A STUDY ON PUF CHARACTERISTICS FOR COUNTERFEIT DETECTION

Chau-Wai Wong and Min Wu
University of Maryland, College Park, USA

ABSTRACT

Low-cost physically unclonable functions (PUFs) can be deployed with consumer products to deter counterfeiting. An intrinsic physical property—unique textures of paper or other surfaces—has received significant interest. Extrinsically introduced features, such as randomly positioned bubbles and fiber segments, have also been deployed in the industry to facilitate authentication. This paper conducts a study to gain a better understanding of factors affecting authentication performance, with a consideration of friendliness under mobile imaging. Comparisons are made for paper-based PUFs of different characteristics. It is found that the density of foreground objects has a dominant impact on authentication performance.

Index Terms— Anti-Counterfeit, PUF, Paper Texture

1. INTRODUCTION

The deployment of physically unclonable functions (PUFs) as a way to deter counterfeiting has been receiving increasing attention in both the research community and industry. Clarkson et al. [1] exploits the surface texture of paper documents as a unique identifier: random, naturally occurring imperfections in the paper texture lead to a unique map of surface norms that can be optically captured by commodity scanners. Voloshynovskiy et al. [2, 3, 4] found that using industrial acquisition devices, high-resolution photos of paper surfaces captured distantly have good authentication performance, whereas the extension into using built-in cameras of mobile phones has acceptable performance at a higher computational cost. The BubbleTag [5] from a "spontaneous" generation of bubbles in a polymer has been deployed commercially for anti-counterfeiting with automated optical authentication or human visual authentication. The FiberTag [5] and Kinde Label [6] use the randomly distributed visible fiber on surfaces to provide uniqueness for anti-counterfeiting, and their verifications rely mainly on human visual inspection. Similarly, the Ramdot [5] is a PUF with randomly distributed color dots to provide uniqueness. A summary of various PUFs is shown in Fig. 1(a).

There are several desirable functionalities for counterfeit detection. Automating PUF authentication enhances user-friendliness and quantitative understanding of the performance. The increased popularity of smartphones also makes it desirable to enable verification using mobile devices. To the best of our knowledge, there is no prior systematic study on factors affecting the authentication performance for a variety of PUF features.

In this paper, we examine the detection performances of four representative PUFs, namely, the surface norm PUFs [1], microstructures [2, 4], BubbleTags [5], and sealed-powder patches. We construct patches with low-cost materials to gain understanding, whereby patches contain high-contrast powder particles randomly distributed and sealed under tape. These lab-produced patches can be captured using mobile phone cameras, and facilitate the study of PUFs' adjustable characteristics without mass commercial production.

2. DETECTION METHOD

We focus on optical features of PUFs and approach the PUF verification problem as an image authentication problem commonly formulated as hypothesis tests. The null hypothesis H_0 corresponds to incorrectly matched pairs of test and reference patches whereas the alternative hypothesis H_1 corresponds to correctly matched pairs. The optimal decision rule maximizing the statistical power is the likelihood-ratio test: rejects H_0 if $\frac{f_1(\mathbf{x})}{f_0(\mathbf{x})} \geq \tau$ holds, where $\mathbf{x}$ represents the test patch, f_0 and f_1 are the probability density functions under null and alternative hypotheses, respectively, and τ is a threshold. A hypothesis test differentiating a known reference patch $\mathbf{w}$ against all other patches can be formulated below:

$$\begin{cases} H_0 : \mathbf{x} = \mathbf{e}_0, & \mathbf{e}_0 \sim N(m\mathbf{1}, \mathbf{\Sigma}_0), \\ H_1 : \mathbf{x} = \mathbf{w} + \mathbf{e}_1, & \mathbf{e}_1 \sim N(\mathbf{0}, \sigma_1^2\mathbf{I}). \end{cases} \tag{1}$$

Here, $\mathbf{e}_0$ stochastically represents any acquired image patch with a non-degenerate covariance matrix $\mathbf{\Sigma}_0$ for image content and acquisition noise, $\mathbf{1}$ is an all 1 vector with the same dimension as $\mathbf{x}$, m corresponds to a value at the center of the linear range of the digital representation of intensity ($m = 128$ for intensity in the range $[0, 255]$), $\mathbf{w}$ deterministically represents the reference patch image, and $\mathbf{e}_1$ is the image acquisition noise (white, with constant variance σ_1^2). Sample correlation coefficient $\hat{\rho}(\mathbf{w}, \mathbf{x})$ against a threshold is used as the decision rule in this paper.

