The Touchless Person Authentication Using Gesture-types Emulation of Handwritten Signature Templates

Marcin Piekarczyk
Institute of Computer Science and Computer Methods
Pedagogical University of Cracow
2 Podchorazych Ave
30-084 Krakow, Poland
e-mail: marp@up.krakow.pl

Marek R. Ogiela
AGH University of Science and Technology
Cryptography and Cognitive Informatics Research Group
30-Mickiewicza Ave
30-0659 Krakow, Poland
e-mail: mogiela@agh.edu.pl

Abstract — The paper proposes a secure real-time user authentication system based on dynamic handwritten signature verification. We discuss the touch-less sensor-based authentication mechanism that relies on remote tracking palm-gestures imitating the handwritten signature pattern of examined person. The appropriate data is gathered from non-invasive sensor device in the form of time-ordered series related to spatial coordinates of the pen-like tool position and velocity. The proposed matching scheme exploits data series analysis in joint with feature-based classification. The discrete cosine transform is used to deal with instability of the genuine patterns. We also consider of using the local sensitivity hashing functions to obtain the better efficiency. The detailed analysis of the experimental results is included, too.

Keywords — handwritten signature; palm-based gestures; dynamic analysis; gesture-based authentication; DCT; DTW; locality sensitive hashing; LSH; touch-less verification

I. INTRODUCTION

Today, biometric systems exploit varied psychological or behavioral modalities as fingerprint, iris, face, voice, gait and also handwritten signatures to authenticate users [10, 25]. This technology has many advantages in the context of usability and security. Biometric signals are considered as hard to steal or copy and can’t be forgotten or lost as ordinary passwords. Within biometrics, handwritten signature verification is continuously researched as a personal authentication method because of its social and legal acceptance and widespread usage [1, 11, 15-19, 21, 23]. On the other side, the huge popularity of smartphones, tablets and other devices controlled by touch and gesture [5-7] allows to apply non-typical security mechanisms for authentication purposes [22-24, 26].

This work is focused on dynamic handwritten signature verification but with utilization of non-standard data acquisition environment. We try to investigate the usability of handwritten signature performed as a gesture to observe biomechanical traits of one’s hand. Our research extends the verification system discussed in [20].

The paper is structured as follows. In Section II we provide basic information how data acquisition is organized. In section III there is a short discussion on handwritten signatures as gestures. Section III covers the description of new proposed method of authentication. Section IV presents experimental results and in Section V we conclude the paper with some discussions on future works.

II. DATA ACQUISITION ENVIRONMENT

In the paper we consider the environment where the hand equipped with simple writing tool like stick, pen or pencil is traced by the remote touchless sensor. Such system should be able to provide the complete information about spatial coordinates and velocity associated with tool’s motion. Proposed working environment is organized like Fig. 1 presents.

![Figure 1: The structure of data acquisition environment for handwritten signatures emulating gestures.](image)

The gathered signal has a continual nature so it is difficult to isolate it clearly. The system should be able to evaluate unambiguously when the user begins and ends performed gesture. Due to this we follows by assumptions proposed in [20] where three steps during the acquisition scheme are required:

- Relocation the hand inside the sensor range,
- Performing the gesture,
- Relocating the hand outside the sensor range.

Before and after the gesture performing user should keep his hand motionless throughout approximately 2 seconds. Such behavior enables the system to isolate the real signal in effective way.

III. GESTURE-BASED SIGNATURE EMULATION

The input gesture is considered as direct imitation of user’s own signature. As opposed to real situations where user signs usually existing paper documents we assume that signature’s...
emulation is performed the same way but in the air. Due to the
two-dimensional character of such pattern the gesture should
be performed along chosen surface e.g. XY or XZ plane. It
allows avoiding the technical problems during the
normalization stage. Moreover, in practical applications the
variant of data acquisition, where the index finger is used
instead of writing tool, may be also analyzed. In such case the
additional tool is useless (advantage), but graphical projection
of the signature is less accurate (drawback), because palm
mechanics works in slightly different and unnatural way.

From the recognition point of view the signature-based
gestures are very promising as biometric templates due to its
spatial and graphical complication [20]. Obviously, the main
challenge is related with instability and variability of signature
shape (see Fig. 2).

![Figure 2. Different realizations of the same user’s signature.](image)

It is common problem very well known in the context of
classical online and offline HSV systems [8, 25]. In our
approach we propose to exploit Discrete Cosine Transform
(DCT) [13] and Locality Sensitive Hashing (LSH) [4, 9] to
deal with it.

IV. PROPOSED MODEL OF AUTHENTICATION

A. Preprocessing

According the assumptions discussed in section II the input
signal $S$ is gathered from the sensor in the form of discrete time
series data (Fig. 3) associated with 3D spatial coordinates and
velocity of tool or finger.

If the XY plane is treated as reference surface, the finally
usable signal can be denoted as (1) where $z(t)$ series is omitted
as insignificant and uninformative.

$$S = \begin{bmatrix} x(t) \\ y(t) \\ v(t) \end{bmatrix}$$

In the preprocessing phase we follow the approach [20] to
isolate the proper signal range. As a result we receive three
data series normalized by value (Fig. 4).

