International Journal of Emerging Technology and Innovative Engineering
Volume 4, Issue 2, February 2018 (ISSN: 2394 – 6598)

Paper Received on: 23.02.2018
Paper Published on: 24.02.2018

MULTI-BIOMETRIC AUTHENTICATION PROTOCOL FOR SMARTPHONES

Sherif T. Amin
Faculty of Computer Science and Information Systems
Jazan University, Jazan, KSA, PO Box 45142
sherif.t.amin@gmail.com

ABSTRACT

Smartphones are increasingly used for different digital services such as social networks or e-commerce. User authentication using passwords on these devices is not friendly enough and does not offer a high level of security to the users. Voice biometrics can provide a popular solution to achieve a high level of security and privacy with the integration of smartphones' fingerprint sensors. We propose in this paper a new protocol combining fingerprint and voice biometrics to improve users' authentication security while maintaining ease of use and respect to privacy. The voice biometrics captured through an authentication word in addition to the authentication fingerprint is considered an effective method for quick authentication. We believe that the proposed solution offers many advantages in terms of security, with respect to privacy. We show through the experimental results the effectiveness of the proposed method even in case of attacks.

General Terms

Pattern Recognition, Security, Biometrics.

Keywords

Authentication, Speaker Recognition, Privacy.

1. INTRODUCTION

A recent survey in 2016 [1] showed that more than 50% of smartphone users are using it immediately after they wake up in the morning. As smartphones integrate more and more personal information (contacts, mail content, media…etc) they become privileged devices for remotely accessing services and storages, this type of information sensitivity handling demands strong authentication for the users. PIN authentication is a modest solution to this kind of problem, nevertheless, it does not constitute a solid proof of identity because it is easy to circumvent. In order to solve this problem, biometrics is increasingly used to increase the level of users' authentication trust. Nevertheless, the biometric data is sensitive and require special attention in terms of security with respect to privacy. The protection of biometric data must be performed during the data life cycle, from storage to manipulation. The standard cryptography will not be able to ensure the data protection during the necessary comparison step (decryption). Several solutions are proposed in literature to ensure protection of biometric data protection either by using crypto-biometrics algorithms [2, 3] or transformation algorithms [4, 5]. In general, biometric authentication is carried out in two steps: enrollment and verification. The first step is to generate the user's biometric reference and then store it. During the verification step, the scanned biometric template is compared against the biometric reference of the alleged individual under authentication verification. User authentication security improvement requires the combination of more than one authentication factor. This can be achieved using different biometrics data to define a multi-biometric system. Our main contribution in this paper is a multi-biometric system that is effective and usable for the improvement of smartphones' user authentication security. We combine two biometrics modalities, namely fingerprint and voice biometrics. We assume in this work that the smartphone used has a fingerprint sensor. This hypothesis is considered to be true because a recent survey estimates that 67% of

smartphones in 2018 will have a fingerprint sensor [7]. The individual's fingerprint reference is encrypted and stored in the smartphone's secured element to ensure its protection. We also use a voice biometric authentication mechanism (how to capture the pattern that combines voice & speech) with a pattern protection scheme. This solution has the advantage of being very simple to use and very fast. The biometric reference is stored in the protected element of the smartphone in the form of a BioCode (binary code linked to the biometric data) this code is revocable in case of attack. This paper is organized as follows. Section 2 provides a brief state-of-the-art voice & speech recognition solutions for user authentication on a smartphone. The proposed method is described in Section 3. Section 4 illustrates the performance of our proposed solution from experimental results. Finally, we conclude and give perspectives in section 5.

