Security Printing in Digital Age

Zhigang Fan, Reiner Eschbach, Shen-ge Wang, and Raja Bala; Xerox Corporation; Webster, NY, USA

Abstract

In security applications, it is desirable to add information into the document that prevents / hinders alterations and counterfeiting. Traditionally, security printing is associated with expensive equipment, specially designed media and/or printing material. The emerging digital printing technology is changing the dynamics of security printing. In addition to numerous newly invented digital security features, many traditional features now can be implemented with digital technology using conventional equipment and material. Furthermore, the flexibility of digital technology enables variable information embedding at a low cost even at a run length of one, thus creating "individualized security printing". This paper will discuss the implication of the digital technology on security printing. It will also provide an overview of several digital security printing technologies we have developed.

1. Introduction

The main goal of security printing is to prevent forgery, tampering, or counterfeiting. Traditionally, security printing protects sensitive paper documents including banknotes, passports, stock certificates and identity cards. It is often associated with expensive equipment, specially designed media and/or printing material, such as unique high-quality paper, fine-line engravings, and high-pressure (intaglio) printing. This was adequate in the past to restrict counterfeiting to the dedicated craftsman with access to a printing press. However, the emerging digital printing technology is changing the dynamics of security printing. Highly sophisticated and technologically advanced reprographic systems are no longer tools limited to the skilled technician but are widely available to, and accepted by, the general public. Ease of use and versatility, facilitated by user-friendly control panels, permit an unskilled user to make faithful, full-color reproductions of any document. Reproduction quality, ease of access, and relative freedom from discovery combine to create an atmosphere within which many individuals may experiment with unauthorized replication of sensitive documents, committing the so-called crime of opportunity. Furthermore, the low reproduction cost encourages counterfeiting of documents of relatively low value. These documents, such as tickets, merchandise packaging, coupons, prescriptions are traditionally not covered by security printing.

While the continuing advancement in digital printing technology has posted significant challenges for anti-counterfeiters, it also offers opportunities for security printing. Many new security features have been invented based on digital technologies. One such an example is digital watermarking [1,2]. In addition to new methodologies and systems, many traditional features can now be implemented using commercially available equipment and material at a very low cost, thanks to digital technology. This expands the range of security printing coverage to many relatively low value documents. Furthermore, the flexibility of digital technology enables cost-effective variable information embedding even at a run length of one, thus creating "individualized security printing".

In this paper, we will introduce several security printing technologies that have been developed in Xerox in the past a few years, which includes MicroText Mark, Correlation Mark, Glossmark® Text, Florescent Mark, InfraRed Text and Guilloché Mark. Among the other advantages, these features are designed to be produced with commercially available xerographic machines with normal materials (CMYK toners) and normal printing conditions. No special toner/ink or paper is required. In addition, the features can be implemented as variable data that can be individualized for each document.

2. Glossmark®

Glossmark® technology generates pictures with effects that are very similar to latent images in traditional security printing. It may embed text or pictures that are not perceptible in straight-on view, but becomes visible under inclined illumination. The effect is illustrated in Figures 1a) and 1b). Figure 1a) shows the document under the normal viewing condition while Figure 1b) gives a snapshot for the same document when it is observed from a tilted angle, in which the hidden strawberry figures become visible.

While traditional latent images are created by varying surface-relief pattern of the ink obtained with Intaglio printing process, Glossmark® is based on orientation dependent gloss. A detailed description of the technology can be found in [3]. Briefly speaking, Glossmark® applies two kinds of halftones for the foreground (say text) and background regions. The halftones match in density/color and shape, but exhibit different gloss characteristics.

Figure 1. *a) (left) the document viewed at normal condition; b) (right) the document viewed at a tilted angle.*

3. MicroText Mark

Micro printing is a traditional feature that has been commonly applied in banknote protection. The small font letters are printed with high resolution offset/intaglio process. The print appears as a thin line to the naked eyes, but the characters can easily be read using a low-power magnifier.

We have designed a special set of MicroText fonts that are printable with a xerographic engine at a smaller than 1 point size. Figure 2a) shows an example of MicroText Mark. In comparison, Figures 2b) is a sample at identical scale of micro printing used in banknotes.