![Figure 3. Example of data acquisition – raw signal.](image)
Subsequently, each series is transformed separately into DCT space according to formula (2).

\[ y[k] = 2f \sum_{n=0}^{N-1} x[n] \cos \left( \frac{\pi}{N} (2n+1) k \right) \quad (2) \]

\[ k = 0, \ldots, N - 1 \]

\[ f = \frac{1}{\sqrt{N}} \text{ if } k = 0 \]

The \( DCT(S) \) signal (3) can be directly used as a basis to create a template structure (Fig. 5).

\[ DCT(S) = \begin{bmatrix} DCT(x(t)) \\ DCT(y(t)) \\ DCT(v(t)) \end{bmatrix} \quad (3) \]

Since most of signal information tends to be concentrated in low-frequency components, DCT exactness can be easily parametrized by choosing first N coefficients for further calculations. The reduction of data size has big impact on the computational complexity of the recognition process.

However, it is important to make the balance between accuracy and effectivity. As result we obtain an approximated representation in the form of (4) and (5).

\[ DCT_N(S) = \begin{bmatrix} DCT(x(t))_1, \ldots, DCT(x(t))_N \\ DCT(y(t))_1, \ldots, DCT(y(t))_N \\ DCT(v(t))_1, \ldots, DCT(v(t))_N \end{bmatrix} \quad (4) \]

\[ DCT_N(S) = \begin{bmatrix} dct^x_1, \ldots, dct^x_N \\ dct^y_1, \ldots, dct^y_N \\ dct^v_1, \ldots, dct^v_N \end{bmatrix} \quad (5) \]

B. LSH and DTW based classifications

When we consider signature-emulated gestures in general it is possible to use the recognition scheme described in [20] for authentication purposes. The mentioned approach relies on the calculating of DTW-based distance [14] and using k-NN classifier for final decision (Fig. 6). The scheme should work properly, because these gestures are based on signature’s emulation process which provides sufficiently complicated signal trajectory and has appropriate distinctive power as pattern.

Unfortunately, in specific situations this approach could have some weakness, in particular, when we refer to its computational complexity. The recognition system requires the calculations of DTW distance between candidate signal and all in-memory patterns. This operation may be computationally ineffective especially in the case when reference database is very large (big data problem). This condition is relatively easy to satisfy in potential practical implementations. Due to this we propose to adapt Local Sensitivity Hashing (LSH) concept to avoid this problem and enhance the authentication algorithm.
The recognition algorithm with proposed modifications is presented in Fig. 7.

![Proposed gesture recognition scheme based on LSH](image)

Figure 7. Proposed gesture recognition scheme based on LSH.

The main difference consists in compilation the DCT signal (template) into hash tables by the LSH algorithm. The hashing data structure aims to organize similar (close) signals in the same neighborhood in hash tables [2] and the LSH is proved to make an approximate k-NN search in sub-linear time [2, 4, 9].

The LSH algorithm works with multi-dimensional data so it is necessary to transform \( DCT_N \) signal (6) into single solid vector \( T \) by concatenating components from all three data series (5).

\[
T(S) = [dct_1^x \ ... \ dct_N^x \ dct_1^y \ ... \ dct_N^y \ dct_1^z \ ... \ dct_N^z]
\] (6)

Finally, we obtain \( T(S) \) as 3N dimensional vector consists of real numbers. Due to this we assume the exploiting of Euclidian instead of Hamming distance as a similarity measure in LSH algorithm to avoid conversion of coefficients to integers.

V. EXPERIMENTAL RESULTS

To evaluate the initial accuracy the limited database was used. The database consists of gestures gathered from five people. Every person performed the gesture for the fifteen times. Three randomly chosen samples belonged to each person have been chosen as representative learning set and stored in the hash tables. The remaining ones were exploited as questioned input data. As a motion sensor during the data acquisition phase the Leap Motion controller [12] has been exploited. The results received during the tests are presented in Tab. I-II.

<table>
<thead>
<tr>
<th>TABLE I.</th>
<th>DTW-BASED SYSTEM PERFORMANCE – 3NN CLASSIFIER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( DCT-10 )</td>
</tr>
<tr>
<td>FRR</td>
<td>11.4</td>
</tr>
<tr>
<td>FAR</td>
<td>2.9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE II.</th>
<th>DTW-BASED SYSTEM PERFORMANCE – 5NN CLASSIFIER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( DCT-10 )</td>
</tr>
<tr>
<td>FRR</td>
<td>22.9</td>
</tr>
<tr>
<td>FAR</td>
<td>5.7</td>
</tr>
</tbody>
</table>

During the trials, the verification system based on LSH algorithm achieves comparable or better scores than best DTW classifier. It is necessary to run both schemes against considerably broader database to evaluate its capabilities especially in case of LSH based scheme where many settings like hash size and number of hash tables can be applied.

VI. CONCLUSIONS

In this article the idea of authentication scheme based on gesture-types emulating handwritten signatures has been discussed. We have also proposed the new automatic recognition scheme using LSH algorithm which is more computationally effective. Preliminary experiments provide the promising results for both authentication schemes. Therefore work is currently being done in deep testing against the considerably larger database and in evaluating how parameters like number of hash tables and hash bit length affects recognition results.

In the future we plan to study the applicability of similar scheme in the context of more complicated user-defined and multi-fingers gestures. Besides, we consider as important to investigate a usefulness of gesture-originated LSH hashes in the field of cryptographic key generation and secret sharing.

ACKNOWLEDGMENT

We kindly acknowledge the support of this study by a Pedagogical University of Cracow Statutory Research Grant.

REFERENCES


Leap Motion, https://www.leapmotion.com/


