never seen as being capable of what can currently be purchased today for less than $100. Where will these technologies go in the future? What might limit quality improvements from both a technological and operating performance for cost standpoint?

The basic categories of printer technology are described in the subsections below, where both innovations and variations on the processes are considered. The electronic printing technology area is in a constant state of flux, and other fields of development including printed displays and electronics may spur the development of printing well beyond the paper-based markets of today. Often, one field drives technology that provides for another field significant opportunity that would not have otherwise occurred.

Printer features and their capabilities are also summarized in Table 2-2. Note that "printers" also include copiers, or devices that only scan and print an image. This encompasses commercial copiers, but also stand-alone multifunction devices that may act as printers, scanners, and fax machines on the home desktop.

While ink-jet technology has the highest number of printers in the market, electrophotography—used in laser printers and most large copiers—provides the maximum overall revenue to the industry. Both of these printer technologies are lucrative investments for corporations, and for this reason their capabilities are expected to continue to advance. It is interesting to note that printer business lines are highly profitable, whereas scanner business lines are not. Currently, the revenue generated by consumables such as toner, ink, and paper makes the difference.

TABLE 2-2 Some Printer Technologies and Capabilities

Technology	Resolution (μm)	Cost	Comments
Electrophotographic (laser)	7-10	Low	Potential primarily for low-volume counterfeiting
Ink jet	7	Low	Attractive for all classes of counterfeiters owing to low cost and high resolution
Thermal	2	Low	Limited by low-image-quality substrate chemistry requirements
Chemical	NA	High	High cost, variable quality, and limited availability of adequate substrate materials
Photographic	NA	High	Produces quality similar to that obtainable with ink-jet printers but at a higher cost

Electrophotography

The electrophotographic process is the basis of the most widely used document-copying machines.[3] It begins with a photoconducting surface that is uniformly statically charged. In many copiers, this is a metal plate with a selenium-based coating. The charged surface is then exposed to a pattern of focused light, usually from a laser or light-emitting diode. This pattern is the image to be printed. Where light falls, the charge dissipates and a "charge image" of the light pattern remains on the photoconductor surface.

The image is developed by dusting the charged surface with a pigmented powder, called toner, which is attracted to the charged areas of the pattern. The powder is then transferred electrostatically to paper and, finally, the toner is fused to the paper with heat. A continuously rotating metal drum moves the plate and paper through the various steps—charging, exposing, developing, and transferring—in a seamless manner.

The quality of electrophotographic images has improved continually since its introduction in the mid-1900s. The critical elements of electrophotography technology for counterfeiting are the development, transfer, and fusing steps. These control the image quality and are also where advancements have resulted in higher quality and lower cost.

In the development of the image, in which the toner material forms the text and images on the printed paper, the size of the toner particles controls the print resolution. As first implemented, particle size in toner averaged about 12 micrometers (μm). In order to improve image resolution to 600 dots per inch, the particle dimension was reduced to 8 μm and the uniformity of particles was improved. Further reductions in size will be necessary for improvements in resolution. Toners that are substantially smaller than this are not only hard to manufacture properly but also are difficult to keep confined to the printer itself; that is, they can be become airborne. Toners with particles as small as 1 or 2 μm can be made, but they can be hazardous if they become airborne and are inhaled by users.

Advances in the materials properties of toner can also help improve resolution during fusing and transfer. By varying the chemistry of the polymer in the toner, printed images can be made to look more like ink on paper rather than having the look of electronic printing. Fusing can have serious implications for durability. Lower-cost printers often do not use fusing techniques that are as durable as those of the faster, more-expensive machines. Folding or creasing of the print can cause poorly adhered toner to fall off at the crease, thus exposing the white substrate and producing an obvious defect. As fusing technology improves, home printers could have the potential to do one-pass, two-sided printing. This means that

[3]Xerox Corporation was the principal investor in electrophotography in its early days. It became more commonly known as "xerography," apparently a catchier name than electrophotography.

registration of the images on each side of the substrate can be significantly better than that achieved by removing the printed sheet, flipping it over, and reinserting it for printing of the second image.

While the quality of electrophotographic products is expected to improve in the next several years, significant engineering challenges remain that will limit the performance of these systems. Improvements in ink-jet printing, the major market competitor for lower-cost electrophotographic printers, will continue to drive print quality.

Ink-Jet Printing

While ink-jet printers predominate in the home printer market, they are also capable of producing some of the highest-quality images of any type of printer. An ink-jet printer is any printer that shoots extremely small droplets of ink on to paper to create an image. The droplets form small dots on the printed page; these dots can range from 10 to 30 dots per millimeter.

The placement of the dots can be very precise. Ink-jet technology is particularly useful because registration in the system is an electromechanical issue that can be solved by straightforward engineering methods and techniques. For this reason, flatbed ink-jet printing has the greatest potential for future use in home printing of high-registration, simultaneously printed front and back images.

One disadvantage of this method is ink bleeding into the paper, resulting in a blurry appearance on some types of paper. These effects may be pronounced with certain types of paper, especially when the ink is water-soluble. The introduction of ultraviolet-curable, water-impervious ink-jet inks would solve the problems of stability, lightfastness, water solubility, dot gain, and spread.

Ink-jet printers fall into three categories: continuous, thermal, and piezoelectric ink jet. Their features and applicability to counterfeiting are described next.

Continuous Ink Jet

Continuous ink jet is one of the oldest ink-jet technologies in use; it is fairly mature and arguably produces the best-quality image obtainable on any type of printer. Continuous ink jet is actually better than photography in many cases in reducing image noise. Continuous ink-jet printers are not, in general, printers for home use. They are often large, and a fair level of maintenance and operator skill is required to get the most out of the device.

In continuous ink-jet technology, a high-pressure pump directs liquid ink from a reservoir through a microscopic nozzle, creating a continuous stream of ink droplets. One of the advantages of continuous ink-jet printing is the very high velocity of the ink droplets, which allows the ink drops to be thrown a long distance to the target. Another advantage is freedom from nozzle clogging, as the jet is always in use. Another key advantage of continuous ink-jet printers has been their ability to produce small drops of ink that can be repeatedly printed at the same or carefully adjacent spot to vary the effective droplet size. This capability produces stunning quality.

It is not expected that continuous ink-jet printer technology will move significantly forward in use in the next 5 to 10 years for two reasons. First, they are inherently complex to maintain and operate. Second, newer ink-jet printers or other types are now approaching the same quality levels attainable using continuous ink-jet technology.

Thermal Ink Jet

Thermal ink-jet printers, also known as bubble-jet printers, are widely available for home use. These printers operate by rapidly heating a small volume of liquid ink and forcing a steam bubble to form that ejects the ink from an orifice. As the bubble cools, the vacuum created draws fresh ink back into the nozzle.

A large investment in this technology has produced a remarkably reliable process. The print cartridge is highly engineered, with 64 or 128 tiny nozzles that are produced using photolithography. To produce an image, the printer runs a pulse of current through the heating elements. Each of the tiny chambers can fire a droplet simultaneously to produce the image.

A disadvantage of this technology for counterfeiters is that the ink must be water-based. Such inks are inexpensive to manufacture, but they may perform best on specially coated media that do not have the feel of currency paper. However, because the print head may be produced at less cost than that for other ink-jet technologies, it is a relatively low cost process.

Research and engineering are currently aimed at producing multiple drop sizes on demand. However, it is not an easy task to control the bubble and its associated heat cycle to produce different-size bubbles reliably. Possible advances in the next 5 or 10 years may also lead to increased process speed. It is not clear at this stage if either of these advances is likely to be realized for home users or only for higher-end users.

Piezoelectric Ink Jet

Most higher-end ink-jet printers use a piezoelectric crystal in each nozzle instead of a thermal heating element. "Piezo-jet" printers utilize a piezoelectric actuator to produce pressure in the liquid-ink chamber. The pressure and drop size generated by the piezoelectric actuator can be controlled better than in bubble-jet printers and can also produce smaller droplets of ink. These variable-size drops and smaller droplets can generate impressive images.

Today, the smallest commercial droplet size available is in the range of 1 picoliter. This corresponds to a drop diameter of about 7.1 μm, or about 3,500 or so drops per inch. Such small droplet sizes are generally not attainable in the bubble-jet schema. However, this very small drop size can be lost on typical paper used for home printing, so it is unknown whether the investment in such improvements would be profitable in the home market over the next 5 to 10 years.

An advantage of piezoelectric ink-jet printing is that it allows a wider variety of inks than does thermal or continuous ink-jet printing. The emerging ink-jet material deposition market uses ink-jet technologies, typically piezoelectric ink-jet, to deposit materials on substrates. Printers that can deposit glues, resins, or waxes onto a variety of substrates have been available since the early 1990s; they are called solid ink-jet or wax-jet printers. While it has advantages in color intensity, solid ink-jet technology has limited droplet size compared with that of bubble-jet or piezo-jet liquid-ink printers because the viscosity of the melted material complicates the jetting of small drops.

The piezoelectric ink-jet technology is currently available on commercial flatbed digital presses, and while they are currently very expensive, they are easily and quickly configured for counterfeiting. This is a major departure from the setup time required for commercial printing presses; it could allow counterfeiters who might work in printing shops to use the digital equipment without alerting their management. In addition, advances in this technology in the next 5 to 10 years may mean that this level of quality may be available for consumer units. Advances may also mean that metallic or plastic particles could be "printed" and someday may be able to simulate some non-image features. For these reasons, piezoelectric ink-jet printers may prove to be the most useful technology to counterfeiters now and in the future.

Thermal Printing

Thermal printing commonly is done in one of three forms: thermal transfer, thermal dye transfer printing, and custom-substrate thermal printing. Thermal transfer, one of the early printing technologies, has come and gone as a technology of choice. Its main advantage has been its reliability and high edge acutance. However, achieving printer pixel density higher than 1,000 pixels per inch is problematic owing

to the requirements for the heater heads. It is not expected that thermal transfer will be able to compete with bubble-jet, piezo-jet, or electrophotographic images as time goes on.

The second form of thermal printing, thermal dye printing, has also been referred to as dye sublimation printing. However, in most cases, sublimation is not the physical process that causes image formation, and hence "thermal dye printing" is the preferred nomenclature. Thermal dye is much like thermal transfer, except that instead of transferring material from a ribbon surface to a substrate, dye is migrated from a ribbon and absorbed into a special substrate under pressure. The main advantage of thermal dye is that it can produce true gray-scale images without any of the usual halftone patterning or other geometrical structures that trick the eye into seeing gray-scale. Such printers produce images very close to those achieved in photography. The main disadvantages of thermal dye are limitations in spatial resolution and speed. Currently, about 600 pixels per inch is the maximum practical density, which is generally low for quality currency generation.

The third form of thermal printing uses custom chemically-treated paper and prints with heater heads not unlike those used in thermal transfer. It generally cannot produce good colors, and like the other forms of thermal printing, this technology is generally low quality and is unlikely to improve in the future to any extent. The specialty substrate, in which the chemicals used for image generation are in the paper, would significantly complicate its use for currency counterfeiting.

All of these technologies are slow, expensive, and require special substrates to achieve the promised quality. Because none of them is a focus of current industry innovation, concerns about future thermal printing developments with respect to counterfeiting are likely unwarranted.

Chemical Printing

No imaging process has seen its world grow smaller more quickly than that of conventional chemical photography. Photography can produce outstanding images, but such images are no longer unique to this process. Electrophotographic and ink-jet processes can produce images in many ways as good as those of photography. Because genuine currency is produced in general with commercial processes—offset, intaglio, and letterpress printing—the images are binary, meaning that each pixel on the banknote either has ink or it has no ink. Hence, photography offers little value over simpler digital processes that are much more reliable and lower cost. Photography is still of use in the generation of printing plates, but this area is also quickly becoming digital.

There is little current activity in either using or improving the quality of nonphotographic chemical printing, and it is not expected that this technology will benefit counterfeiters in the foreseeable future. Problems of chemistry control, quality, and maintenance were the factors that killed the early chemical copiers when electrophotographic processes came on the market. These factors are still a barrier to this technology today.

Image-Printing Implications

Modern digital printers available to ordinary users can provide stunning quality at or above that available from photochemistry just a few years ago. The various electronic and other printing processes described above have varied advantages in image quality. The quality of digital presses and advanced electrophotographic printing has risen to the point that it is expected to replace offset printing in the near future. This means that the value of using offset printing as a tool to deter the counterfeiting of the images on banknotes is limited.

As in image capture, image printing is now at pixel density levels—2,400 to 3,600 pixels per inch—that are at the limits of human vision. However, improvements in image quality could come from printing images other than in binary mode. Current ink-on-paper printing such as offset and intaglio are binary processes. To simulate the look of gray—as in a watermark—commercial printing devices and most electronic printers print black ink in a patterned fashion. This patterning results in "aliasing" artifacts,

because lines are not single strokes but a collection of dots that look at normal viewing distance like single strokes.

The most useful feature of electrophotographic laser printers is that the laser beam can be turned on and left on while it is writing horizontal image structures such as a horizontal rule or line. Vertical rules are created by "stacking" pixels on top of each other. The ability to keep the beam on in the horizontal (often called the fast) direction yields higher-quality lines in electrophotographic as compared with ink-jet printers. These timing issues that affect beam placement are well understood and well used.

New approaches in both ink-jet and electrophotographic printers can produce some levels of gray, and multiple gray-level printing could produce dramatic improvements in image quality. In electrophotography, toner particulate size control and toner management as well as fusing technology (which depends on toner chemistry) will continue to set the limits for electrophotography laser printers.

Current ink-jet printers must produce only one drop of ink at a time, and each drop must be placed adjacent to the previous drop or drops to produce a line. Such lines often look a bit ragged and do not reproduce intaglio-printed structures well. The size of the ink-jet orifice and the ability to print reliably using small orifices will set the limits for ink-jet pixel density. Inks with multiple densities of the same hue may achieve different tones in the image but with much-reduced patterning. This approach has the advantage of using existing transport and mechanical systems and changing only the supply packages for printers in place.

