# Variation Detection applied in User Signature Verification

Matheus L. dos Santos [1]
Marcelo K. Albertini [1]
Rodrigo F. de Mello [1]

**Abstract:** Behavior studies have been conducted by scientists and philosophers who approach subjects such as star and planet trajectories, society organizations, living beings evolution and human language. With the advent of computer, new challenges have been observed in order to explore and understand the behavior variations of interactions with systems. Motivated by those challenges, this work proposes a new approach to automatically cluster, detect and identify behavior patterns. In order to validate this approach, we have modeled the knowledge embedded in interactions of handwriting signatures. The generated knowledge models were, afterwards, employed to verify signatures. Obtained results were compared to other related approaches presented in SVC2004, the First International Signature Verification Competition.

## 1 Introduction

Behavior studies have been conducted by different scientists and philosophers. Great philosophers analyzed object interactions (such as: animals, nature, stars, human behavior, etc.) in order to understand them. Among those are: Plato [24] who, by considering behavior studies, established a philosophical understanding about society, politics and metaphysics. Aristotle [4], as part of his research interests, investigated causality and its influence on human behavior. Galileo [12] considered sky observations to determine the position and trajectories of planets. Darwin [9] analyzed the animal behavior and the habitat to propose the natural selection theory.

During the last century, Skinner and Chomsky [28, 8] investigated the human behavior, trying to understand how human language and learning evolves over time. Finally, the interests on object behavior have been very important along the centuries. With the advent of computer science, a series of new possibilities on behavior study has brought up. They are consequences of new forms of interaction, such as: the use of mouse, keyboard and other devices as well as instant messaging applications.

[1]Universidade de São Paulo
Instituto de Ciências Matemáticas e de Computação
Department of Computer Science
Av. Trabalhador Sãocarlense, 400
Phone: +55 (16) 3373-9675
Zip 13560-970 - São Carlos - SP - BRAZIL
matheusls@gmail.com, {albertini, mello}@icmc.usp.br

Among the researches targeting new interaction forms are the works presented in the First International Signature Verification Competition (SVC2004) [30]. That event promoted the competition of recognition techniques applied on digitally-obtained handwritten signatures. Techniques have considered the user behavior during the writing, instead of the signature picture. Datasets were made available to evaluate and compare the different submitted approaches.

Motivated by the behavior analysis and by the possibility of improving the human-computer interaction, this work proposes a new approach to automatically group, detect and identify behavior pattern variations. Behavior profiles are obtained, which support the study of objects such as user interactions, application operations, system intrusions, user authentication, etc. The approach considers clustering techniques [3, 7, 19], Markov Chains [22, 10] and Theory of Information [27, 5].

In order to validate the proposed approach, we conducted experiments aiming at recognizing digitally-obtained handwritten signatures. We considered the datasets of SVC2004 and compared the results to other approaches.

Related work is presented in section 2. The techniques involved in the proposed approach are presented in section 4. Section 5 presents the experiments on signature verification. The obtained results and analysis are presented in section 6. Finally, section 7 describes conclusions and future work.

## 2 Related Work

There are different approaches to group, classify, evaluate and analyze user behavior [6, 13, 20, 21, 23, 26].

Brosso [6] proposes an user authentication system for computer networks, which considers behavior analysis and face recognition to define the confidence level of an user. The behavior analysis applies context awareness concepts, which studies the adaptations of applications, people and objects over time [25]. Besides context awareness, this work considers five semantic dimensions (*Who*, *Where*, *What*, *When*, *Why*), defined by Abowd [1, 2], which is employed in the specification and modeling of contextual information. Such information supports the relevance level. An user behavior matrix is defined according to the context awareness information. This information summarizes the user characteristics, locality, system interactions, habitual behavior and user confidence constraints.

Godoy & Amandi [13] propose a technique to identify user interests according to the historical web profile. This technique was implemented in the Web Document Conceptual Clustering algorithm [14], which supports the estimation of a profile without previous knowledge about the user interests. Profiles are organized in hierarchical trees, where the most usual

interests are at the higher levels. The relevance of user interests is defined according to the frequency of terms in accessed web pages.

Lee et al. [20] proposed PRORD (*Proactive Request Distribution*), a new load balancing policy for distributed web servers. PRORD estimates future accesses by considering web cache information. Estimatives are employed to preload web pages and reduce the request time completion.

Macedo et al. [21] propose WebMemex, a recommendation system which analyzes historical user navigation profiles. WebMemex obtains HTTP request information through Web proxy interception. Thus, it grabs request information such as: IP address, user ID, user lifetime (the time the user is active) and the URL addresses. Such information is stored in a database which also contains links associated to the currently accessed document.

Pepyne et al. [23] propose an user profile classification method which employs queuing theory and logistic regression. It is applied to network security systems aiming at identifying specific user groups, such as the ones which execute periodic tasks. According to the authors, this approach helps to find out frauds by analyzing user anomalous behavior.

## 3 Signature Verification

This paper focuses on a signature verification application due to the available datasets and different approaches to be compared against [18, 29, 15].

Kholmatov & Yanikoglu [18] propose an approach to classify digitally-obtained handwritten signatures. It recognizes signatures by evaluating dynamic features, such as the pen pression on the surface, angle in between the pen and the writing surface and speed, instead of signature pictures (static approaches). Authors compare signatures by selecting three characteristics: the difference in between $x$ and $y$ coordinates, the difference in between signature points and the angles in between points.

Skrbek [29] integrate a handwritten signature recognition algorithm to TPS (Trusted Pocket Singer[2]). TPS is a handheld-sized PDA (Personal Digital Assistant) which has a LCD touch screen and executes the GNU/Linux operating system. The recognition algorithm employs DTW (Dynamic Time Warping) dissimilarity measure to compare signature segments.

