Investigation about Authentication Biometrics using Keystroke Dynamics

Gláucya C. Boechat, Jeneffer C. Ferreira, and Edson C. B. Carvalho Filho

Abstract—This paper uses a Keystroke Dynamics in biometric authentication. The user is identified for the habitual rhythm to type your complete name in a conventional keyboard. Two features (e.g., durations of keystrokes, and latencies between keystrokes) and experiments using samples for genuines and impostors user were performed using two pattern classification techniques. The results show that the use of the Keystroke Dynamics is simple and efficient for personal authentication, getting optimum resulted using 90% of the features with 3.83% FRR and 0% FAR using classifier weight measure.

Index Terms — Biometrics, Keystroke Dynamics, pattern recognition.

I. INTRODUCTION

Lately, are necessary uses personal authentication to protect information of a system, assuring that only authorized people can access or modify the data [1]. Three methods different exist from authentication [2]: the first method of authentication is based on something that the person knows, as password and personal document. The second method of authentication is based on something that the person possesses, as magnetic card or smart cards, and third method of authentication is based in that the person is, as your physical or behavioral characteristic, that distinguishes a person of the others. The first two methods in spite of being a form of authentication very diffused, it presents vulnerability in term of safety.

Due to these problems, in the third method the person presents a characteristic its, cannot be forged and nor be forgotten. Among the physical characteristics exist, for example, the geometry of the hand, face, iris and the features considered behavioral as digital signature, voice and the Keystroke Dynamics [3].

Biometric treated in this paper is the Keystrokes Dynamics, related with the way or habitual rhythm of as a person it types a password, words/phrases or text in a terminal [4]. Each person possesses a different rhythm of typing of the other, even an imposter having knowledge of the password of a person, which if it tries to pass, difficulty will go to be authenticated [5]. The Keystroke Dynamics is relatively a cockroach technique; it needs only a keyboard and software for authentication, different of the others biometrics techniques that possess one high cost of the captation devices and analysis of the necessary data in the authentication, and can also be used with or without the knowledge of the person.

Some features can be extracted of the keystroke rhythm as; the time that a key is pressed (keystroke duration), the time between successive keys (keystroke latency), speed of the keystroke, placement of the fingers and pressure that the person applies when pressing a key (pressure keystroke) [6].

The remaining of this paper is organized in four sections. In the section 2 are presented works published in the area. In the section 3 the proposed methodology is discussed: the extraction of features and the used classifier. The experiments are presented and discussed in the section 4, and finally the conclusions are found in the section 5.

II. RELATED WORKS

The first study using the Keystroke Dynamic for identification it happened at the beginning of the decade of 80 for Gaines et al. [7], in their experiments made with seven would secrete using statistical method T-Tests for classification and authentication. For the composition of the pattern the keystroke latency was used among digraphs of an English text, words and sentences random, but just for digraphs that happened more than 10 times. The work resulted in a 4% FRR and ZeroFAR.

In the work of Bleha et al. [8] they used password and phrase. The analyzed characteristic was keystroke latency between keys with Bayes Classifier and Minimum Distance. First experiment accomplished with nine volunteers in a period of nine weeks, second with ten volunteers, in a period of five weeks and 26 volunteers in a period of eight weeks. The tests were accomplished with ten worth users and 22 impostors, resulting in 3.1% FRR and 0.5% FAR.

Joyce and Gupta [5] in its experiments with 33 persons used the following data: username, password, firstname, lastname.

The extracted feature was keystroke latency between two consecutive keys and using statistical classification. Where collected 8 patterns for formation of the set of training and 5 patterns for the set of test having as resulted 0.17% FAR and 13.3% FRR.

Monrose and Rubin [4] collected sample of 63 users, in a period of 11 months, extracted features: keystroke duration and keystroke latency, using Bayes Classifier with 92.14% of
success.

Cavalcanti et al. [9] Used statistical classifier, analyzing the features: keystroke duration and keystroke latency, from 24 volunteers, resulting in a 6.04% FRR and ZeroFAR.

