Sensitivity of different correlation measures to print-and-scan process

Iuliia Tkachenko, Christophe Destruel, Olivier Strauss, William Puech

https://doi.org/10.2352/ISSN.2470-1173.2017.7.MWSF-335

Sensitivity of different correlation measures to print-and-scan process

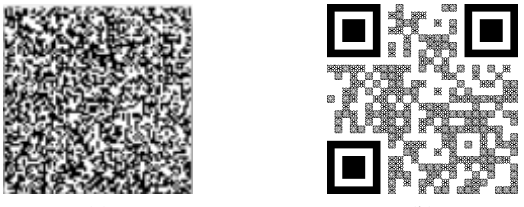
Iuliia Tkachenko [1] *, ***Christophe Destruel*** [2], ***Olivier Strauss*** [3], ***William Puech*** [3]
[1] ***L3i, University of La Rochelle, France***
[2] ***Authentication Industries, Montpellier, France***
[3] ***LIRMM, UMR CNRS 5506, University of Montpellier, France***

Abstract

The authentication of printed documents is a nowadays challenge. One of the promising solutions for document authentication is the use of copy sensitive graphical codes that can offer data storage and support authentication. Both data decoding and physical authentication are based on comparison between printed-and-scanned samples and original numerical codes. In this paper we want to evaluate different existing correlation measures (Kendall and Spearman) and to propose a new Kendall weighted correlation metric. We propose to evaluate this new method by considering its ability to decode stored messages and to evaluate document authenticity.

Introduction

Nowadays the printed document authentication is a hot topic. There exists different techniques to protect document against falsification and to detect counterfeits: watermarking [5], text hashing [6], document feature extraction [7] and Copy-Detection Graphical Codes (CDGC) [1].
The CDGC are one of the most promising solutions thanks to cheap generation and easy integration. Graphical codes are black-and-white images that contain machine readable data and are sensitive to print-and-scan process. Two examples of such graphical codes are copy sensitive pattern [1, 8] (Fig. 1.a) and Two Level QR (2LQR) code [2] (Fig. 1.b).



(a) (b)

Figure 1: Copy-detection graphical codes: a) copy sensitive pattern, b) 2LQR code.

The use of such codes for authentication is based on impact of print-and-scan process that significantly changes the image structure: using either image comparison (pixel by pixel) or correlation measure (usually Pearson correlation [4]) an application should be able to detect non-authorized code duplication. However, the pixel by pixel comparison is performed after binarization of the printed-and-scanned (P&S) CDGC and this approach gives inaccurate authentication results. The use of Pearson correlation is also questioned: the correlation values after print-and-scan process are quite small, and the gap of values between authentic code and non-authentic codes is tiny. This poor discrimination ability is a source of major authentication problems and implies a trade-off between minimization of false positive and true negative.
In this paper we study alternative correlation measures (Spearman, Kendall) for security graphical codes (we use the 2LQR code as a reference code).
The P&S process cruelly changes the structure of such code. We want to compare these alternative measures with existing copy detection metrics [3] considering two axes: code readability (pattern detection capacities) and code authentication.
The two targets of this paper are 1) Find the most efficient measure for authentication of printed-and-scanned documents using CDGC; 2) Identify the metrics that can be efficiently used for textured pattern detection after P&S process.
The rest of the paper is organized as follows. First we talk about CDGC and list the existing copy-detection metrics [3]. Then we introduce the alternative correlation measures and the proposed Kendall weighted correlation metric. The database description and experimental results are presented after. Finally, we conclude and discuss the perspectives.

State of the art

The CDGC is an interesting path for document authentication both for academic and industrial researchers. This popularity of CDGC is due to easy integration process, low generation cost and possibility of automatic verification using publicly accessible devices (scanners and smartphones).
Even if it exists different techniques inherited from printing history to protect a document against counterfeit, we focus this section on graphical codes sensitive to P&S process. For example, specific papers, inks, changing backgrounds, holograms or added components are not addressed. The techniques presented in this section are based on two statements:

- The "information loss principle" [1]: every time an image is printed or scanned, some information is lost about the original digital image. Printing and scanning processes are affected by noise, blur and other changes [10]. The loss could be minimal and imperceptible by Human Visual System (HVS) but it could be significant for authentication test.
- Each printing and copying device has its own signature. The use of this signature that characterizes the specific modifications done by the device is employed for the authentication test. Specific image analysis systems can detect alterations

*Work done while the author was with Authentication Industries

made to laser printed documents even if the alteration is invisible by HVS [9].

These two statements are in fact two points of views on the same mechanism as the lost of information on a document and the specific signature of devices used (printers, scanners and copiers) are deeply linked.
In this section, we present two CDGC types and discuss copy detection measures that are used for these CDGC.

