Can Copy Detection Patterns be copied? Evaluating the performance of attacks and highlighting the role of the detector

Elyes Khermaza, Iuliia Tkachenko, Justin Picard

Can Copy Detection Patterns be copied? Evaluating the performance of attacks and highlighting the role of the detector

Elyes Khermaza
Scantrust
Lausanne, Switzerland

Iuliia Tkachenko
LIRIS, UMR CNRS 5205,
Université Lumière Lyon 2
Bron, France
iuliia.tkachenko@liris.cnrs.fr

Justin Picard
Scantrust
Lausanne, Switzerland
justin.picard@scantrust.com

***Abstract*—Copy Detection Patterns (CDP) have received significant attention from academia and industry as a practical mean of detecting counterfeits. Their security level against sophisticated attacks has been studied theoretically and practically in different research papers, but for reasons that will be explained below, the results are not fully conclusive. In addition, the publicly available CDP datasets are not practically usable to evaluate the performance of authentication algorithms. In short, the apparently simple question: "are copy detection patterns secure against copy?", remains unanswered as of today. The primary contribution of this paper is to present a publicly available dataset of CDPs including multiple types of copies and attacks, allowing to systematically compare the performance level of CDPs against different attacks proposed in the prior art. The specific case in which a CDP is the same for an entire batch of prints, which is of practical importance as it covers applications with widely used industrial printers such as offset, flexo and rotogravure, is also studied. A second contribution is to highlight the role played by the CDP detector and its different processing steps. Indeed, depending on the specific processing involved, the detection performance can widely outperform the CDP bit error rate which has been used as a reference metrics in the prior art.**

***Index Terms*—copy detection pattern, public dataset, authentication, copy detector**

I. Introduction

The global economic value of counterfeiting and piracy has been estimated at $4.2 trillion per year[1]. In order to fight this threat which bears on citizens, brands and government organizations, different classes of methods were deployed especially for the protection of packaging and legal documents. Optical watermarks carrying an authenticating image, and special means as specially manufactured inks or substrates with a controlled distribution [11] are among the most popular. The use of measurable but not reproducible characteristics of the document surface is an approach inspired from biometrics for detecting counterfeits [5]. The verification of these characteristics may be done with a mobile device, avoiding the need for a dedicated reader [18], [12]. Similarly, a print signature can be extracted from the randomness of the printing process [21]. One alternative is to characterize the printer and extract a signature which can be retrieved during verification [4], [10]. This paper will focus on a method based on printing digital patterns which are designed to be sensitive to direct duplication, the so-called Copy Detection Pattern (CDP). In contrast to previously mentioned approaches, the CDP does rely on the randomness of the printing process but is based on extracting a signature. Several versions of CDP can be found in the literature [7], [9], [16]. Recently there were different attempts to test security limits of CDPs against duplication, by optimizing the generation of counterfeits using neural networks [13], [14], [19], [20].

The first important contribution of this paper is to present a new dataset of CDPs that consists of originals and fakes created using a number of state of the art estimation attacks. This dataset[2] contains of more than 27'500 CDPs images (scans and corresponding templates) and is the largest public dataset for now. The second contribution is a study of a novel attack on batch CDPs which represents the industrial applications where the same CDP is printed on a large number of items, using for instance an offset or flexogravure printer. With our dataset, we want to verify the validity of the theoretical argument that CDPs printed several times are vulnerable to averaging attacks [1]. The third contribution is the study of different ways of improving the discrimination performance of the authentication test.

The rest of the paper is organized as follows. We present the CDP and the authentication process in Section II. We then discuss the considered estimation attacks in Section III. We describe the CDP dataset and discuss the experimental results in Section IV. Finally, we conclude and overview the future paths in Section V.

