Received May 30, 2019, accepted August 14, 2019, date of publication August 26, 2019, date of current version September 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2937465

A Watermarking Technique to Secure Printed Matrix Barcode—Application for Anti-Counterfeit Packaging

HOAI PHUONG NGUYEN[1,2], FLORENT RETRAINT[2], FRÉDÉRIC MORAIN-NICOLIER[1], AND ANGÈS DELAHAIES[1]

[1]CReSTIC Laboratory, University of Reims Champagne-Ardenne, 51100 Reims, France
[2]Institute Charles-Delaunay, University of Technology of Troyes, 10300 Troyes, France

Corresponding author: Florent Retraint (florent.retraint@utt.fr)

ABSTRACT Counterfeiting of consumer goods is a critical problem which causes various negative impacts for consumers, enterprises and the whole economic ecosystem. Anti-counterfeit labels and packaging is one of the main solutions to help enterprises protect their brand against this concern. In this paper, we introduced a novel watermarking technique, which embeds a particular random micro-texture into a matrix barcode and transforms this one into a security layer for making packaging anti-counterfeited. The secured matrix barcode is hard to be reproduced by counterfeiters. In fact, any degradations caused by the counterfeiting process will change the statistical behaviors of the embedded micro-texture. Statistical detectors based on the hypothesis testing framework are also introduced to classify authentic and counterfeited printed barcodes. Experimental results confirm the usability and the effectiveness of the proposed anti-counterfeiting solution.

INDEX TERMS Anti-counterfeiting, printed watermarking, matrix code, statistical hypothesis testing.

I. INTRODUCTION AND STATE OF ART

Nowadays, counterfeiting of consumer goods is becoming an ongoing concern for consumers, enterprises and the whole society. We can discover counterfeit goods in many domains, such as toys, food, textiles, medication, etc. Consumers are the first victims. They receive poor-quality goods at an excessive price, and these products may threaten their health and safety. The circulation of these products also involves social costs and the losses of unpaid tax for governments. For legitimate-brand companies, they lost a part of their market. Consumers' bad experiences caused by counterfeit products can also endanger the reputation and value of the brand.

Companies have to have more awareness for fighting against counterfeiters to protect themselves and their consumers. They have to make sure that their trademark is adequately protected against the menace. A myriad of technologies [1], such as holograms [2], RFID [3]–[5] ou NFC tags [6], [7], biometric markers or inks [8],... are proposed to preserve and certify the authenticity of products. These solutions vary considerably in their sophistication and cost. For low-cost products, such as medicines or textiles, companies are not willing to pay for an expensive RFID tag or hologram. A cheaper solution would be more appreciated in this case.

Using matrix barcodes, such as QR codes [9], is a cheap and effective solution to embed the identification or tracking information of products in their packaging. However, they cannot be used as a security element for fighting counterfeiting. These codes are easy to be copied or regenerated. We can reproduce them without any difficulty from the message embedded, or we can create a fake one by scanning and reprinting an original printed code (Scan & Reprint attack). Therefore, the standard printed matrix barcodes are not appropriated to be used to verify the authenticity of products. However, we can improve the standard ones using watermarking techniques to make them hard to be copied or regenerated, and so a solution for product authentication.

Watermarking has been applied widely for multimedia copyright protection. Especially for digital images, a lots of works have been proposed in the literature such as [10]–[16] and so on. For printed images, some other works can be cited here [17]–[19]. Using watermarking to protect especially printed QR codes have been also proposed in several works.

Vongpradhip and Rungraungsilp [20] proposed to protect QR code by embedding an invisible watermark in the frequency domain. The authors in [21] and [22] suggested

The associate editor coordinating the review of this article and approving it for publication was Bora Onat.

inserting a secret message by using the error correction capacity of the QR code. This manipulation decreases the error correction capacity of the standard code. Keni *et al.* [23] developed a product authentication scheme using hash chains and printed QR codes. Their works focus only on the communication between the readers and the authentication server. The prevention of the code cloning is only considered in his scheme by limiting the number of times a product could be authenticated.

Picard [24] proposed a graphical code, called Copy-Detection pattern (CDP), which is printed on documents or packages. The pattern is sensible with the loss of information when documents go through a Print&Scan process. By measuring the amount of information contained in a scanned CDP, a CDP detector can decide the authenticity of the document. Reliable performance measurements, based on a Neyman-Pearson hypothesis test, of this authentication system were given in a work of Ho *et al.* [25]. Baras and Cayre [26] proposed also an application of this graphical code in protecting 2D matrix barcodes.

Tkachenko *et al.*, in [27], proposed to substitute the black modules of standard QR codes with a set of specific textured patterns in such a way that a private message can be encoded, which creates a second level of storage. The texture patterns are chosen to be sensitive to the Print-Scan (P&S) process. The public level of this code is read as normal as the one of the standard QR code. The private level is decoded by maximizing the correlation between each black module with the set of initial (numeric) patterns then linking it to a corresponding code-word. A copy attack implies two successive P&S processes, which degrade the patterns. The authenticity of the code is decided by thresholding the mean of the previously mentioned correlation. One of the limits of this approach is that the authentication process requires an exchange of original numerical texture patterns.

Wang *et al.* [28] exploited the particular optical characteristics of K, one of the four printed ink colors of a CMYK printer, the only color which can be rendered in infrared. The authors introduced an infrared watermarking technique to embed hidden information into the explicit graphic QR code, which permits its authentication. Teraura [29] also proposed to exploit the same characteristics of black ink under infrared to introduce a Double-Encode Two-Dimension code used for counterfeit prevention.

Standard matrix barcodes constitute of black modules on a white background. In our previous work [30], we proposed to substitute the background by a specific random texture, which is sensitive to P&S processes. The embedded texture does not affect the readability of the standard one. By studying the texture within the scanned barcodes, we can manage to take a decision on its authenticity. The proposed texture behaves randomly, and its behavior can be modeled statistically. A detector basing on the hypothesis testing framework was also proposed.

In this paper, we improve the previous solution by proposing a new statistical model to characterize the texture. By exploiting this model with the hypothesis testing framework, we proposed different powerful detectors to authenticate the proposed secured codes. For the sake of simplicity, we focused our study on QR barcodes. However, the proposed solution is, in general, also valid for another 2D matrix barcodes. We have compared the proposed solution with other detection techniques and security solutions for QR codes authentication. Experimental results show that the proposed solution is promising.

II. ORGANIZATION OF THE PAPER

The remainder of this paper is organized as follows. Firstly, in the section III, a description of the proposed secured QR code is given. In the section IV, we introduce a statistic of images in the DCT (Discrete Cosine Transform) domain. The statistical model of this statistic is also given. In the section V, we proposed a set of detectors by casting the detection problem in a hypothesis testing framework using the statistical model introduced in the previous section. Experimental results are given in the section VI. Finally, the paper is concluded by the section VII.

III. DESCRIPTION OF W-QR CODE

A. CONCEPT

The presentation of QR codes on physical surfaces implies a printing process. The reading of the codes implies after that a scanning process. Both these two processes add distortions. Therefore, the image treated by the reading/authentication system can be considered as a degraded version of the original digital code. A standard QR code is basically used to encode and transmit information. By its conception, the distortions caused by the P&S process, considered as noise, do not disturb the reading of the information transmitted. However, in authentication scenarios, these distortions can be interested thank to the physically unclonable characteristics of the P&S process [25].

Denote I_o and I respectively the original numerical code and the scanned image of the printed code. Assume that we can manage to model and stabilize the P&S process, denote $f_\theta^{PS}(.)$ the stochastic function which transforms I_o to I:

$$I = f_\theta^{PS}(I_o) \tag{1}$$

where θ is a set of unknown parameters which characterizes the stochastic behavior of the related P&S process. The function $f_\theta^{PS}(.)$ is physically unclonable. In practice, it is extremely hard to characterize this function. Its inverse function is therefore much more difficult to be figured out. By knowing I, it is hard to retrieve I_o. Inversely, it's also difficult to obtain a similar I by having I_o, unless you have the same printing system which is characterized by $f_\theta^{PS}(.)$. When I_o is a standard QR code, which simply consists of black and white modules, even when the function $f_\theta^{PS}(.)$ and its inverse are unknown, we can easily retrieve I_o basing on the information encoded. In order to exploit the P&S process as a key element to develop secured QR codes, we proposed to modify I_o to make it complicated so that retrieving I_o

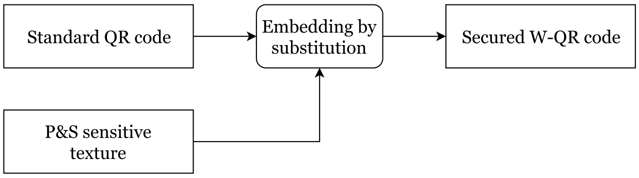


FIGURE 1. Proposed flowchart for the construction of W-QR.

from I requires a certain knowledge of the employed P&S process, not only the information encoded. In fact, we proposed to substitute the black and/or white modules of the standard codes by a specific texture. The texture embedded is configured so that they change the behavior of the codes under the P&S process but they do not disturb the normal reading of the information encoded. The figure 1 describes the general construction flowchart for our proposed secured QR code (a.k.a W-QR).