Kalera et al. [15] propose an off-line approach to recognize paper-and-pencil handwritten signatures. Information is, therefore, obtained from the resulting picture.

[2] Available at: http://truposign.sit.fraunhofer.de.

## 4 Proposed Approach

This paper proposes a new approach to automatically group, detect and identify behavior pattern variations. It is composed of the following steps: definition of data distributions to characterize user interactions; artificial neural network grouping; groups, this is clusters, and their visiting order are used to compose Markov Chains; the Shannon's Entropy is used to measure the complexity of behavior shown by every Markov Chain [27]; signature comparison by using Entropy variations.

In order to exemplify and validate the proposed approach, we consider the user signature dataset published by the First International Signature Verification Competition[3] (SVC2004) [30]. It contains signature information of $40$ different users. There are $40$ signatures for each user. The $10$ first ($S1$ – $S10$) are true, and consecutively written (these are used for training), the next $10$ signatures ($S11$ – $S20$) are also true, but they were captured in one week intervals (simulating real situations). The $20$ last ($S21$ – $S40$) are false trained signatures.

The database is also divided in two parts: $Task1$ and $Task2$. Both ($Task1$ and $Task2$) contain information on signatures of $40$ users according to the previous description. The differences of $Task1$ and $Task2$ are the stored information per signature. $Task1$ contains four attributes per signature: the $x$ coordinate, the $y$ coordinate, the timestamp and the pen button status[4] ($1$ = pen is touching the tablet, $0$ = pen is not touching it). $Task2$ stores other three attributes: the azimuth (pen rotation), high and pressure. Either the information of $Task1$ or $Task2$ are stored in text files named as U$z$S$k$.TXT, where $z$ is the user identifier (from $1$ to $40$) and $k$ is the signature identifier (from $1$ to $40$). The dataset information was digitally captured by using a tablet WACOM Intous. Data were acquired at a sample rate of $10$ milliseconds. $Task1$ was considered in our experiments.

The next sections present each step of the proposed approach and a corresponding example.

### 4.1 Step 1 – Data distributions

In the first step of the proposed approach, user interaction information is analyzed and represented by different data distributions. For the database $Task1$, there are signature coordinates and timestamp information. To better represent such data (Table 1), we proposed seven different distributions to characterize user behavior: $DD1$, $DD2$, $DD3$, $DD4$, $DD5$, $DD6$ and $DD7$.

$DD1$ represents the differences in between the $x$ and $y$ coordinates for data points $p_k = (x_k, y_k)$ and $p_{k-1} = (x_{k-1}, y_{k-1})$. $DD2$ computes the time interval in between every

[3] Available at: http://www.cse.ust.hk/svc2004/

[4] The status indicates whether the pen in on the tablet.

consecutive signature point (where Timestamp(.) is a function which returns the data point timestamp). $DD3$ represents the signature point frequency (where Label(.) is a function to label equal data points). In this situation, a label is defined for each different signature point, when a point is repeated, it receives the same label. Distributions $DD4$ and $DD5$ are generated by computing the derivative in between consecutive signature points, however, in distribution $DD5$, the derivative is divided by time. Distribution $DD6$ and $DD7$ represent the Euclidean distances in between signature points. However, $DD7$ divides those distances by the time interval (handwriting speed). An example of $DD2$ is presented in Figure 1.

**Table 1.** Equations of Data Distributions

| Distribution | Equation |
|---|---|
| $DD1$ | $(x_k - y_k) + (x_{k-1} - y_{k-1})\ \forall k$ |
| $DD2$ | $\text{Timestamp}(x_k, y_k) - \text{Timestamp}(x_{k-1}, y_{k-1})\ \forall k$ |
| $DD3$ | $\text{Label}(x_k, y_k)\ \forall k$ |
| $DD4$ | $\frac{(x_k, y_k)}{(x_{k-1}, y_{k-1})}\ \forall k$ |
| $DD5$ | $\frac{\frac{(x_k, y_k)}{(x_{k-1}, y_{k-1})}}{\text{Timestamp}(x_k, y_k) - \text{Timestamp}(x_{k-1}, y_{k-1})}\ \forall k$ |
| $DD6$ | $\text{Euclidean}((x_k, y_k), (x_{k-1}, y_{k-1}))\ \forall k$ |
| $DD7$ | $\frac{\text{Euclidean}((x_k, y_k), (x_{k-1}, y_{k-1}))}{\text{Timestamp}(x_k, y_k) - \text{Timestamp}(x_{k-1}, y_{k-1})}\ \forall k$ |

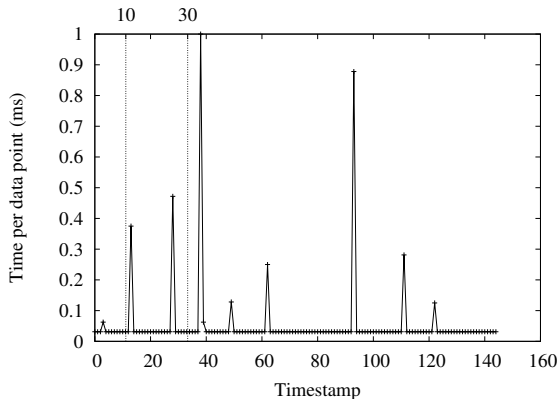



**Figure 1.** Data distribution example

The relevance of creating several data distributions is presented in section 5, which

describes experimental results. During the experiments, we observed that every user can be better characterized by one distribution.

### 4.2 Step 2 – Grouping and Markov Chains

In this step, the user data distributions are grouped by using an artificial neural network. User behavior is, therefore, represented by Markov Chains.

We considered the SONDE (Self-Organizing Novelty Detection) artificial neural network [3], which clusters data and automatically generates Markov Chains and Entropy curves. SONDE groups similar patterns in same clusters and creates new neurons to represent non-expected patterns. Figure 2 depicts how input patterns are grouped.

