A watermarking technique to secure printed QR-Codes

Statistical hypothesis testing

Hoai Phuong Nguyen†, Florent Retraint⋆, Marc Pic∗
Frédéric Morain-Nicolier†, Agnès Delahaies†
⋆ CREsTIC, University of Reims Champagne-Ardenne, France
† LM2S, ICD, University of Technology of Troyes, France
∗ Group SURYS, Paris, France

Contact Information:
Lab. of System Modeling and Dependability
Charles Delaunay Institute
University of Technology of Troyes
12 Rue Marie Curie
10004 Troyes, France
Email: hoai_phuong.nguyen@utt.fr

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. We present a novel technique that permits to create a secure printed QR code which is robust against Scan & Reprint attack. The code, named as W-QR 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 test.

Concept of W-QR Code

Construction

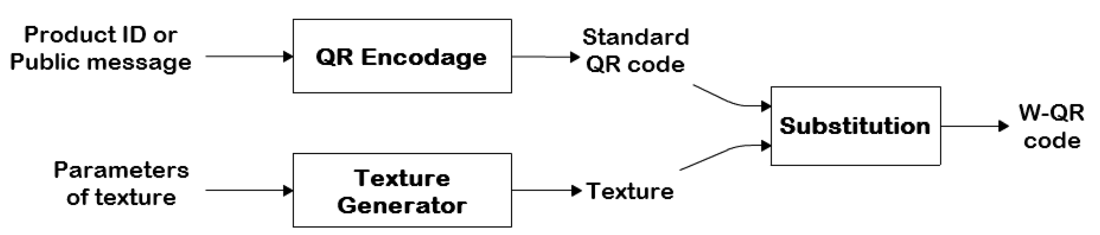

Figure 1: Proposed flowchart for the construction of W-QR

Reading and Authentication

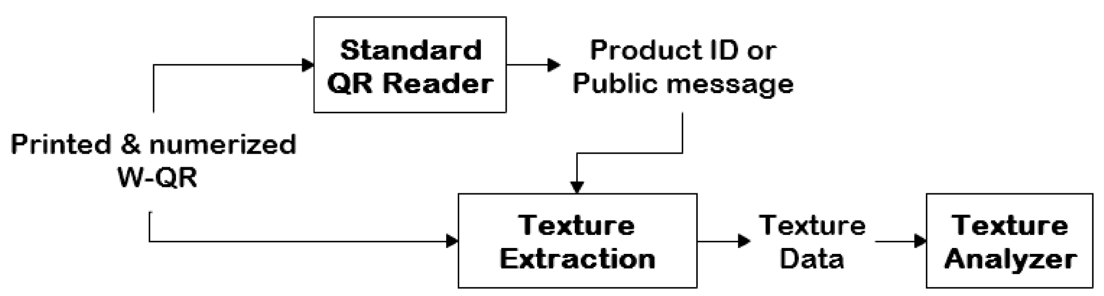

Figure 2: Proposed flowchart for the reading and validation of W-QR

Clipping Gaussian Noise Texture

The Clipping Gaussian Noise (CGN) texture is characterized by a couple of two parameters (μ, σ). A CGN texture is created from a matrix of μ-mean and σ-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 (μ, σ).
Denote $\text{CGN}_{\mu,\sigma}$ the texture characterized by the couple (μ, σ). The figure below shows an example of the $\text{CGN}_{200,70}$ texture and its histogram.

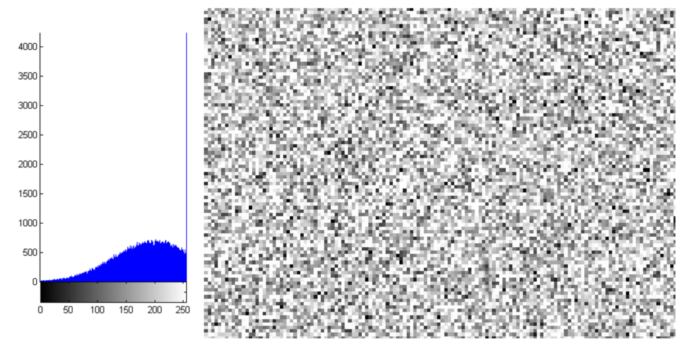

Figure 3: CGN (right to left): the texture and its histogram

Proposed Statistical Detector

Noise Local Variance Model

NLV is the local variance of noise which is calculated within each 8x8 block of image [1]. Distribution of NLV values of a given image could be approximated by a Gamma distribution.