In the work of Costa et al. [6] used the features: keystroke duration and 3 keystroke latencies between two keys, interval of time to the next key to be pressed, interval of time to press two consecutive keys and the interval of time to liberate two consecutive keys. Used classifier using Occult Models of Markov (HMM) they Obtained 4.5% EER. Other works were developed using the Keystroke Dynamics as in [10] for recognition in virtual keyboard or in [11] that use correlation between keys as measured feature. A marketed product using the Keystroke Dynamics is the biopassword [14] could be adapted to the system of login of Windows NT/2000/XP.

III. METHODOLOGY

In the moment of the authentication of the user in a system some features can be obtained of the Keystroke Dynamics as, the keystroke duration and keystroke latency between successive keys, and the considered important aspects to have a good authentication are presented to follow them.

A. Base of Data

The formation of the pattern of the Keystroke Dynamics is obtained through the capture in the way as the user types your full name, containing 40 characters in the maximum. The used base was acquired of the work of Cavalcanti [9], in the process of acquisition the user informed your name 20 times in each moment that entered in the system, in the total of three sections and five times in the other users' name for formation of the impostors’ data. As result this acquisition a group of 24 classes, tends each class on mean 60 patterns of the user legitimize and 50 patterns of user impostors.

B. Features

The features are extracted from the user's keystroke for formation of template and later for verification. Two features were extracted during the keystroke: keystroke duration and keystroke latency. Keystroke duration is the interval of time that a key is pressed and liberated. Keystroke latency is the interval of time the pressed of between two consecutive keys [12] interval of time to liberate a key and press the key successor. In the Fig. 1 shows the extracted features: keystroke duration (duration) e keystroke latency (interval) of the word “IVAN”.

![Fig. 1. Extracted features of the Keystroke Dynamics](image)

The features extracted for formation of the pattern form the Features Vector (1) possessing keystroke duration and keystroke latency. Example in the Fig.1:

Features Vector = \[ I_{tp}, V_{tp}, A_{tp}, A_{tp}, N_{tp}, N_{tp} \]

(1)

\[ I_{tp} \]: Keystroke Duration of the key (I), that is, time that the user leads for press and liberate the key (I).

\[ V_{tp} \]: Keystroke Latency between of the keys (V) and (I), that is, interval of time that the user leads for liberate the key (I) and press the key (V).

The Keystroke Duration is just composed by positive whole values, however, The Keystroke Latency can contain positive values as negative. The negative value happens when the user before of liberate the key press the key successor. This usually happens with users that it possesses practice of typing.

C. Prototypes

Is the prototype generated of the Mean (\( \mu \)) and standard deviation (\( \sigma \)) that are calculated for each feature (\( P_{ij} \)) of the pattern with size \( n \), done compose by \( N \) pattern of the class, in agreement with the following equations:

\[
\text{Mean}(\mu) = \frac{1}{N} \sum_{i=1}^{N} P_{ij}
\]

(2)

\[
\text{Standard Deviation}(\sigma) = \frac{1}{N-1} \sum_{i=1}^{N} |P_{ij} - \mu|,
\]

(3)

D. Classifier Non-Weight Measure

The Classifier is responsible for the process of decision of the authentication. In this paper the authentication of the type verification is used, classifying accepts or it rejects the user, based on Criterion of Separation (Threshold). The Classifier verifies the similarity between the pattern to be verified and the template of the prototypes, using the Distance Pattern between the vector of feature of the pattern and the prototype. The distance is calculated from the equation (4):

\[
D(\text{pattern, template}) = \frac{1}{n} \sum_{i=1}^{n} |X_i - \mu_i| \sigma_i
\]

(4)

E. Classifier Weight Measure

Weighted probability measure: some features are more reliable than others simply because they come from a larger sample set [15]. Furthermore, let each component of the pattern vectors be the Mean (\( \mu \)), standard deviation (\( \sigma \)), number of occurrences (\( o \)), and data value for the \( in \) feature. The score is calculated from the equation (5):

\[
\text{Score}(\text{pattern, template}) = \sum_{i=1}^{n} \left( s_i \cdot w_i \right)
\]