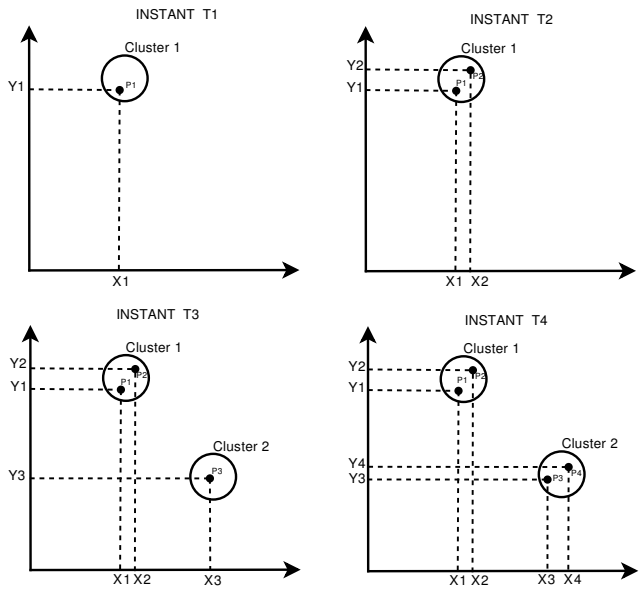



**Figure 2.** Example of grouping

The user behavior is estimated at every time instant, when a Markov Chain is computed. Each state of the Markov Chain is represented by a neuron of SONDE. As SONDE groups a new pattern, it estimates a new Markov Chain, which represents the instantaneous user behavior.

By using the same example of Figure 2, Figure 3 presents transition matrices and the

respective instantaneous Markov Chains for the handwritten signature. The transition matrix is updated at every new grouping, this is, the matrix stores the executed transition **from** state $x$ **to** state $y$. According to the example in Figure 3, the first input pattern was grouped at the state 0 ($instant1$). Then, at the $instant2$, the second pattern was also grouped at 0, but in this situation, as it is the second input pattern, it happens a transition in between the first and the second group (or neuron). Those state modifications are updated in the transition matrix (**from** 0 **to** 0, in this circumstance). Following those steps, for each new input pattern, the transition matrix is updated.

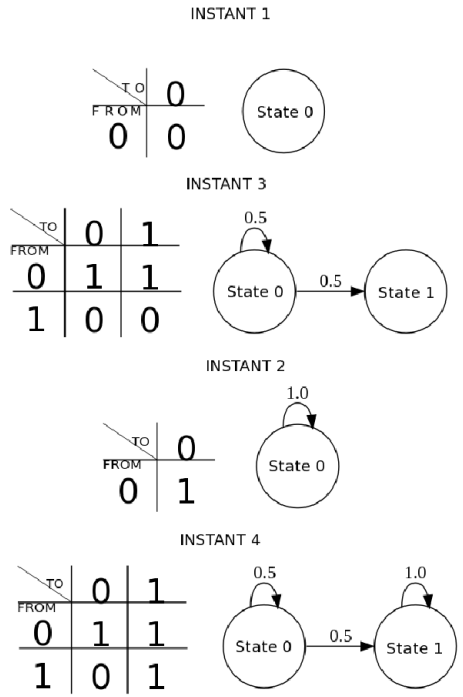



**Figure 3.** Example of the transition matrix and Markov Chains

After grouping, identify the state transition probabilities (transition matrix) and update Markov Chains at every time instant. The next step of the approach consists in computing the Shannon's Entropy, of the Markov Chains and, therefore, represent the user behavior.

### 4.3 Step 3 – Entropy measurement

After grouping the seven previously presented distributions (generated in Step 1), we have a set of Markov Chains for each one. Then, we measure the Entropy (by Shannon [27]) of Markov Chains for every data distribution.

For each distribution on the user signature dataset, a characteristic curve is generated, which depicts user behavior modifications. Figure 4 represents an example of Entropy curve (user behavior) for the data distribution $DD2$. In another section, we will observe that every user is better represented by a different curve.

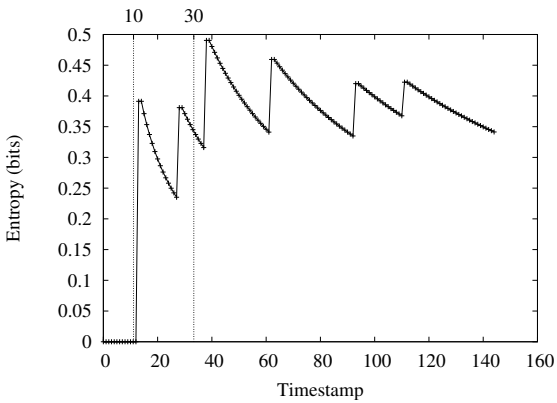



**Figure 4.** Example of an Entropy curve which represents the user signature behavior using data distribution $DD2$

The next step is responsible for comparing user profiles (Entropy curves) according to their signatures.

### 4.4 Step 4 – Dissimilarity measurements

This step makes comparisons in between user profiles to indicate true and false signatures. At the same time, this step validates the proposed approach. Two techniques are employed to compare Entropy curves: DTW (Dynamic Time Warping) [17] and CDM (Compression-based Dissimilarity Measure) [16].

The result analysis was conducted by comparing Entropy curves of a true signature against a false one (considering the same user and data distribution). We expect that true signatures of the same user present similar Entropy variations. Figures 5 and 6 depict the

behavior difference in between true and false signature of the same user in the same data distribution. In such scenario, we observe a high degree of similarity in between true signatures (Figure 5(a) and 5(b)) and a low degree when considering false ones (Figure 6(a) and 6(b)). The true signatures present similar distributions, Entropy levels and timestamps. On the other hand, the false signatures present lower Entropy levels and greater timestamps (apparently, people need additional time to fake a signature).