Thermal printers can produce excellent vertical or horizontal lines, but their limited pixel density compared with that of electrophotographic and ink-jet printers is expected to render them inferior both now and in the future.

Market drivers are a final consideration for high-end printing equipment. One result of gains in desktop technologies and their capability to produce professional-looking results is that small professional printing houses across the country are going out of business and often selling their equipment for as little as 10 percent of its original cost. This may bring a professional setup well within the price range of the petty criminal. With a good computer, a pirated copy of Adobe Photoshop, a digital direct-to-plate machine, and a used Heidelberg press, a petty criminal with considerable skill might start an offset money-printing workshop in his garage. Straight-to-plate technology, in which a computer design can be digitally inked onto printing plates, can turn older equipment into very modern presses. This technology in particular may be a threat because the ease of setup is a significant advantage.

SUBSTRATES AND ADDITIONAL ELEMENTS

Each type of digital printing method discussed above has its own special substrate requirements for optimal image printing. While new substrate capabilities are always emerging, the nature of the various electronic printing technologies restricts the range and types of substrates that work well.

Most types of paper work well in electrophotographic printers. The two principal restrictions in these printers are the ability of the paper-feeding system to handle the substrate material and the substrate interactions with the electrostatic subsystems such as image transfer and fusing.

Many electrophotographic printers can easily handle light- to heavyweight papers, well within the range of currency substrates. Some newer printers can print on both sides automatically, but back-to-front registration of printed features would in general not be nearly as good as that achieved in offset printing.

The look and feel of the substrate—including the paper surface, stiffness, and intaglio texture—are difficult for most counterfeiters and technologies to reproduce using current desktop image-reproduction technology.

Ink-jet printing can be either more or less tolerant of substrate differences, whereas electrophotographic printers are less sensitive to substrate quality. Paper-feeding requirements are still important, but ink jets can generally feed a wider array of substrate thicknesses. Card stock, shiny or matte finishes, and vellums can be used, because the paper path is usually very short and throughput speeds are low. The only additional requirement of substrates used with ink-jet printers is that they permit

the ink to dry and adhere to their surface properly. Liquid ink must to some extent wick into the substrate surface for adhesion. Solid ink is almost substrate-independent, although the quality of the image might vary.

Features that affect light transmitted through the substrate—the watermark and security strip—also pose challenges, because most image reproduction is based on reflected light. Banknote features used in machine authentication (e.g., special inks) are difficult to simulate with desktop printing technology.

While thermal printers are unlikely to be used for counterfeiting, they may be used as part of a larger system. For example, laser thermal printing could be used to apply special symbols or thin foil features over a previously ink-jet-printed page. Electrophotographic printing can also be used to affix foil or holographic features.

SUMMARY OF DIGITAL IMAGING TRENDS

The counterfeiting threats from the digital imaging system components are summarized here to contribute to an understanding of trends as they relate to planning for new currency features. Table 2-3 summarizes the usefulness of security features in deterring counterfeiting that uses digital age tools. A number of features for digital imaging tools expected to be introduced in the next 5 years would allow the casual counterfeiter to achieve what only a specialist can do today.

Image-Acquisition Technology

Digital images that appear on FRNs can be acquired using art software, digital cameras (including cell phone cameras), and a variety of digital scanning equipment. Current technology encompasses a variety of devices offering very cost-effective capture of images with adequate quality. In the future, improvements in consumer-grade scanners are possible, but they will not overcome the limitations on counterfeiting presented by substrate quality and the printing processes used to produce FRNs. Expected significant improvements in digital photography will enable the ordinary user to obtain results of the quality that professional counterfeiters can produce today.

Image-Processing Technology

Digital image processing of FRN images can be done using a wide variety of software tools, ranging in cost from free to inexpensive to very expensive. Current capabilities with such software are highly dependent on the skill of the user. In the future, substantial improvements in automation are expected to help the ordinary user process images like an expert. These improvements may include automatic contrast and brightness enhancement, optimal unsharp masking, and color balancing, and they could extend to many other areas. Significant increases in processing speed and automation capabilities may enable a user with little or no training to optimize images with high bit depth. Automated capabilities such as line-width control, uniform image appearance, and color balance would enable an ordinary user to easily obtain an optical image that is very faithful to the original.

Image-Printing Technology

The capability needed to print captured and processed images is the limiting step in the counterfeiting process at the present time. Current printers for home use, primarily thermal ink-jet printers, offer very-low-cost image printing. Other types of ink-jet printers and electrophotographic printer technologies produce counterfeits that can be passed, even though no counterfeits produced with such equipment are currently able to withstand minimal scrutiny by a trained money handler. Thermal

TABLE 2-3 Usefulness of Security Features in Deterring Digital Age Counterfeiting

Features	Ink-Jet Printer	All-in-One Device	Color Copier	Flatbed Ink-Jet Printer	Digital Press	High-Quality Scanner	Imaging Software
Overt							
Substrate	++++	++++	+++	++	++	NA	NA
Tactility (or feel)	+++	++	+++	++	++	NA	NA
Watermark	+++	++++	+++	+	+	+++	+
Plastic strip	+++	+++	+++	++	+	+	—
Intaglio printing	++++	++++	+++	+	—	NA	NA
Offset color blending	++	++	+	—	—	—	—
Optically variable ink	+++	+++	+++	+	++	+	—
Intaglio microprinting	++	++	+	—	—	—	—
Offset microprinting	++	++	++	+	—	—	—
Colored threads	++	++	++	+	+	—	—
Machine-readable							
Paper fluorescence	+++	+++	++	—	—	NA	NA
Magnetic ink	++++	++++	++	—	++	NA	+
Magnetic ink pattern	++++	++++	++++	+	+	NA	NA
Color-shifting inks	++++	++++	++++	+	+	NA	—
Digital CDS	++++	—	—	+	—	+	+++
Digital BDS	—	—	++	—	—	—	—
Fluorescent thread	++++	++++	+++	—	+	NA	NA

NOTE: ++++, high deterrence value; +++, good deterrence value; ++, some deterrence value; +, low deterrence value; —, does not use this technology; NA, not applicable; CDS, counterfeit deterrence system; BDS, banknote detection system.

printing and digital photography are available but are not specifically useful for printing counterfeit notes; however, they are useful for simulating specific features.

In the future, the capabilities of electrophotographic printers will continue to advance in terms of image quality, image maintenance, and color quality. While fine lines and small details may be possible to reproduce through the use of smaller toner particles than are available today, the introduction of particles smaller than 4 to 5 micrometers is unlikely because of environmental and performance factors. A more useful improvement in electrographic printers for counterfeiters would be an improvement in gray-scale printing. Having even four levels of gray compared with the option for on-or-off imaging of most current products could provide significant advantages in image appearance.

Ink-jet printers will continue to improve, but it is unlikely that droplet volumes will fall below the current level of 1 picoliter. Improvement in the number and design of ink nozzles is also expected to increase the print speed, but more importantly, would also allow for the use of inks with the same color but differing density, thus improving both color and gray-scale image printing. Variable droplet size and placement, combined with new ink formulations and innovative curing cycles, may also help impart texture to the note or could enable printing of optically variable features.

An important class of printers consists of copiers, or devices that only scan and print an image. This includes commercial copiers, but also stand-alone multifunction devices that may act as printers, scanners, and fax machines on the home desktop. When these are used only to scan and copy, they may bypass the image-acquisition and processing steps.

EMERGING TECHNOLOGIES

The growing availability of low-cost, high-performance hardware and software for scanning, processing, and printing images remains the primary threat to secure currency. However, the emergence of some technologies that go beyond image printing may soon overtake those recognized methods.

The Convergence of Printing, Manufacturing, and Biology

A number of emerging tools use technology invented for printing on paper, although the tools themselves are designed for other processes. Examples include the high-volume manufacture of microelectronic circuits,[4] smaller-volume prototyping processes,[5,6] and even printing of biological material to aid analysis.[7] Printing-based manufacturing systems offer levels of resolution and registration that significantly exceed the current or projected capabilities of conventional ink-on-paper printers.

The target applications for this technology—such as printing flexible electronic circuits—demand very low-cost high-throughput operation, and large-area printing. Goals include rates of 100 square meters per hour, with the ability to process substrates larger than 5,000 square meters with accurate registration.

The range of "inks" that can be printed by these systems include not only the dyes and toners used in conventional printers, but also color-shifting and other optically active inks. Functional materials for the semiconductor elements of thin-film transistors or the electroluminescent layers of emissive displays have also been printed. New ink-jet printing processes can also print "inks" made of a variety of metals, glasses, and plastics, which implies that simple printing processes may be able to simulate non-image features, such as the metallic print on the security strip.

Although access to these manufacturing systems is not expected to be widespread, it will increase if their use broadens to more distributed manufacturing systems. It is also possible that some of the features of these advanced systems could migrate into low-cost desktop printers.

Some specific technologies in this area include the following:

- *Flexography, or flexographic printing*, is a dominant printing technology for labels, tags, boxes, packaging, and objects with rough or uneven surfaces. This method uses flexible (often elastomeric) printing plates mounted on cylindrical supports and inked with rollers. The resolution and registration that can be achieved with standard systems is approximately 30 microns. It may be possible to integrate high-resolution printing plates, formed using soft lithography technology, with commercial flexographic printing systems to improve the resolution and registration by a factor of 10—to approximately 3 microns, or better. These systems are being investigated for their potential to print metallic interconnects in large-area circuits and antennas.
- *High-speed ink-jet printing* in manufacturing systems uses piezoelectric or thermal print heads for high-speed, large-area patterning—up to 100 square meters per hour. These printers involve hundreds of active nozzles, each operating independently, at frequencies of up to tens of kilohertz. Recent work focuses on applications in the manufacturing of display systems and

[4]Proceedings of the IEEE. 2005. Special issue on Flexible Electronics Technology. Vol. 93.

[5]A.V. Kumar and A. Dutta. 2003. Investigation of an electrophotography based rapid prototyping technology. Rapid Prototyping Journal 9:95-103.

[6]See http://www-me.mit.edu/people/research/sachs.htm. Accessed April 2006.

[7]See http://www.shimadzu-biotech.net/pages/news/1/press_releases/2004_07_23_chip.php. Accessed April 2006.

certain components of packages for microelectronics. Large-area, high-resolution displays that use organic light-emitting diodes or circuits patterned by ink jet are possible. Sophisticated control devices enable excellent repeatability in the printing. Machine vision provides the ability to perform registration in real time during printing. Experimental printers are capable of printing droplets with diameters of 5 microns or less, with registration at even finer scales, particularly when patterns of wetting and nonwetting regions on the substrate are used to confine the printed droplets. The range of inks that can be printed is broad.

- *Screen printing* uses a squeegee-type blade to push viscous inks through patterned openings in a screen mesh. Existing applications include the low-resolution patterning of decals, signs, and textiles. Screen printing is also commonly used to define some features on printed circuit boards. Recent developments indicate that improved printers and screens can achieve resolution near 10 to 20 μm with good registration.
- *Laser-induced thermal transfer printing* uses a focused laser beam to selectively transfer layers of solid-material "inks" from a "donor" sheet to a target substrate. The basic printing mechanism is similar to that of a conventional thermal transfer printer. The use of lasers in place of resistive heaters, however, can improve the resolution significantly, to levels that are comparable to the spot size of the laser, near 2 μm. The overlay registration is as good as the resolution. Large areas and high patterning speeds are possible with rigid and flexible substrates. Inks range from electroluminescent organics, to metals, to colored and black dyes, to semiconducting polymers, to carbon nanotube composites, to biological tissues. The most well developed potential applications of this printing technique are for the production of organic light-emitting display devices, and color filters for liquid-crystal displays. In the latter case, the printed material consists of stacks of charge transport and emissive layers. In the former, dye-doped polymers are used.
- *Ink-jet printers* can print a wide range of materials in addition to those commonly used for printing images. The "inks" include liquid suspensions of nanomaterials, such as carbon nanotubes and buckyballs, colloidal particles, nanoparticles, and nanowires—metals and semiconductors, with magnetic and dielectric properties. Biomaterials, including deoxyribonucleic acid, or DNA, have also been printed. Active materials—semiconducting or light-emitting materials—as well as passive dielectric and photocurable polymers are also printable. Many of these unconventional inks might be used to simulate features, such as optically variable images, that appear on currency. Ink-jet technology can also be used to pattern classes of materials that are themselves not directly printable. In these cases, printed polymers or waxes may be used as sacrificial masking layers for patterning other materials. After use, these layers can be removed. In this way, both positive and negative patterns can be produced by ink-jet techniques.

Improvised Counterfeiting Devices

Probably the most significant change in digital imaging trends in the past decade is the increasing availability of sophisticated software toolsets and modular hardware. While clever hobbyists have always been able to use innovative methods to produce counterfeits, it is important to remember that the dedicated counterfeiter may also be a skilled technologist. Improvised printed devices, made from parts available from various printer vendors, may enable smart operators to build hybrid devices for improved counterfeit image quality.

No hardware or software is immune to tampering by smart users, and some users will always be able to evade the software countermeasures intended to prevent counterfeiting by either writing their own code or detecting the applicable subroutines. Enterprising counterfeiters may be able to produce or appropriate their own toner materials or inks and thus may be able to further improve existing printing technology.

Modern currency is produced using three different printing processes—intaglio, offset, and letterpress—and special substrates that include watermarks and inserted identification strips. A growing

question is whether modern digital reproduction and its developments over the next few years can simulate all features found in currency that is authentically produced.

