EURASIP Journal on Information Security
a SpringerOpen Journal

RESEARCH Open Access

Document authentication using graphical codes: reliable performance analysis and channel optimization

Anh Thu Phan Ho[1*], Bao An Mai Hoang[2], Wadih Sawaya[1] and Patrick Bas[3]

Abstract

This paper proposes to investigate the impact of the channel model for authentication systems based on codes that are corrupted by a physically unclonable noise such as the one emitted by a printing process. The core of such a system for the receiver is to perform a statistical test in order to recognize and accept an original code corrupted by noise and reject any illegal copy or a counterfeit. This study highlights the fact that the probability of type I and type II errors can be better approximated, by several orders of magnitude, when using the Cramér-Chernoff theorem instead of a Gaussian approximation. The practical computation of these error probabilities is also possible using Monte Carlo simulations combined with the importance sampling method. By deriving the optimal test within a Neyman-Pearson setup, a first theoretical analysis shows that a thresholding of the received code induces a loss of performance. A second analysis proposes to find the best parameters of the channels involved in the model in order to maximize the authentication performance. This is possible not only when the opponent's channel is identical to the legitimate channel but also when the opponent's channel is different, leading this time to a min-max game between the two players. Finally, we evaluate the impact of an uncertainty for the receiver on the opponent channel, and we show that the authentication is still possible whenever the receiver can observe forged codes and uses them to estimate the parameters of the model.

1 Introduction

The problem of authentication of physical products such as documents, goods, drugs, and jewels is a major concern in a world of global exchanges. The World Health Organization in 2005 claimed that nearly 25% of medicines in developing countries are forgeries [1], and according to the Organization for Economic Co-operation and Development (OECD), international trade in counterfeit and pirated goods reached more than US$250 billion in 2009 [2].

1.1 Addressed problem and related works

Authentication of physical products is generally done by using the stochastic structure of either the materials that composes the product or of a printed package associated to it. Authentication can be performed for example by recording the random patterns of the fiber of a paper [3], 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. Another solution is to rely on the degradation induced by the interaction between the product and a physical process such as printing, marking, embossing, carving, etc. Because of both the defaults of the physical process and the stochastic nature of the matter, this interaction can be considered as a physically unclonable function (PUF) [4] that cannot be reproduced by the forger and can consequently be used to perform authentication. In [5], the authors measure the degradation of the inks within printed color tiles and use discrepancy between the statistics of the authentic and print-and-scan tiles to perform authentication. Other marking techniques can also be used; in [6], the authors propose to characterize the random profiles of laser marks on materials such as metals (the technique is called LPUF for laser-written PUF) to use them as authentication features.

*Correspondence: phanho@telecom-lille.fr
[1] Institut-Telecom-LAGIS, Telecom-Lille, Rue Guglielmo Marconi, Villeneuve-d'Ascq 59650, France
Full list of author information is available at the end of the article

We study in this paper an authentication system which uses the fact that a printing process at very high resolution can be seen as a stochastic process due to the nature of different elements such as the paper fibers, the ink heterogeneity, or the dot addressability of the printer. Such an authentication system has been proposed by Picard et al. [7,8] and uses 2D pseudo-random binary codes that are printed at the native resolution of the printer (2,400 dpi on a standard offset printer or 812 dpi on a digital HP Indigo printer).

The principle of the studied system in this paper is depicted in Figure 1:

- The original code is secretly exchanged between the legitimate source and the receiver.
- Once printed on a package to be authenticated, the degraded code will be scanned then thresholded by an opponent (the forger). It is important to note that at this stage thresholding is necessary for the opponent because the industrial printers can only print dots, e.g., binary versions of the scanned code.
- The opponent then produces a printed copy of the original code to manufacture his forgery.
- The receiver performs a test on an observed scanned code, being either the scanned version of the original printed code or the scanned version of the fake code. Using his knowledge on the original code, he establishes a statistical test in order to perform authentication.

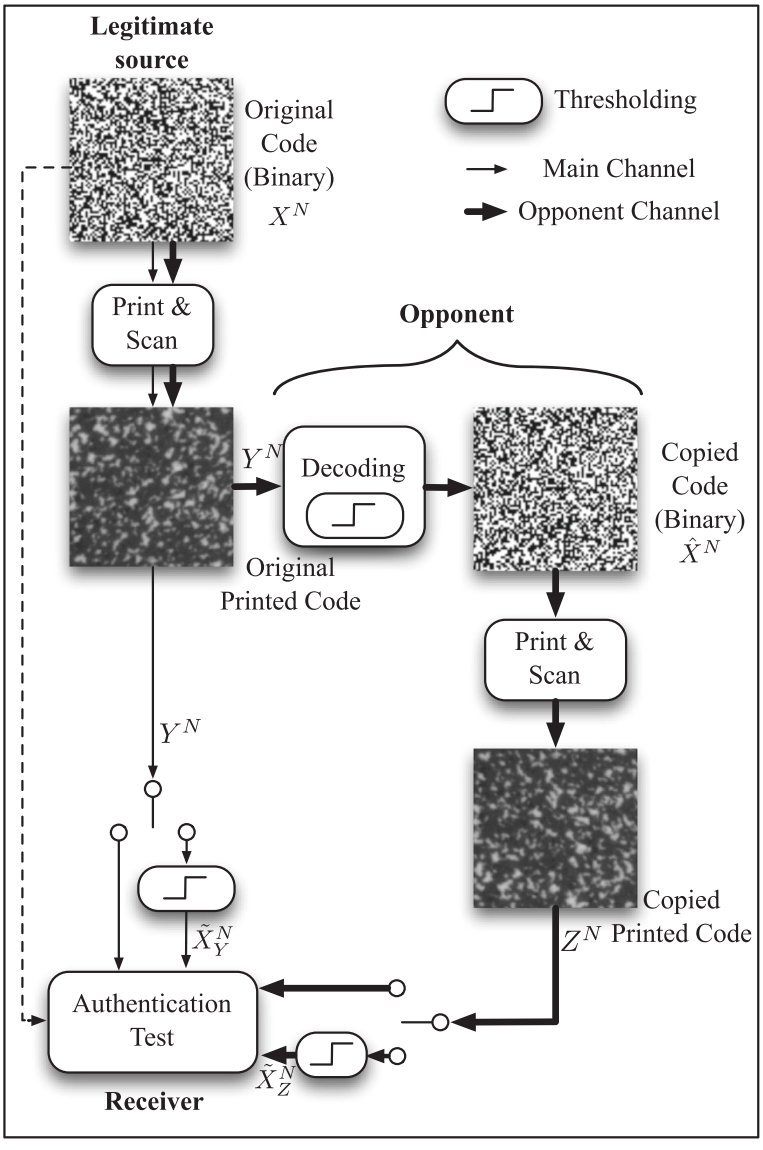

Figure 1 Principle of authentication using graphical codes.

One advantage of this system over previously cited ones is that it is easy to deploy since the authentication process needs only a scan of the graphical code under scrutiny and the seed used to generate the original one: no fingerprint database is required in this case.

The security of this system solely relies on the use of a PUF, i.e., the impossibility for the opponent to accurately estimate the original binary code. Different security analysis have already been performed with respect to (w.r.t.) this authentication system or to very similar ones. In [9], the authors have studied the impact of multiple printed observations of same graphical codes and have shown that the power of the noise due to the printing process can be reduced in this particular setup, but not completely removed due to deterministic printing artifacts. In [10], the authors use machine learning tools in order to try to infer the original code from an observation of the printed code; their study shows that the estimation accuracy can be increased without recovering perfectly the original code. In [11], the authors propose a print and scan model adapted to graphical code and derive attacks and adapted detection metrics to counter the attacks. In [12], the authors consider the security analysis in the rather similar setup of passive fingerprinting using binary fingerprints under informed attacks (the channel between the original code and the copied code is assumed to be a binary symmetric channel). They show that in this case the security increase with the code length, and they propose a practical threshold when type I error (originally detected as a forgery) and type II error (forgery detected as an original) are equal.

1.2 Notations

We denote sets by calligraphic font, e.g., $\mathcal{X}$, random variables (RV) ranging over these sets by the same italic capitals, e.g., X, and their outcomes in lowercase letters, e.g., x. $E_X[.]$ denotes the expectation over X. The cardinality of the set $\mathcal{X}$ is denoted by $|\mathcal{X}|$. The sequence of N variables $(X_1, X_2, ..., X_N)$ is denoted X^N.

1.3 Setup

The binary graphical code can be seen as an authentication sequence x^N chosen at random from the message set $\mathcal{X}^N$ and shared secretly with the legitimate receiver. In our authentication model, x^N is published as a noisy version y^N taking values in the set of points $\mathcal{Y}^N$ (see Figure 1). An opponent may observe y^N and, naturally, tries to retrieve the original authentication sequence. He obtains an estimated sequence $\hat{x}^N$ and publish a forgery as a sequence z^N taking value in the same set of points $\mathcal{Y}^N$, hoping that it will be accepted by the receiver as coming from the legitimate source. When observing a sequence o^N, which may be one of the two possible sequences y^N or z^N, the destination has to decide whether this observed sequence comes from the legitimate source or not.

The authentication model involves two channels $\mathcal{X} \rightarrow (\mathcal{Y}, \mathcal{Z})$, and in the rest of the paper, we define the main channel as the channel between the legitimate source and the receiver, and the opponent channel as the channel between the legitimate source and the receiver but passing through the counterfeiter channel (see Figure 1). The two channels $\mathcal{X} \rightarrow (\mathcal{Y}, \mathcal{Z})$ are considered being discrete and memoryless with conditional probability distribution $P_{YZ|X}(y, z \mid x)$. The marginal channels $\mathrm{P}_{Y|X}$ and $\mathrm{P}_{Z|X}$ constitute the transition probability matrices of the main channel and the opponent channel, respectively.

As we shall see in the rest of the paper, authentication performances are directly impacted by the discrimination between the two channels and can be maximized by channel optimization.

Note that the authentication sequence x^N is generated using a secure pseudo-random number generator (PRNG) having a sufficiently large key space to prevent brute-force attacks. The seed of the PRNG can practically be transmitted using both a secure lossless communication channel and via a key distribution system so that the receiver can generate x^N from the seed. The security of such a system is beyond the scope of this paper.

1.4 Contributions of the paper

The goal of this paper is twofold:

- Firstly, it provides reliable performance measurements of the authentication system based on a Neyman-Pearson hypothesis test (i.e., to compute accurately the probability of rejecting an authentic code and the probability of non-detecting an illegal copy, denoted as type I and type II errors, respectively). An asymptotic expression which is more accurate than the Gaussian expression is first proposed to compute these probabilities of errors; then, the importance sampling simulation method is provided to practically estimate them. We evaluate the impact of the Gaussian approximation of the test with respect to its asymptotic expression.
- Secondly, the computation of type I and type II errors are used to derive the most favorable channels for authentication. We show first that it is in the receiver's interest to process directly the scanned grayscale code instead of a binary version. Then, the error probabilities are used to compute for a given channel model, the configuration which maximizes the authentication performance.

This paper is an extension of [13] in which we use the generalized Gaussian distribution family instead of the Gaussian distribution as in [13]. Moreover, the analytical

formulation of these probabilities is practically confirmed by using an importance sampling method, a Monte Carlo strategy of numerical simulation that can be used to compute rare events. We also present how to design the channel in order to maximize the authentication performance for different cases of generalized Gaussian distributions and when the opponent is either passive (he undergoes the same channel as the receiver) or active (he can adapt his channel).