B. CLIPPING GAUSSIAN NOISE TEXTURE

The key problem in the proposed concept is the choice of the texture. There may be a lot of solutions for that; we can mention a type of texture proposed in [31]. In this paper, we propose to use the Clipping Gaussian Noise (CGN) texture described as follows. The CGN texture is created from an image of a 2D random Gaussian signal by replacing all values which are out of a predefined interval, denoted as clipping interval, by the interval boundary. In the case where the value of a pixel of an image is an integer encoded by 8 bits, its value varies from 0 to 255. A 2D random Gaussian signal, which is quantized to be an integer signal, takes its values over all the set of integers. By defining the clipping interval as [0, 255], the texture is created by replacing all the values which are higher than 255 by 255, and all the ones which are smaller than 0 by 0. The replacement creates an artificial clipping effect, which produces a texture saturated in the bright-rank or the dark-rank or both depending on the parameters configuring the random signal. In this condition, we can characterize the CGN texture by the mean μ and the standard deviation σ of the Gaussian random signal. Let denote $T_{\mu,\sigma}$ as the obtained texture. Figure 2 gives an illustration of the CGN texture; the texture presented in the figure is $T_{200,70}$.

In order to take in account the effect of the choice of the clipping interval, it is proposed to scale the previous signal by a factor ϵ and centered it around a value μ_0. So that, the final numeric definition of the proposed texture should be given as follows:

$$I_o = \mu_0 + \epsilon(T_{\mu,\sigma} - E(T_{\mu,\sigma})) \tag{2}$$

where $E(.)$ denotes the average operation.

In this work, we opted to substitute only the white background of the code by the proposed texture. The black modules are still black. Hence, the authenticity of the W-QR codes is decided from only the textured background. A set of preprocessing operations are needed to separate the two regions. In the context of this paper, we will not detail these operations. Figure 3 illustrates different versions of the proposed W-QR codes.

IV. STATISTICAL MODEL

Let divide an image into non-overlapping blocks and study each one in the frequency domain. In our work, the Discrete Cosine Transform (DCT) is employed to transform spatial images into a frequency presentation. We plan to work with JPEG format images. Since the JPEG compression algorithm is processed over 8 × 8 non-overlapping blocks, to assure the independence between the blocks; the size 8 × 8 block-size is opted in our study. Denote $\mathcal{I}$ the set of block index and z_i^s, $i \in \mathcal{I}$ and $s \in \{1, 2, \cdot\cdot, 64\}$, the $s-$th DCT coefficient of the i-th block. Denote $\mathcal{Z}_s = \{z_i^s | i \in \mathcal{I}\}$, the set of DCT coefficients within the s-th subband of all considered blocks.

Prior researches [32], [33] proved that the DCT coefficients within a subband can be considered as a sample of an independently and identically distributed (i.i.d) random variable. For printed W-QR images, the texture-embedded zone contains statistically the same information in their original digital version. They also passed through the same printing

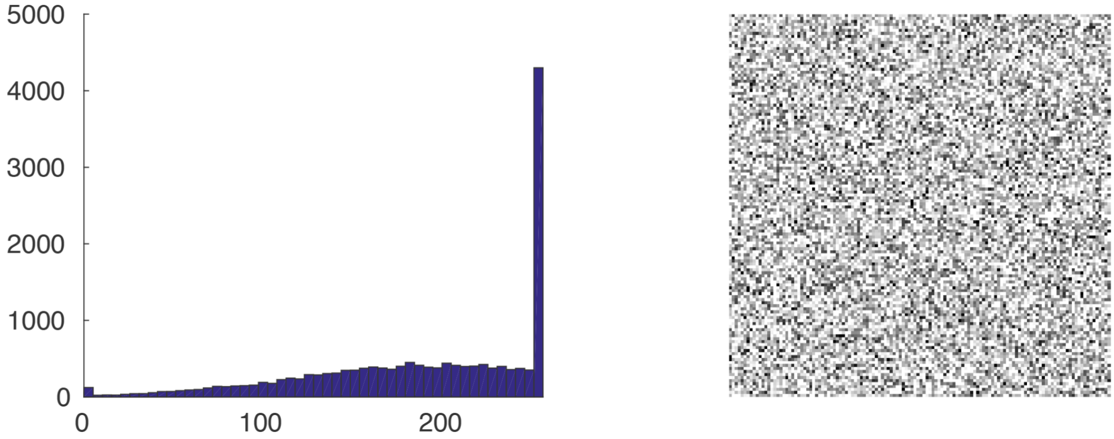


FIGURE 2. The digital version of CGN texture (right) and its histogram (left).

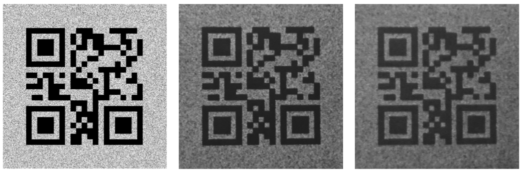


FIGURE 3. Different versions of W-QR (left to right): numeric version, printed genuine one, fake one created by printing the scanned version of the second one.

and acquisition process, which are assumed to be stable. The distortions caused by these processes are then probably similar between images. Consequently, the statistical behavior of these images in frequency domain should be similar, so that, in the DCT domain, the coefficients within a given subband should follow the same distribution for all images.

Falsified printed W-QR images, which were for example created by scanning genuine printed W-QR and then reprinting, should be affected by several distortions, that make them different from images of the genuine one. This difference can be observed in the frequency domain. By studying the statistical behavior of DCT coefficients, we can manage to detect falsified W-QR codes from genuine ones. Studying directly the distribution of DCT coefficients may be difficult. Under the assumption that $\mathcal{Z}_s$ is a sample of an i.i.d random variable, it is proposed to use the Variance Model presented in the Appendix to simplify our study.

Considering a given subband s, let devide $\mathcal{Z}_s$ into non-overlapping N-length subsets. Without lost of generality, the subband index will be omitted. For each element z_i, $i \in \mathcal{I}$, of $\mathcal{Z}_s$, let define x_i as follows:

$$x_i = (z_i - \bar{z})^2 \tag{3}$$

where $\bar{z}$ is the mean of the subset which contains z_i. Denote $X_s = \{x_i, i \in \mathcal{I}\}$, assuming that $\mathcal{Z}_s$ is i.i.d, Theorem 6 gives us that:

$$X_s \rightarrow \Gamma(\frac{1}{2}, 2\frac{N-1}{N}\sigma_0^2) \tag{4}$$

where σ_0 is the standard deviation of $\mathcal{Z}_s$.

V. IMAGE TEXTURE IDENTIFICATION SOLUTION

In the DCT domain, we have in total one DC subband and 63 AC subbands. The difference between genuine and falsified images is more significant in the low-level AC subbands. We may opt to exploit the subbands where the difference is the most significant to build a detector using the hypothesis testing framework. One-subband-sample-based detectors are proposed in detail in section V-A. We can also accumulate the difference from a sample of more than one subbands. Section V-B proposes a strategy to combine the statistics from these samples to build a detector.

A. ONE-SUBBAND-SAMPLE-BASED (OSSB) DETECTOR

For a given subband s, it is proposed to exploit the set X_s, considered also by $X = \{x_i, i \in \mathcal{I}\}$ in this case by omitting the index s, to build the detector. Noting that Z_s behaves differently from images of authentic textures to images of falsified ones. Hence, following Equation 4, our problem now is to decide between two hypotheses defined as follows:

$$\begin{cases} \mathcal{H}_0 : X \rightarrow \Gamma(a, b_0) \\ \mathcal{H}_1 : X \rightarrow \Gamma(a, b_1), b_1 \neq b_0 \end{cases} \tag{5}$$

where $a = \frac{1}{2}$. The parameter b_0 is known. The parameter b_1 can be known or unknown. In this paper, we focus on designing a test that allows us to guarantee a prescribed false alarm probability. Let

$$\mathcal{K}_{\alpha_0} = \{\delta : \mathbb{P}_{\mathcal{H}_0}[\delta(X) = \mathcal{H}_1] \leq \alpha_0\} \tag{6}$$

be the class of tests with a false alarm probability upper-bounded by α_0. Here $\mathbb{P}_{\mathcal{H}_k[E]}$ stands for the probability of event E under hypothesis $\mathcal{H}_k$, $k \in \{0, 1\}$. Assuming that b_1 is known, a Likelihood Ratio Test is given. We also proposed a Generalized Likelihood Ratio Test which covers the lack of knowledge of b_1.