The use of anticounterfeiting techniques to protect FRNs is by its nature primarily a defensive approach. Advancing imaging and printing technology may be making better weapons available to potential counterfeiters faster than authentic currency is gaining deterrents; thus, the judicious exploration of the ways that a counterfeiter might exploit weaknesses in the currency system using available and improving equipment is an important part of any comprehensive defensive plan.

CONCLUSIONS

A range of excellent, reliable, and cost-effective digital printers for consumer use are available today at very affordable prices. Innovation and skilled engineering have resulted in this progress, and while innovation will continue, some physical limits may dominate the possible improvements in image quality.

Image-capture, processing, and reproduction technologies, both current and predicted, pose a significant threat to the security of Federal Reserve notes—particularly because the security of FRNs depends on the casual viewing of two-dimensional printed features in reflected light. Emerging technologies are targeted at dramatic improvements in desktop capabilities. These improvements will continue to limit the ability of any two-dimensional printed image to deter widespread counterfeiting successfully. The committee concludes that images involving other classes of features—images viewed in transmitted light, light-reflecting features, or other complex optical features—offer a substantial challenge to primitive and hobbyist counterfeiters and a costly barrier to petty and professional criminal counterfeiters.

An obvious consideration for the future is the goal of incorporating in image-processing software the ability to disable the processing of image patterns that are unique to currency in all digital tools. Because digital printing devices depend on software, the potential to disable the devices from reproducing these identified patterns is also a pertinent issue. Whereas simple copy protection may deter an opportunistic counterfeiter, the growing availability of online “hacks” means that a criminal with intent will not be deterred. A more sophisticated approach would be to add features to banknotes that intentionally frustrate image-capture capabilities or that generate unwanted patterns when scanned and processed images are printed. Some successful features on currency today are optical features that cannot be directly captured by present-day input scanners but can be seen by the human eye.

3

A Systems Approach to the Counterfeiting Threat

To assist in understanding current counterfeiting trends and to help assess the potential effectiveness of various countermeasures, the system of distribution and use of U.S. banknotes bears examination. Such an overview can reveal approaches or combinations of approaches that may be more effective than focusing only on one step in the process. For example, much attention may be given to preventing the production of a counterfeit note, but somewhat less attention may be paid to preventing its casual circulation.

While U.S. dollars are recognized worldwide as legal tender, their distribution and use vary in some interesting ways. Currently, approximately $720 billion in U.S. banknotes are in worldwide circulation. This amount is increasing by about 6.5 percent per year.[1] The rate of counterfeiting of U.S. banknotes is estimated to be 5 counterfeits per million notes circulating in 2002. As expected, however, more $100 notes than $1 notes are counterfeited; the number of $100 notes is higher than the average, and is estimated at 30 counterfeits per million.[2]

COUNTERFEITING AT HOME AND ABROAD

Approximately two-thirds of the value of U.S. currency in circulation and 70 percent of all $100 notes in circulation are estimated to reside overseas, in both dollarized and nondollarized countries.[3] In many foreign countries, U.S. currency is accepted in transactions as a global currency; it is often stockpiled against political and economic uncertainty; and it can provide a stable, anonymous liquid asset to individuals and corporations. The remaining one-third of the value of U.S. currency is held domestically.[4] In contrast to foreign holdings of U.S. currency, domestically held currency primarily circulates; relatively little is held long term.

Counterfeits are discovered in two main ways: (1) The counterfeiters are found through law enforcement procedures and their products are seized, usually in large quantities. (2) Merchants or banks discover counterfeit notes after they have been passed into circulation.

Forensic science can identify common features among discovered notes that can be traced to unique characteristics of the counterfeiting process. These distinctions can allow the counterfeits to be classified

[1]E. Foster, Federal Reserve Board. 2005. Presentation to this committee, May 24.

[2]J. Haslop, De La Rue. 2005. Presentation to this committee, July 21.

[3]E. Foster. See note 1 above. Dollarized economies are those that have adopted the U.S. dollar as their official national currency.

[4]L. DiNunzio and L. Clarke. 2004. The new color of money: safer, smarter, more secure. Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques V, R.L. van Renesse (ed.), Vol. 5310, pp. 425-439.

TABLE 3-1 U.S. Banknote Counterfeiting in Fiscal Year 2005: Production Technology, Class of Counterfeiter, and Amount (in U.S. dollars)

Primary Production Technology	Primary Criminal Class	Domestic Passed ($)	Domestic Seized ($)	Foreign Passed ($)	Foreign Seized ($)
Ink-jet printing	Hobbyist, petty criminal	29,153,845	5,940,531	29,984	642,841
Electrophotography	Hobbyist, petty criminal	2,164,475	758,045	8,690	9,920
Offset press (domestic)	Professional	2,264,582	1,608,682	72,593	7,186,140
Offset press (foreign)	Professional	21,244,276	1,290,340	746,910	11,971,514
Intaglio press (foreign)	State-sponsored	1,401,300	5,083,200	3,939,200	531,200
TOTAL		56,228,478	14,680,798	4,797,377	20,341,615

SOURCE: Data provided to this committee by the U.S. Secret Service.

according to their sources. Table 3-1 presents a snapshot of the magnitude of U.S. banknote counterfeiting for fiscal year 2005; these numbers are typical of the counterfeiting threat in recent years. The counterfeits are classified by the U.S. Secret Service according to their source, either domestic or foreign, and according to whether they were discovered before or after they were passed into circulation. These data provide some insights into the patterns and practices of counterfeiters.

Given the distribution of notes, it is not surprising that the most-counterfeited note abroad is the $100 note. Because foreign cash handlers generally screen U.S. banknotes more carefully than do U.S. cash handlers, the annual dollar value of passed counterfeit notes reported abroad is constant and small. It is estimated at less than $5 million, although this number is not reliably measured.[5] The high scrutiny paid abroad to U.S. notes means that foreign counterfeiters must invest more resources to produce a reasonably high quality product. Typically this necessitates traditional methods such as offset or intaglio printing, high-quality paper, and reasonable simulations of security features—and large operations.

The U.S. anticounterfeiting strategy overseas, therefore, focuses on enforcement with good success. Seizures of counterfeit banknotes in foreign countries decreased from $350 million in 1995 to $20 million in 2005 as the U.S. Secret Service succeeded in shutting down large counterfeiting operations, particularly in Colombia (reportedly the source of 40 percent of counterfeit U.S. currency) and as diplomatic efforts curtailed operations in Bulgaria.[6] Other large producers of counterfeit U.S. currency include Mexico, Nigeria, and North Korea.

As compared with foreign counterfeiting of U.S. banknotes, domestic counterfeiting is considerably more opportunistic, is generally smaller in scale, and focuses on smaller bill denominations. In the United States, the $20 note is the most widely used note, primarily because it is most commonly distributed through automated teller machines, or ATMs. It is also the most counterfeited note domestically. Note that, according to data in Table 3-1, in foreign countries counterfeit seizures outstrip passed notes by a factor of four. However, the reverse is true in the United States. Domestic counterfeits tend not to be stockpiled, and in the United States, passed notes exceed seized notes by a factor of four.

Counterfeiting technology follows digital reproduction technology trends. In 1995, for example, less than 1 percent of counterfeit notes detected in the United States were digitally produced. By 2005, that number had grown to nearly 35 percent worldwide and 54 percent within the United States, according to

[5]L. Felix, Bureau of Engraving and Printing. 2005. Presentation to this committee, May 24.
[6]L. Felix. See note 5 above.

data in Table 3-1 (ink-jet printing and electrophotography).[7] Currently, ink jet is the primary technology that can easily and cheaply simulate the look of a current Federal Reserve note (FRN). The widespread availability of a variety of ink-jet printers means that notes may be printed in widely dispersed locations on a very irregular schedule and may be almost impossible to track.

The total dollar value of domestically passed notes is around $40 million to $50 million annually and is approximately constant over time.[8] Because Federal Reserve machine readers capture all counterfeits that pass through Federal Reserve banks at the end of the currency's life, this number is a good lower bound of the counterfeiting activity in the United States. However, the estimate does not include counterfeit notes that are withdrawn from circulation by a recipient who neither reports it nor passes it on to others.

THE IMPACT OF COUNTERFEITING

Counterfeiting can have a number of impacts on individuals, companies, financial institutions, and the nation that issues the currency. The most obvious impact may be perceived to be economic. However, the total value of counterfeit notes passed (about $61 million in 2005) is less than 0.01 percent of the value of currency in circulation and an even smaller portion of the total U.S. economy.[9] Counterfeiting of banknotes is very small compared, for instance, with counterfeiting of credit cards or of branded goods. The counterfeited-products business engenders huge losses, ranging to 5 to 8 percent of worldwide sales of brand products, and credit card fraud accounted for more than $750 million in losses in the United States in 2004.[10]

Good design and strong enforcement policies have enabled U.S. currency to achieve one of the lowest rates of counterfeiting of any major currency—only five notes per million—despite its worldwide circulation. In contrast, the euro is estimated to be counterfeited at 65 notes per million, the British pound at 160 notes per million, and the Canadian dollar at 1,000 notes per million.[11]

Counterfeiting may also have psychological effects. Governments (and their enemies) have long realized that counterfeiting is a national security issue. For instance, in an attempt to destabilize the Continental government, the British government counterfeited U.S. currency during the American Revolution;[12] likewise, the Union sent counterfeit Confederate dollars south during the Civil War,[13] and during World War II, the German government manufactured a high-quality counterfeit of the British 5-pound note (termed the White Fiver).[14]

The psychological impact created by counterfeiting can be measured in economic terms, however. As in most economic markets, the consumer response to a threat is not proportional to the threat itself: stock market crashes are the archetypical example. An illustration of the psychological impact of counterfeiting is provided by the Bank of Canada, which reports that when counterfeit Canadian $100 notes reached a level of 300 notes per million, as many as 11 percent of merchants stopped accepting $100 notes.[15] Thus, U.S. anticounterfeiting strategies are intended to maintain consumer confidence in U.S. currency, just as terrorist-sponsored counterfeiting is intended to undermine it.

---

[7]L. Pagano, U.S. Secret Service. 2005. Presentation to this committee, May 24.

[8]L. Felix, Bureau of Engraving and Printing. 2005. Presentation to this committee, May 24.

[9]U.S. Department of the Treasury. 2003. The Use and Counterfeiting of United States Currency Abroad, Part 2. The second report to the Congress by the Secretary of the Treasury, in consultation with the Advanced Counterfeit Deterrence Steering Committee, pursuant to Section 807 of Public Law 104-132. Available at http://www.federalreserve.gov/boarddocs/rptcongress/counterfeit2003.pdf. Accessed April 2006. Note that the percentages of counterfeits will vary if reported as the percentage of banknotes or the percentage of monetary value.

[10]Credit card fraud in the U.S. 2005. The Nilson Report, Vol. 830, p. 8.

[11]J. Haslop, De La Rue. 2005. Presentation to this committee, July 21.

[12]See, for example, http://www.secretservice.gov. Accessed March 2006.

[13]G. Tremmel. 2003. Counterfeit Currency of the Confederate States of America. Jefferson, N.C.: McFarland.

[14]Bank of England Fact Sheet. 2003. Available at http://www.bankofengland.co.uk/banknotes/factnote.pdf. Accessed March 2006.

[15]J.F. Chant. 2004. Bank of Canada Review. Ottawa, Ontario: Bank of Canada. P. 43.

TABLE 3-2 Some Classes of Counterfeiters, Their Methods and Technologies, and Deterrent Features on U.S. Banknotes

Criminal Class	Methods	Technologies	Deterrent Features on U.S. Banknotes
Primitive	Uses manual artistry and crafting supplies	Skilled artistry, bleaching	Fine lines and microprinting, security strip
Hobbyist	Uses electronic devices and crafting supplies commonly found in homes, offices, and universities	Ink-jet printers, color copiers, scanners, all-in-one devices	Paper quality and watermark, special inks and printed images, fine lines and microprinting, security strip
Petty criminal	Deliberately seeks commercially available materials to augment available digital processes	Specialty inks and materials, bleaches	Fine lines and microprinting, special inks and printed images
Professional criminal	Has the means to manufacture special materials or to appropriate controlled materials	Lithographic printing, materials for sophisticated simulation of features	Machine-readable features
State-sponsored	Has full resources to duplicate all technology	Duplicate of technology used by the government	Machine-readable features

The economic impact of a loss of confidence in U.S. currency could be high. If the billions of dollars in U.S. currency currently residing overseas were suddenly "called in," there would be ramifications throughout all sectors of the U.S. economy. More subjective, but also critical, is the political advantage to issuing a global currency. The loss of U.S. prestige and influence abroad owing to a lack of confidence in the dollar is not readily measurable, but it would be nonetheless severe.

Finally, although the total economic cost of counterfeiting is low, the personal cost to someone left holding a worthless note may be high. When a counterfeit note is identified, it loses its value. Because this cost accrues to an innocent party—usually a retailer or service provider—it is in the best interest of any government to protect its citizens from this threat.

PORTRAIT OF A COUNTERFEITER

According to the former chair of the U.S. House Banking Committee, Congressman Michael Castle, "The classic movie cliché of the ink-stained master engraver painstakingly touching up his counterfeit printing plates, has now given way to amateurs."[16] This statement describes the new class of counterfeiters that has emerged in step with the evolution of modern information technology tools.

Counterfeiters can be characterized in five groups of criminal types. Each criminal group represents a different threat based on the technology available to them, and different features of FRNs address these different threats. Each of the features on current U.S. banknotes has been simulated or duplicated by members of these various groups.

The five types of counterfeiters can be characterized by the technologies and the methods they use, as indicated in Table 3-2, or by the characteristics of their activities as described in Table 3-3. The two tables together provide a reasonably complete indication of the activities and capabilities of each type. Table 3-4 expands on counterfeiters' methods for passing notes.

