Authentication of rotogravure print-outs using a regular test pattern

Iuliia Tkachenko, Alain Trémeau, Thierry Fournel

Authentication of rotogravure print-outs using a regular test pattern

Iuliia Tkachenko, Alain Trémeau, Thierry Fournel
Preprint

***Abstract*—The medicine falsification is an important problem nowadays which represents a real danger for human lives. Therefore, it is important to find a cheap and efficient solution that can be used for all kinds of medicines. In this paper, we explore the domain of pharmaceutical packaging printed on blister foils using rotogravure process. It was shown that the chemical etching has a stochastic nature that can be spotted by correlation or classical machine learning methods. We propose an authentication system that uses a novel regular test pattern for authentication of blister foils. Thanks to this regular test pattern we can identify the cylinder used for printing and the position of the regular test pattern engraved on the authentic cylinder, as well as easily reject the fake patterns printed using counterfeiter cylinder and rotogravure press. The proposed identification/authentication system cannot be easily attacked as it is not possible to imitate the signature of chemical etching process. Additionally, we will shortly discussed the possibility to enlarge the proposed system to another types of engraving processes and formulate some future paths for this work.**

***Index Terms*—authentication, graphical code, anti-copy pattern, medicine packaging, blister foils, rotogravure printing**

I. Introduction

The World Health Organization (WHO) estimates that 1 in 10 medical products in low- and middle-income countries is substandard or falsified[1]. The falsified medicines are dangerous for human health and life. The WHO as well as other international organizations point out the importance of this problem and look for solutions to detect and decrease the number of counterfeited medicines all over the world.

The medicine protection is based on some security elements that are inserted to the pharmaceutical packaging. However, due to international regulations and the cost of security features for pharmaceutical companies, the graphical design complexity is minimal [4]. The most common solutions are 1) the use of some specific inks or specific sticky labels [40] and 2) the use of holograms. Both solutions are visible by naked eye and supposed to be user friendly. Nevertheless, it is extremely difficult to verify the authenticity of these security elements by non-professionals, moreover these solutions could increase the cost of medicines. Therefore these solutions are not used for the protection of cheap medicine blister foils.

The recent drugs packaging are marked with 2D barcodes which are used for track-and-trace and serial numbers for fighting against medicine counterfeits. Several novel user-friendly solutions were developed to increase the security of packaging[2]. Nevertheless, these solutions use barcodes that can be easily copied by a counterfeiter. Another solution consists of the use of intrinsic texture features of the packaging material [42], [32]. The system presented in [32], [33] uses a machine learning approach and a pre-defined database to identify the manufacturer and the product using some physical textures that are found on blister and carton packaging of medicines. This authentication system uses the support characteristics of packaging in order to ensure the authenticity of medicines. This solution works well, but needs a lot of data to train an accurate authentication model.

Another promising solution is security printing. Indeed, security printing is a robust and low cost solution while using some copy sensitive graphical codes [29], [37]. Nevertheless, these difficult-to-predict security elements are often printed on high resolution printers and on cardboard, by batch where appropriate. Meanwhile the blister packaging is the most used support for medicines (especially for cheap ones) printed at a good resolution but not necessary at the highest one.

In order to print on blister foils we need to use specific printing devices. One of the commonly used printing processes is rotogravure printing which is significantly different in comparison with inkjet and laser printing techniques. Taking into account the specific conditions of production process of medicine packaging, in particular the printing of aluminium foil covering the blisters of medicines, it is important to find a solution that is similar to printer/scanner forensics [24], [14], [25], and can be verified by professionals (as pharmacists), and ideally by the final customers.

The rotogravure printing process is based on some particular and important steps that will be discussed in details in Section III. One of these steps is the engraving process of cylinder that is used for printing process. The basis of this study is to use the variation of chemical reactions during cylinder engraving process as well as the stochastic nature of rotogravure printing process. Our hypothesis about the nature of rotogravure printing was: each engraved cylinder has its own signature due to the randomness during the engraving process. We have shown in our previous works that 1) each rotogravure printing system has its own signature [38] and that the engraving process signature is more important than the press signature [39]. Indeed, the engraving process can

Iuliia Tkachenko is with LIRIS, Université Lumière Lyon 2, CNRS, France. Alain Trémeau, Thierry Fournel are with Laboratory Hubert Curien, Université Lyon-UJM Saint-Etienne,CNRS, France.
The e-mail of corresponding author: iuliia.tkachenko@liris.cnrs.fr

[1]WHO article about substandard and falsified medicines https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products

[2]An example of user-friendly verification system: https://sproxil.com/sproxil-products/sproxil-defender-brand-protection-anti-counterfeiting/

be considered as physically unclonable function due to the same stochastic nature as the printing process by laser printer [12]. In order to identify the blisters that were printed using the authentic cylinder and press, we introduce in this paper a specific regular test pattern, presented in Section IV-B.
The advantages of the suggested authentication system with regular test pattern are:

- protection of health care system with the detection and control of the counterfeited medicines thanks to a low-cost trace tag;
- easy verification by professionals but also potentially by consumers (with standard smart cameras equipped with proper optical lenses).

The proposed authentication system is based on the characteristics of the chemically-engraved cylinder of a rotogravure printing device [39]. These characteristics differ a lot from well-studied laser and inkjet printings. The proposed system can in particular be useful for the low-cost batch authentication of blister foils in medicine, medical or food packaging. We have tested the system experimentally on metallic blisters with some cylinders and presses especially engraved for our experiments. Its resistance to counterfeiting is then evaluated through different attacks.
The main contributions of this work are the following:

1) We propose a regular test pattern that suffers from random effects due to the chemical engraving process, see Section IV-B. The resulting local irregularities are digitally spotted by classical correlation or sparse coding and non-negative least squares classifier for authentication purpose. The construction of the proposed security element is simple and scalable such that it can easily be inserted into any artwork and be printed on packaging. Therefore, beyond engraving a proposed regular test pattern, no special means are required (i.e. no additional cost) when embedding such element to the packaging artwork.
2) We conducted an investigation of rotogravure printing and showed the possibility to identify not only the cylinder used for printing, but also the place on the cylinder used for printing, see Section V-B and Section V-C.
3) We propose two authentication systems that can efficiently reject the fake samples (i.e. samples printed using another engraved cylinder). The security of the proposed authentication system is based on the stochastic nature of the chemical engraving process, see Section V-D.
4) We study the impact of printing support on authentication. It was shown that the samples printed using the same cylinder and press on different supports (blister and strip) cannot be easily separated while using the classical metrics as Pearson correlation, see Section V-E. A further investigation of this path will be done on future.
5) We created a database of regular test patterns[3] that can be used to study and to model the rotogravure printing process. This database consists of 900 images of regular test pattern engraved on two different cylinders and printed using two different presses, more details are given in Section V-A.

The rest of the paper is organized as follows. Existing printing solutions are overviewed in Section II. The main production steps of the printing process using rotogravure and the characterization of this process are explained in Section III. Then we present the suggested authentication system and describe a novel regular test pattern in Section IV. The experimental results are demonstrated in Section V. We discuss the possible attacks and the future paths in Section VI. And finally, we conclude in Section VII.

II. Overview of existing printing solutions

The continuous increase of counterfeit supplies in the market and of products manipulations due to the current pandemic situation[4] encourages engineers and researchers to look for solutions that enable to protect packaging, or documents, as well as the associated data. In addition to the use of special substrates and special inks, different combinations of devices and techniques have been suggested for the authentication of valuable objects [40], as Optical Variable Devices (OVDs) including holograms and kinegrams, and intaglio printing. Nevertheless, these solutions are based on regulated productions funded on restrictive means and know-how which can require expertise at verification stage.
The nowadays requirements for printing protection techniques are: 1) easy integration and generation processes; 2) low cost; 3) fast and automatic verification process; 4) use of standard printing techniques without specific papers and inks; 5) use of common devices for verification (scanners, high resolution cameras or mobile phones); 6) reliable verification by any user; 7) good level of global protection and difficulty of fraud (the counterfeiting process might be expensive).
The development of protection elements based on physical characteristics resulting from the packaging manufacturing process or document production process, can satisfy all these requirements. Such characteristics may come from substrate components as paper fibers, the printing process, or their interaction. Whatever the form of the data associated to an object, such as text or image, they suffer from various distortions after printing like low-pass filtering, rotation, scaling, translation, contrast and luminance adjustments, in addition to various types of noises [22]. In such a framework, different solutions have been investigated to prevent unauthorized duplication of paper documents and packaging via some print elements. The main three approaches for anti-copy protection are the following:

1) Material unclonable characteristics-based approach.
In the series of patents [7], [8], [9], [10], the authors suggested to use Measurable But Not Duplicable (MBND) characteristics. These MBND physical characteristics are the fibers of the paper material and the shape of engraved dots used to ensure unclonability of packaging

[3]The data set is publicly available https://perso.liris.cnrs.fr/itkachenko/pages/dataset_regpat.html

[4]Inquiry into fake COVID-19 products progresses https://ec.europa.eu/anti-fraud/media-corner/news/13-05-2020/inquiry-fake-covid-19-products-progresses_en

and documents. Their authentication system is based on the extraction of MBND characteristics from a security tag and on the representation of these characteristics in numerical form. Then a reference numeral is either printed on the reference product or stored in a registration database for further authentication. Many efforts have been achieved recently for such a verification using mobile phone camera, for example for paper documents in [41], [42] or for drug packaging classification and manufacturer identification in [32], [33].

