Document Forensics based on Steganographic Anti-Counterfeiting Markings and Mobile Architectures

F. P. Beekhof
University of Geneva
Beekhof@cui.unige.ch

S. Voloshynovskiy *
University of Geneva
Battelle Bat. A
7, route de Drize 1227
Carouge 4 Switzerland
svolos@cui.unige.ch

O. Koval
University of Geneva
Koval@cui.unige.ch

R. Villan
University of Geneva
Villan@cui.unige.ch

E. Topak
University of Geneva
Topak@cui.unige.ch

ABSTRACT

In this paper we present a feasibility study of printed document forensics based on steganographic anti-counterfeiting markings using portable devices. We propose two system architectures and analyze their pros and contres for mass usage. Furthermore, we perform an analysis of the probability of error that can be attained in the system based on steganographic anti-counterfeiting markings and explicit the conditions to reach reliable performance.

Categories and Subject Descriptors

E.4 [**Coding and Information Theory**]: Error Control Codes

Keywords

Yellow Dots, Document Security

1. INTRODUCTION

Despite the permanently increasing value and use of electronic information carriers in recent years, printed document still remain the most common and widely used form of information exchange and distribution in modern society. Many types of printed documents need to be secured by adding some specific features that allow efficient protection of their copyright, to trace the source of documents to specific printers, or to allow the investigation of counterfeiting and forgeries.

Historically, ways to secure printed documents include the use of special inks [4], special paper [15], anti-copying visible patterns [13], embedded holograms or microtext [14]. Besides a high cost of embedding, usually expensive equipment is required to perform a validation of a document that is protected in this way; thus rendering the cost prohibitive for some applications, as well as limiting the possibility of verification to a restricted circle of authorized parties. Moreover, most of these techniques are based on proprietary designs which considerably restrict the usage of cryptographic principles.

Several methods exist to embed information into a document which can be used to aid forensic analysis without being visible to the human eye. Embedding hidden data into text or images is an important topic of research, which can be found for example in the work of Voloshynovskiy et al. [18] on information-theoretic analyses of document authentication. Data-hiding in printed documents can be considered as an alternative to the above-mentioned non-informative protection methods, where secret information containing copyright information, time stamps, authenticity protection etc., is embedded into the document by modifying its semantic and syntactic content [18, 5, 8, 9] or its structural features, such as inter-symbol, inter-line or inter-word spaces, the positioning of the symbols, or the luminance of the printed characters [17, 1]. Several methods exist to embed information into a document which can be used to aid forensic analysis without being visible to the human eye.

Whilst being cheap at the embedding stage, which can usually be implemented at the software level and using commodity printers, the verification stage remains complicated and inconvenient for an ordinary user due to the necessity to exploit various scanning devices. Besides, these kinds of markings introduce various alterations into the document content and/or layout that might be not acceptable in some applications.

Recently, it was realized that the above security concerns can be addressed with a forensic analysis. Forensic techniques for printed documents can be classified in two groups: passive techniques that investigate intrinsic features of the document introduced by the printing process, and active techniques where an intrinsic signature is embedded by modulation of the parameters of this process.

*Contact Author

e-Forensics 2008, January 21-23, 2008, Adelaide, Australia.

In 2005, Buchanan et al. [2] published a study of microscopic imperfections of the surfaces of several kinds of documents, such as paper or plastic cards, using the diffuse scattering of a focused laser cast upon the document. It has been demonstrated that this is a robust and accurate method to identify documents.

Another approach by Mikkilineni et al. [12] consists in the study of the intrinsic signatures of printers, which are those features in the printed document that are characteristic for a particular printer, model, or product family.

An interesting method, proposed by Chiang et al. [3], is to embed information into a document by manipulating a laser printer to subtly control the banding to encode information. Banding is a kind of image artifact which is introduced during the printing process on a laser printer.

