Authentication of Holograms with Mixed Patterns by Direct LBP Comparison

Marie-Neige Chapel

L3i, La Rochelle University

La Rochelle, France

https://orcid.org/0000-0002-6754-9896

Musab Al-Ghadi L3i, La Rochelle University La Rochelle, France musab.alghadi@univ-lr.fr Jean-Christophe Burie

L3i, La Rochelle University

La Rochelle, France
jean-christophe.burie@univ-lr.fr

Abstract—In order to combat fraud, identity documents and currencies often include security elements such as guilloches, micro prints or holograms. This paper aims to authenticate such documents from videos acquired with a smartphone by analyzing the holograms. The proposed method consists of recognizing all the patterns of the hologram to determine if the document is genuine or not. The Local Binary Patterns (LBP) descriptor is used in this paper to represent the features of a hologram. For a given document, Multi LBP Models are built as a reference model. This model is then compared to the LBP models of the tested hologram to decide if the hologram exist or not in the document and then to determine if the document is genuine or not. Experiments are carried out on holograms of French Passports and Euro banknotes. The results show that the proposed strategy allows to determine if the document is an authentic document or falsified in a good accuracy. The code is available at https://github.com/mnchapel/authentication_ of_holograms_with_mixed_patterns_by_direct_lbp_comparison.

 ${\it Index\ Terms} \hbox{--} \hbox{authentication, recognition, hologram, local binary pattern}$

I. INTRODUCTION

With the digital transformation of the society, many companies propose now to their consumers digital services accessible with mobile devices such as smartphones. Some of these digital services require user identity authentication during the registration process. The enrollment requires providing an identity document (ID) such as identity card, passport, driving license to ensure the user's legitimacy.

The user takes a self-picture or records a short video of his ID, which is then processed manually offline by a human operator or automatically by a dedicated algorithm. The task of this algorithm is to determine the identity of the user by extracting some information such as the first name, the surname or even the picture. For some systems, these data are not sufficient to ensure the identity of the user. Indeed, fraudsters can create a fake ID document with false information. To combat any forgery style, several security elements such as guilloches, micro prints and holograms have been integrated in the IDs. These elements make it difficult, if not impossible, to produce counterfeit or fake IDs.

The hologram is defined as a visual object that represents a range of visual patterns. These patterns are important features

This work is part of the IDECYS project (n° DOS0098984/00) supported by BPI France in the Framework of the FUI AAP25 program.

to confirm the authenticity of a given ID and may be achieved directly by checking the similarity of the hologram patterns in the foreground of an ID to the hologram patterns of an authentic version of the same country.

In this paper, we propose a new hologram detection model for ID authentication. The model is based on LBP descriptor [1] to represent the features of the hologram patterns. Indeed, different types of holograms exist: 2D holograms with structural and color changes; 3D holograms with images, holograms with kinematic effects, etc. In our work, we consider the holograms with several patterns that are visible when rotating and tilting the document and therefore depending on the point of view and lighting conditions. This is why a video is required, as input, to be able to catch the different patterns.

In the context of our study, the acquisition of this video is done by the user in an indoor environment. However, the acquisition conditions are not controlled. Lighting conditions can be variable according to the presence of direct lights or windows. Moreover, the movements of the documents to make the patterns of the hologram appear are not imposed. The user is free to rotate and tilt the document as he/she wants.

The rest of the paper is organized as follows. Section 2 presents the methods in the literature dealing with hologram authentication. Then section 3 details the proposed approach. The dataset and the evaluation of the proposed method are presented in section 4 and section 5 respectively. Finally, the conclusion and the perspectives are given in section 6.

II. RELATED WORK

In this section, we explore some of the most relevant stateof-the-art works in fraud detection for ID authentication.

In 2014, Hartl et al. [2] proposed an approach to detect holograms based on their principal attribute: appearance variation. Several images of the document are first registered together and used to create a stack. An appearance error is then computed for each corresponding pixel of the stack. A high error indicates the presence of a hologram. The detection of a hologram is not sufficient to attest that the document is genuine. It is necessary to verify that the hologram detected is the one expected.