In this example, it is not hard to visually separate a true and false user profile. However, we need dissimilarity measurements to make such comparisons on computers. Section 5 presents experimental results comparing user signature profiles.

## 5 Experiments and Results

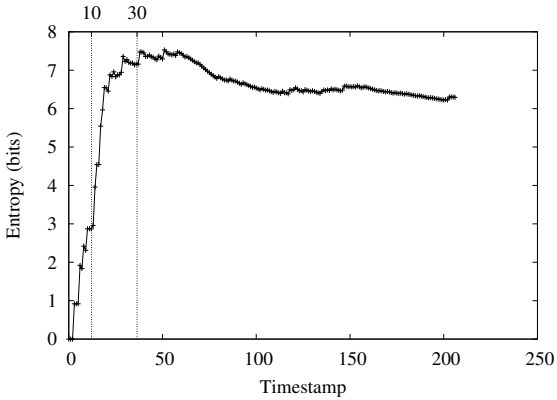
Experiments were conducted considering the same rules proposed in SVC2004. According to competition rules, 10 experiments are executed for each user, considering the random selection of 5 true out of the 10 first and true signatures ($S1$ – $S10$) of the training dataset. In each experiment, training results are compared against true signatures, written in one week intervals ($S11$ – $S20$), 20 false and trained signatures ($S21$ – $S40$), and 20 false signatures randomly selected (considering true signatures of other users). In this way, each user is tested 10 times and his/her training signatures are compared to other 10 true and 40 false ones, resulting in 50 comparisons for each experiment.

Figure 7 presents the dissimilarity results obtained by employing DTW and CDM measurements using data distribution $DD2$. In such figure, the average sum of errors and the confidence intervals[5] are computed for 50 signatures, begin the first ten true, the next twenty (in range 11 and 30) are false trained and the last 20 are signatures of different users (randomly selected), therefore, they are also false. The results of DTW are presented in logarithmic scale, which improves the visualization.

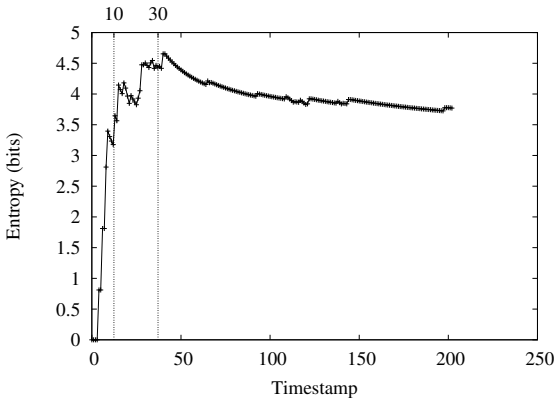
The previously presented experiment (Figure 7) was conducted by using information on the signatures of a single user (user 1 of the database $Task1$ of SVC2004). The same experiments were conducted for all the 40 database users, considering the dissimilarity measurements DTW and CDM to compare profiles.

As the amount of information generated by experiments is very large (seven data distributions per user in a total of 40 users, with 2 dissimilarity measurements), the result analysis is therefore complex. For this reason, a very commonly considered technique, named Receiver Operating Characteristic (ROC curve)[11], was employed to improve evaluation and analysis.

[5]Confidence interval of 95% – as there are few samples, equals to 10 (number of tests according to the considered dataset), we adopted the t-Student probability distribution to compute such intervals ($t_{0.025-10} = 2.228$).



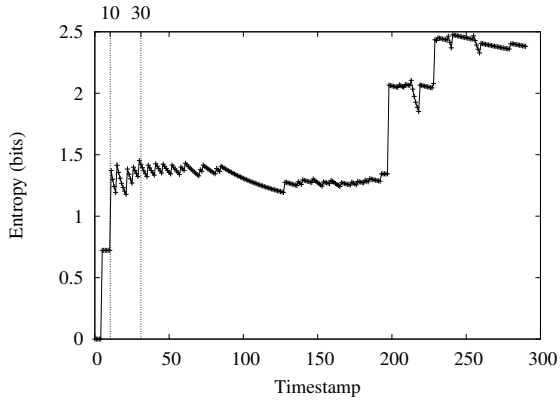

(a) Signature 1 - True



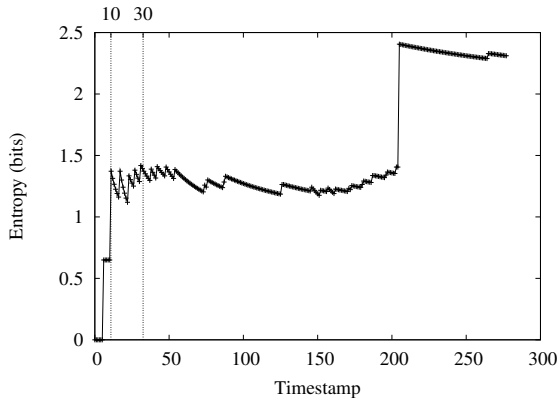

(b) Signature 2 - True

**Figure 5.** Behavior comparison in between true signatures (1 and 2) of the same user

The ROC curve depicts the sensitivity variation (or true positive rate) and specificity (or false negative rate) for different scenarios. In this situation, the false positives are represented by false signatures identified as true and the true positives as true signatures correctly identified. An ideal curve is the one which tends to the top left region of the space, this is, it