Another option is proposed by Villán et al. [16] and by Kamijo et al. [10], both describe the use of 2D barcodes, which can be printed on a document using special ink or other matter to hide the barcode.

In fact, intrinsic marking of documents has a longer history and start much earlier than in the end of the nineties. As was reported in [7], most color printers produce so-called "steganographic anti-counterfeiting markings". These markings are very small yellow dots [11] printed on paper by certain color laser printers, that were introduced as a way to aid law enforcement agencies to track the source of currency and tickets printed by counter-feiters on color laser printers (Figure 1).

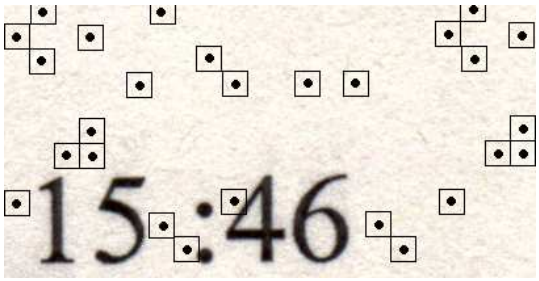

Figure 1: A fragment of a scanned document printed by an HP 4600dn containing steganographic anti-counterfeiting markings shown in black with a surrounding rectangle.

The existence and widespread application of this technology has been a cause of concern over privacy issues, given the possibilities to track and trace the origin of printed documents by any organization. We propose to take a positive view on the situation; given that these markings are present and cannot be controlled by the users of the printer, they can be put to good use, for example in the field of document security.

Thus, the main goal of the paper can be formulated in the following way: We would like to design a system able to trace back the source of a printed document based on the steganographic anti-counterfeiting system, which should be available for ordinary customers, and analyze its performance in terms of attainable probability of decoding error. Moreover, we would like to propose this service for users equipped with mobile phones with cameras.

The rest of the paper has the following structure: the general architecture of the system is proposed in Section 2, Section 3 presents an analysis of a steganographic anti-counterfeiting code produced by certain printer models manufactured by Xerox. Finally, Section 4 concludes the paper.

Notations We use capital letters to denote scalar random variables X, corresponding small letters x to denote their realizations. We use $X \sim p_X(x)$ or simply $X \sim p(x)$ to indicate that a random variable X is distributed according to $p_X(x)$.

2. PRINTED DOCUMENT FORENSIC ANALYSIS USING MOBILE PHONES

Recent and expected advances in the cameras built-in in most portable devices have made it possible to consider services offering automated document forensics with considerable ease and speed and without the use of special equipment, making forensic analysis available for almost every owner of a mobile phone.

Depending on the particular application scenario, two system architecture designs are proposed: a "portable-device-only" design and a "server-based" design. In the first case, depicted in Figure 2, a portable device is used for data acquisition, data processing, forensic analysis, and report generation. In other words, an image of the document is taken with a camera in a mobile phone, which is then processed by specialized software installed on the device, and the result of the performed test is provided to the customer in any available suitable form, for example as a text report, visualized on the screen or in audio through the speaker. In such a case, when the complete system is housed in a portable device, it is fully distributed and thus it is completely independent of any external resources and can be characterized by an enhanced security level. However, it would require adaptations to every phone, which are often different for every phone model.

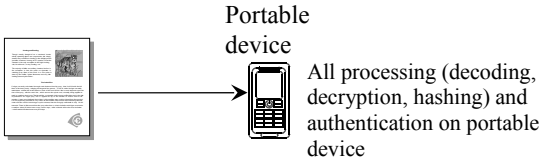

Figure 2: Schematic view of the portable-device-only solution.

In order to overcome this drawback, we consider the server-based solution shown in Figure 3. This scenario assumes the use of portable devices only for data-acquisition, communication and reporting. Contrary to the portable-device-only design, all the required data processing and report generation are performed on the server. Data is exchanged between these functional parts of the system via MMS, SMS, e-mail or any other suitable communication protocols.

