Synchronous One Time Biometrics With Pattern Based Authentication

Patrick Lacharme, Christophe Rosenberger

Synchronous One Time Biometrics With Pattern Based Authentication

Patrick Lacharme and Christophe Rosenberger
Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
patrick.lacharme@ensicaen.fr christophe.rosenberger@ensicaen.fr

***Abstract*—One time passwords are commonly used for authentication purposes in electronic transactions. Nevertheless, providing such a one time password is not really a strong authentication proof because the token generating the passwords can be given by an impostor. In order to cope with this problem, biometric recognition is more and more employed. Even if biometric data are strongly linked with the user, their revocability nor diversity is possible, without an adapted post-processing. Biometric template protection schemes, including the BioHashing algorithm, are used to manage the underlying privacy and security issues. These schemes are used for the protection of several biometric modalities, but are not necessary adapted for all of them. In this paper, we propose a new protocol combining protected biometric data and a classical synchronous one time password to enhance the security of user authentication while preserving usability and privacy. Behavioral biometrics is used to provide a fast and a usable solution for users. We show through experimental results the efficiency of the proposed method.**

***Keywords*-Authentication, BioHashing, behavioral biometrics.**

I. Introduction

User authentication with mobile device is more and more envisaged for applications on the Internet and electronic transactions. One Time Password (OTP) is a popular solution for user authentication applications. In 2011, the total revenue of such solutions was estimated to 770 millions dollars [1]. The classical form factor is a physical token but more and more OTP are provided as a software application on mobile devices and are asynchronous (based on the use of a challenge). Even if this solution is secure and usable, it does not constitute a strong identity proof as anybody finding the OTP token could use it. In order to solve this problem, biometrics is more and more used to increase the level of confidence of user authentication. Nevertheless, a static biometric authentication possesses the same vulnerabilities than a standard static authentication if the exchanged data are eavesdropped and replayed. Moreover, biometric data are sensitive and require a particular attention in terms of security and privacy. Biometric data protection should be realized during all the life cycle of the data including the storage and the handling. A biometric authentication is realized in two steps : the enrollment and the verification phases, where a query biometric template is compared to the reference one. Standard cryptography as symmetric encryption (or hash functions) does not ensure the data protection during the comparison step because two biometric data from the same individual are not exactly identical and, consequently, the comparison can not be realized on the encrypted domain. Several ways are proposed to achieve the protection of biometric data, including adapted cryptographic schemes (fuzzy commitment, homomorphic encryption) and feature transformations (including the Biohashing algorithm). All these schemes should ensure security, diversity and revocability of the biometric data. The objective of this paper is not to propose a new scheme for biometric template protection. For more details on these schemes, we refer the reader to the detailed survey [2].

The first contribution of this paper is to propose a generalization of the synchronous one time passwords by adding a biometric feature protected by a biometric template protection scheme. A patent in 2007 [3] proposed to define a preliminary version of synchronous one time biometrics while protecting the biometric data with a classical encryption scheme. This approach has an important drawback because the matching of biometric templates requires a decryption that is a very sensitive step. We extend in this paper this solution through the feature transformation of biometric template. Second, we use for the first time to our knowledge a specific biometric modality with the Biohashing algorithm: biometric pattern drawn on a touch screen. This solution has the advantage to be very simple to use and very quick. Experiments are carried out on a home made benchmark dataset composed of 34 users with 15 samples for each and show the benefit of the proposed solution. This paper is organized as follows. Section 2 provides a presentation of feature transformation template protection schemes, with a description of the Biohashing algorithm. The computation of biometric features from pattern drawing is described in Section 3. Section 4 presents the proposed solution to compute the synchronous one time biometrics. Section 5 illustrates through experimental results the benefit of the proposed solution. Finally, we conclude and give some perspectives in section 6.

II. Feature transformation and BioHashing

A feature transformation is a function F using a key K (that is typically a random seed or a password), applied to a biometric template T. The transformed template $F_K(T)$ is stored in a database or in a personal device.

