Photo-Response Non-Uniformity -Based Physical Unclonable Functions Using In User Authentication

Bade Ankamma Rao[1], Srirama Bala Sowndarya [2]
[1]Assistent Professor, Dept of MCA
[2]Dept of MCA
[1, 2] St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

Abstract- *Multifactor user authentication systems enhance security by augmenting passwords with the verification of extra items of data like the possession of a specific device. This paper presents an innovative user authentication theme that verifies the possession of one's smartphone by uniquely characteristic its camera. High-frequency parts of the photo-response unsimilarity of the optical sensor square measure extracted from raw pictures and used as a weak physical unclonable perform. a completely unique theme for efficient transmission associate degreed server-side verification is additionally designed supported adaptational random projections and on an innovative fuzzy extractor exploitation polar codes. the safety of the system is completely analyzed underneath completely different attack scenarios each on paper and through an experiment.*

Keywords- User authentication, PRNU, random projections, fuzzy extractors, polar codes.

I. INTRODUCTION

The very large diffusion in everyday life of web-based services like social networks, internet banking, cloud-based storage, requires the development of user authentication tech-niques that are both secure and user friendly [1]. In this sense, the traditional mechanism based on secret passwords shows several shortcomings. Security means that long and unpredictable passwords should be generated and remembered, which is not user friendly. As a consequence, short and easily predictable passwords are commonly reused, which considerably reduces the security of the system.

Recently, several solutions have been proposed for providing an additional level of security in current user authentication systems. A common approach is to resort to a multifactor authentication scheme, in which the knowledge of a secret password is complemented with the possession of one, or more, physical or software tokens [2]. Typical solutions cur-rently implemented on several existing web services are the generation of one-time passwords (OTPs) on a dedicated token, or receiving a OTP by text message on the user's smartphone [3], [4], [5]. Even if multifactor authentication effectively solves the security problem, the existing solutions typically reduce user friendliness. As an alternative, several authors have proposed authentication systems based on the possession of unique signals that are not easily reproducible. A natural choice is using biometric traits like fingerprints, irises, or faces [6], [7], [8]. An innovative approach consists in deriving a secret from some physical characteristics of an integrated circuit that are deemed unique, implementing a so-called physical unclonable function (PUF) [9].

In this paper, we propose a novel authentication system that relies on an unclonable physical property of digital image sensors named photo-response non-uniformity (PRNU). The PRNU is a sensor-specific multiplicative noise pattern that has enjoyed great popularity in the last decade because it can be used to solve several forensic problems. Examples of its many applications are: determining which camera has acquired a given photo [10], [11], clustering collections of images by their source camera [12], [13], camera-based image retrieval [14], [15] and detecting and localizing image forgeries [16], [17].

The concept proposed in this paper is to use the PRNU of the camera sensor of the user's smartphone as a weak PUF [9], that can be used as a possession factor in a multifactor authentication scheme, or even employed in a single step authentication protocol. Due to the ubiquitous diffusion of smartphones, such a system is potentially much user friendlier than existing solutions, enabling the implementation of an application that automatically acquires pictures, computes a compact code derived from the sensor PRNU and transmits it to a remote verification server requiring minimal or no user interaction. However, turning this idea into a practical authen-tication system requires to solve several important problems, as well as rigorously show the security of such solutions.

First, the PRNU survives JPEG compression, as well as some image processing operations, and it can be found in photos that are publicly available, e.g., on social networks [18]. Luckily, the

PRNU is inevitably degraded by such operations, while in the framework of user authentication, the legitimate user has full control over the camera and could extract the PRNU with an arbitrarily high quality. In the following, we consider extracting the PRNU from RAW images and keeping only its high-frequency components. Since JPEG compression acts as a lowpass filter, the high-frequency components are unavailable or severely degraded in publicly available images and can only be estimated if one has access to the raw data.

Second, the PRNU has the same size as the image sensor. Sending a complete PRNU signal over a mobile connection could be impractical in several scenarios, as well as storing the reference PRNUs of a large number of users at the server side. In this case, we propose to compress the PRNU using random projections. Recent results show that this technique can reduce the PRNU size by several orders of magnitude, without significantly affecting the matching performance [14]. Moreover, this also provides an additional security layer since the actual PRNU is never disclosed and if a compressed PRNU is compromised this can be revoked and replaced by a freshly generated compression.

Lastly, the server should not store a copy of the PRNU, or its compressed version. This problem can be solved by resorting to techniques used for biometric template protection [19], [20]. Namely, we present an innovative implementation of a secure sketch and a fuzzy extractor based on polar codes, which is specifically tailored to compressed PRNUs. Since in the proposed system an attacker may have a partial knowledge of the PRNU from publicly available photos, the proposed construction incorporates a specific coding technique for the wiretap channel based on polar codes, which effectively prevents the attacker from gaining access to the system.