(a) Signature 21 - False

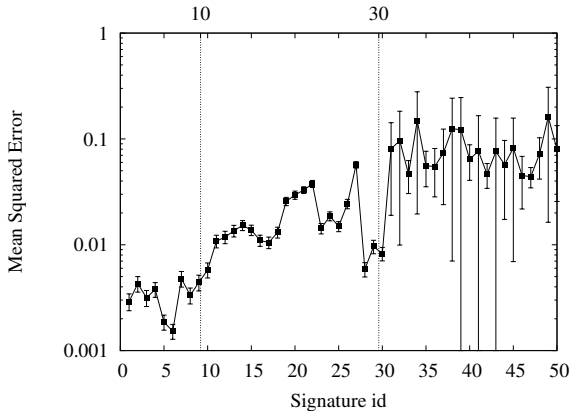



(b) Signature 22 - False

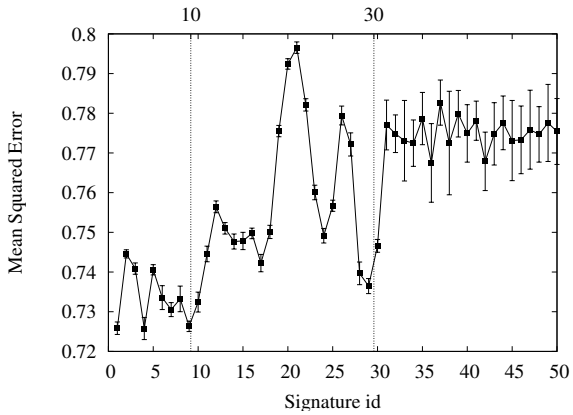
**Figure 6.** Behavior comparison in between false signatures (21 and 22) of the same user

presents high rate of true positives and low rate of false positives.

For each error curve generated in experiments, all error values were evaluated along the $y$ axis (using Mean Squared Error – MSE) and the false positive and true positive rates




(a) DTW




(b) CDM

**Figure 7.** Example of the results according to the SVC2004 rules – data distribution $DD2$

computed accordingly. In the same way the results are presented in SVC2004, we generated two ROC curves for each user and data distribution: the first compares true against false trained signatures and the second compares true to 20 randomly selected signatures of

different users.

From the ROC curve, we can visualize all relations among true and false positive rates for a certain data distribution. ROC curves summarize all experimental results, containing the comparisons of true signatures, false trained signatures and the ones of other users (also false).

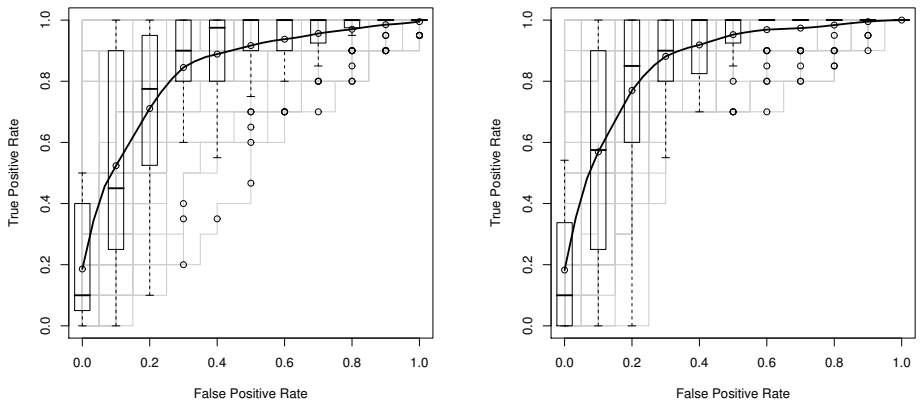
By analyzing the curves, either obtained using DTW or CDM, we observe that, for false trained signatures, the data distribution $DD3$ has presented the best results to identify profiles (higher true positive and lower false positive rates). Analyzing the ROC curves that summarize the comparison of true signatures against the ones of other users, we observe that DTW has presented better results with the distribution $DD1$ and CDM with $DD2$. A summary of the best distribution for each user is presented in Table 2.

**Table 2.** Percentage of signatures that each distribution is the best discriminator

| Distribution | **DTW** | |
|---|---|---|
| | False trained | Other users |
| $DD1$ | 20.0% | 72.5% |
| $DD2$ | 17.5% | 10.0% |
| $DD3$ | 47.5% | 17.5% |
| $DD4$ | 7.5% | 0.0% |
| $DD5$ | 2.5% | 0.0% |
| $DD6$ | 5.0% | 0.0% |
| $DD7$ | 0.0% | 0.0% |
| Distribution | **CDM** | |
| | False trained | Other users |
| $DD1$ | 22.5% | 30.0% |
| $DD2$ | 15.0% | 35.0% |
| $DD3$ | 52.0% | 30.0% |
| $DD4$ | 2.5% | 0.0% |
| $DD5$ | 0.0% | 0.0% |
| $DD6$ | 2.5% | 5.0% |
| $DD7$ | 5.0% | 0.0% |

However, this does not imply that there is a best distribution to represent all users. According to section 4.1, each user has a distribution to better present his/her interaction and, consequently, the behavior. To confirm this concept, four ROC curves were generated, two presenting comparison results of true signatures and false trained ones and, two more comparing the true signatures to the ones of other users. Those curves (Figures 8 and 9) present

results for both dissimilarity techniques, average, median, quantiles and outliers which summarize results for each one of the 40 users, considering their best data distribution.