On the principles of data selection, the data $\mathbf{x}$ should be capable of being well modeled in the probabilistic sense as shown in Eq. (1). Nonuniform lighting and glare due to light reflection should first be removed by preprocessing. Although

Originally published at IEEE ICIP 2015. Updated to correct typographical errors; no substantive changes made.

SUMMARY OF VARIOUS PUFS

Category	Name	Visual Feature(s)
Paper texture based PUFs	norm map [1]	3D structure of texture surface
	microstructure [2-4]	appearance to a camera with moderate distance
PUFs with significant visual features	BubbleTag [5]	2D/3D bubble shape and location
	FiberTag, Ramdot [5] / Kinde Label [6]	shape and location
	sealed powder on paper	shape and location

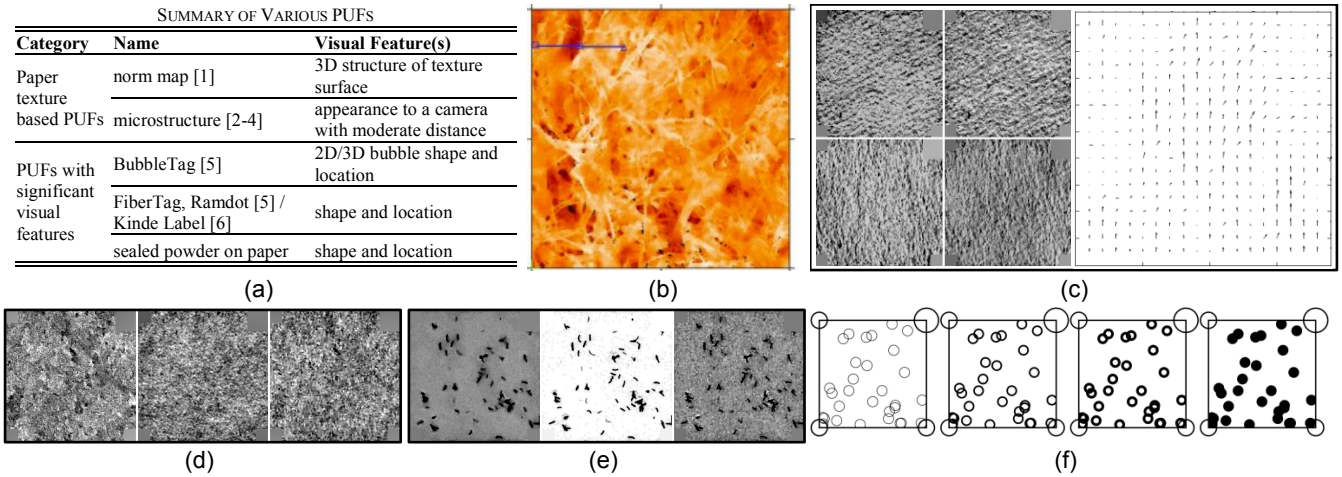

Fig. 1: (a) Summary of PUFs. (b) 1mm-by-1mm region of a topography map of a paper surface captured by a confocal microscope, reproduced from [7]. (c) A surface of cotton paper scanned from 4 perpendicular orientations and the resulting estimated norm map. (d)–(e) A paper surface and a powder PUF, respectively, captured by the following devices: scanner, iPhone 6, and Pantech Tablet. (f) Simulated BubbleTags in 2D view with design parameters $r_{\text{out}} = 10$ and $r_{\text{in}} = 9, 7, 5, 0$.

we consider the patch intensity feature as the data $\mathbf{x}$ in this paper, random projections (RPs) [2], binarized RPs [2], and SIFT descriptors [3, 4], can be chosen to represent the test patch. We leave the study of these features to future work.