2) Printed anti-copy element-based approach.
This approach investigates some elements designed or selected for their high sensitivity to the printing process. The impact of noise resulting from a printing alters either a hard-to-predict graphical code for which reversing the print-and-scan process is difficult or a properly predefined test pattern whose deviation after printing is used as signature. These two types of originally binary anti-copy elements correspond to the subclasses of Copy Sensitive Graphical Codes (CSGCs) [28], [30], [37], [26] and Print Test Patterns (PTPs) [44], [31], respectively.
Recent research works showed the vulnerability of CSGCs based approaches to deep-learning based estimation attacks [43], [1]. Nevertheless, the countermeasures based on pre-processing technique [16] and the use of similarity metrics combinations [35] showed the usability of such solution in real-world applications for packaging protection.
3) Forensics approach.
By analogy to image forensics, this approach aims at identifying the printer and possibly the scanner [2] that were used to produce a given hardcopy document/packaging and its scanned version. The printer and captured device identifications are more complex problems than camera identification as some mechanical and optical components are involved in the process of captured document production chain [11]. Some recurrent features are extracted from printed characters according to different techniques as gray-level co-occurrence matrix [23], [24], noise energy, contour roughness and average gradient of characters edges [34]. Next these features are classified using different machine learning methods (LDA, SVM, etc.) in order to identify the printer. For source scanner identification, in [14], [15] the authors use the imaging sensor pattern noise. In the last years, some forensics methods based on deep learning appear [5], [25]. In [25] authors also presented a human-interpretable extension of forensics algorithms that can aid human experts to interpret the forensics results. Recently, it was shown that the use of shape descriptors under a microscopic scale with lightweight implementation can successfully be used for identification of printing sources in real-world applications [27]. In this work the dot samples printed using conventional offset, waterless offset and electrophotography printing technologies were studied.
Another interesting approach uses the high energy patches of printed document in siamese networks architectures in order to find texture similarities between documents printed by the same printers [6]. This solution is interesting as it gives good results in open and closed set conditions.

All the mentioned solutions, especially the recent forensics systems [27], [6] and CSGC based authentication systems [16], [35], achieve good identification/authentication results. Nevertheless, almost all cited solutions were tested on coated or uncoated paper using laser printers. Therefore, these solutions are not adapted for the medicine blister foils protection.
The objective of this paper is to introduce a regular test pattern and to use it as an anti-copy mean. The regular structure of the proposed pattern is altered by the rotogravure printing engraving process, so that it can be used to identify the cylinder used for printing, and thus to authenticate a given packaging as in printer profiling.

III. Rotogravure printing process

Rotogravure printing is often used for production of magazines, catalogs and packaging (from extremely thin foils to thick cardboard) thanks to rapid and cheap printing process, production of high-quality images and intense rich colors. We highlight the main steps of the packaging production in Section III-A. And we discuss the most common characteristics of rotogravure printing in Section III-B.

A. Main printing process steps

The packaging production process using rotogravure printing consists of three main steps: 1) design of artwork; 2) cylinder engraving according to the designed artwork; 3) printing using the engraved cylinder/s.

Design of artwork. The design of artwork is achieved by using a graphics editor software. Then, it is pre-processed in order to define the main engraving parameters. For this purpose the following steps are performed: 1) define the width of lines; 2) correct the edges, manage the overlaps, and minimize the color border imperfections; 3) define the number of colors used and the order of cylinders used for printing process; 4) define the screen angles depending on packaging material used; 5) define the dots shape and the cells depth. When all the pre-processing steps are done, the artwork is ready to be engraved on a cylinder.

Engraving of cylinder. The cylinder can be engraved using three different technologies: chemical etching, electromechanical or laser engraving. Depending on engraving process used the form of dots and edges change. For example, the chemical etching produces better borders, as the cylinder engraving can engrave half-dots (thanks to the variable dots area, illustrated in Fig. 1). On the other hand, with electromechanical engraving, the sharpness of edges is ensured by the dots of same shape (inverted pyramid shape) but with smaller depth and area.
After engraving, the cylinder is polished to remove the imperfections and to get a consistent surface. Finally, the cylinder passes an inspection before going to the press.
In this paper, we focus exclusively on cylinders engraved using chemical etching. This engraving process is the oldest

one. One of the properties of this process is its dots shape variability at a micro-scale, as it is complicated to control the chemical reactions and almost impossible to standardize [17]. This microscopic changes can be seen as a signature that characterizes a cylinder. This signature can be exploited as discussed in Section IV-A.

Printing process. The printing press consists of several color units, as each primary color is printed using a specific engraved cylinder. One color unit consists of an engraved cylinder, a press and an ink pan, as illustrated in Fig. 1. The engraved cylinder rotates through the ink pan. The cylinder cells that correspond to image areas to be printed pick the ink from the ink pan. The non-image areas and the over quantity of ink are scarped by a blade before the ink is transferred to the support (paper or blister) surface. After each ink unit, the ink is dried using high velocity air nozzle dryer.

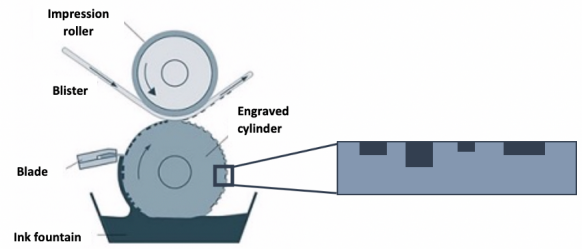


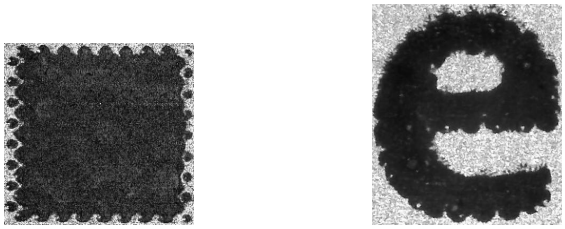
Fig. 1. A color unit of rotogravure press. While the cylinder is engraved using chemical etching, the cells can have variable depth and variable area to ensure sharper image borders.

Due to the specific ink characteristics and mechanical imperfections of the press, the images printed by the rotogravure device have also micro variations that can be considered as a press signature (see Section IV-A).

B. Rotogravure printing characterization

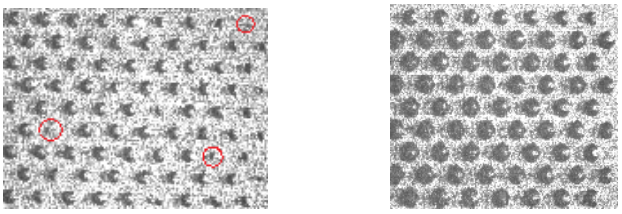
The images printed with rotogravure process have several distinguishable characteristics that differ from other well-known printing technologies like offset or flexographic [17]. In this section, we mentioned several characteristics that were easily identifiable during our experiments.

The first typical characteristic of rotogravure printing is serrated edges presented on all printed types and line works. These serrated edges are almost invisible by naked eye, but can be observed when zooming in as illustrated in Fig. 2.



(a) (b)

Fig. 2. Example of serrated edges on a) the edges of a block pattern and b) letters observed by using a ZEISS microscope with $\times 5$ magnification.



(a) (b)

Fig. 3. Example of a) missing dots in a uniform patch printed with resolution 152 lpi and b) "doughnuts" in a uniform patch printed with resolution 136 lpi. The images were captured using a ZEISS microscope with $5\times$ magnification.