A. Related works and contribution

The idea of using high frequency components of PRNU has been recently introduced in a different context in [21]. The authors considered the case of fingerprint-copy attacks [22], where an attacker wants to plant a fingerprint in an image but only has access to JPEG images of the camera, while the defender has access to RAW data. The user authentication scenario significantly differs from a copy attack and provides unique requirements. Our goal is to show that an attacker that can only access JPEG-compressed images cannot reliably estimate the high-frequency components of the PRNU that the legitimate user employs as fingerprint. In our analysis, the legitimate user has full control over the raw image quality, and the number of images that can be used to generate the reference and test fingerprints. The attacker potentially has access to a large number of high-quality JPEG images and tries to extract a fingerprint that is highly correlated with the legitimate one. In this work, we assume that an attacker can only access public images in JPEG format and we do not consider the possible theft of RAW images. With respect to [21] we also provide a different fingerprint extraction method that is not constrained to work on 8 8 blocks. A significantly larger database with RAW and JPEG images, mostly from smartphone cameras, has been assembled in order to test attacks with hundreds of high-quality JPEG images.

The use of random projections for biometric template pro-tection has been proposed in a number of works [23], [24], [25], [26], and later extended also to PUFs [27]. With respect to existing papers, we introduce a novel adaptive random projection technique, similar to a technique proposed in [28] and then further expanded and carefully analysed in [29]. Moreover, using the PRNU as a PUF requires an ad-hoc design of the fuzzy extractor, for which we provide an original construction based on polar codes and a rigorous security analysis. Finally, we provide a rigorous security analysis of the whole proposed system under different attack scenarios.

Very recently, the authors of [30] proposed to combine several device sensor features, including PRNU, and apply machine learning for smartphone authentication. The paper provides some interesting insights on the distinctiveness of smartphone sensors, however security issues are not addressed and a complete authentication system is not discussed. The possibility of using PRNU for authentication is also discussed at high level in this recent contribution [31], but no technical solutions are proposed, and a rigorous security analysis is not provided.

II. RELATED WORK

The following subsections provide some background ma-terial to help the reader understanding the rest of the paper. We first (Sec. II-A) present some notation used throughout the paper. Sec. II-B recalls the basics of PRNU of digital imaging sensors. Sec. II-C introduces random projections, a useful dimensionality reduction method. Sec. II-D discusses fuzzy extractors, a set of techniques to extract uniform randomness from a source that is not exactly reproducible. Finally, Sec. II-E reviews polar codes, a channel coding technique.

A. Notations

Lower-case (upper-case) bold symbols denote real-valued vectors (matrices). Lower-case letters indicate scalars or bit strings. Upper-case letters denote random variables.

Symbols P and E denote the probability and expectation operators, respectively.

The predictability of a random variable A is measured by the min-entropy, defined as $H_1(A) = \log(\max_a P(A = a))$. A variable whose min-entropy is m bits is as hard to predict as a uniformly random string of m bits.

If the adversary observes a variable B which is correlated with A, the expected predictability of A can be expressed by
the average min-entropy of given , defined as ~
j
A B $H_1(A|B) = \log(E_b[2^{H_1(A|B=b)}])$.

It is also useful to define how much two random variablesdiffer using the statistical distance between variable A and B, defined as $d_S(A; B) = \frac{1}{2} \sum_v |P(A = v) - P(B = v)|$.

Table I summarises the main symbols used throughout the paper, along with their description.

B. PRNU

PRNU [11], [32] of imaging sensors is a property unique to each sensor array due to the different ability of each individual optical sensor to convert photons to electrons. This difference is mainly caused by impurities in silicon wafers and its effect is a noise pattern affecting every image taken by that specific sensor. Hence, the PRNU can be thought of as a spread– spectrum fingerprint of the sensor.

The literature on camera forensics [11], [33] widely consid-ers the PRNU as unique for each camera since it has very large entropy and therefore the probability of two cameras having the same pattern is negligible. For instance, Bayram et al. [34] estimate the entropy of the PRNU to be 20 bits per pixel, and considering that the PRNU has the same pixel size as the sensor, and the value for each pixel is uncorrelated with the others, the PRNU has very large discriminative power. Being a multiplicative pattern, its strength with respect to other noise sources depends on the brightness of the acquired image.

The PRNU characterizing one sensor can be extracted from a set of images (typically, 20 to 50 smooth images are enough). The procedure to extract the fingerprint k of a sensor from a set of pictures depends on the model used to characterize the optical sensor. The sensor output o can be modelled as

$$o = o^{id} + o^{id}\, k + e\,; \qquad (1)$$

where o^{id} is the ideal sensor output, o^{id} k is the PRNU term and e collects other sources of noise. Assuming to be able to obtain through proper filtering a denoised version of o, referred to as o^{dn}, then this can be used as an approximation of the ideal sensor output and subtracted from each side of (1) to obtain the so-called noise esidual, which can be modeled as:

$$\mathbf{r} = \mathbf{o} - \mathbf{o}^{dn} = \mathbf{o} \cdot \mathbf{k} + \tilde{\mathbf{e}}\,, \qquad (2)$$

where ~ e accounts for e and for the non-idealities of the model [11]. Supposing that a certain number C of images is available, the maximum likelihood estimate b^k can be obtained a

$$\hat{\mathbf{k}} = \sum_{l=1}^{C} \left(\mathbf{r}^{(l)} \cdot \mathbf{o}^{(l)}\right) \Big/ \sum_{l=1}^{C} (\mathbf{o}^{(l)})^2. \qquad (3)$$

