AUTHENTICATION USING GRAPHICAL CODES: OPTIMISATION OF THE PRINT AND SCAN CHANNELS

A-T. Phan Ho, B-A Mai Hoang, W. Sawaya

Institut Mines-Telecom, TELECOM-Lille
LAGIS UMR 8219 CNRS
Rue Guglielmo Marconi
59000 Villeneuve d'Ascq, France

P. Bas

LAGIS UMR 8219 CNRS
Ecole Centrale de Lille, Cité Scientifique
59651 Villeneuve d'Ascq, France

ABSTRACT

In this paper we propose to cast the problem of authentication of printed documents using binary codes into an optimization game between the legitimate source and the opponent, each player tries to select the best print and scan channel to minimize/maximize his authentication performance. It is possible to solve this game by considering accurate computations of the type I and type II probability errors and by using additive stochastic processes to model the print and scan channel.

Considering the print and scan models as Lognormal or Generalized gaussian additive processes, we maximize the authentication performances for two different security scenarios. The first one considers the opponent as passive and assumes that his print-and-scan channel is the same as the legitimate channel. The second scenario devises a minimax game where an active opponent tries to maximize the probability of non-detection by choosing appropriate parameters on his channel. Our first conclusions are the facts that (i) the authentication performance is better for dense noises than for sparse noises for both scenarios, and (ii) for both families of distribution, the opponent optimal parameters are close to the legitimate source parameters, and (iii) the legitimate source can find a configuration which maximizes the authentication performance.

Index Terms— Authentication, Hypothesis testing, minimax game, print and scan models.

1. INTRODUCTION

The authentication of printed materials, which consists in bringing a forensic evidence that materials are genuine, is a huge challenge nowadays and can be used to prevent forgeries of valuable items, such as identity documents, or products, such as drugs by securing their associated packages. Authentication can be done either 1) by characterizing the "fingerprint" of the package, for example by recording the random patterns of the fiber of the package or the paper [1], but such a system is practically heavy to deploy since each product needs to be linked to its high definition capture stored in a database, or 2) by relying on the degradation induced by the interaction between the materials and a physical process such as printing, marking, embossing or carving. Since both the physical process and the matter are stochastic, the interaction between the two entities can be considered as a Physically Unclonable Function (PUF) [2] that cannot be reproduced by the forger and can consequently be used to perform authentication.

We study here the authentication system first proposed by [3], and based on the use of a printed binary code to perform authentication. The whole system is depicted in Figure 1: the legitimate source prints an original secret random code x^N (a binary matrix of N elements) on a document or a package and the receiver scans it to perform authentication as the opponent may have manufactured his forgery and generates his copied code. In order to generate this copy, the opponent observes the printed and scanned version y^N of x^N (step 1 in Figure 1) and extracts a binary code $\hat{x}^N$ (step 2). This step is unavoidable due to the fact that an industrial offset printer can only use binary input to generate dots of inks. With this second print and scan process, the copied code z^N generated by the opponent (step 3) has a different distribution than the initial printed and scanned code y^N. This distinction drives the authentication system (step 4).

2. PRINT AND SCAN MODELS AND AUTHENTICATION

2.1. Principle of the authentication system

The legitimate receiver observes a gray level code o^N, and we assume that the random observed sequence $(O^N \mid x^N)$ (conditioned to the secretly shared binary code x^N) is independent and identically distributed (i.i.d.). The Neyman Pearson test is expressed as:

$$L = \log \frac{P(o^N \mid x^N, H_1)}{P(o^N \mid x^N, H_0)} \underset{H0}{\overset{H1}{\gtrless}} \lambda. \qquad (1)$$

where H_0 is the hypothesis that the observed sequence comes from an original source with distribution $P(O \mid x\,, H_0)$, and

