AUTHENTICATION OF FINGERPRINT SCANNERS

Vladimir I. Ivanov and John S. Baras

Institute for Systems Research, University of Maryland, College Park, MD 20742, USA
{vivanov, baras}@umd.edu

ABSTRACT

Fingerprint scanners have unique patterns that can be used to distinguish one scanner from another one. The pattern, which we call *scanner pattern*, stems from the variability of device characteristics at silicon level and is caused by imperfections of the conversion from the input to the scanner (i.e., the object applied to it) to its output (i.e., the digital image). The scanner pattern is a sufficiently unique and persistent intrinsic characteristic of the fingerprint scanners even to those of the same technology, manufacturer, and model. We propose a simple and extremely accurate algorithm that is able to distinguish the pattern of one scanner from the pattern of another scanner of exactly the same model by extracting the pattern from a single image, acquired with each scanner. In this way, the scanner pattern can be used to enhance the security of a biometric system by authenticating the scanner, used to acquire a particular fingerprint image, and thus detect attacks on the scanner. Combining the biometric authentication with a scanner authentication leads to a two-part authentication, which we call *bipartite authentication*, that verifies both the identity of the user and the "identity" of the fingerprint scanner.

Index Terms— Authentication, biometric authentication, fingerprint scanner, pattern noise, scanner pattern.

1. INTRODUCTION

A fingerprint scanner essentially converts the biometric information, i.e., the surface or subsurface of the skin of a fingertip, into a digital signal, typically a digital image. In practice, this conversion process can never be perfect. The persistent and largely time-invariant part of the imperfections induced by the fingerprint scanner in this process we call *scanner pattern*. The process parameter variations in semiconductors [1] are indirect evidence for the existence of the scanner pattern.

The established term for the imperfections of interest in digital cameras is "pattern noise." A promising method, proposed in [2], for identifying digital cameras from images is based on one strong component of the pattern noise: the pixel nonuniformity noise (which is multiplicative to the signal). The reference pattern noise is computed by averaging noise residuals extracted with a wavelet-based denoising algorithm from the images. The image in question is denoised in the same way and its noise residual is compared with the reference noise pattern using correlation. Besides the large number of images required for computing the reference noise pattern (in the order of tens to a hundred), the algorithm is also very complex and computationally intensive. An enhancement of the described work is [3], where the identification problem is solved using a joint estimation-detection approach. An extension of [2] to flatbed desktop scanners is proposed in [4]. Another approach [5] characterizes the pattern noise of flatbed scanners using three groups of features that capture the statistics of: (a) the noise residual, (b) the subband wavelet coefficients, and (c) the prediction error in smooth regions. Principal Component Analysis is then applied to the resulting 60 features, and Support Vector Machines are used for classification. Studies also have been done on identifying cameras in cell phones using binary similarity measures, image-quality measures, and higher order wavelet statistics [6].

The only work on identifying biometric scanners the authors are aware of is [7], where Barlow *et al.* applied the algorithm for identifying digital cameras proposed in [2] to 16 optical and 4 capacitive fingerprint scanners. Although they used many images from several subjects, generalizing their approach as a solution for fingerprint scanner identification is difficult because the maximum number of scanners of the same technology, manufacturer, type, and model was only 3 (optical scanners, in two of their sets). Two of the 3 capacitive scanner brands used were from the same manufacturer, but of different models, and only 2 of the 4 capacitive scanners were of the same model. Since the algorithm (of [2]) has been developed for digital cameras, its high accuracy when applied to optical scanners is not surprising. The highest accuracy reported for optical scanners using a single image for computing the noise reference pattern was 99.65%; however, most of the errors in the confusion matrix were among scanners of the same (optical) model. In the other dataset they used, to achieve accuracy of 98%, 64 training images were needed; with a single training image, the accuracy dropped to 85%. But the most problematic is their third dataset where even for

Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

optical scanners (of the same model), there were many identification errors, and the overall accuracy with a single training image dropped to 45%. Reasonable accuracy was achieved with 128 training images, but even there, it was below 90%. Clearly, these results cannot serve as proof for the ability of the algorithm of [2] to identify individual fingerprint scanners of the same model, especially when only a single training image is available and within a large pool of scanners. One possible explanation is that the image acquisition process in capacitive fingerprint scanners is very different from that of optical scanners [8] (and in digital cameras in this respect), for which reason the assumption that the algorithm of [2] can detect and extract photo-response nonuniformity noise in capacitive fingerprint scanners is not plausible.