To improve further the quality of the estimation, artifacts shared among cameras of the same brand or model can be removed by subtracting row and column averages. In the case of color images, the estimation must be performed separately on each color channel, and then an RGB–to–gray conversion can be applied.Finally, a pair of ingerprint vectors k1, k2 is typically compared using their correlation coefficient, defined a

$$\rho = \frac{\mathbf{k}_1^T \mathbf{k}_2}{\|\mathbf{k}_1\|_2 \|\mathbf{k}_2\|_2}.$$

C. Random projections

Random projections (RPs) are a method for dimensionality reduction [35]. A collection X Rn of signals living in a high-dimensional space can be embedded with low distortion into low-dimensional representations Y Rm (also known as measurements, or random projections, with m < n) by computing inner products with random vectors. In matrix form this is written as y = x, for x 2 X , y 2 Y, and where is often referred to as sensing matrix. Measurements can also be quantized to achieve more storage-efficient representations. The key property of random projections is that they approxi-mately preserve distances. A classic result is that real-valued random projections, where the sensing matrix is made of independent and identically distributed (i.i.d.) Gaussian entries, are a mapping that satisfies the Johnson-Lindenstrauss (JL) lemma [36], meaning that `2 distances are nearly preserved. A key property following from the JL lemma is that the number of measurements m depends only on the desired distortion on distances between signals introduced by the embedding, and on the number of signals that are to be

embedded but not on the dimensionality of input space n. Of particular interest are binary random projections that are computed with a sensing matrix made of i.i.d. Gaussian entries, and then quantized to one bit by keeping the sign of the measurement. The Hamming distance between the resulting binary vectors approximately preserves the angle between the signals in the original space [37], i.e.,

$$\mathbb{P}\left(\text{sign}(\boldsymbol{\phi}_i^T \mathbf{u}) = \text{sign}(\boldsymbol{\phi}_i^T \mathbf{v})\right) = 1 - \frac{\theta}{\pi},$$

being $\theta = \cos^{-1}\left(\frac{\mathbf{u}^T\mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|}\right)$, and $\boldsymbol{\phi}_i$ the i-th row of $\boldsymbol{\Phi}$.

is often impractical to use a fully random sensing matrix,either because the high dimensionality of the signals requires to generate too many random numbers or because performing the full matrix-vector product is too computationally intensive.Circulant matrices with randomized column signs [38] are an appealing solution ecause they allow to generate only the first row of the sensing matrix and compute the measurements using the FFT.In [14], [15], RPs were used to perform imensionality reduction of PRNU patterns, showing significant gains in terms of storage requirements as well as in the complexity of the match or search in large database operations.

Fuzzy extractors denote a set of techniques for extracting nearly uniform randomness from sources of information that are neither exactly reproducible nor uniformly distributed [20]
[19]. These techniques were originally developed for gener-ating strong keys from biometric data, however they can be applied to any form of noisy data used for authentication, like PUFs. More precisely, such techniques rely on two primitives: 1) a fuzzy extractor that extracts nearly uniform randomness from an input in an error-tolerant way, i.e., close inputs are guaranteed to generate the same randomness; 2) a secure sketch producing public information about a secret input w that does not reveal anything about w, yet allows to recover w when combined with another value that is sufficiently close to w.

In our scheme, we will employ a slightly relaxed definition of secure sketches and, in turn, of fuzzy extractors, that accounts for a negligible probability of not recovering the secret input w. This definition applies when the error pattern on w can be modeled by a binary symmetric channel with crossover probability p (BSC-p).

Definition 1. An (n; m; m;~ p;)-secure sketch consists in a pair of functions SS : f0; $1g^n$! f0; 1g and Rec : f0; $1g^n$ f0; 1g ! f0; $1g^n$ with the following properties:

1) Correctness: if w0 is the output of a BSC-p when the input is w, then Rec(w^0; SS(w)) = w with probability at least 1 .

2) Security: if then ~ j .
$H_1(W) = m$ $H_1(W\ SS(W)) \quad m\sim$

Definition 2. An (n; m; `; p; ; )-fuzzy extractor consists in a pair of functions Gen : f0; $1g^n$ ! f0; 1g` f0; 1g and Rep : f0; $1g^n$ f0; 1g ! f0; 1g` with the following properties:

1) Correctness: if (x; s) = Gen(w) and w^0 is the output of a BSC-p when the input is w, then Rep(w^0; s) = x with probability at least 1 .

2) Security: if (x; s) = Gen(w) and $H_1(W) = m$ then $d_S((X; S); (U`; S))$ , where U` is a uniformly distributed string of ` bits.