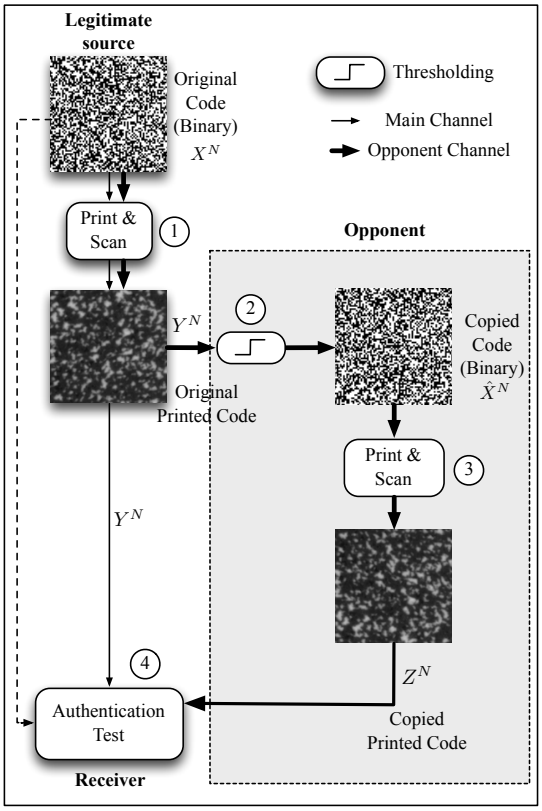

Fig. 1. Principle of authentication using graphical codes.

H_1 is the hypothesis that the observed sequence is a fake and have distribution $P(O \mid x,\, H_1)$. Practically, distribution $P(O \mid x\,,\, H_0)$ models one print and scan process used by the legitimate parts, whereas $P(O \mid x\,,\, H_1)$ is the distribution modeling the decoder, the printer used by the opponent part, and the scanner of the legitimate receiver.

2.2. Asymptotic expressions of α and β

Before considering our optimization game in section 3, we recall [4], where a method to compute reliably type I error probability α (the probability to consider a genuine code as a copy) and type II error probability β (the probability to not detect a copy) has been presented. Contrary to the Gaussian approximation of L which provides inaccurate error probabilities when the threshold λ in (1) is far from its the mean value, this solution uses the Chernoff bound [5] as very small error probabilities of type I and II may be desired [6]. For i.i.d. random sequences, the distribution of the random variable $L = \sum_i \ell(O_i/x_i)$ depends on the origin (H_0 or H_1) of the observed code o^N, and for any real number s, the semi-invariant moment generating function of each $\ell(O_i/x_i)$ is $\mu_\ell(s;\, H_j) = \sum_{x=0,1} \mu_{\ell/x}(s;\, H_j) = \sum_{x=0,1} \log E_{O|x,H_j}\left[e^{s\ell(O/x)}\right]$. Type I and II errors may then be tightly expressed for sufficiently large N (with approximately $N/2$ white and $N/2$ black dots), as:

$$\begin{aligned} \alpha \quad &= \quad \Pr(L \geq \lambda \mid H_0), \\ &\underset{N\to\infty}{\to} \quad \frac{1}{\tilde{s}_0\sqrt{N\pi\mu''_\ell(\tilde{s}_0;\, H_0)}} e^{\frac{N}{2}\left[\mu_\ell(\tilde{s}_0;\, H_0) - \tilde{s}_0\mu'_\ell(\tilde{s}_0\,;\, H_0)\right]}. \end{aligned} \tag{2}$$

and

$$\begin{aligned} \beta \quad &= \quad \Pr(L \leq \lambda \mid H_1), \\ &\underset{N\to\infty}{\to} \quad \frac{1}{|\tilde{s}_1|\sqrt{N\pi\mu''_\ell((\tilde{s}_1;\, H_1)}} e^{\frac{N}{2}\left[\mu_\ell(\tilde{s}_1;\, H_1) - \tilde{s}_1\mu'_\ell(\tilde{s}_1\,;\, H_1)\right]}. \end{aligned} \tag{3}$$

where $\mu'_\ell(\tilde{s}_j;\, H_j)$ and $\mu''_\ell(\tilde{s}_j;\, H_j)$ are respectively the first and second derivatives of $\mu_\ell(s;\, H_j)$ at value $\tilde{s}_j$ such that $\frac{N}{2}\mu'_\ell(s;\, H_j) = \lambda$.