2. PREVIOUS WORK

Biometric authentication in smartphones is an emerging problem with relatively increasing patterns. A NIST report [8] proposes several recommendations concerning the acquisition of biometric data on smartphones and considers the following modalities: face and iris digital signatures. Most literature papers are devoted to a particular modality, for example, the references [9, 10] on the speaker recognition, other articles [11, 12] deal with recognition based on keystrokes dynamics. Many articles offer to capture biometric data provided from the tactile capabilities of the touch screen [13]. Most of these studies use methods used for keystrokes or signature dynamics. For example, the concept of TapPrint which was proposed by Miluzzo et al. [14] generalizes the notion of keystroke dynamics over the tactile characteristics of the touch screen. The proposed method was based on exploiting smartphone's accelerometer behaviormetrics data collected during entering text on a touch screen. The effectiveness of recognition is understood between 80% and 90%. The work done by Luca et al. [15] is very interesting because it combines the password-based pattern and biometrics. They proposed a system and have it tested with 34 users. They got a performance 19% for FRR (False Rejection Rate) and 21% for the FAR (False Acceptance Rate). In 2013, a method has been proposed [16] combining several information with the correlation factor or the Dynamic Time Warping DTW as a similarity measure method. The Equal Error Rate (EER) was close to 17%. Many solutions related to biometric smartphone authentication problems with specific modalities are provided in [17, 18]. Even though the use of several biometric modalities can limit the error rate (including the False Acceptance Rate), the use of additional biometric data poses privacy protection problems. Few contributions consider this problem on smartphones. As previously mentioned we propose a new authentication solution combining the fingerprint and the identification of speaker with his specific password pronunciation. The first modality is present in the most smartphones and the biometric reference model is securely stored in a secure item. Using the approach of speaker identification and his biometric password pronunciation signature allows to improve the level of security while providing a practical (fast interaction) and easy to protect authentication solution.

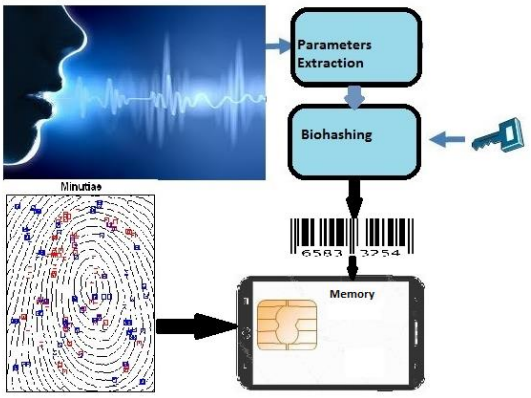


Fig. 1: User Enrollment

3. PROPOSED METHOD

The general principle of the proposed method is given in Figures 1 and 2. During the enrollment phase, the user needs to provide his or her fingerprint to the smartphone's sensor in order to generate its reference template. The calculated model (all the minutiae detected) will be stored on a dedicated secure element. The user must also speak his or her private password through the smartphone's microphone. The application extracts several parameters according to his or her biometric pronunciation of the access password (pitch, emotions, speaking style etc.), Figure 3 shows the steps followed to identify a speaker.