From the above definitions, it is evident that a fuzzy ex-tractor can be constructed on top of a secure sketch, provided that one can extract sufficiently uniform randomness from the secret input w [20].

III. PROPOSED TECHNIQUE

The main idea of the proposed technique is to use the PRNU fingerprint of the optical sensor of a user's device, e.g. a smartphone or a tablet, as a PUF for authentication. An overview block diagram is shown in Fig. 1.

In a first phase, the user enrolls into the system by providing a high quality estimate of the device fingerprint, obtained from a certain number of photos acquired in controlled conditions. Instead of directly sending the fingerprint, which usually consists in millions of real numbers, the user first compresses it by means of random projections. The user also stores some side information related to the seed of the pseudorandom number generator and the positions of the entries with largest magnitude (outliers) within those random projections, which will be then used in the authentication phase. The exact algorithm as well as the role of the outliers will be made clear in the following sections. At the server side, the compressed fingerprint is processed by a fuzzy extractor. Namely, the server extracts a uniformly random bit string from the compressed fingerprint and stores a secure hash of this bit string, together with a secure sketch of the fingerprint.

In the authentication phase, the user reproduces a noisy version of the device fingerprint by acquiring a fresh set of photos and compressing the resulting fingerprint according to the stored side information. The server then uses the fuzzy extractor scheme for reproducing the secret bit string from the received compressed fingerprint and the secure sketch, and

compares the recovered bit string with the stored secure hash. If the user provides a version of the compressed fingerprint sufficiently close to the enrolled one, then the server can reproduce the same bit string of the enrollment phase and grants access to the system; otherwise, it denies access.

With respect to existing authentication systems based on biometrics/PUFs and fuzzy extractors, the proposed technique introduces two important novelties. First, the actual PRNU-based PUF is obtained by means of a novel compression technique based on adaptive random projections. Besides re-ducing the size of the transmitted fingerprint, this technique provides an additional security layer, as will be discussed in the following sections. Secondly, the PRNU of a sensor is not a completely private information, since it can be approximated from public photos acquired by that sensor. In order to solve

VERIFICATION

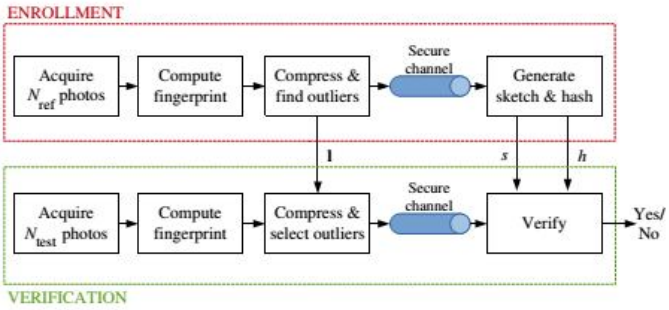

Fig. 1. System block diagram.

this problem, we introduce a novel fingerprint estimation technique that relies on RAW data acquired by the sensor, which is not usually available from public photos. Moreover, we design the fuzzy extractor in such a way that it is robust with respect to illegitimate fingerprints obtained from public photos. In the following sections, we will discuss the details of both PRNU-based PUF computation and user verification based on the proposed fuzzy extractor.

IV. PRNU-BASED PUF

This section describes in detail the client-side functional blocks introduced in the previous section concerning finger-print extraction and compression.

A. Fingerprint extraction

In order to devise a PUF for the authentication scheme, we propose to use high frequency components of the PRNU pattern estimated from RAW photos. The motivation is to obtain a fingerprint that is capable of discriminating different sensors and, at the same time, that is uncorrelated with any estimate that can be extracted from JPEG data. In the following we propose an extraction method from RAW images and then model JPEG images to devise an extraction method that better approximates the output of the extraction method from RAW images, in order to study an attack tailored to the proposed system. Since the RAW acquisition process can be controlled and the fingerprint extraction has to run efficiently on a user's smartphone, we suppose that the user acquires approximately flat images to streamline the extraction process.

1) Extracting high-frequency PRNU from RAW data: The process described in this section is summarized in Fig. 2. It is important to notice that since the authentication process relies on photos taken at that specific moment rather than using already available photos, the acquisition process can be controlled, i.e., it is possible to select the shooting parameters so to acquire photos that will yield the highest quality estimates of the PRNU. In particular, the exposure should be as high as possible without saturating the pixel values and the content should be uniform and possibly out of focus so that the scene can be well approximated by a constant value. Moreover, we can use a set of fixed values for ISO sensitivity, aperture, and focal length, so that different PRNU estimates will not be affected by those shooting parameters.

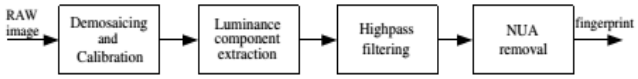

Fig. 2. Fingerprint extraction procedure.