When the bottoms of cells do not release ink quickly during printing, the ink transfer is altered inducing missing dots (Fig. 3.a) or partially inked dots providing the so-called "doughnuts" (Fig. 3.b). Recently six types of dot patterns (including four types of "doughnuts" patterns) have been identified in [3]. The authors showed the possibility to use differences of geometrical shapes of printed dots for differentiation of print document from reprinted one.

As reported in [20], many physico-chemical parameters play a role in such alterations as ink viscosity. The low viscosity eases ink transfer from cells to the substrate and causes a limited sharpness of printed images [13]. The ambient temperature as well as the ink characteristics are in general assumed to be constant and well controlled: they are not taken into account in the present work.

IV. Novel authentication system

In this section, we present a novel security pattern that can be used for the cylinder identification and packaging authentication. First we discuss the general idea of rotogravure process signatures in Section IV-A. Next, the proposed regular test pattern is presented in Section IV-B. The proposed authentication system is then introduced in Section IV-C and two solutions for printing system profiling are exposed in Section V-D.

A. Printing process signatures

Let W be an artwork (a digital image) designed for cylinder engraving and in fine packaging, and E be a proposed regular test pattern placed n times in artwork W at positions E_i ($i = 1, \cdots, n$). A cylinder where the digital regular test pattern was engraved $n = 6$ times is depicted in Fig. 4.

In a previous work, we spotted that each engraved cylinder of a specific rotogravure printing system transmits its own spatial "signature" that can be measured by image correlation [38]. We showed thus the uniqueness of letters/characters printed using rotogravure process. However, as rotogravure printing process consists both of engraving process and printing process, we did not know which process impacts more the signature. In another work [39], we showed that there exists a cylinder signature and that this signature is more important than the signature of press. We showed that a simple machine learning method (based on minimization of distance between the PCA features of image or based on Non-Negative Least Squares classifier) allows the identification of the cylinder

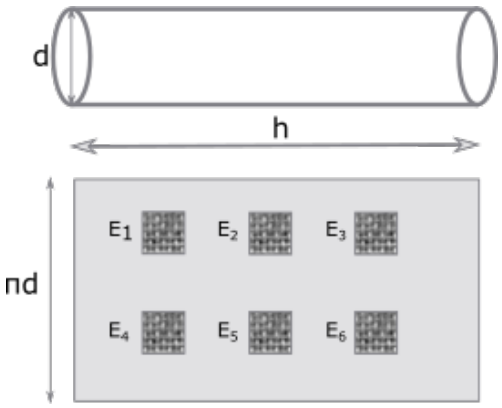
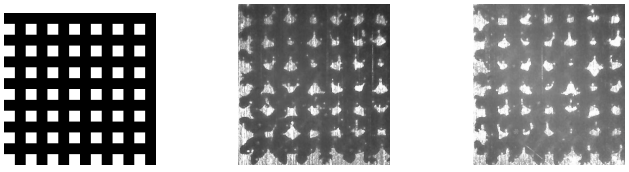


Fig. 4. The same test pattern is engraved in $n = 6$ different positions on the same cylinder.

used.
In this paper, our objective is to show that it is even possible to identify the position of engraved regular pattern on the cylinder (and thus in the artwork W) as the engraving process induces micro-differences between the same pattern engraved several times which are represented by the different image features. This will help us to be more accurate while the authentication is done.

B. Regular test pattern construction

In the Section III-B, we stated that the printed lines have serrated edges and dots have random shapes due to chemical reactions of the etching process. Next in the Section IV-A, we stated that each engraved cylinder has a signature. This leads us to the idea to consider a grid as a regular test pattern to be engraved at the printing system resolution and to be used to distinguish the different engraved versions of the same regular pattern. The resulting image (roughly speaking a matrix of white dots) will be exploited in the goal to discriminate packages printed from a certain cylinder and from a certain engraved version of the regular test pattern using image correlation or image sparse coding (see Section IV-D). The digital regular test pattern (a part of) is shown in Fig. 5(a). The rotogravure process produces intrinsically enough randomness to discriminate between two prints obtained from two different engravings of this regular test pattern on the cylinder as illustrated in Fig. 5(b-c).



(a) (b) (c)

Fig. 5. An illustration of a) proposed regular test pattern E, b) printed regular test pattern in position E_1, and c) printed regular test pattern in position E_4.

We can observe very different shapes between the corresponding holes in these prints. The source of a print, an engraved version of the test pattern, can be identified on the cylinder (equivalently the corresponding regular test pattern can be located in the artwork).

C. Proposed authentication system

As the engraved cylinder signature has the biggest impact on the printed images [39], we propose an authentication system based on cylinder signature which takes also into account the position where regular test pattern E is placed into the artwork W.
Let $E_i = \Pi_a(\Sigma_a(E)), i = 1, \cdots, n$ be an authentic test pattern E printed in the i^{th} position, where Σ_a is the signature of the engraving process and Π_a is the signature of the press. As shown experimentally (see Section V-B), all patterns E_i, printed using the same place in the cylinder and the same press, have some specific characteristics thanks to the cylinder and press signatures. Therefore, we can hypothesis that all these patterns belong to the same class Λ_i ($\forall E_i \in \Lambda_i$).
From the opponent side, anyone can easily retrieve the underlying structure of regular test pattern E, and capture some features. Whatever, counterfeiters need to produce their own cylinder in order to produce the counterfeits and to use another press for printing:

$$E_i^c = \Pi_c(\Sigma_c(E)), i = 1, \cdots, 6,$$

where Σ_c is the signature of the counterfeiter engraving process and Π_c is the signature of the counterfeiter press. Therefore, the counterfeited patterns E_i^c would belong to another class of patterns Λ_i^c and should be spotted during authentication process.
Taking into account the signature of the engraving process and the press, we can formulate the authentication test as a hypothesis test:

$$H_0 : E' \in \Lambda_i,$$

$$H_1 : E' \notin \Lambda_i,$$

where E' is a new captured security pattern to be tested and $\Lambda_i, i = 1, \cdots, n$ are the authentic classes of security patterns engraved in authentic cylinder.
The overview of the proposed authentication system is presented in Fig. 6. First, the authority center collects some samples E_i^k $(k = 1, \cdots, m)$ for each position i $(i = 1, \cdots, n)$ during the packaging printing process. Next, these samples are used to find the profile (signature) of the cylinder and press used (this corresponds to the model M in Fig. 6) using either some image processing (IP) tools (like correlation, distance, etc.) or some machine learning (ML) methods (classical or based on neural network approach). During the authentication process, the authority center captures an image of the packaging to be tested, denoted as E', and tries to identify whether it was printed using the authentic cylinder and press, using the model M. If an image E' does not have the same signature as samples E_i, this packaging is considered as a fake.

D. Printing system profiling

We propose to use two types of approaches for printing system profiling.

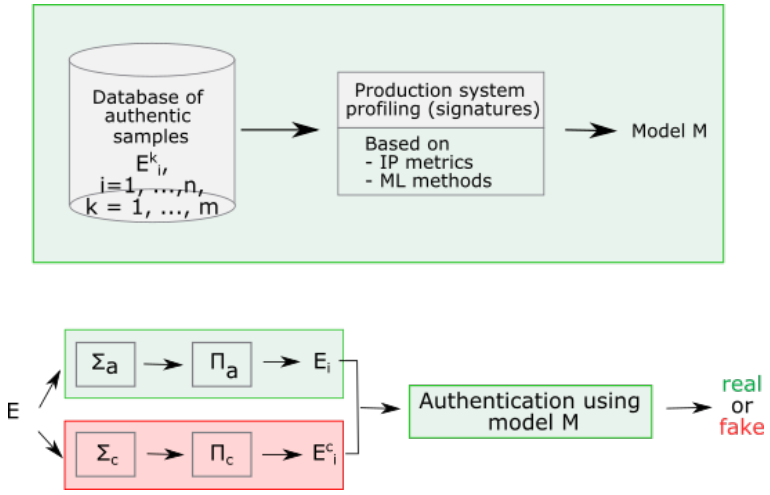


Fig. 6. Overview of the proposed authentication system.