[1]The Economic Impacts of Counterfeiting and Piracy. International Chamber of Commerce, 2016

[2]The dataset of CDPs templates and scans is accessible on Kaggle https://www.kaggle.com/scantrust/copy-detection-pattern-dataset

II. Authentication using CDP

A CDP is a noisy maximum entropy image generated with a secret key. CDPs are preferably generated as binary images since printing is, with few exceptions, a binary process. An example of original digital CDP is illustrated in Fig. 1.a.

(a) (b)

Fig. 1. Example of CDP a) an original random binary image before printing (I) and b) its degraded by P&S version ($\tilde{I}$).

A. Information loss principle

The detection of counterfeits with a CDP relies on information loss [7], which applies to each printing and scanning process. A Print-and-Scan (P&S) process, being a stochastic process [6], impacts any CDP by changing both its structure and image quality (see illustration in Fig. 1.b). The noise altering a CDP is difficult to characterize [8] as each printer and scanner has its own characteristics.

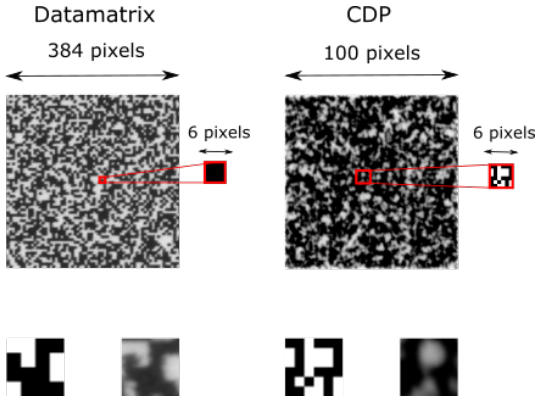


Fig. 2. A comparison of CDP with Datamatrix: in the case of Datamatrix an elementary unit is bigger, thus the information loss principle does not impact a lot to the code structure.

The CDP is often compared to 2D barcodes such as the Datamatrix due to the visual outward resemblance. Nevertheless, we illustrate in Fig. 2 that the elementary unit of Datamatrix is much larger than the elementary unit of CDP. Therefore, the information loss principle does not impact the Datamatrix structure. For example, the correlation measure between a digital Datamatrix and its P&S degraded version can be over 0.9, in comparison the correlation between the digital and P&S CDP is around $0.45 - 0.55$ depending on printer and scanner resolutions. Therefore, the pattern elementary unit size, $u \times u$ pixels (illustrated in Fig. 2), as well as the overall pattern size have a great impact both on the authentication process and on the ability of counterfeiters to reproduce the pattern. In practice, the elementary unit size of CDP is 1 pixel or 2×2 pixels in order to take the maximum advantage of the information loss principle.

B. Theoretical definition of the authentication system

CDP authentication consists of two main steps. The first one is the registration step during which the pattern is generated then printed on an item with the authorized printer, to form an original CDP. The second step is dedicated to verification: after scanning with an authorized reader, the scanned CDP is passed to an authentication test (whose parameters are adjusted during a preliminary registration step). If the test is positive, the item is considered as authentic.

The most frequent attack attempt is as follows: scanning (at high resolution) an item with a printed CDP, estimating the original digital structure of the CDP and reprinting the document with the estimated CDP. In this scenario, we denote I as the digital CDP, its print denoted as $\Pi(I)$, where $\Pi(\cdot)$ is the noisy process due to printing with the authorized device, and the verification scan by the authentication center as $\Sigma(\Pi(I))$, where $\Sigma(\cdot)$ is the corresponding noisy scanning process.

Thus, the pattern in the opponent channel can be described as $\Sigma(\Pi'(\hat{I}))$, where $\hat{I}$ is the CDP estimated by the attacker and $\Pi'(\cdot)$ is the noisy opponent printing process.

The authentication test can be formulated as a hypothesis test:

$$\mathcal{H}_0 : \tilde{I} \sim \Sigma(\Pi(I)),$$
$$\mathcal{H}_1 : \tilde{I} \nsim \Sigma(\Pi(I)),$$

where $\tilde{I}$ is a grayscale image of CDP that receives by the authentication center. It can be either an original CDP (i.e. $\Sigma(\Pi(I))$) or a counterfeited one (i.e. $\Sigma(\Pi'(\hat{I}))$).