In order to obtain all the patterns to authenticate a hologram, several approaches rely on images taken by a device with LEDs arranged inside a hemisphere to have different angles of incidence on the document. In a first work, Kwon and Park [3] proposed a pattern matching in the frequency domain taken by a hemisphere. Later, the authors improved their method [4] to handle rotation of the hologram by estimating the angle by edge tracking and realign it in the frequency domain. Later, Hartl et al. [5] used images taken on a hemisphere and use them as reference images for the authentication. To compare an image with the reference set, the user has to retrieve the position of the shot with the hemisphere, i.e., the same incident angle between the light, the document and the observer. To do so, the authors have also realized a substantial work on a system to guide the user with augmented reality [6] [2] [7] [5]. Soukup et al. [8] used the hemisphere to first analyze the hologram. From this, the authors have proposed two descriptors to discriminate the genuine hologram from the fake ones. The method was then tested on holograms with common perturbations, like crease or shift and tilt, to demonstrate its robustness [9]. Later, the essential appearance properties captured by a Convolution Neural Network (CNN) was proposed by Soukup et al. [10]. In addition, the authors also proposed a portable ring-light module that can be mounted on a smartphone to avoid the use of the hemisphere.

The use of specific devices cannot be considered for our application. To capture the holograms, we can only rely on a device owned by the majority of the population: a smartphone. This is what Kada et al. [11] recently proposed. In each frame of the video, pixels are selected based on specific properties such as saturation, value, shape, and hues. This selection process helps identify the potential holographic regions within the document. Then, parts of the hologram are extracted from each frame and accumulated to reconstruct the complete the hologram. Their method extracts the hologram if it exists, but does not verify if it is the expected one.

In the next section, we present an approach that uses video captured in an environment similar to that of the end-user, i.e., indoor with lights and windows, with a smartphone to compute a reference model of the hologram to be authenticated.

III. PROPOSED METHOD

The proposed method in this paper is based on the LBP, a visual descriptor used for classification, first introduced by Ojala et al. [1]. We choose the LBP as feature for its robustness against illumination variation, since the shots will be taken in a semi-constraint environment. Several approaches combine LBP feature with histograms, like in face recognition [12] and background subtraction [13]. But, as explained by Yang and Chen [14] in their study, the use of histogram does not keep the spatial consistency of the subject, a fundamental characteristic for the shape recognition. For this reason, we choose to directly compare the binary code of the LBP features between a reference model and an image to test. Furthermore, since the size of the images is less than 100×100 the comparison can be performed in real time.

We propose to recognize all the patterns of a hologram independently and merge the results obtained to authenticate

or not the hologram. Fig. 1 presents the patterns to recognize for one hologram on the French passport.



Fig. 1. The three patterns of the hologram at the upper right corner of the French passport. From left to right: "RF", "Wind rose" and "France".

A. Preprocessing

Before creating any model, the raw images are preprocessed in order to remove most of the non-relevant information and to highlight the pattern of the hologram. After a grayscale conversion, the *Discrete Cosine Transform* (DCT) is applied on the images, and the frequencies are filtered to keep only the mid-range ones that highlight the pattern. An example of the preprocessing step for one image is presented in the Fig. 2.

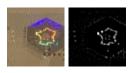


Fig. 2. Example of the preprocessing step on one hologram image. Left: the original image. Right: the image after the preprocessing step.

B. Local Binary Pattern Model

The computation of the LBP feature is quite simple. For each pixel of the preprocessed image, we compute the LBP vector feature as follows:

$$LBP = (s(I_c - I_0), s(I_c - I_1), ..., s(I_c - I_{P-1}))$$
(1)

where I_c is the intensity of the pixel to analyze, I_p with $p \in \{0, P-1\}$ the intensity of a pixel in the neighborhood, P is the number of neighborhood pixels, and $s(I_c-I_p)$ is defined by:

$$s(x) = \begin{cases} 1 & x \ge 0\\ 0 & otherwise \end{cases} \tag{2}$$

Fig. 3 presents the LBP operator applied on one pixel and the result obtained on a full image.

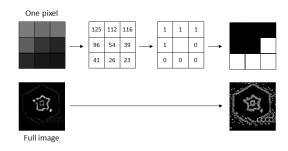


Fig. 3. Basic LBP operator for one pixel (top) and the LBP feature image for a full preprocessed image (bottom).