Graphical codes

A security element constructed with respect to the "information loss principle" is the Copy Detection Pattern (CDP) [1]. A CDP is a noisy, maximum entropy image, generated with a secret key. A CDP is designed to be maximally sensitive to the copying process. It has large variation in high frequencies that are the most difficult to capture by the scanning device. In addition, it has a non-predictable content that secures against reproduction attack. The CDP is impossible to verify by HVS. In order to determine whether a printed document is an original or a copy we first need to scan it. Then, a specific software compares the pixel values from the digital and the scanned CDP. The comparison can be made by a correlation score, a distance, a combined score of different features [1] or by using the copy detection metrics sensitive to P&S process [3]. Due to CDP sensitivity to reproduction, the print quality needs to be reasonably good and the printer, the media and the scanner must be of known types [3].
The Two Level QR (2LQR) code [2] can also be used to detect unauthorized document duplication [11]. This 2LQR code has two storage levels, where the second level is constructed using specific textured patterns. These textured patterns can be chosen to be sensitive to P&S process. Despite the P&S impact, the first (public) level is readable all the time. The second (private) level is sensitive to P&S degradation, thus the information stored in this level is not readable in a copy.

Copy detection measures

The most used authentication test for CDP is the comparison of original CDP with binarized version of P&S CDP [12]. But thanks to research interest on this topic, several original copy-detection measures were suggested [3]. In this paper we are interested on two of them: entropy metric and prediction error metric.
Based on information theory, the **entropy metric** [3] is computed as follows:

$$H = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i), \tag{1}$$

where $X = \{x_1, \cdots, x_n\}$ is the vector of CDP pixels and $p(x_i) = Pr(X = x_i)$ is the probability mass function of X.
Based on linear prediction of signal processing, the **prediction error metric** [3] is calculated as follows:

$$F_{prediction} = \frac{1}{(M-1)(N-1)} \sum_{i=1}^{M-1}\sum_{j=1}^{N-1} |c_{i,j} - \hat{c}_{i,j}|, \tag{2}$$

where $c_{i,j}$ is the CDP pixel at location i, j, M and N are dimensions of CDP, and the prediction of $c_{i,j}$ is defined as:

$$\hat{c}_{i,j} = c_{i,j-1} + c_{i-1,j} - c_{i-1,j-1}. \tag{3}$$

The distinctive feature of these metrics is that the original CDP is not used during authentication test. All what we need is to calculate the authentication threshold earlier. According to authors of [3], these metrics can perfectly distinguish the copy CDP from the original one.
Till now the authentication test of 2LQR code was performed using **Pearson correlation**:

$$cor(P,S) = \frac{\sum_i \sum_j (C^*(i,j))(S^*(i,j))}{\sqrt{\sum_i \sum_j (C^*(i,j))^2}\sqrt{\sum_i \sum_j (S^*(i,j))^2}}, \tag{4}$$

where C and S are the original and scanned textured patterns, $C^*(i,j)$ (rsp. $S^*(i,j)$) are the central values of patterns C (rsp. S) defined by $C^*(i,j) = C(i,j) - \mu_C$ (rsp. $S^*(i,j) = S(i,j) - \mu_S$) with $\mu_C = \frac{1}{k}\sum_i \sum_j C(i,j)$ (rsp. $\mu_S = \frac{1}{k}\sum_i \sum_j S(i,j)$).
Nevertheless, experimental results show sometimes tiny gaps between originals and copied codes (see results in [11]). We decided to evaluate different metrics to improve the authentication ability for 2LQR codes and we compared them to the three metrics mentioned in this section.

Suggested copy detection measures

We suggest to use experimental approach to evaluate alternative correlation metrics: Kendall, Spearman [4] and the new proposed Kendall weighted correlation. We apply these metrics on our database to compare the results with thus obtained using the reference methods described in the previous section.

Kendall correlation

The **Kendall rank correlation coefficient** evaluates the degree of similarity between two sets of ranks given to the same set of objects [4]. We have two random variables $X = x_1, \cdots, x_r$ and $Y = y_1, \cdots, y_r$. Any pair of observations (x_i, y_i) and (x_j, y_j) are called *concordant* if the ranks for both elements agree:

$$\begin{gathered}\text{if } Rank(x_i) > Rank(x_j) \text{ and } Rank(y_i) > Rank(y_j),\\ \text{or if } Rank(x_i) < Rank(x_j) \text{ and } Rank(y_i) < Rank(y_j).\end{gathered}$$

The pairs are called *discordant*,

$$\begin{gathered}\text{if } Rank(x_i) > Rank(x_j) \text{ and } Rank(y_i) < Rank(y_j),\\ \text{or if } Rank(x_i) < Rank(x_j) \text{ and } Rank(y_i) > Rank(y_j).\end{gathered}$$

If $Rank(x_i) = Rank(x_j)$ and $Rank(y_i) = Rank(y_j)$, they are neither concordant, nor discordant.
The Kendall τ rank correlation is calculated from formula:

$$\tau = \frac{N_c - N_d}{\frac{1}{2}r(r-1)}, \tag{5}$$

where N_c is the number of concordant pairs, N_d is the number of discordant pairs. The variables X and Y, in our case, are vectors of original and scanned textured pattern pixels.

