ISSN:1991-8178

**Australian Journal of Basic and Applied Sciences**

Journal home page: www.ajbasweb.com

# An Efficient Multimodal Biometric System for Secured Authentication

Veeramalai Sankaradass, A. Merry Ida, W. Ancy Breen, P.K. Sheela Shantha Kumari

*Department of Computer Science and Engineering Vel Tech High Tech Dr. Rengarajan Dr. Sagundhala Engineering College, Chennai, Tamil Nadu, India*

**ARTICLE INFO**

***Article history:***
*Received 25 March 2015*
*Accepted 28 May 2015*
*Available online 14 June 2015*

***Keywords:***
*Multimodal biometrics, keystroke dynamics, iris recognition*

**ABSTRACT**

Multimodal biometric system is the budding technology that is used in various applications for authentications. In the existing technologies most widely used technologies are thumb print biometrics and face authentication for physiological biometrics. But thumb biometrics is highly vulnerable to spoofing attacks which has security lacks and face authentication creates more memory in the database. Hence we retain the multimodal biometric technology and propose new concepts called keystroke dynamics and iris recognition using the system which can assure more accuracy, identification of individuals over long period of time can be made easily. Also the system makes use of both physiological and behavioural biometrics which gives more accuracy.

**© 2015 AENSI Publisher All rights reserved**.

**To Cite This Article:** Veeramalai Sankaradass, A. Merry Ida, W. Ancy Breen, P.K. Sheela Shantha Kumari, An Efficient Multimodal Biometric System for Secured Authentication. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 759-767, 2015*

## INTRODUCTION

Pattern classification systems are commonly used in security-related applications like biometric authentication, network intrusion detection, and spam filtering, to discriminate between a ”legitimate" and a ”malicious" pattern class (e.g., legitimate and spam emails).A biometric system is a essentially a pattern recognition system .Contrary to traditional ones, these applications have an intrinsic adversarial nature since the input data can be purposely manipulated by an intelligent and adaptive adversary to undermine classifier operation. Known examples of attacks against pattern classifiers are: submitting a fake biometric trait to a biometric authentication system (spoofing attack), manipulating the content of spam emails to get them past spam filters (e.g., by misspelling common spam words to avoid their detection).

It is now acknowledged that, since pattern classification systems based on classical theory and design methods do not take into account adversarial settings, they exhibit vulnerabilities to several potential attacks, allowing adversaries to undermine their effectiveness. The biometrics can be classified as unimodal and multimodal .The unimodal biometrics, which uses only one biometric information as evidence, are widely used today, in spite of inherent advantages also have limitations in terms of accuracy and vulnerability. To overcome these issues in Unimodal biometrics multimodal biometrics was used. Multimodal biometric systems are those which utilize, or are capability of utilizing, more than one physiological or behavioral characteristic for enrollment, verification, or identification.

The aim of multi biometrics is to reduce one or more of the following:

1. False accept rate (FAR)
2. False reject rate (FRR)
3. Failure to enroll rate (FTE)

Multi modal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. The existing multimodal system uses the face recognition and fingerprint authentication. Though the system is efficient there are certain disadvantages like more time consuming, inaccuracy etc.

An efficient biometric system that utilizes the fullest of the multimodal biometrics is proposed. This system also makes use of the biometric fusion which combines the measurements from different biometric traits to enhance the strength. This system uses the biometric technologies keystroke dynamics and iris recognition.

### *Related works:*

The multimodal system, in the existing work is made up of a fingerprint and a face matcher. In the design phase the enrollment of authorized users (clients) takes place (Battista Biggio, 2014; Lívia Araújo, 2005). The reference templates of their biometric traits are stored into a database, together with the corresponding identities.

**Corresponding Author:** Veeramalai Sankaradass, Department of Computer Science and Engineering Vel Tech High Tech Dr. Rengarajan Dr. Sagundhala Engineering College, Chennai, Tamil Nadu, India
E-mail: veera2000uk@gmail.com

In operation, each user provides the requested biometric traits to the sensors, and claims the identity of a client. Then, each matcher compares the submitted trait with the template of the claimed identity, and provides a real-valued matching score: the higher the score, the higher the similarity (Trupti, 2012).

