Biometric Secret Path for Mobile User Authentication: A Preliminary Study

Michael Beton, Vincent Marie, Christophe Rosenberger

Biometric Secret Path for Mobile User Authentication: A Preliminary Study

Michael Beton
National School of Engineering
ENSICAEN - France
mickael.beton@ecole.ensicaen.fr

Vincent Marie
National School of Engineering
ENSICAEN - France
vincent.marie@ecole.ensicaen.fr

Christophe Rosenberger
GREYC research lab
ENSICAEN - France
christophe.rosenberger@ensicaen.fr

***Abstract*—In this paper, we study a recent biometric modality for user authentication on mobile devices. The proposed solution is a two-factor user authentication scheme and gives some high guarantees on user's identity. We first use the knowledge of user's password represented by a secret path on a grid composed of 9 points. Second, the behavior of the user while giving its path is analyzed to verify its identity. This solution is implemented as an Android application for mobile devices. Experimental results on an own made biometric database show promising results.**

I. Introduction

World has now about 6 Billion cell phone subscribers [1]. Mobile devices are used for accessing different services: email, internet, payment, games... For sensitive services such as mobile payment, a strong user authentication is required. Classical solutions use password or PIN code to realize this task. We argue in this paper that biometrics is the only user authentication solution. Indeed, only this technology has a relationship between the user and its authenticator. Biometric authentication systems are increasingly used in real life applications such as border control, e-commerce, *etc.*

There exist three types of biometric modalities that can be used to verify the identity of an user: 1) Biological analysis such as DNA or EEG signals, 2) Behavioral analysis such as keystroke dynamics or signature dynamics, 3) Morphological analysis such as fingerprint or face. When using a biometric system, two important steps have to be considered. The first one concerns the enrollment whose objective is to generate user's model (called biometric reference) from one or multiple biometric captures. The second one concerns the verification of user's identity by comparing the reference of the supposed user and a biometric capture.

The paper is organized as follows. Section 2 is dedicated to the state of the art on biometric authentication on mobile devices. In the section 3, we propose a new biometric system combining the secret path representation of passwords and the associated behavior while typing it. Section 4 is dedicated to experimental results on an own made biometric database. Last, section 5 concludes this work and gives some perspectives.

II. State of the art

In the literature, biometric based mobile authentication is an emerging issue, with relatively few references. The NIST report [2] 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 [3] and more recently [4] focused on speaker verification for mobile deices. 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 [5], along with eye detection, or in [6], 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 [7], where hand images are acquired by a mobile device without any constraint in orientation, distance to camera or illumination. The author of [8] 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 [12]. 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 [9], [10], and [11] 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.

Many recent papers propose to use this sensor to capture biometric data [13], [14], [15]. Most of these studies use methods used for keystroke or signature dynamics. As for example, the concept of TapPrint has been proposed by Miluzzo et al. [16] 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. [17] 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).

We can see that many works have been done to propose biometric systems for user authentication on mobile devices. Most of solutions are classical modalities implemented on a mobile device. The user experience is in general not good and not very well fitted for a mobile device.

In the next section, we propose a biometric system for mobile device providing a better security while permitting a very good usability based on the work proposed by Luca et al. [17].

III. Proposed system

The biometric system 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 secret path. We use the classical Android unlock screen approach (see Figure 1). This approach to enter a password is quicker and is more usable for a mobile device. Second, the behavior of the user while giving the secret path is analyzed. These information are combined to make the decision concerning the identity verification of the user. In the next sections, we detail the enrollment and verification steps of the proposed biometric system.

A. Extracted features

Many information are collected during the capture process. Figure 3 gives an example of biometric capture for a given password:

- X position: the X position of the finger on the touch screen is recorded during the capture,

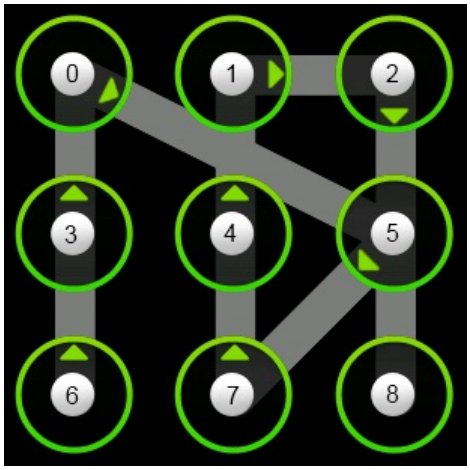


Fig. 1. Classical Android unlock screen

- 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 (note that some devices provide an imprecise measure of this information),
- Time: the time needed to reach each point is recorded,
- Point position: while typing the secret path, we collect information on the position on the points describing the secret path. As for example, in the figure 1, the users begins by the point 6 then 3 ... When the location (X,Y) is inside a green circle, we collect the point position number, otherwise this value equals -1.