2 The authentication channel

2.1 Channel modeling

Let $\mathrm{T}_{V|X}$ be the generic transition matrix modeling the whole physical processes used, more specifically the printing and scanning devices. The entries of this matrix are conditional probabilities $T_{V|X}(v \mid x)$ relating an input alphabet $\mathcal{X}$ and the output alphabet $\mathcal{V}$. In practical and realistic situations, $\mathcal{X}$ is a binary alphabet standing for black (0) and white (1) elements of a digital code, and the channel output set $\mathcal{V}$ stands for the set of gray-level values with cardinality K (for printed and scanned images, $K = 256$). Transition matrix $\mathrm{T}_{V|X}$ may conceptually be any discrete distribution over the set $\mathcal{V}$, but we will focus in Section 4.4 on some common and realistic distributions when analyzing numerically the performance.

The marginal distribution of the main channel $\mathrm{P}_{Y|X}$ is equivalent to one print and scan process, and consequently, we have $\mathrm{P}_{Y|X} = \mathrm{T}_{V|X}$. On the other hand, $\mathrm{P}_{Z|X}$ depends on the opponent processing while he has to retrieve the original sequence before reprinting it. We aim here at expressing this marginal distribution considering that the opponent tries to restore the original sequence before publishing his fraudulent sequence z^N.

When performing a detection to obtain an estimated sequence $\hat{x}^N$ of the original code, the opponent undergoes errors. These errors are evaluated with probabilities $P_{e,W}$ when confusing an original white dot with a black and $P_{e,B}$ when confusing an original black dot with a white. This distinction is due to the fact that the distribution $\mathrm{T}_{V|X}$ of the physical devices is arbitrary and not necessarily symmetric. Let $\mathcal{D}_{\mathcal{W}}$ be the optimal decision region for decoding white dots obtained after using classical maximum likelihood decoding:

$$\mathcal{D}_{\mathcal{W}} = \left\{ v \in \mathcal{V} : \; P_{Y|X}(v \mid X = 1) > P_{Y|X}(v \mid X = 0) \right\}. \tag{1}$$

Error probabilities $P_{e,W}$ and $P_{e,B}$ are then equal to

$$P_{e,B} = \sum_{v \in \mathcal{D}_{\mathcal{W}}} P_{Y|X}(v \mid X = 0), \tag{2}$$

$$P_{e,W} = \sum_{v \in \mathcal{D}^c_{\mathcal{W}}} P_{Y|X}(v \mid X = 1). \tag{3}$$

where $\mathcal{D}^c_{\mathcal{W}}$ is the complementary region in the set $\mathcal{V}$. The channel $X \to \hat{X}$ can be modeled as a binary input binary output (BIBO) channel with transition probability matrix $\mathrm{P}_{\hat{X}|X}$:

$$\begin{bmatrix} P_{\hat{X}|X}(\hat{x} = 0 \mid x = 0) & P_{\hat{X}|X}(\hat{x} = 1 \mid x = 0) \\ P_{\hat{X}|X}(\hat{x} = 0 \mid x = 1) & P_{\hat{X}|X}(\hat{x} = 1 \mid x = 1) \end{bmatrix} = \begin{bmatrix} 1 - P_{e,B} & P_{e,B} \\ P_{e,W} & 1 - P_{e,W} \end{bmatrix} \tag{4}$$

As we can see in Figure 1, the opponent channel $\mathcal{X} \to Z$ is a physically degraded version of the main channel. Thus, $X \to \hat{X} \to Z$ forms a Markov chain with the relation $P_{\hat{X}Z|X}(\hat{x}, z \mid x) = P_{\hat{X}|X}(\hat{x} \mid x) T_{Z/\hat{X}}(z \mid \hat{x})$, where $\mathrm{T}_{Z|\hat{X}}$ is the transition matrix of the counterfeiter physical device. Components of the marginal channel matrix $\mathrm{P}_{Z|X}$ are

$$\begin{aligned} P_{Z|X}(v \mid x) &= \sum_{\hat{x}=0,1} P_{\hat{X}Z|X}(\hat{x}, \; v \mid x) \\ &= \sum_{\hat{x}=0,1} P_{\hat{X}|X}(\hat{x} \mid x) T_{Z|\hat{X}}(v \mid \hat{x}). \end{aligned} \tag{5}$$

Finally, we have

$$\begin{aligned} P_{Z|X}(v \mid X = 0) &= (1 - P_{e,B}) T_{Z|\hat{X}}(v \mid \hat{X} = 0) \\ &\quad + P_{e,B} T_{Z|\hat{X}}(v \mid \hat{X} = 1), \end{aligned} \tag{6}$$

$$\begin{aligned} P_{Z|X}(v \mid X = 1) &= (1 - P_{e,W}) T_{Z|\hat{X}}(v \mid \hat{X} = 1) \\ &\quad + P_{e,W} T_{Z|\hat{X}}(v \mid \hat{X} = 0). \end{aligned} \tag{7}$$

2.2 Receiver's strategies: thresholding or not?

Two strategies are possible for the receiver.

2.2.1 Binary thresholding

As a first strategy, the legitimate receiver first decode the observed sequence o^N using a maximum likelihood criterion based on the main channel marginal distribution $\mathrm{P}_{Y|X}$. He then restores a binary version $\tilde{x}^N$ of the original message x^N using the same decision region as defined by (1) and naturally undergoes errors.

- In the main channel, i.e., when $O^N = Y^N$, error probabilities are equivalent to (2) and (3).

- In the opponent channel, i.e., when $O^N = Z^N$, we make use of (6) and (7) to express the corresponding error probabilities:

$$\tilde{P}_{e,W} = \sum_{v \in \mathcal{D}^c_{\mathcal{W}}} P_{Z|X}(v \mid X = 1), \tag{8}$$

$$\tilde{P}_{e,W} = (1 - P_{e,W}) \sum_{v \in \mathcal{D}^c_{\mathcal{W}}} T_{Z|\hat{X}}(v \mid \hat{X} = 1) + P_{e,W} \sum_{v \in \mathcal{D}^c_{\mathcal{W}}} T_{Z|\hat{X}}(v \mid \hat{X} = 0).$$

$$\tilde{P}_{e,W} = (1 - P_{e,W}) P'_{e,W} + P_{e,W}(1 - P'_{e,B}) \tag{9}$$

where $P'_{e,W} = \sum_{v \in \mathcal{D}^c_{\mathcal{W}}} T_{Z|\hat{X}}(v \mid \hat{X} = 1)$ and $P'_{e,B} = \sum_{v \in \mathcal{D}_{\mathcal{W}}} T_{Z|\hat{X}}(v \mid \hat{X} = 0)$. The same development yields

$$\tilde{P}_{e,B} = (1 - P_{e,B}) P'_{e,B} + P_{e,B}(1 - P'_{e,W}). \tag{10}$$

For this first strategy, the opponent channel may be viewed as the cascade of two binary input/binary output channels:

$$\begin{bmatrix} 1 - \tilde{P}_{e,B} & \tilde{P}_{e,B} \\ \tilde{P}_{e,W} & 1 - \tilde{P}_{e,W} \end{bmatrix} = \begin{bmatrix} 1 - P_{e,B} & P_{e,B} \\ P_{e,W} & 1 - P_{e,W} \end{bmatrix} \times \begin{bmatrix} 1 - P'_{e,B} & P'_{e,B} \\ P'_{e,W} & 1 - P'_{e,W} \end{bmatrix}. \tag{11}$$

As we will see in the next section, in this particular case, the test to decide whether the observed decoded sequence $\tilde{x}^N$ comes from the legitimate source or not is tantamount to counting the number of erroneous decoded dots.

2.2.2 Gray-level observations

In the second strategy, the receiver performs his test directly on the received sequence o^N without any given decoding. We will see in Section 3.3 that this strategy is better than the previous one (see Section 3.2).

3 Impacts of the receiver's strategies on hypothesis testing

We consider here testing whether, for a given fixed input $(x_1, \ldots, x_N)$, an observed independent and identically distributed (i.i.d.) sequence $(o_1, \ldots, o_N \mid x_1, \ldots, x_N)$ is generated from a given distribution $P_{Y|X}$ or if it comes from an alternative hypothesis associated to distribution $P_{Z|X}$, $(o_i \mid x_i)$ belonging to a discrete finite set $\mathcal{V}$. Practically, we are interested in performing authentication after observing a sequence of N samples $(o_i \mid x_i)$, attesting whereas this sequence comes from a legitimate source or from a counterfeiter. The receiver establishes then a decision based on a predefined statistical test and assigns one of the two hypothesis H_0 or H_1 corresponding, respectively, to each of the former cases. According to this test, the space $\mathcal{V}^N$ will be partitioned into two regions $\mathcal{H}_0$ and $\mathcal{H}_1$. Accepting hypothesis H_0 while it is actually a fake (the observed N sample sequence belongs to $\mathcal{H}_0$ while H_1 is true) leads to an error of type II having probability β. Rejecting hypothesis H_0 while actually the observed sequence comes from the legitimate source (the observed N sample sequence belongs to $\mathcal{H}_1$ while H_0 is true) leads to an error of type I with probability α. It is desirable to find a test with a minimal probability β for a fixed or prescribed probability of type I. An optimal decision rule will be given by the Neyman-Pearson criterion. The eponymous theorem states that under the constraint $\alpha \leq \alpha^*$, β is minimized if only if the following log-likelihood test infers the choice of H_1:

$$\log \frac{P^N(o^N \mid x^N, H_1)}{P^N(o^N \mid x^N, H_0)} \geq \gamma, \tag{12}$$

where γ is a threshold verifying the constraint $\alpha \leq \alpha^*$.

3.1 Authentication via binary thresholding

In the first strategy, the final observed data is $\tilde{x}^N$ and the original sequence x^N is a side information containing two types of data ('0' and '1'). The conditional distribution of each random component $(\tilde{X}_i \mid x_i)$ of the sequence $(\tilde{X}^N \mid x^N)$ is the same for each given type. We compute now the probabilities that describe the two random i.i.d. sequences $(\tilde{X}^N \mid x^N)$, one per data type, and for each of the two possible hypothesis. We derive then the corresponding test from (12). Under hypothesis $H_j, j \in \{0, 1\}$, these probabilities are expressed conditionally to the known original code x^N. Let $\mathcal{N}_B = \{i : x_i = 0\}$ and $\mathcal{N}_W = \{i : x_i = 1\}$, with $N_B = |\mathcal{N}_B|$ and $N_W = |\mathcal{N}_W|$. Because of i.i.d. sequences, we have

$$P^N(\tilde{x}^N \mid x^N, H_j) = \prod_{i=1}^{N} P(\tilde{x}_i \mid x_i, H_j),$$

$$P^N(\tilde{x}^N \mid x^N, H_j) = \prod_{i \in \mathcal{N}_B} P(\tilde{x}_i \mid 0, H_j) \times \prod_{i \in \mathcal{N}_W} P(\tilde{x}_i \mid 1, H_j).$$

Under hypothesis H_0 the channel $X \to \tilde{X}$ has distributions given by (2) and (3) and we have:

$$P^N\left(\tilde{x}^N \mid x^N, H_0\right) = (P_{e,B})^{n_{e,B}} (1 - P_{e,B})^{N_B - n_{e,B}} \times (P_{e,W})^{n_{e,W}} (1 - P_{e,W})^{N_W - n_{e,W}},$$

where $n_{e,B}$ and $n_{e,W}$ are the number of errors $(\tilde{x}_i \neq x_i)$ when black is decoded into white and when white is decoded into black, respectively.