1) LIKELIHOOD RATIO TEST (LRT) FOR TWO SIMPLE HYPOTHESES

In virtue of the Neyman-Pearson lemma [34], the most powerful test δ solving the problem 5 is the Likelihood Ratio Test given by the following decision rule:

$$\delta(X) = \begin{cases} \mathcal{H}_0 \text{ if } \Lambda(X) = \sum_{i\in\mathcal{I}} \Lambda(x_i) < \tau \\ \mathcal{H}_1 \text{ if } \Lambda(X) = \sum_{i\in\mathcal{I}} \Lambda(x_i) \geq \tau \end{cases} \tag{7}$$

where τ is the solution of the following equation:

$$\mathbb{P}_{\mathcal{H}_0}[\Lambda(X) \geq \tau] = \alpha_0 \tag{8}$$

and $\Lambda(x_i)$, the log-likelihood ratio of the observation x_i, is given as follows:

$$\Lambda(x_i) = log\frac{\mathcal{L}_1(x_i)}{\mathcal{L}_0(x_i)} = a \times log\frac{b_0}{b_1} + x_i \times (\frac{1}{b_0} - \frac{1}{b_1}) \tag{9}$$

where $\mathcal{L}_j(x_i), j \in \{0, 1\}$ is the likelihood function for the observation x_i under hypothesis $\mathcal{H}_j$, which is defined as follows:

$$\mathcal{L}_j(x_i) = \frac{1}{\Gamma(a)b_j^a} x_i^{a-1} exp(-\frac{x_i}{b_j})$$

So that,

$$\Lambda(X) = anlog\frac{b_0}{b_1} + (\frac{1}{b_0} - \frac{1}{b_1})\sum_{i\in\mathcal{I}} x_i \tag{10}$$

where n is the size of $\mathcal{I}$. The first term of $\Lambda(X)$ is constant, which could be omitted. Let define $\Lambda_1(X) = (\frac{1}{b_0} - \frac{1}{b_1})\sum_{i\in\mathcal{I}} x_i$. Under hypothesis $\mathcal{H}_k$, $k \in \{0, 1\}$, by employing the Central Limit Problem, we have that:

$$\Lambda_1(X) \sim \mathcal{N}(m_k, v_k) \tag{11}$$

where

$$m_k = nab_k\frac{b_1 - b_0}{b_0 b_1} \tag{12}$$

$$v_k = nab_k^2 \frac{(b_1 - b_0)^2}{b_0^2 b_1^2} \tag{13}$$

Let define

$$\Lambda^\star(X) = \frac{\Lambda_1(X) - m_0}{\sqrt{v_0}} \tag{14}$$

the rule 7 can be rewritten as follows:

$$\delta^\star(X) = \begin{cases} \mathcal{H}_0 \text{ if } \Lambda^\star(X) < \tau^\star \\ \mathcal{H}_1 \text{ if } \Lambda^\star(X) \geq \tau^\star \end{cases} \tag{15}$$

where $\tau^\star$ is a constant defined mathematically in function of the prescribed false-alarm probability. The decision threshold $\tau^\star$ and the power function $\beta_{\delta^\star}$ are given in the following theorem:

Theorem 1: When $b_j, j = \{0, 1\}$, are known, to obtain the prescribed false-alarm probability α_0, the decision threshold and the power function of the test $\delta^\star$ are given by:

$$\tau^\star = \Phi^{-1}(1 - \alpha_0) \tag{16}$$

$$\beta_{\delta^\star} = 1 - \Phi(\frac{m_0 - m_1 + \tau^\star\sqrt{v_0}}{\sqrt{v_1}}) \tag{17}$$

where $\Phi(.)$ and Φ^{-1} denote respectively the cumulative distribution function of the standard Gaussian random variable and its inverse.

2) GENERALIZED LIKELIHOOD RATIO TEST (GLRT)

When b_1 is unknown, the problem now is to verify whether the inspected texture image is to belong to the defined $\mathcal{H}_0$ texture family. By replacing b_1 in the equation 9 by $\hat{b}$, a consistent estimate of the scale parameter of the Gamma distribution, we obtain:

$$\hat{\Lambda}(x_i) = a \times log\frac{b_0}{\hat{b}} + x_i \times (\frac{1}{b_0} - \frac{1}{\hat{b}}) \tag{18}$$

where

$$\hat{b} = \frac{1}{na}\sum_{i \in \mathcal{I}} x_i \tag{19}$$

So that,

$$\hat{\Lambda}(X) = \sum_{i \in \mathcal{I}} \hat{\Lambda}(x_i) = \frac{1}{b_0}\sum_{i \in \mathcal{I}} x_i - na \times log(\frac{1}{n}\sum_{i \in \mathcal{I}} x_i) + C \tag{20}$$

where $C = nalog(b_0/a)$ is a constant which will be omitted in the following developments. We can rewrite the equation 20 by omitting the constant C as follows:

$$\hat{\Lambda}(X) = \frac{n}{b_0}\left[\bar{X} - ab_0 log(\bar{X})\right] \tag{21}$$

where $\bar{X}$ is the mean of the sample X, given by:

$$\bar{X} = \frac{1}{n}\sum_{i \in \mathcal{I}} x_i$$

Under hypothesis $\mathcal{H}_k, k \in \{0, 1\}$, by invoking the Central Limit Theorem, we have that:

$$\bar{X} \to \mathcal{N}(\mu_k, \sigma_k^2) \tag{22}$$

where

$$\sigma_k = \sqrt{\frac{a}{n}} b_k \quad \text{and} \quad \mu_k = ab_k. \tag{23}$$

Let $X^\star = \frac{\bar{X} - \mu_k}{\sigma_k}$, we have that:

$$X^\star \to \mathcal{N}(0, 1) \tag{24}$$

and under hypothesis $\mathcal{H}_k$, it follows that:

$$\hat{\Lambda}(X) = \frac{n}{b_0}\left[\sigma_k X^\star + \mu_k - \hat{\mu}_0 log(\mu_k)\right] - \frac{n}{b_0}\mu_0 log(\frac{\sigma_k}{\mu_k}X^\star + 1) \tag{25}$$

Taylor's theorem gives that:

$$log(\frac{\sigma_k}{\mu_k}X^\star + 1) \approx \frac{\sigma_k}{\mu_k}X^\star - \frac{\sigma_k^2}{2\mu_k^2}(X^\star)^2 \tag{26}$$

By combining the equations 25, 26 and 23, we obtain that:

$$\hat{\Lambda}(X) \approx \frac{1}{2}\left(X^\star + c_k\right)^2 + d_k, \tag{27}$$

where

$$c_k = \sqrt{na}\frac{b_k - b_0}{b_0}, \tag{28}$$

$$d_k = na\frac{b_k - b_0 log(ab_k)}{b_0} - \frac{1}{2}c_k^2. \tag{29}$$

Particularly, we have that $c_0 = 0$. Let define:

$$\hat{\Lambda}^\star(X) = 2\left(\hat{\Lambda}(X) - d_0\right). \tag{30}$$

Then, under hypothesis $\mathcal{H}_0$ we have that $\hat{\Lambda}^\star(X) \approx (X^\star)^2$, which behaves like a chi-square random variable with one d.f. So that, we have the following theorem:

Theorem 2: Under the hypothesis $\mathcal{H}_0$:

$$\hat{\Lambda}^\star(X) \to \chi^2(1). \tag{31}$$

Following Neyman-Peason lemma, the most powerful test $\hat{\delta}$ solving 5 is the Generalized Likelihood Ratio Test given by the following decision rule:

$$\hat{\delta}(X) = \begin{cases} \mathcal{H}_0 \text{ if } \hat{\Lambda}^\star(X) < \hat{\tau} \\ \mathcal{H}_1 \text{ if } \hat{\Lambda}^\star(X) \geq \hat{\tau} \end{cases} \tag{32}$$

where, again to ensure $\hat{\delta}$ to be in the class $\mathcal{K}_{\alpha_0}$, $\hat{\tau}$ is the solution of the equation

$$\mathbb{P}_{\mathcal{H}_0}\left(\hat{\Lambda}^\star(X) \geq \hat{\tau}\right) = \alpha_0 \tag{33}$$

Theorem 3: The threshold decision $\hat{\tau}$ and the power function $\beta_{\hat{\delta}}$ of the test $\hat{\delta}$ are given as follows:

$$\hat{\tau} = \Phi^{-1}_{\chi_1^2}(1 - \alpha_0), \tag{34}$$

$$\beta_{\hat{\delta}} = 1 - \Phi_{\chi^2_{1,\lambda}}\left(\hat{\tau} + 2(d_0 - d_1)\right), \tag{35}$$

where $\Phi^{-1}_{\chi_1^2}(.)$ denotes the inverse cumulative distribution function of a chi-square random variable with one d.f; $\Phi_{\chi^2_{1,\lambda}}$ denotes the cumulative distribution function of a non-central chi-square random variable with one d.f and the non-centrality parameter $\lambda = c_1^2$.