Since our images are quite small, we applied the LBP operator on a 3×3 neighborhood. The set of LBP vectors obtained after this step is called the LBP model, named as M in the rest of this paper.

C. Multi LBP Model

To differentiate genuine holograms from the fake ones, the LBP models that represent the desired patterns are used as references. In theory, one LBP model per pattern should be enough, but the variations in holograms appearance make the choice of one image as a reference complicated. Fig. 4 presents three different appearances for the hologram at the upper right corner in French passport with their LBP models.

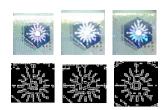


Fig. 4. Different appearances of the same pattern. The original images (top), the LBP models (bottom), cropped to the pattern.

To overcome this problem, we propose to use several LBP models to build a reference model called *Multi LBP Model*. Those models are selected automatically among a set of images labeled as the relevant pattern by computing a distance matrix between all the LBP models. Then, the K LBP models with the maximum distance are selected to constitute the *Multi LBP Model*, named as MM. To this end, we use the Hamming distance d_H to create the distance matrix DM as follows:

$$DM(i,j) = d_H(M^i, M^j) \tag{3}$$

where $i, j \in \{0, L\}$ with L the number of LBP models. The images that make up the Multi LBP Model are cropped, as presented in Fig. 4, to remove noise and keep the pattern only. Without any prior knowledge on the pattern, we choose to crop them manually for simplicity.

D. Similarity Metrics

Our method relies on a comparison between the Multi LBP Models and the image to test. It should be noted that several patterns can appear simultaneously in the same image. When the case arises, the corresponding patterns are assigned to the same image. The proposed approach does not try to find the best pattern for each image but try to determine if a pattern appears in the image independently of the others, and thus can assign several patterns to one image.

We define the similarity with two metrics: the Hamming distance d_H and the non-uniform distance d_{NU} . The Hamming distance is used to select the best LBP Model inside the Multi LBP Model MM^k with $argmin_k = d_H(MM^k, M)$ and $k \in K$. If the distance between MM^k and M is less than a threshold λ_{LBP} , then the image contains the corresponding pattern. In reality, we find out that images that contain little information, mainly black images, are considered

as containing a pattern when using the LBP distance. To overcome this problem, we define the second following metric:

$$d_{NU} = \frac{\sum_{n=0}^{N-1} \left(nu(MM_n^k) \cap nu(M_n) \right)}{\sum_{n=0}^{N-1} nu(MM_n^k)}$$
(4)

$$nu(M) = \begin{cases} 1 & \sum_{b=1}^{B-1} (LBP_0 - LBP_b) = 0\\ 0 & otherwise \end{cases}$$
 (5)

where B is the number of bits of LBP. This metric defines the percentage of non-uniform color in common between MM^k and M. The images with a low d_{NU} reflect models without patterns and can be rejected with a threshold λ_{NU} .

Two mechanisms are used to overcome the misalignment problem when comparing two models. The first one is the use of the template matching algorithm between each model of the reference model with the test model. All the models inside the reference model are cropped to keep only the interesting part as explained in the subsection III-C but the test images are kept as they are without any cropping. Here, the template matching algorithm solves the translation misalignment, but we still have to solve these due to rotation and scale. To overcome these types of misalignment, we compare each pixel with its spatial corresponding, i.e., same coordinates, into the reference image but also with its 8-neighbors. From these nine values, the minimum one is kept to compute the similarity.

E. Classification and Authentication

In order to determine the value of the thresholds to apply on both metrics proposed in the previous section, λ_{LBP} and λ_{NU} , we plot the results in a graph. An example of graphical results for a video is presented in Fig. 5. We observe that the images which contain the expected pattern have a small d_H and a big d_{NU} as expected, but they are spread out on a diagonal. Rather than defining a threshold for each metric, we propose to use an ellipse defined on the metric results obtained with images of a video chosen for the learning phase. Thus, the classification parameters are automatically determined and do not require the user to find the thresholds empirically. Let $X_n = (d_{NU}, d_H)$ be a 2D point and X the set of these points. The ellipse angle E_{α} , center E_c and size E_s are defined by:

$$E_{\alpha} = \arctan\left(V_{PCA}(X) \cdot V_{LDA}(Proj_{PCA}(X))\right) \quad (6)$$

$$E_c = (Len_x/2, Len_y/2) \tag{7}$$

$$E_s = (Len_x, Len_y) \tag{8}$$

where $Len_x = \max_x(X_n) - \min_x(X_n)$ respectively for $y, V_{PCA}(X)$ is the eigenvectors matrix computed with the *Principal Component Analysis* (PCA) method, $V_{LDA}(X)$ with the *Linear Discriminant Analysis* (LDA) method and $Proj_{PCA}(X)$ the projection to the principal PCA component subspace.

To authenticate the hologram, we combine the results obtained for each pattern. If a sufficient number of images are

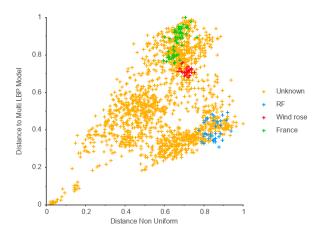


Fig. 5. The result metrics for one video. Each point is an image and the color defines the attributed label. Here the "RF" pattern is the one expected.

TABLE I SMARTPHONE CHARACTERISTICS.

Year	Model	Frame size	Frame rate
2020	Pixel 4a	1920 x 1080	30
2015	Nexus 6P	1280 x 720	30
2014	Iphone 6	1920 x 1080	30
2012	Nokia Lumia 920	1280 x 720	30

classified as the expected pattern then the pattern is estimated authentic. If at least two patterns are authenticated, then the hologram is defined as genuine.

IV. DATASET

In order to test our method, we have created a dataset which contains holograms from two types of document: the French passport and the euro banknotes. Unfortunately, we cannot make this dataset publicly available, as these holograms are security measures to combat fraud. However, we detail below the protocol used to create the dataset. Interested readers will be able to generate their own dataset.

A. Acquisition

For each document we used four smartphones, with and without the flashlight, which makes a total of eight videos per document. All the shots were taken indoor to be in the same conditions than the final user. The characteristics of the smartphones used for the acquisition process and the ones of the captured documents are presented respectively in the tables I and II.

TABLE II DOCUMENT CHARACTERISTICS.

Туре	# Holograms	# Patterns	# Example
French passport	2	3-3	10
Banknote 5€	1	2	3
Banknote 10€	1	2	5
Banknote 20€	1	2	4

B. Holograms Extraction

The extraction of the hologram images is done in three steps: tracking, registration and cropping. The first step is to track the document into the video stream. Since we focus here on the authentication of the holograms, we use a quite simple tracking method to track the document. The four corners of the document for the first frame are given by the user. Then the keypoints [15] extracted on the document, i.e., in the rectangle defines by the corners, are tracked using an optical flow algorithm [16]. Thanks to the tracking, the corners of the document are estimated for all the frames in the video. This method is not optimized, but it is more than enough to construct the dataset. From the four corners, it is possible to realign the document as flat by estimating a homography. Finally, since the holograms are on fixed positions for all the same document types, it is easy to crop the image to extract the region of interest.

C. Labeling

We propose two types of labeling: one to construct our Multi LBP Models (cf. III-C), and another one for the test. The first one is a strict labeling, i.e., each image has only one label and the pattern must be visible in the LBP image representation. For the second labeling, each image can have one or several labels according to the appearing patterns. Fig. 6 presents examples of this two labeling on the french passport.













Fig. 6. Two types of labeling. Left: only one pattern is visible in the images. Used for the Multi LBP Models and the automatic threshold. Right: several patterns are visible in the images. Used to test the method.

D. Counterfeit Documents

Since we do not have access to real counterfeit documents, we manually create two types of fake: scan and glossy. The first one is the simplest manner to create a fake document: scan and print it. For the second one, the pattern shape is cut and a glossy sheet is used to reproduce the reflective characteristic of a hologram. For both types of counterfeit only one pattern is reproduced per copy and only for the two holograms of the French passport, presented in the Fig. 7. We are aware that our counterfeits are not representative, but they allow us to check our method on the simplest versions.