- Under hypothesis H_1, the channel $X \rightarrow \tilde{X}$ has distributions given by (9) and (10), and we have

$$P^N\left(\tilde{x}^N \mid x^N, H_1\right) = (\tilde{P}_{e,B})^{n_{e,B}}(1-\tilde{P}_{e,B})^{N_B-n_{e,B}} \times (\tilde{P}_{e,W})^{n_{e,W}}(1-\tilde{P}_{e,W})^{N_W-n_{e,W}}.$$

Applying now the Neyman Pearson criterion (12), the test is expressed as

$$L_1 = \log\frac{P^N\left(\tilde{x}^N \mid x^N, H_1\right)}{P^N\left(\tilde{x}^N \mid x^N, H_0\right)} \underset{H0}{\overset{H1}{\gtrless}} \gamma, \tag{13}$$

$$L_1 = n_{e,B}\log\left(\frac{\tilde{P}_{e,B}(1-P_{e,B})}{P_{e,B}(1-\tilde{P}_{e,B})}\right) + n_{e,W}\log\left(\frac{\tilde{P}_{e,W}(1-P_{e,W})}{P_{e,W}(1-\tilde{P}_{e,W})}\right) \underset{H0}{\overset{H1}{\gtrless}} \lambda_1, \tag{14}$$

where $\lambda_1 = \gamma - N_B\log\left(\frac{1-\tilde{P}_B}{1-P_B}\right) - N_W\log\left(\frac{1-\tilde{P}_W}{1-P_W}\right)$. This expression has the practical advantage to only count the number of errors in order to perform the authentication task but at a cost of a loss of optimality.

3.2 Authentication via gray-level observations

In the second strategy, the observed data is o^N. Here again, the conditional distribution of each random component $(O_i \mid x_i)$ of the sequence $(O^N \mid x^N)$ is the same for each type of data of X. The Neyman Pearson test is expressed as

$$L_2 = \log\frac{P^N(o^N \mid x^N, H_1)}{P^N(o^N \mid x^N, H_0)} \underset{H0}{\overset{H1}{\gtrless}} \lambda_2, \tag{15}$$

which can be developed as

$$L_2 = \sum_{i\in\mathcal{N}_B}\log\frac{P_{Z|X}(o_i \mid 0)}{P_{Y|X}(o_i \mid 0)} + \sum_{i\in\mathcal{N}_W}\log\frac{P_{Z|X}(o_i \mid 1)}{P_{Y|X}(o_i \mid 1)} \underset{H0}{\overset{H1}{\gtrless}} \lambda_2, \tag{16}$$

$$L_2 = \sum_{i\in\mathcal{N}_B}\log\left((1-P_{e,W})\frac{T_{Z|\hat{X}}(o_i \mid 0)}{T_{Y|X}(o_i \mid 0)} + P_{e,W}\frac{T_{Z|\hat{X}}(o_i \mid 1)}{T_{Y|X}(o_i \mid 0)}\right) + \sum_{i\in\mathcal{N}_W}\log\left((1-P_{e,B})\frac{T_{Z|\hat{X}}(o_i \mid 1)}{T_{Y|X}(o_i \mid 1)} + P_{e,B}\frac{T_{Z|\hat{X}}(o_i \mid 0)}{T_{Y|X}(o_i \mid 1)}\right) \underset{H0}{\overset{H1}{\gtrless}} \lambda_2. \tag{17}$$

Note that the expressions of the transition matrix modeling the physical processes $\mathrm{T}_{Y|X}$ and $\mathrm{T}_{Z|\hat{X}}$ are required in order to perform the optimal test.

3.3 Authentication with thresholding vs authentication without thresholding

In this setup and without loss of generality, we consider only the Gaussian model with variance σ^2 for the physical devices $\mathrm{T}_{Y|X}$ and $\mathrm{T}_{Z|\hat{X}}$. Figure 2 compares the receiver operating characteristic (ROC) curves associated with the two different strategies. Note that the error probabilities are computed using the results given in the next section (see Section 4.2). We can notice that the gap between the two strategies is important. This is not surprising since the binary thresholding removes information from the gray-level observation, yet this has a practical impact because one practitioner can be tempted to count the number of errors as given in (14) as an authentication score for its easy implementation. The information theoretical analysis presented in the Appendix confirms also that authentication is more accurate without thresholding, and this result is in line with *the remark of Blahut in [14] where in p108 he writes that 'information is increased if a measurement is made more precise [...] (i.e. with a refinement of the set of measurement outcomes).'*

Moreover, as we will see in Section 5, the plain scan of the graphical code can be used whenever the receiver needs to estimate the opponent's channel.

4 Toward reliable performance evaluation

In the previous section we have expressed the Neyman-Pearson test for the two proposed strategies resumed by (14) and (17). These tests may then be practically performed on the observed sequence in order to make a decision about its authenticity. We aim now at expressing the error probabilities of types I and II and comparing the two possible strategies described previously. Let $m = 1, 2$

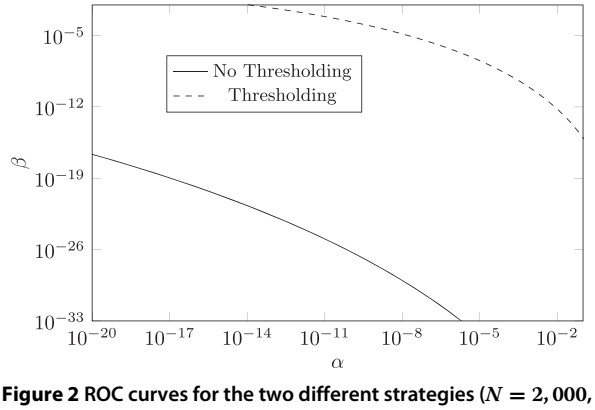

Figure 2 ROC curves for the two different strategies ($N = 2,000$, $\sigma = 52$). α is the probability of rejecting an authentic code and β the probability of non-detecting an illegal copy.

be the index denoting the strategy; a straightforward calculation gives

$$\alpha_m = \sum_{l>\lambda_m} P_{L_m}(l \mid H_0), \tag{18}$$

$$\beta_m = \sum_{l<\lambda_m} P_{L_m}(l \mid H_1). \tag{19}$$

where $P_{L_m}(l \mid H_j)$ is the distribution of the log-likelihood ratio L_m under hypothesis H_j.

4.1 Gaussian approximation

As the length N of the sequence is generally large, we use the central limit theorem to study the distributions P_{L_m}, $m = 1,\ 2$ (a similar strategy was proposed in [15]).

- For the binary thresholding strategy, $n_{e,W}$ and $n_{e,B}$ in (14) are binomial random variables depending on the origin of the observed sequence. Let N_x stand for the number of data of type x in the original code and $P_{e,x}$ the cross-over probabilities emerging from type x in the BIBO channels (4) or (11). When N is large enough, the binomial random variables can be approximated with a Gaussian distribution. We have

  $$n_{e,x} \sim \mathcal{N}(N_x P_{e,x},\ N_x P_{e,x}(1 - P_{e,x})). \tag{20}$$

  From (14), L_1 is a weighted sum of Gaussian random variables and one can obviously deduce the parameters of the normal approximation describing the log-likelihood L_1.
- For the second strategy, i.e., when the receiver tests directly the observed gray-level sequence, the log-likelihood L_2 in Equation 17 may be expressed as two sums of i.i.d. and becomes

  $$L_2 = \sum_{i\in\mathcal{N}_B} \ell(o_i,\ 0) + \sum_{i\in\mathcal{N}_W} \ell(o_i,\ 1) \underset{H0}{\overset{H1}{\gtrless}} \lambda_2, \tag{21}$$

  where $\ell(v,\ x)$ is a function $\ell :\ \mathcal{X} \times \mathcal{V} \to \mathbb{R}$ having some distribution with mean and variance equal to

  $$m_x = E[\,\ell(V,\ x) \mid H_j] = \sum_{v\in\mathcal{V}} \ell(v,\ x) P(v \mid x,\ H_j), \tag{22}$$

  and

  $$\mathrm{var}[\,\ell(V,\ x) \mid H_j] = \sum_{v\in\mathcal{V}} (\ell(v,\ x) - m_x)^2 P(v \mid x, H_j), \tag{23}$$

  with $\mathrm{P} = \mathrm{P}_{Y|X}$ (respectively $\mathrm{P} = \mathrm{P}_{Z|X}$) for $j = 0$ (respectively 1). The central limit theorem is then used again to approximate the distribution of L_2 and compute type I and type II error probabilities.

4.2 Asymptotic expression

In this section, we drop the subscribe m denoting the strategy as all the subsequent analysis is common for both of them. One important problem is the fact that the Gaussian approximation proposed previously provides inaccurate error probability values when the threshold λ in (18) and (19) is far from the mean of the log-likelihood random variable L. Chernoff bound and large deviation theory [16] are preferred in this context as very small error probabilities of types I and II may be desired [17]. Given a real number s, the Chernoff bound on type I and type II errors may be expressed as

$$\alpha = \Pr(L \geq \lambda \mid H_0) \leq e^{-s\lambda} g_L(s;\, H_0) \text{ for any } s > 0, \tag{24}$$

$$\beta = \Pr(L \leq \lambda \mid H_1) \leq e^{-s\lambda} g_L(s;\, H_1) \text{ for any } s < 0, \tag{25}$$

where the function $g_L(s;\, H_j)$, $j = 0,\ 1$ is the moment generating function of the random variable L defined as

$$g_L(s;\, H_j) = E_{P_L(L|H_j)}\left[e^{sL}\right]. \tag{26}$$

where expectation is performed with respect to distribution $P_L(L \mid H_j)$. Reminding that L is a sum of N independent random variables, asymptotic analysis in probability theory (when N is large enough) shows that bounds similar to (24) and (25) are much more appropriate for estimating α and β than the Gaussian approximation especially when λ is far from $E[L]$, namely when bounding the tails of a distribution [16,17]. The tightest bound is obtained by finding the value of s that provides the minimum of the right-hand side (RHS) of (24) and (25), i.e., the minimum of $e^{-s\lambda} g_L(s;\, H_j)$ for each $j = 0,\ 1$. Taking the derivative, the value s that provides the tightest bound under each hypothesis is such that [a]

$$\lambda = \left.\frac{\frac{\mathrm{d}g_L(s;H_j)}{\mathrm{d}s}}{g_L(s;\, H_j)}\right|_{s=\tilde{s}_j} = \left.\frac{\mathrm{d}}{\mathrm{d}s} \ln g_L(s;\, H_j)\right|_{s=\tilde{s}_j}. \tag{27}$$

We introduce the semi-invariant moment generating function after an acute observation of the identity (27). The semi-invariant moment generating function of L is

$$\mu_L(s;\, H_j) = \ln g_L(s;\, H_j). \tag{28}$$

This function has many interesting properties that ease the extraction of an asymptotic expression for (24) and (25) [17]. For instance, this function is additive for the sum of independent random variables, and we have

$$\mu_L(s;\, H_j) = \sum_{i\in\mathcal{N}_B} \mu_{i,0}(s;\, H_j) + \sum_{i\in\mathcal{N}_W} \mu_{i,1}(s;\, H_j), \tag{29}$$

where $\mu_{i,x}(s;\, H_j)$ is the semi-invariant moment generating function of the random component $\ell(O_i,\ x)$ when the

observed sequence comes from the distribution associated to hypothesis H_j. In addition, relation (27) may be expressed as the sum of the derivatives at the value $\tilde{s}_j$ optimizing the bound:

$$\lambda = \sum_{i\in\mathcal{N}_B} \mu'_{i,0}(\tilde{s}_j\,;\,H_j) + \sum_{i\in\mathcal{N}_W} \mu'_{i,1}(\tilde{s}_j\,;\,H_j). \tag{30}$$