Image Processing (IP) metric approach. We store in a database the template of the regular pattern engraved in each position, i.e. images $E_i, i = 1, \cdots, n$ (in this case $m = 1$). At the same time, a small validation data set is used to identify an optimal authentication threshold (Th) experimentally. It is calculated as a minimal correlation value between the templates E_i and the validation data set images $V_i^k, i = 1, \cdots, n, k = 1, \cdots, m$: $Th = \min \text{cor}(E_i, V_i^k)$.
When a new sample E' is captured, the Pearson correlation values $cor_i = \text{cor}(E_i, E'), i = 1, \cdots, n$ are computed. Then the maximal correlation value is compared with the authentication threshold Th:

$$\max_i\{cor_i\} \begin{cases} > Th & \text{authentic,} \\ < Th & \text{fake.} \end{cases}$$

Machine Learning (ML) approach. We used the classification method based on Non-Negative Least Squares (NNLS) described in [18]. The NNLS classifier consists of two steps:

1) Sparse coding, this step is needed to solve the NNSL optimization problem:
$$\min_X \frac{1}{2}\|b - AX\|_2^2,$$
where A is the training set consisting of $m \times i$ images, b is a new sample, X is a coefficient vector.
2) Sparse interpreter, this step consists to predict the class label corresponding to sample b using max-function: $l = \max(X)$.

In our authentication problem, the matrix A consists of m samples of the same regular pattern engraved in same position, i.e $E_i^k, i = 1, \cdots, n, k = 1, \cdots, m, m = \{1, 5, 10\}$. That gives us in total $m \times i$ samples in training data set. It means that in the sparse coding step, we have m coefficients in vector X for each position i of the test pattern.
We propose to slightly modify the sparse interpreter step, by calculating the sum of coefficients that correspond to the same position: $t_i = \sum_{k=1}^{m} X(E_i^k), i = 1, \cdots, n$. Then, for class label identification we use the max-function ($l = \max_i(t_i), i = 1, \cdots, n$) and for authentication we compare the $\max_i(t_i)$ with the authentication threshold Th calculated experimentally using the validation data set. This threshold Th is equal to the minimal t_i value ($\min_i(t_i)$) in validation data set.

V. Experiments

In our experiments, we used cylinders engraved using chemical etching. A black and white image of the regular test pattern was printed on aluminum strips. This regular test pattern E was engraved $n = 6$ times in each cylinder (see Fig. 4).
The database created is introduced in Section V-A.The existence of press and cylinder signatures is experimentally demonstrated in Section V-B. Then, cylinder identification is discussed in Section V-C. Finally, results of packaging authentication, based on regular pattern, are presented in Section V-D and impact of printing support to authentication is discussed in Section V-E.

A. Database description

We created an artwork with proposed regular test pattern that was then used by the printer agency in order to chemically engrave two cylinders (C_1 and C_2). When the cylinders were engraved, the printing agency used them to print our samples on blister foils. The printing was done using two different rotogravure printing machines for aluminium foils[5] (P_1 and P_2). After printing, all regular patterns were captured using an USB-microscope[6] with $\times 5$ magnification.
The digital pattern is defined by a grid to be printed at 178 lpi (lines per inch). In the experiments we investigated only a 6×6 part of the whole grid (which takes up to an area of 1 cm^2 after printing). After the USB-microscope capturing process, the size of the analyzed images is 432×452 pixels. The database created consists of samples printed using two presses (P_1 and P_2) and two engraved cylinders (C_1 and C_2).

[5]Suddha Group rotogravure printing machines for aluminium foils: https://www.suddhagroup.com/rotogravure-printing-machine.html
[6]Bodelin Proscope Microscope

Such variability of samples is needed in order to cover the following situations:

- images printed using variable presses but with the same cylinder (P_1C_2 vs P_2C_2) - the attacker has access to the authentic cylinder. This situation is not realistic;
- images printed using the same press but with variable cylinders (P_1C_1 vs P_1C_2) - the attacker has access to the authentic press. This situation is also not realistic;
- images printed using variable presses and cylinders (P_1C_1 vs P_2C_2) - the attacker does not have access both to the authentic cylinder and to the authentic press. It is the most realistic case.

It is important to investigate all these situations, even if some are not realistic, in order to evaluate the accuracy of the methods proposed from a statistical and analytical point of view. The database consists of 300 samples for each chemically engraved cylinder and press i.e. 900 samples in total as detailed in Table I. Thanks to the stochastic nature of chemical etching and rotogravure printing process, we can assume that the data set size is statistically sufficient to draw first conclusions about the efficiency of the proposed authentication systems.

	E_1	E_2	E_3	E_4	E_5	E_6
P_1C_1	50	50	50	50	50	50
P_1C_2	50	50	50	50	50	50
P_2C_2	50	50	50	50	50	50

TABLE I
DESCRIPTION OF OUR DATABASE WITH DIFFERENT COMBINATIONS OF CYLINDERS AND PRESSES USED FOR TESTS.

This database was used for all experiments presented in the following sections. For signature investigations in Section V-B, a small random sub-set of images was used. For cylinder and press identification experiments (presented in Section V-C), we randomly chose 18 regular test patterns (one per class) for training and the rest of data set was used for tests. For authentication experiments (discussed in Section V-D), the training data set contains $m = 5$ or $m = 10$ random samples of regular test pattern in each position $E_i, i = 1, \cdots, 6$, for the construction of the model M. The test data set contains 45 or 40 random regular test patterns from each position $E_i, i = 1, \cdots, 6$. The train and test data sets are independent. The experimental results presented in Section V-C and in Section V-D show the mean values obtained after five tests, i.e. the training and testing stages were performed five times using randomly permuted data.

B. Printing signatures

As reported in Section III, the rotogravure printing process consists of engraving process and printing process. It was shown in [39] that the printing signature consists of cylinder signature and press signature and that the cylinder signature impacts more the printed images than the press signature.
We propose to use the t-SNE method (T-distributed Stochastic Neighbor Embedding) [21] to separate the data in clusters, in order to show the impact of each signature. The t-SNE method consists to embed high-dimensional points in low dimensions in a way that respects similarities between points. In our case the input data are of 432x452 dimensions. Nearby points in the high-dimensional input space correspond to nearby embedded low-dimensional points. On the other hand, distant points in the high-dimensional input space correspond to distant embedded low-dimensional points. In Fig. 7 - Fig. 9 the low-dimensional space is of dimension two. The output dimensions of the t-SNE method are dependent of the input data processed. For these experiments, we have used the MATLAB t-SNE implementation[7] with City block distance and previous PCA dimension reduction to 50 components for better visualization. The axes of Fig. 7 - Fig. 10 correspond to 2-D embedding of our high-dimensional data, meanwhile the axes of Fig. 11 correspond to 3-D embedding of our data.
In a first experiment, we fixed the engraved cylinder (C_2) and used two presses (P_1 and P_2) for printing the samples (Fig. 7). The first experiment shows us whether the signature of press affects the quality of printed patterns. We clearly see in Fig. 7 that 50% of the clusters are fused. This confirms the conclusion from [39] that the signature of press impacts less the printed patterns than the signature of cylinder.

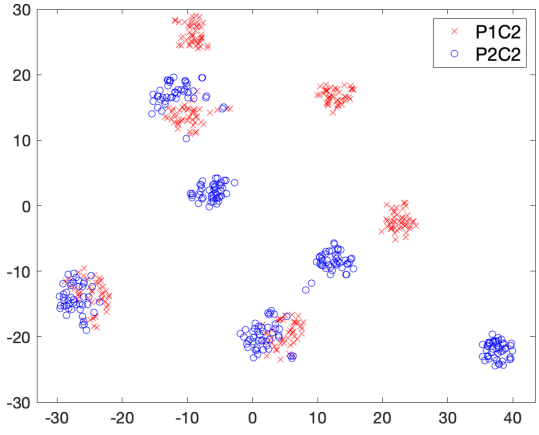


Fig. 7. Impact of press signature. Comparison of samples printed using the same engraved cylinder (C_2) but using two presses (P_1 and P_2). For each cylinder there is six clusters, one for each regular pattern position. Clusters highlighted in red (resp. blue) belongs to the class P_1C_2 (resp. P_2C_2).

In a second experiment, we fixed the press (P_1) and used two engraved cylinders (C_1 and C_2) for printing the samples (Fig. 8). This experiment shows us whether the signature of cylinder is more important than the signature of press. Oppositely to Fig. 7, in Fig. 8 the clusters are well separated, this confirms the importance of cylinder signature.
Finally, in a third experiment, we used two presses (P_1 and P_2) and two engraved cylinders (C_1 and C_2) for printing the samples (Fig. 9). This experiment is similar to the case of a real attack, when the authority center uses the press P_1 and the authentic cylinder C_1, meanwhile an attacker uses the press P_2 and the counterfeited cylinder C_2. In this case, the clusters are also well separated (see Fig. 9), that demonstrates that it is possible to identify the samples printed by a counterfeiter.