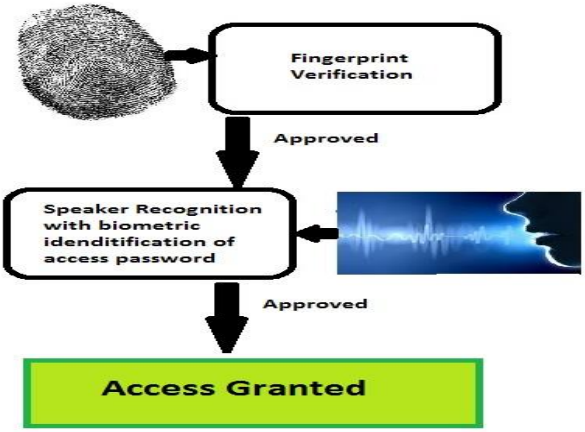


Fig.2: Muli-Biometric Verification

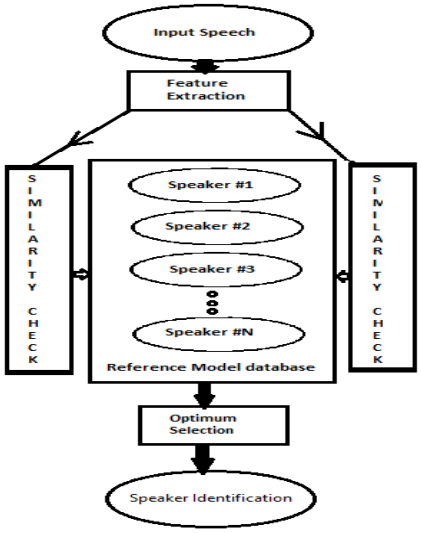


Fig. 3: Speaker Identification

We then use the BioHashing algorithm to protect this model. For this algorithm, we need a secret key to be able to revoke the BioCode generated in case of attack. This secret key can be a binary representation of the password uttered and can be concatenated with other information such as the IMEI number of the smartphone (smartphone identifier. During the verification phase, the user must provide his fingerprint to authenticate himself. The fingerprint captured is compared to user's stored reference in the secure element of the smartphone. If his identity is checked, he then proceeds to the next step which is his or her spoken password or passphrase. The speaker verification part is shown in Figure 4. In both phases a BioCode is calculated and compared to the reference user's BioCode in the smartphone. If both biometric systems accept the user's inputs, he or she will be authenticated. We do make an authentication based on a decision fusion (not having access to the comparison score of both biometric algorithms).

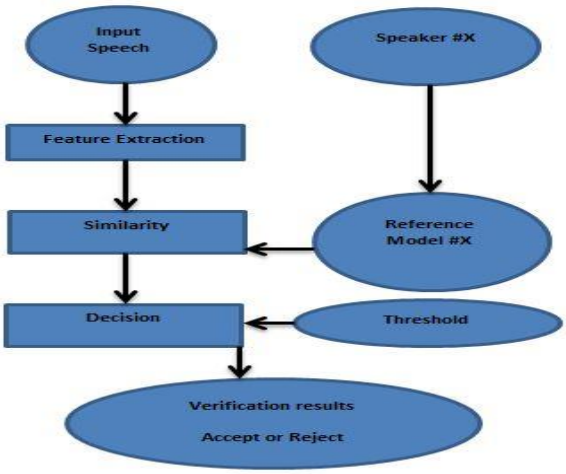


Fig. 4: Speaker Verification

3.1 Fingerprint Verification

In this paper we proposed the fingerprint's digital imprint as the first biometric modality. Most smartphones integrate a fingerprint sensor. The legitimate user of the smartphone must enlist first by providing one or more captures of his or her fingerprint. The reference model (a set of minutiae) is stored in the secured element (SE) which is usually incorporated within the smartphone or the fingerprint sensor. The comparison score between a new fingerprint capture and the model of the user's reference is also computed within the SE and a decision value is provided (the score will not be available for safety reasons). Concerning privacy, this solution is appropriate, because the biometric reference is stored in the SE. In terms of security, the solution is also interesting even if the enrollment process is carried out by the user which usually registers his fingerprint in non-controlled environment. We can expect that a smartphone is a personal object; the enrollment process should be done by the smartphone's owner. As for performance, it is described by the value of the False Acceptance Rate (FAR) corresponding to the percentage of successful attacks by an impostor. For smartphones, the FAR targeted level is 0: 005% [19], corresponding to the security level 3. It is difficult to verify this value without obtaining the score provided by the corresponding algorithm. The False Rejection Rate (FRR) corresponding to the recognition problems of the legitimate users is supposed to be less than 2 %. No studies related to the evaluation of state of the art commercial fingerprint sensors on smartphones are currently available due to the non-availability of a large number of users to provide meaningful results.