Chernoff bounds on type I and type II errors (24) and (25) may then be expressed as

$$\begin{aligned}\alpha &= \Pr(L \geq \lambda \mid H_0)\\ &\leq \exp\left[\sum_{i\in\mathcal{N}_B}\left(\mu_{i,0}(\tilde{s}_0\,;\,H_0) - \tilde{s}_0\mu'_{i,0}(\tilde{s}_0\,;\,H_0)\right)\right.\\ &\quad\left.+\sum_{i\in\mathcal{N}_W}\left(\mu_{i,1}(\tilde{s}_0\,;\,H_0) - \tilde{s}_0\mu'_{i,1}(\tilde{s}_0\,;\,H_0)\right)\right],\end{aligned} \tag{31}$$

and

$$\begin{aligned}\beta &= \Pr(L \leq \lambda \mid H_1)\\ &\leq \exp\left[\sum_{i\in\mathcal{N}_B}\left(\mu_{i,0}(\tilde{s}_1\,;\,H_1) - \tilde{s}_1\mu'_{i,0}(\tilde{s}_1\,;\,H_1)\right)\right.\\ &\quad\left.+\sum_{i\in\mathcal{N}_W}\left(\mu_{i,1}(\tilde{s}_1\,;\,H_1) - \tilde{s}_1\mu'_{i,1}(\tilde{s}_1\,;\,H_1)\right)\right].\end{aligned} \tag{32}$$

The distribution of each random component $(O_i \mid x_i)$ in the sequence $(O^N \mid x^N)$ is the same for each type of data X, and consequently, $\mu_{i,x}(s\,;\,H_j) = \mu_x(s\,;\,H_j)$, i.e., $\mu_{i,x}(s\,;\,H_j)$ is independent from i for each type of data x. The RHS in (31) and (32) can be simplified as

$$\begin{aligned}\exp\left[N_B\left(\mu_0(\tilde{s}_j\,;\,H_j) - \tilde{s}_j\mu'_0(\tilde{s}_j\,;\,H_j)\right) + N_W\left(\mu_1(\tilde{s}_j\,;\,H_j)\right.\right.\\ \left.\left. -\ \tilde{s}_j\mu'_1(\tilde{s}_j\,;\,H_j)\right)\right].\end{aligned} \tag{33}$$

Roughly speaking, Cramér's theorem [16] states that for sufficiently large N, the upper bounds expressed for $j = 0,\ 1$ in (33) are also lower bounds for α and β, respectively. Thus, one can write for $N_B \approx N_W \approx N/2$:

$$\lim_{N\to\infty}\frac{2}{N}\ln\alpha = \left[\mu(\tilde{s}_0;\,H_0) - \tilde{s}_0\mu'(\tilde{s}_0\,;\,H_0)\right], \tag{34}$$

$$\lim_{N\to\infty}\frac{2}{N}\ln\beta = \left[\mu(\tilde{s}_1;\,H_1) - \tilde{s}_1\mu'(\tilde{s}_1\,;\,H_1)\right], \tag{35}$$

where $\tilde{s}_0 > 0$, $\tilde{s}_1 < 0$, $\mu(\tilde{s}_j;\,H_j) = \mu_0(\tilde{s}_j;\,H_j) + \mu_1(\tilde{s}_j;\,H_j)$, $\mu'(\tilde{s}_j;\,H_j) = \mu'_0(\tilde{s}_j;\,H_j) + \mu'_1(\tilde{s}_j;\,H_j)$. A modified asymptotic expression including a correction factor is evaluated for the sum of an i.i.d random sequence (see [17], Appendix 5A), and for large N, we have

$$\begin{aligned}\alpha &= \Pr(L \geq \lambda \mid H_0),\\ &\underset{N\to\infty}{\rightarrow} \frac{1}{\tilde{s}_0\sqrt{N\pi\mu''(\tilde{s}_0;H_0)}}\exp\left\{\tfrac{N}{2}\left[\mu(\tilde{s}_0;\,H_0) - \tilde{s}_0\mu'(\tilde{s}_0\,;\,H_0)\right]\right\}.\end{aligned} \tag{36}$$

and

$$\begin{aligned}\beta &= \Pr(L \leq \lambda \mid H_1),\\ &\underset{N\to\infty}{\rightarrow} \frac{1}{|\tilde{s}_1|\sqrt{N\pi\mu''(\tilde{s}_1;H_1)}}\exp\left\{\tfrac{N}{2}\left[\mu(\tilde{s}_1;H_1) - \tilde{s}_1\mu'(\tilde{s}_1;H_1)\right]\right\},\end{aligned} \tag{37}$$

where $\mu''(\tilde{s}_j;\,H_j) = \mu''_0(\tilde{s}_j;\,H_j) + \mu''_1(\tilde{s}_j;\,H_j)$ is the second derivative of the semi-invariant moment generating function of $\ell(V,\,x)$ defined by

$$\ell(\nu,\,1) = \log\left((1-P_{e,W})\,\frac{T_{Z|\hat{X}}(\nu\mid 1)}{T_{Y|X}(\nu\mid 1)} + P_{e,W}\,\frac{T_{Z|\hat{X}}(\nu\mid 0)}{T_{Y|X}(\nu\mid 1)}\right), \tag{38}$$

$$\ell(\nu,\,0) = \log\left((1-P_{e,B})\,\frac{T_{Z|\hat{X}}(\nu\mid 0)}{T_{Y|X}(\nu\mid 0)} + P_{e,B}\,\frac{T_{Z|\hat{X}}(\nu\mid 1)}{T_{Y|X}(\nu\mid 0)}\right). \tag{39}$$

4.3 Numerical computations of α and β via importance sampling

This section addresses the problem of estimating numerically type I and type II error probabilities, i.e., α and β. Monte Carlo simulation method [18] gives accurate solution since these probabilities can be expressed as expectations of a function of a random variable governed by a given probability distribution. We have

$$\alpha = \sum_{\nu^N\in\mathcal{H}_1} P^N(\nu^N \mid x^N,\,H_0), \tag{40}$$

$$= \sum_{\nu^N\in\mathcal{V}^N} P^N(\nu^N \mid x^N,\,H_0)\phi(\nu^N;\,\mathcal{H}_1), \tag{41}$$

where $\phi(\nu^N;\,\mathcal{H}_1) = 1$ whenever $\nu^N \in \mathcal{H}_1$ and zero if not. The probability of type I error is then expressed as the expectation of $\phi(\nu^N;\,\mathcal{H}_1)$ under distribution $P^N(\nu^N \mid x^N,\,H_0)$. In the same way, type II error probability β is the expectation of $\phi(\nu^N;\,\mathcal{H}_0)$ under distribution $P^N(\nu^N \mid x^N,\,H_1)$. In the sequel, we denote $P^N(\nu^N \mid x^N,\,H_0) = P^N_{Y|X}$ and $P^N(\nu^N \mid x^N,\,H_1) = P^N_{Z|X}$, and we have

$$\alpha = E_{P^N_{Y|X}}\left[\phi(V^N;\,\mathcal{H}_1)\right], \tag{42}$$

$$\beta = E_{P^N_{Z|X}}\left[\phi(V^N;\,\mathcal{H}_0)\right]. \tag{43}$$

Monte Carlo methods make use of the law of large numbers to infer an estimation for α and β by computing numerically an empirical mean for $\phi(\nu^N;\,\mathcal{H}_1)$ and $\phi(\nu^N;\,\mathcal{H}_0)$, respectively. Clearly, the computer runs N_{trials},

each one generating an i.i.d. vector v^N, where samples v_n are driven from distributions $P_{Y|X}$ and $P_{Z|X}$, respectively, which gives the following estimates:

$$\hat{\alpha} = \frac{1}{N_{\text{trials}}} \sum_{i=1}^{N_{\text{trials}}} \phi((v^N)^{(i)}; \mathcal{H}_1),$$

$(v_n)^{(i)}$ being generated from $P_{Y|X}$

$$\hat{\beta} = \frac{1}{N_{\text{trials}}} \sum_{i=1}^{N_{\text{trials}}} \phi((v^N)^{(i)}; \mathcal{H}_0),$$

$(v_n)^{(i)}$ being generated from $P_{Z|X}$.

The Monte Carlo estimator is unbiased ($\hat{\alpha} \to \alpha$ and $\hat{\beta} \to \beta$) almost surely, and the rate of convergence is $N_{\text{trials}}^{-1/2}$. Recalling that for a zero mean and unit variance Gaussian random variable U, $P(|U| \leq 1.96) = 0.95$, the confidence interval at 0.95 obtained from each estimation is

$$[\hat{\alpha} - \frac{1.96\sigma_\alpha}{\sqrt{N_{\text{trials}}}}, \hat{\alpha} + \frac{1.96\sigma_\alpha}{\sqrt{N_{\text{trials}}}}] \tag{44}$$

$$[\hat{\beta} - \frac{1.96\sigma_\beta}{\sqrt{N_{\text{trials}}}}, \hat{\beta} + \frac{1.96\sigma_\beta}{\sqrt{N_{\text{trials}}}}], \tag{45}$$

where σ_α (resp. σ_β) is the standard deviation of the random variable $\phi((V^N)^{(i)}; \mathcal{H}_1)$ (resp. $\phi((V^N)^{(i)}; \mathcal{H}_0)$). As $\phi((v^N)^{(i)}; \mathcal{H}_1)$ and $\phi((v^N)^{(i)}; \mathcal{H}_0)$ are Bernoulli random variables with parameter α and β, respectively, their variances are easily deduced, e.g., $\sigma_\alpha^2 = \alpha - \alpha^2 \approx \alpha$ and $\sigma_\beta^2 = \beta - \beta^2 \approx \beta$. When α and β are very small, accurate estimations are then difficult to achieve with realistic number of trials. Roughly speaking, the number of trials needed is $N_{\text{trials}} > \frac{10^3}{\alpha}$ (or $N_{\text{trials}} > \frac{10^3}{\beta}$) when the desired confidence interval at 0.95 is constrained to be about a tenth of the expected value of α or β. Actually, we need to evaluate numerically very small values of α and β to draw the curve $\beta(\alpha)$ evaluating the performance of a given test statistic. The required number of trials fails to be realistic. We propose then to use the importance sampling method [18] which enables us to generate rare events and thus reduce considerably the required number of trials. Let us consider distributions $Q_{Y|X}$ and $Q_{Z|X}$ over the set $\mathcal{V}$ such that $Q_{Y|X}$ and $Q_{Z|X} > 0$ and rewrite (42) and (43) as

$$E_{P_{Y|X}^N}\left[\phi(V^N; \mathcal{H}_1)\right] = E_{P_{Y|X}^N}\left[\phi(V^N; \mathcal{H}_1)\frac{Q_{Y|X}^N}{Q_{Y|X}^N}\right],$$

$$E_{P_{Z|X}^N}\left[\phi(V^N; \mathcal{H}_0)\right] = E_{P_{Z|X}^N}\left[\phi(V^N; \mathcal{H}_0)\frac{Q_{Z|X}^N}{Q_{Z|X}^N}\right].$$

One can then alternatively express type I and type II error probabilities by

$$\alpha = E_{Q_{Y|X}^N}\left[\phi(V^N; \mathcal{H}_1)\frac{P_{Y|X}^N}{Q_{Y|X}^N}\right], \tag{46}$$

$$\beta = E_{Q_{Z|X}^N}\left[\phi(V^N; \mathcal{H}_0)\frac{P_{Z|X}^N}{Q_{Z|X}^N}\right]. \tag{47}$$

Monte Carlo simulation with importance sampling method gives the following two estimates:

$$\hat{\alpha} = \frac{1}{N_{\text{trials}}} \sum_{i=1}^{N_{\text{trials}}} \phi\left((v^N)^{(i)}; \mathcal{H}_1\right) \times \left[\frac{P_{Y|X}^N((v^N)^{(i)} \mid x^N)}{Q_{Y|X}^N((v^N)^{(i)} \mid x^N)}\right],$$

$(v^N)^{(i)}$ being generated from $Q_{Y|X}^N$, (48)

$$\hat{\beta} = \frac{1}{N_{\text{trials}}} \sum_{i=1}^{N_{\text{trials}}} \phi\left((v^N)^{(i)}; \mathcal{H}_0\right) \times \left[\frac{P_{Z|X}^N((v^N)^{(i)} \mid x^N)}{Q_{Z|X}^N((v^N)^{(i)} \mid x^N)}\right],$$

$(v^N)^{(i)}$ being generated from $Q_{Z|X}^N$. (49)

The problem of importance sampling is to choose an adequate function $Q_{V|X}$ such that the variance of the estimated probabilities in (48) and (49) are very small. The number of trials will be considerably reduced and accurate estimations of very low values of α and β may be possible. Let

$$Q_{Y|X}(s, v \mid x) = \exp\left(-\mu_x(s; H_0) + s\ell(v, x)\right) P_{Y|X}(v \mid x)$$

and

$$Q_{Z|X}(s, v \mid x) = \exp\left(-\mu_x(s; H_1) + s\ell(v, x)\right) P_{Z|X}(v \mid x)$$

be tilted distributions over the set $\mathcal{V}$, and $\mu_x(s; H_j)$ the semi-invariant moment generating function of $\ell(v, x)$ distributed under hypothesis H_j.