The Biohashing algorithm, described below, belongs to this class of transformation. During the authentication step, the same transformation is applied to the query template T' with the same key K and a comparison is realized between $F_K(T)$ and $F_K(T')$. It is generally considered that, given the transformed template $F_K(T)$ and the key K, it is possible to recover the original template T (or a close approximation) as presented in [4]. Thus it is preferable to store this key in a second support, even if the reconstruction of the original template depends strongly to the used biometric modality. The performance of the authentication system is generally estimated with FMR (False Match Rate computing the ratio of false negative verification) FNMR (False Non Match Rate calculating the ratio of false positive verification) rates and the feature transformation should not decline the performance of the system. In fact, this approach tends to improve the performance of the biometric system without any protection (but a the key K is necessary).

The Biohashing algorithm is applied to biometric templates, represented by real-valued vector of fixed length (the metric used to evaluate the similarity between two biometric features is the Euclidean distance) and generates binary templates of length lower or equal to the original length (the metric used to evaluate the similarity between two transformed templates is the Hamming distance). This algorithm has been originally proposed for face and fingerprints by Teoh *et al.* in [5], where the fingerprint features are, in a first time, transformed in a real-values vector of fixed length, called Fingercode (this step is not useful and not described in this paper). The Biohashing algorithm is applied, in a second time, on this fingercode and generates a binary template called BioCode. At the end of the enrollement phase, the fingercode is discarded and the BioCode (with the associated seed) is stored. The biohashing algorithm can be applied on any biometric modalities, that can be represented by a real values vector of fixed length.

The Biohashing algorithm transforms the biometric template $T = (T_1, \dots T_n)$ in a binary template $B = (B_1, \dots B_m)$, with $m \leq n$, as following (see Figure 1) :

1) m pseudorandom orthonormal vectors $V_1, \dots, V_m$ of length n are generated from the random seed (typically with the Gram Schmidt algorithm).
2) For $i = 1, \dots, m$, compute the scalar product $x_i =< T, V_i >$.
3) Compute the binary template $B = (B_1, \dots, B_m)$ with the quantization process:

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

where τ is a given threshold, generally equal to 0.

The performance of this algorithm is ensured by the scalar products with the orthonormal vectors, as detailed in [6]. The quantization process of the last step ensures the non-invertibility of the data (even if $n = m$, because each coordinate of the input T is a real value, whereas the coordinates of the output B is a single bit). Finally, the random seed guarantees the diversity and revocability properties. We present in the next section the biometric modality we use as input of the Biohashing algorithm.

III. Biometric pattern based authentication

In the literature, biometric based mobile authentication is an emerging issue, with relatively few references. The NIST report [7] details some recommendations concerning portable biometric acquisition station and considers the following modalities: fingerprint, face and iris. Most of papers are devoted to a particular modality. We can mention the references [8] and more recently [9] focused on speaker verification for mobile devices. The first deals with text-dependent speaker verification, while the latter proposes a new method to extract features from speech spectra called *slice features*.

Face recognition is dealt with in the paper [10], along with eye detection, or in [11], where a real time training algorithm is developed for mobile devices. The authors propose to extract local face features using some local random bases and then to incrementally train a neural network. Image processing also concerns hand biometrics on mobile as in the reference [12], where hand images are acquired by a mobile device without any constraint in orientation, distance to camera or illumination. The author of [13] details an iris recognition system, based on a three-step pre-processing method relying on (a) automatic segmentation for pupil region, (b) helper data extraction and pupil detection and (c) eyelids detection and feature matching.

Apart from the literature dedicated to biometric solutions for mobile authentication related to a specific modality, some papers propose an overview on the underlying topic. We can mention the recent paper [14]. The authors focus on biometrics on mobile phone through some standard modalities (fingerprint, speaker recognition, iris recognition, gait) and propose a new application to ECG measurement and remote telecardiology, with an extra portable heart monitoring device. Some recent papers [15], [16], and [17] deal with keystroke dynamics based recognition. The first paper makes a study about user identification using keystroke dynamics-based authentication (KDA) on mobile devices, relying on 11-digit telephone numbers and text messages as well as 4-digit PINs to classify users. The second develops a more efficient KDA process, with optimized enrollment and verification steps, whose principle is extended in the latter paper for touch screen handled mobile devices, along with a pressure feature measurement.