B. MULTIPLE-SUBBANDS-SAMPLE-BASED (MSSB) DETECTOR

When more than one subband are taken in account in the decision process, denote $\mathcal{I}_{sub}$ the set of interested subbands. Our goal is now to decide between two hypotheses defined for $\forall j \in \mathcal{I}_{sub}$ as follows:

$$\begin{cases} \mathcal{H}_0 : X_j \rightarrow \Gamma(a, b_{j0}) \\ \mathcal{H}_1 : X_j \rightarrow \Gamma(a, b_{j1}), b_{j1} \neq b_{j0} \end{cases} \tag{36}$$

Let denote $Xj = \{x_{ji}, i \in \mathcal{I}\}$, we have that:

$$\mathbb{P}(X_{j,\forall j \in \mathcal{I}_{sub}} | \mathcal{H}_k) = \prod_{j \in \mathcal{I}_{sub}} \prod_{i \in \mathcal{I}} \mathbb{P}(x_{ji} | \mathcal{H}_k) \tag{37}$$

where $k \in \{0, 1\}$. The log-likelihood ratio is then defined as follows:

$$\Lambda(X_{j,\forall j \in \mathcal{I}_{sub}}) = log \frac{\mathbb{P}(X_{j,\forall j \in \mathcal{I}_{sub}} | \mathcal{H}_1)}{\mathbb{P}(X_{j,\forall j \in \mathcal{I}_{sub}} | \mathcal{H}_0)}. \tag{38}$$

So that,

$$\Lambda(X_{j,\forall j \in \mathcal{I}_{sub}}) = \sum_{j \in \mathcal{I}_{sub}} \sum_{i \in \mathcal{I}} \Lambda_j(x_{ji}) \tag{39}$$

where

$$\Lambda_j(x_{ji}) = log \frac{\mathbb{P}(x_{ji} | \mathcal{H}_1)}{\mathbb{P}(x_{ji} | \mathcal{H}_0)}. \tag{40}$$

1) LRT FOR MULTIPLE SUBBANDS

In the case where we know $b_{j1}, \forall j \in \mathcal{I}_{sub}$, from the equations 10 and 39, we obtain:

$$\Lambda(X_{j,\forall j \in \mathcal{I}_{sub}}) = \mathcal{C} + \sum_{j \in \mathcal{I}_{sub}} \left(\frac{1}{b_{j0}} - \frac{1}{b_{j1}} \right) \sum_{i \in \mathcal{I}} x_{ji} \tag{41}$$

where $\mathcal{C}$ is a constant. For $j \in \mathcal{I}_{sub}$, $k \in \{0, 1\}$, and n the size of $\mathcal{I}$, denote:

$$m_{jk} = nab_{jk} \frac{b_{j1} - b_{j0}}{b_{j0} b_{j1}}, \tag{42}$$

$$v_{jk} = nab_{jk}^2 \frac{(b_{j1} - b_{j0})^2}{b_{j0}^2 b_{j1}^2}. \tag{43}$$

We have demonstrated in the previous section (ref. eq.11) that under hypothesis $\mathcal{H}_k$, we have:

$$\left(\frac{1}{b_{j0}} - \frac{1}{b_{j1}} \right) \sum_{i \in \mathcal{I}} x_{ji} \sim \mathcal{N}(m_{jk}, v_{jk}). \tag{44}$$

Hence, under $\mathcal{H}_k$:

$$\Lambda(X_{j,\forall j \in \mathcal{I}_{sub}}) \sim \mathcal{N}(m_k, v_k). \tag{45}$$

where $m_k = \mathcal{C} + \sum_{j \in \mathcal{I}_{sub}} m_{jk}$, and $v_k = \sum_{j \in \mathcal{I}_{sub}} v_{jk}$. Let define $\Lambda^\star(X_{j,\forall j \in \mathcal{I}_{sub}}) = \frac{\Lambda(X_{j,\forall j \in \mathcal{I}_{sub}}) - m_0}{\sqrt{v_0}}$, the decision rule is now exactly the same as defined in the equation 15. The theorem 1 is also verified in this case.

2) GLRT FOR MULTIPLE SUBBANDS

In this case, $b_{j1}, j \in \mathcal{I}_{sub}$ are unknown. An estimation of b_{j1} can be obtained from the sample as follows:

$$\hat{b}_{j1} = \frac{1}{na} \sum_{i \in \mathcal{I}} x_{ji} \tag{46}$$

By replacing b_{j1} by their consistent estimates $\hat{b}_{j1}$ in the equation 39, we obtain an estimate of $\Lambda(X_{j,\forall j \in \mathcal{I}_{sub}})$ as follows:

$$\hat{\Lambda}(X_{j,\forall j \in \mathcal{I}_{sub}}) = \mathcal{C} + \sum_{j \in \mathcal{I}_{sub}} \frac{n}{b_{j0}} \left[\bar{X}_j - ab_{j0} log(\bar{X}_j) \right] \tag{47}$$

where $\mathcal{C}$ is a constant which will be omitted in the next developments, and

$$\bar{X}_j = \frac{1}{n} \sum_{i \in \mathcal{I}} x_{ji}.$$

For $k \in \{0, 1\}$, denote that:

$$X_j^\star = \frac{\bar{X}_j - \mu_{jk}}{\sigma_{jk}} \tag{48}$$

where $\mu_{jk} = ab_{jk}$, and $\sigma_{jk} = \sqrt{\frac{a}{n}} b_{jk}$. Like in the equation 24, we obtain:

$$X_j^\star \sim \mathcal{N}(0, 1) \tag{49}$$

From the equations 47 and 48, by the same argument as given in the previous section to obtain the equation 27, we have:

$$\hat{\Lambda}(X_{j,\forall j \in \mathcal{I}_{sub}}) \approx \sum_{j \in \mathcal{I}_{sub}} \frac{1}{2} \left(X_j^\star + c_{jk} \right)^2 + \sum_{j \in \mathcal{I}_{sub}} d_{jk}, \tag{50}$$

where c_{jk} and d_{jk} are constant defined as follows:

$$c_{jk} = \sqrt{na} \frac{b_{jk} - b_{j0}}{b_{j0}}, \tag{51}$$

$$d_{jk} = na \frac{b_{jk} - b_{j0} log(ab_{jk})}{b_{j0}} - \frac{1}{2} c_{jk}^2. \tag{52}$$

Note that $c_{j0} = 0, \forall j \in \mathcal{I}_{sub}$. Let denote:

$$\hat{\Lambda}^\star(X_{j,\forall j \in \mathcal{I}_{sub}}) = 2 \left(\hat{\Lambda}(X_{j,\forall j \in \mathcal{I}_{sub}}) - \sum_{j \in \mathcal{I}_{sub}} d_{j0} \right) \tag{53}$$

then

$$\hat{\Lambda}^\star(X_{j,\forall j \in \mathcal{I}_{sub}}) \approx \sum_{j \in \mathcal{I}_{sub}} \left(X_j^\star \right)^2. \tag{54}$$

We can manage to obtain the following theorem.