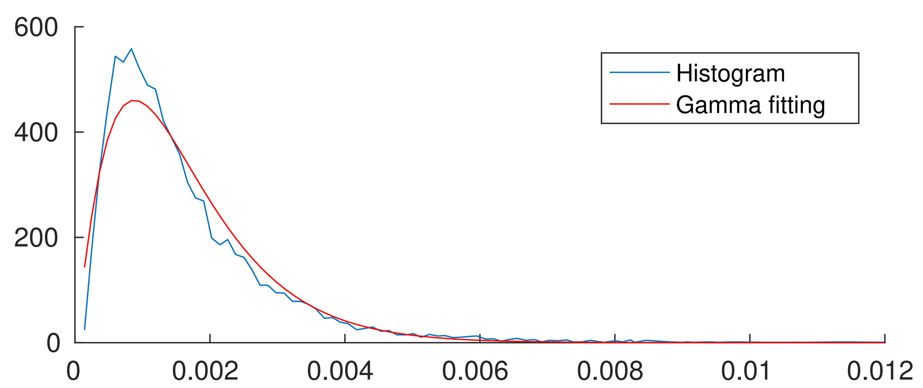

Figure 4: Histogram of block variance compared with its Gamma fitting curve

The distribution of NLV observed from images of falsified textures behaves much differently from the ones of falsified textures.

Statistical Test

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

$$\begin{cases} \mathcal{H}_0 : \{X \sim \mathcal{G}(a,b)\}, & (a,b) \text{ are known} \\ \mathcal{H}_1 : \{X \nsim \mathcal{G}(a,b)\} \end{cases} \quad (1)$$

where $\mathcal{G}(a,b)$ denotes a Gamma distribution with a and b respectively the form and scale parameters of the distribution.
From a recent work of José *et al.*, in [2], 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:

$$\hat{\beta}_n = \frac{1}{n}\sum_i^n (X_i - \bar{X})(Z_i - \bar{Z}) \quad (2)$$

It is proved that under $\mathcal{H}_0$, we have that:

$$S = \frac{\sqrt{n}}{\eta}(\hat{\beta}_n - b) \xrightarrow{d} \mathcal{N}(0,1) \quad (3)$$

where $\eta^2 = b^2(1 + a\psi_1(a))$, and $\psi_1(.)$ denotes the trigamma function.
For a given prescribed false-alarm probability α_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 cdf of the standard Gaussian random variable.