In this paper, we propose a simple, yet extremely accurate algorithm that is able to distinguish one fingerprint scanner from another scanner of exactly the same manufacturer, type, and model using only a single image, acquired with each scanner. The algorithm extracts scanner patterns from the two images using wavelets, selects parts of these patterns, and computes the correlation coefficient as a similarity score between them. We tested the algorithm with 2,160 images acquired with 24 capacitive fingerprint scanners of exactly the same model, and based on the histograms, we compute a decision threshold and estimate the equal error rate. The proposed algorithm can be used to enhance the security of a biometric system by authenticating the scanner that acquired a specific fingerprint image, e.g., by detecting an attack on the scanner, which is one of the possible attacks on biometric systems [9]. Combining biometric authentication with scanner authentication leads to an improved, two-part authentication, which we call *bipartite authentication*, that verifies both the identity of the user and the "identity" of the fingerprint scanner.

2. ALGORITHM

The scanner pattern, as an intrinsic characteristic of the conversion process that changes very little over time, can be a function of many and diverse factors, e.g., the specific sensing method, the silicon technology being used, the chip layout, the circuit design, and the post-processing. Furthermore, pinpointing the exact factors, much less quantifying them, is difficult because such information is proprietary. Nevertheless, our general observation is that the scanner pattern is mainly caused by non-idealities and variability in the sensing matrix and the subsequent signal processing within the fingerprint scanner. Finally, the exact relationship between the fingerprint pattern and the scanner pattern in the composite signal (the digital image), can be very complex, mathematically intractable, or even impossible to determine because it is specific for the scanner manufacturer and usually proprietary.

We propose the following 3-step algorithm using wavelets for scanner pattern extraction and correlation coefficient for matching. Let $g_e(i,j)$ and $g_q(i,j)$ be the pixel values at row i and column j of the two acquired images, where the subscript e (from *enrolled*) refers to one of the two images and the subscript q (from *query*) to the other image. This referencing is conditional because all processing is the same for each image.

1. *Wavelet extraction.* Each image is decomposed using 2D wavelets and then reconstructed by setting the LL-subband coefficients to 0, yielding the signals $n_e(i,j)$ and $n_q(i,j)$. The biorthogonal wavelets with decomposition order 5 and reconstruction order 1 gave the best results, but other wavelets, e.g., Daubechies or symlets, both of order 2 (4-tap filter length), also work well.

2. *Masking.* We observed that selecting only some of the pixels based on the magnitude of their values from $n_e(i,j)$ and $n_q(i,j)$ is necessary. Therefore, the signal $s_e(i,j)$ (and similarly $s_q(i,j)$) is constructed using:

$$s_e(i,j) = \begin{cases} n_e(i,j) & \text{if } |n_e(i,j)| \le \theta \\ NU & \text{otherwise} \end{cases} \tag{1}$$

   where NU denotes a mark that the corresponding pixel will not be used for further processing. We achieved the best results with $\theta = 4$, but 3 or 5 is also possible.

3. *Correlation matching.* We propose using the correlation coefficient as a matching score because it is a simple and robust method for measuring the strength of linear relationship and has been already used in similar context [2, 7]. Furthermore, correlation is the optimal method (that minimizes the probability of error) for detecting signals in presence of additive white Gaussian noise; it is also the conventional method for detecting digital watermarks. Thus, the matching score is:

$$corr(\mathbf{t_e}, \mathbf{t_q}) = \frac{(\mathbf{t_e} - \bar{\mathbf{t_e}}) \cdot (\mathbf{t_q} - \bar{\mathbf{t_q}})}{\|\mathbf{t_e} - \bar{\mathbf{t_e}}\| \, \|\mathbf{t_q} - \bar{\mathbf{t_q}}\|}, \tag{2}$$

   where $\mathbf{t_e}$ and $\mathbf{t_q}$ are vectors derived from $s_e(i,j)$ and $s_q(i,j)$, respectively, by taking only the common useful pixels (i.e., the pixels marked with NU are discarded) and then ordering the common useful pixels in vector form. $\bar{\mathbf{t_e}}$ and $\bar{\mathbf{t_q}}$ are the means of the elements of vectors $\mathbf{t_e}$ and $\mathbf{t_q}$, respectively. The decision is match if $corr(\mathbf{t_e}, \mathbf{t_q})$ is greater than a predetermined decision threshold (discussed in Section 4).

3. RESULTS

We acquired raw images with 24 TouchChip® scanner modules of UPEK, all using TCS1 sensors – the only capacitive (and generally solid-state) fingerprint sensors that are FIPS-201 certified. With each scanner, we acquired 30 images for three fingers: an index, thumb, and little finger of one person, with each set having $(24 \cdot 30) = 720$ images per finger, giving a total of $(3 \cdot 720) = 2,160$ images for all 3 fingers. Each image has $360 \cdot 256$ pixels, with pixel values from 0 to 255.