Proposition 1. *The mean of the log-likelihood function $\ell(v, x)$ governed by the tilted distributions $Q_{Y|X}(s, v \mid x)$ is $\mu_x'(s; H_0)$.*

Proof. We have indeed

$$\begin{aligned}\sum_{v\in\mathcal{V}} \ell(v,x) Q_{Y|X}(s,v|x) &= \sum_{v\in\mathcal{V}} \ell(v, x)\exp(-\mu_x(s; H_0)+s\ell(v,x)) \\ &\quad \times P_{Y|X}(v \mid x), \\ &= \frac{\sum\limits_{v\in\mathcal{V}} \ell(v, x)\exp\left(s\ell(v, x)\right) P_{Y|X}(v|x)}{\exp\left(\mu_x(s;H_0)\right)};\end{aligned}$$

since $\mu_x(s;\, H_0) = \log\left(g_x(s;\, H_0)\right)$, the denominator of the previous expression is simply $g_x(s;\, H_0)$:

$$\sum_{v\in\mathcal{V}}\ell(v,x)Q_{Y|X}(s,v|x) = \frac{\sum\limits_{v\in\mathcal{V}}\ell(v,x)\exp\left(s\ell(v,x)\right)P_{Y|X}(v|x)}{\sum\limits_{v\in\mathcal{V}}\exp\left(s\ell(v,\,x)\right)P_{Y|X}(v\mid x)},$$
$$= \frac{\frac{\mathrm{d}g_x(s;H_0)}{\mathrm{d}s}}{g_x(s\,;\,H_0)},$$

Finally, we have

$$\sum_{v\in\mathcal{V}}\ell(v,\,x)Q_{Y|X}(s,v\mid x) = \mu'_x(s;\,H_0). \tag{50}$$

The same development yields

$$\sum_{v\in\mathcal{V}}\ell(v,\,x)Q_{Z|X}(s,v\mid x) = \mu'_x(s;\,H_1). \tag{51}$$

When choosing $s = \tilde{s}_0$ for $Q_{Y|X}(s,v\mid x)$ and $s = \tilde{s}_1$ for $Q_{Z|X}(s,v\mid x)$, the mean of the log-likelihood function $\ell(v,\,x)$ governed by these tilted distributions will be equal to the threshold λ of the test 30. □

Proposition 2. *The variances of the estimations in (48) and (49) go to zero as the number of dots is sufficiently large.*

Proof. To show this, let o^N be the observed samples coming from the main channel, e.g., driven from the tilted distribution $Q^N_{Y|X}(\tilde{s}_0,\, v^N\mid x^N)$. We have

$$Q^N_{Y|X}(\tilde{s}_0,o^N|x^N) = \exp\Bigg(-\sum_{i\in\mathcal{N}_B}\mu_{i,0}(\tilde{s}_0;H_0)-\sum_{i\in\mathcal{N}_W}\mu_{i,1}(\tilde{s}_0;H_0) + \tilde{s}_0\sum_{i\in\mathcal{N}_B}\ell(o_i,\,0)+\tilde{s}_0\sum_{i\in\mathcal{N}_W}\ell(o_i,\,1)\Bigg) \times P^N_{Y|X}(o^N\mid x^N).$$

Recalling that $\mu(\tilde{s}_j;\,H_j) = \mu_0(\tilde{s}_j;\,H_j)+\mu_1(\tilde{s}_j;\,H_j)$, for $N_B \approx N_W \approx N/2$, we have

$$Q^N_{Y|X}(\tilde{s}_0,\,o^N\mid x^N) = \exp\left(-\frac{N}{2}\mu(\tilde{s}_0;\,H_0)+\tilde{s}_0\left(\sum_{i\in\mathcal{N}_B}\ell(o_i,\,0) + \sum_{i\in\mathcal{N}_W}\ell(o_i,\,1)\right)\right)P^N_{Y|X}(o^N\mid x^N).$$

By the law of large numbers, the sum of $N/2$ log-likelihood functions of the observed samples $(o_i\mid x)$ governed by the tilted distribution, converges in probability to its mean value as N is sufficiently large:

$$\sum_{i\in\mathcal{N}_B}\ell(o_i,\,0)\xrightarrow{P}\frac{N}{2}\sum_{v\in\mathcal{V}}\ell(v,\,0)Q_{Y|X}(\tilde{s}_0,v\,|\,0)=\frac{N}{2}\mu'_0(\tilde{s}_0;\,H_0),$$

$$\sum_{i\in\mathcal{N}_W}\ell(o_i,\,1)\xrightarrow{P}\frac{N}{2}\sum_{v\in\mathcal{V}}\ell(v,\,1)Q_{Y|X}(\tilde{s}_0,v\,|\,1)=\frac{N}{2}\mu'_1(\tilde{s}_0;\,H_0).$$

Recalling that $\mu'(\tilde{s}_j;\,H_j) = \mu'_0(\tilde{s}_j;\,H_j)+\mu'_1(\tilde{s}_j;\,H_j)$, and from proposition 1, we have

$$\left(\sum_{i\in\mathcal{N}_B}\ell(o_i,\,0)+\sum_{i\in\mathcal{N}_W}\ell(o_i,\,1)\right)\xrightarrow{P}\frac{N}{2}\mu'(\tilde{s_0};\,H_0).$$

Equivalently, when observed samples come from the opponent channel, e.g., drawn from the tilted distribution $Q^N_{Z|X}(\tilde{s}_1,\,v^N\mid x^N)$, we have

$$\left(\sum_{i\in\mathcal{N}_B}\ell(o_i,\,0)+\sum_{i\in\mathcal{N}_W}\ell(o_i,\,1)\right)\xrightarrow{P}\frac{N}{2}\mu'(\tilde{s}_1;\,H_1).$$

Finally, we have

$$Q^N_{Y|X}(\tilde{s}_0,o^N\,|\,x^N)\xrightarrow{P}\exp\left(-\frac{N}{2}\left(\mu(\tilde{s}_0;H_0)-\tilde{s}_0\mu'(\tilde{s}_0;\,H_0)\right)\right) \times P^N_{Y|X}(o^N\mid x^N) \tag{52}$$

and

$$Q^N_{Z|X}(\tilde{s}_1,\,o^N\,|\,x^N)\xrightarrow{P}\exp\left(-\frac{N}{2}\left(\mu(\tilde{s}_1;\,H_1)-\tilde{s}_1\mu'(\tilde{s}_1;\,H_1)\right)\right) \times P^N_{Z|X}(o^N\mid x^N). \tag{53}$$

The variance of $\phi(V^N;\,\mathcal{H}_1)\frac{P^N_{Y|X}}{Q^N_{Y|X}}$ when V^N is governed by the tilted distribution $Q^N_{Y|X}(\tilde{s}_0,\,v^N\mid x^N)$ is then (the function $\phi(.)$ being 0 or 1)

$$\mathrm{var}_{Q^N_{Y|X}}\left[\phi(V^N;\,\mathcal{H}_1)\frac{P^N_{Y|X}}{Q^N_{Y|X}}\right]$$
$$= E_{Q^N_{Y|X}}\left[\phi^2(V^N;\,\mathcal{H}_1)\left(\frac{P^N_{Y|X}}{Q^N_{Y|X}}\right)^2\right]-\alpha^2,$$
$$= E_{P^N_{Y|X}}\left[\phi(V^N;\,\mathcal{H}_1)\left(\frac{P^N_{Y|X}}{Q^N_{Y|X}}\right)\right]-\alpha^2,$$
$$\xrightarrow{P}E_{P^N_{Y|X}}\left[\phi(V^N;\mathcal{H}_1)\left(\frac{1}{\exp\left(-\frac{N}{2}\left(\mu(\tilde{s}_0;H_0)-\tilde{s}_0\mu'(\tilde{s}_0;H_0)\right)\right)}\right)\right]-\alpha^2.$$

The denominator in the expectation, i.e., $\exp\left(-\frac{N}{2}\left(\mu(\tilde{s}_0;\,H_0)-\tilde{s}_0\mu'(\tilde{s}_0;\,H_0)\right)\right)$, is simply the inverse of the

Cramér-Chernoff bound proposed in (34). We then have

$$\mathrm{var}_{Q_{Y|X}^N}\left[\phi(V^N;\mathcal{H}_1)\frac{P_{Y|X}^N}{Q_{Y|X}^N}\right] \xrightarrow{P} \alpha E_{P_{Y|X}^N}\left[\phi(V^N;\mathcal{H}_1)\right]-\alpha^2.$$

Finally, since $E_{P_{Y|X}^N}\left[\phi(V^N;\mathcal{H}_1)\right]=\alpha$ (42), the variance goes to zero as N is large enough:

$$\mathrm{var}_{Q_{Y|X}^N}\left[\phi(V^N;\mathcal{H}_1)\frac{P_{Y|X}^N}{Q_{Y|X}^N}\right] \xrightarrow{P} 0.$$

The same development gives

$$\mathrm{var}_{Q_{Z|X}^N}\left[\phi(V^N;\mathcal{H}_0)\frac{P_{Z|X}^N}{Q_{Z|X}^N}\right] \xrightarrow{P} 0.$$

□

4.4 Practical performance analysis

Without loss of generality, we use in our analysis a generalized Gaussian distribution to model the physical device, i.e., the association of a printer with a scanner, used by the legitimate source $T_{Y|X}(v \mid x)$ and by the counterfeiter $T_{Z|\hat{X}}(v \mid \hat{x})$:

$$p(v \mid x)=\frac{b}{2a\Gamma(1/b)}e^{-(|v-m(x)|/a)^b}, \tag{54}$$

where $m(x)$ is the mean and the parameter a can be computed from the variance $\sigma^2=\mathrm{var}[V]$:

$$a=\sqrt{\sigma\Gamma(1/b)/\Gamma(3/b)}. \tag{55}$$

The parameter b is used to control the sparsity of 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. The resulting distribution is first discretized then truncated to provide values within $[0,\ldots,255]$ to model a scanning process. Each channel is parametrized in this case by four parameters, two per each type of dots, $m_b=m(0)$ and σ_b for black dots and $m_w=m(1)$ and σ_w for white dots. Note that other print and scan models that take into account the gamma transfer function or additive noise with input dependent variance can be found in [19], but the general methodology of this paper is not dependent on the model and can still be applied.

Figure 3 illustrates the different effects of the generalized Gaussian distributions on the main and the opponent channels of same mean and variance and $b=1$ (Laplacian distribution), $b=2$ (Gaussian distribution), and $b=6$, i.e., close to a uniform distribution.

In order to assess the accuracy of the computations of α and β using either the Gaussian approximation given by (18) and (19), the asymptotic expression given by (36) and (37), or the Monte Carlo simulations using importance sampling given by (48) and (49), we derive ROC curves for generalized Gaussian distributions and $b=\{1,2,6\}$.

