AUTHENTICATION OF USER VIA KEYBOARD AND MOUSE DYNAMICS

Prof. A. A. Muzumdar[1],Rahul Godage[2], Gawali Suraj[3], Ghorpade Manoj[4], Akshay Kale[5], Anil Gangawane[6].

[1,2,3,4,5,6]*Department of Computer Engineering,*
Sanjivani College of Engineering, Kopargaon, Maharashtra, India.

ABSTRACT

Many of the authentication or security system uses numeric characters for password protection, however this system fails from several attacks. Attacks are like Brute force,social engineering etc. In today's world Biometric Technology which produces high accurate processing, but Biometric Technology requires special purpose or additional hardware and large processing power to fulfill the user requirement. The advanced techniques which analyze the behavioral characters of the user is called Behavioral Biometrics. These techniques implement using mouse dynamics. The mouse dynamics technique recognize and extract the movement and characters of user, At the time of interaction between the user interact with the computer. This information which is extracted is then later used for the authentication purpose. The existing system achieves better work in continuous authentication.

Keywords:*Behavioral Biometric, Mouse Dynamics, Biometric Authentication.*

1. INTRODUCTION

In today's scenario, mostly websites and systems are uses alphabetic password for verification and authentication of user. However this verification system not doing that much work to protect the system from illegal access at the time of user has started his active session. The important tasks of user authentication and verification is most important than before .For most the sensitive systems such as net banking, it is critical to provide security to user accounts. In less critical system such as monitors in a computing social
networks, online forums or laboratory a hijacked session are still misused to spread viruses or
spam, possibly damaging a user's reputation and other systems.

High risk of the system or total cost of not-authorized use of a system is more, continuous verification authentication of user's identity is more important. Continuous User Authentication is relying onbehavioral biometrics supplied by the user behavioral characteristics.It dynamically checks the user identity throughout a session. This is known as continuous authentication. Continuous authentication is very much useful in applications like intrusion detectionfor dynamic or continuous monitoring applications.

The disadvantage of identification or verification methods that only depend on confidential lead to theintroduction of *user verification* techniques which are used in conjunction with confidential baseduser identification. Verification methods authenticate the useridentity according to behavioral and physiological biometricswhich are assumed to be relatively constant to each user, and harder to steal. The verification may be performed firstly during login throughout the session.Then, biometric measure of the user is taken at periodic or regular intervals when the user starts session and is compared with patterns or gesture or measurements which were collected in previously. Common behavioral biometrics includeThe

characteristics of user interaction with the input devices like the mouse and keyboard.In Physiological biometrics, iris patterns and other physiological features that are unique for each individual. Thus, systems utilizing biometric user verification require a hacker who wants to infiltrate the system not only to steal the confidence of the user but also to bogus or dummy or fake the user's behavioral and physiological biometricsmaking identity thefts much harder.

In this paper, we suggest a behavioral biometric-based approach that verifies users based mouse movement. In general, in re-authentication system for practical, it must have the following features:

A. Accuracy

Not only most of the system accurately identify the fake, it can also have probability of reusing a true user, avoid inconvenience to true users.

B. Quick response

The system should be able to give fast verification decision. In other words, system should be able to differentiate a user in a periodic manner.

C. Difficult to forge

Even if a user's profile data is known by the faker, it will become very tough to detect fake a normal biometric behaviors in a continuous manner and then avoid the verification system.Our new approach overcomes all of these difficulties, delivering a fast and accurate verification which is based on biometrics which are hard to forge. The basic agendaof our new approach is to consistently keep the track of mouse movements of a person, and extract angle-based metrics, later then use Support Vector Machines for accurate user verification. The important feature of our approach is to make good use of the every pointangle based behavioral metrics of mouse movements, which areunique from user to user and independent of the computing platform, for user verification.

This paper first captures or detects the user behavior or movements at the time of interaction between user and the mouse, then it generate mouse gestures and checks consistently at the time of user should conduct the active session and provides verification or authentication to the users. The mouse gestures are drawn in keystroke.The behavioral biometrics is depends on the behavior of the users. A biometric system includestwo phases:

1. *Enrollment phase* and
2. *Verification phase*.

In theenrollment phase, user will draw a set of pattern several times on a monitor using mouse. Then features or patterns are extracted from this captured database, analyze them and train the NN (neural network) that will later consider for identification. In the second phase that is, the system will ask to user and check a subset of pattern or gesture drawn during the first phase that is enrollment phase for authentication.