3.2 Speaker Recognition

The biometric system we propose to use in this study aims to increase security for a fast logical access control on a smartphone. We propose to recognize the legitimate user by verifying a password uttered by him. This approach to enter a password using voice rather than touch screen is faster and friendlier for a smartphone device. Secondly, the behavior of the user when uttering his password will be analyzed. Many information can be collected during the capture process such as:

- What is being said,
- What language is being spoken,
- Who is speaking,
- Gender of the speaker,
- Age of the speaker,
- Emotion,
- Stress level
- Cognitive load level
- Depression level
- Is the person sleepy
- Is the person sober or not.

In this study, we used a frame by frame feature extraction system to make a digital reference of the

voice signature. We took the password speech (amplitude vs time) parsed it into a feature extraction model which was from 20 to 30 milliseconds frame, with a shift of 10 milliseconds. We had a Universal Background Model UBM which incorporated an abundant number of speakers classified based on gender, and we also had a speaker model which incorporated speakers' password speeches which needs to be verified. We compared each speaker model against the extracted features to determine the level of match then we worked out what is going to be the likelihood of being the legitimate user. Then for the same user we determine the level of match against the universal background model UBM to determine what the likelihood of this person being a male or a female to be. After that we make a decision between both likelihoods (the speaker model and universal background model) by computing the likelihood ratio. .

3.3 BioHashing Protection

The Biohashing algorithm being applied on the speech biometric modalities, in which its data were represented by a fixed length vector of real numbers generates a binary model called BioCode of length less than or equal to the vector's original size. This algorithm was originally proposed for the face and the fingerprints digital imprints by Teoh et al. in [4]. The Biohashing algorithm can be applied on all biometric modalities, which can be represented by a fixed length vector of real numbers. This transformation requires a secret related to the user. The comparison of BioCodes is performed by calculating the Hamming distance. The Biohashing algorithm transforms the biometric model

$T = (T_1 \dots T_n)$ into a binary model $B = (B_1 \dots B_m)$ called BioCode where with $m \leq n$, as follows:

1. m orthonormal random vectors $V_1 \dots V_m$ of length n are generated from a secret random seed server (typically with the Gram Schmidt algorithm).
2. For $i = 1, \dots, m,$, we calculate scalar product $x_i < T, V_i >$
3. We compute the BioCode $B = (B_1 \dots B_m)$ with the quantification process:

$$B_i = \begin{cases} 0 & if\ x_i < \tau \\ 1 & if\ x_i \geq \tau \end{cases}$$

Where τ is a given threshold, usually equal to 0 .

The performance of this algorithm is provided by the scalar product with orthonormal vectors, as it is detailed in [20]. The quantification process guarantees the non-reversibility of data (even if $n = m$) because each coordinate of the input T is a real value, while the BioCode B is binary. Finally, the random seed guarantees both diversity and revocability properties.

4. SYSTEM VALIDATION

In this section, we present our experimental results for the validation of the proposed system.

4.1 Experimental Details

The protocol followed in this study is as follows, we first used a set of biometric data captured when the user utter a secret password. The data was collected on a Samsung Note 4 smartphone. The speakers utter the same unique passwords several times as well as many "impostor" speakers (the same password provided by the impostor speaker). 50 users have participated in this experiment each provide 4 unique utterances of the same password. This experimental configuration can be considered the worst case where an attacker knows the uttered password. The 50 users provided 4 passwords' utterance described by 10 subsampled signals at 600 values (time normalization). We have also added the total time to utter the password. So the size of the biometric model is 6000 (concatenating all the signals sub-sampled and the input time). In total, we have a subset of 50 times 4 = 200 biometric captures 6000 with real values for the Biometric model. Given the configuration of BioHashing, we define the parameter values as follows:

- Size of the input parameters: n = 6000,
- Size of BioCode: m = 850 (arbitrary choice, it takes m <n to guarantee non- reversibility),
- As the uttered password is the same for all users, in the calculation of the reference BioCode the pattern code will be the same for all users
- Comparison algorithm: Hamming distance.