3. PAPER TEXTURE BASED PUFS

The uniqueness of the inherent 3D structure of paper surface formed by overlapped and inter-twisted wood fiber has been exploited for authentication purposes [1, 2]. The visual appearance of a surface depends on a light source and the observer's position: if the observer is right above the surface when the light source is approximately in parallel with the surface, the observer can only see one side of the paper structure being lighted by from the direction that light is coming from; if the observer is far above the surface and the light source is far away and perpendicular to the surface, a better view of the surface can be observed. Fig. 1(b) shows a 1mm-by-1mm region of a topography map of a copy paper surface [7] captured by a confocal microscope in which the imperfect "surface" comprising of fibers is clearly shown.

We create a PUF registration container to facilitate the experiments in this paper. The PUF container as shown in Fig. 1(f) facilitates precise registration. Considering 600 ppi printing resolution, our container is a square box of 400-by-400 in pixels, the line width is 5 pixels, and there are four circles at the corners. A preliminary alignment based on four boundaries can be achieved using the Hough transform, and subpixel resolution refinement with perspective transform compensation is then carried out based on the circle markers.

Surface Norm Map A photometric stereo approach was used in [1] to estimate the projected normal directions of at all integer-pixel locations of the surface (*aka* the norm map) by using images scanned from 4 different orientations of the paper: $0°$, $90°$, $180°$, and $270°$. The norm map is an intrinsic property of a surface. The lighting in scanners forms a line source and the imaging sensor is close to the paper surface. The paper is assumed fully diffuse, and the amount of the reflected light is proportional to the cosine of the angle between the direction of incidence and the surface normal. The projection of the normal vector onto the xy-plane can thus be estimated by using the above 4 scans of the paper surface, without knowing the direction of incidence light. The estimate is the difference between two scans in exactly opposite directions, which cancels the effect of the unknown incidence direction of the scanner light.

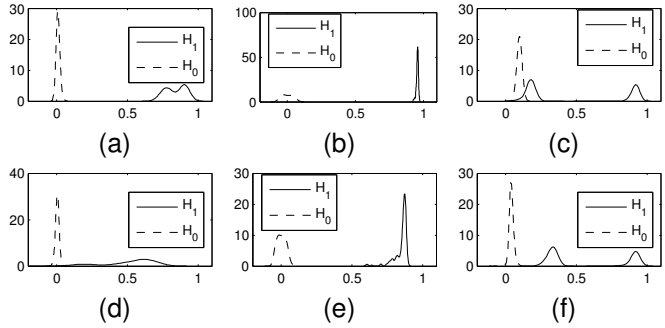

Fig. 2: Estimated PDFs of sample correlation coefficient $\hat{\rho}$ for correctly and incorrectly matched cases. (a–b): Datasets #2–3 (test) vs. #1 (ref.) of scanner 2450, and (d–e): Datasets #1–3 (test) of scanner GT vs. #1 (ref.) of scanner 2450. Test statistics: (a)(d) length, and (b)(e) x-component of norm vector. Estimated PDFs of $\hat{\rho}$ for (c) cotton paper, (f) copy paper. Datasets acquired by scanner 2450.

We estimate norm maps for 49 independent PUFs. The acquisition procedure is repeated using 2 Epson scanners: Perfection 2450 and GT-2500. Sample patches for scanner 2450 and the resulting norm map estimate are shown in Fig. 1(c). Correlation analysis is carried out between norm maps estimated from the *same* scanner as well as from *different* scanners. Normal vector's length, x- and y-components

are used for correlation analysis. The left 4 plots of Fig. 2 reveal that the distributions of sample correlation coefficient $\hat{\rho}$ for correctly matched patches (H_1) and incorrectly matched patches (H_0) are generally far apart, suggesting a very good authentication performance of the norm map under well-controlled acquisition condition. This is especially true when patches are obtained from the same scanner. When reference patches and test patches are from different scanners, the x- and y-component features have slightly lower performances, whereas the norm length is no longer reliable.