2. LITERATURE SURVEY

The aim of the biometric based system in user authentication is focusing on "who you are?" Biometric is very distinctfrom conventional user verification system, which focuses on either "what you have?" or "what you know?" Unfortunately, a material like an Identity card or a key can be stolen, lost or missed; the password which is memorized should be divulged or forgotten. Conversely, a biometric based approach is relies on unique and derived or originated characteristics of a human user which is getting being authenticated. In the biometrics user can't easily steal or acquire and can't be disremember or lost. That is the case behind biometrics to make it very attractive and popular for user authentication. Biometrics can be classified in two phases: 1) Physiological and 2) Behavioral [4]. In Physiological biometrics, like facial recognition and fingerprint, have concentrated considerable attention in research

[11,13].The drawback of these biometrics is thatthey need particular hardware, which can be very hard for wide deployment. For the user authentication or verification over the web, one cannot always rely on the existence of hardware at the user side. In contrast, behavioral biometrics usinginteraction between user and computer can take down date from input devices, such as physical objects like keyboards, mouse and mice. Providing user verification or authentication in an convenient and accessible manner. Behavioral biometrics has gained very much popularity with keystrokedynamics. Our approach provides an improved verification strategy and far more users, leading us to reverse their hypothesis. For getting terribly high accuracy, the number of mouse actions which are captured in advanced are needed to verify a user's identity is extremely high in the reality and practically. Specifically,in oldest or traditionalapproaches it requires nearly about 2,000 aggregate mouse movements before a user can be recognized, and is impracticable or useless for real-time deployment.

In the opposite side, our aim is to provide a system better or competent for online re-authentication. Firstly we implement a finer-grained data collection methodology, allowing us to collect far more data in less time. We also take a support vector machines (SVMs), which are approximately faster than the neural networks employed in [6,7]. Thus, our system can form a decision in just several mouse clicks. More recently, a survey is conducted on the mouse dynamics with a comparative experiment [2]. It notices that mouse dynamics research should be more conscious to reduce approving time and take the effect of environmental variables into account. It can be seen later that, compared to other works, our approach also achieves high accuracy but only requires a small amount of biometric data. Likewise, we look into the effect of environmental factors (different physical objects, mice, and time) andpresent that our approach is approximately able-bodied across different real time operating environments.

Graphical password or drown patterns [2,12] are a similar form of user authentication; It depends on Human Computer interaction[HCI] through a pointing device. Authenticate a user. Mouse dynamics differ in that they differentiate between users by *how* the users move and click the mouse, rather than wherethe users click. Graphical passwords Make a record of user clicks on the screen, and subsequently use this sequence as a substitute password. Such systems are supporting to our work, and can be deployed or used together. However, one may use a graphical password system while passively capturing a user's behavioral movements with mouse, utilizing the passively recorded measurements as a secondary sure or unfailing to verify the user's identity. This is Same as that of password hardening with keystroke dynamics as in[5].

3. EXISTINGMETHODS OF VERIFICATION USING MOUSE DYNAMICS

Behavioral biometrics on computer system is based on mouse dynamics and keystroke dynamics. "False Acceptance Rate" (FAR) is used for measurement of performance of behavioral biometrics, the ratio at which an attack is inaccurately characterized as a valid user, and False Rejection rate (FRR), and the ratio at which a login attempt by authentic user is incorrectly characterized as an attack. We also define an Equal Error Rate (EER) that is the point at which both FAR and FRR are equal. If FAR is high the system will be less likely to perceive or appreciate a legitimate or legal user as an attacker but there is also a higher chance that an attacker will be appreciated or known as a legal user. On the other hand if FRR is high the system will become much more obtrusive on the part of legal users by frequently incorrectly or erroneously login them out of the system but it will be not much likely to recognize an attacker as a legal user. In the real life applications the desired objective is to keep FAR and FRR at approximately at the same level.