Figure 4 illustrates the gap between the estimation of α and β using the Gaussian approximation and the asymptotic expression or the Monte Carlo simulations. The Monte Carlo simulations confirm the fact that the derived Cramér Chernoff bounds are tight, and the difference between the results obtained with the Gaussian approximation are very important especially for close to uniform channels. We can also notice that for the same channel power, the authentication performances are better for $b=6$ then for $b=2$ and $b=1$.

5 Optimal configurations for authentication

The goal of this section is to derive configurations that are optimal regarding authentication, i.e., to derive configurations that for a given α minimize β.

5.1 Optimal configurations by modification of the printing channel

5.1.1 Problem setting

This authentication problem can be seen as a game where the main goal of the receiver, for a given false alarm probability α, is to find a channel that minimizes the probability of missed detection β. Practically, this means that the channel can be chosen by using a given quality of paper, a different ink, and/or by adopting an appropriate 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 $\hat{X}$.

We analyze two scenarios described below:

- The legitimate source and the opponent have identical printing devices; 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 missed detection β^* such that

$$\beta^*=\min_{\mathcal{C}}\beta(\alpha). \tag{56}$$

In this case, the opponent is passive and has no strategy but duplicating the graphical code.

- The opponent can modify its printing channel $\mathcal{C}_o$ (here, we assume that he can change the variance of its noise), practically it means that he can modify one or several parameters of the printing setup without

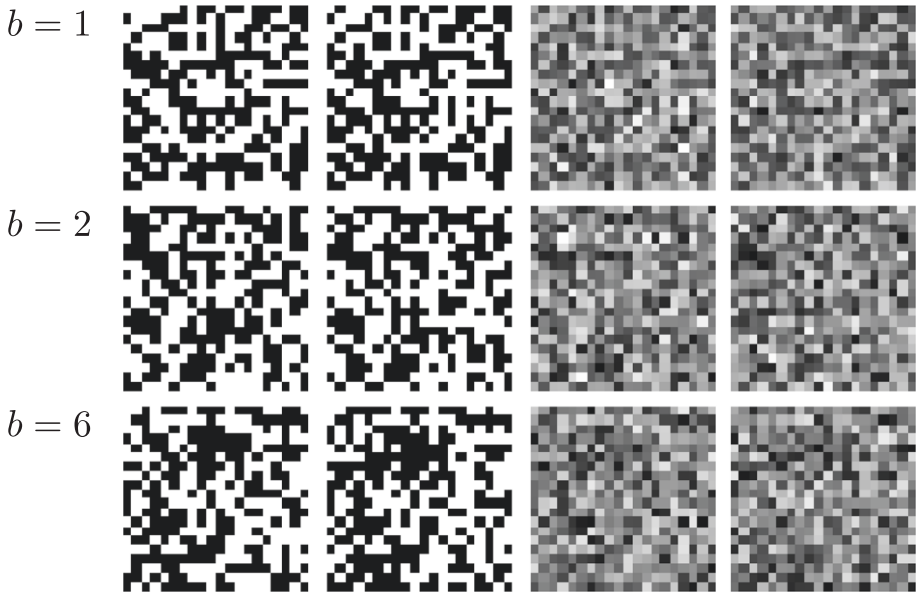

Figure 3 Example of a 20 × 20 code which is printed and scanned by an opponent. Main and opponent channels are identical, $m_b = 50$, $m_w = 150$, $\sigma_b = 40$, and $\sigma_w = 40$.

being detected. The opponent then tries to maximize the probability of false detection by choosing the adequate printing channel, and the legitimate sources will adopt the printing channel $\mathcal{C}_l$ which will minimize the probability of false detection. We end up with what is called a min-max game in game theory, where the optimal β^* is the solution of

$$\beta^* = \min_{\mathcal{C}_l} \max_{\mathcal{C}_o} \beta(\alpha). \tag{57}$$

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

Because the expressions of $\beta(\alpha)$ is not simple and have to be computed using the asymptotic expressions (31) and (32), we cannot solve this problem analytically and we have to use numerical calculus instead.

We conduct this analysis for the generalized Gaussian model, where we assume that the parameters m_b and m_w are constant for the main and the opponent channels (which implies that the scanning process has the same calibration for the two types of images). We assume that the main channel and the opponent channel variances are respectively denoted σ_m^2 and σ_o^2 and are identical for black and white dots.

5.1.2 Passive opponent

Here, the opponent has to undergo a channel identical to the main channel; the only parameter of the optimization problem (56) is consequently σ_m. Figure 5 presents the evolution of β w.r.t. σ_m for $\alpha = 10^{-6}$ and $m_b = 50$, $m_w = 150$. 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 $b = 1$. 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 very small, hence the estimation of the original code is easy) or very large (i.e., when the print and scan noise is so important that the original and forgery become equally noisy).

5.1.3 Active opponent

In this setup, the opponent can use a channel of different variance σ_o^2 than the main channel σ_m^2 and tries to solve the game defined in (57). Figure 6 shows the evolutions of β w.r.t. σ_o for different σ_m. We can see that in each case it is in the opponent interest to optimize his channel. Note that even if we assume that the opponent print and scan channel is perfect ($\hat{\mathbf{x}}^N = \mathbf{z}^N$), because the input of the printer has to be binary and because the opponent will make decoding errors by estimating the original code, the copied printed code will be necessarily different from the original printed code (see Figure 1), which implies a perfect discrimination between the two hypotheses.

Figure 7 shows the evolution of best opponent strategy $\max_{\sigma_o} \beta$ w.r.t. σ_m. By comparing it with Figure 5, we can see that the opponent's probability of non-detection can be multiplied by one or several orders of magnitude ($\times 10^7$ for $b = 1$, $\times 10^5$ for $b = 2$, and $\times 10$ for $b = 6$).

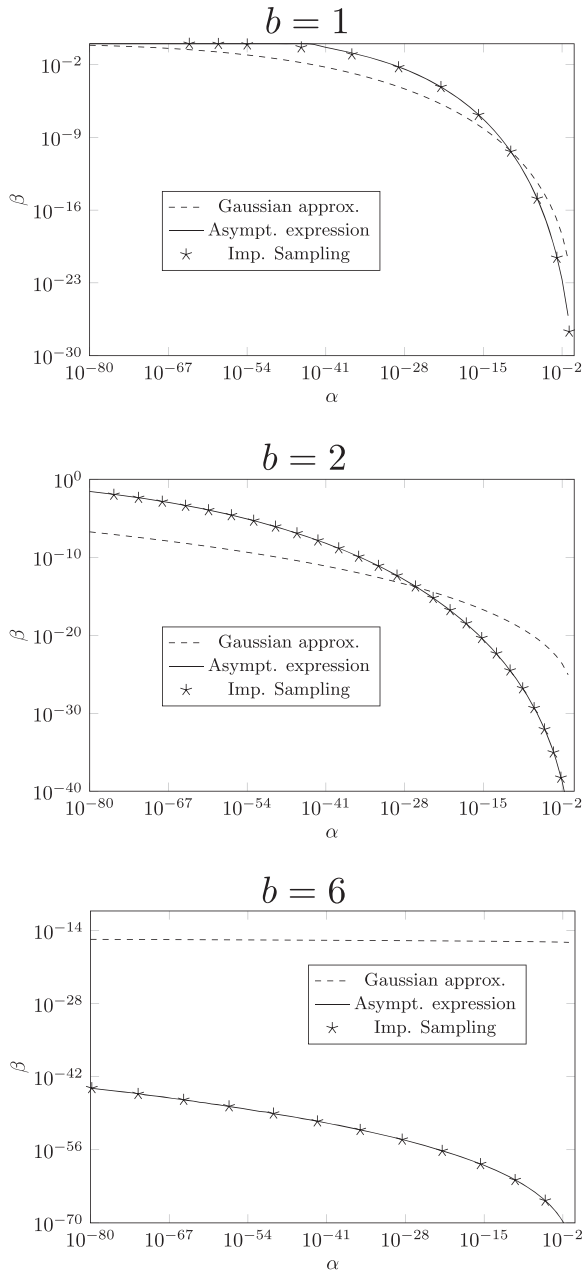

Figure 4 Comparison between the Gaussian approximation, the asymptotic expression, and Monte Carlo simulations for $b = 1$, $b = 2$, and $b = 6$. Main and opponent channels are identical, $m_b = 50$, $m_w = 150$, $\sigma_b = 40$, and $\sigma_w = 40$.

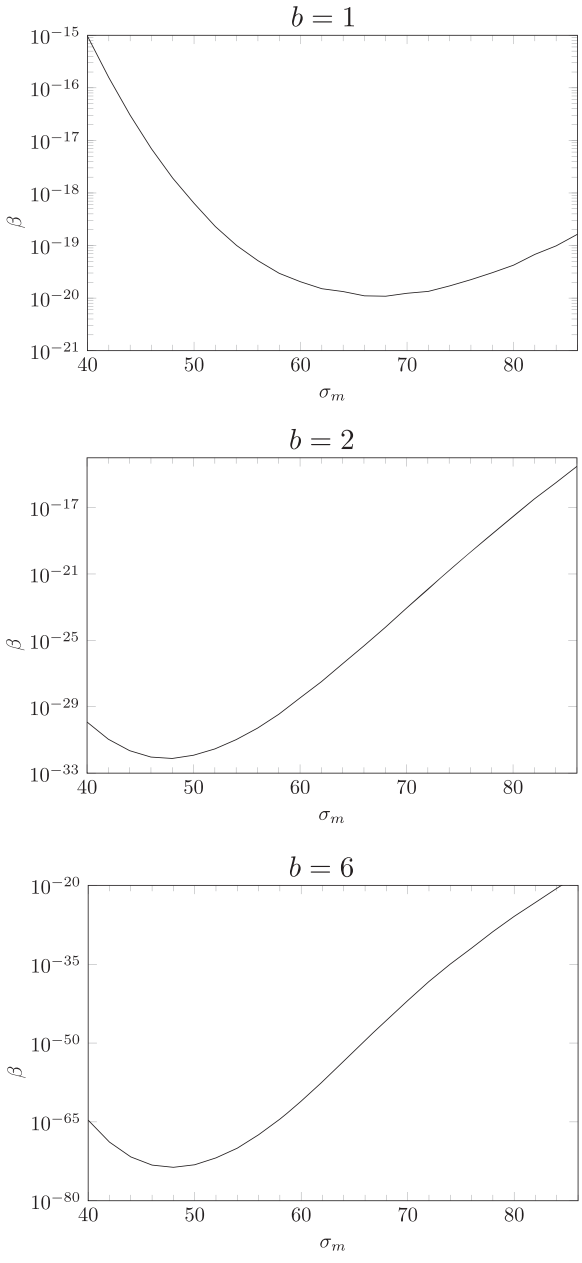

Figure 5 Evolution of β w.r.t. σ_m ($\alpha = 10^{-6}$). Main and opponent channels are identical, $m_b = 50$ and $m_w = 150$.

6 Impact of the estimation of the print and scan channel

The previous scenarios assume that the receiver has a full knowledge of the print and scan channel. Here, we assume that the receiver also has to estimate the opponent channel before performing authentication. From the estimated parameters, the receiver will compute a threshold and a log-likelihood test. Depending on the number of observations N_o, the estimated model and test will decrease the performance of the authentication system.