3.1. Images of one and the same finger

We first applied the algorithm to images with fingerprints of one finger, for which we chose the index finger because typically it is used for biometric authentication. For $g_e(i,j)$ and $g_q(i,j)$, we chose each of the 720 images in the set, yielding to $720(720+1)/2 = 259,560$ comparisons. The normalized (integrating to 1) histograms of the self correlation coefficients (the two images were acquired with the same scanner) and cross correlation coefficients (the two images were acquired with two different scanners) are shown in Fig. 1.

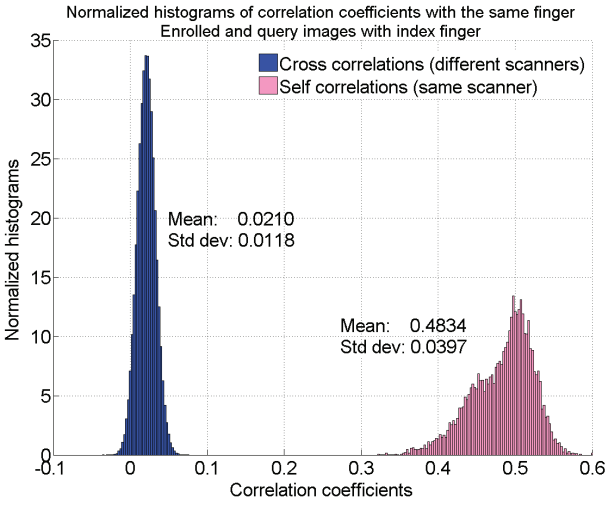

Fig. 1. Normalized histograms of the correlation coefficients when both $g_e(i,j)$ and $g_q(i,j)$ are with index finger

3.2. Images of two different fingers

To demonstrate that the proposed algorithm does not depend on the finger, next we applied it to two images where one of them contains one finger and the other image contains a different finger. It is known that thumbs typically have much wider ridges and valleys than little fingers (of the hands of one and the same person). Also typically, index fingers have narrower ridges and valleys than thumbs, and wider than little fingers. The histograms of the correlation coefficients where $g_e(i,j)$ are images with the index finger and $g_q(i,j)$ are images with the thumb are shown in Fig. 2, and the results where $g_e(i,j)$ are images with the thumb and $g_q(i,j)$ are with the little finger are shown in Fig. 3. As in Section 3.1, each set for a finger contains 720 images, thus yielding $(720 \cdot 720) = 518,400$ comparisons in each case (because here the two fingers are different). Since all processing is symmetric, the choice which finger is in $g_e(i,j)$ and which in $g_q(i,j)$ is immaterial.

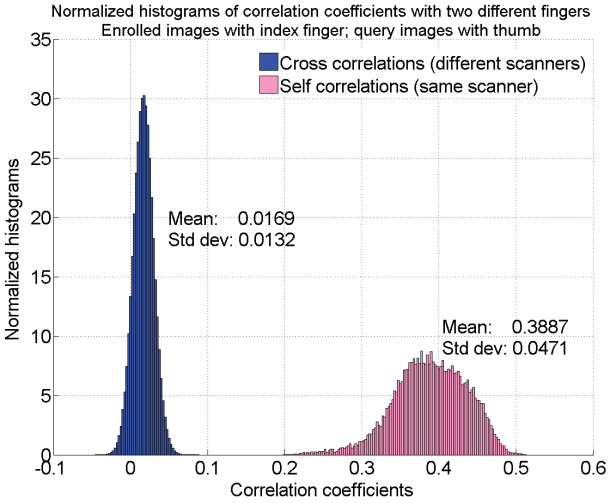

Fig. 2. Normalized histograms of the correlation coefficients when $g_e(i,j)$ is with index finger and $g_q(i,j)$ is with thumb

4. DECISION THRESHOLD AND ERROR RATE

No decision errors were registered for any of the 1,296,360 comparisons, which is also visible from the clear separation of the histograms in the three figures. We computed an estimate for the Equal Error Rate (when FAR = FRR) for the third case (which is the worst one of the three) by fitting Gaussian PDFs (see Fig. 3). The histogram with cross correlation coefficients fits extremely well with $N(0.0145, 0.0124^2)$, and $N(0.3646, 0.044^2)$ well approximates the histogram with self correlation coefficients. Based on the fitted PDFs and the computed decision threshold of 0.0915, the EER is $2.8 \cdot 10^{-10}$.