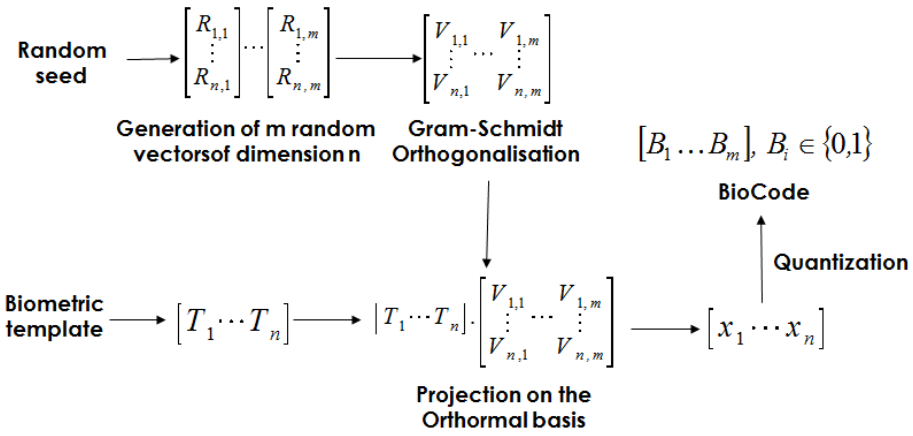

Figure 1. General principle of the BioHashing algorithm

Many recent papers propose to use touch screen to capture biometric data [18]. Most of these studies use methods used for keystroke or signature dynamics. As for example, the notion of TapPrint has been proposed by Miluzzo et al. [19] where the concept of keystroke dynamics is generalized to touch screen. The proposed method is based on the location of the tap on the key associated to a letter or by analyzing gyroscope information. The system has been tested on 10 volunteers with a total number of 40000 taps. The recognition efficiency is between 80% and 90%. The work done by Luca et al. [20] is very interesting because it combines pattern based password and biometrics. They proposed a system and test it with 34 users. They obtained a performance of 19% for the FRR value (False Rejection Rate) and 21% for the FAR (False Acceptance Rate). A method in 2013 has been proposed [21] combining multiple information compared with the Pearson Correlation and the Dynamic Time warping (DTW) methods. The equal error rate (EER) is near 17% which the best result for this biometric modality. We can see that many works have been done to propose biometric systems for user authentication on mobile devices. Most of solutions used classical modalities (such as fingerprint or face) implemented on a mobile device. The user experience is in general not good and not very well fitted for a mobile device.

The biometric system we propose to use in this work intends to increase security for a quick logical access control to the mobile device. It is composed of a two factor approach. We intend to first recognize the user by the knowledge of a password represented by a pattern. We use the classical Android unlock screen approach (see Figure 2). This approach to enter a password is quicker and is more usable for a mobile device. Second, the behavior of the user while drawing the pattern is analyzed. Many information are collected during the capture process:

- X position: the X position of the finger on the touch screen is recorded during the capture,
- Y position: the Y position of the finger on the touch screen is also recorded,
- Pressure: the pressure of the finger on the touch screen is captured (provided by the Android OS),
- Finger size: ratio of pixels where the finger is in contact with the touch screen,
- Tilt: orientation information from the accelerometer sensor.

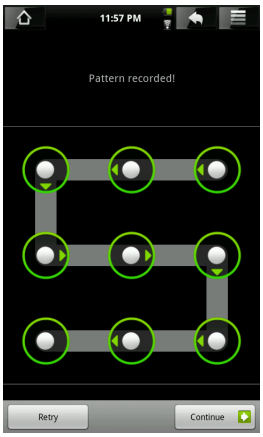

Figure 2. Classical Android unlock screen

As the time needed to draw the same pattern can be different for each capture, signals are undersampled to a fixed length. A constant size description is necessary to use this template as input in the BioHashing algorithm.

IV. Synchronous One Time Biometrics

A. Description of the solution

The proposed method combines biometric data acquired with the previous biometric system and a classical

synchronous one time password. A biometric feature transformation is used for the protection of the biometric template and the generation of dynamic BioCodes (to avoid the replay attack). In the rest of this section, we use the Biohashing terminology for the feature transformation for simplicity and without loss of generality. Like all biometric systems, two steps are necessary to be defined: enrollment and verification.