[7]MATLAB t-SNE implementation: https://fr.mathworks.com/help/stats/tsne.html

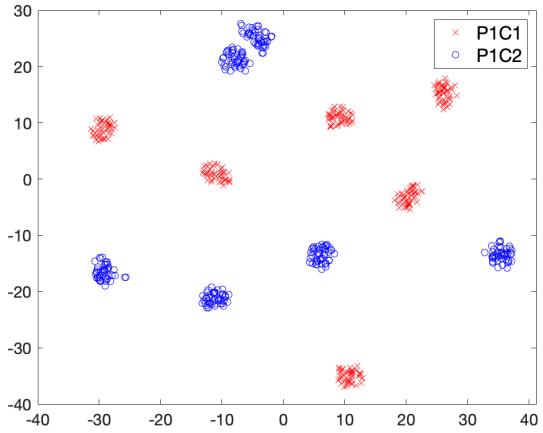


Fig. 8. Impact of cylinder signature. Comparison of samples printed using two engraved cylinders (C_1 and C_2) and one press (P_1). or each cylinder there is six clusters, one for each regular pattern position. Clusters highlighted in red (resp. blue) belongs to the class P_1C_1 (resp. P_1C_2).

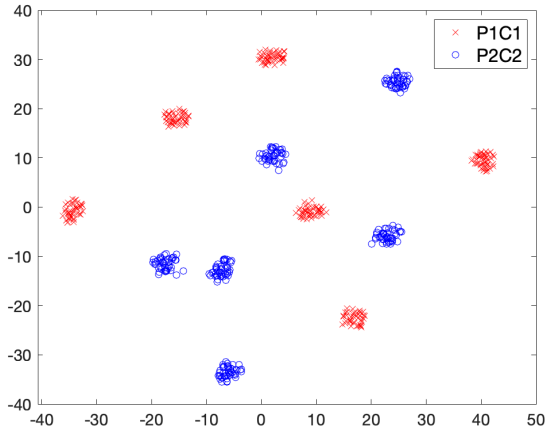


Fig. 9. Impact of cylinder and press signatures. Comparison of samples printed using two engraved cylinders (C_1 and C_2) and two presses (P_1 and P_2). or each cylinder there is six clusters, one for each regular pattern position. Clusters highlighted in red (resp. blue) belongs to the class P_1C_1 (resp. P_2C_2).

It could be noted from Fig. 7 - Fig. 9 that every time the t-SNE can easily separate the data of each class (printing configuration) in 6 clusters. From this observation, we can conclude that the position of the image in the cylinder has to be also taken into account and that we can identify not only the cylinder used but also the position on the cylinder used to print the regular pattern E. We illustrate in Fig. 10 the t-SNE plot of regular pattern images E_1 and E_2 that come from the database P_1C_1. We will take into account this property for the authentication process as it could improve separation results between authentic and fake regular patterns.

We showed in Fig. 8 and Fig. 9 that it is possible to separate the two groups of six clusters with two dimensions only. On the other hand with two dimensions we cannot separate the two groups of six clusters shown in Fig. 7. We tried to increase the dimension of the output space and we did not succeed to separate the two groups of six clusters with three dimensions (see Fig. 11). This confirms our assumption that the impact of the press signature is presented but less significant than the impact of the cylinder signature.

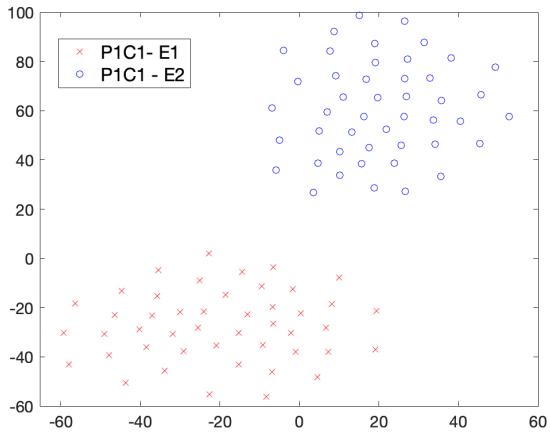


Fig. 10. The two clusters (highlighted in red and blue) represent the same test pattern E engraved in different positions on the same cylinder (C_1) and printed with the same press (P_1).

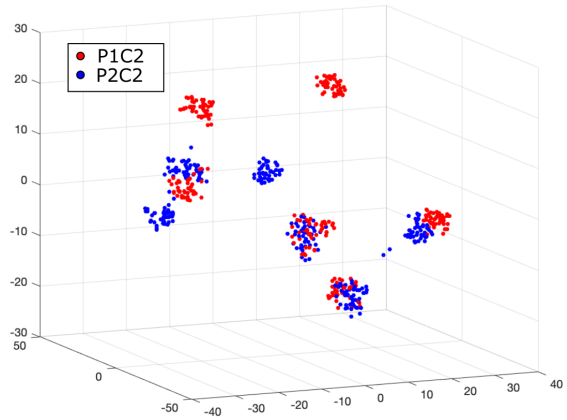


Fig. 11. Impact of press signature in 3D visualization. Comparison of samples printed using the same engraved cylinder (C_2) but using two presses (P_1 and P_2). For each cylinder there is six clusters, one for each regular pattern position. Clusters highlighted in red (resp. blue) belongs to the class P_1C_2 (resp. P_2C_2).

C. Cylinder identification

Based on the visualization results presented in the previous section, we propose to perform the cylinder identification with one of the following methods using only one random regular test patter per class as a class reference image.

Image processing approach - Maximization of Pearson correlation. The confusion matrix of printer identification is presented in Table II. This Table shows that in each case the cylinder is correctly identified, but due to the small impact

Predicted		Actual P_1C_1						P_1C_2						P_2C_2					
		E_1	E_2	E_3	E_4	E_5	E_6	E_1	E_2	E_3	E_4	E_5	E_6	E_1	E_2	E_3	E_4	E_5	E_6
P_1C_1	E_1	**100**																	
	E_2		**100**																
	E_3			**100**															
	E_4				**100**														
	E_5					**100**													
	E_6						**100**												
P_1C_2	E_1							**44.35**						31.11					
	E_2								**70.22**						15.22				
	E_3									**89.13**									1.74
	E_4										**99.56**								
	E_5											**92.61**						9.33	
	E_6												**62.67**			8.44			10.43
P_2C_2	E_1							55.65						**68.89**					
	E_2								29.78						**84.78**			10.22	
	E_3												2.67			**91.56**			
	E_4										0.44						**100**		
	E_5											7.39						**80.44**	
	E_6									10.87			34.67						**87.83**

TABLE II

CONFUSION MATRIX OF CORRELATION VALUE BASED CYLINDER IDENTIFICATIONS COMPUTED USING ONE RANDOM SAMPLE PER POSITION OF REGULAR TEST PATTERN (GROUNDTRUTH ACCORDING THE COLUMNS), IN PERCENTAGES. RIGHT AND WRONG MEAN CLASSIFICATIONS PER CYLINDER AFTER 5 CROSS-VALIDATIONS.

of the press signature on the printed pattern, sometimes we cannot identify the press correctly.

Remarque: We also tested the Spearman correlation as it gives better results for some copy sensitive graphical codes [36]. In the case of the proposed regular test pattern, the Spearman correlation gives worst results for printer identification and authentication.

Machine learning approach - Use of NNLS (Non-Negative Least Squares) sparse coding classifier [19], [18]. We used the Sparse Representation Toolbox of MATLAB version 1.9 that is publicly available[8]. The classification results are presented in confusion matrix Table III. Results shown in tis table are comparable to those shown in Table II.

These experimental results show that the use of only one sample per class can efficiently separate the samples to the correct classes and almost with 100% accuracy identify the cylinder used for printing the regular test pattern.

D. Authentication using a proposed regular test pattern

For authentication experiments, the samples printed using the press P_1 and the cylinder C_1 were considered as authentic, meanwhile the samples printed using presses P_1 and P_2 with the cylinder C_2 were considered as fake packaging.