5. APPLICATION: BIPARTITE AUTHENTICATION

The proposed algorithm, based on extracting and matching the scanner pattern, can be used to verify the authenticity of a fingerprint scanner, i.e., to authenticate the scanner and detect attacks on the scanner, e.g., a malicious scanner replacement or replay at the output of the scanner of a stolen image of the authentic fingerprint [8]. This type of attack is becoming increasingly feasible in portable devices (e.g., PDAs, smart phones, and even laptops) because they can be easily stolen, giving the attacker physical access to them and thus the ability to launch so powerful an attack. The scanner authentication consists of:

- *Scanner enrolment*: extracting and recording the scanner pattern of the legitimate, authentic fingerprint scanner from one (or more) images;
- *Scanner verification*: extracting the scanner pattern from a query image, comparing it to the scanner pat-

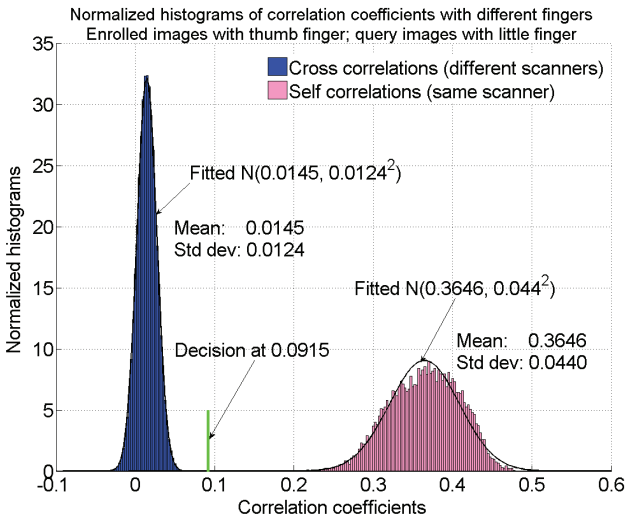

Fig. 3. Normalized histograms of the correlation coefficients when $g_e(i,j)$ is with thumb and $g_q(i,j)$ is with little finger

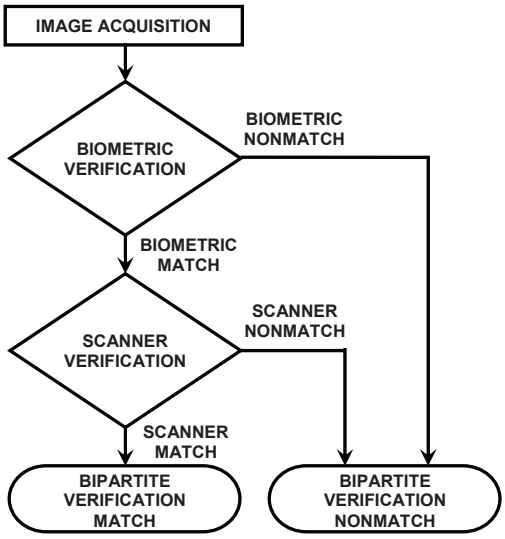

Fig. 4. Flow diagram of the bipartite verification

tern of the authentic scanner, and outputting a *scanner match* decision if the two scanner patterns are sufficiently similar.

We hereby introduce the term *bipartite authentication* to denote the combination of a biometric authentication and a scanner authentication, consisting of *bipartite enrolment* and *bipartite verification*, an example flow diagram for which is shown in Fig. 4. The biometric verification and the scanner verification operate on the same image. To improve the performance, similarly to biometric enrolments, several images (e.g., 3) can be used for scanner enrolment. For a given (single) query image, the correlation coefficient of each pair {enrolled image, query image} is computed and then their average is compared with the decision threshold.

6. DISCLAIMER

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government.

7. REFERENCES

[1] Patrick Drennan, "Device mismatch in bicmos technologies," in *Proceedings of the 2002 Bipolar/BiCMOS Circuits and Technology Meeting*, Sept. 2002, pp. 104–111.

[2] Jan Lukas, Jessica Fridrich, and Miroslav Goljan, "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, June 2006.

[3] Mo Chen, Jessica Fridrich, Miroslav Goljan, and Jan Lukas, "Determining image origin and integrity using sensor noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, Mar. 2008.

[4] Nitin Khanna, Aravind K. Mikkilineni, George T. C. Chiu, Jan P. Allebach, and Edward J. Delp, "Scanner identification using sensor pattern noise," in *Proceedings of SPIE Security, Steganography, and Watermarking of Multimedia Contents IX*, Jan. 2007, p. 65051K (2007).

[5] Hongwei Gou, A. Swaminathan, and Min Wu, "Intrinsic sensor noise features for forensic analysis on scanners and scanned images," *IEEE Trans. on Information Forensics and Security*, vol. 4, no. 3, pp. 476–491, Sept. 2009.

[6] Oya Celiktutan, Bulent Sankur, and Ismail Avcibas, "Blind identification of source cell-phone model," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 553–566, Sept. 2008.

[7] Nick Bartlow, Nathan Kalka, Bojan Cukic, and Arun Ross, "Identifying sensors from fingerprint images," in *2009 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, June 2009.

[8] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar, *Handbook of Fingerprint Recognition*, Springer, London, 2nd edition, June 2009.

[9] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, June 2006.