Theorem 4: Under the hypothesis $\mathcal{H}_0$, Let denote N_s the size of $\mathcal{I}_{sub}$, we have:

$$\hat{\Lambda}^\star(X_{j,\forall j \in \mathcal{I}_{sub}}) \rightarrow \chi^2(N_s). \tag{55}$$

Following Neyman-Pearson lemma, the decision rule is then defined as follows

$$\tilde{\delta}(X_{j,\forall j \in \mathcal{I}_{sub}}) = \begin{cases} \mathcal{H}_0 \text{ if } \hat{\Lambda}^\star(X_{j,\forall j \in \mathcal{I}_{sub}}) < \tilde{\tau} \\ \mathcal{H}_1 \text{ if } \hat{\Lambda}^\star(X_{j,\forall j \in \mathcal{I}_{sub}}) \geq \tilde{\tau} \end{cases} \tag{56}$$

where, in order to ensure that $\tilde{\delta}$ is in the class $\mathcal{K}_{\alpha_0}$, $\tilde{\tau}$ is the solution of the following equation:

$$\mathbb{P}_{\mathcal{H}_0}\left(\hat{\Lambda}^{\star}(X_{j,\forall j\in\mathcal{I}_{sub}}) \geq \tilde{\tau}\right) = \alpha_0. \qquad (57)$$

Theorem 5: The threshold decision $\tilde{\tau}$ and the power function $\beta_{\tilde{\delta}}$ of the test $\tilde{\delta}$ are given as follows:

$$\tilde{\tau} = \Phi^{-1}_{\chi^2_{N_s}}(1-\alpha_0), \qquad (58)$$

$$\beta_{\hat{\delta}} = 1 - \Phi_{\chi^2_{N_s,\lambda}}\left(\tilde{\tau} + 2\sum_{j\in\mathcal{I}_{sub}}(d_{j0}-d_{j1})\right), \qquad (59)$$

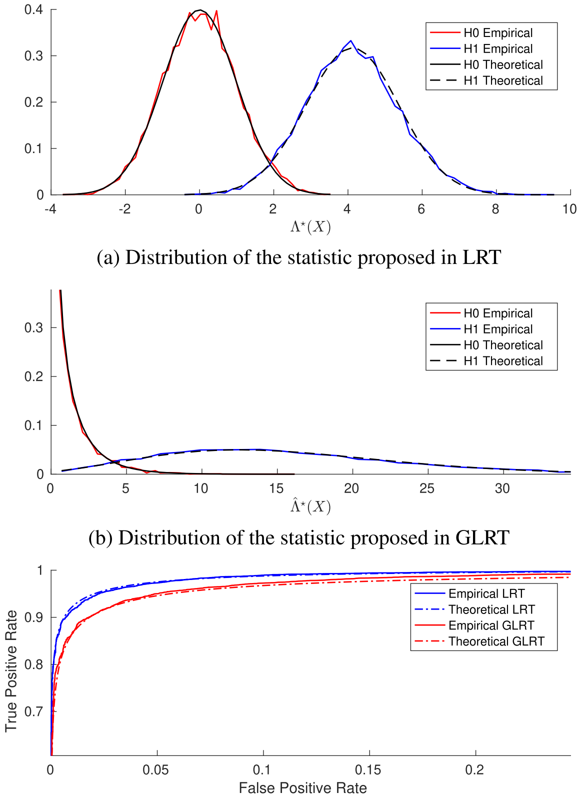
where $\Phi^{-1}_{\chi^2_{N_s}}(.)$ denotes the inverse cumulative distribution function of a chi-square random variable with N_s d.f; $\Phi_{\chi^2_{N_s,\lambda}}$ denotes the cumulative distribution function of a non-central chi-square random variable with N_s d.f and the non-centrality parameter $\lambda = \sum_{j\in\mathcal{I}_{sub}} c^2_{j1}$.

VI. NUMERICAL EXPERIMENTS

The construction of a real images database consumes too much time, especially in the case of our study, where we need a large number of images to validate the detectors proposed in the previous section. Therefore, we decided to test the proposed detectors first on a simulated database. The proposed detectors were first validated by simulated data which satisfy the given hypothesis, see section VI-A. In the section VI-B, we tested the proposed detectors on simulated images. The section VI-C gives the classification results of our detectors on a small real image database.

A. DETECTOR VALIDATION

In order to make sure that the construction of our detectors is correct, we test these detectors on simulated data, where we know exactly all the parameters of the tests. We generate 20000 data samples, one half for $\mathcal{H}_0$ hypothesis and the other half for $\mathcal{H}_1$ hypothesis. Each data sample is composed by 64 Gamma random variable subsamples. These Gamma random variables are characterized by a shape constant of $1/2$, and by a scale constant b_{jk}, where $j \in \{1, .., 64\}$ denotes the subsample index, and $k \in \{0, 1\}$ denotes the hypothesis index. The set of $\{b_{jk}\}$ is estimated from simulated images used in the section VI-B. Without the loss of generality, we took the first subsample to build the OSSB detectors. All the 64 subsamples were taken to build the MSSB detectors. Figure 4 gives a comparison between the empirical and theoretical distributions of the statistics proposed in the OSSB detectors, and a performance comparison between these detectors. Each empirical curve is well fitted by its theoretical counterpart. There is some loss of detection power observed in the case of the GLRT detector in comparison to the LRT detector. The lack of prior knowledge about the $\mathcal{H}_1$ hypothesis is the main cause of this detection power loss. We also obtained the same results for the MSSB detectors. Theses detectors outperform their OSSB-version counterpart.



(a) Distribution of the statistic proposed in LRT

(b) Distribution of the statistic proposed in GLRT

(c) ROC curvres

FIGURE 4. (a),(b) - Empirical and theoretical distributions of the statistics proposed in the OSSB detectors, and (c) - the performance comparison between these detectors.

B. CLASSIFICATION OF SIMULATED IMAGES

Print & Scan process introduces many kinds of distortions [35]. To produce simulated images, we have to mimic digitally the Print & Scan process, which is very complicated to model. There is no work in the literature which provides a complete model of the whole process. We separate the P&S process into two successive ones: the printing one and the acquisition one. The acquisition process is simply simulated by adding into images acquisition noise, which follows the heteroscedastic noise model proposed by T. H. Thai *et al.* in [36], [37]. The model provided for RAW images is employed for the sake of simplicity. This model is characterized by a couple of parameters (a, b), which models the linear relation between the variance and the expectation of image noise. The printing process involves many complicated digital and physical operations. To obtain a precise simulation of the process, it has to study each of these operations. We don't have the ambition to simulate the whole process because it is out of our expertise. In this study, by the limit of our knowledge, we tried only to produce some identified distortions in original images to obtain their simulated printed version. These operations are introduced in the Figure 5 and in the next paragraphs.

The proposed simulation of the printing process starts by scaling the initial digital image. In fact, due to the different nature of images in the digital and physical spaces, the image

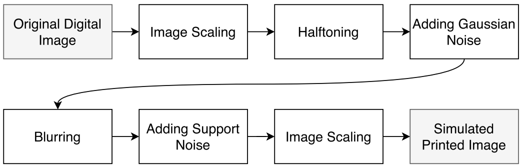


FIGURE 5. Proposed simulation of the printing process.

must be resampled to be adapted with the printer's resolution. After that, because that printers, especially Laser or Ink-jet models, can only print out black dots, the image to be printed has to be processed by a reprographic technique (i.e., halftoning, dithering) before being physically processed. The reprographic operation permits to transforms a gray image into another presentation, which consists only of black patterns. Furthermore, other unidentified distortions may be introduced during the digital operations of the printing process, such as quantification errors, rounding errors, etc. In our simulation scheme, we assumed that these distortions can be modeled by a zero-mean Gaussian noise. There are also distortions introduced during the physical operations. For Ink-jet printing technique, ink drops are physical objects. When they are projected onto paper, they transform into 2D dots with bigger radius. There would be some superposition between nearby dots. We can use a blurring process (i.e., 2D median or Gaussian filter) to simulate this physical effect. Furthermore, printing paper is not uniform. Physical micro-textures of the paper will affect the appearance of the final printed image. In our simulation, to take into account this deformation, some specific texture extracted from an image of a piece of real paper, is embedded into the simulated image. Real printed images are on physical support (i.e., paper). When we take a photo of a real object by a digital camera, photons emitted from the object would be projected onto the photovoltaic cells of the camera sensor. In function of the number of photons received, these cells will produce an electrical signal, which will be converted after that by a Analog/Digital Converter to produce a very first digital version of the image. Hence, this version is just a projection of the physical image onto a digital space. We assume that the camera sensor is ideally positioned so that the mentioned projection is orthogonal to the sensor plane. This projected version can be, therefore, considered as a scaling version of the printed one. The final simulated image is finally obtained by adding heteroscedastic noise on the projected image.

In our study, we have to create simulated version of genuine and falsified images. Figure 6 describes briefly the construction flowchart of proposed simulated images. Genuine images go through one P&S process. Meanwhile, falsified images go through two successive P&S process. In reality, the first scanning process and the second printing process are driven by counterfeiters to produce falsified codes from genuine codes. In general, these processes are not identical to the ones used in the creation of genuine codes. Samples of simulated images are given in the figure 7.