The RAW image is first demosaiced and color calibrated to obtain image o = [r; g; b]. The luminance component of such image is then obtained by applying the transformation

= 0:299r + 0:587g + 0:114b :

It is possible to extract an estimate of the high-frequency components of the PRNU pattern to be used as fingerprint by means of a highpass filter (hereafter denoted as HPF) applied to the luminance component of the demosaiced and color calibrated image. This filter can be implemented as a product in the DCT domain. In Sec. VII we explore two possible solutions where the filtering is performed blockwise (to mimic JPEG), or on the whole image. Hence a first estimate of the fingerprint is:

k^{RAW} = HPF ( ) o^{id} HPF (k) + e^{0}: ----------(5)

Since the scene, represented by the term oid, is flat it is clear that a highpass version of the PRNU pattern is observed. When multiple images o(l) are available the fingerprint is jointly estimated as

$$\mathbf{k}^{\mathrm{RAW}} = \frac{\sum_l \mathbf{o}^{(l)} \cdot \mathrm{HPF}\left(\boldsymbol{\lambda}^{(l)}\right)}{\sum_l (\mathbf{o}^{(l)})^2}. \qquad (6)$$

in (1) we can approximate the image after JPEG compression, denoted as oJPG, as a lowpass filtered version of the original, where the cutoff frequency of the filter essentially depends on the compression quality factor. We denote such lowpass filter with LPF.

$$_{o}\mathrm{JPG} = \mathrm{LPF}\ {}_{o}\mathrm{id} + {}_{o}\mathrm{id}_{k} + e = \mathrm{LPF}\ {}_{o}\mathrm{id} + \mathrm{LPF}\ {}_{o}\mathrm{id}_{k} + e0:$$

Conventionally, one wants to estimate k by means of flat images so that oid const:, obtaining after denoising the noise residual

$$r = o^{id}\ \mathrm{LPF}\ (k) + e^{00}: \qquad (7)$$

It is clear that using flat images one can only observe a lowpass version of the PRNU pattern. However, if the image is not flat, the noise residual is

$$r = \mathrm{LPF}\ o^{id}k + e^{00}: \qquad (8)$$

The idea is to replicate the extraction procedure used for RAW data, i.e. highpass filtering, but on the noise residual since the attacker does not have control on the quality of the JPEG images and the flat assumption may or may not hold. First, the luminance noise residual is extracted, then it is filtered with the same highpass filter used to extract the RAW fingerprint and finally a weighted average as in (6) is performed if multiple images are available. Finally, mean removal and Wiener filtering are performed as post-processing operations. Notice that according to (8) the noise residual is a lowpass version of the PRNU modulated by the input image. If highpass filtering is performed one obtains

$$_{r}0 = \mathrm{HPF}\ \mathrm{LPF}\ {}_{o}\mathrm{id}_{k} + e\sim = F\ {}_{o}\mathrm{id}_{k} + e\sim:$$

This means that if the highpass filter is properly designed only a very weak signal can be observed due to the leakage of the combination of the two filters, represented by F . The experimental results show that higher correlation values can be achieved by this method instead of using the conventional method that does not include the highpass filter in the extrac-tion chain. Notice that this procedure is not optimal, as the optimal extraction method would retrieve HPF (k). However, this would require solving a challenging deconvolution prob-lem to disentangle the PRNU term from the image content in the observed LPF $o^{id}k$.

We remark that the existence of methods that improve the estimation of the high-frequency PRNU components beyond what we proposed in this section does not compromise the overall authentication scheme described in this paper. In fact, the legitimate user has full access to the RAW data provided by the device and can increase the difficulty of an attack by increasing the cutoff frequency of the filter or increasing the number of acquired photos to achieve arbitrarily high fingerprint quality levels.

B. Fingerprint compression

Since the fingerprint must be sent to a server for verification purposes, it is of paramount importance to compress it to a size that makes transmission over bandlimited channels manageable. The objective of the compression step is to transform the real-valued, high-dimensional fingerprint into a short binary code. Correlated fingerprints must be mapped into similar binary codes.

In Sec.II-C we presented binary-quantized random pro-jections, characterized by the property that their Hamming distance concentrates around the angle between the original uncompressed fingerprints. One can therefore use them to obtain compact binary codes. Since the fingerprints are high-dimensional objects, a complexity issue arises in the calcula-tion of the random projections. This can be solved by using circulant random matrices with randomized column signs, as shown in [14]. For such matrices, only the first row must be generated at random and the matrix-vector product can be efficiently performed using the FFT.

In this paper, however, we propose to use a modified version of such random projections, that we call adaptive random projections [29]. The key property of adaptive random projections is that some randomness is traded for a better (more compact) representation of signals correlated with a particular signal of interest. This solution has three main advantages in the context of the proposed user authentication system: more compact codes allow to save transmission time; more compact codes allow a more efficient and easier design of the fuzzy extractor at server side;adaptivity allows to preserve as much as possible of the inter-class correlation gap between fingerprints extracted from JPEG data and fingerprints extracted from RAW data; this also simplifies the design of the channel code in the fuzzy extractor because it

maximizes the margin between the bit-error probability observed by a legitimate user and that observer by an attacker.