From these raw data, we can extract more information such as (see Figure 2):

- Time T_i: it corresponds to the total time the finger is inside the green circle of the point P_i in the secret path,
- Time Δ_i : it corresponds to the time needed by the user to reach the following point. It is computed from the last point touched on point P_i (called A) and the first point touched on point P_{i+1} (called B). The value Δ_i is computed from the difference of time-stamp between B and A,
- Time $Total$: it computes the total time the user nees to enter the secret path.

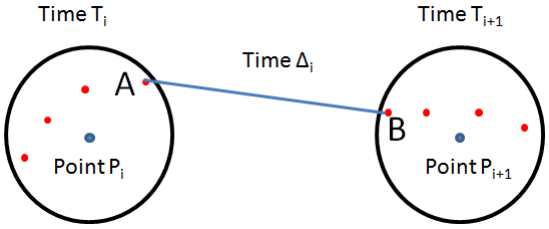


Fig. 2. Features extraction

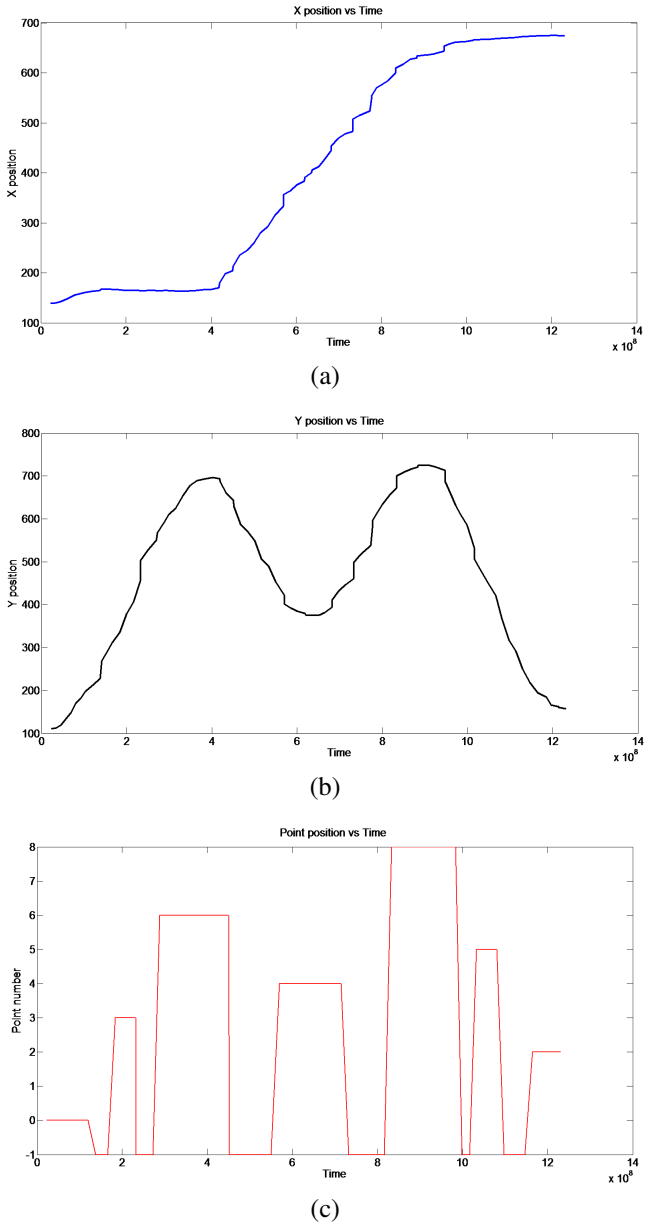


Fig. 3. Example of captured data: (a) X position, (b) Y position, (c) Point position

B. Enrollment

To generate the biometric reference, we ask the user to enter 5 times the chosen password represented by a path. Note that the quantity of extracted features can be different for different captures.