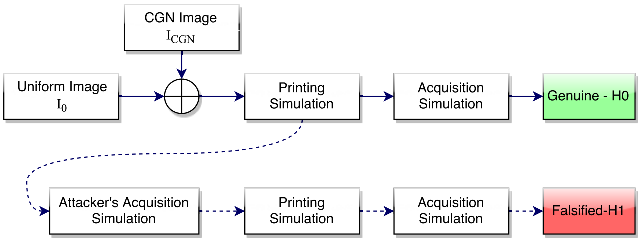
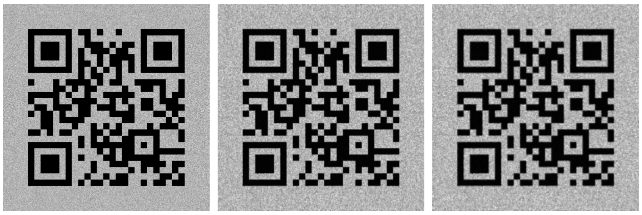


FIGURE 6. Construction flowchart for simulated images.



(a) Numerical (b) Genuine (c) Falsified

FIGURE 7. Sample of simulated images.

We generated 2000 simulated images, half of them genuine, other half are falsified. The CGN texture is created in the configurations given in the following table

TABLE 1. Parameters of CGN textures.

μ_0	ϵ	μ	σ
0.7	0.3	0.7843	0.3137

The noise models of the main acquisition process and the counterfeiter's acquisition process are configured respectively by $(a_0, b_0) = (4.5e-5, 5e-7)$ and $(a_1, b_1) = (7.5e-5, 1e-6)$. For the printing simulation, numerical image is firstly scaled up by a factor of 2. Then, a dithering algorithm using unclustered dot screen with 64 gray levels is applied. After adding some white noise, the image pass through a Gaussian filter to be blurred. Paper noise is extracted and embedded into the image after that. Finally, the image is scaled down by $\frac{1}{2}$ to obtained the final simulated printed image.

The difference between simulated genuine and falsified images is hardly visualized directly. However, in DCT domain, we can easily observe the discrimination between them. The figure 8 shows the distribution of DCT coefficients within the subband $(1, 2)$ under different hypotheses. Similar results are also obtained for the other DCT subbands.

Both OSSB and MSSB detectors were studied in this simulation. Without loss of generality, the subband $(1, 2)$ is opted to build the OSSB detectors. For the MSSB detectors, all the 64 subbands were used. In all of the cases, we obtained empirical distributions which were fitted correctly by their theoretical counterpart, Figure 9. The numerical results show that our proposed detectors have very high performance. The MSSB detectors behave better than the OSSB ones.

We also implemented an SVM classificator using the LBP descriptors as described in [38] to classify simulated images.

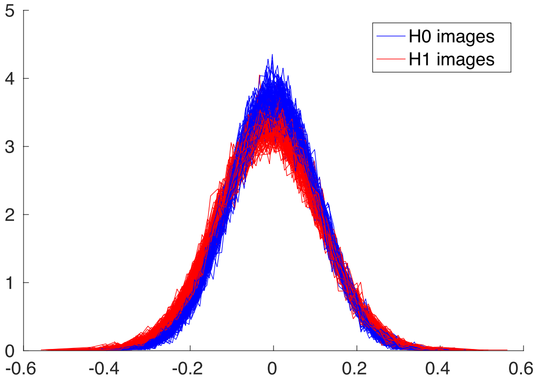


FIGURE 8. Distribution of DCT coefficients of images within subband (1, 2) under different hypotheses. Each curve represents the DCT coefficient histogram computed from one image. 100 images of each hypothesis were used to produce this diagram.

This classificator is used to compare with our proposed detectors. The SVM-LBP detector need to have data from both of the two hypotheses for training. So that, to be fair, we compare the SVM-LBP detector with our MSSB-LRT one.

Figure 10 gives the classification performance comparison between our proposed MSSB detectors and SVM-LBP one for simulated images of size 64 × 64 and 128 × 128. In both of the cases, the MSSB-LRT detector outperforms the SVM-LBP one. In the case of 128 × 128 image size, the MSSB-LRT detector manages to obtain a perfect classification.

The proposed WQR code has been also compared with the 2LQR code proposed by Tkachenko *et al.* [27] in term of authentication's performance. The same simulation process described as above has been applied on 2LQR digital codes to create simulated images of their authentic and falsified counterparts. Both of the two solutions can authenticate correctly all simulated images. In order to visualize the difference in the authentication's performance of the two solutions, it is supposed that falsified codes were created by printing the digital codes using a printing system lightly different from the one used to create authentic code. In this situation, by testing also on simulated images, the performance curves of the two solutions are given in the Figure 11. The proposed solution outperforms the reference one.

C. CLASSIFICATION OF REAL IMAGES

For real W-QR codes, only blocks situated in the background are interested. For the sake of simplicity, images without QR codes are used in this experiment. By using the same

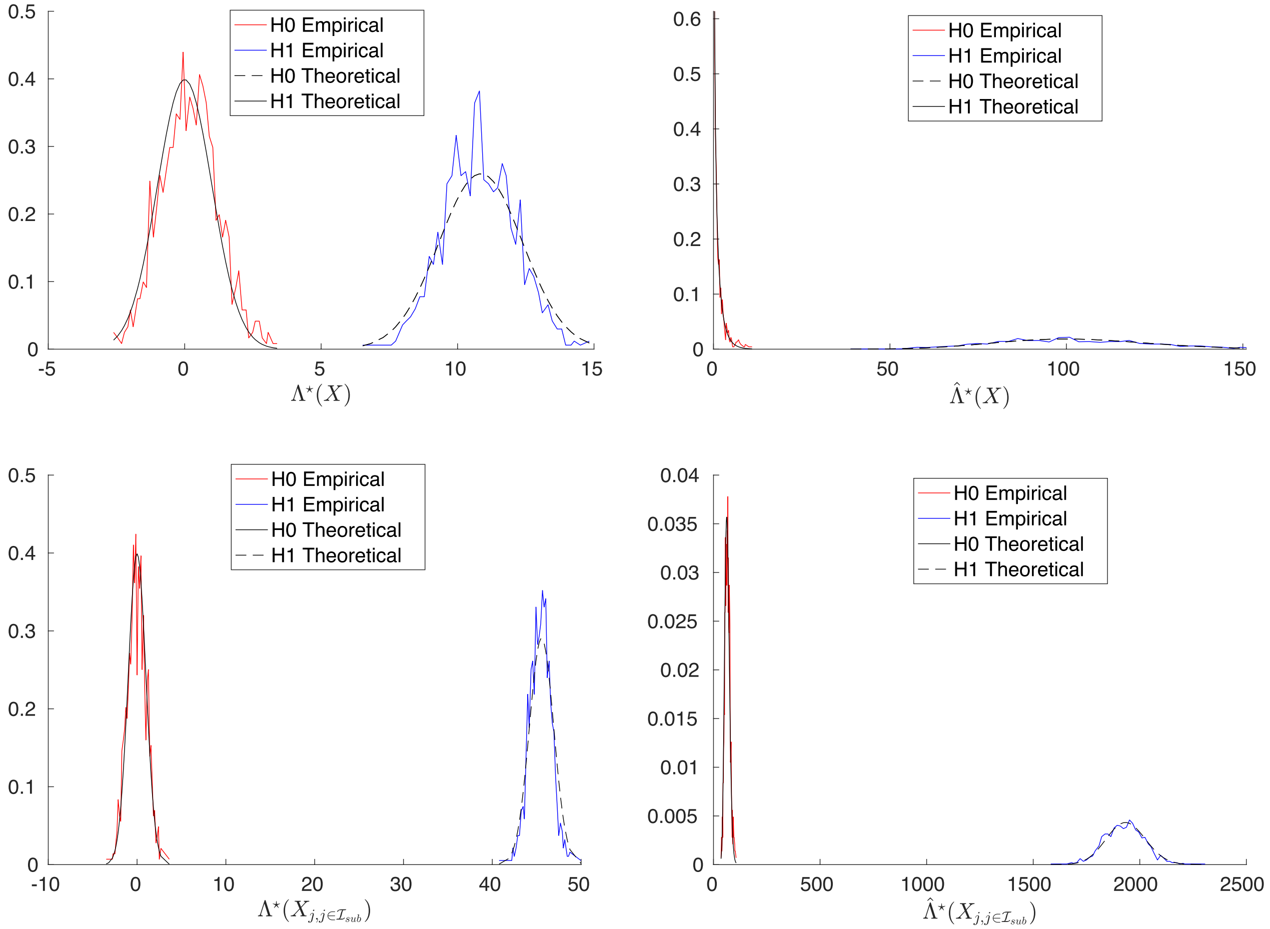
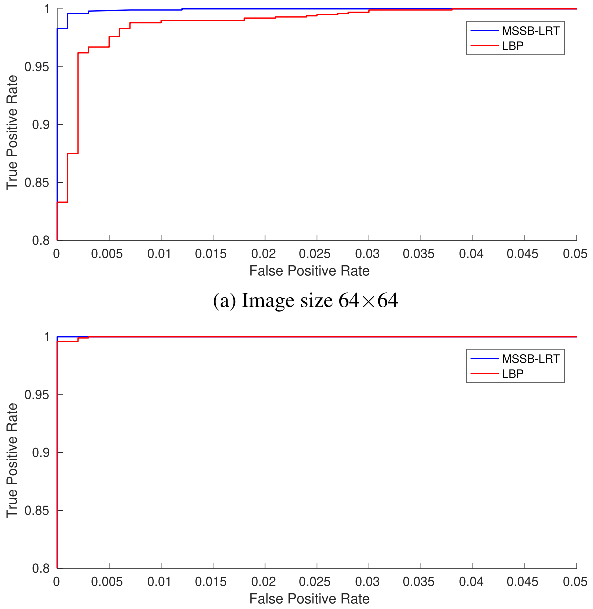


FIGURE 9. Empirical and theoretical distributions of the different proposed tests statistic introduced in the proposed detectors: OSSB-LRT (top-left), OSSB-GRLT (top-right), MSSB-LRT (bottom-left), and MSSB-GLRT (bottom-right).