For comparison with the digital original CDP, one may use a metric such as a distance or a correlation coefficient [3]. In addition, a distortion threshold ϵ has to be calculated in advance and used for comparison by the authentication center.

C. Detector components

It was shown that authenticating using a grayscale CDP is more efficient than using a CDP after thresholding [6]. That is why the Bit Error Rate (BER) that is commonly used in authentication tests in related scientific papers is preferably avoided in practical implementations. A commonly used metrics is the Pearson correlation. We list below a number of techniques that can be used as part of the authentication test in order to further improve the separability between the original printed CDPs and fakes printed CDPs:

- the use of template resizing: scaling the template by an integer factor (by a factor 2 to 4) allows a more precise sub-pixel matching.
- the use of template matching techniques to take into account sub-pixel geometric distortion following the P&S process. It consists in matching the slightly cropped template with the grayscale scan by maximizing the correlation score.
- the use of high pass filtering (such as unsharp masking) before the correlation score calculation reduces the low

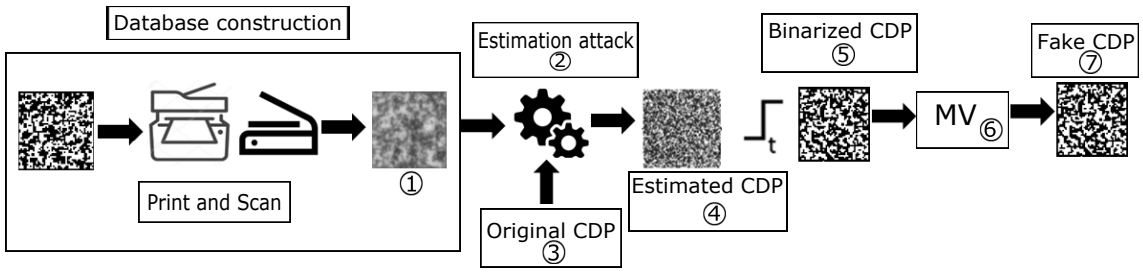


Fig. 3. An overview of estimation attack.

frequencies which are less discriminative and, thus, increases the separation between originals and copies.

These techniques increase the separability between the originals and fakes, as will show the experimental results in Section IV-C.

III. Estimation attack overview

It was shown in [17] that the simple duplication by a copy machine or by creation of any copy without processing of the CDP before reprinting is ineffective. Therefore, in this paper we focus on estimation attacks. The estimation attacks aim at predicting the original, digital form of a CDP using image processing or machine learning approaches.

This estimation attack consists of a sequence of steps, some of which (the original printing at registration, and verification) are controlled by the competent authority. Let us note that an attacker can learn from genuine prints and available (high resolution) scanners if s/he knew the corresponding original digital CDPs. In this way, the attacker can build a training dataset for learning a model and applying it at the end to estimate CDPs. The pipeline of estimation attack is illustrated in Fig. 3.

The main steps of the estimation attack are as follows:

1) Building a training dataset. An attacker builds a dataset, preferably using devices of the same brand and model as those used by the authority and authentication centers. Therefore, this step consists of printing and scanning of N_{train} CDP images that will then be cropped (with re-sizing and orientation correction).
2) Development of the estimation model. An attacker uses N_{train} images prepared in the previous step together with their digital versions in order to identify the correct parameters for the best CDP estimation. The estimation accuracy can be analyzed with the BER: a smaller BER corresponds to a better estimation.
3) Retrieval and scan of an authentic CDP $\tilde{I}$ from any given authentic packaging.
4) Reconstruction of the digital version of the current CDP using the estimation model. The output images of most of the estimation methods (based on deep learning) are grayscale images with values in interval $(0, 1)$.
5) Binarization of the current output image using an optimal threshold in order to obtain a black-and-white image.
6) Majority voting for the construction of a final fake binary CDP image $\hat{I}$. The estimation process is done pixel by pixel such that the $v \times v$ elementary units resulting from the binarization operation are not necessarily homogeneous (i.e. of the same color). A majority vote in each $v \times v$ elementary unit allows the decision providing a fully black otherwise white $u \times u$ units.
7) Printing the (fake) estimated CDP $\Pi'(\hat{I})$, with the goal of obtaining a good estimation of the original CDP I that will fool the authentication test (i.e. $\Sigma(\Pi'(\hat{I})) \sim \Sigma(\Pi(I))$).

A. Image processing attack

One of the most simple attack is the use of thresholding methods to binarize the printed and scanned CDP $\Sigma(\Pi(I))$. In this paper, we use the classical Otsu thresholding as a baseline method (denoted as "Otsu" in the rest of the paper). Nevertheless, it was shown that this attack is not very effective [2].

In order to improve the estimation results, we apply some pre-processing operations. It is known that the unsharp mask significantly increases the sharpness of scanned images. Therefore, we perform an estimation attack using unsharp masking before the binarization using Otsu method (denoted as "Otsu+unsharp" in the rest of the paper). The parameters of the unsharp mask were estimated using a train dataset of N_{train} CDP images.

B. Attacks based on neural network approach

The use of neural networks for attacks is a whole new topic of research. Several recent papers [14], [19], [20] presented initial results, that were promising. These results show us the potential of neural networks to create copies that fool an authentication test. In this paper, we take the implementation proposed in [14] and adapt this implementation to our CDP image size.

C. Averaging attack for batch CDP

In this paper, we would like to study the case of CDPs printed by batch. It was shown theoretically that it is possible to generate a fake CDP that will pass the authentication test by using only a dozen of scans of a same genuine CDP [1]. Nevertheless, this attack was experimentally studied only once using a different type of anti-copy code [15], and has not been tested on CDPs. We built a novel dataset described in

Section IV-A and attempted to produced copies that would pass the authentication test.

Let $C_i, i = 1, \cdots, n$ be digital CDPs. Each C_i was printed and scanned m times that gives us $P_i^j, i = 1, \cdots, n, j = 1, \cdots, m$ samples for estimation attack. An attacker uses all m samples per code to estimate the digital CDP version.

First of all, the samples $P_i^j, i = 1, \cdots, n, j = 1, \cdots, m$ are binarized using either image processing or neural networks. After binarization (step 5) and before the majority vote (step 6), the averaging of corresponding pixel values is applied to a batch of codes.

This averaging step consists in counting the number of black and white pixels for each position in the matrix. If the majority of binarized batch samples have a white pixel in this position, the pixel on the estimated code will also be white, otherwise it will be black. This averaging step helps leveraging the redundancy of the CDP printed by batch and to better estimate the original structure of CDP.

IV. Experiments

In this section, we present the CDP dataset, the estimation results for both types of attacks (estimation per CDP and estimation per batch of printed CDPs) and we discuss the possible evaluation scores in order to improve the separability between original and fake samples.

A. Dataset description

We built two datasets[2]: 1) print of unique CDP (5'000 originals with corresponding templates and 10'000 copies) and 2) print of CDP per batch (2'500 originals with corresponding templates and 10'000 copies).

For both datasets, the digital CDP has size of 52×52 pixels, with $u = 1$ p/e which is defined at 600 ppi, printed with 600 dpi and scanned with 2400 dpi using printer Canon IR-ADV C5535i. Therefore, the printed and scanned codes have the size of 208×208 pixels (so that $v = 4$ p/e).