Spearman correlation

The **Spearman rank correlation** (named also Spearman's rho) is the second most popular bivariate correlational technique [4]. Suppose we have two random variables $X = x_1, \cdots, x_r$ and $Y = y_1, \cdots, y_r$, that are converted to ranks:

$$Rank(x_1), \cdots, Rank(x_r)$$

and

$$Rank(y_1), \cdots, Rank(y_r).$$

Note that: $Rank(min(x_i)) = 1$ and $Rank(max(x_i)) = r$. The Spearman's rho for pairs

$$[Rank(x_1), Rank(y_1)], \cdots, [Rank(x_r), Rank(y_r)]$$

is computed from formula:

$$\rho = 1 - \frac{6\sum d_i^2}{(r^3 - r)}, \tag{6}$$

where $d_i = Rank(x_i) - Rank(y_i)$ is the difference between the ranks. The variables X and Y, in our case, are vectors of original and scanned textured pattern pixels.

Kendall weighted correlation

In this section we explain the proposed **Kendall weighted correlation** that can be efficiently used for textured pattern detection and copy detection. We call this metric Kendall weighted correlation as we calculate probability values during a pre-processing step to weight a Kendall measure. This pre-processing step consists of calculation concordant and discordant pairs probabilities p_1 and p_2. This step is computed from a representative set of T P&S patterns $\mathscr{E}_l = \{E_l^1, \cdots, E_l^T\}$, where $l = 1, \cdots, q$. Then, during the recognition step, the number of concordant and discordant pairs (see Kendall correlation equation (5)) is calculated using earlier calculated probabilities p_1 and p_2 as weight. The flowchart of recognition algorithm is illustrated in Fig. 2.

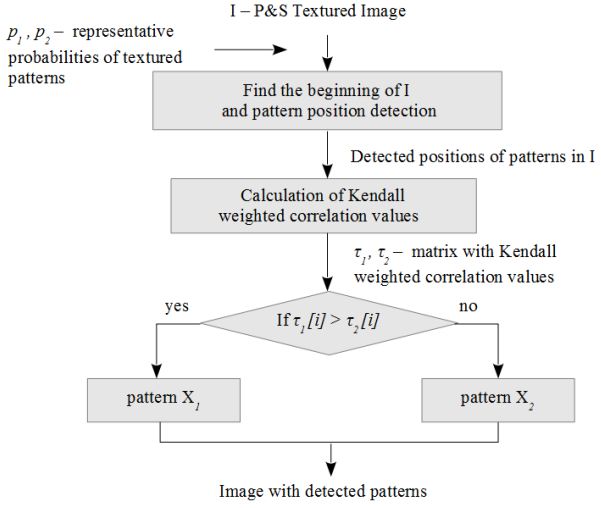


Figure 2: Textured pattern recognition using Kendall weighted correlation.

We suppose that x_t^i, with $t = 1, \cdots, T$ and $i = 1, \cdots, r^2$, is a vector of T grey level values of one pixel of representative set $\mathscr{E}_l$, $l = 1, \cdots, q$.
During the *pre-processing step* we calculate:

1. The probabilities that the pixel from a vector $x_{t_1}^i$ is smaller than the pixel from a vector $x_{t_2}^j$

$$p_1^{i,j} = p(x_{t_1}^i < x_{t_2}^j), t_1 = t_2 = 1, \cdots, t, i = j = 1, \cdots, r^2. \tag{7}$$

2. The probabilities that the pixel from a vector $x_{t_1}^i$ is bigger than the pixel from a vector $x_{t_2}^j$

$$p_2^{i,j} = p(x_{t_1}^i > x_{t_2}^j), t_1 = t_2 = 1, \cdots, t, i = j = 1, \cdots, r^2. \tag{8}$$

The characterization step could be done once for every textured pattern, during the creation of the 2LQR code.
During the *recognition step*, for each patch $Y_s = y_1, \cdots, y_{r^2}$ (where Y_s is a scanned textured pattern) from scanned 2LQR code we calculate:

