DETECTION AND DETERRENCE OF COUNTERFEITING OF VALUABLE DOCUMENTS

Cormac Herley[1], *Poorvi Vora*[2] *and Shawn Yang*[3]

[1]Microsoft Research, One Microsoft Way, Redmond, WA
[2]Computer Science Dept., George Washington University, Washington DC
[3]Cisco Systems, San Jose, CA

ABSTRACT

Counterfeiting of valuable documents is an increasingly serious problem. Banknotes, drivers licenses, passports, diplomas and stock certificates are all the subjects of increasingly frequent and accurate counterfeiting efforts. This is in part due to the performance improvements of consumer inkjet printers. Design features which required great labor and skill to reproduce on an engraved-plate printing process pose essentially no difficulty to a counterfeiter armed with an accurate scanner and high-resolution color printer. We show how simple changes in banknote design coupled with possible changes in rendering engines can make the task of counterfeiting enormously more difficult.

1. INTRODUCTION AND BACKGROUND

Counterfeiting of valuable documents has surged with the improvements in performance of low cost color printers and scanners [5]. Creating a passable version of a banknote previously required considerable investment and expertise, but is now easily accomplished on readily available equipment without skill or investment [1]. This has created a problem for the issuers of valuable documents, in that design features which historically were hard to replicate without expensive equipment no longer present a barrier to a counterfeiter. An obvious example is the fine engraving work that historically graced many currency designs: to replicate such an engraving required much skill and labor. A high resolution scanner captures all of the detail without effort however. Similarly, the characteristic "banknote green" used on the back of the US notes used to be a hard color to match exactly if the ink had to be physically mixed, but even very thin lines can be created in composite color on 600dpi or higher printers that look almost perfect to the naked eye. These facts have created a new burden for the designers of valuable documents [1].

Documents such as drivers licenses and passports which generally bear a picture of the holder and are non-transferable can be protected using a number of interesting approaches [4]. It is also increasingly common for drivers licenses and passports to have machine readable magnetic strips that allow verification that no tampering has occurred. Documents such as banknotes, stock certificates and bonds present a harder problem, since they are not bound to any particular holder and generally change hands after a visual inspection only.

There are several approaches to deterring counterfeiting of documents. Chief among them:

1. Print valued documents with features that cannot be reproduced on consumer color printers
2. Embed features in valued documents that are recognizable to a machine
3. Have rendering engine (*e.g.* printer) check for embedded marks or features of the valued documents to be protected.

Each of these approaches has difficulties. An extensive examination of design features that are difficult to produce on consumer printers is given in [1]. There are many features in widespread use in the banknotes of various countries around the world. For example: Holographic tabs (euro zone, Switzerland), Metallic tabs (Canada), Saturated Color Patches (UK, euro zone), Transparent Tab (Brasil), Plastic substrate (Australia, Brasil), See-throughs (euro zone, UK, Canada, Brasil). Unfortunately many of these features such as holograms, reflective tabs and transparent patches are expensive and require a post-printing processing stage, and thereby increase the cost per note. Several (such as metallic tabs) are more fragile than others and can decrease the useful life of the note. Even metallic tabs can be simulated with printing [3].

Embedding features that allow positive determination of authenticity have clear value. Many countries print banknotes on acidic paper thereby allowing a simple test by applying a litmus ink. These verify authenticity of documents rather than preventing counterfeiting, which is our interest. Thus we focus on checking for attempted counterfeiting at the point of printing. We focus primarily on US banknotes, but will examine other documents also.

2. TECHNOLOGY

2.1. Detecting Valuable Documents

Requiring printers and other color reproduction devices to detect valuable documents sounds like a promising line of enquiry. Call a document that is to be printed $\mathbf{x}$. Ideally, we would like a simple test of the form:

$$D(\mathbf{x}) \begin{array}{c} \text{No Print} \\ > \\ < \\ \text{Print } \mathbf{x} \end{array} \text{threshold.} \quad (1)$$

That is by comparing a sufficient statistic [6] that depends on the document with a threshold we decide whether or not to print. As with many detection problems there is a tradeoff between the false positive and false negative rates. Here a false negative ($D(\mathbf{x}) <$ threshold when $\mathbf{x}$ is protected document) implies that a counterfeiter manages to circumvent the system and print a valuable document. A false positive ($D(\mathbf{x}) >$ threshold when $\mathbf{x}$ is not a protected document) means a legitimate user is prevented from using the device. Clearly both outcomes are very undesirable. The problem is further complicated by the need to keep the computational cost low. An obvious test, in the case of US currency, might involve searching for an overt feature like the president's face. However we would have to search for this feature at every possible orientation (*i.e.* the image of the counterfeit note might appear at any angle in the document) unless we chose a rotationally invariant feature. Recall *every* document will have to be subjected to scrutiny. If we could devise a test as in (1) which had very low false negative and positive rates, this might still not be useful if calculating $D(\mathbf{x})$ slowed the printing of each page appreciably. To be concrete a delay of even a second per page would greatly reduce the throughput of the printer.