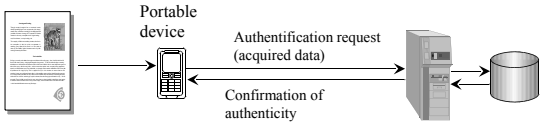

Figure 3: Schematic view of the server-based solution.

Taking into account the independence of the server-based solution of any particular model of mobile phone, we suggest to use it for the printed document forensic analysis based on steganographic anti-counterfeiting markings. It is assumed that images of documents are acquired by regular mobile phones equipped with a camera, which means that a key advantage of the general mobile architecture is its widespread availability without extra cost. The entire process is shown in more detail in Figure 4. We also assume that the forensic analysis of documents should be robust to variations in the parameters of camera image sensors and resolutions.

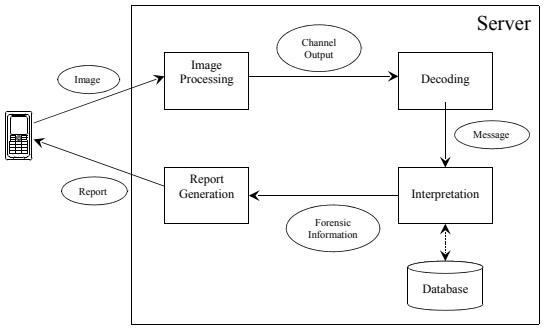

Figure 4: Schematic view of the mobile architecture in detail.

3. STEGANOGRAPHIC ANTI - COUNTERFEITING MARKINGS

In this section, we will investigate the feasibility and reliability of automated document forensic analysis using steganographic anti-counterfeiting markings.

3.1 The Xerox Docucolor Code

The Electronic Frontier Foundation describes the details of the code of yellow dots which are produced by Xerox DocuColor printers [6], see Figure 5. In this code, the dots carrying data are arranged in a rectangular pattern of 7 rows and 14 columns, augmented by a parity row and a parity column, making a total of 120 dots. This means that each data dot is associated with two parity dots, which means the code can be seen as a kind of Low-Density Parity-Check (LDPC) code. There is even a parity dot for the column which holds the parity dots for each row, which is not common in LDPC codes.

Only one codeword is present in every document, but the pattern representing this codeword is repeated throughout the entire document. Likewise, we speak of a dot when we refer to a single dot in a given pattern in a printed document, whereas we speak of a bit to indicate one bit of the codeword. This differentiation is justified because when the pattern is

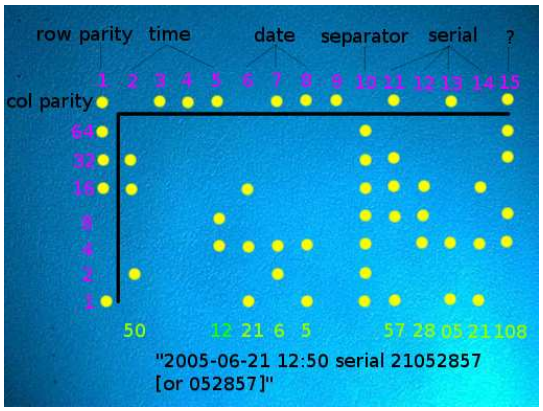

Figure 5: The code produced by Xerox DocuColor Printers, image courtesy of the Electronic Frontier Foundation.

repeated throughout the document, several dots in different patterns will refer to the same bit in the codeword.

Given a codeword, one can obtain another codeword by flipping at least four bits: 1) a data bit, 2) the corresponding column parity bit, 3) the corresponding row parity bit, and 4) the column parity bit of the row parity bits. A code with a Hamming distance of four can correct at most one erroneous bit without a residual probability of error. The robustness is further boosted by the fact that the pattern is repeated over an entire page, which is understandable given the desire to trace the source of a document when only a small part of it is available.