Scanned Surface (acquired at close distance) We now examine the authentication performance of the raw scanned images from which norm maps are estimated. We scan paper using two opposite directions so that the appearances of the obtained images are highly different due to the closely positioned lighting-imaging system.

Our experimental results show that the distribution of $\hat{\rho}$ for the correctly matched patches has two peaks: high at 0.9 for patches scanned in the same direction, and low at 0.2 for patches scanned in opposite directions, as shown in Fig. 2(c) and (f). The bimodal distribution of H_1 confirms that the patch appearance is highly affected by the scanning direction when the lighting-imaging system is close to the paper. Hence, except in highly controlled cases in which scanner model and scanning direction are known, the images obtained by scanners are not good for being directly used for authentication purposes. This is true over different types of paper, such as cotton paper, copy paper, and card stock.

Microstructure (acquired at moderate distance) Instead of capturing images using directional linear light and closely placed imaging sensors, Voloshynovskiy et al. [2, 3] captured images using two industrial cameras at a high elevation and a light source of a circular ring shape. The resulting images give an overview of the paper surface lit by the light source (*aka* the microstructure). Cameras with lower resolution on mobile devices were also tested recently for capturing the surfaces under uncontrolled light sources [4], whereby the performance was considerably worse than the industrial camera setup.

We test authentication performance using cameras on mobile devices. The aligned patches captured using different acquisition devices are shown in Fig. 1(d) with nonuniform lighting and glare removed. Although a general similarity exists among the patches, small details differ a lot. Experiments show that for the same patches, correlation values are not high using mobile for capturing (mean values are only around 0.2 to 0.4 for various combinations of acquisition devices for test and reference patches.) Fig. 3 shows estimated PDFs, a sample PDF under H_0 and its bounds, and the resulting ROC bounds.

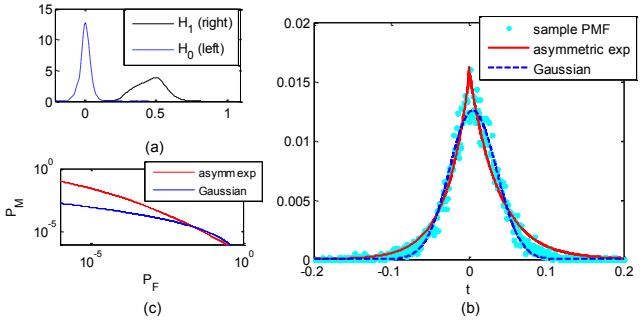

Fig. 3: (a) Estimated PDFs of $\hat{\rho}$, (b) sample PMF and its bounds, and (c) ROC bounds for light green card stock. At $P_f = 10^{-3}$, the miss rate P_m ranges from 10^{-4} to 10^{-3}. Both test and reference datasets are acquired using iPhone 6.

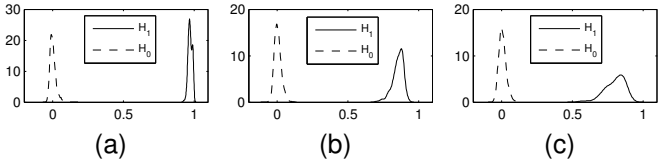

Fig. 4: Estimated PDFs of $\hat{\rho}$ for (a) scanner vs. scanner (ref.), (b) iPhone 6 vs. scanner (ref.), and (c) Pantech Tablet vs. scanner (ref.).

4. PUFS WITH HIGH CONTRAST

The paper texture-based PUFs require controlled acquisition conditions, such as scanners and industrial cameras, to achieve good authentication performances, or give limited performances when consumer-grade cameras are used in non-controlled settings. This motivates us to examine another class of PUFs that have high-contrast visual features and investigate their performances when the authentication is carried out using mobile cameras. As reviewed earlier, the FiberTag [5] and Kinde Labels [6] use a random pattern of visible fibers as a unique identifier. Ramdot [5] uses randomly positioned color dots as a unique identifier, whereas BubbleTag [5] uses the randomly positioned bubbles in a polymer.