Expressed as a conventional detection problem we seem to have an almost impossible task: how to minimize the false positive and negative rates while keeping the cost of calculation of $D(\mathbf{x})$ as close to zero as possible. Previous approaches [2] suffer from the fact that their complexity, while low, still represents a large burden.

2.2. Multi-level Detection and Deterrence

The reason $D(\mathbf{x})$ is complex is that the test in (1) must return a binary decision and make almost no errors. We expect the test to be expensive if it must be really sure of its decisions. We propose an alternative approach which takes a multi-level approach to detecting protected documents:

$$S(\mathbf{x}) \begin{array}{c} \text{Print } \mathbf{x}' \\ > \\ < \\ \text{Print } \mathbf{x} \end{array} T_s, \quad (2)$$

where $\mathbf{x}'$ is a distorted version of the document. Observe that in contrast to the test in (1) a version of the document is always printed. However, if the document is regarded as possibly suspicious it is distorted somewhat before printing. This deformation is carefully chosen to maximize the inconvenience to a counterfeiter while minimizing the inconvenience to legitimate users.

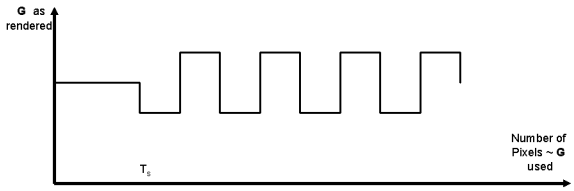

Fig. 1. Selective mis-rendering function. Once greater than a threshold amount of banknote green is used that color is dynamically mis-rendered as a function of the numer of pixels of that color used.

For example, a large amount of "banknote green" in a document might indicate a *possible* attempt at counterfeiting a banknote. Instead of refusing to render our device might then selectively mis-render the document. If this can be done in such a fashion that makes the counterfeiters job difficult, while imposing minimal inconvenience on others it may prove worthwhile. This requires two things:

- Suspicious features on valuable documents that can be detected with insignificant computational effort (*i.e.* $S(\mathbf{x})$ is easy to calculate)
- Capabilities of the rendering engine that can be modified to cause noticeable degradation on valuable documents but negligible degradation for other documents (*i.e.* $\mathbf{x}'$ is visually distinguishable from $\mathbf{x}$ if it is a protected document, but not otherwise.)

Next, we address these two requirements in turn.

Fig. 2. Selective mis-rendering of obverse of US currency. Once greater than a threshold amount of banknote green is used that color is dynamically mis-rendered using the distortion function in Figure 1. The visible bands of alternating light and dark green make the note difficult to pass. Note the bands are designed to be clearly visible when printed with accurate color reproduction on an inkjet printer. They may be more or less visible for monitor or other print conditions.

2.3. Features of Valuable Documents Easily Detected

Here we examine the question of finding a function $S()$ such that computing $S(\mathbf{x})$ will place negligible computational burden on the print engine. A feature suitable for use as the first level detection mechanism is one that counts the amount of a particular color that is used. The obverse of a US banknote is a characteristic green **G**, printed on a yellow substrate **Y**. Pixels of a counterfeit US note will be either this particular green **G**, the yellow **Y**, or a convex combination of the two: $\alpha\mathbf{G} + (1-\alpha)\mathbf{Y}$, for $0 \leq \alpha \leq 1$. There is thus a range of colors which might reasonably pass for banknote green, and use of a large number of pixels in this color green could be regarded as suspicious. Thus, let us define

$$S(\mathbf{x}) = \#\text{ pixels s.t. } \alpha\mathbf{G} + (1-\alpha)\mathbf{Y}, \alpha > 1/2. \quad (3)$$

It may not be obvious why (3) is inexpensive to compute. Since ink and toner printers generally use the subtractive CMYK color space rather than the additive RGB space the document must first be converted from one space to the other. To adjust for printer non-linearities this is done (almost universally) in a look-up table:

$$\begin{pmatrix} \mathbf{x}.c \\ \mathbf{x}.m \\ \mathbf{x}.y \\ \mathbf{x}.k \end{pmatrix} = LUT \begin{pmatrix} \mathbf{x}.r \\ \mathbf{x}.g \\ \mathbf{x}.b \end{pmatrix}. \quad (4)$$

Here, $\mathbf{x}.c$ means the cyan plane of the document and so on. The fact that an LUT is used means that we can evaluate (3) for negligible additional computation. We can label every RGB location in the LUT for which

$$\alpha\mathbf{G} + (1-\alpha)\mathbf{Y}, \alpha > 1/2.$$

A counter is then incremented each time the suspicious region is accessed, allowing a record of the number of times the suspicious color has been used.

Choice of the threshold in (2) now also becomes simple. Suppose $\mathbf{x}_{\$20}$ is a document that contains an image of a US $20 bill and when rendered gives $S(\mathbf{x}_{\$20})$, then we might choose $T_s = S(\mathbf{x}_{\$20})/5$. This would mean that after a document had used 20 % of the banknote green required to render a note suspicion would be raised. Once the counter exceeds a threshold the document is classified as suspicious, and use of deterrence can begin.