The main thing key stroke focuses is how the user types and not what the user types. The latencies between the user's typing pattern (Fabian Monrose, 2000), the pressure applied, keystroke duration is used to form a unique signature of the user. The biometric information of an individual is always unique .Biometric can be physiological or behavioral both used to identify an individual effectively .The typing pattern also forms the basis of non – static biometric systems. A pattern recognition system involves representation, extraction and classification of data. The main application of keystroke authentication is to restrict root level access to a server.

The static keystroke in user authentication to differentiate between a legitimate and a imposter user (Zhong, 2012). Here the features like dwell time and flight time in calculation of keystroke is used. As samples are collected in this system, a special adaptation mechanism is used to reduce false rejection rate. Whenever the user types the password and the keystroke time taken is some what less than those of the samples collected then the new keystroke time is added to samples, and the oldest one is neglected.

The effective normalization, localization and quality enhancement methods are provided (Sabarigiri, 2012). Normalization is necessary to eliminate the illumination effects and the effect of varying distances. Localization identifies the iris part alone which leads to effective classification of images.

An effort to conceal the existence of embedded information by putting forward the art of hiding information through Steganography (Epp,2011). Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. The paper discusses how digital images can be used as a carrier to hide messages .Also it analyses the performance of some of the steganography tools and introduces the reader to various concepts of stenography (Arvind Kumar, 2010).

The personal identification based on thumb impression as an experimental setup, findings, & analysis. Features of biometric characteristics of thumb print are extracted and stored into the database in text format. The matching algorithm uses these text formatted features for matching purpose & identification (Lívia Araújo, 2005). Here minutiae feature points extracted from input fingerprint during identification mode is matched with minutiae feature points from database.

The basic concepts and techniques used to create and evaluate an Iris Recognition System. A fusion mechanism and a Circular Hough Transform are being implemented to detect the iris boundaries in the eye's digital image (Sabarigiri, 2012).

The Haar wavelet is used in order to extract the deterministic patterns in a person's iris in the form of a feature vector. The first step is image acquisition. Then, the pictures' size and type are manipulated. Once the preprocessing step is achieved, it is necessary to localize the iris and unwrap it. Here, the texture of the iris can be extracted using Wavelets. Finally, the coded image is compared with the already coded iris in order to find a match or detect an imposter.

The skin tone regions of images are used as biometric feature. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding (Arvind Kumar, 2010). Before embedding secret data is needed to be encrypted using stream cipher encryption scheme RC4.Skin color tone detection is performed by using HSV color space.DWT is the frequency domain in which this biometric steganography is implemented. Secret data is embedded in one of the high frequency sub and by tracing the number of skin pixels in that band. Different embedding steps are embedded on the cropped region of the image.ie value of this cropped region will act as a key at the decoder side.

The score of the finger print and the face matcher are xfing and xface respectively. Finally, the matching scores are combined through a proper fusion rule to decide whether the claimed identity is the user's identity (genuine user) or not (impostor user).

The system suffers from some of the disadvantages like:

- More time consuming
- Face authentication, comparatively requires more pixel position for authentication, which ultimately increases the database size.
- Recognition of twins in face recognition is not easy and can mislead at times.
- Finger print recognition suffers from spoofing attacks.
- Low recognition rate
- Facial features may change over time.
- Face recognition can be affected by illumination.

To overcome the difficulties and drawbacks in the existing work an efficient multimodal system is proposed.

***Proposed system:***

In the proposed system we retain the use of multimodal biometrics and use two new technologies called keystroke dynamics and iris recognition. Keystroke dynamics comes under behavioral biometric. The behavioral biometric of Keystroke Dynamics uses the manner and rhythm in which an

individual types characters on a keyboard or keypad. Iris recognition comes under physiological biometrics. The raw measurements used for keystroke dynamics are dwell time and flight time

- Dwell time is the time duration that a key is pressed
- Flight time is the time duration in between releasing a key and pressing the next key

In this system there are two phases:
1. Enrollment 2.Authentication

### *A. Technologies:*

#### *1. Keystroke Dynamics:*

Keystroke dynamics is considered as a strong behavioral Biometric based Authentication system. It is a method of measuring the rhythm in which an individual types characters on a keyboard or keypad. Keystroke dynamics is the detailed timing information that describes exactly when each key was pressed and when it was released as a person is typing.

#### *2. Iris Recognition:*

Iris recognition is a method of Identifying people based on unique patterns within the ring-shaped region surrounding the pupil of the eye. The iris usually has a brown, blue, gray, or greenish color, with complex patterns that are visible upon close inspection. Because it makes use of a physiological characteristic, iris recognition is considered a form of biometric verification.