We consider that the opponent uses a different printing device unknown from the legitimate party. According to (6) and (7), the parameters to be estimated are $P_{e,W}$, $P_{e,B}$, m_b, m_w, and $\sigma = \sigma_b = \sigma_w$. We use the classical expectation maximization (EM) algorithm combined with Newton's method to solve the maximization step as these

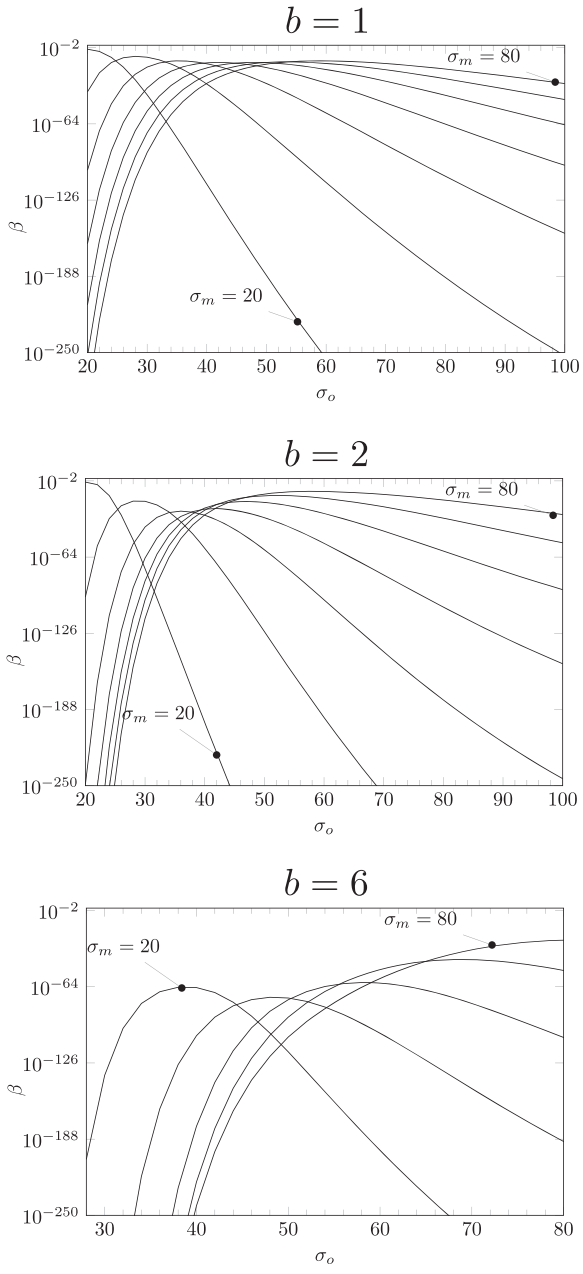

Figure 6 Evolution of the probability of non-detection β w.r.t. σ_o for different σ_m. The plots arriving from left to right show σ_m varying from 20 to 80 with an increment of 10. $m_b = 50$, $m_w = 150$, and $\alpha = 10^{-6}$.

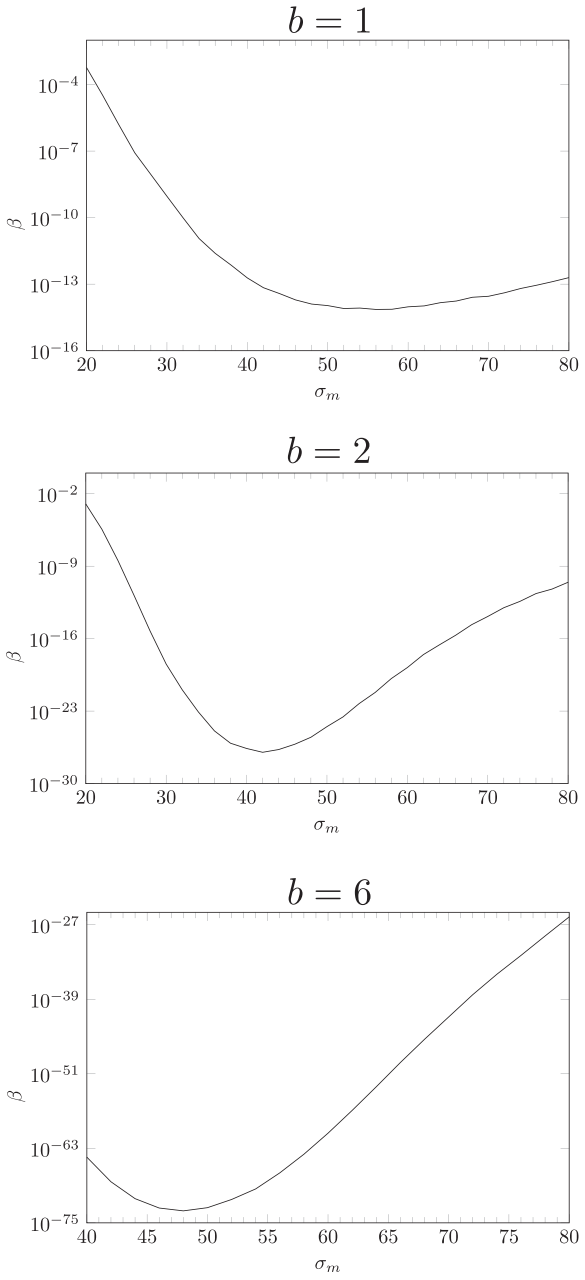

Figure 7 Evolution of best opponent strategy $\max_{\sigma_o} \beta$ w.r.t. σ_m. $m_b = 50$, $m_w = 150$, and $\alpha = 10^{-6}$.

distributions are discrete and have the finite support of the gray-level range.

Figure 8 shows the authentication performances using an estimated Gaussian model ($b = 2$) from $N_o = 2,000$ observed symbols. We can notice that the performance is very close to an exact knowledge of the model. This analysis shows also that if the receiver has some assumptions of the opponent channel and enough observations, he should perform model estimation instead of using the thresholding strategy. Figure 9 shows the importance of model estimation when comparing it to a blind authentication test when the receiver assumes that both the opponent channel and his channel are identical.

7 Conclusions

This paper brings numerous conclusions on the authentication using binary codes corrupted by a manufacturing stochastic noise:

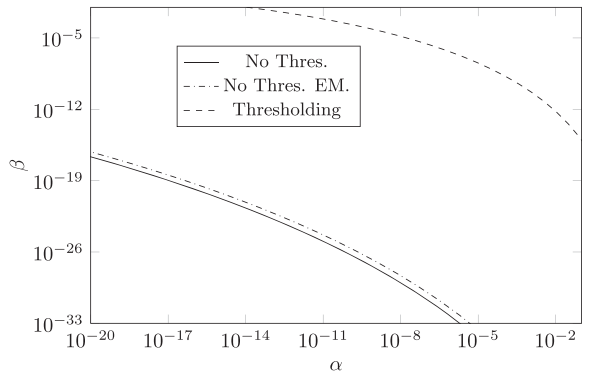

Figure 8 Authentication performance using model estimation with the EM algorithm ($N = 2,000$, $N_o = 2,000$, $\sigma = 52$, $m_b = 50$, and $m_w = 150$). The asymptotic expression is used to derive the error probabilities.

- The nature of the receiver's input is of upmost importance, and thresholding is a bad strategy with respect to getting an accurate version of the genuine or forged code, except if the system requires it, due for example to computational requirements.
- The Gaussian approximation used to compute the ROC of the authentication system are not valuable anymore for very low type I or type II errors. Cramér Chernoff bound or Monte Carlo simulations using importance sampling can be used instead to achieve accurate values of these probabilities. The proposed methodology is not impacted by the nature of the noise and can be applied for different memoryless channels that are more realistic for modeling the printing process.

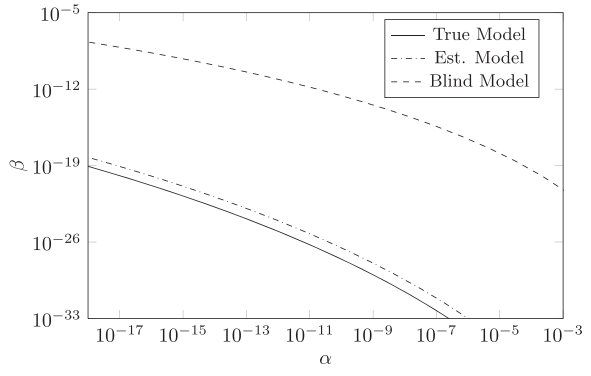

Figure 9 Importance of model estimation when compared to a blind authentication test. ROC curves comparing different degrees of knowledge about the opponent channel while the true opponent printing process model has parameters ($\sigma = 40$, $m_b = 40$, and $\mu_w = 160$). 'True model': the receiver knows exactly this model, 'Blind model': the receiver uses arbitrarily his printing process to model it, and 'Est. model': the receiver estimates the opponent channel using $N_o = 2,000$ observations.

- It is in the opponent's interest to adapt its channel in order to decrease the authentication performances of the system; this can be possible by solving a max-min game.
- If the opponent's print and scan channel remains unknown for the receiver, he can use estimation techniques such as the EM algorithm in order to estimate the channel.

Our future works will consist in evaluating the impact of the noise model on the authentication performance; this first analysis suggests that sparse distributions are less favorable for authentication than dense distributions, but this has to be confirmed by a deeper study.

Endnote

[a]One can show that $e^{-s\lambda} g_L(s; H_j)$ is a convex function of s.

Appendix

Information theoretic comparison between hypothesis testing with and without thresholding

In this appendix, we aim at establishing an inequality between the average of the two log-likelihood tests (14) and (15). The greater is the discrimination between the two distributions involved in the log-likelihood test, the best is the authentication performance. The expected value of the log-likelihood test (12) with respect to any of the two distributions involved in the ratio is the Kullback-Leibler divergence or *discrimination* defined as

$$L(P^N_{Y|X}; P^N_{Z|X}) = \sum_{\nu^N \in \mathcal{V}^{\mathcal{N}}} P^N_{Y|X}(\nu^N \mid x^N) \log \frac{P^N_{Y|X}(\nu^N \mid x^N)}{P^N_{Z|X}(\nu^N \mid x^N)}, \tag{58}$$

the base of the logarithm being arbitrary. In the remainder of this paper, we settle on base 2.

In ([14], p. 114), the author provides an interesting inequality relating the discrimination to type I and type II errors in hypothesis testing. This relation is stated by the following lemma:

Lemma 1. *(see the former reference for the proof) For any partition $(\mathcal{H}_0, \mathcal{H}_1)$ of the observation space $\mathcal{V}^N$, the probabilities of type I and II errors satisfy*

$$L(P^N_{Y|X}; P^N_{Z|X}) \geq \alpha \log \frac{\alpha}{1-\beta} + (1-\alpha) \log \frac{1-\alpha}{\beta}. \tag{59}$$

In our authentication model, the likelihood test is performed conditionally to an available side information involving two types of data x. One type for black points and the second one for white points in the original code. In accordance to this, we express now the discrimina-

tion quantity for the two proposed strategies in order to establish the desired inequality:

$$L(P^N(\tilde{X}^N \mid x^N, H_0)\,;\, P^N(\tilde{X}^N \mid x^N, H_1)) = \sum_{\tilde{x}_1} \cdots \sum_{\tilde{x}_N} P^N\left(\tilde{x}^N \mid x^N,\, H_0\right) \log \frac{P^N\left(\tilde{x}^N \mid x^N,\, H_0\right)}{P^N\left(\tilde{x}^N \mid x^N,\, H_1\right)}, \tag{60}$$

and

$$L(P^N(O^N \mid x^N, H_0)\,;\, P^N(O^N \mid x^N, H_1)) = \sum_{v_1} \cdots \sum_{v_N} P^N_{Y|X}(v^N \mid x^N) \log \frac{P^N_{Y|X}(v^N \mid x^N)}{P^N_{Z|X}(v^N \mid x^N)}. \tag{61}$$