We suppose having 5 captures of each measure. We denote a signal by S_i, $i = 1..5$. In order to generate the biometric reference of the user, we apply the following process for each available signal:

Int Function $Enrollment(S_1, .., S_5)$
{
$Median : array[1..5]$

for $i = 1 \rightarrow 5$ **do**
  $Temp : array[1..5]$
  for $j = 1 \rightarrow 5$ **do**
    if $i \neq j$ **then**
      $Temp(j) \leftarrow Matching(S_i, S_j)$
    end if
  end for
  $Median(i) \leftarrow Median(Temp)$
end for

$Return \min(Median)$
}

Where $Matching$ computes the similarity / distance score between the two signals described in the next sections, and $Median$ is a function computing the median value of 5 values.

C. Verification

For the verification step, the same data are captured. To compare the biometric capture with the biometric reference of the supposed user, we propose to use two different approaches.

1) Correlation:

The main difficulty of the matching process is that the size of data is in general different. To cope this problem, we propose first to define a sub-sampling of the captured data. We interpolate data to fit a certain size (in this work, 100 points). To compare the two feature vectors, we propose to use the Pearson correlation factor:

$$Corr(S_1, S_2) = \frac{Cov(S_1, S_2)}{\sigma^2(S_1).\sigma^2(S_2)}$$

where $Cov(S_1, S_2)$ is the covariance between the variables S_1 and S_2 and $\sigma(S_1)$ is variance value of the variable S_1.

We compute the absolute value of the correlation factor between X position, Y position, Pressure and Time of the biometric reference and the capture. We sum these values and we divide by 4 to obtain a similarity score between 0 and 1.

2) Dynamic Time Wrapping:

Dynamic time warping (DTW) is an algorithm for measuring similarity between two sequences which may vary in time or size [18]. A well known application is automatic speech recognition, to cope with different speaking speeds. Other applications include speaker recognition and online signature recognition.

Figure 4 gives an example of computation between two signals having different sizes.

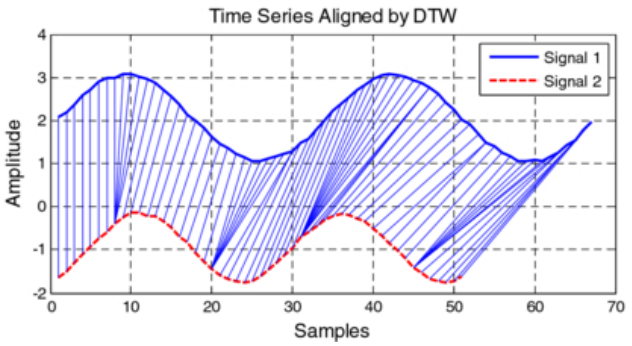


Fig. 4. Example of DTW computation on two signals (source [19])

The DTW algorithm is given below:

$S_1 : array[1..n]$
$S_2 : array[1..m]$

Int Function $DTWVerification(S_1, S_2)$ {

$DTW \leftarrow array[0..n, 0..m]$

for $i = 1 \rightarrow n$ **do**
  $DTW[i, 0] \leftarrow \infty$
end for

$DTW[0, 0] \leftarrow 0$

for $i = 1 \rightarrow n$ **do**
  for $j = 1 \rightarrow m$ **do**
    $cost \leftarrow d(S_1[i], S_2[j])$
    $mini \leftarrow \min($ $DTW[i-1, j]$,
      $DTW[i, j-1]$,
      $DTW[i-1, j-1])$
    $DTW[i, j] \leftarrow cost + mini$
  end for
end for

return $DTW[n, m]$
}

where S_1 and S_2 correspond to the two signals to be compared (it could be in our case the X position, Y position or Pressure) and $d()$ is the Euclidean distance.

3) Fusion:
In order to improve performance results of a biometric system, it is possible to use a multi-biometrics approach [20]. It consists in combining multiple modalities, algorithms or features. In this paper, we propose to use score fusion consisting in combining scores provided by multiple features or algorithms. We used a simple and classical approach consisting in summing the scores provided by different information.

D. Decision

Based on the matching score, we have to decide if the authentication is successful or not. The identity of the user is verified if the matching score is higher (for the correlation approach) or lower (for the DTW distance) than a threshold set by an administrator.

In the next section, we show some experimental results on this biometric system with the two strategies for the verification step.