With regard to the fingerprint, we used the fingerprint databases FVC2002 DB2, FVC2004 DB1 and FVC2004DB3 [21]. Figure 5 shows an image of each database. We can see that the fingerprints are very different and representative of the different types of fingerprints (acquired with sensors using different technologies). These databases have fingerprints of 100 individuals with 8 samples per person. In order to implement multi-biometric database we took into consideration the fingerprints of the first 50 individuals. For each FVC dataset, we have 50 × 10 = 500 fingerprint samples.

(a) *(b)* *(c)*

Fig. 5: Database used: (a) FVC2002 DB2,

(b) FVC2004 DB1, (c) FVC2004 DB3

In order to evaluate the performance of the proposed method, we used the following methodology. We used the first fingerprint sample of each user as a model reference, concerning the uttered password data; we used it to calculate the reference BioCode. As we do not have access to the value of the digital impression

generated by the fingerprint sensor (that is, the value of the corresponding score), we simulate the result of the score by considering the algorithm Bozorth3 provided by NIST [22]. This algorithm does not does not provide a performance equivalent to commercial comparison algorithms, therefore the performance is underestimated. We calculated the legitimate results as following. We consider all the reference fingerprints and we compare them with each sample available belonging to the same individual. We consider twice these scores because the biometric model has 20 samples. For the biometric password, we compare the reference Biocode with all other BioCodes of the same individual. We are getting $20 \times 50 = 1000$ legitimate scores for each base FVC data. We have a similar process to simulate an impostor attack by considering all biometric samples belonging to another user. We get $20 \times 50 \times 49 = 49000$ legitimate scores for each FVC database. Given these two sets of scores we can calculate their distribution in order to estimate how much the scores imposters are different from legitimate ones. Secondly, we calculate the value of the Equal Error Rate (EER) which is a well-known measure in biometrics that measures the behavior of the biometric system when the threshold of decision is configured to have the same rate value for both False Rejection Rate (FRR) and False Acceptance rate (FAR).

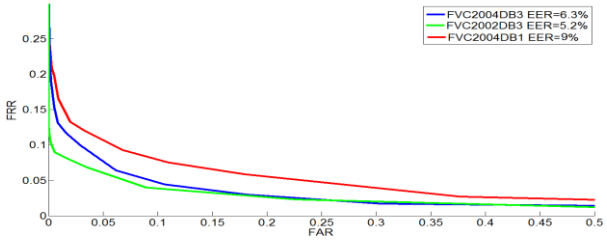
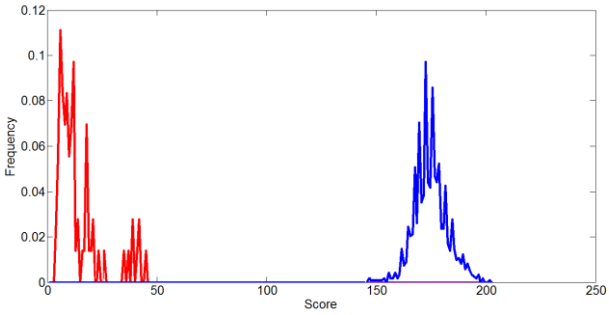


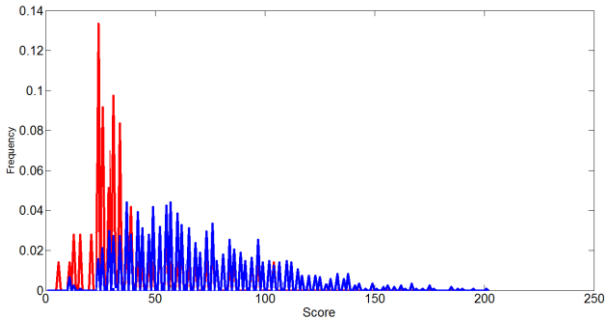
Fig. 6: EER fingerprints recognition performance curve for the 3 FVC databases