Low-Cost Sealed Powder PUF We create an experimental PUF with dark flocking powder from craft stores as the foreground, to understand the performances of PUFs with the randomly distributed visible fiber. The powder is randomly dropped on the paper surface to form a unique pattern, and the pattern is sealed by transparent adhesive tape. The design parameters of this powder PUF include the density of the powder and the spatial distribution. This lab-produced PUF [examples in Fig.1(e)] helps us understand the authentication performance of the PUFs as a function of design parameters.

Fig. 4 shows that once high-resolution registration is achieved, the authentication performances for sealed powder PUFs are very good. We observe from experiments that a better camera and higher powder density lead to a larger margin between the densities of H_0 and H_1.

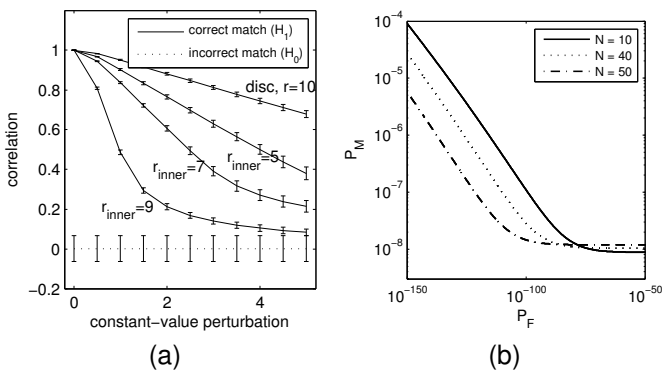

Fig. 5: (a) Mean-std errorbar plot of PDFs of $\hat{\rho}$ under H_1 for $r_{\text{out}} = 10$ and different r_{in}'s. The PDF under H_0 with the maximum std range is displayed as the worst case. (b) ROC curves for different numbers of foreground circles, N.

Simulated BubbleTag The 2D appearance of BubbleTag can be modeled as open circles. The grayscale version of Ramdots can be modeled as filled circles/discs. We simulate BubbleTag and Ramdot PUFs by a set of foreground circles with different boundary widths. Foreground circles with pseudorandom locations are drawn at 600 ppi digitally, and then recaptured via downsampling to 300 ppi. Printing and scanning noise is assumed to be negligible. Misalignment is added in the form of constant-value perturbation.

Fig. 1(f) shows circles with same outer radius 10 and different inner radiuses 0, 5, 7, and 9; each patch has 30 circles. Our examination result shown in Fig. 5(a) reveals that filled circles as foreground objects are less sensitive than unfilled ones, and circles with thicker boundaries are less sensitive than thinner ones. For a patch with circles of boundary width d, the convexity of the curve for averaged correlation under H_1 w.r.t. perturbation starts to change around perturbation level d.

Fig. 5(a) shows that it is possible to have poor authentication performance when alignment is imprecise. As alignment algorithms are usually capable of achieving subpixel precision, we consider the scenario that the length of the displacement vector is uniformly distributed between 0 and 0.5, and carry out experiments to understand the factors affecting authentication performance. We build on the case of circle inner radius $= 7$ [second patch in Fig. 1(f)]: we fix the circle size, and change the density by changing the number of circles for the PUF. The result in Fig. 5(b) shows a better performance for higher density.

PUF Modeling The experiments and simulations in the previous sections show that authentication performance depends on several factors, including alignment precision, and shape and density of appearance features. In order to go from a qualitative understanding of factors affecting the authentication performance of PUFs to quantitative knowledge, it is beneficial to model the problem into several subproblems that can be solved analytically or numerically. Due to the space limitation, we briefly summarize how we approach the problem, with this divide-and-conquer strategy.