3.1. KEYSTROKE BASED METHODS

In 1980 Gains et al. [15] was researched in the area .He was the first researcher who invented user authentication and verification via keyboard dynamics. The research was conducted on a small group consisting of 7 professional typists. Their work demonstrated that there is a "signature" to human typing, in which they were distinguished left handed typists from right handed ones. Joyce and Gupta [14] developed classification techniques based on latencies between the time the user presses a key and releases it as well as the time that passes between to keystrokes. This keystroke method is not suitable for monitoring continuous user verification as it requires users to type a text in a structured way. Monrose and Rubin [12] considered using multiple classifiers such as Euclidean distance measure, probabilistic measure and a third one which was an optimized version of the second classifier with the addition of weighted scores. The method was tested in an uncontrolled setting in order to better simulate a real life environment. Their method resulted in a FAR rate of 10%. Neural network (NN) was used in many earlier user authentication methods then against to it, Yu and Cho were implemented a support vector machine (SVM) based classifier in their research or methodology. The verification of the user was done by recording there keystrokes at the time of user were typing a password and result were in a FAR rate of 0% and FRR of 3.69%.

3.2. MOUSE BASED METHODS

Gamboa and Fred [14] envisioned mouse based biometrics as a substitute for text based passwords. Their technique required the user to detect similar pairs of images on tiles and verification was did on the basis of characteristics of the user's mouse movements from one tile to the another tile. The system was checked on a approximately 50 users and produced EER of 0.7% for 100 mouse strokes which lasted 1 second each. That puts the detection time under 2 minutes. Pusara and Bordley [13] proposed a web based verification method which recorded participant's mouse movements while they were browsing a web site. While users were browsing website, they were separated by using C5.0 decision tree algorithm. The method concluded in FAR of 0.46% and FRR of 1.7s5% with a highly variable detection time between 1 and 14.5 minutes. Ahmed and Traore [15] developed a method. This monitored user's interaction with a mouse throughout the whole session and extracted certain features which were then aggregated into histograms that were used to determine the identity of each user. Here a binary neural network was used as a distributer and the method achieved a FAR of 4.6% and FRR of 24% for a user session continuing about 4 minutes. The system was envisioned as a replacement for text based passwords. The system achieved FAR of 3.5% and FRR of 4.0%

Table 1. Comparison of existing user verification method

Source	FRR	FAR	Data required	Settings	Notes
[1]	2.4549%	2.4614%	2000 mouse actions	Continuous	Free mouse movements
[11]	0%	0.36%	2000 mouse actions	Continuous	Free mouse movements
[6]	2%	2%	50 mouse strokes	Static	Mouse movements from a game
[12]	1.75%	0.43%	Not specified	Continuous	Applies to a certain application
[14]	11.2%	11.2%	3600 mouse actions	Continuous	Free mouse movements
[13]	4%	3.5%	Not specified	Static	Mouse movements from a game
[4]	9.5%	17.66%	30 mouse actions	Continuous	Free mouse movements
[17	1.3%	1.3%	20 mouse actions	Continuous	Free mouse movements

4. MOUSE MOVEMENT MEASUREMENT AND IT'S CHARACTERIZATION

4.1 DATA COLLECTION

In data collection, we gather two different sets of the data. In which the first set of data is recorded froma physical environment, known as the controllableset; while the second set of data is from an online panel or forum inthe field, called as the field set. In data collection process, we are inviting 20 peoples from different age category and from different environment, they need to draw pattern to give input to authentication system. Basis on their input, this captured or collected data will be later used for extracting the pattern, In the field set, nearly thousand or more unique user'smouse events are recorded or captured by JavaScript code, and this recorded information isprovided passively through AJAX requests to the internet server.

On one side, these users are unknown but can be identifiable or distinguishedthrough unique login names. However, the quantity of data collected or gathered for a selective user is not sure. A individual user could be start his session by logging in and perform frequentmouse actions for a long time, or one could leave by just performing one click. On the other side, this information of usersis utilized to serve as for generating frequent patterns for both training andtesting purposes.The raw mouse movements or movements during events are represented as tuples of continuous the timestamp and Cartesian coordinate pairs. Where, each tuple isin the form of _action-type, *t, x, y,* where action-type is like mouse action type (*mouse-click* or a *mouse-move*),here *t*is stands forthe timestamp for the mouse movement, *x* and*y* are the x co-ordinate,and the y co-ordinate respectively. Timestamps in data collection phaseare collected in milliseconds.