The enrollment step for the user consists in generating a *Reference BioCode* given its behavior when drawing a chosen pattern (biometric data) and the pattern code (that is considered as the seed value of the BioHashing algorithm). This *Reference BioCode* is sent to the service provider (bank, identity provider...). The user obtains from the service provider a synchronous OTP (as a software application on the mobile device). This OTP is personalized for the user

The verification step (described in Figure 3 consists in computing in the user side the *Capture BioCode* from the biometric template and the pattern code as a seed with the Biohashing algorithm. The Biohashing algorithm is applied once more with the *Capture BioCode* as input and the OTP value at the considered event (time or counter) to generate the *Dynamic Capture BioCode*. On the service provider side, the *Reference BioCode* (stored during the enrollment step) is combined with the OTP related to the user with the BioHashing algorithm in order to generate the *Dynamic Reference BioCode*. The Hamming distance between the *Dynamic Reference BioCode* and the the *Dynamic Capture BioCode* allows the service provider to decide if the user is authenticated or not.

B. Discussion

The proposed method meets many requirements:

- Usability: it is very easy and quick for a client to provide an identity proof within the proposed method. Moreover, it is possible to use the same pattern for several service provider by concatenating the pattern code with a number related to the service provider as for example during the generation of the *Reference BioCode*.
- Security: the client send its identity proof to the service provider through the *Dynamic Capture BioCode*. As we use an OTP as seed in the BioHashing algorithm, the replay attack is not anymore possible. Note that this identity proof could be verified *a posteriori* given the value of the OTP, this aspect guarantees non repudiation.
- Revocability : is possible for a client to revoke its biometric data by changing its pattern.
- Linkability : the use of an OTP generator permits to generate dynamic BioCodes to avoid linkability attacks (given different BioCodes). Previous studies have shown that the mutual information of BioCodes generated from the same template and different seeds is low and cannot be used to link identities [22].
- Non-invertibility : it is not possible to recover the biometric raw data (given different BioCodes) as the BioHashing is non invertible function if the seed is unknown. The non-invertibility is ensured even if the pattern data is known by an attacker (as long as the OTP generator is secure).

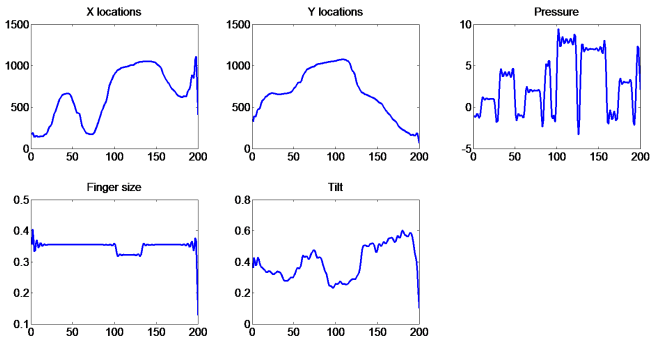

Figure 4. Pattern drawing biometric features

V. Experimental results

We define in this section experimental results for the validation of the proposed method.

A. Protocol

We detail the protocol we followed in this study.

1) Biometric data:

In this work, we used a biometric dataset of data captured when users draw a single pattern:

- Data have been collected on a Nexus 7 mobile phone with Android 4.4.2 with a touch screen having a resolution of 800 x 1280 pixels. We developed an Android application to collect data mentioned in the paper,
- The pattern was the same for all users and is defined by the following pattern code "1235987". This experimental setup can be considered as the worst case where an attacker knows the pattern to draw.
- 34 users participated to this experiment,
- Each user provided 15 samples described by 5 signals undersampled to 200 values (time normalization). Figure 4 presents the data of the first sample for user 1. The x-axis corresponds to the time and the y-axis to feature value. So, the template size is 1000 (by concatenating all undersampled signals),

In total, we have a subset of $34 \times 15 = 510$ biometric templates of size 1000 real values.

