# A WATERMARKING TECHNIQUE TO SECURE PRINTED QR CODES USING A STATISTICAL TEST

*H.Phuong Nguyen*[⋆] *Agnès Delahaies*[⋆] *Florent Retraint*[†]
*D.Huy Nguyen*[†] *Marc Pic* [*] *Frédéric Morain-Nicolier*[⋆]

[⋆] CReSTIC, URCA, Reims France
[†]LM2S, ICD, UTT, Troyes, France
[*] Group SURYS, Paris, France

## ABSTRACT

The QR (Quick Response) code is a two-dimensional barcode, which was designed for storage information and high-speed reading applications. Being cheap to produce and fast to read, it becomes actually a popular solution for product labeling. Ones try to make QR code a solution against counterfeiting. In this paper, we present a novel technique that permits to create a secure printed QR code which is robust against Scan & Reprint attack. The code is constructed by replacing the background of the standard one by a specific textured pattern which does not affect the normal reading of the encoded message. Scan & Reprint attacks lead to the degradation of the texture and change its statistical characteristics, which can be detected thanks to a statistical hypothesis testing. The experimental results show a good performance of the proposed solution.

*Index Terms*- QR code, counterfeiting, watermarking, statistical hypothesis testing, Scan & Reprint attack

## 1. INTRODUCTION

Nowadays, counterfeiting is a growing problem all over the world. It happens in many domains, especially in industry. Counterfeit products cause financial losses for legitimate brands, involve social costs and the losses of unpaid tax for governments. The ultimate victims of counterfeiting are the consumers. They receive poor-quality goods at an excessive price and these products may threaten their health and safety. Bad experiences caused by these products of consumers may then inevitably lead to the loss in terms of brand image.

Companies are becoming increasingly aware of the problems of counterfeiting. These ones want vitally to make sure that their trademark are adequately protected and to implement anti-counterfeiting policies to deal with the menace. A myriad of technologies, such as holograms, RFID ou NFC tags, biometric markers and inks,... can be employed to protect and authenticate genuine products [1]. These solutions vary considerably in sophistication and cost. In order to be implemented, the solution must be cost-effective. For low-cost products, such as basic medicines, companies will not want to pay for an expensive RFID tag or an hologram to protect it. A cheaper solution would be more appreciated in this case.

Printed QR code [2] is a cheap and effective solution to embed identification or tracking information of products. However, it does not contain any element which permits to prevent the illegal reproduction of the code by imitation. Ones can regenerate the code from the message embedded or create a falsified one by scanning an reprinting the genuine printed code (Scan & Reprint attack). Therefore, we can not use standard printed QR codes to authenticate products. However, we can improve the standard one to make itself robust against imitation, and so a solution to authenticate products.

We may refer to the state-of-art in the field of printed document authentication.

A technique [3] using specific graphical codes, which are sensitive with the loss of information when images go through a Print&Scan process, called copy detection patterns, permits to distinguishing original document from its copies. This technique is used in [4] and [5] to fight against counterfeiting.

Tkachenko *et al.*, in [6], proposed to substitute the black modules of standard QR code 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 Print-Scan (P&S) process. The public level of this code is read as normal as standard QR code. The private level is decoded by maximizing the correlation values between each black module with the set of initial (numeric) patterns then linking it to the corresponding codeword. A copy attack implies two successive P&S processes, which degrade the patterns. Authenticity of the code is decided by evaluating the pattern degradation with a threshold of the mean of the mentioned correlation values. The limit of this approach is that the authentication process required an exchange of original numerical texture patterns.

In this paper, we present a novel technique to secure printed QR code. The code, named as W-QR where W stands

978-1-5090-5990-4/17/$31.00 ©2017 IEEE

for *watermarked*, is created by substituting the background of standard QR code by a specific random texture. The texture employed must be sensitive with P&S processes in such a way that we can manage to make a decision in the authentication of the W-QR by studying the texture. A particular random textured pattern have been proposed, which have a stable statistical behavior that can be modeled.