During the registration phase, a high-quality version of the fingerprint k 2 Rn is available. A vector with n i.i.d. Gaussian entries is generated and circularly convolved with k using the FFT to implement a circulant sensing matrix. The result of this operation is first subsampled to keep the first

m_{pool} values. The $m < m_{pool}$ entries with largest magnitude are identified and their locations l stored locally on the userdevice as side information. Finally, the sign of the entries at those locations is saved as compressed fingerprint w of m bits. During the verification phase, a test fingerprint k^0 is presented for compression, and its projections are computed by keeping only the sign of the entries indexed by l.

The value of m_{pool} determines the storage overhead required for the location information. Choosing m outliers from a larger pool improves the adaptivity to the reference signal but increases the storage overhead. The effect of adaptivity is shown in Fig. 3 where the expected value of the Ham-ming distance between the binary codes is plotted against the correlation coefficient between the original uncompressed fingerprints. Notice that the adaptive method allows to achieve smaller values for the Hamming distance and maximize the margin between the class of invalid fingerprints having very low correlation values and the class of valid fingerprints having higher correlation values.

However, some artifacts may be present, either because of the blockiness introduced by a blockwise highpass filter or because of non-unique artifacts (NUA) [33] such as CFA interpolation, linear pattern, etc.. Such artifacts may introduce ambiguities in the camera detection process and should be removed. Hence, as a post-processing operation we remove row and column means in a checkerboard pattern and perform Wiener filtering to suppress any periodic artifact. Such post-processing operations are well known in the literature to suppress non-unique artifacts. Some cameras may provide cor-rections for optical distortions, typically involving a resampling step. Such artifacts are notably difficult to remove and lower the detection rate in camera identification applications [42],
[43]. However, since we access the RAW data before any kind of post-processing, our PRNU estimates will not contain this kind of artifacts.

2) Extracting high-frequency PRNU from JPEG data: The scope of this section is to develop a method to extract a fingerprint from JPEG images in such a way that it achieves the highest possible correlation with the fingerprint extracted from RAW data as described in the previous section. This method is what would be used by an attacker having access to publicly available JPEG images.

JPEG compression uses a quantization table in the discrete cosine transform (DCT) domain to shrink the coefficients in a way that preserves perceived visual quality. This typically results in many high frequency coefficients being set to zero, thus losing all the information associated to high frequencies. If we follow the usual model for the acquired image presented

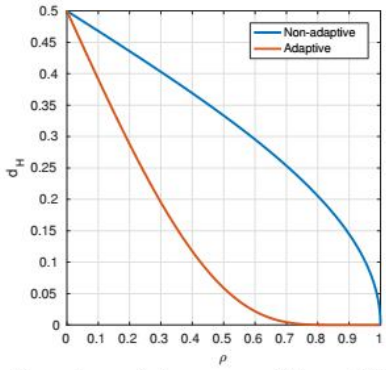

Fig. 3. Adaptive random projections. $m_{pool} = 2^{20}$, $m = 2^{15}$

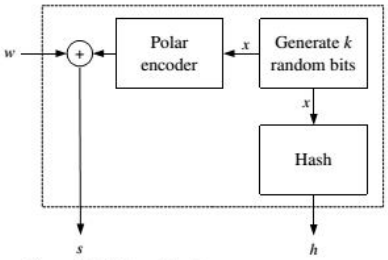

Fig. 4. Generation of sketch and hash.

V. CONCLUSION

In this paper, comparative studies of different controllers are studied and performance is evaluated according to time domain functions. It is observed that all controllers able to maintain the set point at the desired value but ZN-PID ,Fuzzy based controllers has slight overshoot, Model Reference Adaptive controller has no overshoot and settles quickly. So it conclude that Model Reference Adaptive Controller is the best controller then other controllers

V. USER VERIFICATION

Due to the non-exact repeatability of the PRNU fingerprint estimation procedure, during the verification phase the user will produce a compressed fingerprint that contains some bit errors with respect to the enrolled fingerprint. Moreover, an attacker having access to a certain number of

publicly available JPEG photos acquired by the user's device may also be able to provide a noisy version of the enrolled fingerprint, albeit with a much higher number of bit errors.

In order to cope with this scenario, we design a novel fuzzy extractor scheme. The proposed solution is based on the fuzzy commitment scheme proposed in [44] and a coding scheme for the wiretap channel that uses polar codes [45]. The proposed scheme is based on a generation function and a verification function, whose block diagrams are depicted in Fig. 4 and Fig. 5, respectively.

During the enrollment phase, the server generates a uni-formly random string x of k bits. From this secret string, the server computes a hash h = SH(x), where SH( ) denotes a secure hashing function, and a secure sketch s = w C(x), where w is the compressed fingerprint received from the user and C denotes a (m; k) error correcting code based on polar codes. The server then discards x and stores h and s.

During the verification phase, the server computes the k-bit string $x^0 = D(w^0 s)$, where w^0 is the noisy fingerprint and D denotes the decoding algorithm of the error correcting code, and authenticates the user only if $SH(x^0) = h$.