The **dataset of unique CDP** consists of 5000 unique CDP images (both templates and printed and scanned versions). We took $N_{train} = 2500$ images for developing the estimation model, $N_{valid} = 1000$ images for validation and $N_{test} = 1500$ images for test. We applied all the mentioned estimation attacks on these CDPs. The estimation results and the authentication results are presented below in this section.

The **dataset of batch CDPs** consists of $n = 50$ unique CDP images. Each image was printed and scanned $m = 50$ times. That gives us in total 2500 printed and scanned versions of 50 unique CDP templates. After that we have applied 4 estimation attacks in fusion with averaging attack. The estimation results show that these attacks work better in term of BER minimization, nevertheless as described in Section IV-C, the authentication process is still quite robust.

B. Estimation results

Here we present the estimation results for both datasets. We evaluate the effectiveness of estimation attack using the BER: the smallest BER corresponds to the best estimation attack.

For the estimation attack "Otsu+unsharp", we experimentally determined the optimal parameters for the unsharp mask using $N_{train} = 2500$ images: radius is $2,875$ and amount is 10.

For the estimation attack using a neural network approach, the images of the training dataset were divided in patches of size $13 \times 13 = 169$. We used the two proposed architectures from [14]: fully connected neural network with 2, 3 and 4 hidden layers (FC2, FC3, FC4 respectively) where the size of each layer equals to the input size (i.e. 169) and bottleneck DNN (BN DNN) model with 2 fully connected hidden layers of size 128 and 64 at the encoder and decoder parts and a latent representation of size 32.

Both networks were implemented using Pytorch library with the following training parameters: number of epochs equal to 25, the batch size equal to 128, the activation function is ReLU, the loss function is MSE (Mean Squared Error), the optimizer used is Adam and the learning rate is: $1e-3$. The training was done on a NVIDIA Tesla K80 GPU.

Estimation per CDP. For the estimation of unique CDPs, the best results are obtained for "BN DNN" and for "Otsu + unsharp" as shown in Table I, for both approaches the BER is around 23%.

	Mean BER	Min BER	Max BER
Image processing approach			
Otsu	33.60%	29.86%	38.40%
Otsu+unsharp	**23.37%**	**19.92%**	**27.08%**
Neural network approach			
FC2	28.06%	25.68%	31.06%
FC3	26.95%	24.33%	30.26%
FC4	24.68%	21.13%	28.64%
BN DNN	**23.27%**	**20.31%**	**26.99%**

TABLE I
ESTIMATION RESULTS PER UNIQUE IMAGE.

We note that in general, the BER results are worse than those reported in state of the art papers. We can suppose that it is due to 1) the smaller size of CDP used (in comparison with state of the art datasets), 2) the impact of printer and scanner used, and 3) the bad adaptation of parameters used in the state of the art networks for our dataset.

Estimation per CDP batch. In the case of estimation per batch, $m = 50$ images were used to predict the structure of the digital CDP. The results are reported in Table II: the column "unique image" signifies the mean BER value calculated for 50 independently estimated CDP (before applying the averaging attack per batch), the column "batch estimation" presents the results of averaging attack. We note that the averaging attack decreases the BER value on average by $6 - 7\%$.

	Unique image	Batch estimation
Otsu	$30.24\% \pm 0.58$	$28.32\% \pm 0.78$
Otsu + unsharp	$25.89\% \pm 0.75$	$18.85\% \pm 0.64$
BN DNN	$25.32\% \pm 0.75$	**18.47% ± 0.77**
BN DNN + unsharp	**25.27 % ± 0.72**	$18.48\% \pm 0.72$

TABLE II
ESTIMATION RESULTS PER BATCH.