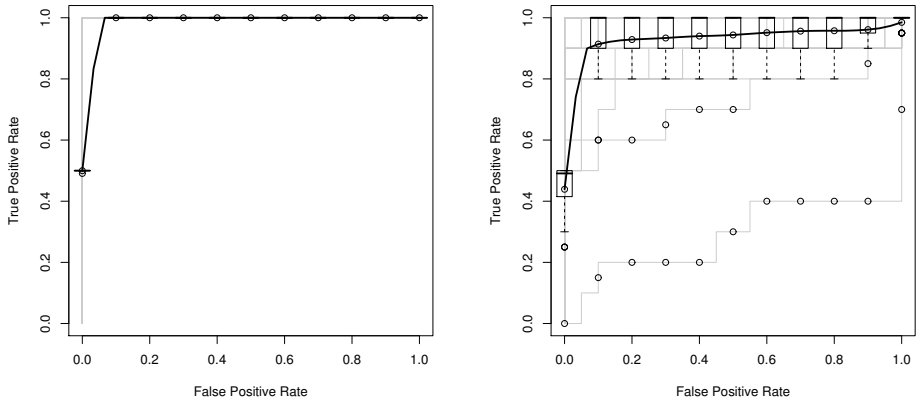

(a) DTW – false trained

(b) CDM – false trained

**Figure 8.** Average of the ROC curves, comparing true signatures to false trained ones and true signatures to the ones of other users – considering DTW and CDM and the best data distributions to characterize each user (Results – Part I)

As expected, the results presented in Figures 8(a), 8(b), 9(a) and 9(b) are better than any of the seven distributions isolated. This result confirms the idea that each user has a distribution which better describes his/her behavior. Figures 8 and 9 present the average of ROC curves of the best data distributions for each experiment.

We also observe a better dissimilarity measurement to compare the signatures of a specific user. Experiments comparing true against false trained signatures presented better results when using CDM, as observed in Figures 8(b) and 8(a), respectively. In experiments comparing true against signatures of other users, DTW generated the best results, respectively depicted in Figures 9(a) and 9(b). As to distributions, the dissimilarity measurement could not be generalized to all users either.




(a) DTW – other users

(b) CDM – other users

**Figure 9.** Average of the ROC curves, comparing true signatures to false trained ones and true signatures to the ones of other users – considering DTW and CDM and the best data distributions to characterize each user (Results – Part II)

## 6 Result Analysis

This section compares the results of the proposed approach to the ones presented in SVC2004. This comparison considers the Equal Error Rate (EER) measurement, as proposed in this competition. EER represents the lower false positive and negative rates for the same threshold. Figure 10 shows the rates of false positive and negative, according to the same threshold. We observe that better results are obtained at the crossing point that better splits the distributions of false positive and negative rates. In this circumstance, the threshold is close to 3 (precisely $2.84787$) and EER is equal to $0,3$ ($30\%$). In this way, the lower EER is, the higher is the precision of the evaluated approach.

In the context of this work, EER was computed for all experiments. Therefore, for each experiment, we obtained the average, the standard deviation and the highest value of EER for each user data distribution ($DD1$, ..., $DD7$). Besides that, as presented in the previous section, we have selected and conducted experiments using the most indicated distributions to characterize user profiles. Tables 3 and 4 show the EERs of experimental results with DTW and CDM, respectively.

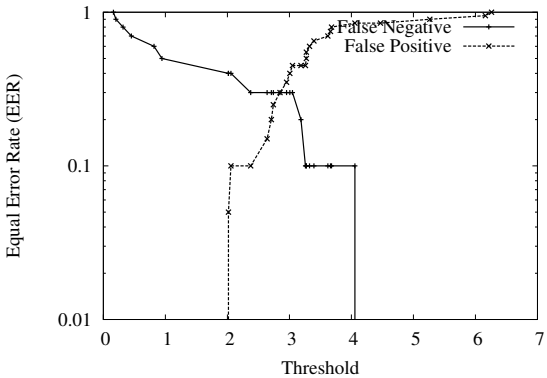



**Figure 10.** Example of the distribution of the false positive and negative rates. The crossing point in between distributions represents the Equal Error Rate (EER)

By analyzing the DTW results, presented in Table 3, we may observe that the average EER of the best user data distributions, containing comparisons against other users, was zero. This confirms that the proposed approach was capable of completely segmenting user profiles, this is, it was able to separate true signatures of the other users'. When considering true signatures and the false trained, the EER for the best user data distributions was $18.25\%$. This value is justified due to, in this approach, the behavior found in false trained signatures approximates to the ones in true signatures.

Similar behavior was observed when employing CDM, according to the results presented in Table 4. However, in this circumstance, experimental results comparing true signatures to other users' (considering the best user data distributions) are worse than the results obtained by DTW. CDM has EER equals to $8.00\%$ against $0.00\%$ for DTW. However, in experiments comparing true signatures to false trained ones, CDM has presented better results. With CDM, using the best user data distributions, the EER was $17.63\%$ while DTW has obtained $18.25\%$.

Those results were compared to the ones obtained by SVC2004 approaches. Table 5 shows the results of the approaches submitted to the competition, according to their performance. By analyzing Table 5, we observe that the best result for experiments comparing true signatures to false trained has EER equals to $2.84\%$ (team 6) and EER equals to $1.85\%$ when comparing to other users' (team 24). In this scenario, the obtained results would be ranked in second-to-last place for CDM (EER $17.25\%$) when comparing true signatures to false trained ones and, in first place, using DTW (EER $0.00\%$), when comparing true signatures to other

**Table 3.** Equal Error Rates using DTW

| Distribution | **True against False trained** | | |
|---|---|---|---|
| | Average | Standard Deviation | Highest |
| $DD1$ | 41.63% | 18.34% | 80.00% |
| $DD2$ | 39.75% | 16.25% | 65.00% |
| $DD3$ | 25.13% | 18.34% | 65.00% |
| $DD4$ | 46.38% | 10.92% | 70.00% |
| $DD5$ | 44.63% | 10.71% | 75.00% |
| $DD6$ | 43.25% | 16.59% | 80.00% |
| $DD7$ | 49.13% | 12.40% | 80.00% |
| **Best** | 18.25% | 12.07% | 40.00% |
| Distribution | **True against Other users** | | |
| | Average | Standard Deviation | Highest |
| $DD1$ | 5.38% | 12.32% | 45.00% |
| $DD2$ | 11.63% | 14.47% | 50.00% |
| $DD3$ | 0.25% | 1.58% | 10.00% |
| $DD4$ | 23.00% | 16.16% | 70.00% |
| $DD5$ | 22.50% | 13.16% | 70.00% |
| $DD6$ | 8.00% | 16.12% | 80.00% |
| $DD7$ | 30.00% | 23.45% | 80.00% |
| **Best** | **0.00%** | **0.00**% | **0.00**% |

users'.