The error correcting code is not a standard (m; k) polar code, but is constructed according to the scheme in [45]. Let

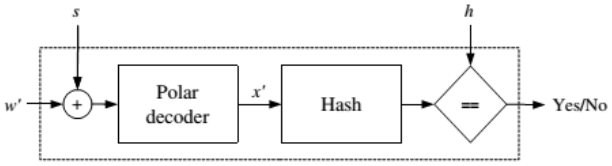

Fig. 5. User verification.

us assume a BSC-p_l for the legitimate channel and a BSC-p_a for the attacker channel, and denote them as Q(l) and Q(a), respectively. The code construction requires choosing security parameter $t > m(1 H_2(p_a))$, where $H_2(p) = p \log_2(p)$ (1 p) $\log_2(1 p)$ denotes the binary entropy function, and verifying that $k + t < m(1 H_2(p_l))$. Then,we define two subsets A_l and A_a A_l of the indices i = 1; : : : ; N satisfying

$$|\mathcal{A}_l| = k + t,\ \forall i \in \mathcal{A}_l, j \notin \mathcal{A}_l, Z(Q_i^{(l)}) \leq Z(Q_j^{(l)})$$
$$|\mathcal{A}_a| = t,\ \forall i \in \mathcal{A}_a, j \in \mathcal{A}_l \setminus \mathcal{A}_a, Z(Q_i^{(a)}) \leq Z(Q_j^{(a)})$$

The encoder generates t uniformly random bits r, assigns them to the bit channels in A_a, and maps the k message bits x onto the remaining channels in A_l n A_a. The code is then generated by using the corresponding rows in G_m. In order to take into account the randomization in the encoding process, in the following the encoder function will be denoted as C(x; r). The decoder simply applies the SCD to the received codeword and discards the t bits corresponding to A_a. It can be checked that the above construction verifies

VI. CONCLUSIONS

We projected a user authentication theme supported victimization the high-frequency parts of the PRNU pattern of optical sensors as a weak PUF. This was shown by experimentation to supply a fingerprint that can't be dependably extracted if solely JPEG compressed pictures area unit offered. Moreover, we tend to devised a sensible theme to transmit such fingerprint to a verification server. within the projected approach, the compression step is intimately joined to the server-side verification practicality enforced via a fuzzy extractor while not the necessity to directly store the fingerprint.

We showed that the system is demonstrably secure beneath dif-ferent attack situations. one among the assumptions created during this paper is that a user doesn't publically disclose RAW pictures nonheritable by the device to be used for authentication functions. this can be a quite affordable assumption since it's not common apply to try and do therefore, particularly for smartphones. all the same, the safety analysis shows that different components of the system like the random projection matrix will guarantee security albeit RAW pictures are leaked.

REFERENCES

[1] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication," Commun. ACM, vol. 58, no. 7, pp. 78–87, Jun. 2015.

[2] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, "Electronic authentication guideline," inNIST Special Publication 800-63-2, 2013.

[3] N. Haller, "The S/KEY One-Time Password System," Internet Requests for Comments, RFC Editor, RFC 1760, February 1995.

[4] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm," Internet Requests for Comments, RFC Editor, RFC 4226, December 2005.

[5] D. M'Raihi, S. Machani, M. Pei, and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm," Internet Requests for Comments, RFC Editor, RFC 6238, May 2011.

[6] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Commun. ACM, vol. 43, no. 2, pp. 90–98, Feb. 2000.

[7] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith, Secure Remote Authentication Using Biometric Data. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 147–163.

[8] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridg-ing the performance gap between theory and practice," IEEE Signal Process. Mag., vol. 32, no. 5, pp. 88–100, Sept 2015.

[9] C. Herder, M. D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," Proc. the IEEE, vol. 102, no. 8, pp. 1126–1141, Aug 2014.

[10] J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," IEEE Trans. on Inf. Forensics and Security, vol. 1, no. 2, pp. 205–214, June 2006.

[11] J. Fridrich, "Digital image forensics," IEEE Signal Process. Mag., vol. 26, no. 2, pp. 26–37, 2009.

[12] R. Caldelli, I. Amerini, F. Picchioni, and M. Innocenti, "Fast image clustering of unknown source images," in 2010 IEEE Int. Workshop on Inf. Forensics and Security, Dec 2010, pp. 1–5.

[13] C. T. Li, "Unsupervised classification of digital images using enhanced sensor pattern noise," in Proc. 2010 IEEE Int. Symposium on Circuits and Systems, May 2010, pp. 3429–3432.

[14] D. Valsesia, G. Coluccia, T. Bianchi, and E. Magli, "Compressed fingerprint matching and camera identification via random projections,"
IEEE Trans. on Inf. Forensics and Security, vol. 10, no. 7, pp. 1472– 1485, July 2015.

[15] ——, "Large-scale image retrieval based on compressed camera iden-tification," IEEE Trans. on Multimedia, vol. 17, no. 9, pp. 1439–1449, Sept 2015.