(5)

\[
s_i = \frac{1}{o_i} \sum_{j=1}^{o_i} \left| X_j - \mu_j \right| \sigma_j
\]

(6)
Where the weight of the feature \( i \) is the ratio of its occurrences relative to all other features in the pattern. Feature that are based on many occurrences are considered more reliable and weighted higher than those features that come for a smaller sample set.

\[
\mathbf{w}_i = \begin{cases} 
0 & \text{if } o_i \text{ is blank} \\
\frac{o_i}{\sum_{k=1}^{n} (o_k)} & \text{otherwise}
\end{cases}
\]  

\( (7) \)

Where the weight of the feature \( i \) is the ratio of its occurrences relative to all other features in the pattern. Feature that are based on many occurrences are considered more reliable and weighted higher than those features that come for a smaller sample set.

\[
\mathbf{w}_i = \begin{cases} 
0 & \text{if } o_i \text{ is blank} \\
\frac{o_i}{\sum_{k=1}^{n} (o_k)} & \text{otherwise}
\end{cases}
\]  

\( (7) \)

**F. Criterion of Separation**

A pattern is only authenticated, if the calculated distance between features vector of the pattern and the template of the prototypes to be inside of the value of the Threshold adopted. The separation criterion or Threshold defines two areas: users and impostors.

\[
D(\text{pattern, template}) < \text{Threshold} \quad \text{(8)}
\]

or

\[
\text{Score(pattern, template)} < \text{Threshold} \quad \text{(9)}
\]

The value of the threshold can admit two forms: assumed the same value for all of the classes and values of independent thresholds for each class, each class is treated individually, depending on the class, can reach better results and more trustful the measure that the number of patterns of prototypes increases.

### IV. Experiments

The experiments were accomplished with 24 classes; containing patterns of the user legitimize and user impostors, these divided in patterns of the Prototypes set and tests, where the Prototypes set is composed by 30 patterns of the class and the test set is composed by 30 class patterns and 50 impostors patterns.

The performance of the system of authentication biometrics is measured through two error rates:

- False Rejection Rate (FRR), also called Error of Type I, represents the percentage to reject incorrectly a legitimate user owed some variation in your normal type of typing. This error cause frustration, the user will have to type the pattern again.

- False Acceptance Rate (FAR), also called Error of Type II, represents the percentage of incorrect acceptance the user impostors as a legitimate user. This type of error is caused by fraud. The authentication systems are configured in accordance with the type of application could have a weak detection (low FRR and high FAR) or a sensitive detection (low FAR and high FRR).

In fig. 2 it show an example of the relationship between FRR and FAR, can observe three important points: the point ZeroFRR indicates the value of FAR when the FRR is equal the zero, the point Equal Error Rate (ERR) indicates the value when FAR and FRR are equal and the point ZeroFAR indicates the value of FRR when the FAR is equal the zero.

Initially, features of the features vector were analyzed: Keystroke Duration and Keystroke Latency, a mean and standard deviation of the 30 patterns for formation of the template and choice of the Threshold for each class. And two experiments were made: one combining keystroke duration and keystroke latency, and other selection of characteristics.

**A. Threshold**

This experiment is to verify the effectiveness of the Threshold, using a Local Threshold attributing thresholds independent for each class, with the features of keystroke duration and the keystroke latency, using classifier Non-Weight Measure and using the mean of 30 patterns for the formation of the Prototypes set varying the values of the Threshold at different moments.

In the first moment the values are between zero and one, with a variation of 0.1. From this result can meet the concentration of the patterns, between an inferior threshold (where FRR = 100% and FAR = 0%) and a superior threshold (FRR = 0% and FAR = 100%), in second moment with a variation of 0.01 of these also new thresholds are found inferior and superior for accomplishment of the following test varying the threshold. The results of the experiments with the variation of the Threshold for FRR when FAR = 0% can be seen in Table I.