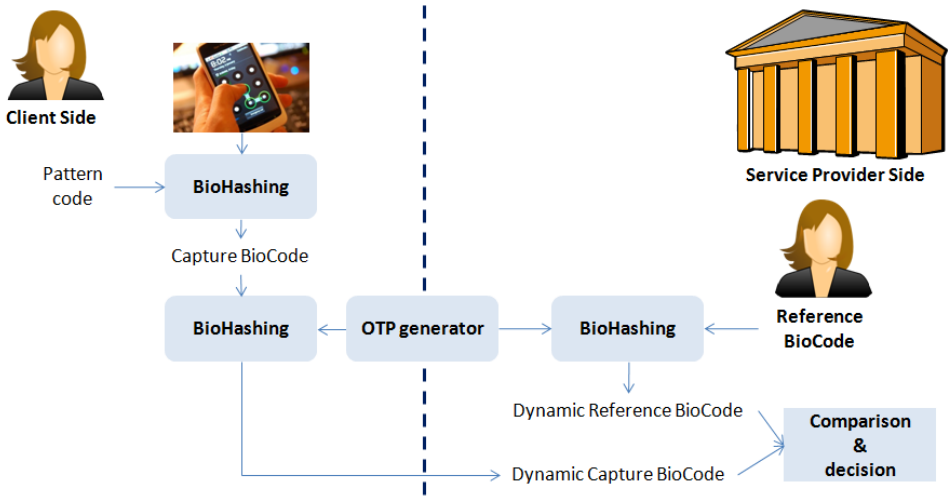

Figure 3. General principle of synchronous one time biometrics (with Biohashing)

2) BioHashing parameters:

Considering the BioHashing setup, we set the parameter values as following (when using notations defined in Section 2):

- Template size: n=1000,
- BioCode size: m=750 for the *Reference BioCode* and *Capture BioCode* and m=512 for *Dynamic Reference BioCode* and *Dynamic Capture BioCode*,
- As the pattern is the same for all users, in the computation of the Reference BioCode, the pattern code is set to "1235987" for all users,
- Matching algorithm: Hamming distance.

3) Performance analysis:

In order to evaluate the performance of the proposed method, we use the following methodology:

- We use the first sample of each user as reference template, the *Reference BioCode* is computed from this biometric data,
- We run a simulation with 1000 generations of OTP,
- For each OTP generation, we choose randomly one of the 14 left samples of the user to simulate a legitimate verification. We compare the *Dynamic Reference BioCode* and *Dynamic Capture BioCode* to generate an intraclass score. We obtain $1000 \times 34 = 34,000$ intraclass scores,
- We have a similar process to simulate impostor attack by choosing a biometric sample from another user and we obtain at the end the same number of interclass scores,
- Given these two sets of scores, we can compute their distribution in order to estimate in which measure impostor scores are different than legitimate ones. Second, we compute the Equal Error Rate (EER) value that is a well known metric in biometrics that measures the behavior of the biometric system when the decision threshold is set to have the same number of false rejected users and false accepted ones.

B. Results

Figure 5 presents the distribution of scores we obtained using this biometric dataset (genuine or intraclass scores are represented in red, impostor or interclass ones in blue). This figure shows clearly that the two distributions are separated without any overlapping. For the 34.000 intraclass scores, the maximal value is 0.29 meaning that in the worst case, 29% of the bits were different between the *Dynamic Reference BioCode* and *Dynamic Capture BioCode*. By looking at this curve, we can expect on this database to have no recognition error that is confirmed by the EER value that equals 0% (without the BioHashing, the touch screen verification performance is estimated to 15%). This is an excellent result considering we use a behavioral biometric modality. The use of the BioHashing algorithm is known to increase the performance of biometric system (if the seed is unknown). This shows the benefit of the proposed method even when the pattern is the same for each user (and the usability of the authentication system).