The relative threats associated with each criminal type are shown in Figure 3-1. These data indicate that the vast majority of counterfeit FRNs are created by hobbyists and petty criminals. Moreover, these

[16]M.N. Castle. 1998. Opening statement for a hearing on using personal computers to counterfeit U.S. currency. U.S. House of Representatives Committee on Banking and Financial Services, Subcommittee on Domestic and International Monetary Policy. Available at http://financialservices.house.gov/banking/33198cas.htm. Accessed March 2006.

TABLE 3-3 Classes of Banknote Counterfeiters, Their Tools, Location, and Impact

Class	Typical Practitioner	Primary Tools	Location	Impact of Activity
Primitive	Unusually motivated individual	Manual artistry	Domestic or foreign	Very low
Hobbyist	Opportunistic young adult, typically works alone	Home office equipment	Domestic	Created largest increase in $20 domestic passed currency (together with petty criminals)
Petty criminal	All ages, criminal intent, typically works alone	Home office equipment plus specialty materials and processes	Domestic	
Professional criminal	Criminal, trained in printing technology, often part of a criminal group	Offset printing, high-end ink-jet printers, specialty materials and processes	Domestic or foreign	Low, stable level of activity
State-sponsored	Professional, profiteer or terrorist, member of a large organization	All materials and processes, including specialty paper, intaglio and offset printing, security features	Foreign	Strategic concern

TABLE 3-4 Methods and Extent of Dissemination of Counterfeit Banknotes, by Class of Counterfeiter

Class	Production Level	Stockpiling	How Notes Are Passed
Primitive	Very small	None	Individually, by counterfeiter
Hobbyist	Small, as needed	None	Individually, by counterfeiter or friends
Petty criminal	Small to moderate, often over years	None to moderate	Individually, by counterfeiter or criminal associates
Professional criminal	Large	Large	Through criminal networks
State-sponsored	Large	Unknown, presumably large	Through various legitimate and illegitimate networks, often by unwitting accomplices

TABLE 3-5 Digital Technology Access, by Class of Counterfeiter

Class	Ink-Jet Printer	All-in-One Device	Color Copier	Flatbed Ink-Jet Printer	Digital Press	High-Quality Scanner	Imaging Software
Primitive	Not applicable—does not use digital technology						
Hobbyist	++++	++++	++	—	—	—	+++
Petty criminal	++++	++++	++++	+	+	++++	++++
Professional criminal	++++	++++	++++	+++	++++	++++	++++
State-sponsored	Not applicable—reproduces government processes directly						

NOTE: Within all counterfeiter classes, additional nondigital techniques may be used to improve note simulations (e.g., craft supplies to reproduce features that use color-shifting ink). ++++, high likelihood of access; +++, good likelihood of access; ++, some likelihood of access; +, low likelihood of access; —, does not use this technology.

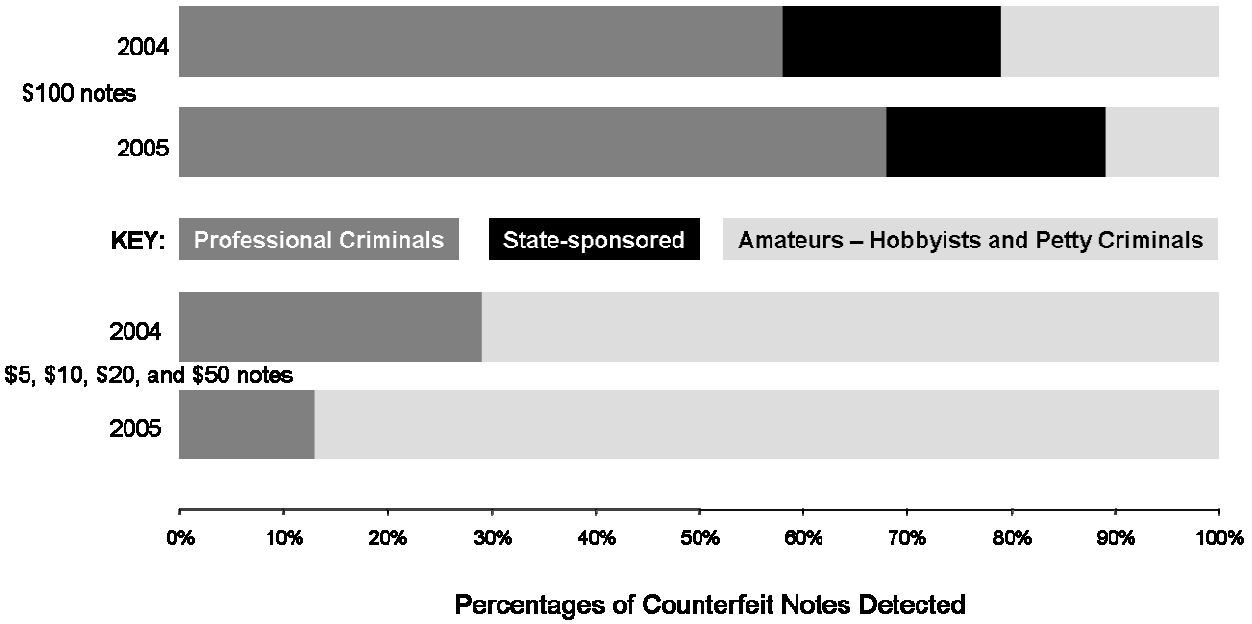

FIGURE 3-1 Comparison of the percentages of counterfeit notes detected in 2004 and 2005. The top two bars represent the percentage of $100 counterfeits by source and show the primary source to be professional criminals. The lower two bars represent percentages by source for the sum of $5, $10, $20, and $50 counterfeits, showing the growing dominance of amateurs (the light grey segments). Note that state-sponsored counterfeits are identified only for $100 notes (the black segments) and that primitive counterfeiters do not account for enough counterfeits to appear on this chart. SOURCE: Data provided to the committee by the U.S. Secret Service.

are precisely the types of counterfeiters most likely to benefit from the new digital scanning, image-processing, and printing technologies. Table 3-5 shows access to various kinds of digital technology by type of counterfeiter.

Following is a more detailed portrait of each of the five types of counterfeiter. These descriptions serve as a prelude to developing a systems view of counterfeiting that will permit associating trends in digital imaging technology with the enhanced capabilities that each type of counterfeiter could employ in the future to reproduce specific features of FRNs.

Primitive

The primitive perpetrator of counterfeiting may use manual artistry to modify a piece of currency in order to increase its value and obtain financial gain. These phony notes are easily detected by attentive cash handlers and when examined by the general public. An example is a note that has cut-and-pasted numbers increasing the denomination of a $10 bill to $100.

The primitive counterfeiter's products are often obvious to the point of parody. They are clearly incompatible with automatic currency authentication equipment and must be passed person-to-person. If the substrate is an existing FRN, it retains the correct feel and may have advanced security features such as a watermark and a security strip, albeit for the wrong denomination.

Such a note may be passed in a number of ways, however. For example, the counterfeiter may try to distract the cashier to prevent scrutiny of the counterfeit. He or she may also rely on the reluctance of a cashier to question the authenticity of a banknote in a point-of-sale situation.

Hobbyist

Over the past decade, desktop publishing has become the dominant tool for counterfeit printing operations in the United States. In fiscal year 2001, an impressive 93 percent of suppressed counterfeiting operations used digital processes; this is a phenomenal increase, from fewer than 20 percent in 1995.[17] This trend, begun in the United States, has continued worldwide. Digital publishing tools, powered by information available on the Internet, are the engines that propel hobbyist counterfeiters.

Hobbyists are typically young adults with a median age of perhaps 18 years. They work as individuals, making only a few notes at a time and printing them "on-demand" from their residence or place of employment. They typically pass these notes personally or via friends in retail transactions. Their counterfeits span a wide range in quality, from a single-sided bill[18] to impressive duplications requiring many hours of refinement in touching up colors, aligning front and back images, and refining enhancements to the printed image to simulate advanced security features using arts and crafts supplies. The $20 note is the common target of this class of counterfeiter because it is the expected note in many transactions.

As is true for primitive counterfeits, the vast majority of these products made by hobbyists are detected at or near the point-of-sale. They rarely are passed more than once and generally are not discovered by a Federal Reserve Bank; rather, 80 percent of these counterfeits are turned over to the U.S. Secret Service by commercial establishments, financial institutions, and law enforcement.[19]

The hobbyist's tools are those typically found in a college dormitory room or home office and include color copiers, scanners, and ink-jet printers. Increasingly, hobbyist counterfeiters are also using all-in-one scanner-and-printer combination devices. The devices may be controlled by a computer with image-processing software to modify the image and connect to the Internet. Instead of learning from master engravers and offset print operators, the hobbyist uses Internet searches to obtain know-how and may tell no one else or share it with a few friends. The designation of "hobbyist" implies that this counterfeiter uses only equipment that is commercially available and that has been obtained for more legitimate uses.

A hobbyist's youthful age and exploratory approach often lead to situations with unexpected consequences. For these reasons, advertisement of the U.S. Secret Service's impressive conviction rate—better than 90 percent—for counterfeiters could significantly reduce the hobbyist's temptation to "make a little money."[20]

Petty Criminal

The counterfeiter in the petty criminal class has a clear criminal intent. These practitioners use the same digital tools as the hobbyist and may supplement their efforts with specific materials such as the best paper and inks. Using the Internet, they develop and share a set of tricks to improve their simulations and to help them pass their phony bills. This includes methods to bypass or negate certain authentication methods, such as the "iodine" starch-detecting pen, as well as to handle the encounter when their creation is questioned. This type of operation is still an individual or small effort, but it differs from the activities of the hobbyist in duration, quantity, or distribution area. Some of the best counterfeits in this class

[17]U.S. Department of the Treasury. 2003. The Use and Counterfeiting of United States Currency Abroad, Part 2. The second report to the Congress by the Secretary of the Treasury, in consultation with the Advanced Counterfeit Deterrence Steering Committee, pursuant to Section 807 of Public Law 104-132. P. 60. Available at http://www.federalreserve.gov/boarddocs/rptcongress/counterfeit2003.pdf. Accessed April 2006.

[18]How Counterfeiting Works, available at http://www.howstuffworks.com. Accessed March 2006.

[19]The Use and Counterfeiting of United States Currency Abroad. 2000. Report to the Congress by the Secretary of the Treasury, in consultation with the Advanced Counterfeit Deterrence Steering Committee, pursuant to Section 807 of PL 104-132.

[20]L. Pagano, U.S. Secret Service. 2005. Presentation to this committee, May 24.

display innovative ways to simulate the security strip, the watermark, and the specialty inks. This class of counterfeiters will likely be the first to challenge the automatic currency authenticators.

As detailed in Table 3-1, it is estimated that the petty criminal and hobbyist together were responsible for 56 percent of the counterfeit notes passed in the United States in 2005.

Professional Counterfeiter

The professional counterfeiter class generates phony bills that are easy to pass to the public. These counterfeiters simulate all of the critical features of genuine notes to some degree; in fact, the simulations often require additional criminal activity in order to acquire controlled materials such as security inks and paper. These counterfeiters are typically part of a larger criminal organization that can include dedicated specialists who sometimes have professional training in the printing business. Their efforts involve generating significant quantities of counterfeits, along with developing the necessary distribution methods—which may also be tied to other criminal endeavors, such as counterfeiting identification cards or other security documents. This type of distribution far surpasses that of the petty criminal.

The U.S. Secret Service actively pursues these criminal organizations, tracking their activity by classifying recovered counterfeits into groups. Each note received by the U.S. Secret Service is characterized, classified with the telltale information that reveals the source, and put into a database. In this way, law enforcement and commercial banking organizations around the world can assist in counterfeit identification.

Much professional counterfeiting activity is located outside the United States, although a substantial fraction of the counterfeit notes may be passed domestically. The target denominations of professionals include the $20, $50, and $100 notes, with the $100 note being the most counterfeited overseas. Judging by the typical amount of currency seized when the government shuts down professional operations, this class of counterfeiters can pose a serious threat. However, continuous enforcement efforts by the U.S. government, often working with foreign governments to change and enforce laws, as well as attention to foreign currency-handling procedures and the introduction of the new currency designs, has kept this potentially significant source of counterfeiters at a low level.

State-Sponsored Counterfeiter

State-sponsored counterfeiters not only plan criminal financial gain but may also have a political goal to reduce confidence in U.S. currency. Thus, they are willing to invest in technologies to duplicate U.S. banknote features exactly. State-sponsored counterfeits may be passed by both legitimate and criminal means. The very-high-quality Supernotes, which duplicate nearly all security features in U.S. $50 and $100 banknotes, are created by this class of counterfeiter and passed by unwitting travelers as well as by terrorist organizations.

Some state-sponsored organizations make their own paper with watermarks and colored threads, make their own specialty inks, and re-author the engraved image. They use the same printing methods—intaglio and letterpress—and may integrate their own forensic features that would enable their own internal discrimination. While these notes would fool most cash handlers and even some machine authenticators, they can still be identified by the Federal Reserve Bank and the U.S. Secret Service. The

U.S. government has recently confirmed earlier suspicions that Supernotes are a state-sponsored activity of North Korea.[21] It has been reported in the media that more than $45 million is estimated to have been passed by this source since 1989.[22]

A SYSTEMS MODEL FOR COUNTERFEITING

Counterfeiting begins—but does not end—with the printing of bogus banknotes. After producing (and possibly stockpiling) notes of a sufficient quality and quantity, the counterfeiter still has work to do. To realize a profit from these efforts, he or she must then exchange the counterfeit notes for cash, goods, or services. After a counterfeit note has been passed, it will circulate until it is detected and removed from the system. Then, and only then, is the economic loss of counterfeiting realized: the last one holding the fake banknote loses.