4.2 Results

First of all, we try to estimate the effectiveness of every biometric system that we combine. The Figure 6 provides the Equal Error Rate curves of the fingerprint system on the three databases. The EER value is between 5.2% and 9 %. We could expect using a commercial system to have a significantly better performance; this value estimates an upper bound of the error. Concerning the recognition performance of biometric password, with a simple Euclidean distance, we get an EER of 27.7%. By applying BioHashing in the best case (password only known by the legitimate user), we get almost perfect recognition with an EER value of 0.005% (see Figure 7). In the worst case (password known by the impostor), the performance is similar to that one obtained without protection. Figure 8 provides the distribution of the scores by combining the fingerprint and the biometric password in the best scenario. We get for each one a perfect recognition for all databases fingerprint. This is obviously excellent results and these results improve by applying only the fingerprint system (see Figure 6). Now, we have to consider the worst case scenario when the impostor has obtained the spoken password associated with the algorithm of BioHashing.



(a)



(b)

Fig 7: Distribution of scores after protection (a) without attack, (b) binary secret key known

We assume that the threshold for the fingerprint system is the one associated with the EER value. For example, for the FVC2004DB1, we get a FAR equal to 9%. We set the threshold value for the biometric password with the same approach. We calculated the False Acceptance Rate in the worst case situation and it's worth 29.8%. This means that if the imposter knows the password, it has a 29.8% chance of breaking the system. Considering the multi-biometric system, he has 9% chances to break the fingerprint system (on FVC2004DB1) and 29.8% for the biometric password. Because these events are independent, we can estimate the False Acceptance Rate (FAR) of the multi-biometric system on FVC2004DB1 at $9\% \times 29.8\% = 2.7\%$. For all fingerprint data sets, the FAR is between 1.5% to 2.7% for the multi-biometric system if the impostor knows the password, and the binary secret key. We can consider this result as very interesting considering all the information necessary to the impostor for this attack are available (temporary possession of the phone, having a fingerprint almost identical to that of the legitimate user, knowledge of the password, the same voice pattern, and the binary secret key).

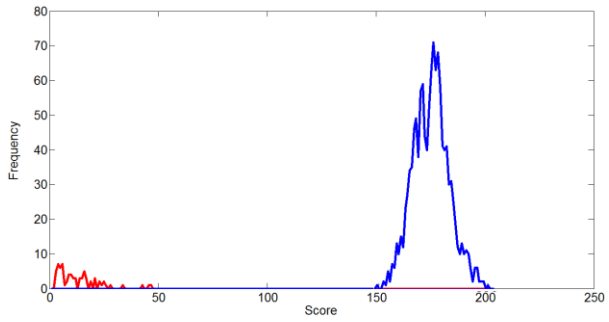


Fig. 8: 2002DB3 Multi-biometric system scores distribution

5. CONCLUSION AND PERSPECTIVES

In this paper, we proposed a multi-biometric authentication system for smartphones by combining fingerprint recognition and a biometric speaker identification system. The proposed system is very fast and easy to use for users, as all of these verification systems are commonly used. The use of fingerprint recognition makes it possible to limit possible attacks if both the uttered passwords and its associated BioHashing generated binary secret key were obtained by the impostor. The use of the second biometric system increases the security of user authentication. In the best case, we get a perfect recognition on the databases tested and a False Acceptance Rate lower than 2.7% in the worst case (the impostor must have access to the smartphone, knows the password and its associated binary secret key generated by the BioHashing algorithm). In the future, we intend to integrate other biometric systems such as facial recognition systems.

6. ACKNOWLEDGMENTS

I would like to express my thanks to all students, faculty members, vice dean and honorable dean of the Faculty of Computer Science and Information Systems at the University of Jazan. In addition, I would like to extend my warmest gratitude to the respected rector of the University well, without their cooperation and support; this study could not have been completed and published.

7. REFERENCES

[1] Ramona Sukhraj. 31 mobile marketing statistics to help you plan for 2017, 2016.