The remainder of this paper is organized as follows. Firstly, in the section 2, we describe the schemes to create and evaluate a general W-QR code. Then, in the section 3, we present the description of the texture that we used to create our W-QR and the statistical model to characterize it. A statistical test based on the proposed model is also given. Experimental results are given in the section 4. Finally, the paper is concluded by the section 5.

## 2. CONCEPT OF W-QR CODE

### 2.1. Construction

The proposed W-QR code has to satisfy two conditions. Firstly, public information of the code could be read normally by standard reading applications. It means that the security level must not interfere with the reading process of the standard information. Secondly, the security level has to be sensitive with the P&S processes and possesses a specific characteristic with permits to authenticate genuine code from fake ones.

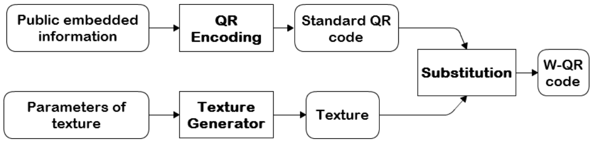

**Fig. 1**. Proposed flowchart for the construction of W-QR.

The figure 1 describes the general construction flowchart for our proposed W-QR. Firstly, binary QR codes, which encodes the product public information, are generated by standard generation algorithms. We generate then a texture which is characterized by a private key or by some secret setting parameters. After that, we combine the generated texture with the binary QR code by substitution to construct W-QR code.

The key problem in this concept is the choice of texture. There may be a lot of solutions for that; we can mention a type of texture proposed in [7]. In this paper, we propose to use our own one, described in the section 3. We opt to substitute the proposed texture with only the background of QR code. Black modules still stay black to ensure the readability of the QR numeric code. The figure 2 gives an example of resulted W-QR code; printed and illegal version are also given next to.

### 2.2. Reading and Authentication

The reading process is simple, described by the flowchart given in the figure 3. Public information encoded by the QR code are decoded by standard reading application. These data are then used to extract precisely the background of W-QR code which contains the embedded texture. By analyzing the characteristics of extracted texture, we manage to make a decision in the authentication of the W-QR code.

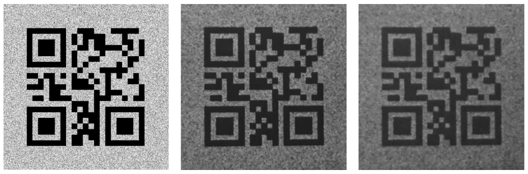

**Fig. 2**. Different versions of W-QR (left to right): numeric version, printed genuine one, fake one created by printing the scanned version of the second one.

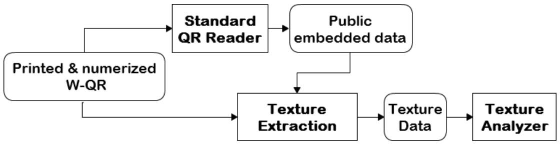

**Fig. 3**. Proposed flowchart for the reading and validation of W-QR.

Perfect fake W-QR code can be produced by attackers when they figure out the private key or the secret parameters of the texture embeded and have on their hand a similar printinng system. However, degradations caused by printing and scanning proccess are irreversible. Therfore, it is extremely hard for attackers to regenerate a correct numeric version of the W-QR code. Even when the construction mecanism of exploited texture is revealed, attackers have also to scan all the parameters space by brute force to find the good ones. It's a time-consuming operation and hard to achieve, especially when they don't have a priori knowlegde about the used printing system of constructor.

## 3. CLIPPING GAUSSIAN NOISE TEXTURE

### 3.1. Concept

The proposed Clipping Gaussian Noise (CGN) texture is characterized by a couple of two parameters $(\mu, \sigma)$. A $M$x$N$ CGN texture is created from a $M$x$N$ matrix of $\mu$-mean and $\sigma$-standard deviation Gaussian noise by replacing all the values which are greater than 255 by 255, and all the values 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 value of $(\mu, \sigma)$. Denote $\text{CGN}_{\mu,\sigma}$ the texture characterized by the couple $(\mu, \sigma)$. The figure 4 shows an example of the $\text{CGN}_{200,70}$ texture and its histogram.