3.2 Performance Analysis

This section presents an analysis of the performance of the Xerox code where we will try to determine p_{error}, the probability that the decoding process fails to recover the embedded message.

3.2.1 The Channel

In this paper, we address only the hard coding regime, which means that the channel output is binary. We consider the problem of printed document forensics as channel coding problem. The channel is assumed to be a Binary Memoryless Channel, where the input is assumed to be generated by a random variable X and the channel output is given by a random variable Y. The model is depicted in Figure 6, where $e_0 = Pr(Y = 1|X = 0)$ and $e_1 = Pr(Y = 0|X = 1)$. In our

Figure 6: Model of the channel. For the analysis, a simplified model is used where both e_0 and e_1 are replaced by p_e.

the analysis, we use a simplified model where the channel is supposed to be a Memoryless Binary Symmetric Channel where the probability of a bit error is $p_e = max(e_0, e_1)$. Intuitively speaking, p_e represents the probability of misinterpreting a single dot on paper. Note that the p_{error} of the simplified channel is greater or equal to that of the asymmetric channel, thus p_{error} for the simplified channel is an upper bound for the first channel.

Let M be the number of times the pattern is repeated in the document. In our analysis, we will first investigate the decoding of a single pattern ($M = 1$), and then consider the influence of repetition ($M > 1$). For this purpose, we define p_{flip} as the probability of error of per bit in the received codeword to be decoded. Evidently, $p_{flip} = p_e$ for $M = 1$; for $M > 1$ we will show that p_{flip} is a function of M and p_e.

3.2.2 Probability of Erroneous Transmission Given p_{flip}

Recall that at most one erroneous bit is tolerated in each received codeword, that contains $N = 120$ bits, and the probability for each individual bit to be erroneous is p_{flip}. The number of flipped bits is a random variable F distributed according to a Binomial probability distribution function, i.e., $F \sim Bin(N, p_{flip})$:

$$p_F(f) = \binom{N}{f} p_{flip}^f \Big(1 - p_{flip}\Big)^{N-f}. \quad (1)$$

Given that either zero or one erroneous bit is acceptable, one obtains the probability of error during decoding:

$$p_{error} = 1 - (1 - p_{flip})^{120} - 120 p_{flip}(1 - p_{flip})^{119}. \quad (2)$$

The only free variable in the equation is p_{flip}, which will be investigated in further detail.

3.2.3 Repetitions and p_{flip}

If the pattern is repeated in the image, one can select the value of a bit based on a majority vote. As said, if only one pattern is present in an image under investigation, then the probability of a bit-error is equal to the chance of falsely interpreting a single dot on paper; i.e., if $M = 1$, then $p_{flip} = p_e$.

Otherwise, p_{flip} is the probability that a single bit is misinterpreted, i.e., the chance that the correctly detected dots do not form a majority. Let K be a random variable representing the number of wrongly detected dots corresponding to a given bit, then K is also Binomially distributed, i.e., $K \sim Bin(M, p_e)$ and $p_{flip} = Pr(K < \frac{M}{2})$.

Unfortunately, majority voting is different for even and odd values of M. Thus, we define m as the maximum allowed number of wrongly detected dots:

$$m = \begin{cases} \frac{M}{2} - 1 & \text{for } M \text{ is even,} \\ \lfloor \frac{M}{2} \rfloor & \text{for } M \text{ is odd.} \end{cases} \quad (3)$$

Let k be a particular realization of K, then p_{flip} can be computed as:

$$p_{flip} = 1 - \sum_{k=0}^{m} \binom{M}{k} p_e^k \Big(1 - p_e\Big)^{M-k}. \quad (4)$$

Once p_{flip} is computed for a given M and p_e, it can be substituted in (2) to compute p_{error}.

3.2.4 Resulting p_{error}

Given that p_{error} is a function of p_{flip} and p_{flip} is a function of M and p_e, it follows that p_{error} is in fact a function of M and p_e. Figure 7 shows p_{error} for different values of M and p_e. It is interesting to see that there are essentially two regions; one where errorless transmission is almost guaranteed, and one where errorless transmission is practically impossible. There is only a small "gray" area where success is uncertain.