VI. Conclusion and Perspectives

The proposed solution permits to generalize the concept of synchronous one time passwords with the use of biometric data. We showed in this paper that the biometric modality can be not only a fingerprint but also a behavioral approach without loosing performance. We believe this solution can be very usable for clients and could be used in many applications. The feature transformation combined with the OTP ensures the security of the biometric data. Moreover, the possibility of reverse or approximate the used biometric data, if the seed is known, is not clear in the case of

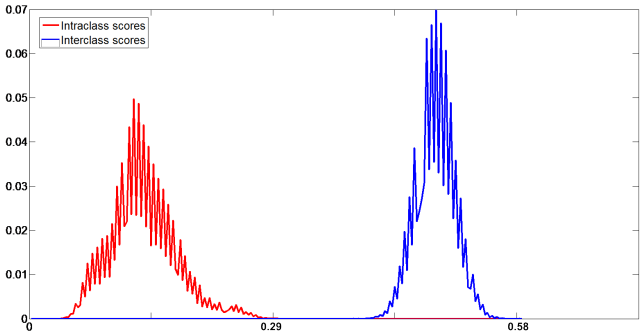

Figure 5. Distribution of scores for 1000 generations of OTP.

our pattern and the advantage of an attacker with such approximation would be relatively modest in terms of user's privacy. Indeed, by definition, the behavior when drawing a pattern on a touch screen can be easily revoked by changing the pattern. As perspectives, we intend to generalize the proposed concept to multi-biometrics. We also would like to use this approach for continuous authentication schemes by providing dynamic BioCodes as identity proof.

REFERENCES

[1] R. Martinez, "An overview and competitive analysis of the one-time password (otp) market," Frost & Sullivan, Tech. Rep., 2011.

[2] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. on Information Security*, vol. 3, 2011.

[3] J. Fouquet, "Time synchronous biometric authentication," Sep. 6 2007, uS Patent App. 11/359,258. [Online]. Available: https://www.google.com/patents/US20070206838

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

[5] A. Teoh, D. Ngo, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, vol. 40, 2004.

[6] A. B. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on biohash," *Pattern Recognition*, vol. 41, pp. 2034–2044, 2008.

[7] S. Orandi and 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/MobileID-BPRS-20090825-V100.pdf.

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

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

[10] A. Hadid, J. Y. Heikkila, O. Silven, and M. Pietikainen, "Face and eye detection for person authentication in mobile phones," in *1st ACM/IEEE International Conference on Distributed Smart Cameras*, 2007.

[11] K. Choi, K.-A. Toh, and H. Byun, "Realtime training on mobile devices for face recognition applications," *Pattern Recognition*, vol. 44, p. 386400, 2011.

[12] A. de Santos-Sierra, C. Sanchez-Avila, J. Guerra-Casanova, and A. Mendaza-Ormaza, *Hand Biometrics in Mobile Devices*. InTech, 2011, ch. Advanced Biometric Technologies, available from: http://www.intechopen.com/books/advanced-biometric-technologies/hand-biometrics-in-mobile-devices1.

[13] J.-S. Kang, "Mobile iris recognition systems: An emerging biometric technology," in *International Conference on Computational Science (ICCS)*, 2010.

[14] S. Wang and J. Liu, *Biometrics on Mobile Phone*. InTech, 2011, ch. Recent Application in Biometrics, pp. 3–22, available from: http://www.intechopen.com/books/recent-application-in-biometrics/biometrics-on-mobile-phone.

[15] N. Clarke and S. Furnell, "Advanced user authentication for mobile devices," *Computers & Security*, vol. 26, pp. 109–119, 2007.

[16] S. Hwang, S. Cho, and S. Park, "Keystroke dynamics-based authentication for mobile devices," *Computer & Security*, vol. 28, pp. 85–93, 2009.

[17] T.-Y. Changa, C.-J. Tsaib, and J.-H. Lina, "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices," *The Journal of Systems and Software*, vol. 85, p. 11571165, 2012.

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

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

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

[21] M. Beton, V. Marie, and C. Rosenberger, "Biometric secret path for mobile user authentication: A preliminary study," in *Computer and Information Technology (WCCIT), 2013 World Congress on*. IEEE, 2013, pp. 1–6.

[22] R. Belguechi, E. Cherrier, and C. Rosenberger, "How to evaluate transformation based cancelable biometric systems?" in *NIST International Biometric Performance Testing Conference (IBPC)*, 2012.