The proposed CGN textures are highly sensitive with the P&S processes. From a printed and scanned version of the

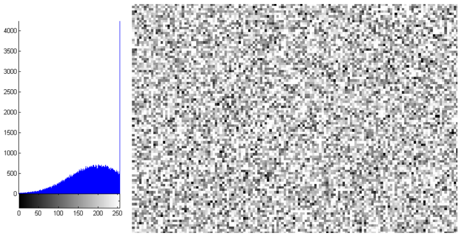

**Fig. 4**. CGN (right to left): the texture and its histogram.

CGN texture, the reconstruction of initial numeric one is extremely hard as we know that the P&S processes are irreversible. From the side of counterfeiters, the guess of the correct $(\mu, \sigma)$ values employed is also highly sophisticated.

A statistical feature is proposed in 3.2 to describe printed and scanned CGN textures, denoted the CGN feature. This one cumulates all the effects of: the choice of $(\mu, \sigma)$ and the degradations caused by P&S processes. Supposing that the textures are scanned in the same conditions, the feature is essentially affected by the choice of the couple $(\mu, \sigma)$ and the printing process.

Therefore, if counterfeiters have the numeric version of CGN texture, but they have not the same printing process as constructors, experimental results show that the proposed feature can still help us to detect falsified textures.

### 3.2. CGN feature

We subdivide the printed and scanned CGN texture image into blocks of size 8x8. This size is chosen to be conforming with the block size of the DCT transformation during the JPEG compression process. For simplicity, the index of blocks will be omitted in the following development. For a given block, denote $N_i$ the value of pixel $i$ with $i \in \{0, 1, .., 63\}$ within the block and $\overline{N}$ the average of these values.

$$\overline{N} = \frac{1}{64} \sum_{j=0}^{63} N_j. \tag{1}$$

The block variance is then defined by:

$$\sigma_b^2 = \frac{1}{63} \sum_{i=0}^{63} (N_i - \overline{N})^2 \tag{2}$$

The pixel values of numeric texture are independently and identically distributed (i.i.d) random variables. Suppose that the noises added to image through Print&Scan processes are i.i.d, we can obtain that the $N_i$ values are also i.i.d random variables. By the same reasoning as given in our previous works [8],[9] we can prove that the distribution of $\sigma_b^2$ can be approximated by a Gamma distribution $\Gamma(\alpha, \beta)$[1].The figure 5 shows the histogram of block variance for a given texture image and its gamma fitting curve.

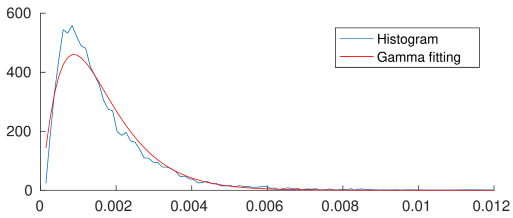

**Fig. 5**. Histogram of block variance compared with its Gamma fitting curve.

Degradations caused by Print&Scan processed involve the change in the distribution of block variance, see figure 6. Therefore, we can exploit the behavior of this distribution as a feature to describe our printed and scanned CGN textures.

### 3.3. Hypothesis testing formulation

From the result illustrated by the figure 6, we found that the distribution of block variance approaches some Gamma distribution, whose parameters can be estimated by calibration, for images of genuine textures. For images of fake textures, the distribution of block variance behaves much differently from the previous ones.

Denote $X = \{X_i\}_{i=1,..,n}$ the set of all block variance values of an image, where $i$ is the block index and $n$ the total number of blocks in image. We can formulate an hypothesis test as follows:

$$\begin{cases} \mathcal{H}_0 : \{X \sim \Gamma(a, b)\}\,, & (a, b) \text{ are known} \\ \mathcal{H}_1 : \{X \nsim \Gamma(a, b)\} \end{cases} \tag{3}$$

From a recent work of José *et al.* in [10], it follows that we can obtain an estimator of the scale parameter by calculating the covariance between $X$ and $Z = log(X)$, that is defined as follows:

$$\hat{\beta_n} = \frac{1}{n} \sum_{i}^{n} (X_i - \bar{X})(Z_i - \bar{Z}) \tag{4}$$

where $\bar{X} = \frac{1}{n} \sum_{i=1}^{n} X_i$ and the same goes for $\bar{Z}$.