(a) Image size 64×64

(b) Image size 128×128

FIGURE 10. Classification performance comparison between MSSB detectors and SVM-LBP one for different sizes of simulated images.

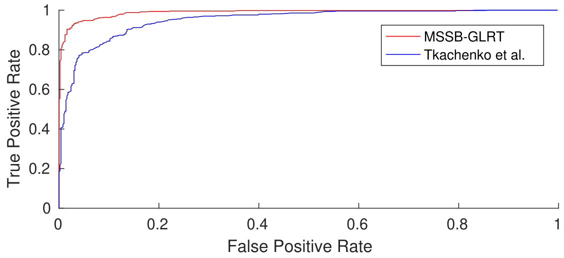


FIGURE 11. Authentication performance comparison between the proposed WQR code and Tkachenko et al.'s 2LQR code.

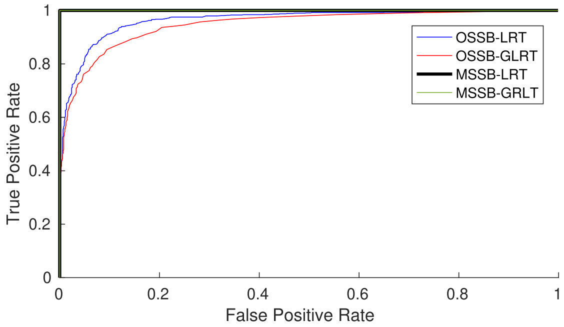


FIGURE 12. Empirical performance of the proposed detectors on real images database.

configuration as used in the simulation case, we created 900 digital images. These images were then printed out by a laser printer in 600 dpi on standard A4 papers to form 900 original 3x3-cm printed samples. After that, by scanning and reprinting each original printed sample, we obtained 900 falsified printed samples.

All the original and falsified printed samples were then digitized by a iPhone 7 camera at its highest resolution under an ISO constant. The distance between the camera and the printed sample is maintained at a constant value. All the images are taken under the best focus conditions. They are cropped to have the size 512 × 512. We took the $(1, 2)$ DCT channel to build the OSSB detectors and the first nine low-frequency AC channels to build the MSSB detectors. Figure 12 gives the empirical ROC curves of the proposed detectors. We manage to classify correctly all images using the MSSB detectors.

VII. CONCLUSION

In this paper, to use QR codes as an anti-counterfeiting solution for product labeling, we introduced a watermarking technique to secure them. A security level, which can prevent the illegal cloning of standard QR codes, is added by substituting the white background of the codes by a specific texture. The printing process will affect the visual behavior of the embedded texture by irreversibly degrading it. Counterfeiters need to have the digital codes and the same printing system as the constructor to produce valid secured codes, which is highly sophisticated. Furthermore, cloning an existing code by scanning and reprinting will change the behavior of embedded texture, and can be detected. Then, by analyzing the embedded texture, we can verify the validity of the printed QR codes, and by consequence, the genuity of the related product. We introduced a statistical model to describe the embedded texture. Basing on the given model, we proposed different code-cloning attack detectors using the framework of statistical hypothesis testing. These detectors were tested on both simulated and real images. We obtained high detection performances with the proposed detectors.

APPENDIX. VARIANCE MODEL

Theorem 6: Let $\mathcal{Z} = \{z_i | i \in \{1, 2, \dots, N\}\}$ is a sample of an independently and identically distributed random variable with the standard deviation σ_0. Considering S the estimate of the sample variance, we have:

$$S = \frac{1}{N-1} \sum_{i=1}^{M} S_i \tag{60}$$

where

$$S_i = (z_i - \bar{z})^2 \tag{61}$$

and $\bar{z} = \frac{1}{N} \sum_{i=1}^{N} z_i$. We have that:

$$S_i \rightarrow \Gamma(\frac{1}{2}, 2\frac{N-1}{N}\sigma_0^2) \tag{62}$$

and

$$S \rightarrow \Gamma(\frac{N}{2}, \frac{2\sigma_0^2}{N}) \tag{63}$$

Note that:

$$z_i - \bar{z} = \frac{1}{N} \sum_{j \neq i} (z_i - z_j).$$

By invoking the Central Limit Theorem, the distribution of $z_i - \bar{z}$ can be approximated by a normal one. Indeed, we have that:

$$E(z_i - \bar{z}) = E(z_i) - E(\bar{z}) = 0,$$
$$Var(z_i - \bar{z}) = Var(\frac{N-1}{N}z_i - \frac{1}{N}\sum_{j\neq i} z_j) = \frac{N-1}{N}\sigma_0^2.$$

So that,

$$z_i - \bar{z} \to \mathcal{N}(0, \sqrt{\frac{N-1}{N}}\sigma_0).$$

Let $\sigma_1 = \sqrt{\frac{N-1}{N}}\sigma_0$, we have that:

$$\frac{z_i - \bar{z}}{\sigma_1} \to \mathcal{N}(0, 1)$$

and so:

$$(\frac{z_i - \bar{z}}{\sigma_1})^2 \to \chi^2(1).$$

Denote $Y = (\frac{z_i - \bar{z}}{\sigma_1})^2$, so we have:

$$\frac{1}{N-1}(z_i - \bar{z})^2 = \frac{\sigma_1^2}{N-1}Y.$$

The Moment Generating Function of $\frac{\sigma_1^2}{N-1}Y$ is defined as follows:

$$M_{\frac{\sigma_1^2}{N-1}Y}(t) = E(e^{t\frac{\sigma_1^2}{N-1}Y}) = M_Y(\frac{\sigma_1^2}{N-1}t) = (1 - \frac{2\sigma_1^2}{N-1}t)^{\frac{-1}{2}}$$

which is identical to the one of a random variable following a Gamma distribution whose shape factor is $\frac{1}{2}$ and the scale factor is $\frac{2\sigma_1^2}{N-1} = \frac{2\sigma_0^2}{N}$. In recap, we have:

$$\frac{1}{N-1}(z_i - \bar{z})^2 \to \Gamma(\frac{1}{2}, \frac{2\sigma_0^2}{N}).$$

By comparing the Moment Generating Function, it gives that the sum of Gamma random variables which have the same scale factor is also a Gamma random variable whose scale factor is identical to the latter and the shape factor is the sum of all previous shape factors. So that, we have obtained the given theorem.

REFERENCES

[1] B. Gianmarco, S. Riccardo, N. F. Igor, T. Aris, and C. Enrico, "Survey of techniques for fight against counterfeit goods and intellectual property rights (IPR) infringing," EU Sci. Hub-Eur. Commission's Sci. Knowl. Service, Joint Res. Centre, Eur. Commission, Brussels, Belgium, 2015.

[2] J. Dittmann, L. C. Ferri, and C. Vielhauer, "Hologram watermarks for document authentications," in *Proc. Int. Conf. Inf. Technol., Coding Comput.*, Apr. 2001, pp. 60–64.

[3] M. O. Lehtonen, F. Michahelles, and E. Fleisch, "Trust and security in RFID-based product authentication systems," *IEEE Syst. J.*, vol. 1, no. 2, pp. 129–144, Dec. 2007.

[4] B. Song and C. J. Mitchell, "RFID authentication protocol for low-cost tags," in *Proc. 1st ACM Conf. Wireless Netw. Secur. (WiSec)*, 2008, pp. 140–147.

[5] C. E. Turcu, C. O. Turcu, M. Cerlinca, T. Cerlinca, R. Prodan, and V. Popa, "An RFID-based system for product authentication," in *Proc. Eurocon*, Jul. 2013, pp. 32–39.