2.3. Models for the print and scan channel

In this paper we use two different families of distributions to model the print and scan channel, but the general methodology of this paper does not depend on the model and can still be applied.

The first one is the Generalized Gaussian distribution which has been chosen because it can model both sparse and dense distributions. The second one is the Lognormal distribution since it has been previously shown by Baras and Cayre [7] that this distribution is an accurate model of the print and scan channel. Note that other print and scan models based on the gamma transfer function or additive noise with input dependent variance can be found in [8].

The distribution $T_{V|x}(v \mid x)$ modeling the physical device, i.e. the association of a printer with a scanner, can be written as (for x taking binary values):

- For the Generalized Gaussian distribution:

$$p(v \mid x) = \frac{b}{2a\Gamma(1/b)} e^{-(|v-m(x)|/a)^b}, \tag{4}$$

where $\Gamma(\cdot)$ is the gamma function, $m(x)$ the mean, and parameters a can be computed for a given variance $\sigma^2(x) = \mathrm{var}[V \mid x]$:

$$a = \sqrt{\sigma(x)\Gamma(1/b)/\Gamma(3/b)}. \tag{5}$$

The parameter b is used to control the sparsity of the the distribution, for example when $b = 1$ the distribution is Laplacian, $b = 2$ the distribution is Gaussian, and $b \to +\infty$ the distribution is uniform.

- For the Lognormal distribution:

$$p(v \mid x) = \frac{1}{vs(x)\sqrt{2\pi}} e^{-\frac{(\log v - m(x))^2}{2s^2(x)}}, \tag{6}$$

where $\log(V \mid x)$ has a Gaussian distribution with mean $m(x)$ and variance $s^2(x)$. The mode of the distribution is $M(x) = e^{m(x)-s^2(x)}$, and the variance is given by $\sigma^2(x) = (e^{s^2(x)} - 1)e^{2m(x)+s(x)^2}$.

To provide values within $[0, \ldots, 255]$ to model a scanning process, we quantize and truncate distributions (4) and (6) . Each channel is parametrized by 4 parameters, 2 per each type of dots. For the Generalized Gaussian distribution the parameters are $m(0)$ and $\sigma(0)$ for black dots and $m(1)$ and $\sigma(1)$ for white dots. The Lognormal distribution can be parametrized by the standard deviations $\sigma(0)$ and $\sigma(1)$ and the modes $M(0)$ and $M(1)$ respectively for black and white dots.

Figure 2 illustrates different realizations X^N, $\hat{X}^N$, Y^N and Z^Nin the case of a Generalized Gaussian distribution when the main and the opponent channels have the same mean and variance, for $b = 1$ (Laplacian distribution), $b = 2$ (Gaussian distribution) and $b = 6$, i.e. close to a uniform distribution. Figure 3 depicts truncated Lognormal distributions having same modes but different standard deviations.

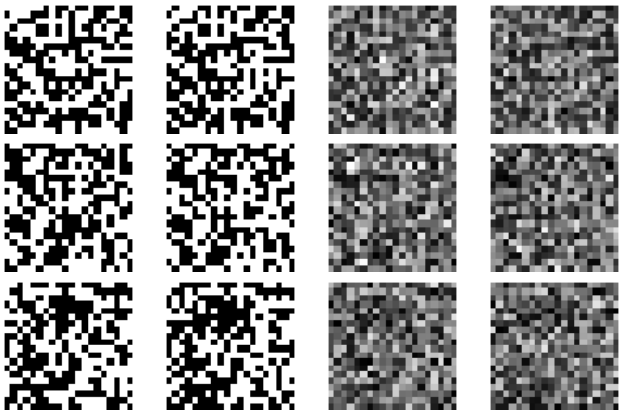

Fig. 2. Example of a 20x20 code which is printed and scanned by an opponent following a Generalized Gaussian distribution for $b = 1$ (first row), $b = 2$ (second row) and $b = 6$ (third row). Columns (a), (b), (c), (d) represent respectively X^N, $\hat{X}^N$, Y^N and Z^N. Main and opponent channels are identical with $m(0) = 50$, $m(1) = 150$, $\sigma(0) = 40$, $\sigma(1) = 40$.