- the number of concordant pairs

$$N_c^{prob} = \sum_i \sum_j p_1^{i,j} \times num(y_i < y_j) + \sum_i \sum_j p_2^{i,j} \times num(y_i > y_j), \tag{9}$$

- the number of discordant pairs

$$N_d^{prob} = \sum_i \sum_j p_2^{i,j} \times num(y_i < y_j) + \sum_i \sum_j p_1^{i,j} \times num(y_i > y_j), \tag{10}$$

where function $num(\varphi)$ corresponds to number of pixels that satisfy the condition φ.
Finally, we calculate the Kendall weighted correlation using the formula:

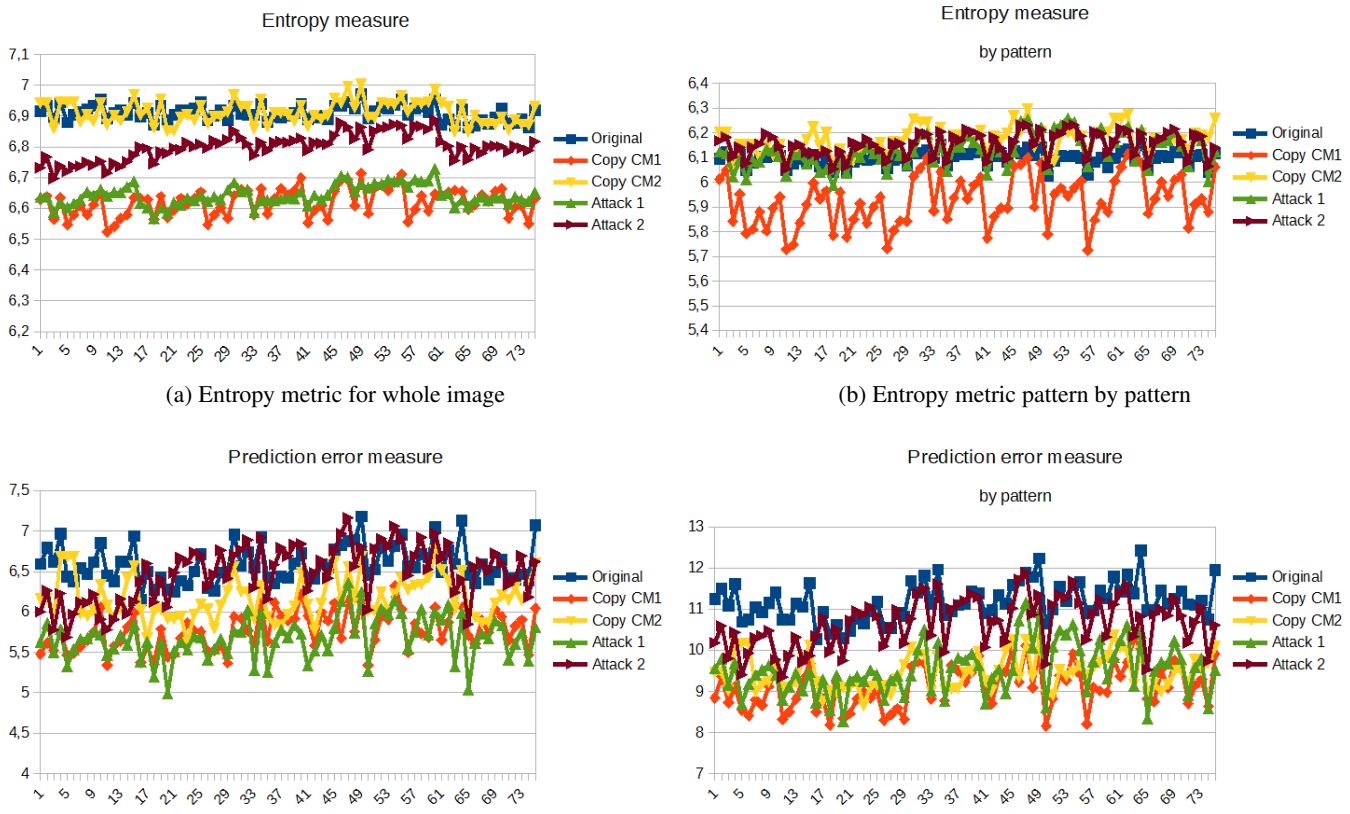
$$\tau_{prob} = \frac{N_c^{prob} - N_d^{prob}}{\frac{1}{2}(r-1)}, \tag{11}$$