IP metric based approach. In a first authentication experiment, we compare the Pearson correlation values between the templates (regular patterns $E_i, i = 1, \cdots, 6$ collected during the printing process) and all other samples of our database. The authentication was done by comparing these correlation values with a threshold set experimentally with a small validation set. Experimentally, we found that for our database the optimal authentication threshold is $Th = 0.7$. The distributions of the correlation values illustrated in Fig. 12 and the Table IV show that the Pearson correlation works well to separate the authentic and fake regular test patterns.

For cross validation, we have performed the same authentication test five times with random permutation of train (one random image) and test (45 images per class) data sets. In addition, we have enlarged the train data set in IP metric based approach in order to slightly improve the authentication results. We have used also $m = 5$ and $m = 10$ samples for each class during calculation of correlation values. Authentication test was done choosing the maximal correlation value among all regular test patterns used for authentication. The obtained results are evaluated using TPR (True Positive Rate), TNR (True Negative Rate) and precision in Table V. We can conclude from this table that the best authentication is obtained when $Th = 0.7$: it enables us to reject almost all fakes, and accept all authentic samples. Nevertheless, from the health care point of view, it is better to chose the $Th > 0.7$ to reject all fake samples. These experimental results also show us that the use of five or ten samples per class can improve the accuracy of this approach.

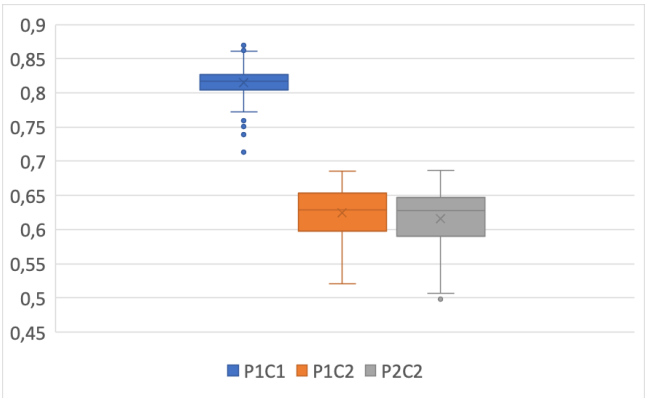


Fig. 12. Authentication of regular patterns using the distribution of Pearson correlation values. Mean values for five tests using one randomly selected regular test pattern as a template. An authentication threshold Th of 0.71 enables to separate authentic (P_1C_1) from fake (P_1C_2, P_2C_2) patterns.

This authentication enables us to state that the classical Pearson correlation can be used for the authentication of a regular test pattern E, as well as for the identification of the part of cylinder used for printing this pattern.

[8]Sparse Representation Toolbox in MATLAB version 1.9 https://sites.google.com/site/sparsereptool/

Predicted		Actual P_1C_1						P_1C_2						P_2C_2					
		E_1	E_2	E_3	E_4	E_5	E_6	E_1	E_2	E_3	E_4	E_5	E_6	E_1	E_2	E_3	E_4	E_5	E_6
P_1C_1	E_1	**100**																	
	E_2		**100**									0.43							0.43
	E_3			**100**															
	E_4				**100**													0.44	
	E_5					**100**													
	E_6						**100**												0.43
P_1C_2	E_1							**50.43**			0.44			27.11					
	E_2								**73.78**						16.52				
	E_3									**94.35**									3.48
	E_4										**93.33**								
	E_5											**95.22**						10.67	
	E_6									1.30	1.33	0.43	**57.33**			3.11		0.44	10
P_2C_2	E_1							49.57						**72.89**					
	E_2								26.22						**83.48**			4.89	0
	E_3												1.33			**96.44**			
	E_4									0.43	4.89		0.44				**100**	0.44	1.30
	E_5											3.91	0.44			0.44		**83.11**	
	E_6									3.91			40.44						**84.35**

TABLE III

CONFUSION MATRIX OF NNLS BASED CYLINDER IDENTIFICATIONS COMPUTED USING ONE RANDOM SAMPLE PER POSITION OF REGULAR TEST PATTERN (GROUNDTRUTH ACCORDING THE COLUMNS), IN PERCENTAGES. RIGHT AND WRONG MEAN CLASSIFICATIONS PER CYLINDER AFTER 5 CROSS-VALIDATIONS.

	P_1C_1	P_1C_2	P_2C_2
Mean value	**0.82**	0.62	0.62
Min value	**0.71**	0.52	0.50
Max value	**0.87**	0.69	0.69

TABLE IV

MEAN PEARSON CORRELATION VALUES RESULTING FROM THE AUTHENTICATION TEST PERFORMED FIVE TIMES WITH RANDOM PERMUTATION OF TRAIN (ONE RANDOM IMAGE) AND TEST (45 IMAGES PER CLASS) DATA SETS.

		Threshold				
		0.8	0.7	0.6	0.5	0.4
$m=1$	TPR	0.73	**0.997**	1	1	1
	FPR	0	0.001	0.73	0.99	1
	Precision	1	0.999	0.41	0.34	0.34
$m=5$	TPR	0.96	**1**	1	1	1
	FPR	0	0.004	0.82	1	1
	Precision	1	0.99	0.38	0.33	0.33
$m=10$	TPR	0.98	**1**	1	1	1
	FPR	0	0.01	0.84	1	1
	Precision	1	0.98	0.37	0.33	0.33

TABLE V

MEAN CLASSIFICATION ACCURACY METRICS WHILE USING IP APPROACH (PEARSON CORRELATION) FOR AUTHENTICATION. TRAINING DATA SET CONTAINS OF $m = 1, 5, 10$ SAMPLES PER CLASS (I.E. TRAINING DATA SET CONTAINS $6, 30$ OR 60 REGULAR TEST PATTERNS AS A REFERENCE).

Nevertheless, the authentication solution based on correlation can sometimes lead to bad results, as the determination of the authentication threshold is done experimentally. To cope with this limitation, we propose to use a state-of-the-art machine learning method to improve the separation between authentic and fake images.

Machine learning based approach. In a second authentication experiment, we use the NNLS classifier presented in Section IV-D. The use of $m = 5$ images per class $E_i, i = 1, \cdots, 6$ offers a good separation between the original regular test patterns (printed using cylinder C_1 and press P_1) and fake regular test patterns (printed using cylinder C_2 with presses P_1 and P_2), see Fig. 13. For this experiment, the number of train samples is $6 \times 5 = 30$ and the number of test samples is $6 \times 45 = 270$.

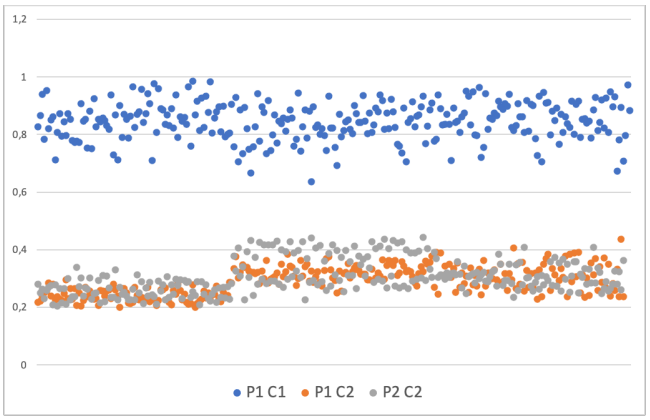


Fig. 13. Distribution of coefficients obtained using the NNLS classifier with 5 samples per class. All authentic samples (blue points) have higher coefficients in comparison with fakes (orange and gray points).

As expected, the training of the classifier with a bigger number of samples gives better classification results. As example, the results using $m = 10$ samples per class are illustrated in Fig. 14. For this experiment, the number of train samples is $6 \times 10 = 60$ and the number of test samples is $6 \times 40 = 240$. In our study case, we do not need to use more than 10 samples per class, as with this number the separation between the two distributions (authentic vs fakes) is already very good.

The results presented in Fig. 13 and Fig. 14 illustrate a very good separation between authentic and fake samples. This kind of results can be obtained while the training data sets are carefully checked and all samples have a good image quality after printing and capturing processes. It is possible to obtain such a database in a real world scenario, as the medicine authentication system should surely be well calibrated.