We focus on a class of PUFs with isotropic foreground appearance features. To assess the authentication performance, the distributions of the test statistic—sample correlation coefficient $\hat{\rho}$—should be known under the correctly matched case (H_1) and the incorrectly matched case (H_0). It is easier to first consider binary images of PUFs. We assume that the level of acquisition noise is not strong enough to flip any of the binary pixels, and that registration error only happens in the form of a global displacement. Thus, in H_1, the acquired patch is identical to the reference patch, with global matching imprecision quantified by a random displacement vector. In H_0, the acquired patch is a random patch, with the same design parameter Γ—the number and the shape of foreground objects—as those in the reference patch. The randomness of test statistic $\hat{\rho}$ under H_1 comes from the random matching imprecision, whereas the randomness of $\hat{\rho}$ under H_0 comes from the randomly distributed foreground objects.

The correlation in both hypotheses is related deterministically to the number of black-to-white pixel flips, $\delta^{0\to1}$, and the number of white-to-black pixel flips, $\delta^{1\to0}$. For the correctly matched case H_1, we have $\delta = \delta^{0\to1} = \delta^{1\to0}$ due to isotropicity, where δ is related to the displacement vector quantifying the alignment imprecision. For incorrectly matched case H_0, the joint distribution of $(\delta^{0\to1}, \delta^{1\to0})$ conditioned on one of a series of combinatoric cases can be analyzed and results can be obtained numerically. Simulated data has confirmed the effectiveness of the model.

5. CONCLUSION AND FUTURE WORK

PUFs have promising features to aid counterfeiting detection. The norm map of paper texture is a good intrinsic feature for authentication purposes, but it requires a controlled imaging setup—different scanners can potentially affect the performance. The raw intensity patch image obtained by a scanner would work if the scanning directions and the incidence direction of the scanner light were well controlled. The intensity maps of patch images obtained by cameras of mobile devices do not have a good performance for pixel-domain correlation detectors, due to the uncontrollable light sources, and limits in camera resolution and focusing capability.

The purposely designed PUFs with high-contrast visual features have very good authentication performance. We have examined the factors affecting the authentication performance, and found that the density of foreground objects has a strong impact on the authentication performance. Our further work will examine other factors such as the autocorrelation structure of the foreground objects, and build on the model we developed to obtain quantitative results on how the performance of PUFs is affected by various factors.

6. REFERENCES

[1] W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J. Halderman, and E. Felten, "Fingerprinting blank paper using commodity scanners," in *Proc. IEEE Symposium on Security and Privacy*, Berkeley, CA, May 2009, pp. 301–314.

[2] S. Voloshynovskiy, M. Diephuis, F. Beekhof, O. Koval, and B. Keel, "Towards reproducible results in authentication based on physical non-cloneable functions: The forensic authentication microstructure optical set (FAMOS)," in *Proc. IEEE International Workshop on Information Forensics and Security (WIFS)*, Tenerife, Spain, Dec. 2012, pp. 43–48.

[3] M. Diephuis and S. Voloshynovskiy, "Physical object identification based on FAMOS microstructure fingerprinting: Comparison of templates versus invariant features," in *Proc. International Symposium on Image and Signal Processing and Analysis (ISPA)*, Trieste, Italy, Sep. 2013, pp. 119–123.

[4] M. Diephuis, S. Voloshynovskiy, T. Holotyak, N. Stendardo, and B. Keel, "A framework for fast and secure packaging identification on mobile phones," in *Proc. SPIE, Media Watermarking, Security, and Forensics 2014*, San Francisco, CA, Feb. 2014, p. 90280T.

[5] Product Overview on BubbleTag™, Ramdot™, FiberTag™, *Prooftag SAS*, Retrieved Jan. 2015. http://www.prooftag.net/

[6] Kinde Anti-Counterfeiting Labels, *Guangdong Zhengdi (Kinde) Network Technology Co., Ltd.*, Retrieved Jan. 2015. http://www.kd315.com/

[7] "High resolution surface topography FRT MicroProf chromatic aberration sensor," in *a product sheet by Inventia*, Aug. 2012.