We calculate the Kendall weighted correlation τ_l^{prob}, $l = 1, \cdots, q$ with every representative set, where q is the number of textured patterns used for private level generation. Then, the maximal Kendall weighted correlation value corresponds to pattern type: if $\hat{\tau}_i^{prob} = \max\{\tau_1^{prob}, \cdots, \tau_q^{prob}\}$, the pattern is recognized as Y_i.
This new metric can also be used for authentication. As in previous work [11], an authentication threshold Th has been determined during the pre-trial phase. And the authentication test consists of comparing the mean value of $\hat{\tau}_m^{prob}, m = 1, \ldots, B$ with threshold Th, where τ_m^{prob} is the maximal Kendall weighted correlation for each textured pattern and B is the total number of textured patterns used in 2LQR code . The document is said to be authentic if this mean value is bigger than Th:

$$mean(\hat{\tau}_1^{prob}, \cdots, \hat{\tau}_B^{prob}) \geq Th.$$

Experiments

In this section we describe the database used and present the experimental results. The main goal of these experiments consist to find the metrics that can differentiate the originals from copies, and even more, the metrics that can differentiate the copied 2LQR codes from attacked.
The database used consists of 75 authentic 2LQR codes (called Original in the rest of the paper) printed and scanned in 600 dpi (with a Brother HL-4150CDN printer and a Canon LIDE210 flatbed scanner) and 150 copied 2LQR codes, i.e direct duplication using 2 copy machines: Canon 4225i and Ricoh C2050 in



(a) Entropy metric for whole image

(b) Entropy metric pattern by pattern

(c) Prediction error metric for whole image

(d) Prediction error metric pattern by pattern

Figure 3: The metric values for original, copied and attacked samples using: a) Entropy metric for whole image, b) Entropy metric for every pattern, c) Prediction error metric for whole image and d) Prediction error for every pattern.

600 dpi resolution (called Copy CM1 and Copy CM2 in the rest of the paper).

In order to test the ability of the proposed metrics to distinguish originals from copies, we attack our code with two complementary approaches.

The *first attack* (called Attack 1 in the rest of the paper) is trivial. We first scan original codes with a 1200 dpi scanner (twice the 600 dpi original printer resolution). The scanned images are binarized using a global threshold. This threshold is visually adapted in order to:

- produce balanced histograms, supposing that the original images have the same number of black and white pixels,
- reveal the maximum number of details in the scanned images.

The binarized image is then printed on a 1200 dpi printer to produce the fake codes.

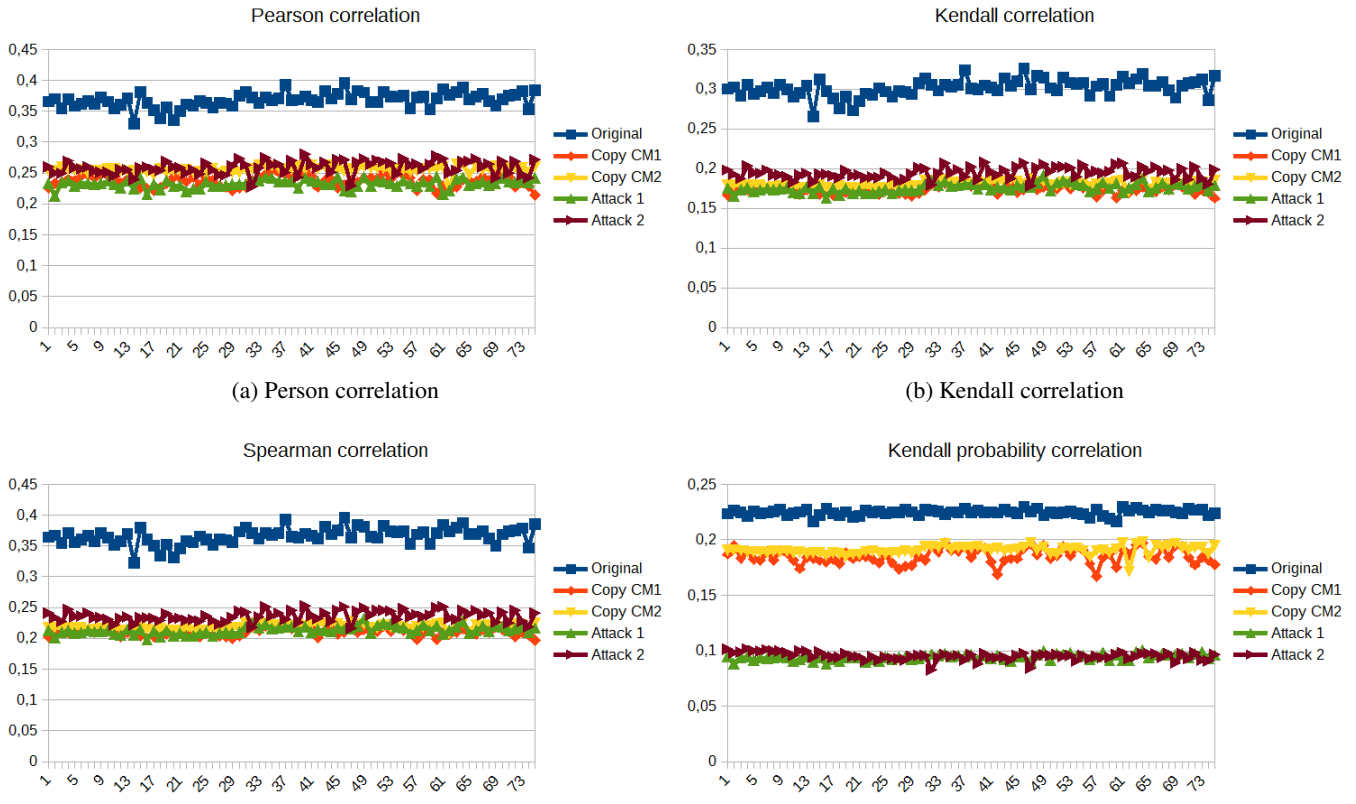
The *second attack* (called Attack 2 in the rest of paper) adds a sharpen stage to the previous attack process. The sharpen enhancement is done before applying the global thresholding. We apply an 8-connected Laplacian filter to try to restore the high frequencies of the original codes. The Laplacian images are then merged with the scanned ones in order to reduce the Laplacian artifacts. The weight used to merge both images is about $w = 90\%$:

$$I = (1-0.9) \times I + 0.9 \times L,$$

where I is a P&S 2LQR code and L is its Laplacian image. We use a very high weight to reveal all details from the scanned image. These images are binarized considering a global threshold determined as described in the previous attack. The final images are then printed on the same 1200 dpi printer.

The comparison will be done using 2 state of the art metrics and 4 correlation measures: 1 metric based on information theory (entropy measure), 1 based on signal processing (prediction error metric) and Pearson, Kendall, Spearman and Kendall weighted correlations.

The state of art metrics were proposed to detect the copies, so we cannot use these metrics for textured pattern detection. That is why, using the metrics given in equations (1)-(2), we only are able to perform authentication tests to detect unauthorized duplication when the 2LQR code is used. These metrics are applied for whole image in [3]. However, as the correlation metrics have been applied to every pattern, we have decided to calculate also these metrics for each pattern. When the metric is calculated for each pattern, the mean value is used for authentication test. We compare the values obtained when apply the metrics to whole images and to each pattern.



(a) Person correlation

(b) Kendall correlation

(c) Spearman correlation

(d) Kendall weighted correlation

Figure 4: The correlation values for original, copied and attacked samples using: a) Pearson, b) Kendall, c) Spearman and d) Kendall weighted correlations.

The first state of the art metric is entropy metric. The Fig. 3.a and Fig. 3.b illustrate the entropy metric for whole image and mean values of entropy metric applied for each pattern in 2LQR code, respectively. We can state that this metric cannot effectively differentiate the original codes from copied and attacked codes.
The second one is the prediction error metric. The results are illustrated in Fig. 3.c and Fig. 3.d for whole image and for each pattern, respectively. From these results we conclude that the state of the art metrics are not effective for 2LQR code authentication. As these metrics were created for maximum entropy images (CDP), it is not applicable for graphical codes with well defined structure.
As we use the 2LQR code for our test database, the correlation metrics are used not only for copy detection, but also for textured pattern detection after P&S process. The mean correlation values for Pearson, Kendall, Spearman and Kendall weighted correlations are illustrated in Fig. 4.a-Fig. 4.d. These figures show that the classical correlation metrics have the same curves, but the gap between original codes and copied/attacked is bigger, when we use the Kendall and Spearman correlations.

The most interesting result is obtained for Kendall weighted correlation. We can notice in Fig. 4.d, that the correlation values are more stable for each type of codes (original, copied or attacked). The additional interesting fact is that this measure better distinguish the copied codes from the attacked. That can be explained by the fact that the attacked samples were binarized

	Min value	Mean value	Max value
Pearson correlation			
dif Orig - Copy CM1	0,0917	0,1310	0,1690
dif Orig - Copy CM2	0,0762	0,1125	0,1514
dif Orig - Attack 1	0,1055	0,1355	0,1735
dif Orig - Attack 2	0,0760	0,1091	0,1445
Kendall correlation			
dif Orig - Copy CM1	0,0949	0,1282	0,1546
dif Orig - Copy CM2	0,0863	0,1215	0,1460
dif Orig - Attack 1	0,0966	0,1258	0,1491
dif Orig - Attack 2	0,0819	0,1074	0,1347
Spearman correlation			
dif Orig - Copy CM1	**0,1157**	**0,1561**	**0,1878**
dif Orig - Copy CM2	**0,1046**	**0,1473**	**0,1771**
dif Orig - Attack 1	0,1173	**0,1526**	**0,1807**
dif Orig - Attack 2	0,0993	**0,1302**	**0,1633**
Kendall weighted correlation			
dif Orig - Copy CM1	0,0263	0,0395	0,0601
dif Orig - Copy CM2	0,0252	0,0343	0,0551
dif Orig - Attack 1	**0,1202**	0,1306	0,1404
dif Orig - Attack 2	**0,1197**	0,1297	0,1437