[6] N. Alzahrani and N. Bulusu, "Securing pharmaceutical and high-value products against tag reapplication attacks using NFC tags," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2016, pp. 1–6.

[7] T. Hongthai and D. Thanapatay, "The development of encrypted near field communication data exchange format transmission in an NFC passive tag for checking the genuine product," in *Proc. 14th Int. Conf. Electr. Eng./Electron., Comput., Telecommun. Inf. Technol. (ECTI-CON)*, Jun. 2017, pp. 889–894.

[8] H. Nam, K. Song, D. Ha, and T. Kim, "Inkjet-printing-based structural coloring for anti-counterfeit applications," in *Proc. Transducers-18th Int. Conf. Solid-State Sens., Actuators Microsyst. (TRANSDUCERS)*, Jun. 2015, pp. 1417–1420.

[9] *Information Technology—Automatic Identification and Data Capture Techniques—Bar Code Symbology—QR Code*, Standard ISO/IEC 18004:2000, Mar. 2000.

[10] O.-J. Kwon, S. Choi, and B. Lee, "A watermark-based scheme for authenticating JPEG image integrity," *IEEE Access*, vol. 6, pp. 46194–46205, 2018.

[11] T. B. Taha, R. Ngadiran, and P. Ehkan, "Adaptive image watermarking algorithm based on an efficient perceptual mapping model," *IEEE Access*, vol. 6, pp. 66254–66267, 2018.

[12] W. Wan, J. Wang, M. Xu, J. Li, J. Sun, and H. Zhang, "Robust image watermarking based on two-layer visual saliency-induced JND profile," *IEEE Access*, vol. 7, pp. 39826–39841, 2019.

[13] Y. Tan, J. Qin, X. Xiang, W. Ma, W. Pan, and N. N. Xiong, "A robust watermarking scheme in YCbCr color space based on channel coding," *IEEE Access*, vol. 7, pp. 25026–25036, 2019.

[14] Q. Su, D. Liu, Z. Yuan, G. Wang, X. Zhang, B. Chen, and T. Yao, "New rapid and robust color image watermarking technique in spatial domain," *IEEE Access*, vol. 7, pp. 30398–30409, 2019.

[15] H. Sadreazami and M. A. Amini, "A robust image watermarking scheme using local statistical distribution in the contourlet domain," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 1, pp. 151–155, Jan. 2019.

[16] J. Liu, J. Huang, Y. Luo, L. Cao, S. Yang, D. Wei, and R. Zhou, "An optimized image watermarking method based on HD and SVD in DWT domain," *IEEE Access*, vol. 7, pp. 80849–80860, 2019.

[17] X. Yong, Y. Yi, T. Haihu, and W. Juanjuan, "Effect of embedding way on printed watermarking image by lithography," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery*, Oct. 2014, pp. 286–289.

[18] N. V. Kumar, K. Sreelatha, and C. S. Kumar, "Invisible watermarking in printed images," in *Proc. 1st India Int. Conf. Inf. Process. (IICIP)*, Aug. 2016, pp. 1–5.

[19] Y. Xiao, W. Zhang, and Y. Xie, "Influence of different color space on digital watermarking for anti-counterfeiting printed images," in *Proc. 27th Chin. Control Decis. Conf. (CCDC)*, May 2015, pp. 1535–1539.

[20] S. Vongpradhip and S. Rungraungsilp, "QR code using invisible watermarking in frequency domain," in *Proc. 9th Int. Conf. ICT Knowl. Eng.*, Jan. 2012, pp. 47–52.

[21] T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen, and T. D. Nguyen, "Robust message hiding for QR code," in *Proc. 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Aug. 2014, pp. 520–523.

[22] P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen, "Secret hiding mechanism using QR barcode," in *Proc. Int. Conf. Signal-Image Technol. Internet-Based Syst.*, Dec. 2013, pp. 22–25.

[23] H. Keni, M. Earle, and M. Min, "Product authentication using hash chains and printed QR codes," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 319–324.

[24] J. Picard, "Digital authentication with copy-detection patterns," *Proc. SPIE*, vol. 5310, pp. 176–183, Jun. 2004.

[25] A. T. P. Ho, B. A. M. Hoang, W. Sawaya, and P. Bas, "Document authentication using graphical codes: Reliable performance analysis and channel optimization," *EURASIP J. Inf. Secur.*, vol. 2014, no. 1, p. 9, Dec. 2014.

[26] C. Baras and F. Cayre, "2D bar-codes for authentication: A security approach," in *Proc. 20th Eur. Signal Process. Conf. (EUSIPCO)*, Aug. 2012, pp. 1760–1766.

[27] I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J.-M. Gaudin, and C. Guichard, "Two-level QR code for private message sharing and document authentication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 571–583, Mar. 2016.

[28] Y.-M. Wang, C.-T. Sun, P.-C. Kuan, C.-S. Lu, and H.-C. Wang, "Secured graphic QR code with infrared watermark," in *Proc. IEEE Int. Conf. Appl. Syst. Invention (ICASI)*, Apr. 2018, pp. 690–693.

[29] N. Teraura, "Counterfeit detection by smartphone using double-encoded two-dimensional code," in *Innovative Mobile and Internet Services in Ubiquitous Computing* (Advances in Intelligent Systems and Computing). Cham, Switzerland: Springer, Jul. 2017, pp. 455–466.

[30] H. P. Nguyen, A. Delahaies, F. Retraint, D. H. Nguyen, M. Pic, and F. Morain-Nicolier, "A watermarking technique to secure printed QR codes using a statistical test," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Nov. 2017, pp. 288–292.

[31] A. E. Dirik and B. Haas, "Copy detection pattern-based document protection for variable media," *IET Image Process.*, vol. 6, no. 8, pp. 1102–1113, Nov. 2012.

[32] T. H. Thai, R. Cogranne, and F. Retraint, "Statistical model of quantized DCT coefficients: Application in the steganalysis of JSteg algorithm," *IEEE Trans. Image Process.*, vol. 23, no. 5, pp. 1980–1993, May 2014.

[33] T. Qiao, F. Retraint, R. Cogranne, and C. Zitzmann, "Steganalysis of JSteg algorithm using hypothesis testing theory," *EURASIP J. Inf. Secur.*, vol. 2015, no. 1, Mar. 2015, Art. no. 2.

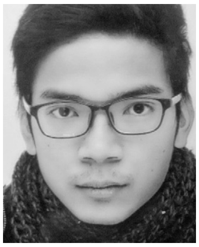
[34] J. Neyman and E. S. Pearson, "IX. On the problem of the most efficient tests of statistical hypotheses," *Philos. Trans. Roy. Soc. London. Ser. A*, vol. 231, nos. 694–706, pp. 289–337, Feb. 1933.

[35] K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran, and I. El-Khalil, "'Print and scan' resilient data hiding in images," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 4, pp. 464–478, Dec. 2006.

[36] T. H. Thai, F. Retraint, and R. Cogranne, "Generalized signal-dependent noise model and parameter estimation for natural images," *Signal Process.*, vol. 114, pp. 164–170, Sep. 2015.

[37] T. H. Thai, F. Retraint, and R. Cogranne, "Camera model identification based on the generalized noise model in natural images," *Digit. Signal Process.*, vol. 48, pp. 285–297, Jan. 2016.

[38] J. Määttä, A. Hadid, and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. IEEE Int. Joint Conf. Biometrics*, Oct. 2011, pp. 1–7.



HOAI PHUONG NGUYEN received the double Engineering Diploma/M.S degrees in information system security from the University of Technology of Troyes, in 2015, and the Ph.D. degree in image processing from the University of Reims Champagne-Ardenne, Reims, France, in March, 2019. His research interests include statistical image processing, hypothesis testing theory, and digital image forensics.

FLORENT RETRAINT received the M.Sc. degree in applied mathematics and the Ph.D. degree in image processing from the National Institute of Applied Sciences of Lyon, France, in 1994 and 1998, respectively. He is currently a Full Professor with the University of Technology of Troyes. His research interests include image modeling, statistical image processing, hypothesis testing theory, and anomaly detection and localization, with a main application to digital image forensics.

FRÉDÉRIC MORAIN-NICOLIER received the M.Sc. degree in applied physics and the Ph.D. degree in image processing from the University of Bourgogne, France, in 2000. He is currently a Full Professor with the University of Reims Champagne-Ardenne, where he is integrated with the CREsTIC Laboratory. His research interests include image processing and analysis, similarity measures and dissimilarity detection, and biomedical imaging.

ANGÈS DELAHAIES received the Ph.D. degree in image processing from the University of Angers, France, in 2011. She is currently an Associate Professor with the University of Reims Champagne-Ardenne. Her research interest includes image comparison and similarity measures and dissimilarity detection.