Under $\mathcal{H}_0$, we can proved that:

$$S = \frac{\sqrt{n}}{\eta} (\hat{\beta_n} - b) \xrightarrow{d} N(0, 1) \tag{5}$$

where $\eta^2 = b^2(1 + a\psi_1(a))$, and $\psi_1(.)$ denotes the trigamma function.

Therefore, for a given prescribed false-alarm probability $\alpha_0$, we propose a test based on the statistics $S$ which rejects $\mathcal{H}_0$ if either $S < \Phi^{-1}(\alpha_0/2)$ or $S > \Phi^{-1}(1 - \alpha_0/2)$, where $\Phi^{-1}(.)$ denotes the inverse of the cumulative distribution function of the standard Gaussian random variable.

[1] The probability density function of a Gamma distribution $\Gamma(\alpha, \beta)$ is given as follows: $f(x) = \frac{\beta^\alpha}{\Gamma(\alpha)} x^{\alpha-1} \exp(-\beta x) \quad \forall x \in \mathbb{R}_+$.

## 4. EXPERIMENTAL RESULTS

We generated 270 W-QR codes with $\text{CGN}_{200,70}$ texture of size 500x500 pixels, which are then printed using a photocopier *Olivetti d-Color MF362 Plus* in 600 dpi on standard A4 paper to form 270 genuine 3x3-cm printed W-QR codes.

Each genuine printed W-QR code are then scanned at 600 dpi resolution and reprinted by the same printer as above at the same resolution. We obtain 270 scanned and reprinted W-QR codes.

The numeric W-QR codes are also printed by an other printer (same model as the previous one) to create illegal W-QR. The goal is to simulate the case that counterfeiters have the numeric version but do not have the same printing process as constructor.

After that, all genuine and illegal W-QR codes are scanned by a Samsung Galaxy S6 phone at its highest resolution under an ISO constant. The distance between the camera and the printed W-QR is also maintained at a constant value. This distance is chosen in such a way that the images obtained are in good focus conditions.

The figure 6 shows a scatter view of the couple $(\beta, \alpha)$ estimated, by using Maximum Likelihood (ML) Estimation, for each images of genuine printed W-QR codes and the illegal ones.

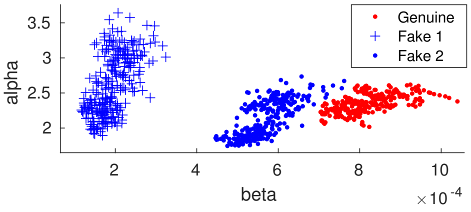

**Fig. 6**. Distribution of couples $(\beta, \alpha)$ of genuine textures and falsified textures created by Scan&Reprint (labeled as Fake 1) and by printing from numeric code but by another printer (labeled as Fake 2); Each dot or cross represents the couple $(\beta, \alpha)$ estimated from one image.

By averaging the values of the couple parameters $(\beta, \alpha)$ estimated from images of genuine textures, we can have an estimation of $b$ and $a$ proposed in the equation (3). We calculated the statistics $S$, described by the equation (5), for every images. The figure 7 gives the empirical histogram of the values of $S$ for different sets of images.

The distribution of $S$ under the set of genuine images behaves like a zero-mean Gaussian distribution. Under the other sets, it maintains the behavior of a Gaussian one but with a non-zero mean. By thresholding the value of $S$ and varying the threshold value, we obtained in the figure 8, the Receiver operating characteristic (ROC) curves when we try to classify our genuine textures with different sets of falsified images.

For the given set of genuine and Scan&Print texture images, we can reach a perfect detection power with a 0 false-alarm rate.