4.1.1 Data Processing

The strategy behind preprocessing is to detect each point and every click action, where click action can be prescribed as mouse movementsafter every click. Continuousmouse actionsare the movements where series of mouse actions or movements with short or no pause betweeneach adjacent step. Within the *i*th point-and-clickaction for a user *c*, we can denote the *j*th mouse move record asmouse-move, *ti, xi, yi_c,j*, where *ti*denotes the timestamp of the*i*th mouse action or movement. Based on the information that belongs toevery point and every click movement, we can find angle-based metrics.

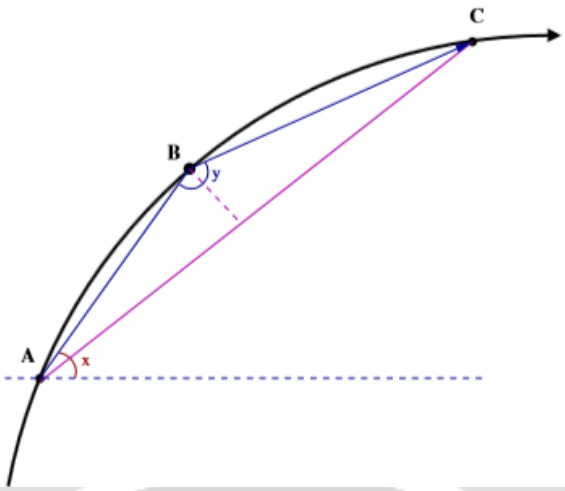

Figure 1: Illustration of angle-based matrix.

4.1.2 Metrics

To understand the mouse action information or data, we define threefine-grained angle-based metrics: i) Direction,

ii)Angle of curvature,

iii)Curvature distance.

These metricsare distinct from the conventional metrics, like speed, and can be accurately characterize a behavior of user'sunique mouse movements, independent of its operation platform.

i) Direction:

We calculate direction for two sequentially gathered points A and B, we can recognize the direction along the line AB traveled from the point A to the next point B. The $\angle AB$ is the angle between that lineto thehorizontal (see angle *x* in Figure 1).

ii)Angle of Curvature:

The angle of curvature is the $\angle ABC$ for any three sequentially capturedPoints A, B, and C; i.e., the angle between the point A to Band from point B to C(angle *y* inFigure 1).

iii) Curvature Distance:

For any three points A,B, and C which are previously recorded, consider the distance of the line from pointA to C . The curvature distance is the ratio ofthe length of*AC* to the perpendicular distance frompoint B to the line

AC (see the perpendicular lines inFigure 1). Note that this metric is unit less because it's ratio of both the two distances.For the comparison, we list out the definition of two traditionalmouse events or action metrics, speed and pause and click, as follows.

• *Speed*

For every point and click movement, we can computethe ratio of the total distance traveled by mouse forthat action partitioned by the whole time taken to fulfillthe action.

• *Pause-and-Click*

For every point and for every click action, wecompute the total time required between the end of themovement and the click event. Thismetric compute the total time spent by pausing betweenpointing towards an object and clicking onit.

4.2 Mouse Movement Characterization

4.2.1 Dependence on Distinct Platforms

We came to know one problem in analysis of our information is that,it might be meaningless or difficult or useless to compare between two different users thoseare working on very dissimilar systems. The entire user's environmentcan affect its set of data: the operating system used, resolution and screen size, font size, sensitivity of mouse pointer, brand of the mouse used,and even the total available space to move the mouse near themouse pad. Speed and acceleration metrics arepoor choices for comparison between users of arbitrary platforms. That is why; these two metrics can be skewed bydifferences in screen resolution and pointer sensitivity. Metrics like pause-and-click are too muchdependent on the content a user is reading. For example, auser tends to take longer pause before clicking on a particular link on a bigcontent page like a wiki article for a muchshorter time before clicking a "submit" button.
This makes a good case to use angle-based metrics forarbitrary user comparison instead. Direction and angle ofcurvature are platform independent because that are not based on screen

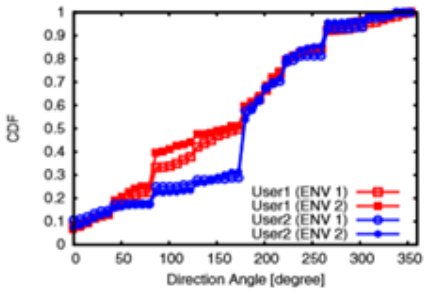

Figure 2: Direction Angle metric plotted for two different users on two different machines each.