Experiments & Results

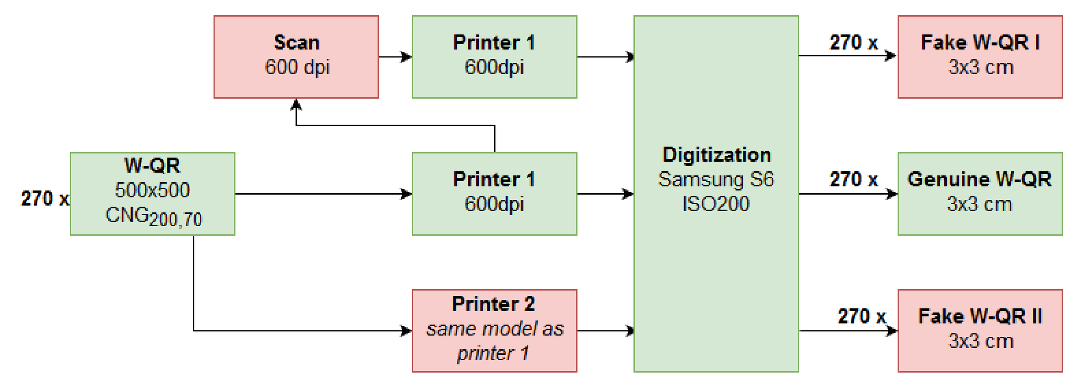

Figure 5: Description of testing database

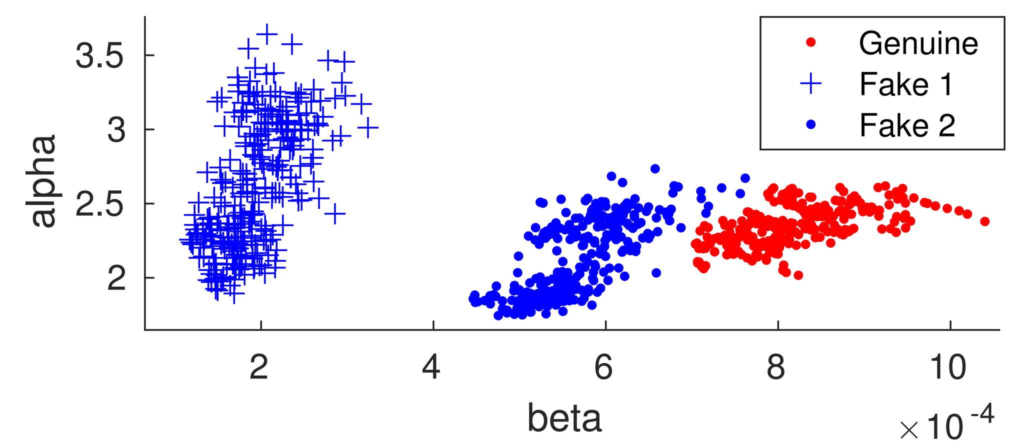

Figure 6: Distribution of couples (β, α) of genuine textures and falsified textures created by Scan&Reprint (labeled as Fake 1) and by printing from numeric code but by another printer (labeled as Fake 2); Each dot or cross represents the couple (β, α) estimated from one image.

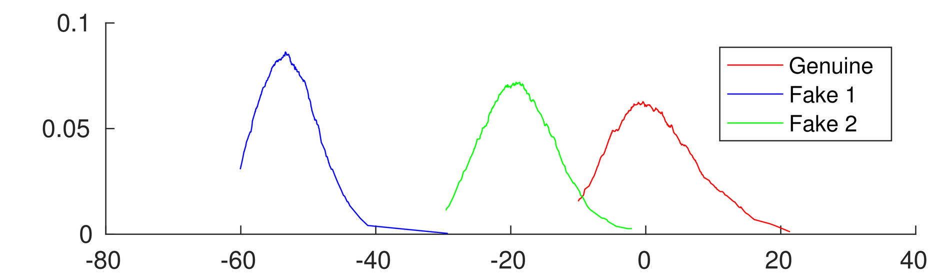

Figure 7: Empirical distribution of the proposed test statistics under different sets of data

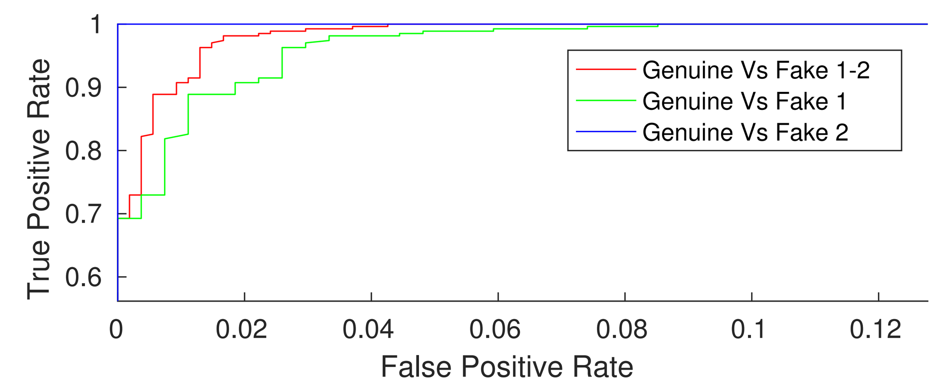

Figure 8: Performance ROC curves

Conclusion

- A novel watermarking technique is proposed to secure printed QR codes, which may be used as a very cheap solution to fight against counterfeiting. A specific random texture, sensitive to Print&Scan processes, is substituted with the background of standard QR code to create a secure one, the W-QR code.
- A performing statistical detector basing on the NLV model is presented.

Forthcoming Research

In a recent work, we propose a novel embedding technique, which makes the texture more sensible to Scan&Reprint attacks. The NLV model was also upgraded and new more powerful statistical detector could be constructed.

References

[1] 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)*, pages 119–123, Dec 2016.

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