IV. Experimental results

In this section, we first define the protocol we followed to illustrate the performance of the proposed biometric system.

A. Protocol

We used an own made database for this work. The one provided by Luca et al. [17] was not possible to be used as the information on the point position (used for time computations) was not available. This database has been acquired with the participation of 15 users. The secret path was simple and composed of 7 points (see figure 5). This secret path is very simple to type and to remember. For a more complex secret path, experimental results should be better. Each user has provided 8 captures of the same secret path.

In total, we have $7 \times 15 = 120$ intra-class authentication attempts and $7 \times 14 \times 15 = 1470$ inter-class attempts (simulating attacks).

Fig. 5. Secret path used for the experiments

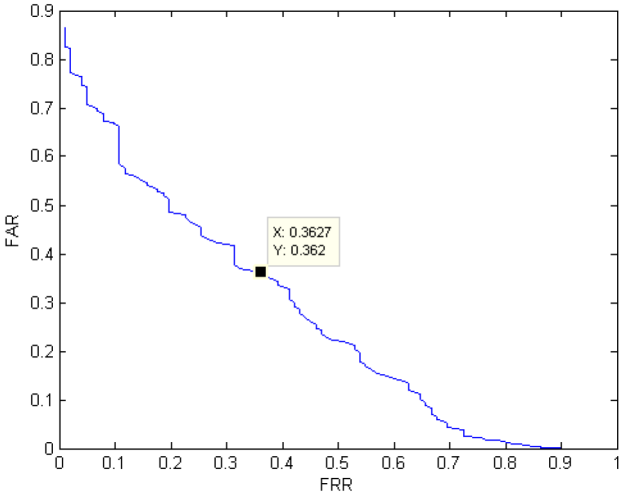
B. Results

We present in this section the results we obtained on this database using the developed Android application.

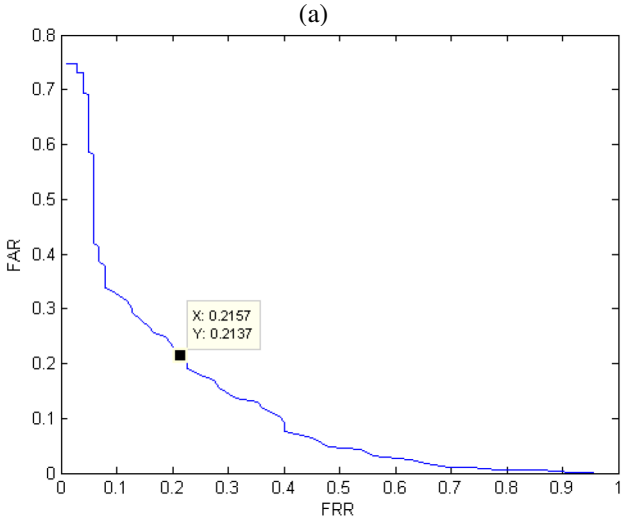
1) Features:
First, we evaluate the benefit of each feature. For this experiment, we used the correlation approach as matching score. We compute the intra-class and inter-class scores using separately X position, Y position and time (pressure information was not precise on the used device). We sum the Pearson correlation factor of X and Y positions (to consider the location information through time). Figure 6 shows the ROC curve using location and time. This curve represents the evolution of the FAR vs the FRR (by testing different values of the decision threshold). As we can see on this figure, the timing information is more interesting than the location (mainly because everybody used the same secret path). We obtain an EER value of 36% for locations and 21% for the time information. Note with an EER value of 21%, results are equivalent as the ones provided by the study of Luca et al. in [17].

2) Matching score:
In this experiment, we compare the results provided by the two matching methods namely correlation and DTW. We used the X and Y locations of the finger trough time and we combine them by summing the scores for X and Y positions. Figure 7 shows the ROC curve while using the DTW. We obtain en EER value near 28% with DTW while we obtained an EER value on the same data of 36% with correlation (see Figure 6 (a)). DTW is more efficient considering recognition performance but in terms of computation time, it is less efficient.

3) Fusion:
In this part, we combine the information on X and Y positions (typing dynamic) and the times through score fusion. The correlation matching approach is used in this case. In this case, we sum the scores (after pre-processing on the correlation matching method to make it evolving as a distance). Figure 8 gives the ROC curve by merging these two features. We obtain an EER value equal to 17%. Many experiments have to be completed but we obtain the best EER value in the state of the art.