3. OPTIMAL CONFIGURATIONS FOR AUTHENTICATION

This authentication problem can be seen as a game where the main goal of the designer of the authentication system is, for a given false alarm probability α, to find a channel that minimizes the probability of misdetection β.

Practically this means that the channel can be chosen by using a given quality of paper, an ink of appropriate density and/or by adopting a given resolution. For example if the legitimate source wants to decrease the noise variance, he can choose to use oversampling to replicate the dots, on the contrary if the legitimate source wants to increase the noise variance, he can use a paper of lesser quality. It is important to recall that because the opponent will have to print a binary version of its observation, and because a printing device at this very high resolution can only print binary images, the opponent will in any case have to print with decoding errors after estimation $\hat{X}$.

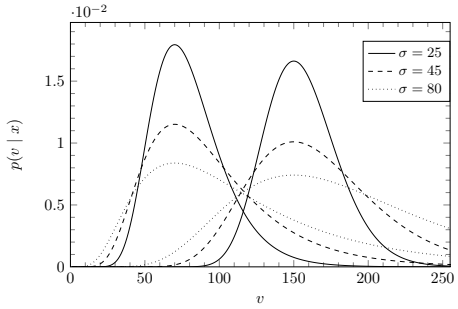

Fig. 3. Representation of the print and scan model for the black dots (on the left) and the white parts of the paper (on the right) for different standard deviations $\sigma(0) = \sigma(1) = \sigma$ with $M(0) = 70$ and $M(1) = 150$ for the Lognormal distribution.

We analyze two scenarios described below:

- The legitimate source and the opponent have identical printing devices (by devices we mean printer, ink, paper, scanner), practically this means that they use exactly the same printing setup. In this case the legitimate source will try to look for the channel $\mathcal{C}$ such that for a given α, the legitimate party will have a probability of misdetection β^* such that:

$$\beta^* = \min_{\mathcal{C}} \beta(\alpha). \tag{7}$$

  In this case, the opponent is defined to be passive.

- The opponent can modify its printing channel $\mathcal{C}_o$, practically it means that he can modify one or several parameters of his printing setup. Actually, we assume that he changes the variance of its noise given that it will be the most efficient way for him to confuse the receiver. The opponent thus tries to maximize the probability of misdetection by choosing his adequate printing channel, whereas the legitimate source will adopt a printing channel $\mathcal{C}_l$ which minimizes the probability of misdetection. We end up with so-called a min-max game in game theory, where the optimal β^* is the solution of:

$$\beta^* = \min_{\mathcal{C}_l} \max_{\mathcal{C}_o} \beta(\alpha). \tag{8}$$

  In this case the opponent is active since he tries to adapt his strategy in order to degrade the authentication performance.

For the Generalized Gaussian model and the Lognormal model, we assume that, respectively, the means $m(0)$ and $m(1)$, and the modes $M(0)$ and $M(1)$ are constant for all the players in the different channels (which implies that the scanning process has the same calibration for the two types of images). We assume also that variances of black and whites dots are equal at each channel and denote them σ_m^2 and σ_o^2 for main and opponent respectively..

3.1. Passive opponent

Here the opponent undergoes a channel identical to the main channel. The only parameter of the optimization problem (7) is consequently σ_m. Figure 4.a and Figure 4.b present respectively the evolution of β w.r.t. σ_m for $\alpha = 10^{-6}$ with $m(0) = 50$, $m(1) = 150$ for the Gaussian channel, and with different modes for the Lognormal distribution.

For each channel configuration, we can find an optimal configuration, this configuration offers a smaller probability of error for $b = 6$ than for $b = 2$ or $b = 1$.