Table 1: Differences of correlation values among originals and copied/attacked samples.

and thus, the initial textured pattern structure was lost. However, even if the correlation values and the gaps between authentic and copied codes of Kendall weighted metric are smaller, the authentication tests can been performed successfully.

The distances among original correlation values and copied/attacked samples are presented in Table 1. We note that the best separation can be obtained using Spearman correlation, as the gap is the biggest almost for all samples. In the same time, the Kendall weighted correlation have a tiny gap between original and copied samples, but a big gap between original and attacked samples. So the Kendall weighted correlation can differentiate the original codes from copied codes, and copied codes from attacked codes.

Another evaluation parameter is the textured pattern detection after P&S process using correlation metrics. Table 2 shows the error probability of incorrect pattern detection and digit decoding. First thing to notice is the detection results in original codes: we can see that the best detection results are obtained using proposed Kendall weighted metric. The Kendall and Spearman correlations present the same capacities of pattern detection. The Pearson correlation has the worst detection results, but still the error probabilities are less than 1%. The number of errors for pattern detection in copied and attacked (first attack) codes are huge, thus the encoded message cannot be retrieved from these codes. This fact in addition to low correlation values make these codes unreadable and unauthentic. The codes obtained after Attack 2 have better pattern detection results. Additionally, using Kendall weighted correlation, the error probability is less than 10%, but in any case it is not sufficient to retrieve the message and the correlation values are so small in comparison with originals (see Fig. 4.d) that these codes cannot be considered as authentic.

	Error probability of incorrect	
	pattern detection	digit decoding
Pearson correlation		
Original	0.97%	0.26%
Copy CM1	31.98%	43.77%
Copy CM2	23.26%	29.30%
Attack 1	34.91%	44.29%
Attack 2	18.00%	18.81%
Kendall correlation		
Original	0.57%	0.25%
Copy CM1	36.33%	49.66%
Copy CM2	28.94%	39.45%
Attack 1	32.85%	42.12%
Attack 2	18.56%	19.54%
Spearman correlation		
Original	0.57%	0.21%
Copy CM1	36.07%	49.59%
Copy CM2	28.94%	39.44%
Attack 1	30.44%	40.22%
Attack 2	18.50%	19.49%
Kendall weighted correlation		
Original	0.05%	0.01%
Copy CM1	20.70%	24.13%
Copy CM2	15.60%	14.92%
Attack 1	20.01%	18.70%
Attack 2	6.97%	3.78%

Table 2: Pattern detection results using correlation metrics.

Conclusions

Copy-detection codes have a lot of applications in our daily life. In this paper we have evaluated the copy detection capacity of 2LQR code. Several copy detection metrics have been proposed earlier for other copy detection codes, but they do not work for 2LQR code. In the beginning, it was proposed to use the Pearson correlation measure for unauthorized document duplication, but the gap between originals and copied codes is sometimes tiny. That is why, we have suggested to use different correlation measures to increase the graphical code authentication capacity. The comparison of classical correlation metrics (Pearson, Kendall and Spearman) have been done. The Kendall and Spearman correlations better separate the originals from the copied and attacked 2LQR codes. In addition, we have propose the novel Kendall weighted correlation, that has more stable values for every type of samples (originals, copied and attacked) and can efficiently differentiate the original codes from copied, and the copied codes from attacked codes.

Additionally, the correlation metrics can be used for textured pattern detection. The experimental results show that the proposed Kendall weighted correlation has the best pattern detection results.

The correlation values and, thus, the authentication threshold are unique for every pair printer-scanner. In future work we want to increase the ability of this Kendall weighted correlation to obtain an invariant copy-detection metric, that can be used for every pair printer-scanner.

References

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

[2] Iu. 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, 11(3):571-583, March 2016.

[3] A. E. Dirik and B. Haas. Copy detection pattern-based document protection for variable media. Image Processing, IET, 6(8):1102-1113, 2012.

[4] N. J. Salkind. Encyclopedia of measurement and statistics. Sage Publications, 2006.