Fig. 7. The counterfeit patterns of the two holograms of the French passport. First row: the scan patterns. Second row: patterns with a glossy sheet.

V. EVALUATION

Our method is evaluated on the dataset presented in the previous section. The solution is available online ¹ and is implemented in C++ with the OpenCV library on a Windows 10 personal computer with an Intel i7 processor. The mean computation time of the pattern evaluation is around 10 ms for the biggest images. Our implementation is a prototype of the proposed method and we can expect a performance gain by optimizing the algorithms.

Most of the parameters are automatically selected, excepted the number of images for each Multi LBP Model and the midrange of DCT frequencies for the preprocessing step. For the first one, we choose to use 8 frames. For the second one, we empirically choose to keep the frequencies between indexes 50 and 1500 for the passports and between indexes 10 and 1500 for the banknotes, according to the zig-zag ordering.

We use the well-known precision (P) (9) and recall (R) (10) measures to evaluate the proposed method.

$$P = \frac{TP}{TP + FP} \qquad (9) \qquad \qquad R = \frac{TP}{TP + FN} \qquad (10)$$

where TP are the true positives, FP false positives and FN false negatives. The results on genuine data per documents, per patterns and per smartphones are presented respectively in the tables III, IV and V.

TABLE III RESULTS PER TYPE OF DOCUMENTS. MEAN P IS THE MEAN PRECISION AND MEAN R IS THE MEAN RECALL.

Document		Holog	gram 0	Holog	Hologram 1		
Туре	Number	Mean P	Mean R	Mean P	Mean R		
	00	0.79	0.09	0.44	0.10		
	01	0.98	0.14	0.62	0.11		
	02	0.95	0.20	0.42	0.07		
	03	0.86	0.12	0.61	0.12		
Doggnort ED	04	0.78	0.11	0.44	0.05		
Passport FR	05	0.68	0.11	0.21	0.01		
	06	0.95	0.15	0.64	0.05		
	07	0.88	0.13	0.63	0.09		
	08	0.91	0.20	0.11	0.01		
	09	0.72	0.06	0.67	0.05		
Banknote 5€	00	0.46	0.66	-	-		
Dalikilote 3€	01	0.33	0.19	-	-		
	02	0.50	0.61	-	-		
	00	0.74	0.11	-	-		
	01	0.89	0.05	-	-		
Banknote 10€	02	0.31	0.00	-	-		
	03	0.89	0.10	-	-		
	04	0.62	0.07	-	-		
Banknote 20€	00	0.96	0.11	-	-		
Dalikilote 20€	01	0.94	0.20	-	-		
	02	0.99	0.18	-	-		
	03	0.94	0.19	-	-		

Our method obtains high precision in general for the passports, 10 and 20 euros banknotes on the hologram 0. The

TABLE IV RESULTS PER PATTERNS. MEAN P IS THE MEAN PRECISION AND MEAN R IS THE MEAN RECALL.

Patterr	ì	Holog	gram 0	Hologram 1		
Туре	Number	Mean P	Mean R	Mean P	Mean R	
	01	0.80	0.10	0.52	0.04	
Passport FR	02	0.85	0.09	0.55	0.09	
•	03	0.90	0.20	0.36	0.06	
Banknote 5€	01	0.47	0.45	-	_	
Banknote 5€	02	0.39	0.53	-	-	
Banknote 10€	01	0.79	0.10	-	-	
Banknote 10€	02	0.60	0.04	-	-	
Banknote 20€	01	0.95	0.15	-	-	
Dankhole 20€	02	0.96	0.20	-	-	

lowest results obtained on these categories are mainly due to unrecognized patterns, i.e., no image is identified as belonging to one or several patterns where the precision is equal to 0. We identified two main reasons: the first one is the misalignment of the document leading to errors during the tracking process. When the four corners of the document are not correctly estimated, the images get some residual rotations due to alignment inaccuracy which impact the similarity measures. The second reason is the definition of the ellipse used by the classification. The area defined by the ellipse is quite small and it happens that the target images are located around the ellipse.