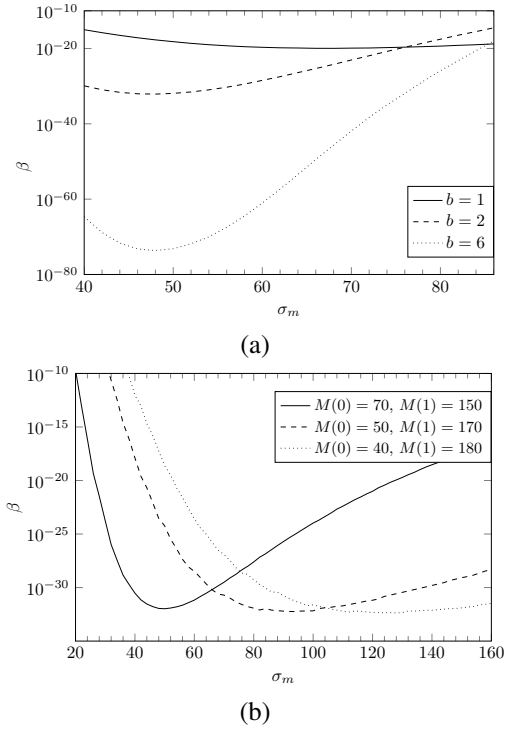

Fig. 4. Evolution of the probability of non detection w.r.t the standard deviation of the channel ($\alpha = 10^{-6}$) for the Generalized Gaussian distribution (a), and Lognormal distribution (b).

3.2. Active opponent

In this setup the opponent can tune his variance σ_o^2 to confuse the receiver with the higher β. Figure 5.a shows the evolutions of β w.r.t σ_o for different σ_m when a Generalized Gaussian channel is assumed. We can see that in each case it's in the opponent interest to optimize his channel.

Figures 5.b and 5.c shows the evolution of the best opponent strategy $\max_{\sigma_o} \beta$ w.r.t σ_m. By comparing it with Figure 4, we can see that the opponent's probability of non detection can be multiplied by one or several orders of magnitude for the Generalized Gaussian distribution ($\times 10^6$ for $b = 1$, $\times 10^5$ for $b = 2$) or for the Lognormal distribution ($\times 10^5$ for each mode separation) but stays the same when the distribution is close to uniform ($b = 6$).

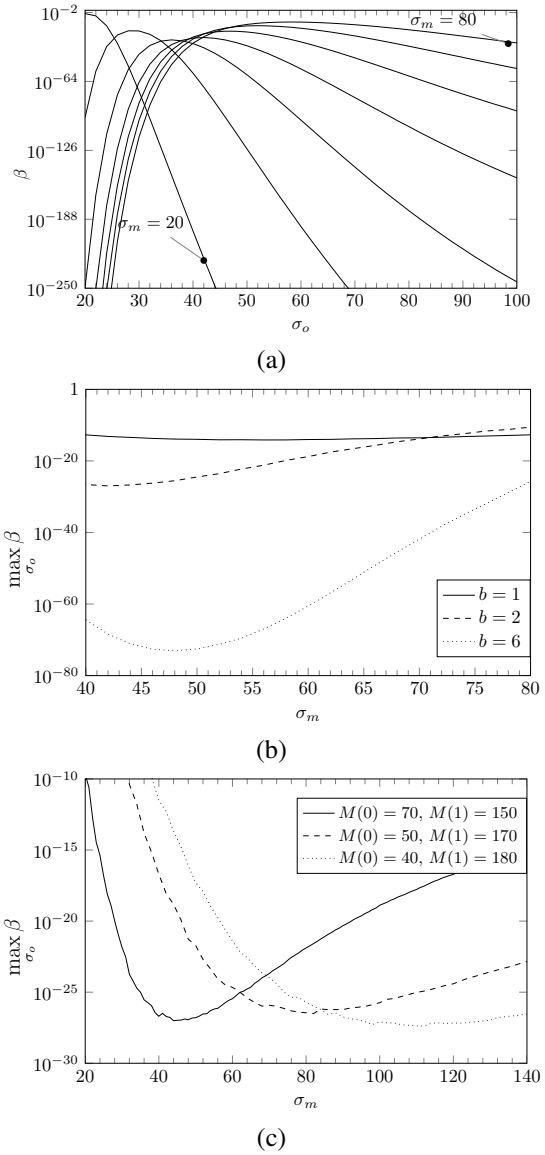

Fig. 5. Evolution of opponent strategy β for the Generalized Gaussian distribution for $b = 2$ (a), and the best opponent strategy $\max(\beta)$ w.r.t the standard deviation of the channel ($\alpha = 10^{-6}$) for the Generalized Gaussian distribution (b) and the for the Lognormal distribution (c).