Nevertheless, we have tested the proposed authentication system while using the random separation of samples into training and testing data sets. The mean classification accuracy metrics are presented in Table VI. We can note that the results are still good, even if random images were used for training. The

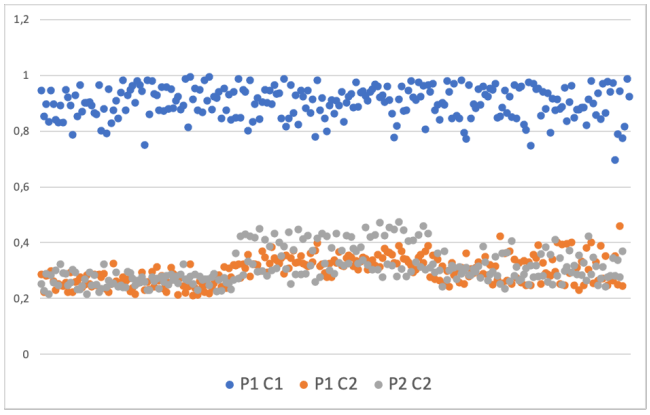


Fig. 14. Distribution of coefficients obtained using the NNLS classifier with 10 samples per class. All authentic samples (blue points) have higher coefficients in comparison with fakes (orange and gray points).

		Threshold				
		0.8	0.7	0.6	0.5	0.4
$m = 5$	TPR	0.72	0.95	**0.99**	0.997	0.999
	FPR	0	0	0	0.01	0.12
	Precision	1	1	1	0.99	0.81
$m = 10$	TPR	0.89	0.98	**0.996**	1	1
	FPR	0	0	0	0.01	0.12
	Precision	1	1	1	0.995	0.80

TABLE VI
MEAN CLASSIFICATION ACCURACY METRICS WHILE USING ML APPROACH (NNLS CLASSIFIER) FOR AUTHENTICATION. TRAINING DATA SET CONTAINS OF $m = 5, 10$ SAMPLES PER CLASS (I.E. TRAINING DATA SET CONTAINS 30 OR 60 RANDOM REGULAR TEST PATTERNS).

threshold $Th = 0.6$ allows us to reject all the fake samples and accept almost all authentic samples.

In this section we have shown that both IP and ML based approaches give good results for authentication of blister foils using the proposed regular test pattern. In addition we have demonstrated, thanks to uniqueness of the engraving process, that we can correctly identify the position of the pattern on the cylinder used for printing. Lastly, we also showed that the samples regular test pattern printed using another cylinder (fake samples) can be easily rejected using both approaches.

E. Impact of printing support to authentication

In order to study the impact of printing support to the suggested authentication system, the proposed regular test pattern was printed on two types of aluminium blister foils having different thickness. The thicker foil is called strip (letter 's' in the figures) and the thinner one is called blister (letter 'b' in the figures). We collected the same number of samples printed on strip and on blister, see details in Table VII.

	E_1	E_2	E_3	E_4	E_5	E_6
P_1C_1s	50	50	50	50	50	50
P_1C_2s	50	50	50	50	50	50
P_1C_1b	50	50	50	50	50	50
P_2C_1b	50	50	50	50	50	50

TABLE VII
DESCRIPTION OF OUR DATABASE USED TO STUDY THE IMPACT OF PRINTING SUPPORT TO AUTHENTICATION.

For authentication, we have used the image processing approach by evaluating the Pearson correlation values. For first experiment, the authentic samples were printed using the press P_1 and the cylinder C_2 on strip support (called P_1C_2s in Fig. 15). The distribution of correlation values is illustrated in Fig. 15. We note that all fake samples have correlation values smaller than 0.7 (the threshold defined in the experiment presented in Fig. 12), thus none of them will be accepted as an authentic packaging. Nevertheless, there are few authentic regular test patterns that have a correlation value smaller than the authentication threshold. This is due to the poor quality of these samples. Therefore, it is important to ensure the printing quality control while preparing the packaging.

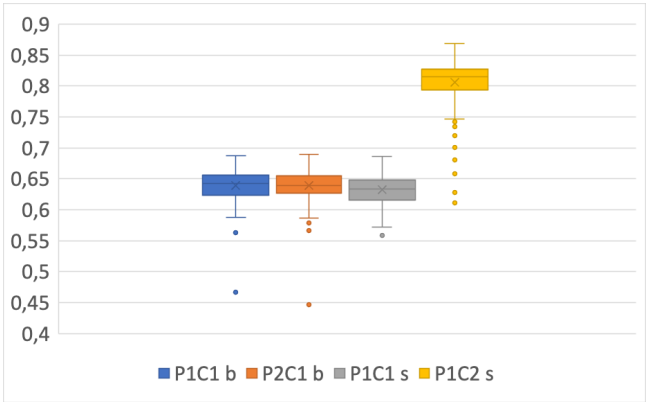


Fig. 15. Authentication of regular test patterns using Pearson correlation. An authentication threshold Th of 0.7 enables to reject all fakes printed on blister (P_1C_1b and P_2C_1b) and on strip (P_1C_1s).

In the second experiment, the authentic samples were printed using press P_1 and cylinder C_1 on strip support (called P_1C_1s) and the fakes were printed using presses P_1 and P_2 and cylinder C_1 on blister. The distribution of correlation values is illustrated in Fig. 16. We note that the separation of authentic and fake samples in this case is not obvious as the signature of engraving process impacts more than the signature of press and of printing support used.

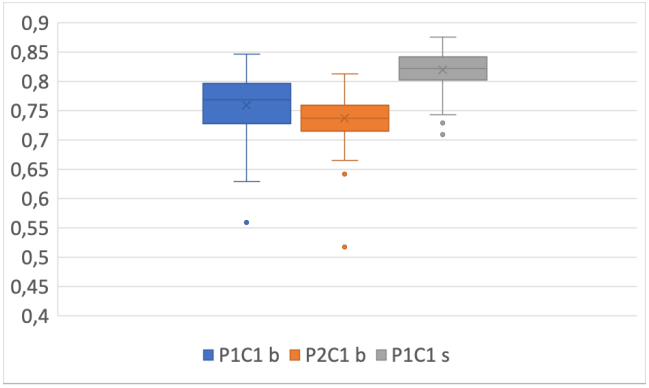


Fig. 16. Authentication of regular test patterns using Pearson correlation. The correlation values of authentic samples printed on strip (P_1C_1s) do not differ a lot from the correlation values of fakes printed on blister (P_1C_1b and P_2C_1b).

The results of this section confirm the conclusion that the signature of the engraving process is the most important. If

a counterfeiter has access to the authentic cylinder, s/he can produce easily acceptable fakes even if the printing support material is not of the same type.

VI. Discussion

In this section, we shortly discuss: 1) the possibility to attack the proposed authentication system and 2) the possibility to extend the proposed authentication system to another engraving processes.

A. Attacks

Taking into account the results presented in Section V, we can conclude that the chemical etching has several unclonable characteristics. Thus, even if an opponent can correctly estimate an authentic artwork W (or even has access to an original artwork W), it will not be really possible to print exactly the same patterns. Therefore, the result will be the same as for duplicating the authentic printing process and for trying pass the authentication test. The unique possibility for fake packaging production is to use the authentic cylinder (see Fig. 16).

Furthermore, packaging protection is in practice obtained from a set of security feature elements. Thus, in case of any doubt, all the corresponding security feature elements would be verified. The use of the proposed regular test pattern can help not only to detect counterfeited packaging but also to identify the cylinder used for its printing as a proof of commitment.

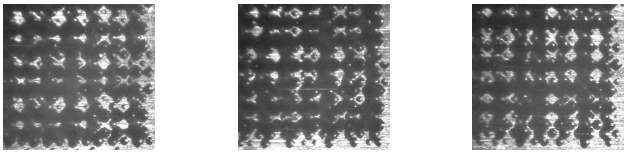
The proposed authentication system has two important constraints that have to be taken into account. First one is the control of the printing process: the printed parameters must be constant all the time. Second one is that the printed samples have to be of good quality. This constraint relates to the first one, as the controllable printing process should produce samples of good quality.

B. Impact of the engraving process in the authentication process

As discussed before, the chemical etching provides unclonable characteristics due to the stochastic nature of chemical reactions [17]. It would be interesting to make also tests with electro-mechanical and laser engraving.

In the case of electro-mechanical engraving, the size and shape of cells are controlled by a program and by a stylus form, respectively. Nevertheless, the observation of some samples printed using electro-mechanically engraved cylinder (see Fig. 17) shows us that the alignment and the size of dots are still variable. Intuitively, this variability could also be used for authentication. Nevertheless, the authentication method used should be adapted as the global methods tested (using Pearson correlation or classification of whole image) did not give us good results.