Contrary to the other holograms, the hologram 1 of the French passport and the hologram 0 of the 5 euros banknotes get low precision. The one of the passport has a special characteristic: the background is not the same for each document. Indeed, this hologram is printed over the image of the face (picture on the passport). When the hologram highly reflects the light, the background is alleviated after the preprocessing step, but it is not always the case. Concerning the hologram on the 5 euros banknote, we note a lot of misclassifications which come from a combination of two factors: the noise and the size of the patterns. The holograms of the banknotes are located on a reflective strip with guilloche, an intricate and repetitive pattern. For the 5 euros banknotes, this guilloche produces enough noise in the LBP Model to confuse the small pattern, 14×14 pixels, with the noise during the image classification. The size of the patterns for 10 and 20 euros banknote are bigger and the shape of the guilloche creates less noise, which explain a better precision for these documents.

The recall value is low, except for the 5 euros banknotes. This result is explained by the size of the ellipse, which is usually small to avoid as much as possible the wrong classifications even if it means rejecting the good ones. In the case of the 5 euros banknotes, we observe that the area covered by the ellipse is bigger than for the other documents which makes it more permissive during the classification step.

The table V indicates that the proposed method is not limited by the type of smartphone. The videos used to compute the Multi LBP Models and the ones used to define the ellipse

¹https://github.com/mnchapel/authentication_of_holograms_with_mixed_patterns_by_direct_lbp_comparison

TABLE V RESULTS PER SMARTPHONES. MEAN P IS THE MEAN PRECISION AND MEAN R IS THE MEAN RECALL.

Document	Smartphone	Holog	gram 0	Hologram 1		
type		Mean P	Mean R	Mean P	Mean R	
	Pixel 4a	0.82	0.13	0.43	0.08	
Passport	IPhone 6	0.86	0.13	0.55	0.05	
FR	Nexus 6P	0.89	0.14	0.52	0.08	
	Nokia Lumia 920	0.82	0.12	0.42	0.05	
	Pixel 4a	0.38	0.45	-	-	
Banknote	IPhone 6	0.44	0.53	-	-	
5€	Nexus 6P	0.47	0.48	-	-	
	Nokia Lumia 920	0.44	0.50	-	-	
Banknote 10€	Pixel 4a	0.79	0.09	-	-	
	IPhone 6	0.64	0.06	-	-	
	Nexus 6P	0.60	0.05	-	-	
	Nokia Lumia 920	0.74	0.07	-	-	
Banknote	Pixel 4a	0.96	0.21	_	_	
	IPhone 6	0.94	0.13	-	-	
20€	Nexus 6P	0.99	0.18	-	-	
	Nokia Lumia 920	0.95	0.17	-	-	

were chosen independently of the type of the smartphone. The only criterion was to have a good visibility of the pattern after the preprocessing step. Moreover, we do not notice any improvement by using the flashlight to recognize the patterns and the user may even find it inconvenient to obtain each pattern of a hologram. A fixed light source seems preferable.

TABLE VI
RESULTS OF AUTHENTICATION ON GENUINE AND COUNTERFEIT FRENCH
PASSPORT FOR THE THREE PATTERNS (1, 2, 3) OF THE HOLOGRAM 0. THE
[] INDICATES THE REPRODUCED PATTERN ON THE COUNTERFEIT
DOCUMENTS. ONLY VIDEOS TAKEN BY THE PIXEL 4A WITH FLASH ARE
PRESENTED HERE FOR CONCISE RESULTS.

Document number	Genuine pattern			Counterfeit scan pattern		Counterfeit glossy pattern			
	1	2	3	1	2	3	1	2	3
0	~	~	~	[1]	×	×	[1]	×	×
1	~	\times	~	×		×	×	$[\mathbf{V}]$	×
2	~	~	~	×	×	$[\times]$	×	\times	[/]
3	~	×	~	-	-	-	-	-	-
4	~	×	~	-	-	-	-	-	-
5	×	~	~	-	-	-	-	-	-
6	~	\times	~	-	-	-	-	-	-
7	~	~	/	-	-	-	-	-	-
8	~	~	/	-	-	-	-	-	-
9	•	~	×	-	-	-	-	-	-

Finally, the robustness of our method was tested on counterfeit holograms (cf. table VI). We observe that our method is able to authenticate the pattern reproduced on the counterfeits. However, to authenticate the document, our method expects that at least two patterns to be authenticated, which is not the case here. In contrast, at least two patterns are authenticated on the genuine documents.