As shown in Figure 3-2, the counterfeiting threat can be described as a system composed of four components. Counterfeit notes flow down the system (1) from production, (2) through stockpiling (3) to the passing of counterfeits, and (4) into circulation, as indicated by the arrows. At each stage, disruptions to the system can be introduced by removing counterfeit notes or by deterring their production; thus, counterfeits may also flow from the components (boxes) to the removal processes (ovals). Note that some counterfeits may spend little or no time in a stockpile, and that a stockpile may sometimes be as simple as a criminal's pocket.

In order to best analyze this system, flows for each class of counterfeiter—in numbers of notes per year, or fractions per denomination—should be measured for each arrow in Figure 3-2. While certain rates are known, such as the rate of seizures, many of the other rates remain unknowable. Without quantification, there is no definitive way to understand (or run experiments to explicate) the effectiveness of any particular feature or combination of features.

Such measurements are complicated by the variation in quality of counterfeits, which means that the percentage of fakes successfully passed, for example, will vary with their quality. While it may be easy to spot some fakes, other, very good counterfeits may take a high level of scrutiny. A common outcome for such scrutiny is to increase the number of false positives, meaning that some genuine notes may be identified as fakes. Therefore, an effective analysis of ways to disrupt a counterfeiting system may include the mathematical probabilities but would also incorporate an assessment of the real-world variables that matter.[23]

Using such a strategic analysis would allow a comprehensive examination of methods for combating counterfeiting. Even without knowing the actual flows, it would be possible to make some allocation decisions if one could estimate, at each stage of the system, the likelihood of detecting a counterfeit bill as a function of the resources expended for detection at that stage. This structure calls for the consideration of ways to deter or prevent production, to empty counterfeit stockpiles, to disrupt the passing of counterfeits, and to remove counterfeits from circulation. A valuable outcome of combining experience with modeling could be a method to allocate funds to detection activities at the different stages to maximize the number of counterfeit bills detected.

[21]See http://www.state.gov/p/inl/rls/nrcrpt/2006/vol2/html/62144.htm, http://www.usdoj.gov/usao/dc/Press_Releases/2005_Archives/Oct_2005/05370.html, and http://www.usdoj.gov/criminal/press_room/speeches/2005_4193_rmrksOprSmokngDrgnNroylChrm082405O.pdf. Accessed March 2006.

[22]B. Gertz. 2005. N. Korea charged in counterfeiting of U.S. currency. Washington Times. December 2. Available at http://www.washtimes.com/world/20051201-103509-5867r.htm. Accessed March 2006.

[23]G.G. Brown, W.M. Carlyle, J. Royset, and R.K. Wood. 2005. On the complexity of delaying an adversary's project. The Next Wave in Computing, Optimization, and Decision Technologies, B.L. Golden, S. Raghavan, and E.A. Wasil (eds.). New York: Springer. Pp. 4-17.

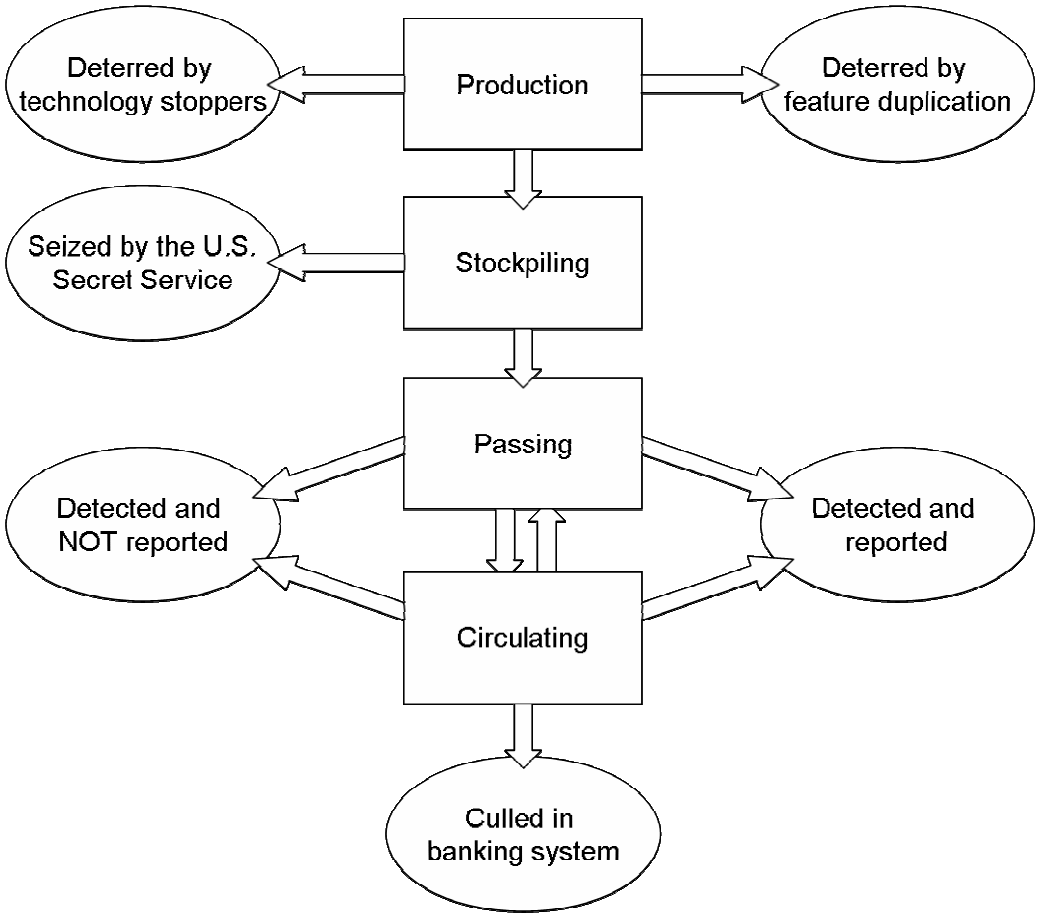

FIGURE 3-2 A systems model for counterfeiting. The boxes indicate the components of the counterfeiting system. The ovals represent processes by which counterfeit notes are removed from the system. Arrows indicate the flow of counterfeit notes.

Banknotes themselves can also be analyzed with this system. They contain a number of overt features, or those that can be verified using normal sight and touch. They also contain a variety of machine-readable features that can be verified through the use of an auxiliary device, such as a black light. How all of these features interact to deter production and disrupt circulation is an important part of the systems approach.

Deterring or Preventing Production

The challenge for counterfeiters is to make a simulation that in their judgment can be passed successfully. The Bureau of Engraving and Printing (BEP) counters this threat by integrating security features into U.S. currency to increase the level of effort necessary to achieve a quality simulation. The BEP's goal is to anticipate threats to the security of U.S. currency and to preempt or counter these threats.

To this end, the BEP participates in the following efforts as part of a comprehensive program to combat the counterfeiting threat:

- The commissioning of various types of studies of currency features and threats, such as studies involving focus groups,[24] and those carried out by the National Research Council;
- Its participation, through the Central Bank Counterfeit Deterrence Group and the Central Bank Cash Machine Group, in international counterfeit-deterrence group activities;
- The design and implementation of new currency features to counteract perceived threats;[25]
- The testing of features and counterfeiting technology in-house and with the U.S. Secret Service and also with external groups organized to test the quality of new features;[26]
- Working with equipment manufacturers and their organizations to develop use limitations on devices that are likely to be used for counterfeiting;[27]
- The support of academic modeling efforts and red teaming;[28]
- The development of secure material supply agreements;
- Working with the U.S. Secret Service on early detection leading to seized counterfeits;
- The development and implementation of educational programs to promote awareness of banknote features; and
- The providing of test notes to assist companies in designing reliable machine authentication technologies.

The first opportunity to combat counterfeiting occurs by deterring note production. An array of new, digital tools is being used by counterfeiters in their attempts to simulate banknotes. The low cost and accessibility of these technologies make them available to far more potential counterfeiters than in the past. These new tools continue to challenge the currency designs, especially image-based features.

One deterrence strategy is to prevent production directly, by limiting the availability, the capabilities, and the use of counterfeiting technology. In fact, this was the first anticounterfeiting strategy implemented by the U.S. government in the 1860s. The distinctive look and feel of intaglio printing could be achieved only by printing processes that were of very limited availability. The usefulness of digital imaging tools can be limited both by technology in the printers and by limiting access to them. By international agreement, commercial color printers prevent the printing of banknotes by recognizing certain features of various major currencies and refusing to process the image further. Similar technology is implemented in digital image-processing software and in some digital scanners. Although these limitations undoubtedly deter casual counterfeiting, they are not proof against a determined hacker. Thus, technology "blocks," even when well implemented, are not a panacea, and if they are poorly implemented they could have serious consequences for the operability of the equipment.

A second way to deter counterfeit production is by incorporating features in the note design that are necessary to create a convincing counterfeit and are also difficult to simulate. Current U.S. currency combines numerous features that present varying levels of challenge to the counterfeiters. Although highly qualitative, Table 3-6 provides some insight for optimizing the use of the limited space on the note and avoiding a saturation of features. The analysis presented in Table 3-6 is based on a logical analysis of

[24]L. Setlakwe and L. DiNunzio. 2004. Comparative analysis of public opinion research in the U.S. and Canada. Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques V, R.L. van Renesse (ed.), Vol. 5310, pp. 13-24.

[25]More information is available at http://www.newmoney.com. Accessed March 2006.

[26]The Reprographic Research Center is a state-of-the-art facility for the testing of banknote designs and counterfeit-deterrent features. Central banks provide funding and set policies for its operation, while banknote printers and law enforcement personnel use the facility for adversarial testing.

[27]S.E. Church, R.H. Fuller, A.B. Jaffe, and L.W. Pagano. 2000. Counterfeit deterrence and digital imaging technology. Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques III, R.L. van Renesse and W.A. Vliegenthart (eds.), Vol. 3973, pp. 37-46.

[28]A red team is a group of independent reviewers organized to provide an objective assessment.

TABLE 3-6 Usefulness of Overt and Machine-Readable Security Features in Deterring Counterfeiting, Evaluated by Class of Counterfeiter

Features	Primitive	Hobbyist	Petty Criminal	Professional Criminal	State-Sponsored
Overt					
Substrate	++++	++++	+++	+	—
Tactility (or feel)	++++	+++	+++	++	—
Watermark	++++	++++	+++	+	+
Plastic strip	++++	+++	+++	++	—
Intaglio printing	++++	++++	+++	+	—
Offset color blending	++	++	+	—	—
Optically variable ink	++++	+++	+++	+	—
Intaglio microprinting	++++	++	+	—	—
Offset microprinting	++++	++	+	—	—
Colored threads	++++	++	+	—	—
Machine-readable					
Paper fluorescence	++++	+++	++	—	—
Magnetic ink	++++	++++	+++	++	—
Magnetic ink pattern	++++	++++	++++	+	—
Color-shifting inks	++++	++++	++++	++	—
Digital CDS	++++	+	—	—	—
Digital BDS	—	—	—	—	—
Fluorescent thread	++++	++++	+++	++	+

NOTE: Overt features can be verified using normal sight and touch. Machine-readable features are those that can be verified through the use of an auxiliary device. CDS, counterfeit deterrence system; BDS, banknote detection system. Symbols indicate the following: ++++, high deterrence value; +++, good deterrence value; ++, some deterrence value; +, low deterrence value; —, does not use this technology.

threats posed by different classes of counterfeiters, the impact of the technologies used by each class of counterfeiter, and the impact of technology on features of FRNs.

While many currency features are difficult for low-level counterfeiters to simulate, there has still been substantial growth in the hobbyist class of counterfeiting in the United States. Clearly, feature-based deterrence is only part of the equation; preventing passing and circulation of obvious counterfeits, as discussed below, is required to make the hobbyist's illegal endeavors unprofitable. Of course, large counterfeiting organizations, particularly state-sponsored counterfeiters for whom profit may be secondary, are minimally deterred by banknote features. Other deterrence methods, including law enforcement and political pressure, are required in these cases.

Emptying the Stockpile

There is no opportunity for counterfeit notes seized from a stockpile to cause harm, so seizing stockpiled counterfeit notes is an effective way to disrupt the counterfeiting system. A stockpile can be

any storage location prior to the passing of the counterfeit; it could be a warehouse, a suitcase, or the pocket of a criminal.

The possession of counterfeit currency is a crime investigated by the U.S. Secret Service. Founded in 1865 to suppress the widespread counterfeiting of U.S. currency, the U.S. Secret Service maintains exclusive jurisdiction for investigations involving the counterfeiting of U.S. currency. To carry out its mission, the U.S. Secret Service works with state and local law enforcement agencies, the Department of the Treasury, and foreign law enforcement agencies to pursue counterfeiters. The committee attributes the low rate of counterfeiting of U.S. banknotes relative to other major currencies in great part to the talents and methods of the U.S. Secret Service in detection and enforcement. The decrease in foreign counterfeiting volume between 1995 and 2004 supports this claim. While there are no statistics to indicate what fraction of stockpiled counterfeits the U.S. Secret Service captures, the fact that the value of seized counterfeits (about $100 million in 2004) is vastly greater than passed counterfeits (less than $15 million annually) indicates great effectiveness in the disruption of the stockpiling of counterfeit banknotes.

The particular effectiveness of the U.S. Secret Service has been attributed to its unique role as a law enforcement unit with an express charter to counter all efforts to counterfeit U.S. currency. There is no question that the U.S. Secret Service provides a unique resource and is the cornerstone of counterfeiting enforcement efforts in the United States and abroad.

Disrupting the Passing of Counterfeits

A counterfeit note does not profit the maker until it is exchanged for other value and passed into circulation; if the note cannot be passed, there is no incentive to counterfeit. Efforts to combat counterfeiting must include strategies to disrupt the passing process. These efforts typically focus on educating the human cash handler and employing reliable machine authentication.