While observing the images of a regular test pattern from Fig. 17, one can note the small local variation of hole shapes (light zones in the images). The first experiments based on the local authentication of sub-parts of regular pattern give us promising results. We can successfully identify the regular pattern position on the cylinder and make the distinction between the samples obtained using electro-mechanical engraving and chemical etching.



(a) (b) (c)

Fig. 17. An illustration of proposed regular pattern E on the cylinder engraved using electro-mechanical technology a) in position E_1 b) in position E_3, and c) in position E_6.

In the near future, we would like to end our experiments with local authentication methods and study samples obtained using a cylinder engraved by a laser. We suppose that the variability of dots shapes should be minimal thanks to the high precision of lasers, but it should be possible in this case to identify the press and the supports that were used for packaging printing.

VII. Conclusion

For a long time the protection of foils is an important issue, especially in medicine. Most of the packaging for cheap and medium market medicines are printed on blister foils using rotogravure process. The majority of existing printing security feature elements are not adapted for such a printing process and support. Therefore, it is important to find novel solution for these packaging.

In this paper, we have proposed an authentication system based on a novel regular test pattern. This authentication system is based on the stochastic nature of chemical etching which is mainly used for cylinder engraving. The experiment results showed that the uniqueness of the chemical etching signature enables: to authenticate the packaging, to identify the cylinder used for printing, and even to identify the exact position of the security regular test pattern on the authentic engraved cylinder. The identification as well as the authentication processes were done using an image processing approach based on a correlation measure and using a machine learning approach based on non-negative least squares.

In the future, we will explore the possibility to use the same regular test pattern for cylinders engraved using electro-mechnical or laser methods. We would also like to improve the authentication results by analyzing independently each hole in the regular test pattern and by using some novel neural network approaches which do not need lots of data for training. Finally, it is important to study the usability of this authentication system on other printing technologies used in packaging production as offset printing or laser printing.

Acknowledgements

This work was partially funded by the project *PackMark* supported by the Indo-French Center for the Promotion of Advanced Research (IFCPAR) under contract IFCPAR-7127. All the printed samples were provided by Sergusa Solutions Pvt Ltd.

REFERENCES

[1] R. Chaban, O. Taran, J. Tutt, T. Holotyak, S. Bonev, and S. Voloshynovskiy. Machine learning attack on copy detection patterns: are 1×1 patterns cloneable? In *2021 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6. IEEE, 2021.

[2] P-J. Chiang, N. Khanna, A. K Mikkilineni, M. V O Segovia, J. P Allebach, G TC Chiu, and E J Delp. Printer and scanner forensics: models and methods. In *Intelligent Multimedia Analysis for Security Applications*, pages 145–187. Springer, 2010.

[3] I. Das, S. Bandyopadhyay, and A. Trémeau. Characterization of prints based on microscale image analysis of dot patterns. *Applied Sciences*, 11(14):6634, 2021.

[4] M. Davison. *Pharmaceutical anti-counterfeiting: combating the real danger from fake drugs*. John Wiley & Sons, 2011.

[5] 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.

[6] A. Ferreira, N. Purnekar, and M. Barni. Ensembling shallow siamese neural network architectures for printed documents verification in data-scarcity scenarios. *IEEE Access*, 9:133924–133939, 2021.

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

[8] R. N. Goldman. Non-counterfeitable document system, December 18 1984. US Patent 4,489,318.

[9] R. N. Goldman. Non-counterfeitable document system, October 8 1985. US Patent 4,546,352.

[10] R. N. Goldman. Non-counterfeitable document system, November 15 1988. US Patent 4,785,290.

[11] R. Hamzehyan, F. Razzazi, and A. Behrad. Printer source identification by feature modeling in the total variable printer space. *Journal of Forensic Sciences*, 66(6):2261–2273, 2021.

[12] 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.

[13] A. Kader and M. Ezzat. The impact of ink viscosity on the enhancement of rotogravure optical print quality. *International Design Journal*, 7(1):103–107, 2017.

[14] N. Khanna and E. J Delp. Source scanner identification for scanned documents. In *Information Forensics and Security, 2009. WIFS 2009. First IEEE International Workshop on*, pages 166–170. IEEE, 2009.

[15] N. Khanna, A. K Mikkilineni, and E. J Delp. Scanner identification using feature-based processing and analysis. *IEEE Transactions on Information Forensics and Security*, 4(1):123–139, 2009.

[16] E. Khermaza, I. Tkachenko, and J. Picard. Can copy detection patterns be copied? evaluating the performance of attacks and highlighting the role of the detector. In *2021 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6. IEEE, 2021.

[17] H. Kipphan. *Handbook of print media: technologies and production methods*. Springer Science & Business Media, 2001.

[18] Y. Li and A. Ngom. Classification approach based on non-negative least squares. *Neurocomputing*, 118:41–57, 2013.

[19] Y. Li and A. Ngom. Nonnegative least-squares methods for the classification of high-dimensional biological data. *IEEE/ACM transactions on computational biology and bioinformatics*, 10(2):447–456, 2013.

[20] X. Lv, C. Liu, Y. Wu, and H. Ipsen. Variation of gravure printing characteristic curves. In *17th IAPRI World Conference on Packaging*, 2010.

[21] L. van der Maaten and G. Hinton. Visualizing data using t-sne. *Journal of machine learning research*, 9(Nov):2579–2605, 2008.

[22] J. Mayer, P. VK Borges, and S. J Simske. *Fundamentals and Applications of Hardcopy Communication: Conveying Side Information by Printed Media*. Springer, 2018.

[23] A. K Mikkilineni, N. Khanna, and E. J Delp. Texture based attacks on intrinsic signature based printer identification. In *Media Forensics and Security II*, volume 7541, page 75410T. International Society for Optics and Photonics, 2010.

[24] A. K Mikkilineni, N. Khanna, and E. J Delp. Forensic printer detection using intrinsic signatures. In *Media Watermarking, Security, and Forensics III*, volume 7880, page 78800R. International Society for Optics and Photonics, 2011.

[25] L. C Navarro, A. KW Navarro, A. Rocha, and R. Dahab. Connecting the dots: Toward accountable machine-learning printer attribution methods. *Journal of Visual Communication and Image Representation*, 53:257–272, 2018.

[26] 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 *Signal and Information Processing (GlobalSIP), 2017 IEEE Global Conference on*, pages 288–292. IEEE, 2017.

[27] Q.-T. Nguyen, A. Mai, L. Chagas, and N. Reverdy-Bruas. Microscopic printing analysis and application for classification of source printer. *Computers & Security*, 108:102320, 2021.

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

[29] J. Picard, Z. Sagan, A. Foucou, and J-P. Massicot. Method and device for authenticating geometrical codes, May 20 2014. US Patent 8,727,222.

[30] J. Picard and J. Zhao. Techniques for detecting, analyzing, and using visible authentication patterns, May 3 2011. US Patent 7,937,588.

[31] 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.

[32] R. Schraml, L. Debiasi, C. Kauba, and A. Uhl. On the feasibility of classification-based product package authentication. In *Information Forensics and Security (WIFS), 2017 IEEE Workshop on*, pages 1–6. IEEE, 2017.

[33] 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.

[34] S. Shang, N. Memon, and X. Kong. Detecting documents forged by printing and copying. *EURASIP Journal on Advances in Signal Processing*, 2014(1):140, 2014.

[35] O. Taran, J. Tutt, T. Holotyak, R. Chaban, S. Bonev, and S. Voloshynovskiy. Mobile authentication of copy detection patterns: how critical is to know fakes? In *2021 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6. IEEE, 2021.

[36] I. Tkachenko, C. Destruel, O. Strauss, and W. Puech. Sensitivity of different correlation measures to print-and-scan process. *Electronic Imaging*, 2017.

[37] 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.

[38] I. Tkachenko, A. Trémeau, and T. Fournel. Authentication of medicine blister foils: Characterization of the rotogravure printing process. In *International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*, 2018.

[39] I. Tkachenko, A. Tremeau, and T. Fournel. Fighting against medicine packaging counterfeits: rotogravure press vs cylinder signatures. In *2020 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6. IEEE, 2020.

[40] R. L. Van Renesse. *Optical document security. Third edition*. Artech House optoelectronics library, 2005.

[41] C-W. Wong and M. Wu. Counterfeit detection using paper PUF and mobile cameras. In *Information Forensics and Security (WIFS), 2015 IEEE International Workshop on*, pages 1–6. IEEE, 2015.

[42] 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.

[43] 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.

[44] 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.