The three first approaches presented in Table 5 (teams 6, 24 and 26) were proposed by the authors referenced in section 3. This does not necessarily imply that the related works in section 3 are the same ones submitted to SVC2004. The objective of SVC2004 was to promote a competition aiming at evaluating different techniques, therefore, the competition did not published additional information on the submitted works, only data authorized by the teams (such as involved people and institutions).

We may mention that, besides the good results, the proposed approach is not specifically focused on signature verification. Actually, it is a new approach to group, detect and identify behavior variations. Consequently, there is still room to tune the experiments to obtain better results for the signature verification domain. Therefore, experiments and comparisons are useful to observe the contributions of the proposed approach and make clear that it can represent behavior in any time series.

**Table 4.** EERs using CDM

| Distribution | **True against False trained** | | |
|---|---|---|---|
| | Average | Standard Deviation | Highest |
| $DD1$ | 38.38% | 15.29% | 65.00% |
| $DD2$ | 36.50% | 16.49% | 70.00% |
| $DD3$ | 23.00% | 17.53% | 60.00% |
| $DD4$ | 44.25% | 11.91% | 65.00% |
| $DD5$ | 41.75% | 12.22% | 65.00% |
| $DD6$ | 40.63% | 14.90% | 85.00% |
| $DD7$ | 39.63% | 11.90% | 75.00% |
| **Best** | **17.63%** | **11.49%** | **40.00%** |
| Distribution | **True against Other users** | | |
| | Average | Standard Deviation | Highest |
| $DD1$ | 33.38% | 24.48% | 80.00% |
| $DD2$ | 23.25% | 26.03% | 90.00% |
| $DD3$ | 17.25% | 21.66% | 60.00% |
| $DD4$ | 47.63% | 24.07% | 90.00% |
| $DD5$ | 44.13% | 22.87% | 95.00% |
| $DD6$ | 34.75% | 23.53% | 90.00% |
| $DD7$ | 41.63% | 25.43% | 95.00% |
| **Best** | 8.00% | 13.05% | 70.00% |

## 7 Conclusions

This paper proposes a new approach to group, detect and identify user behavior by employing an artificial neural network, Markov Chains and Entropy measurement. The user behavior is represented by Entropy curves obtained from instantaneous Markov Chains. Such variations are employed to make comparisons among user profiles by using the dissimilarity measurements CDM and DTW.

Experiments were conducted to validate the proposed approach. They involved user interaction information when digitally handwriting their signatures. We considered a database proposed in SVC2004. Experimental results were summarized in ROC curves which allowed to evaluate the approach efficiency and compare it against others.

The analysis of those experiments allowed to confirm the approach ability to segment user profiles according to interactions during signature handwriting. We draw such conclu-

**Table 5.** Results of the approaches submitted to SVC2004

| Team ID | **True against False trained** | | |
|---|---|---|---|
| | Average | Standard Deviation | Highest |
| **6** | **2.84%** | **5.64%** | **30.00%** |
| 24 | 4.37% | 6.52% | 25.00% |
| 26 | 5.79% | 10.30% | 52.63% |
| 19$b$ | 5.88% | 9.21% | 50.00% |
| 19$c$ | 6.05% | 9.39% | 50.00% |
| 15 | 6.22% | 9.38% | 50.00% |
| 19$a$ | 6.88% | 9.54% | 50.00% |
| 14 | 8.77% | 12.24% | 57.14% |
| 18 | 11.81% | 12.90% | 50.00% |
| 17 | 11.85% | 12.07% | 70.00% |
| 16 | 13.53% | 12.99% | 70.00% |
| 4 | 16.22% | 13.49% | 66.67% |
| 12 | 28.89% | 15.95% | 80.00% |
| Team ID | **True against Other users** | | |
| | Average | Standard Deviation | Highest |
| 6 | 2.79% | 5.89% | 50.00% |
| **24** | **1.85%** | **2.97%** | **15.00%** |
| 26 | 5.11% | 9.06% | 50.00% |
| 19$b$ | 2.12% | 3.29% | 15.00% |
| 19$c$ | 2.13% | 3.29% | 15.00% |
| 15 | 2.04% | 3.16% | 15.00% |
| 19$a$ | 2.18% | 3.54% | 22.50% |
| 14 | 2.93% | 5.91% | 40.00% |
| 18 | 4.39% | 6.08% | 40.00% |
| 17 | 3.83% | 5.66% | 40.00% |
| 16 | 3.47% | 6.90% | 52.63% |
| 4 | 6.89% | 9.20% | 48.57% |
| 12 | 12.47% | 10.29% | 55.00% |

sion based on the EER result, for DTW, of $0.00\%$, when comparing true signature to other users'. In experiments comparing true signatures to false trained ones, we obtained an EER equals to $17.63\%$ (for CDM). This result is expected once the approach intends to group, detect and identify user behavior and, therefore, the false trained signatures are capable of faking some of the original aspects.

Finally, results allow to conclude that the proposed approach can be employed in different application domains, which motivates further work on process behavior characterization (to improve scheduling in operating systems), identification of web users, computer network traffic behavior and user authentication.

## 8 Acknowledgments

This paper is based upon work supported by Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), Brazil and Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of FAPESP or CAPES.