[5] A.T.-S. Ho and F. Shu, "A print-and-scan resilient digital watermark for card authentication," in Information, Communications and Signal Processing, and Fourth Pacific Rim Conference on Multimedia, 2003, vol. 2, pp. 11491152.

[6] R. Villn, S. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Pun, "Tamper-proofing of Electronic and Printed Text Documents via Robust Hashing and Data-Hiding," in Proc. Proceedings of SPIE-IS&T Electronic Imaging 2007, Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, USA, 2007.

[7] S. Shang, N. Memon and X. Kong, "Detecting documents forged by printing and copying", in EURASIP Journal on Advances in Signal Processing, Springer, vol. 1, pp. 1-13, 2014.

[8] C. Baras and F. Cayre, 2d bar-codes for authentication: A security approach, in Signal Processing Conference (EUSIPCO), Proceedings of the 20th European, 2012, pp. 17601766.

[9] J. Tchan, "The development of an image analysis system that can detect fraudulent alterations made to printed images", In Electronic Imaging 2004, pages 151-159. International Society for Optics and Photonics, 2004.

[10] L. Yu, X. Niu, and S. Sun, "Print-and-scan model and the watermarking countermeasure," in Image and Vision Computing. 2005, vol. 23, pp. 807814, Elsevier.

[11] Iu. Tkachenko, W. Puech, O.Strauss, C. Destruel, J.M. Gaudin "Printed document authentication using two level QR code", International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2016, Shanghai, China, 2016.

[12] A. T. Phan Ho, B. A. Mai Hoang,W. Sawaya, and P. Bas, "Document authentication using graphical codes: impacts of the channel model, in Proceedings of the first ACM workshop on Information hiding and multimedia security, Montpellier, France, 2013, IH&MMSec 2013, pp. 8794, ACM.

Author Biography

Iuliia TKACHENKO *received the M.S. degree in Applied Mathematics from Dnipropetrovsk National University, Ukraine in 2010, the M.S. degree in Cryptography and Information Security from University Bordeaux 1, France in 2012 and the Ph.D. degree in Computer Science from the University of Montpellier, France, in 2015. Currently she is a Post-Doc researcher in University of La Rochelle, Laboratory L3i, France. Her research interests include multimedia security, hybrid document authentication, semantic hashing, information hiding and cryptography.*

Christophe DESTRUEL *received his Engineer's Degree from the University of Toulouse, France, in 1995. He worked for 10 years in collaboration with the french Spatial Agency on research programs related to its main fields of interest, Computer Graphics and Image Processing, to develop the use of 3D paradigm in space imaging. He is now the Scientific Director of the start-up Authentication Industries that proposes innovative solutions to authenticate valuable documents. Respecting industrial constraints, his contributions have been published in various international conferences.*

Olivier STRAUSS *is an associate professor in Signal and Image Processing in Montpellier University, France. He received his Ph.D. in Signal Processing from the Montpellier University in 1991 and obtained his accreditation to supervise research in 2008. His current research interests include signal and image processing, computer vision, medical imaging, uncertainty management, advanced statistics and imprecise probability theories. He is currently head of the robotics department and member of the scientific council of Montpellier University.*

William PUECH *received a diploma in Electrical Engineering from the University of Montpellier, France, in 1991 and a Ph.D. Degree in Signal-Image-Speech from the Polytechnic National Institute of Grenoble, France in 1997. He started his research activities in image processing and computer vision. He served as a Visiting Research Associate to the University of Thessaloniki, Greece. From 1997 to 2000, he has been an Assistant Professor at the University of Toulon, France, with research interests including methods of active contours applied to medical images sequences. Between 2000 and 2008, he has been Associate Professor and since 2009, he is full Professor in image processing at the University of Montpellier, France. He works in the LIRMM Laboratory (Laboratory of Computer Science, Robotic and Microelectronic of Montpellier). His current interests are in the areas of protection of visual data (images, videos and 3D objects) for safe transfer by combining watermarking, data hiding, compression and cryptography. He has applications on medical images, cultural heritage and video surveillance. He is the head of the ICAR team (Image & Interaction) and he has published 39 journal papers, 16 book chapters and more than 100 conference papers. W. Puech is associate editor of J. of Advances in Signal Processing, Springer, Signal Processing: Image Communications, Elsevier, Signal Processing, Elsevier and IEEE Transactions on Dependable and Secure Computing. He is reviewer for more than 15 journals (IEEE Trans. on Image Processing, IEEE Trans. on Multimedia, IEEE Trans. on Circuits and Systems for Video Technology, IEEE Trans. on Information Forensic and Security, Signal Processing: Image Communication, Multimedia Tools and Applications ...) and for more than 10 conferences (IEEE ICIP, IEEE ICASSP, EUSIPCO, ...).*