People who use U.S. currency are the first line of defense against counterfeiting. Because the primary opportunity to pass a counterfeit note is the first point-of-sale, the key people are those who handle currency as a part of their job. Therefore, the evident first line of defense is the public, the often inexperienced clerk at the counter or the taxicab driver, those who are the most likely points-of-sale for the criminal fraternity. In Canada, studies have shown that 78 percent of counterfeits are detected by individuals and businesses.[29] Even the high-quality Supernote was first detected not by a machine, but by an experienced cash handler who noticed an improper "feel" to the note.[30] Clearly, the most efficient way to prevent the passing of counterfeit notes is to design banknotes that can be authenticated at the point-of-sale, and the optimal overt security feature is distinguishable and inimitable for the casual handling of the banknote in the split seconds it is transferred. Specifically, the note should contain security features that are visible, usable, and known.

An effective visible feature is one that is easy to authenticate regardless of light levels and the fitness of the note, and therefore creates minimum delay at the point-of-sale. A usable feature does not require out-of-the-ordinary methods such as a magnifying glass, transmitted light, or a machine. The third factor, ensuring that a feature is known, is the most elusive. Knowledge of features does not necessarily mean that a user can name them, but it may be evidenced in an unconscious kind of habitual knowledge. The number of features and the fact that older banknote issues are not devalued can make such education a complex and layered undertaking.

As a result of the public education effort for the new $20 note, public recognition of the currency features increased to 85 percent in the United States. While the impact of feature recognition has not been quantified in the United States, similar educational efforts in Canada have dramatically decreased the acceptance of counterfeit notes by cash handlers.[31] Thus, educating cash handlers to recognize security features is undeniably an important factor in counterfeit deterrence.

[29]J.F. Chant. 2004. Bank of Canada Review. Ottawa: Bank of Canada. P. 45.
[30]S. Church, Bank of Canada. 2005. Presentation to this committee, July 21.
[31]S. Church. See note 30 above.

Education and knowledge are tremendously important for combating the passing of counterfeit notes. In 1996, the Federal Reserve System and the U.S. Department of the Treasury began a worldwide public education campaign with the objectives of, first, communicating to the general public that there will be no recall or devaluation of older FRNs, and, second, providing information that will enable the public, law enforcement personnel, central banks, depository financial institutions, and other cash handlers to authenticate the new series notes. The BEP's outreach program has included cash handlers, merchants, business and industry associations, and the media.

One of the most basic yet revolutionary methods intended to disrupt passage of counterfeits is the growth of machine authentication. This is not a new concept—in the 18th and 19th centuries, gentlemen of business carried pocket-size scales to ensure that the coins they received were of the correct weight for their value. In those days of coin shaving, it was prudent and socially acceptable to authenticate coins before accepting them. In the 21st century, the concept is being revisited by electronic currency authenticators.

Over the past 15 years, advances in low-cost sensor technology have enabled the machine-reader market to grow in size and scope, while machine readers shrink in cost and footprint. Currently, over $64 billion passes through vending-type note acceptors per year in the United States, with 10 million to 20 million daily transactions;[32] in addition, the retail and banking sectors process billions through machine counters yearly. As sensors continue to decrease in size and cost, machine readers will add authentication capabilities and will become even more pervasive, particularly in consumer cash-handling applications.

Because notes rejected by a machine reader at the point-of-sale are currently neither tallied nor removed from circulation, no comprehensive statistics are available on the impact of machine readers on the passing or attempted passing of counterfeits. However, industry representatives report that even low-end denominators detect and capture 90 percent of domestic counterfeits, with authenticators nearing 100 percent.[33] Therefore, machine readers represent a significant deterrent to the passing of counterfeits. Because rejected notes are typically returned to the consumer, this tool does not require the cash handler to deal with the consequences of accepting a counterfeit, making machine readers particularly attractive to the retail sector. Such authenticators are already in widespread use in Europe and Canada, and their offer of hassle-free security from counterfeits may be attractive to U.S. retailers as well. An increase in the use of machine authenticators could result in a commensurate decrease in the frequency of passing.

As machines replace human cashiers, they may increasingly become the first line of defense against the passing of counterfeit notes. It is therefore important to design notes for reliable machine authentication. Current machine denominators and authenticators sense a variety of features, and it is important for currency design to maintain and add features that target the requirements for both human and machine authentication. Specifically, the ideal machine-readable feature—

- Can be sensed by a point sensor moving across the note,
- Is readable from both long-side-first and short-side-first feed directions,
- Emits a strong and reliable signal,
- Is independent of orientation and face,
- Can be reliably located despite manufacturing and reading tolerances, and
- Provides series identification.

Removing Counterfeits from Circulation

Once a counterfeit note is finally identified, it should be removed from circulation. Even though repeated passing does not result in additional monetary damage, it is the final person in the chain who will feel the impact. Unfortunately, removing counterfeits from circulation is not always as straightforward as

[32]R.R. Bernardini. 2004. New security features and their impact on low-cost note readers. Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques V, R.L. van Renesse (ed.), Vol. 5310, pp. 52-62.

[33]Cummins-Allison Corporation, Mount Prospect, Ill. 2005. Discussions during a subcommittee visit, October 7.

it seems. Several factors affect the efficiency of counterfeit removal and any subsequent law enforcement investigation.

Currently, there is no incentive for public interception of a counterfeit note close to the initial distribution point. In fact, there is a disincentive to turn in a counterfeit, as the finder of a counterfeit note receives no compensation and may even be subject to uncomfortable questioning by law enforcement officers and a considerable time penalty.[34] The committee agreed that they themselves, as hypothetical holders of a counterfeit note, would rather destroy it (or keep it as a souvenir) rather than contact the authorities. Similarly, manufacturers of currency-handling equipment report that some retailers tend not to purchase dedicated counterfeit-detection modules for their machine counters in order to avoid the inconvenience of dealing with counterfeits that cash handlers accepted at the point-of-sale.[35] There is no question that such an attitude toward counterfeit identification interferes with the identification and removal of counterfeit notes, as well as with the eventual capture of the counterfeiters responsible.[36]

It may be possible to provide incentives to citizens who turn in counterfeit notes. A primary objection to such a policy is that it would provide an opportunity to counterfeiters to exchange their products for genuine currency. But more importantly, it might engender an impression in the public eye that counterfeiting is a victimless crime in which the government sustains the loss. This would result in even less incentive for citizens to identify or condemn passers of bogus notes. A system is desirable, however, that would decrease the time, trouble, and stigma of turning in a counterfeit. A culture that encourages finding and turning in counterfeits to authorities would be very valuable.

As currency circulates, particularly domestically, it is processed through the banking system, often many times before it wears out. Branch banks typically process their cash deposits through desktop currency-counting machines, which incorporate authentication technology. Nearly all branch banks also use machine counter-sorters that can sort, face, count, authenticate, stack, and band notes. Both of these classes of machines have a near-perfect identification record for counterfeit notes, so when they are used, passed counterfeits are removed from circulation when they pass through a bank. Any counterfeit notes that might escape the branch banks' systems are captured at the Federal Reserve Bank, which use a proprietary machine reader that senses a wide range of overt and machine-readable features.

CONCLUSIONS

Looking at the counterfeiting threat as a system may reveal approaches or combinations of approaches which may be more effective than that of focusing only on one step in the process. For example, much attention may be given to the preventing production of a counterfeit note, but somewhat less attention may be paid to preventing its casual circulation.

At the present time, U.S. currency has one of the lowest rates of counterfeiting of any major currency. These factors help maintain U.S. banknotes as a global currency. However, even when counterfeiting rates are low, the psychological threat can be high. For example, if the counterfeiting risk is perceived to become too large, foreign holders could divest their U.S. currency, causing widespread economic impacts as well as a loss in U.S. political prestige. It is therefore in the national interest to preserve the actual and perceived security of U.S. currency.

Counterfeiters may be classified into five categories:

- *Primitive counterfeiters*—who do not use digital technology, but create counterfeits using little more than manual artistry to modify a piece of currency in order to increase its value and obtain financial gain;

[34]A well-meaning citizen will receive negative compensation in this case, because the counterfeit must be surrendered to authorities!

[35]Cummins-Allison Corporation, Mount Prospect, Ill. 2005. Discussions during a subcommittee visit, October 7.

[36]The U.S. Secret Service estimates that up to five times as much counterfeit currency is in circulation as is recovered each year.

- *Hobbyists*—who counterfeit occasionally and use typical desktop computer equipment and available crafting supplies, sometimes in creative ways;
- *Petty criminals*—who counterfeit in a dedicated manner and actively invest in specialized computer equipment and materials;
- *Professional counterfeiters*—who focus the efforts of a large group of people on the sophisticated production and distribution of counterfeits; and
- *State-sponsored counterfeiters*—who may use the very same high-precision equipment that the government uses to manufacture notes.

Today, domestic counterfeiting—dominated by the first four classes of counterfeiters—focuses on the $20 note and is primarily a for-profit enterprise. Foreign counterfeiting—primarily primitive, professional, and state-sponsored—currently centers on the $100 note and may be engaged in to generate revenue as well as to support other illegal activities. It is possible, however, that several trends, including the following, will affect this balance:

- Lower-cost, higher-performance image-printing equipment;
- Improved global purchasing access—which could allow counterfeiters to find and purchase specialized materials or surplus printing machinery more easily; and
- Improved communication that facilitates information sharing among counterfeiters—which may include access to expertly processed image files, leads on sources for specialty raw materials, ideas for ways to simulate features, and connections to a distribution network for counterfeit products.

These trends enable a professional counterfeiter to expand operations dramatically with minimal cost; they may also allow a petty criminal to enter the realm of the professional without previous connections to the underworld. For example, wide distribution of counterfeit notes may be possible through communication within an Internet-based community.

The counterfeiting threat may be described by a systems model with four components. Counterfeit notes flow down the system from production through stockpiling to passing and circulation. Counterfeit deterrence focuses on disrupting or preventing each of these components. Thus, a comprehensive response to counterfeiting must include ways to do the following:

- Prevent or deter production, through the use of technology blockers and note features that are difficult to simulate;
- Empty counterfeit stockpiles, through law enforcement programs;
- Disrupt passing of counterfeit currency, by means of public education and machine authentication of currency; and
- Remove counterfeits from continued circulation, through the identification of counterfeit currency by individuals and by special methods within the banking system.

Banknote features are important elements of counterfeiting deterrence at each stage of this system. Because each class of counterfeiter engages in the four components differently, the impact of different deterrence efforts will vary among the counterfeiting classes; however, each effort fulfills an important role in preserving the security of U.S. currency.

Appendixes

Appendix A

Biographical Sketches of Committee Members

Robert E. Schafrik, *Chair*, is currently the general manager of the Materials and Process Engineering Department at GE Aviation. He is responsible for the development of advanced materials and processes used in GE's aeronautical turbine engines and their marine and industrial derivatives. He oversees materials application and engineering activities supporting design engineering, manufacturing, and field-support activities worldwide. He also operates a state-of-the-art in-house laboratory for advanced materials development, characterization, and failure analysis. Before joining GE in November 1997, Dr. Schafrik served in two concurrent positions within the National Research Council, which he joined in 1991: director of the National Materials Advisory Board and director of the Board on Manufacturing and Engineering Design. He also served in the U.S. Air Force. His career highlights there included research metallurgist, manufacturing technologist, materials application engineer, manager of F-16 engine programs, and headquarters manager of air superiority weapons programs. Dr. Schafrik has a Ph.D. in metallurgical engineering from Ohio State University, an M.S. in information systems from George Mason University, an M.S. in aerospace engineering from the Air Force Institute of Technology, and a B.S. in metallurgy from Case Western Reserve University.

Martin A. Crimp is a professor of chemical engineering and materials science at Michigan State University. He is an expert in the development and use of a variety of advanced characterization and imaging tools. His research applies a variety of innovative analysis tools to describe and illustrate the design, performance, and failure of advanced materials. Some examples include the creative use of scanning electron microscopy to image atomic-scale features through electron channeling contrast imaging; the use of electron energy-loss spectroscopy to study environmental and radiation effects on carbon nanotubes; and the use of advanced transmission electron microscopy techniques such as convergent-beam electron diffraction to study the growth of nanowires and nanostructures. Dr. Crimp has a Ph.D. from Case Western Reserve University and M.S. and B.S. degrees from Michigan Technological University.

Charles B. Duke is vice president and senior research fellow in the Xerox Innovation Group. Before taking this position, he was deputy director and chief scientist of the Pacific Northwest Division of the Battelle Memorial Institute and affiliate professor of physics at the University of Washington. He received his Ph.D. in physics from Princeton University in 1963 following a B.S. summa cum laude with distinction in mathematics from Duke University in 1959. Dr. Duke is a fellow and an honorary member of the American Vacuum Society, a fellow of the American Physical Society, a fellow of the Institute of Electrical and Electronics Engineers, a member of the Materials Research Society, and a life member of

Sigma Xi. In 1977, he received the Medard W. Welch Award in Vacuum Science and Technology. In 1981, Dr. Duke was named one of the Institute for Scientific Information's 1,000 internationally most cited scientists. In 1993 he was elected to the National Academy of Engineering and in 2001 to the National Academy of Sciences. He has written more than 350 papers on surface science, materials research, semiconductor physics, and the electronic structure of molecular solids; he holds several patents on the use of feedback in the design of digital imaging and printing systems; he has also written a monograph on electron tunneling in solids and has edited three books: *Surface Science: The First Thirty Years* (1994), *Color Systems Integration* (1998), and *Frontiers in Surface and Interface Science* (2002).

Alan Goldstein is a professor of biomaterials and holds the Fierer Chair of Molecular Cell Biology at Alfred University. His work focuses on structure-function studies of protein binding to materials surfaces, including both biochemical and molecular modeling approaches. Dr. Goldstein has published extensively on the topic of converging technologies in biology, nanotechnology, information technology, and cognitive sciences, and his research ranges from protein engineering to biomimetic materials to mineral phosphates. Specific projects include the biochemistry of interactions between glass fibers and the extracellular matrix; molecular mechanics and molecular dynamics modeling to simulate the adsorption to materials surfaces; and the application of electrophoretic methods to study protein adsorption layers on glass and ceramic surfaces. Dr. Goldstein holds a B.Sc. from New Mexico State University in agronomy and a Ph.D. in genetics from the University of Arizona. He received the Biotechnology Faculty Research Award in 1995 from the California State University Program for Education and Research in Biotechnology.