2.4. Mis-rendering the document

Here we examine suitable deformations $\mathbf{x}'$ of the document that will be visually apparent on valuable documents, while making little difference to legitimate documents. While large blocks of **G** appear on banknotes that color seldom occurs *over contiguous regions* in other images or documents. Certainly many innocent documents will have $S(\mathbf{x}) > T_s$. However, natural images which contain a lot of green will often contain **G** interspersed with other shades of green, rather than in large blocks. Images of trees and vegetation, for example, usually contain a lot of texture rather than solid blocks of constant color.

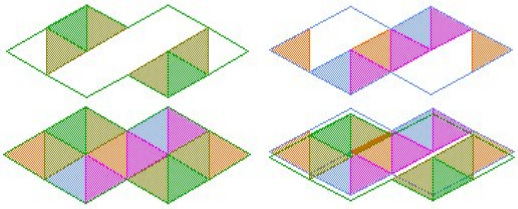

Fig. 3. See-through alignment pattern used in an Argentinian banknote. Top line: the two patterns are printed on opposite sides of the page. Bottom Line: when aligned correctly a recognizable pattern appears (left). When aligned incorrectly the pattern is clearly improperly rendered (right).

One suitable deterioration that makes a counterfeiter's life difficult is to deliberately mis-render **G**, once suspicion has been aroused. An example is shown in Figure 1 where we show the intensity of green that we actually render as a function of the amount of that suspicious color that is used. At first banknote green is rendered correctly; when the amount used on a single page exceeds $S(\mathbf{x}_{\$20})/5$ we mis-render subsequent uses of that color. This is done dynamically so that the intensity of rendered **G** varies with period $S(\mathbf{x}_{\$20})/20$. This has the effect that several bands of green of varying intensity will appear on the counterfeited note. In Figure 2 we show an attempt to print a banknote. Observe that clearly visible bands show up that will make the note difficult to pass. Also note that this will happen independently of the rotation of the note as indicated in Figure 4. In Figure 5 we show another image that contains a lot of green, including an above threshold amount of the "suspicious" banknote green. This also is subjected to mis-rendering. However, since the suspicious color is dispersed and the image contains a lot of texture, there is no noticeable degradation in quality.

A second example of selective deterioration is by exploiting design features known as "see-throughs." These are patterns where half the design is on the front of the note and half is on the back. An example is shown in Figure 3. They are present in the design of most major currencies, an example being the note amount on the top left of the euro notes. When held to the light the two halves form a recognizable pattern. This pattern, however, is very sensitive to alignment. Even slight mis-alignment will be very noticeable. A simple deformation to make rendering of such

Fig. 4. Selective mis-rendering of obverse of US currency. Observe that the bands are visible even if printed at an angle.

Fig. 5. Selective mis-rendering of image. Once greater than a threshold amount of banknote green is used that color is dynamically mis-rendered as a function of color used. Above: original image with $S(\mathbf{x}) > T_s$. Below: image rendered with distortion function shown in Figure 1.

features difficult is deliberate unpredictability of alignment. Generally printers start rendering at the top left corner of a page, and dependably begin at a certain location. If instead we jitter the begin location by a small random amount vertically and horizontally we make it very difficult to align the front and back accurately. That is, if the top left of the page is $(0, 0)$, the printer may generally begin printing at a position (x_0, y_0). If this is dependable and repeatable a counterfeiter may produce notes with excellent "see-through" reproduction. Instead however, once $S(\mathbf{x}) > S(\mathbf{x}_{\$20})/5$, and the document is regarded as suspicious, we render subsequent pages instead starting at $(x_0, y_0) + (\Delta_x, \Delta_y)$ where both Δ_x and Δ_y are random numbers uniformly distributed on $(-2.5mm, 2.5mm)$. Thus in printing a suspicious document a counterfeiter cannot count on alignment better than 5mm. This makes it very difficult to produce accurate renditions of "see-throughs." An example is shown in Figure 3.

3. ACKNOWLEDGEMENTS

The authors would like to acknowledge that most of this work was performed while they were at Hewlett Packard. They would like to thank Neerja Raman for encouragement and support.

4. REFERENCES

[1] Committee on Next-Generation Curency Design. *Counerfeit Deterrent Features for the Next-Generation Currency Design*. National Research Council, 1992.

[2] D. Gruhl and W. Bender. Information hiding to foil the casual counterfeiter. *Information Hiding Workshop*, 1998.

[3] R. D. Hersch, F. Collaud, and P. Emmel. Reproducing color images with embedded metallic patterns. *ACM Trans. on Graphics*, 22(3):427–436, July 2003.

[4] L. O'Gorman and I. Rabinovitch. Secure identification of documents via pattern recognition and pubic-key cryptography. *IEEE. Trans. PAMI*, 1998.

[5] United States Treasury Dept. *The Use and Counterfeiting of United States Currency Abroad*. 2003. http://www.federalreserve.gov/boarddocs/rptcongress.

[6] H. L. van Trees. *Detection, Estimation and Modulation Theory: Part I.* Wiley, 1968.