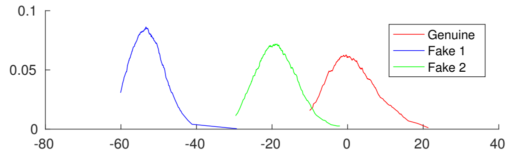

**Fig. 7**. Empirical distribution of the proposed test statistics $S$ under different sets of data.

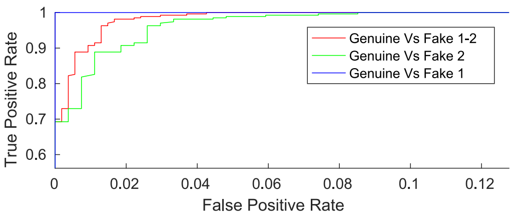

**Fig. 8**. ROC curves- Performance of classification between genuine textures and different sets of falsified ones.

A 800x800 pixels size version of numeric W-QR was also created to compared with the initial one. These codes are printed by the same printer as the 500x500 ones but they are scaled (by the printing process) to have the same dimension in printed version as the previous ones. By varying the size of numeric codes, we modify the content of textures and so the distribution of block variance, figure 9. In other words, we can propose to play with the size of numeric code to increase the diversity of printed W-QR codes.

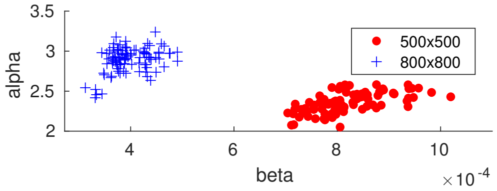

**Fig. 9**. Distribution of couples $(\beta, \alpha)$ of genuine textures at different resolution.

## 5. CONCLUSIONS

In this paper, we proposed a novel watermarking technique to secure printed QR codes, which may be used as a very cheap solution to fight against counterfeiting. A specific random texture, sensitive with Print&Scan processes, is substituted with the background of standard QR code to create a secure one. A statistical test is used to detect falsified QR codes. Experimental results confirmed the relevance of the proposed solution.

# References

[1] Baldini Gianmarco, Satta Riccardo, Nai Fovino Igor, Tsois Aris, and Chechi Enrico, “Survey of techniques for fight against counterfeit goods and intellectual property rights (ipr) infringing,” Tech. Rep., EU Science Hub - The European Commission’s science and knowledge service, 2015.

[2] ISO/IEC, “Information Technology—Automatic Identification and Data Capture Techniques—Bar Code Symbology—QR Code,” ISO/IEC 18004:2000, International Organization for Standardization, Mars 2000.

[3] Justin Picard, “Digital authentication with copy-detection patterns,” in *Proc. SPIE*, 2004, vol. 5310, pp. 176–183.

[4] C. Baras and F. Cayre, “2d bar-codes for authentication: A security approach,” in *2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*, pp. 1760–1766.

[5] Anh Thu Phan Ho, Bao An Mai Hoang, Wadih Sawaya, and Patrick Bas, “Document authentication using graphical codes: reliable performance analysis and channel optimization,” *EURASIP Journal on Information Security*, vol. 2014, no. 1, pp. 9.

[6] 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 Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 571–583, Mars 2016.

[7] A. E. Dirik and B. Haas, “Copy detection pattern-based document protection for variable media,” *IET Image Processing*, vol. 6, no. 8, pp. 1102–1113, November 2012.

[8] H. P. Nguyen, F. Retraint, F. Morain-Nicolier, and A. Delahaies, “Face spoofing attack detection based on the behavior of noises,” in *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Dec 2016, pp. 119–123.

[9] T. N. C. Doan, F. Retraint, T. H. Thai, and C. Zitzmann, “Quality factor estimation of JPEG compressed images,” in *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 104–108.

[10] José A. Villaseñor and Elizabeth González-Estrada, “A variance ratio test of fit for gamma distributions,” *Statistics & Probability Letters*, vol. 96, pp. 281–286, January 2015.