VI. CONCLUSION

In this paper, we proposed a method to authenticate holograms by pattern recognition based on a direct LBP com-

parison. The results obtained on our dataset are interesting. The simplicity of the recognition approach based on a direct LBP comparison, allows very fast computation time and let us consider reaching real time on a smartphone. However, initial limitations have been raised on too small patterns and non-static background. Several avenues for improvement can be considered. Among the existing ones there are the techniques of user guidance with augmented reality proposed by Hartl et al. [2] [5] [6] [7]. The tracking step can also be improved with more robust methods. A better tracking means less registration errors and potentially more patterns recognized with the direct LBP comparison. Concerning the noise due to the background, we can consider using some background removing approaches or to modify the preprocessing step to reduce the noise.

REFERENCES

- T. Ojala, M. Pietikainen, and D. Harwood. Performance evaluation of texture measures with classification based on kullback discrimination of distributions. *Proceedings of 12th International Conference on Pattern Recognition*, 1:582–585, 1994.
- [2] A. Hartl, C. Arth, and D. Schamlstieg. AR-based hologram detection on security documents using a mobile phone. Advances in Visual Computing, pages 335–346, 2014.
- [3] H.-J. Kwon and T.-H. Park. An automatic inspection system for hologram with multiple patterns. SICE Annual Conference 2007, pages 2663–2666, 2007.
- [4] H.-J. Kwon and T.-H. Park. Automated optical inspection for holograms with mixed patterns. *The International Journal of Advanced Manufac*turing Technology, 54:215–221, 2011.
- [5] A. Hartl, C. Arth, J. Grubert, and D. Schamlstieg. Efficient verification of holograms using mobile augmented reality. *IEEE Transactions on Visualization and Computer Graphics*, 22:1843–1851, 2016.
- [6] A. Hartl, J. Grubert, D. Schamlstieg, and G. Reitmayr. Mobile interactive hologram verification. *IEEE International Symposium on Mixed and Augmented Reality*, pages 75–82, 2013.
- [7] A. Hartl, W. Isop, C. Arth, and D. Schamlstieg. Towards mobile recognition and verification of holograms using orthogonal sampling. *IEEE International Symposium on Mixed and Augmented Reality Workshops*, pages 75–80, 2015.
- [8] D. Soukup, S. Stolc, and R. Huber-Mörk. Analysis of optically variable devices using a photometric light-field approach. *Media Watermarking*, *Security, and Forensics*, 9409, 2015.
- [9] S. Stolc, D. Soukup, and R. Huber-Mörk. Invariant characterization of dovid security features using a photometric descriptor. *IEEE Interna*tional Conference on Image Processing (ICIP), 2015.
- [10] D. Soukup and R. Huber-Mörk. Mobile hologram verification with deep learning. IPSJ Transactions on Computer Vision and Applications, 9, 2017.
- [11] O. Kada, C. Kurtz, C. van Kieu, and N. Vincent. Hologram detection for identity document authentication. *Pattern Recognition and Artificial Intelligence*, pages 346–357, 2022.
- [12] T. Ahonen, A. Hadid, and M. Pietikäinen. Face recognition with local binary patterns. *European conference on computer vision*, pages 469– 481, 2004.
- [13] T. Bouwmans, C. Silva, C. Marghes, M. S. Zitouni, H. Bhaskar, and C. Frelicot. On the role and the importance of features for background modeling and foreground detection. *Computer Science Review*, 28:26– 91, 2018.
- [14] B. Yang and S. Chen. A comparative study on local binary pattern (lbp) based face recognition: Lbp histogram versus lbp image. *Neurocomputing*, 120:365–379, 2013.
- [15] P. F. Alcantarilla, J. Nuevo, and A. Bartoli. Fast explicit diffusion for accelerated features in nonlinear scale spaces. *IEEE Trans. Patt. Anal. Mach. Intell*, 34:1281–1298, 2011.
- [16] J.-Y. Bouguet. Pyramidal implementation of the affine lucas kanade feature tracker description of the algorithm. *Intel corporation*, 5, 2001.