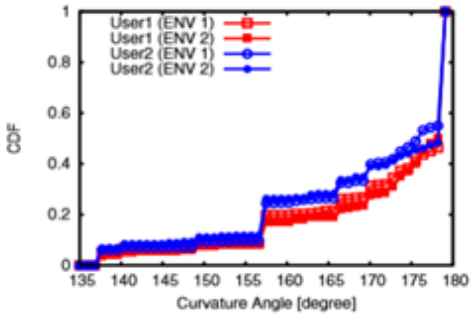

Figure3: Angle of Curvature metric plotted for two different users on two different machines each.

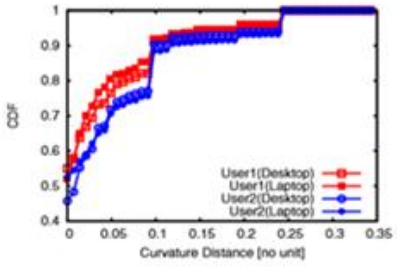

Figure 4: Curvature Distance metric plotted for two different users on two different machines each.

size or any other element of the user's environment. Similarly, curvature distance is defined as a ratio of distances

On the screen, and thus self-adjusts for the user'sparticular environment. A ratio can be compared to anotheruser's ratio across two different platforms. Figure 2, 3, and 4 showing the comparison between two different users with theangle-based metrics. We can view that the cumulative distributionfunction (CDF) curves for the same user's unique or individual data are too much similar and also well synchronized in shape, evenacross platforms. This shows that angle-based metricsare comparatively stable on different platforms.

4.2.2 Uniqueness of Angle-Based Metrics Across Different Users

Feature of angle-based metrics is, they are unique across every user. For the same user it not only have very similar angle-based results on distinct platforms,but also different users have different angle-based results,even on same platforms.Again, as shown in Figures 2, 3, and 4, even though each user's CDF is consistent across different platforms; there is agap between distinct users' CDF curves, however on the similar platform. While thedistinct users' CDF curves in both speed and pause-and-click are nearly coupled on the similar environment, there isa distinct gap between the same user's two curves for different environments. Since the nearest matching curve foreither user is the curve of the *other* user under the same environment, it can be so much hard to uniquely differentiate people using these metrics. Together with the platform independence discussed above,this makes angle-based metrics superior to speed and pause and click for user verification. Note that for easy presentation,we are only comparing the difference in the mouse dynamicsbetween the pair of users. However, the similar observationholds for the other users.

5. SYSTEM ARCHITECTURE:

This paper pose new verification method which verifies a user based on each individual's behavior with system. This method requires the mouse events generated during interaction of user and also keystroke dynamics. It takes aggregation of its coordinates and different activities before accurate user verification process. Personal individual mouse action that increases the preciseness while decreasing the time that is needed to identity the identity by the user since the Verification of fewer actions are done by the histogram- based approach. A biometric-based user verification system is necessarily a gesture recognition system that attains biometric information from an individual user, extracts a characteristic set to demonstrate a individual user signature and constructs a identification or verification model by training it on the set of signatures.

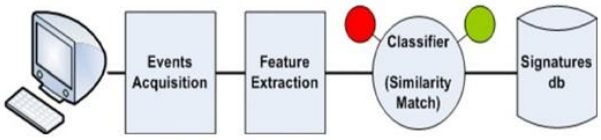

Fig. 5. A General Block Diagram of Proposed System

Fig. 5 describes the architecture of a behavioral biometrics for user verification system. Such systems contains the following components,

A) Feature Acquisition- Collects the events created by the number of input devices used for the dealing (e.g. keyboard, mouse) via their drivers. During feature acquisition following Procedure is done:

1. A feature acquisition module responsible for acquiring the events that are produced by the mouse. Every event is set as a quartet (x coordinate, y coordinate, event type, timestamp).

2. An action extractor module transforms the acquired events into the mouse actions. Each action is extracted and associated with its events it required to facilitate the extraction of the different features proposed in Section.

B) Feature Extraction- Which constructs a signature that characterizes the behavioral biometrics of the user.
1. A model of feature extractor extract characteristics from the given action. Since dissimilar feature extractors are required for different types of actions.
2. In learning process actions DB stores the event .