We add here the estimation attack "BN DNN + unsharp", which means that we apply the unsharp mask before the estimation with BN DNN as the use of unsharp mask significantly

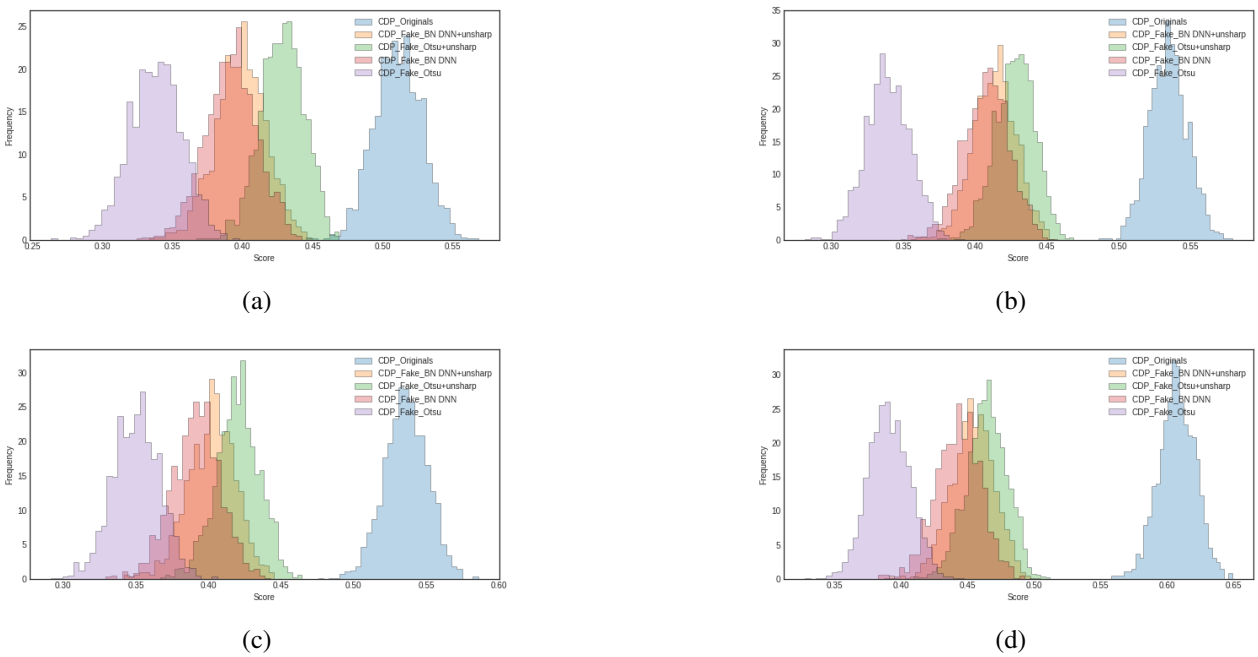


Fig. 4. The histograms of authentication scores a) without image pre-processing, b) matching of template CDP with search space of 2 pixels, c) unsharp masking with radius 2 and amount 4, d) use of both template matching with search space of 2 pixels and unsharp masking with radius 2 and amount 4.

improve the estimation results in case of image processing based attacks.

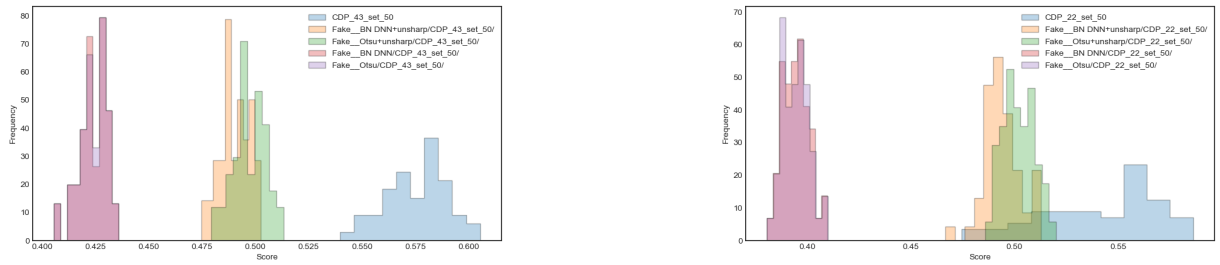
C. Authentication scores improvement

For our authentication test we use the Pearson correlation score calculated between the template CDP and the test scanned CDP. All the estimated CDPs were printed and scanned using the same printer and scanner.