3.3. Analysis

When facing a passive opponent, it is not surprising to notice that in each case β is important whenever σ_m is very small, i.e. when the print and scan noise is negligible hence the estimation of the original code by the opponent is easy; or very large; i.e. when the print and scan noise is so important that the original and forgery become equally noisy. The legitimate source will consequently avoid a channel that generates noise of very small or very large variance.

For an active opponent, the active scenario offers a saddle point satisfying (8) either for Generalized Gaussian or Lognormal distribution. This means that even if the adversary owns ideally perfect print and scan devices ($\sigma_o \to 0$, $o^N = \hat{x}^N$), it is not to his advantage to use it since the authentication is still efficient due to the decoding errors he will create by generating the binary code $\hat{X}^N$.

Another general remark is to notice that the optimal opponent parameters are very close to the optimal parameters of the passive scenario, which means that the adversary has little room to maneuver when choosing his best attack (see Figures 4 (a) and 5 (b,c)) and nearly no room when the noise is close to uniform ($b = 6$).

For Generalized Gaussian distribution, it is important to notice that for distributions of same variance, dense distributions yields to better authentication performance than sparse distributions for both scenarios (see Figures 4 (a) and 5 (b)). This is due to the fact that a distribution close to uniform tend to create a bigger overlap between the two decision regions than a sparse distribution that will generate codes mainly lying in the original one.

For the Lognormal distribution we can notice that the authentication performances are similar for different values of modes, both for a passive and an active opponent (see Figures 4 (b) and 5 (c)). However, the larger the difference, the larger the optimal standard deviation, which means that it is in the designer strategy to force the opponent to generate decoding errors in this case.

4. CONCLUSIONS AND PERSPECTIVES

In this paper we have proposed to cast the problem of authentication of printed documents using binary codes into an optimization game between the legitimate source and the opponent, each player potentially tries to select the best print and scan channel to minimize/maximize his authentication performance. This game was possible by considering accurate computations of the type I and type II probability errors and by using additive stochastic processes to model the print and scan channel.

We have shown that for both the Generalized and Lognormal distributions the game can be tractable, and that it is in the interest of the legitimate source to adopt a channel which is close to the uniform distribution.

Our future work will consist in finding, using information theoretic arguments, what can be the best additive channel for this setup.

5. ACKNOWLEDGEMENTS

This work was partly supported by the National French project ANR-10-CORD-019 “Estampille”.

REFERENCES

[1] T. Haist and H.J. Tiziani. Optical detection of random features for high security applications. *Optics communications*, 147(1-3):173–179, 1998.

[2] G.E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th annual Design Automation Conference*, pages 9–14. ACM, 2007.

[3] J. Picard. Digital authentication with copy-detection patterns. In *Electronic Imaging 2004*, pages 176–183. International Society for Optics and Photonics, 2004.

[4] A-T. Phan Ho, B-A. Hoang Mai, W. Sawaya, and P. Bas. Document Authentication Using Graphical Codes: Impacts of the Channel Model. In *ACM Workshop on Information Hiding and Multimedia Security*, pages ACM 978–1–4503–2081–8/13/06, Montpellier, France, June 2013.

[5] A. Dembo and Z. Ofer. *Large deviations techniques and applications*, volume 38 of *Stochastic Modelling and Applied Probability*. Springer, 2010.

[6] R.G. Gallager. *Information theory and reliable communication*, volume 15. Wiley, 1968.

[7] C. Baras and F. Cayre. Towards a realistic channel model for security analysis of authentication using graphical codes. In *Information Forensics and Security (WIFS), 2013 IEEE International Workshop on*, pages 115–119. IEEE, 2013.

[8] C.-Y. Lin and S.-F. Chang. Distortion modeling and invariant extraction for digital image print-and-scan process. In *Proceedings of International Symposium on Multimedia*, 1999.