C) Classifier- Consists of an inducer (e.g. SVM,NN etc.) that is accustom to build the user checking model by training on past behavior, often given by samples. During process of verification, the generated model is needed to categorize new samples achieved from the user.

D) Signature Database- To train model a database of behavioral signatures that is used. Entry of a username, the signature of the user is obtained again for verification method .During the verification using mouse dynamics of user following steps are followed,

1. Features are taken from the actions via a process that is same as the acquired during the acquisition stage.
2. The extracted features are stored in an Action Collector DB.
3. Once a enough number of actions are captured (From to a predefined threshold m) they are send to the classifier according to the type of action.
4. The Classifier predicts for each of the trained users, the probability that each of them performed each m actions.
5. A (layer 2) decision module integrates the probabilities to obtain a last result. The user keystroke beat are measure to develop a individual biometric class of the users typing gesture or pattern for authentication. The information available for every keypad can be recorded which helps to determine: Dwell time that is the time a key pressed and Flight time that is the time between “key up” and the next “key down”. Furthermore, recorded keypad timing information is then processed through neural algorithm, which helps to decide a primary patternfor future differentiation. Similarly for identification and authentication tasks used to create for future gesture or pattern of an vibration information. Information required to analyze keypad dynamics is gained by logging of keystroke.

6. CONCLUSION

This paper was presented novel based method for the user verification based on mouse activity. The proposedtechnique, a highly secured password pattern can be created. This can prevent the hackers from accessing the highly confidential files. The proposed new concept is not only limited to a specific application or area; but also it can be used as an alternative for all the other type of passwords in the areas where ever possible. User Verification System is done by mouse signature and keystroke dynamics it will provide additional security layer.

7. REFERENCES

[1] E. Stobert, A. Forget, S. Chiasson, et al. Exploring usability effects of increasing security in click-based graphical passwords.In Annual Computer Security Applications Conference (ACSAC), 2010.
[2] Z. Jorgensen and T. Yu.On mouse dynamics as a behavioral biometric for authentication. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS ’11, pages 476–482, 2011.

[3] Ahmed A.A.E, Traore I, A new biometric technology based on mouse dynamics, IEEE Transactions on Dependable and Secure Computing 4, (2007), p. 165-179.
[4] R. V. Yampolskiy and V. Govindaraju. Behavioral biometrics: a survey and classification. Int. J. Biometrics, 1(1):81–113, 2008.
[5] F. Monrose, M. K. Reiter, and S. Wetzel.Password hardening based on keystroke dynamics. In ACM Conference on Computer and Communications Security (CCS), pages 73–82, 1999.
[6] A. A. E. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. IEEE Transactions on Dependable and Secure Computing, 4(3):165–179, 2007.
[7] Y. Nakkabi, I. Traore, and A. A. E. Ahmed.Improving mouse dynamics biometric performance using variance reduction via extractors with separate features. IEEE Transactions on Systems, Man, and Cybernetics, 40(6):1345–1353, 2010.
[8] Pusara M, Brodley C.E, User re-authentication via mouse movements. Proceedings of the 2004 ACM, workshop on Visualization and data mining for computer security, (2004), p. 1-8.
[9] Monrose F, Rubin A, Authentication via Keystroke Dynamics, Proceedings of the 4th ACM conference on Computer and communications security, (1997), p. 48-56.
[10] Joyce R, Gupta G, Identity authorization based on keystroke latencies, ACM 33 (2), (1990), p. 168-176.
[11] P. Gupta, S. Ravi, A. Raghunathan, and N. K. Jha.Efficient fingerprint-based user authentication for embedded systems. In Proceedings of the 42nd annual Design Automation Conference (DAC), pages 244–247, 2005
[12] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle.Multiple password interference in text passwords and click-based graphical passwords.In ACM Conference on Computer and Communications Security (CCS), 2009.
[13] C. Mallauran, J.-L.Dugelay, F. Perronnin, and C. Garcia. Online face detection and user authentication. In Proceedings of the 13th annual ACM international conference on Multimedia (MM), pages 219–220, 2005.
[14] Gamboa H, Fred A, A Behavioral biometric system based on human computer interaction, Proceedings of SPIE 5404, (2004), p. 381-392.
[15] Gaines R, Lisowski W, Press S, Shapiro N, Authentication by keystroke timing: some preliminary results, Rand Corporation, (1980).