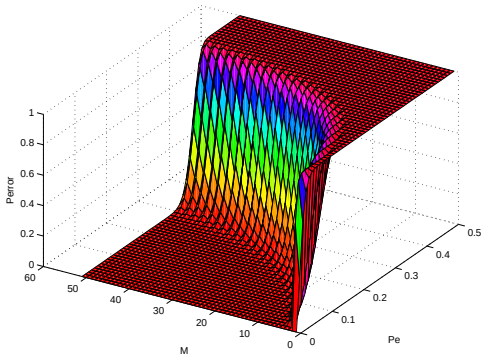

Figure 7: The probability of wrongly decoding the pattern, p_{error}; as a function of M, the number of repetitions, and the probability of erroneous detection of a single dot on paper, p_e.

The conditions for reliable operations can be characterized as follows. When $M < 5$, reliable operations cannot to be expected for almost any value of p_e. The situation rapidly improves for values of M between 10 and 30, where successful operations can be expected for increasing values of p_e. For M greater than 30, the reliability does not seem to improve significantly any more.

3.2.5 Requirements for Practical Use

In practice, the number of repetitions M depends mainly on the size of the area of the document that is in the image. The probability of correctly determining the presence of a dot depends on numerous hardly predictable circumstances: the lighting conditions, the quality of the camera in the mobile device, whether or not the photographer managed to avoid moving the camera whilst pressing the shutter, et cetera. Fortunately, the only technical matter is the quality of the camera, which, as has been pointed out in the introduction, is steadily improving.

3.3 Expected Benefits

Depending on the particular type of markings on a document, one may expect to be able to derive the vendor, the manufacturer and the model or family. In some cases, even the serial number of the printer and the time and date may be available.

For a malicious person, it is not trivial to produce "fake" dots or to remove them from the original. Using a color printer to make fake dots or to copy an original document inherently introduces interference between the fake dots and the dots produced by the printer itself, albeit some models exists that do not produce dots.

Likewise, a regular non-color copy machine or printer can be used to make copies of an original document, but the

markings will not appear. Thus, if such a document is found, it is trivial to prove it is not an original.

4. CONCLUSION

In this paper we consider the problem of forensics of printed documents based on steganographic anti-counterfeiting markings and portable devices. In particular, we proposed two forensic system architectures, i.e., the portable-device-only solution where the entire verification process including printed document acquisition, necessary data processing and forensic report generation is fully organized on a mobile device, and the server-based design where the portable device is used only for acquisition and report generation purposes. We analyze the particularities of both architectures and suggest to exploit the latter for mass use. Furthermore, in order to reveal the accuracy of the forensic analysis based on steganographic anti-counterfeiting markings, we investigated the probability of error of the intrinsic pattern decoding and underlined the influence of the pattern repetition in the body of the document on system reliability.

Acknowledgments

This paper was partially supported by SNF Professeur Boursier grants PP002 – 68653, 114613 and 200021–111643, by the European Commission through the IST Programme under contract IST – 2002 – 507932 – ECRYPT, FP6 – 507609 – SIMILAR and Swiss IM2 projects.

The information in this document reflects only the authors views, is provided as is and no guarantee or warranty is given that the it is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

5. REFERENCES

[1] P. V. Borges and J. Mayer. Document watermarking via character luminance modulation. In *ICASSP 2006 Proceedings, IEEE International Conference on Acoustics, Speech and Signal Processing*, volume 2, pages 317–320, May 2006.

[2] J. D. R. Buchanan, R. P. Cowburn, A.-V. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, and M. T. Bryan. Forgery: 'fingerprinting' documents and packaging. *Nature*, 436(7050):475–475, 2005.