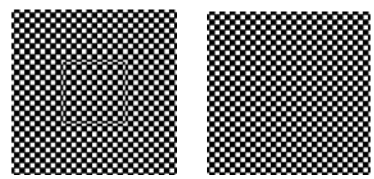
Figure 2*. a) (left) MicroText Mark; b) (right) micro text used in banknotes.*

4. Correlation Mark

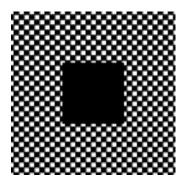
Like GlossMark®, Correlation Mark technology also produces images with two halftone screens of similar density/color characteristics, but different spatial details [4,5]. The hidden information is embedded by alternating the screens applied. It is not visible in normal viewing condition, but become obvious when the document is superimposed by a transparent "key" overley (see Figure 3).

Figure 3. *hidden Correlation Mark information becomes visible when superimposed by a key.*

The key is printed with a pattern that has different correlation factors with the two halftone screens. For example, it may be positively correlated with one screen and uncorrelated (or negatively correlated) with the second one. When superimposed, different correlations generate moiré of different strengths in foreground and background areas, and the hidden information becomes visible. This is illustrated in Figures 4a)-4c).



a) b)



c)

Figure 4*. a) exemplar halftone patterns; b) exemplar key; c)viewed with superimposed key.*

5. Guilloché Mark

Guilloché is also a standard feature to protect documents. It is used as background patterns on virtually all currency notes and passports. The Guilloché patterns are designed to be hard to reproduce, but at the same time, they are stationary, meaning every passport has the same pattern as all passports from that country, every monetary note has the same pattern as the same note from the country, any credit card has the same pattern, etc. Guilloché Mark provides a variable data version of Guilloché, where, for example, the credit card number is embedded in the Guilloché and thus every credit card has a different pattern (to a decoder) while having the identical human visual impression.

Guilloché Mark is composed of a set of “character patterns”, which resembles each other in general, but differ from each other in minute details. Each character pattern embeds a symbol, e.g. a character. The character patterns are derived from a common base pattern. The base pattern has the property that there is no artificial discontinuity if two base patterns are placed next to each other, whether in horizontal or vertical direction. The character patterns are generated by making subtle changes in the interior parts of the base pattern. An example of the base pattern is given in Figure 5a). Figures 5b)-5d) show three different character patterns. As the boundary portions of the character patterns are not altered, they can be seamlessly assembled to form seemly periodic Guilloché patterns.

a) b) c) d)

***Figure 5**. a) base pattern; b)-d) character patterns.*

Figure 6 shows an example for Guilloché Mark, in which the banking information is coded into the background Guilloché. The embedded information can be retrieved after the document is scanned and matched to a dictionary of the character patterns.

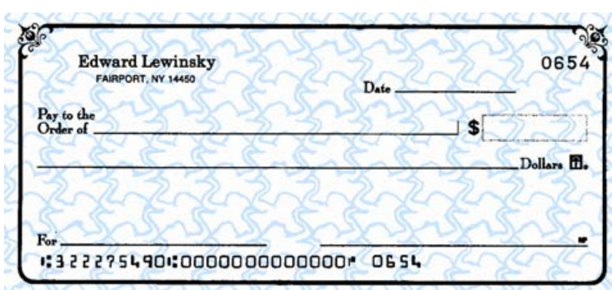


***Figure 6**. Exemplar Guilloché Mark.*

6. Florescent Mark

In traditional security printing, florescent effects are achieved by applying special dyes that show photo-excitation. The dyes fluoresce under ultraviolet (UV) light and show up as words, patterns or pictures and are typically invisible under normal lighting.

Florescent Mark does not rely on special dyes. It is based on the fact that most substrates used in standard digital color printing contain optical brightening agents that cause emission when exposed to a UV light source. Toner is an effective blocker of UV light, so a pattern with high toner area coverage will yield a low excitation. Florescent Mark applies different CMYK combinations or different halftone overlapping strategies to foreground and background regions thus modifying the respective area coverages. Both areas exhibit a close match in color under normal light, while producing visible luminance contrast under UV light. This is illustrated in Figure 7.