Elizabeth A. Holm is a distinguished member of the technical staff in the Materials and Process Modeling Department at Sandia National Laboratories. She is a computational materials scientist with a longstanding interest in bringing materials modeling to industrial practice. Over her 13 years at Sandia, she has worked on simulations to improve processes to make materials for advanced lighting, on prediction of microcircuit aging and reliability, and on the processing of innovative bearing steels. Her research areas include the theory and modeling of microstructural evolution in complex polycrystals, the physical and mechanical response of microstructures, and the wetting and spreading of liquid metals. Dr. Holm obtained her B.S.E. in materials science and engineering from the University of Michigan, an S.M. in ceramics from the Massachusetts Institute of Technology, and a Ph.D. in materials science and engineering and scientific computing from the University of Michigan. She has received several professional honors and awards, is a fellow of ASM International, and serves on the National Materials Advisory Board and the board of directors of the Minerals, Metals, and Materials Society. Dr. Holm has authored or coauthored more than 80 publications.

Pradeep K. Khosla is currently the dean of the College of Engineering and the Philip and Marsha Dowd Professor in the College of Engineering and School of Computer Science at Carnegie Mellon University. Dean Khosla is a leading researcher in enabling technologies for rapidly deployable systems through composition (for example, using hardware and software building blocks) and collaboration (for example, among autonomous robots and software agents). His vision of an intelligent system involves several specialized components that can be composed rapidly to create a system and that collaborate with one another to achieve the desired behavior. Achieving this goal requires the pursuit of research in seemingly diverse but philosophically connected areas, including agent-based control of distributed intelligent systems, agent-based methods for distributed design and manufacture, the ensuring of quality of service in heterogeneous networks, reconfigurable robots, composable simulations for intelligent computer-aided design, gesture-based programming, and the design of real-time software systems. He received a B. Tech from the Indian Institute of Technology in Kharagpur, India, and M.S. and Ph.D. degrees from Carnegie Mellon University.

Carolyn R. Mercer is a project manager at the NASA Glenn Research Center. She is an aerospace engineer and an optical engineer, using lasers and light in new ways to measure aerodynamic properties. She has developed technologies for integrated vehicle health management, intelligent propulsion systems, and instrumentation systems for aerospace ground testing. Dr. Mercer's specific experience includes using optics to measure the flow inside engines to test designs for improving fuel economy, using structured laser illumination to measure the shape of solid surfaces for manufacturing processes, and devising a liquid crystal/laser device to measure fluid temperature, density, or concentration for microgravity science. Dr. Mercer has a bachelor's degree in aeronautic and astronautic engineering from Ohio State University, an M.S. degree in physics from Cleveland State University, and a Ph.D. in optical science from the University of Arizona. She has published more than 30 papers, holds two patents, and has edited a book entitled *Optical Metrology for Fluids Combustion and Solids*, which was published in 2003.

Stephen M. Pollock is a professor at the University of Michigan and an international scholar in the mathematical modeling of systems, sequential decision analysis, and operations research. His work in understanding how to make critical trade-offs in complex decision-making processes has been applied to such diverse problems as military search and detection, manufacturing process monitoring, and design of adaptive radiation treatment plans. He has a B.Eng.Phys. from Cornell University and an M.S. in physics and Ph.D. in physics and operations research from the Massachusetts Institute of Technology. Dr. Pollock has been involved in teaching and applying a wide variety of operations research methods, with the aim of understanding and influencing operational phenomena in industrial and military settings, as well as in the public sector, medicine, and biology. He has authored more than 60 technical papers, has coedited two books, and has served as a consultant to more than 30 industrial, governmental, and service organizations. He has been associate editor and area editor of *Operations Research*, senior editor of *IIE Transactions*, associate editor of *Management Science*, and on the editorial boards of other journals. He has served on advisory boards for the National Science Foundation, as a member of the Committee on Applied and Theoretical Statistics of the National Research Council (NRC), and as a member of the Army Science Board. He was president of the Operations Research Society of America in 1986, was awarded the 2001 Kimball Medal by the Institute for Operations Research and the Management Sciences (INFORMS), and was named a founding INFORMS Fellow in 2002. Dr. Pollock is a member of the National Academy of Engineering.

Arthur Ragauskas is a fellow of the International Academy of Wood Science and the Technical Association of the Pulp and Paper Industry (TAPPI). His research program at the Georgia Institute of Technology is directed at understanding and exploiting innovative sustainable lignocellulosic materials. This multifaceted program seeks to develop new and improved applications for nature's premiere renewable biopolymers, including cellulose, hemicellulose, and lignin. Dr. Ragauskas has been a Luso-American Foundation teaching fellow at the Universidade da Beira Interior, Portugal; an invited guest teaching professor at Chalmers University of Technology, Sweden, and the South China University of Technology. He has authored more than 185 papers, patents, and conference proceedings. He is an associate editor for the *Journal of Pulp and Paper Science*, *Holzforschung*, *Journal of Wood Chemistry and Technology*, and has served on several advisory boards and review panels including those for the European Commission Research Directorate, J. Paul Getty Trust, TAPPI, the National Science Foundation, and the U.S. Department of Agriculture and the U.S. Department of Energy. Dr. Ragauskas obtained his honors B.Sc. degree in chemistry in 1980 and his Ph.D. in 1985 from the University of Western Ontario.

John A. Rogers is a professor at the University of Illinois at Urbana-Champaign and an interdisciplinary scientist, seeking to understand and exploit interesting characteristics of "soft materials," such as polymers, liquid crystals, and biological tissues. The goal of his work is to control and induce novel electronic and photonic responses in these materials in addition to developing new soft lithographic and

biomimetic approaches for patterning them and guiding their growth. This work combines fundamental studies with forward-looking engineering efforts in a way that promotes positive feedback between the two. Some highlights of his recent work include the first flexible paperlike displays, tunable microfluidic optical fiber, stamping techniques with nanometer resolution, and liquid-crystal modulators built on optical fiber tips. Dr. Rogers received degrees in physics and chemistry from the University of Texas at Austin and a Ph.D. degree in physical chemistry from the Massachusetts Institute of Technology. In addition to his more than 120 publications, he has nearly 60 patents and patent applications in areas ranging from acoustics to neural networks to nanofabrication to fiber optics and organic electronics. More than 30 of these are licensed or in active use. Dr. Rogers was named a Robert B. Woodward Scholar by Harvard University and was selected by the National Academy of Engineering as one of the top 100 young engineers and by *Technology Review* magazine as one of the top 100 young innovators for the 21st century.

Barton Rubenstein creates indoor and outdoor sculpture with and without water for public and private spaces, including corporate, commercial, and academic institutions as well as private residences. He typically works with bronze, stainless steel, stone, and glass. Dr. Rubenstein has received several awards for his artwork, lectures frequently about his work, and has been featured in numerous newspaper articles across the country. He has worked with various art forms throughout his career, including lithography, etching, woodcuts, architectural drawing, and sculpture. He trained in physics and mechanical engineering at Haverford College, Pennsylvania, and then completed his M.Sc. and Ph.D. degrees at the Weizmann Institute of Science, Israel, studying the brain and visual sciences. This research in neuroscience focused on how people visually perceive the world. His research attempted to elucidate various anomalies of visual perception, such as camouflage and, more generally, the processes at work within the visual system. Published work of his research has appeared in *Science*, *Journal of the Optical Society of America*, and *Scientific American*, as well as in *Time Magazine* and on National Public Radio. He is the principal of Rubenstein Studios.

Michael A. Smith is the director of research and university alliances at France Telecom R&D, San Francisco. He is a specialist in video content analysis and the author of numerous papers and a book on the subject. His research interests include visualization and indexing for multimedia libraries; multimodal audio and video processing; media interfaces between people and machines for mobile and fixed platforms; and e-learning for disadvantaged communities. His innovations include patented video analysis and summarization technology, which is licensed by media management companies. Before joining France Telecom, Dr. Smith founded AVA Media Systems and worked as a visiting professor in the Computer Vision Research Center at the University of Texas at Austin. He has served as a visiting professor at Morehouse College in Atlanta and at the University of Campinas in Brazil and as a guest lecturer at the University of California at Berkeley. He is also the director for a broadening participation alliance for underrepresented students pursuing graduate degrees in computer science. Dr. Smith holds a Ph.D. in electrical and computer engineering from Carnegie Mellon University, an M.S. in electrical engineering from Stanford University, and a B.S. degree in electrical engineering from North Carolina A&T University and Tuskegee University.

Gary K. Starkweather received his B.S. in physics from Michigan State University in 1960 and a master's degree in optics from the University of Rochester in 1966. He has spent more than 40 years in the imaging sciences and holds more than 44 patents in the fields of imaging, color and hard-copy devices. From 1962 to 1964, he worked for Bausch & Lomb, Inc., in Rochester, New York. From 1964 until 1988 he was employed by Xerox Corporation, where he became a senior research fellow. While at the Xerox Palo Alto Research Center (PARC), he invented the laser printer. Dr. Starkweather has received a number of awards for this work, including the Xerox President’s Achievement Award (1977), the Johann Gutenberg Prize from the Society for Information Display (1987), and the David Richardson Medal from the Optical Society of America (1991). From 1988 until 1997, he was employed by Apple

Computer as an Apple Fellow involved in publishing and color imaging products and research. In 1994, he received a Technology Academy Award for his consulting work with Lucasfilm and Pixar on color film scanning. In 2002, he was inducted into the Technology Hall of Fame at COMDEX. He has recently retired from Microsoft research as an architect working on displays and information processing. He has published many papers and has written a book chapter entitled "High Speed Laser Printers" for Academic Press. He continues to serve on several technical committees involved in display and color-related imaging issues and has lectured at both Stanford University and the University of California at Los Angeles. He is a member of the National Academy of Engineering.

Dennis J. Trevor is technical manager of the Optical Materials Group of OFS Laboratories in Murray Hill, New Jersey, formerly part of Lucent Technologies Bell Laboratories. He led the development and assisted in the implementation of the first commercial Sol-Gel process used in optical fiber preform manufacture. Currently he is developing new applications using this technology in related fields of photonics. His additional work in material growth methods includes chemical reaction studies of metal clusters, active oxygen source growth of high-T_c superconductor films, and very low pressure chemical vapor deposition of silicon and germanium alloys. In his 15 years at Bell Laboratories, Dr. Trevor has also developed experimental methods to improve our understanding in a wide range of fields, from semiconductor plasma processing to surface diffusion in electrochemical corrosion. He received his B.S. in chemistry at the Illinois Institute of Technology in 1975 and his Ph.D. in physical chemistry from the University of California at Berkeley in 1980. He has more than 50 publications and holds several patents.

Appendix B

Features of Current U.S. Banknotes

This appendix describes the materials and manufacturing processes used in the production of U.S. banknotes. It discusses how these production elements combine to result in effective banknote features. The section on the vulnerability of current features describes some methods being used to simulate genuine banknote features.

CREATING UNIQUE FEATURES ON GENUINE BANKNOTES

Special papermaking and printing processes are required in the manufacture of U.S. banknotes in order to implement their design. The features of a U.S. banknote fall into three general categories: (1) substrate, (2) additional elements, and (3) the printed image. These features can be detected through visual means, through tactile means, and through a variety of detection schemes that are augmented by devices. It is important to understand how these features are produced in order to understand their interactions with one another and their effectiveness in U.S. banknotes.

Substrate

The cotton and linen paper that is the substrate for U.S. banknotes is not only a base for the printed image and additional substrate elements, it is also a feature itself. The substrate is an intentionally designed feature of currency—it contributes to the look of the note, the feel of the note, the denomination of the note, and the authenticity of the note. The distinct feel of a crisp, new bill is very recognizable. Through engineering of the paper substrate, this characteristic feel can withstand folding, crumpling, soiling, and even laundering.

The substrate also has a distinctive look. The paper used for U.S. banknotes is a blend of two cellulosic plant fibers, flax (also known as linen) and cotton. It is supplied to the Bureau of Engraving and Printing (BEP) by a single manufacturer, Crane and Company in Dalton, Massachusetts. Processing of the substrate, which is tightly controlled, includes the use of selected plant fibers and additives and the development and use of specialized methods for pulping, washing, refining, screening, pressing, and bleaching.

The sources of raw materials are selected by optimizing quality and cost. Both the flax and cotton materials are primarily sourced from waste products from the textile industry. This approach is cost-effective because papermaking can utilize the shorter fibers that make poor thread for cloth. Currently, U.S. currency is made from nominally 25 percent flax and 75 percent cotton fibers. An assortment of papermaking chemicals—color, strength, and sizing agents—are added to the raw materials. No starch or

BOX B-1 Papermaking

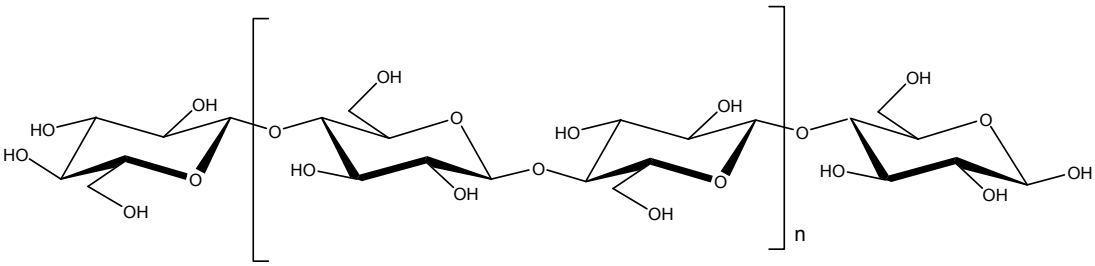

FIGURE B-1 The structure of cellulose (ß-1,4-D-glucopyranose).