[16] J. Luka´s,˘ J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," in Electronic Imaging 2006, vol. 6072. Int. Society for Optics and Photonics, 2006, pp. 60 720Y–60 720Y–11.

[17] G. Chierchia, D. Cozzolino, G. Poggi, C. Sansone, and L. Verdoliva, "Guided filtering for PRNU-based localization of small-size image forgeries," in 2014 IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), May 2014, pp. 6231–6235.

[18] M. Goljan, J. Fridrich, and T. Filler, "Large scale test of sensor fingerprint camera identification," in Proc. SPIE, Media Forensics and Security, vol. 7254, 2009, pp. 72 540I–72 540I–12.

[19] J.-P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in International Conference on Audio-and Video-Based Biometric Person Authentication. Springer, 2003, pp. 393–402.

[20] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM Journal on Computing, vol. 38, no. 1, pp. 97–139, 2008.

[21] E. Quiring and M. Kirchner, "Fragile sensor fingerprint camera iden-tification," in 2015 IEEE Int. Workshop on Information Forensics and Security (WIFS), Nov 2015, pp. 1–6.

[22] M. Goljan, J. Fridrich, and M. Chen, "Defending against fingerprint-copy attack in sensor-based camera identification," IEEE Trans. on Inf. Forensics and Security, vol. 6, no. 1, pp. 227–236, March 2011.

[23] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," IEEE Trans. on Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 1892–1901, Dec 2006.

[24] A. B. J. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," IEEE Trans. on Syst., Man, Cybern., Part B, vol. 37, no. 5, pp. 1096–1106, Oct 2007.

[25] E. T. Anzaku, H. Sohn, and Y. M. Ro, "Multi-factor authentication using fingerprints and user-specific random projection," in 12th Int. Asia-Pacific Web Conf. (APWEB), April 2010, pp. 415–418.

[26] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representa-tions," IEEE Trans. on Pattern Anal. Mach. Intell., vol. 33, no. 9, pp. 1877–1893, Sept 2011.

[27] S. Shariati, L. Jacques, F. X. Standaert, B. Macq, M. A. Salhi, and P. Antoine, "Randomly driven fuzzy key extraction of unclonable images," in 2010 IEEE Int. Conf. on Image Processing, Sept 2010, pp. 4329–4332.

[28] T. Holotyak, S. Voloshynovskiy, O. Koval, and F. Beekhof, "Fast physical object identification based on unclonable features and soft fingerprinting," in 2011 IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), May 2011, pp. 1713–1716.

[29] D. Valsesia and E. Magli, "Binary adaptive embeddings from order statistics of random projections," IEEE Signal Processing Letters, vol. 24, no. 1, pp. 111–115, Jan 2017.

[30] I. Amerini, P. Bestagini, L. Bondi, R. Caldelli, M. Casini, and S. Tubaro, "Robust smartphone fingerprint by mixing device sensors features for mobile strong authentication," Electronic Imaging, vol. 2016, no. 8, pp. 1–8, 2016.

[31] J. Yan, "Novel security and privacy perspectives of camera fingerprints," in Twenty-fourth International Workshop on Security Protocols, April 2016.

[32] J. Luka´s,ˇ J. Fridrich, and M. Goljan, "Determining digital image origin using sensor imperfections," in Proc. SPIE Electronic Imaging, Image and Video Comm. and Processing, vol. 5685, 2005, pp. 249–260.

[33] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining image origin and integrity using sensor noise," IEEE Trans. on Inf. Forensics and Security, vol. 3, no. 1, pp. 74–90, March 2008.

[34] S. Bayram, H. Sencar, and N. Memon, "Efficient sensor fingerprint matching through fingerprint binarization," IEEE Trans. on Inf. Foren-sics and Security, vol. 7, no. 4, pp. 1404–1413, 2012.

[35] I. K. Fodor, "A survey of dimension reduction techniques," Center for Applied Scientific Computing, Lawrence Livermore National Labora-tory, vol. 9, pp. 1–18, 2002.

[36] W. B. Johnson and J. Lindenstrauss, "Extensions of Lipschitz mappings into a Hilbert space," Contemporary Mathematics, vol. 26, 1984.

[37] M. S. Charikar, "Similarity estimation techniques from rounding algo-rithms," in Proc. 34th Annual ACM Symposium on Theory of Comput-ing, ser. STOC '02. New York, NY, USA: ACM, 2002, pp. 380–388.

[38] A. Hinrichs and J. Vyb´ıral, "Johnson-Lindenstrauss Lemma for Circu-lant Matrices," Random Struct. Algorithms, vol. 39, no. 3, pp. 391–398, Oct. 2011.

[39] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," IEEE Trans. on Inf. Theory, vol. 55, no. 7, pp. 3051–3073, July 2009.

[40] R. Pedarsani, S. H. Hassani, I. Tal, and E. Telatar, "On the construction of polar codes," in Information Theory Proc. (ISIT), 2011 IEEE Int. Symposium on, July 2011, pp. 11–15.