As explained in Section II-C, the authentication scores can be improved using some pre-processing techniques. We illustrate the obtained results depending on pre-processing used in Fig. 4. If we do not use any pre-processing before the correlation score calculation, we will get a small overlap between the originals and fakes as illustrated in Fig. 4.a. This means that only a small amount of fakes can pass the authentication test. More precisely there are $2.3\%, 0.67\%, 0.13\%, 0\%$ of fakes estimated using "Otsu+unsharp", "BN DNN+unsharp", "BN DNN" and "Otsu", respectively that can be considered as authentic. For fakes estimated using "Otsu", the difference between the worst authentic score and best fake score is 0.048. When we apply some pre-processing of the grayscale CDP image before correlation score calculation, we get a better separation of the score distributions, and no more overalp between originals and copies. Fig. 4.b illustrates the distribution separation while using template matching with a search space of 2 pixels. Fig. 4.c illustrates the distribution separation when using unsharp masking with radius 2 and amount 4. Finally, the best separation of scores distributions is obtained when applying both pre-processing operations (template matching and unsharp masking) as shown in Fig. 4.d. These results show that the use of pre-processing steps before calculation of correlation scores does help to protect the CDPs against estimation attacks.

For the attack by batch, the authentication threshold ϵ is calculated per batch, as is done in practical implementations. We illustrate only the case where the authentication scores were calculated using the best proposed image pre-processing, i.e. the authentication scores were calculated using both template matching with search space of 2 pixels and unsharp masking with radius 2 and amount 4. The minimal score values for original CDP batches are in the range $0.43 - 0.54$. In the same time, the minimal score values for estimated CDP batches are smaller: "Otsu" - $0.34 - 0.39$, "Otsu+unsharp" - $0.43 - 0.48$, "BN DNN" - $0.34 - 0.39$, "BN DNN+unsharp" - $0.41 - 0.48$. In general, the authentication score depends on CDP image quality and the distribution of black and white pixels in the CDP. Therefore, the distribution of scores is difficult to be predicted. We illustrated two possible cases of scores distribution in Fig. 5. In some cases, there are more estimation errors and the distributions of scores are well separated as illustrated in Fig. 5.a. In other cases, the overlap between the original and fake score distributions is significant and thus a large amount of fake CDPs will pass the authentication test as illustrated in Fig. 5.b.

Identically to the unique CDP dataset, the fakes that can pass the authentication test are those produced using "Otsu+unsharp" and "BN DNN" estimation attacks. In total, the number of fake CDP codes that pass the authentication score is the following: 0% of fakes estimated by "Otsu", 32.4% of fakes estimated by "Otsu+unsharp", 0% of fakes estimated using "BN DNN", 19.76% of fakes estimated by



(a) (b)

Fig. 5. The histograms of authentication scores while using the batch CDP scenario with both template matching with search space of 2 pixels and unsharp masking with radius 2 and amount 4. An example of a) perfect separation between the originals and the fakes and b) bad separation between the originals and the fakes produced using "Otsu+unsharp" and "BN DNN+unsharp" estimation attacks.

"BN DNN+unsharp".

Based on these results, we can conclude that the choice of authentication threshold ϵ is very important and we need to find a trade-off between the number of rejected original CDP and the number of accepted fake CDP. In practice, it is preferable to accept the maximal number of originals.

V. Conclusions and perspectives

In this paper, we studied the security aspects of Copy Detection Pattern (CDP) under estimation attack. We have built two large datasets: one with unique CDPs and one with CDPs printed by batch. Experimentally, it was shown that the use of Pearson correlation as authentication score is quite robust for authentication, nevertheless some fakes can pass the authentication test. In order to increase the gap between the original and the fake CDPs, we have proposed to use some pre-processing operations. These operations allow to fully separate the original scores from fakes in the case of unique CDP. However, these techniques are not sufficient to guarantee full separation for the batch CDP as the estimation process is more accurate.