Cellulose, the most abundant natural polymer on Earth, is the major component of all papermaking fibers, including those used in the manufacture of U.S. currency. This natural polymer is composed of long linear chains of ß-1,4-glucopyranose in the $^4C_1$ chain conformation with equatorially oriented hydroxyl groups as illustrated in Figure B-1. The degree of polymerization of these chains ranges from 15,000 for unprocessed cotton to as low as 1,000 in a bleached kraft pulp. The hydroxyl groups on these linear cellulose chains form strong hydrogen bonding networks within and between cellulose chains.

Although cellulose has four crystalline polymorphs (cellulose I, II, III, and IV) only cellulose I is found in nature. Bundles of cellulose molecules, known as microfibrils, have been shown to contain both crystalline (50 to 70 percent) and amorphous regions.

Cellulose-to-cellulose hydrogen bonds are the primary theoretical fiber-to-fiber bonding mechanism. The maximizing of the fiber surface area, fiber-to-fiber contact, and hydrogen bonding are important factors in the optimization of fiber-fiber bonding. Fiber surfaces available for bonding may be developed during the beating/refining of cellulosic pulps owing to internal and external fibrillation. In general, the greater the fiber surface area available, the greater the extent of bonding. Fiber-to-fiber contact occurs when water is removed during wet pressing and the drying process. In cellulose, hydrogen bonding occurs between hydroxyl groups.

Many different high-volume grades of virgin paper exist. In essence, the papermaking process is an aqueous-based system in which cellulosic plant fibers are first mechanically treated to remove impurities and improve subsequent process stages. The next stage is often a pulping treatment that chemically removes unwanted materials. The resulting pulp is screened, washed, and may undergo subsequent chemical bleaching. The processed cellulosic fibers may then be mechanically refined to enhance the fiber bonding capacity before introduction into the papermachine.

At the papermachine, the pulp is diluted and delivered to a porous moving belt or drum that facilitates water removal and the initial formation of a sheet of paper. In subsequent operations, presses and drying cylinders are used to remove the remaining water. In addition, papermakers utilize the papermachine to introduce an assortment of papermaking chemicals that enhance physical and optical properties of the paper. In the production of currency paper, manufacturers extend the capabilities of the papermaking process to facilitate the controlled introduction of watermarks, colored threads, security strips, and other anticounterfeiting technologies.

clay agents are employed in currency paper, although these are added to most other high-quality papers to improve brightness. This difference contributes to the unique look of currency paper.[1] See Box B-1 for further details on papermaking, which convey the difficulties inherent in duplicating the "feel" of genuine currency paper.

Added Elements

A number of additional items are added to the substrate during the papermaking process. These include short fibers that are visually apparent as short red and blue threads in the paper itself. A

[1]Information available at http://www.currencyproducts.com/what_to_look_for/substrate_features.html. Accessed March 2006.

watermark is made during the papermaking process in the $5, $10, $20, $50, and $100 notes. The watermark depicts the same historical figure as that shown on the respective bills' engraved portraits.

Higher-denomination notes also incorporate security strips, made of thin plastic embedded in the notes in the final stages of papermaking; these are marked by metallic print indicating the denomination of each note. In newer notes, the strip also contains a tiny graphic of American flags.[2] The strips have a unique position on each denomination as well as a unique fluorescent color under ultraviolet lighting: The $5 strip is blue; the $10, orange; the $20, green; the $50, yellow; and the $100, red.[3]

Specifications for the paper, including the embedded elements, ensure that U.S. banknotes have a consistent look, feel, and strength. These specifications encompass thickness, opacity, roughness, porosity, resistance to tearing, tensile strength, fluorescence, folding endurance, thread bonding, color, ash, pH, and embedded-fiber density.

Image

After the paper is delivered to the BEP as stacks of cut sheets, it is printed in a multistage printing process, front and back. Each sheet will be cut into 32 U.S. banknotes at the end of the printing process. For the $10, $20, and $50 notes, the first step is an offset process that prints a colored background simultaneously on the front and back of the sheet of notes. The background offset-printed colors are different for each denomination. The offset press is capable of maintaining register within approximately ±0.008 millimeters.

Next, the sheets are intaglio printed in separate steps on the front and back. The largest and most noticeable element of the intaglio-printed image is the portrait ($5, Lincoln; $10, Hamilton; $20, Jackson; $50, Grant; $100, Franklin). The portrait is also printed slightly off-center to open up space to enable the addition of the watermark and also to reduce image wear caused by folding the note in half.

On all but the $1 and $2 notes, the portrait is large enough to accommodate microprinting and fine-line details. Microprinting is used to print 0.2 mm tall letters with a line width of 0.05 mm. The production line width is approximately 0.1 mm, with a spacing of 0.1 mm. Microprinting and fine-line printing are used because they are difficult to reproduce with low-resolution electronic devices and can be viewed by the sharp-sighted or with a simple, low-power magnifier.

Inks are used in a variety of ways in banknote printing to create security features in the images. For example, infrared and magnetic patterns are incorporated that can be detected by machine.[4] Color-shifting ink is used to print the denomination in the lower right corner of the $10 notes and higher denominations. The ink is optically variable, and shifts colors on the older $10 and $100 notes from green to black, and from copper to green on the new $10, $20, and $50 notes.[5] The printed image on the note also contains "symbols of freedom" such as a torch ($10), an eagle ($20), and a national flag ($50). All of the inks used are purchased from a single source, SICPA, headquartered in Lausanne, Switzerland. SICPA provides security inks for over 85 percent of the world's banknotes.[6]

Finally, the offset printing on the newest notes (the redesigned $10, $20, and $50) contains two additional features aimed at counterfeit deterrence. Patterns and ink colors known as the banknote detection system (BDS) are used to prevent counterfeiting using color copiers. An additional digital counterfeit deterrence system (CDS) is also incorporated into the line pattern that interferes with the ability to reproduce banknotes digitally.

---

[2]Information available at http://www.pbs.org/wgbh/nova/moolah/anatomypaper.html and http://www.moneyfactory.gov/newmoney/main.cfm/currency/aboutNotes. Accessed March 2006.

[3]Information available at http://www.jascoinc.com/literature/pdf/appnotes/FP_01.02.pdf and http://www.stopfraud.com/prod06.htm. Accessed March 2006.

[4]Laser Technology Identifies Counterfeit Currency, in Photonics Spectra, August 2005. Available at http://www.photonics.com/spectra/applications/XQ/ASP/aoaid.391/QX/read.htm. Accessed March 2006.

[5]More information on color-shifting inks is available at http://www.moneyfactory.gov/newmoney/main.cfm/currency/new20#ink. Accessed March 2006.

[6]Information available from SICPA at http://www.sicpa.com/731/764/729/752.asp. Accessed March 2006.

FEATURE EFFECTIVENESS

While it is very difficult to say with certainty which are the most important features on current notes, there are some indicators for which features are important to the different types of users of banknotes:

- The features most used by the general public are reported to be the overall "look" and the overall "feel" of the note. The discriminators reported in checking for counterfeits when a banknote looks or feels different include the watermark, security strip, color-shifting ink, fine lines, and microprinting.
- The features most used by current machine readers are the transmissive optical spectrum and printed image, magnetic patterns, ultraviolet fluorescence, ultraviolet spectrum, and the infrared properties. Low-end readers may sense only one feature; high-end readers may use 10 or more measurements to authenticate and denominate each note.
- The features most used by the blind community to authenticate notes are the tactile features. There are no features available for use by the blind public to denominate or authenticate U.S. banknotes without using a machine reader.

It is interesting to note the overlap in responses of these users; both general and blind users identified the importance of the tactile feel of the note. It is also interesting to note which features are not used. For example, most overt counterfeit-deterrent features—such as the color-shifting inks, substrate properties, watermark, security strips, microprinting, and the Federal Reserve seal—are not currently used by machine readers because they are difficult to sense, to locate, or to verify. These features are also apparently rarely used by the general public, and some are not used at all, even by experienced cash handlers.

On the Vulnerability of Features

A variety of vulnerabilities drive currency design. Overall, features can be vulnerable in two main modes, and the two have less to do with trends in digital equipment and more to do with criminal motivation. Table B-1 summarizes the various printing processes considered, their quality implications, spatial resolutions, and general costs. This table provides a quick review of the processes available to the counterfeiter and their relative vulnerability as well.

As has been discussed, every feature on a U.S. banknote today is vulnerable to determined counterfeiters. These counterfeiter are willing to seek out specialized materials and equipment and are willing to search the Internet for special inks, image files, and tips on which digital printers and software will make a good counterfeit. Their motivation is criminal gain, which drives the depth of their effort and the scale of their operation.

Deterring a determined counterfeiter is possible through the combination of (1) features that are difficult to simulate and (2) an educated cash-handling public that is inspired to understand the distinctive nature of these features. However, there are no features on currency today—issued by any country—that a dedicated counterfeiter would find impossible to simulate and pass into circulation.

Casual counterfeiters, conversely, are more easily deterred. These counterfeiters may use equipment and materials that are easily accessed to make a few "pretty good" notes on an occasional basis. They are motivated merely by the opportunity; for example, they may take unwitting advantage of the lack of banknote detection systems in all-in-one devices or cell phone cameras. Today's U.S. banknote provides

TABLE B-1 Information Age Technologies Employed by Counterfeiters

Technology	Availability	Cost	Capability	Use Limitations[7]
Internet	Home	Low	Provides information, know-how, image files, access to useful materials	
Thermal ink-jet printers	Home	Low	Sufficient image resolution but does not reproduce non-image features	
All-in-one devices	Home	Low	Sufficient image resolution but does not reproduce non-image features	
Thermal transfer printing	Home	Low	Uses smooth, glossy paper; does not reproduce non-image features	
High-quality scanners	Home and office	Moderate	Captures image with sufficient resolution and no obvious artifacts	
Color copiers and color laser printers	Office and home	Moderate	Sufficient image resolution but does not reproduce non-image features	
High-quality digital cameras	Home and office	Low	Captures image with sufficient resolution and some image processing	
Image-processing software	Home and office	Low	Easily handles the larger high-resolution files needed to counterfeit	
Flatbed ink-jet printers	Commercial and printing centers	High	Sufficient resolution and use of special inks can simulate watermark, colored threads, special inks, and some level of print relief	
Digital press	Commercial printing	High	Duplicates the resolution used to print currency	

only a few features that would deter such a counterfeiter. However, even if a counterfeiter makes no attempt to simulate the more difficult features, an uneducated public can facilitate their quick financial gain.

A larger threat is looming as well: the increasing availability of currency-accepting devices that remove the human cash handler from the transaction. The growth in the use of these devices is expected to eventually balance the importance of human-recognized and machine-readable features in deterring currency counterfeiting. A result of the wider availability of cash accepters is the possibility that they can more easily fall into the hands of potential counterfeiters. The would-be crooks, including hobbyists, could easily refine their methods until their notes are accepted by the reader. One possible way to address this activity is to incorporate technology in currency readers that flag such efforts.

[7]Pursuant to the Federal Advisory Committee Act § 15(b)(4), 5 U.S.C. App., data in this column has been withheld.

Novel Methods to Simulate Features

Users of U.S. currency have a habitual knowledge of the color and feel of the substrate. The color of the paper is not printed but is a result of the complex papermaking process, and the feel is unique to the fibers inside and the printing on the note.

In order to incorporate genuine currency paper into their products, some counterfeiters use common household bleach on $1 notes. By masking most of the printing on the note, for example, only the denomination might be bleached away and then reprinted. This technique has been made much easier through the ability of printers to handle thicker paper and new color-matching capabilities.

The color of the traditional intaglio-printed ink and of the new offset-printed background inks is also imprinted in the subconscious of many users of U.S. banknotes. Today, the subtle colors in many currencies are created using spot color inks and pigments. Many of these are nearly impossible to reproduce with a conventional desktop printer's combination of cyan, magenta, yellow, and black (CMYK) inks. However, new software and hardware tools are emerging that can improve an RGB (red, green, blue) monitor's WYSIWYG (what you see is what you get) color capabilities. These tools are intended to enable an artist working in CMYK to more accurately repair color problems on-screen before having to surmount the hardware issues within an RGB printer's software. These tools are common among experts today.

A simpler approach to circumventing the limitations in standard color reproduction may be to empty an ink-jet cartridge and refill it with spot color ink. This could more perfectly reproduce the characteristic green that says "money" to most people. Duotone printing provides another low-cost tool to the counterfeiter.

Magnetic ink is a particularly difficult material to simulate. One solution is to incorporate nanoscale magnetic particles into suspension in today's inks. The chemistry of ink-jet inks is very complex, but it may be very reasonable to suspend magnetic nanoparticles in them for the short times—on the order of hours—needed to print hundreds or thousands of sheets.

Finally, novel methods of using image-acquisition and image-processing software can more easily simulate the features on banknotes. For example, instead of scanning an entire note and re-creating it line by line, the tools common to today's art software can enable a would-be counterfeiter to scan and edit features independently. This approach looks at selected portions of the note one at a time and is done in sizes and ways that are allowable under current usage constraints.[8] Because a counterfeiter may only scan and incorporate the features that make a note easy to recognize, many printers and copiers may not recognize the final product as a banknote. In addition, once a counterfeiter completes this task, it is a simple matter to share the image file with others via the Internet.

[8]For example, see the images on the software demonstration page at CSS Zen Garden, a demonstration of what can be accomplished visually through CSS-based design. Available at http://www.csszengarden.com/?cssfile=/126/126.css&page=7. Accessed March 2006.