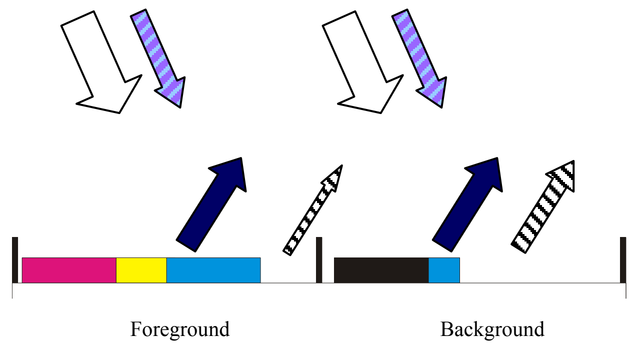


***Figure 7**. Different toners are used in foreground and background. They show same appearance under normal light (solid arrows), but different responses under UV (textured arrows).*

7. InfraRed Text

Similar to Florescent Mark, InfraRed Text requires only standard xerographic material. It is known that the black (K) toner commonly has different infrared absorption than the color (CMY) toners[6]. InfraRed Text is created by varying UCR/GCR (Under Color Removal / Gray Color Replacement) strategy to print a given color. Two different combinations of CMYK that give the same the appearance under normal illumination would appear different under IR illumination.

8. Conclusion

The rapid progresses in digital technologies provide both challenges and opportunities for security printing. In this paper, we presented several recently developed security features, which can be produced using standard xerographic equipment, materials, substrates and printing processes. The zero cost nature of the features extends the coverage of the security printing and makes protection of relatively low value documents, such as tickets and coupons affordable. In addition, these features can be easily individualized for each document thus creating “individualized security printing”. The sensitive information in the document such as name, identification number, dollar amount, can be protected by individually matching to the security features. Although the features proposed can be separately applied, a combination of them becomes extremely powerful.

References

1 F. Mintzer etal, “Effective and ineffective digital watermarks”, Proc. IEEE Int. Conf. Image Processing, vol. 3 Oct. 1997, pp. 9-13.

2 N. F. Johnson and S. Jajodia, “Exploring steganography: seeing the unseen”, IEEE Computer, vol 31, Feb. 1998, pp. 26-34.

3 B. Xu, S. G. Wang, C. Liu, “Glossmark®: An Inovative Digital Watermark”, Proc. ICISH’04, pp 252-255, Xian, China, Aug. 2004.

4 S. G. Wang, and K. T. Knox, “Embedding Digital Watermarks in Halftone Screens”, Proc. Electronic Imaging Conference, Jan. 2001.

5 Z. Fan, “Information Embedding Using Two-Layer Conjugate Screening”, Proc. Electronic Imaging Conference, Jan. 2004.

6 T. Bugnon, M. Brichon, and R. D. Hersch, “Model-Based Deduction of CMYK Surface Coverages from Visible and Infrared Spectral Measurements of Halftone Prints”, Proc. Electronic Imaging Conference, Jan. 2007.

Author Biography

Dr. Zhigang (Zeke) Fan joined Xerox Corporation Research and Technology in 1988 where he is currently a principal scientist. Dr. Fan’s research interests include various aspects of image processing and recognition. He has authored and co-authored more than 70 technical papers, as well as over 120 patents and pending applications. Dr. Fan is associate editor for the IEEE Transactions on Image Processing.

Reiner Eschbach is a Research Fellow at the Xerox Innovation Group. His research interests include color image processing, automatic image processing and security. He is the IS&T's 2003 Visiting Lecturer. He is also the former Editor of the Recent Progress Series of the IS&T as well as past Secretary and Publications Vice President of the IS&T Board of Directors. He is Associate Editor for the IEEE Trans. on Image Processing in the areas of scanning, display and printing; and a member of the SPIE Publications Committee.

Shen-ge Wang is a principal scientist with Xerox Corporation. He received a BS degree in Instrumental Mechanics from Changchun Institute of Optics, China and a Ph.D. degree in Optics from University of Rochester, respectively. His current research includes image processing, halftoning and printer modeling.

Raja Bala received the Ph.D. degree from Purdue University in Electrical Engineering. Since then, he has been employed at the Xerox Innovation Group, where he is a Principal Scientist conducting research in color science and color management. His research interests include device characterization, gamut-mapping, optimal color transformations, and novel imaging techniques utilizing spatial and spectral context. Raja has over 80 patents and publications in the field of color imaging, and is a member of IS&T