[2] H. Chabanne, J. Bringer, G. Cohen, B. Kindarji, et G. Zemor. Optimal iris fuzzy sketches. Dans IEEE first conference on biometrics BTAS, 2007.

[3] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva, et Fabio Scotti. A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates. Dans BTAS 2010, 2010.

[4] A.B.J. Teoh, D. Ngo, et A. Goh. Biohashing : two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition, 40, 2004.

[5] A. Nagar, K. Nandakumar, et A. K. Jain. Biometric template transformation : A security analysis. Proceedings of SPIE, Electronic Imaging, Media Forensics and Security XII, 2010.

[6] C. Rathgeb et A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. on Information Security, 3, 2011.

[7] Statista. Penetration of smartphones with fingerprint sensors worldwide from 2014 to 2018, 2016.

[8] S. Orandi et R. M. McCabe. Mobile id device. best practice recommendation. NIST Special Publication 500-280, 2009. Available from : http ://www.nist.gov/itl/iad/ig/upload/MobileIDBPRS-20090825-V100.pdf.

[9] A. Kounoudes, A. Antonakoudi, V. Kekatos, et P. Peleties. Combined speech recognition and speaker verification over the fixed and mobile telephone networks. Dans Proceedings of the 24th IASTED International Conference on Signal processing, Pattern Recognition, and Applications, pages 228–233, 2006.

[10] A. Roy, M. Magimai.-Doss, et S. Marcel. A fast parts-based approach to speaker verification using boosted slice classifiers. IEEE Trans. on Information Forensics and Security, 7 :241–254, 2012.

[11] S. Hwang, S. Cho, et S. Park. Keystroke dynamics based authentication for mobile devices. Computer & Security, 28 :85–93, 2009.

[12] T.-Y. Changa, C.-J. Tsaib, et J.-H. Lina. A graphicalbased password keystroke dynamic authentication system for touch screen handheld bile devices. The Journal of Systems and Software, 85 :1157 ?1165, 2012.

[13] N. Sae-Bae, N. Memon, et K. Isbister. Investigating multi-touch gestures as a novel biometric modality. Dans IEEE Fifth International Conference on Biometrics : Theory, Applications and Systems (BTAS), 2012.

[14] E. Miluzzo, A. Varshavsky, S. Balakrishnan, et R. Choudhury. Tapprints : your finger taps have fingerprints. Dans Proceedings of the 10th international conference on Mobile systems, applications, and services, 2012.

[15] A. De Luca, A. Hang, F. Brudy, C. Lindner, et H. Hussmann. Touch me once and i know it's you! : implicit authentication based on touch screen patterns. Dans Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems, 2012.

[16] Michael Beton, Vincent Marie, et Christophe Rosenberger. Biometric secret path for mobile user authentication: A preliminary study. Dans Computer and Information Technology (WCCIT), 2013 World Congress on, pages 1–6. IEEE, 2013.

[17] Abdulaziz Alzubaidi et Jugal Kalita. Authentication of smartphone users using behavioral biometrics. IEEE Communications Surveys & Tutorials, 18(3) :1998–2026, 2016.

[18] Attaullah Buriro. Behavioral Biometrics for Smartphone User Authentication. Thèse de doctorat, University of Trento, 2017.

[19] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner,W. Timothy Polk, Sarbari Gupta, et Emad A. Nabbus. Nist special publication 800-63-2 : Electronic authentication guideline. Rapport technique, NIST, 2013.

[20] A. B.J. Teoh, Y. W. Kuan, et S. Lee. Cancellable biometrics and annotations on biohash. Pattern Recognition, 41 :2034–2044, 2008.

[21] Davide Maltoni, Dario Maio, Anil Jain, et Salil Prabhakar. Handbook of fingerprint recognition. Springer Science & Business Media, 2009.

[22] Kenneth Ko. Users guide to export controlled distribution of nist biometric image software (nbisec). NIST Interagency/Internal Report (NISTIR)- 7391, 2007.