(a)



(b)

Fig. 6. ROC curves by using the correlation matching score and (a): X and Y positions, (b) time.

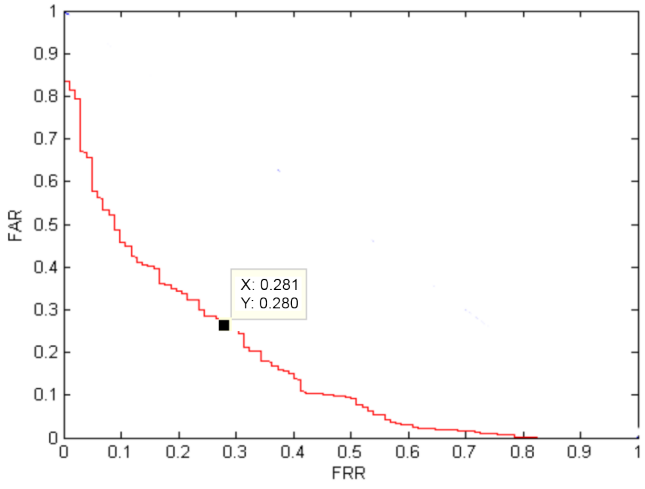


Fig. 7. ROC curve by using the DTW matching score and X,Y positions.

V. Conclusion and Perspectives

In this paper, we address user authentication on mobile devices using biometrics. The proposed solution consists in analyzing the way of typing a password by the user through a secret path. Many information can be recorded during the typing of the secret path such as time, X position, Y position, pressure to help user's recognition. We showed some preliminary results on an Android application. Different matching methods have been used such as the Pearson correlation and DTW. Experimental results on a real database

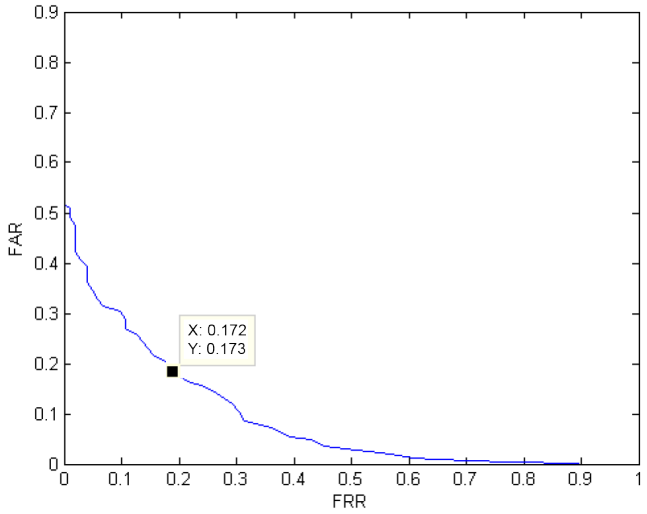


Fig. 8. ROC curve by using the correlation matching score by taking into account X,Y locations and Time.

acquired with a mobile phone, showed encouraging results with an EER value equal to 17% corresponding to the best one in the state of the art.

Many perspectives concern this study. First, we intend to acquire a new benchmark with more users and captures. We plan to ask users to type more complex secret paths. We also plan to combine matching algorithms and features to improve results.

REFERENCES

[1] "Measuring the information society," International Telecommunication Union, Tech. Rep., 2012.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

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

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

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

[11] 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.

[12] 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.

[13] 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.

[14] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: a novel approach to authentication on multi-touch devices," in *Proceedings of the 2012 ACM annual conference on human factors in computing systems*, 2012.

[15] U. A. Johansen, "Keystroke dynamics on a device with touch screen," Gjovik University College, Tech. Rep., 2012.

[16] 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.

[17] 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.

[18] T. Vintsyuk, "Speech discrimination by dynamic programming," *Kibernetika*, vol. 4, pp. 81–88, 1968.

[19] Z. Dong, H. L. Zhao, F. Gu, and A. D. Ball, "Phase-compensation-based dynamic time warping for fault diagnosis using the motor current signal," *Measurement Science and Technology*, vol. 23, p. 12, 2012.

[20] R. Giot, B. Hemery, E. Cherrier, and C. Rosenberger, *Signal and Image Processing for Biometrics*. Wiley, 2012, ch. Chapter 9 - Multibiometrics, pp. 167–194.