In future work, we would like to improve the estimation results using neural networks and study improvements of authentication score calculation which increase the discrimination between originals and fakes.

References

[1] C. Baras and F Cayre. Towards a realistic channel model for security analysis of authentication using graphical codes. In *2013 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 115–119. IEEE, 2013.

[2] M. L Diong, P. Bas, C. Pelle, and W. Sawaya. Document authentication using 2d codes: Maximizing the decoding performance using statistical inference. In *IFIP International Conference on Communications and Multimedia Security*, pages 39–54. Springer, 2012.

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

[4] A. Ferreira, L. Bondi, L. Baroffio, P. Bestagini, J. Huang, J. A. dos Santos, S. Tubaro, and A. Rocha. Data-driven feature characterization techniques for laser printer attribution. *IEEE Transactions on Information Forensics and Security*, 12(8):1860–1873, 2017.

[5] R. N. Goldman. Non-counterfeitable document system, December 27 1983. US Patent 4,423,415.

[6] A-T. Phan Ho, B-A. Mai Hoang, W. Sawaya, and P. Bas. Document authentication using graphical codes: Reliable performance analysis and channel optimization. *EURASIP Journal on Information Security*, 2014(1):9, 2014.

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

[8] J. Picard. On the security of copy detectable images. In *NIP & Digital Fabrication Conference*, volume 2008, pages 796–798. Society for Imaging Science and Technology, 2008.

[9] J. Picard and P. Landry. Two dimensional barcode and method of authentication of such barcode, March 14 2017. US Patent 9,594,993.

[10] S. B Pollard, S. J Simske, and G. B Adams. Model based print signature profile extraction for forensic analysis of individual text glyphs. In *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on*, pages 1–6. IEEE, 2010.

[11] R.L van Renesse. Optical document security. *Boston: Artech House*, 1998.

[12] R. Schraml, L. Debiasi, and A. Uhl. Real or fake: Mobile device drug packaging authentication. In *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, pages 121–126. ACM, 2018.

[13] O. Taran, S. Bonev, T. Holotyak, and S. Voloshynovskiy. Adversarial detection of counterfeited printable graphical codes: Towards" adversarial games" in physical world. In *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2812–2816. IEEE, 2020.

[14] O. Taran, S. Bonev, and S. Voloshynovskiy. Clonability of anti-counterfeiting printable graphical codes: a machine learning approach. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brighton, United Kingdom, May 2019.

[15] I. Tkachenko and C. Destruel. Exploitation of redundancy for pattern estimation of copy-sensitive two level QR code. In *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6. IEEE, 2018.

[16] 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*, 11(3):571–583, 2016.

[17] I. Tkachenko, W. Puech, O. Strauss, C. Destruel, and J-M. Gaudin. Printed document authentication using two level QR code. In *Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International Conference on*, pages 2149–2153. IEEE, 2016.

[18] C-W. Wong and M. Wu. Counterfeit detection based on unclonable feature of paper using mobile camera. *IEEE Transactions on Information Forensics and Security*, 12(8):1885–1899, 2017.

[19] R. Yadav, I. Tkachenko, A. Trémeau, and T. Fournel. Copy sensitive graphical code estimation: Physical vs numerical resolution. In *2019 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6. IEEE, 2019.

[20] R. Yadav, I. Tkachenko, A. Trémeau, and T. Fournel. Estimation of copy-sensitive codes using a neuronal approach. In *ACM workshop on Information hiding and multimedia security*, Paris, France, June 2019.

[21] B. Zhu, J. Wu, and M. S. Kankanhalli. Print signatures for document authentication. In *Proceedings of the 10th ACM conference on Computer and communications security*, pages 145–154. ACM, 2003.