[3] P.-J. Chiang, G. N. Ali, A. K. Mikkilineni, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp. Extrinsic signatures embedding using exposure modulation for information hiding and secure printing in electrophotographic devices. *Proceedings of the IS&T's NIP21: International Conference on Digital Printing Technologies*, 20:295–300, October/November 2004.

[4] I. Cox, M. L. Miller, and J. A. Bloom. *Digital watermarking*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2002.

[5] E. J. Delp. Is your document safe: An overview of document and print security. In *IS&Ts NIP18: International Conference on Digital Printing Technologies*, pages 0–0, September 2002.

[6] Electronic Frontier Foundation. Docucolor tracking dot decoding guide. *http://www.eff.org/Privacy/printers/docucolor/*, 2005.

[7] Electronic Frontier Foundation. Is your printer spying on you ? *http://www.eff.org/Privacy/printers/*, 2005.

[8] A. Eskicioglu and E. Delp. An overview of multimedia content protection in consumer electronics devices. *Signal Processing: Image Communication*, 16:681–699, 2000.

[9] A. Eskicioglu, J. Town, and E. Delp. Security of digital entertainment content from creation to consumption. *Signal Processing: Image Communication*, March 2003.

[10] K. Kamijo, N. Kamijo, and M. Sakamoto. Electronic clipping system with invisible barcodes. In *MULTIMEDIA '06: Proceedings of the 14th annual ACM international conference on Multimedia*, pages 753–762, New York, NY, USA, 2006. ACM Press.

[11] P. K. Mazaika. Method for invisible embedded data using yellow glyphs. *US Patent 6,708,894 B2*, March 2004.

[12] A. K. Mikkilineni, O. Arslan, P.-J. Chiang, R. M. Kumontoy, J. P. Allebach, G. T.-C. Chiu, and E. J. Delp. Printer forensics using svm techniques. *Proceedings of the IS&T's NIP21: International Conference on Digital Printing Technologies*, 21:223–226, October 2005.

[13] J. Picard. Digital authentication with copy-detection patterns. In R. L. van Renesse, editor, *Optical Security and Counterfeit Deterrence Techniques V. Edited by van Renesse, Rudolf L. Proceedings of the SPIE, Volume 5310, pp. 176-183 (2004).*, pages 176–183, June 2004.

[14] R. A. Steenblik and M. J. Hurt. Unison micro-optic security film. In R. L. van Renesse, editor, *Optical Security and Counterfeit Deterrence Techniques V. Edited by van Renesse, Rudolf L. Proceedings of the SPIE, Volume 5310, pp. 321-327 (2004).*, pages 321–327, June 2004.

[15] R. L. van Renesse. Paper based document security – a review. In *Proceedings of the European Conference on Security and Detection*, pages 75–80, April 1997.

[16] R. Villán, S. Voloshynovskiy, O. Koval, and T. Pun. Multilevel 2D Bar Codes: Towards High Capacity Storage Modules for Multimedia Security and Management. *IEEE Transactions on Information Forensics and Security*, 1(4):405–420, December 2006.

[17] R. Villán, S. Voloshynovskiy, O. Koval, J. Vila-Forcén, E. Topak, F. Deguillaume, Y. Rytsar, and T. Pun. Text Data-Hiding for Digital and Printed Documents: Theoretical and Practical Considerations. In *Proceedings of SPIE-IS&T Electronic Imaging 2006, Security, Steganography, and Watermarking of Multimedia Contents VIII*, San Jose, USA, January 15–19 2006.

[18] S. Voloshynovskiy, O. Koval, R. Villán, E. Topak, J. Vila-Forcén, F. Deguillaume, Y. Rytsar, and T. Pun. Information-Theoretic Analysis of Electronic and Printed Document Authentication. In *Proceedings of SPIE-IS&T Electronic Imaging 2006, Security, Steganography, and Watermarking of Multimedia Contents VIII*, San Jose, USA, January 15–19 2006.