## References

[1] Gregory D. Abowd, Anind K. Dey, Peter J. Brown, Nigel Davies, Mark Smith, and Pete Steggles. Towards a better understanding of context and context-awareness. In *HUC '99: Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing*, pages 304–307, London, UK, 1999. Springer-Verlag.

[2] Gregory D. Abowd and Elizabeth D. Mynatt. Charting past, present, and future research in ubiquitous computing. *ACM Trans. Comput.-Hum. Interact.*, 7(1):29–58, 2000.

[3] Marcelo Keese Albertini and Rodrigo Fernandes de Mello. A self-organizing neural network for detecting novelties. In *SAC '07: Proceedings of the 2007 ACM symposium on Applied computing*, pages 462–466, New York, NY, USA, 2007. ACM.

[4] Aristotle. *De Anima*. 34 Editora, 1 edition, 2006. ISBN: 8573263512.

[5] Arieh Ben-Naim. *Entropy Demystified*. World Scientific Publishing Company, 2007.

[6] Maria Ines Lopes Brosso. *Autenticação Contínua de Usuários em Redes de Computadores*. Ph.d. theses, Politécnica da Universidade de São Paulo, São Paulo, SP, Brazil, 2006.

[7] Gail A. Carpenter, Stephen Grossberg, and David B. Rosen. Art 2-a: an adaptive resonance algorithm for rapid category learning and recognition. *Neural Netw.*, 4(4):493–504, 1991.

[8] Noam Chomsky. A review of B. F. Skinner's Verbal Behavior. *Language*, 35(1):26–58, 1959.

[9] Charles Darwin. *A Origem das Espécies*. Martin Claret, 1 edition, 2004. ISBN: 8572325840.

[10] E. B. Dynkin, T. Kovary, and D. E. Brown. *Theory of Markov Processes*. Dover Publications; Dover Ed edition, 2006.

[11] V. Froelicher, K. Shetler, and E. Ashley. Better decisions through science: Exercise testing scores. *Current Problems in Cardiology*, 28(11):589–620, 2003.

[12] Galileo Galilei. *The private life of Galileo*. Nichols and Noyes, 1870.

[13] Daniela Godoy and Analia Amandi. User profiling for web page filtering. *IEEE Internet Computing*, 9(4):56–64, 2005.

[14] Daniela Godoy and Analia Amandi. Modeling user interests by conceptual clustering. *Inf. Syst.*, 31(4):247–265, 2006.

[15] Meenakshi K. Kalera, Sargur N. Srihari, and Aihua Xu. Offline signature verification and identification using distance statistics. *IJPRAI*, 18(7):1339–1360, 2004.

[16] Eamonn Keogh, Stefano Lonardi, Chotirat Ann Ratanamahatana, Li Wei, Sang-Hee Lee, and John Handley. Compression-based data mining of sequential data. *Data Min. Knowl. Discov.*, 14(1):99–129, 2007.

[17] Eamonn Keogh and Chotirat Ann Ratanamahatana. Exact indexing of dynamic time warping. *Knowl. Inf. Syst.*, 7(3):358–386, 2005.

[18] Alisher Kholmatov and Berrin Yanikoglu. Identity authentication using improved online signature verification method. *Pattern Recogn. Lett.*, 26(15):2400–2408, 2005.

[19] T. Kohonen, S. Kaski, K. Lagus, J. Salojrvi, J. Honkela, V. Paatero, and A. Saarela. Self organization of a massive document collection, 2000.

[20] Heung Ki Lee, Gopinath Vageesan, Ki Hwan Yum, and Eun Jung Kim. A proactive request distribution (prord) using web log mining in a cluster-based web server. In *ICPP '06: Proceedings of the 2006 International Conference on Parallel Processing*, pages 559–568, Washington, DC, USA, 2006. IEEE Computer Society.

[21] Alessandra Alaniz Macedo, Khai N. Truong, José Antonio Camacho-Guerrero, and Maria da Graça Pimentel. Automatically sharing web experiences through a hyperdocument recommender system. In *HYPERTEXT '03: Proceedings of the fourteenth ACM conference on Hypertext and hypermedia*, pages 48–56, New York, NY, USA, 2003. ACM Press.

[22] S.P. Meyn and R.L. Tweedie. *Markov Chains and Stochastic Stability*. Springer-Verlag, London, 1993.

[23] D.L. Pepyne, Jinghua Hu, and Weibo Gong. User profiling for computer security. *American Control Conference, 2004. Proceedings of the 2004*, 2:982–987 vol.2, 2004.

[24] Platão. *A República*. Martins Fontes, 1 edition, 2006. ISBN: 8533623267.

[25] Bill Schilit and M. Theimer. Disseminating active map information to mobile hosts. *IEEE Network*, 8(5):22–32, 1994.

[26] Adelir José Junior Schuler and Anderson Luiz Fernandes Perez. Análise do perfil do usuário de serviços de telefonia utilizando técnicas de mineração de dados. *RESI - Revista Eletrônica de Sistemas de Informação*, 7(1):65–67, 2006.

[27] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423 and 623–656, July and October 1948.

[28] Burrhus Frederic Skinner. *Sobre o Behaviorismo*. Pensamento-Cultrix, 1999. ISBN: 8531603609.

[29] Miroslav Skrbek. Signature dynamics on a mobile electronic signature platform. In *GI Jahrestagung (Schwerpunkt "Sicherheit - Schutz und Zuverlässigkeit")*, pages 329–332, 2003.

[30] Dit-Yan Yeung, Hong Chang, Yimin Xiong, Susan George, Ramanujan Kashi, Takashi Matsumoto, and Gerhard Rigoll. *SVC2004: First International Signature Verification Competition*, volume 3072/2004, pages 16–22. Springer Berlin / Heidelberg, 2004.