<table>
<thead>
<tr>
<th>Threshold Variation</th>
<th>%FRR (ZeroFAR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0,1</td>
<td>68,33</td>
</tr>
<tr>
<td>0,01</td>
<td>5,87</td>
</tr>
<tr>
<td>0,001</td>
<td>4,58</td>
</tr>
<tr>
<td>0,0001</td>
<td>4,21</td>
</tr>
<tr>
<td>0,00001</td>
<td>4,21</td>
</tr>
<tr>
<td>0,000001</td>
<td>4,21</td>
</tr>
</tbody>
</table>

**B. Features**

Experiments with only a feature: Keystroke Duration or Keystroke Latency; varying the classifier, and the mean of 30 pattern for the formation of the Prototypes set varying the values of the Threshold 0.00001, and the Classifiers: Classifier Weight Measure and Classifier Non-Weight Measure. It is
observed in table II that for each feature the two classifier obtained result similar and the results only using the feature Keystroke Duration were a little better that in the use only of the Keystroke Latency.

| TABLE II | FRR ADOPTING (ZEROFAR) |
|-----------------|-----------------|-----------------|
| Classifier      | Keystroke Duration | Keystroke Latency |
| Non-Weight Measure | 7.79             | 9.63             |
| Weight Measure   | 7.79             | 9.63             |

C. Combination of the Feature Keystroke Duration and Keystroke Latency

This experiment was made using the combination of the features Keystroke Duration and Keystroke Latency. Purpose of the combination is to diminish the rates and to improve the security of the system. Can be observed in Table III the results using the Classifier Weight Measure were superior to results only using Classifier Non-Weight Measure.

| TABLE III | FRR ADOPTING (ZEROFAR) |
|-------------|-----------------|-----------------|
| Classifier   | Keystroke Duration | Keystroke Latency |
| Non-Weight Measure | 4.21             |                 |
| Weight Measure          | 4.12             |                 |

D. Select of Features

With intention to find a subset from the set of features that it can reduce the errors rates. An experiment was made selecting N features of the features vector with the minors of standard deviation, eliminating the features less significant. Using the combination of the features keystroke duration and the keystroke latency, and the mean of 30 patterns for the formation of the Prototypes set varying the values of the Threshold 0.00001, and the Classifiers: Classifier Weight Measure and Classifier Non-Weight Measure. It is observed in Table IV that selecting 90% of the characteristics obtained a reduction of the FRR passing the 4.08% which ZeroFAR for Classifier Non-Weight Measure and 3.83% FRR which ZeroFAR for Classifier Weight Measure.

| TABLE IV | FRR ADOPTING (ZEROFAR) WHEN THE SELECTION OF FEATURE VARIES |
|-----------------|-----------------|-----------------|
| Classifier      | % feature 70 80 90 100 |                  |
| Non-Weight Measure | 5.04 4.5 4.08 4.21 |                  |
| Weight Measure   | 4.79 4.5 3.83 4.12 |                  |

The methodology proposal uses two characteristics of the Keystroke Dynamic: Keystroke duration and keystroke latency. Some experiments were made observing the changes in different aspects boarded in the methodology. Comparison of the features, the best resulted were found when combined as features, and when analyzed the separate features the Keystroke Duration better were resulted that the Keystroke Latency. Comparison of the classifiers, the best resulted were found when used the Classifier Weight Measure obtaining results superiors compared to the results obtained by the Classifier Non-Weight Measure.

Experiment with selection of features that aim at obtain minors errors rates from with the elimination of certain features, Experiment with selection of features that aim at obtain minors errors rates from with the elimination of certain features, was found when selecting 90% of the characteristics.

Comparing with the work of Cavalcanti et. al [9] it was possible to improve the rates for 3.83% FRR and ZeroFAR. For future works, it intends to combine Keystroke Dynamics with techniques physical biometrics, where the process of personal authentication from physical or behavioral characteristic.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the Cavalcanti et. al for making available the base of data, without her would not be possible make the work.

REFERENCES