For the sake of simplicity, we develop proofs and details for the second strategy only and give results for the thresholding case for which all developments are likewise the former. Regarding the additivity theorem ([14], theorem 4.3.7) for independent sequences and reminding that the distribution of each component of the sequence $(O^N \mid x^N)$ is the same for each type of data x, the discrimination quantity becomes

$$\begin{aligned} L(P^N(O^N \mid x^N, H_0)\,;\, P^N(O^N \mid x^N, H_1)) &= N_W \times \sum_{v \in \mathcal{V}} P_{Y|X}(v \mid 1) \log \frac{P_{Y|X}(v \mid 1)}{P_{Z|X}(v \mid 1)} \\ &\quad + N_B \times \sum_{v \in \mathcal{V}} P_{Y|X}(v \mid 0) \log \frac{P_{Y|X}(v \mid 0)}{P_{Z|X}(v \mid 0)}. \end{aligned} \tag{62}$$

Given a composition (or relative frequency) for X $P_X = \{N_W/N\,,\ N_B/N\}$, we have

$$\begin{aligned} &L(P^N(O^N \mid X^N, H_0)\,;\, P^N(O^N \mid X^N, H_1)) \\ &\quad = N \times L(P_{Y|X};\, P_{Z|X} \mid P_X), \end{aligned} \tag{63}$$

where $L(P_{Y/X};\, P_{Z/X} \mid P_X)$ is the average discrimination. Similarly, we obtain for the first strategy the relation

$$L(P^N(\tilde{X}^N|X^N, H_0); P^N(\tilde{X}^N|X^N, H_1)) = N \times L(P_{e,x}; \tilde{P}_{e,x} \mid P_X). \tag{64}$$

Corollary 1. *Given an i.i.d outcome $X^N = x^N$ with composition, or type P_X, for any partition of the observation space $(\mathcal{H}_0,\ \mathcal{H}_1)$, the probabilities of type I and II errors satisfy*

$$L(P_{Y|X}; P_{Z|X} \mid P_X) \geq \frac{1}{N}\left(\alpha \log \frac{\alpha}{1-\beta} + (1-\alpha) \log \frac{1-\alpha}{\beta}\right). \tag{65}$$

Proof. The proof is straightforward by combining (59) and (63). □

Corollary 2. *Consider a partition of the observation space $(\mathcal{H}_0,\ \mathcal{H}_1)$ with probability of type I error α; then, the probability of type II error is lower bounded by*

$$\beta \geq 2^{-[NL(P_{Y|X};P_{Z|X}|P_X)+h(\alpha)]/(1-\alpha)}. \tag{66}$$

Proof. From the previous corollary, we have

$$-(1-\alpha)\log\beta \leq NL(P_{Y|X};\, P_{Z|X} \mid P_X) - \alpha \log \alpha - (1-\alpha)\log(1-\alpha) + \alpha \log(1-\beta).$$

Setting $h(\alpha) = -\alpha \log \alpha - (1-\alpha)\log(1-\alpha)$, which is the binary entropy (≤ 1), and observing that $\alpha \log(1-\beta) \leq 0$, we can write the inequality

$$-(1-\alpha)\log\beta \leq NL(P_{Y|X};\, P_{Z|X} \mid P_X) + h(\alpha). \tag{67}$$

□

It is desired that this lower bound is very small which is obviously possible with large values of the quantity $L(P_{Y|X};\, P_{Z|X} \mid P_X)$.

Theorem 1. *For the two strategies of the receiver, we have $L(P_{Y|X};\, P_{Z|X} \mid P_X) \geq L(P_{e,x};\, \tilde{P}_{e,x} \mid P_X)$*

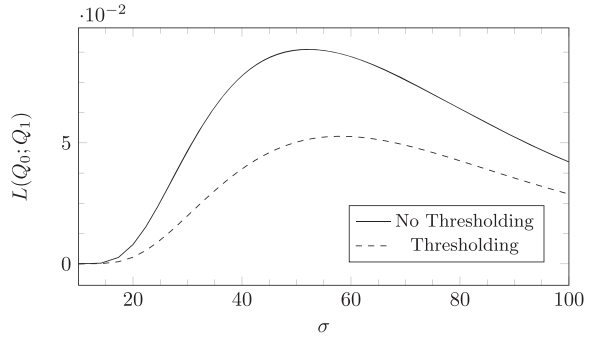

Figure 10 Comparison between the Kullback-Leibler divergences. Kullback-Leibler divergence function for the two different strategies w.r.t. the standard deviation of the Gaussian model of the physical devices.

Proof.

$$
\begin{aligned}
&L(P_{Y|X};\, P_{Z|X} \mid P_X)\\
&\quad= \sum_{x=0,1} P_X(x) \sum_{v\in\mathcal{V}} P_{Y|X}(v \mid x) \log \frac{P_{Y|X}(v \mid x)}{P_{Z|X}(v \mid x)},\\
&\qquad \sum_{x=0,1} P_X(x) \sum_{v\in\mathcal{D}_{\mathcal{W}}} P_{Y|X}(v \mid x) \log \frac{P_{Y|X}(v \mid x)}{P_{Z|X}(v \mid x)},\\
&\qquad + \sum_{x=0,1} P_X(x) \sum_{v\in\mathcal{D}^c_{\mathcal{W}}} P_{Y|X}(v \mid x) \log \frac{P_{Y|X}(v \mid x)}{P_{Z|X}(v \mid x)},\\
&\quad\overset{(a)}{\geq} \sum_{x=0,1} P_X(x) \sum_{v\in\mathcal{D}_{\mathcal{W}}} P_{Y|X}(v \mid k) \log \frac{\sum\limits_{v\in\mathcal{D}_{\mathcal{W}}} P_{Y|X}(v \mid x)}{\sum\limits_{v\in\mathcal{D}_{\mathcal{W}}} P_{Z|X}(v \mid x)},\\
&\qquad + \sum_{x=0,1} P_X(x) \sum_{v\in\mathcal{D}^c_{\mathcal{W}}} P_{Y|X}(v \mid x) \log \frac{\sum\limits_{v\in\mathcal{D}^c_{\mathcal{W}}} P_{Y|X}(v \mid x)}{\sum\limits_{v\in\mathcal{D}^c_{\mathcal{W}}} P_{Z|X}(v \mid x)},\\
&\quad\overset{(b)}{=} \sum_{x=0,1} P_X(x) \left(P_{e,x} \log \frac{P_{e,x}}{\tilde{P}_{e,x}} + (1-P_{e,x}) \log \frac{(1-P_{e,x})}{(1-\tilde{P}_{e,x})} \right),\\
&\quad= \sum_{x=0,1} P_X(x) L(P_{e,x}, \tilde{P}_{e,x} \mid x),\\
&\quad= L(P_{e,x}, \tilde{P}_{e,x} \mid P_X).
\end{aligned}
$$

□

(a) is obtained from the log-sum inequality: $\sum_{i=1}^{N} a_i$

$$\log \frac{a_i}{b_i} \geq \left(\sum_{i=1}^{N} a_i \right) \log \frac{\sum\limits_{i=1}^{N} a_i}{\sum\limits_{i=1}^{N} b_i}.$$

(b) since $P_{e,x} = \sum_{v\in\mathcal{D}_{\mathcal{W}}} P_{Y|X}(v \mid x)$, $\tilde{P}_{e,x} = \sum_{v\in\mathcal{D}_{\mathcal{W}}} P_{Z|X}(v \mid x)$, $1-P_{e,x} = \sum_{v\in\mathcal{D}^c_{\mathcal{W}}} P_{Y|X}(v \mid x)$, $1-\tilde{P}_{e,x} = \sum_{v\in\mathcal{D}^c_{\mathcal{W}}} P_{Z|X}(v \mid x)$.

Figure 10 plots a comparison between the Kullback-Leibler divergences with and without thresholding w.r.t. the variance of Gaussian model of the physical devices, we can see that the divergence is smaller with thresholding than without.

Competing interests
The authors declare that they have no competing interests.

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

Author details
[1]Institut-Telecom-LAGIS, Telecom-Lille, Rue Guglielmo Marconi, Villeneuve-d'Ascq 59650, France. [2]LAGIS, Telecom-Lille, Rue Guglielmo Marconi, Villeneuve-d'Ascq 59650, France. [3]CNRS-LAGIS, Cite Scientifique, 59651, Villeneuve-d'Ascq 59650, France.

Received: 21 October 2013 **Accepted:** 17 April 2014
Published: 5 June 2014

References

1. WCO, Global congress addresses international counterfeits threat immediate action required to combat threat to finance/health. http://www.wcoomd.org/en/media/newsroom/2005/november. Accessed 14 Nov 2005
2. WCO, Counterfeiting and piracy endangers global economic recovery, say global congress leaders. http://www.wipo.int/pressroom/en/articles/2009/article_0054.html. Accessed 3 Dec 2009
3. T Haist, HJ Tiziani, Optical detection of random features for high security applications. Optic. Comm. **147**(1–3), 173–179 (1998)
4. GE Suh, S Devadas, Physical unclonable functions for device authentication and secret key generation, in *Proceedings of the 44th Annual Design Automation Conference* (ACM, San Diego, 2007), pp. 9–14
5. MD Gaubatz, SJ Simske, S Gibson, Distortion metrics for predicting authentication functionality of printed security deterrents, in *16th IEEE International Conference on Image Processing (ICIP), 2009* (Cairo, IEEE, Piscataway, 2009), pp. 1489–1492
6. SS Shariati, FX Standaert, L Jacques, B Macq, MA Salhi, P Antoine, Random profiles of laser marks, in *Proceedings of the 31st WIC Symposium on Information Theory in the Benelux* (Rotterdam, 11–12 May 2010)
7. J Picard, J Zhao, Improved techniques for detecting, analyzing, and using visible authentication patterns. WO Patent WO/2005/067,586 (28 July 2005)
8. J Picard, C Vielhauer, N Thorwirth, Towards fraud-proof, ID documents using multiple data hiding technologies and biometrics, in *SPIE Proceedings–Electronic Imaging, Security and Watermarking of Multimedia Contents VI* (San Jose, 2004), pp. 123–234
9. C Baras, F Cayre, 2D bar-codes for authentication: a security approach, in *Proceedings of EUSIPCO 2012* (Bucarest, 27 Sept 2012)
10. M Diong, P Bas, C Pelle, W Sawaya, Document authentication using 2D codes: maximizing the decoding performance using statistical inference, in *Communications and Multimedia Security* (Springer, Kent, 2012), pp. 39–54
11. AE Dirik, B Haas, Copy detection pattern-based document protection for variable media. Image Process. IET. **6**(8), 1102–1113 (2012)
12. F Beekhof, S Voloshynovskiy, F Farhadzadeh, Content authentication and identification under informed attacks, in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)* (IEEE, Tenerife, 2012), pp. 133–138
13. Ho A-T Phan, Mai B-A Hoang, W Sawaya, P Bas, Document authentication using graphical codes: impacts of the channel model, in *ACM Workshop on Information Hiding and Multimedia Security* (Montpellier, ACM, New York, 2013)
14. RE Blahut, *Principles and Practice of Information Theory*, vol. 1, ((Addison-Wesley, 1987)
15. J Picard, Digital authentication with copy-detection patterns. Electron. Imaging. **5310**, 176–183 (2004)
16. A Dembo, *Large Deviations Techniques and Applications*. Stochastic Modelling and Applied Probability, vol. 38. (Springer, 2010)
17. RG Gallager, *Information Theory and Reliable Communication*, vol. 15. (Wiley, 1968)
18. JM Hammersley, DC Handscomb, G Weiss, Monte Carlo methods. Phys. Today. **18**, 55 (1965)
19. C-Y Lin, S-F Chang, Distortion modeling and invariant extraction for digital image print-and-scan process, in *Proceedings of International Symposium on Multimedia Information Processing* (Taipei, Dec 1999)

doi:10.1186/1687-417X-2014-9
Cite this article as: Phan Ho *et al.*: **Document authentication using graphical codes: reliable performance analysis and channel optimization.** *EURASIP Journal on Information Security* 2014 **2014**:9.