### *B. Enrollment Phase:*

The enrollment phase initial phase of the system and it is for enrolling the users when they wish to use the system. The biometric traits of the user are captured or extracted and it is stored in the database and also certain basic details of the user are stored in the database. We use two different biometric technologies here, one is keystroke dynamics and the other one is iris recognition .In the keystroke dynamics the input parameter what the user give is the PIN number and using that pin number the time taken by the user to enter the number is stored. The methodology here is the system calculates the Dwell time which is the time duration that a key is pressed and Flight time, the time duration in between releasing a key and pressing the next key.

The important thing in keystroke computation is the key code which is nothing but the string which user types and three time-features down-down (DD), down-up (DU), and up-down (UD) time (Lívia Araújo, 2005; Zhong, 2012). The feature of the user is now extracted and stored in the data base. This time will also be intimated to the user, while calculated because the user needs to remember this as a parameter while log in.

Similarly in the iris recognition the input parameter will be the user iris. The steps in iris trait extraction are:
1.Image Acquisition: Where the image of the user's eye is captured
2. Localization: the iris and pupil part of the user's eye image are detected and this is the format in which the image will be stored in the database
3. Normalization: Before storing into database iris region needs to be normalized to compensate for the variations such as illumination variations which will make the radial size of the pupil change accordingly. Then the iris code is generated and then it is stored in the iris data base.

### *C. Authentication Phase:*

The authentication phase takes place when user log onto the system. In our approach two step authentications is carried out .In the first step user types the PIN number and this is the place where keystroke dynamics work. The behavior of the user will be detected and will be compared with the template in database and a match score is generated based on the accuracy.

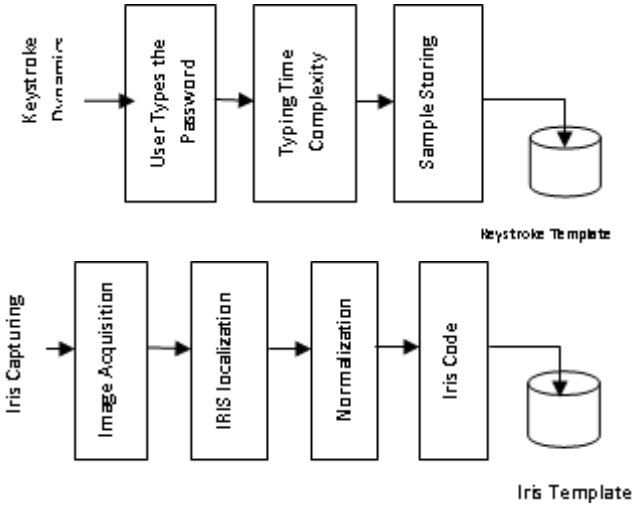


**Fig. 1:** Enrollment phase.

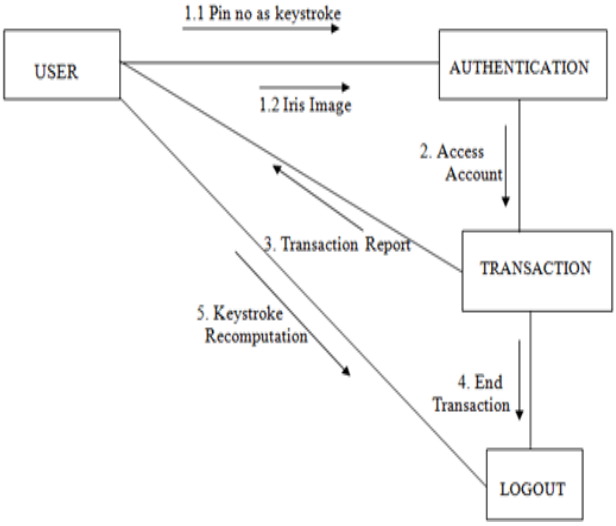


**Fig. 2:** Collabration diagram.

Then the next step will be iris recognition. The iris image of the user will be captured and the feature will be extracted .Here for enhanced security we are using the data hiding concept. The advantage is even if the illegitimate user breaks the first step of authentication, he would not know that there is a data hiding taking place at the background and the image that he uploads will fail to authenticate and he will fail in his attempt. For data hiding the user will type the password which he gave in registration phase. Then he uploads the iris image. Now the system extracts the feature from iris image uploaded, the extracted feature is then XORed with the password. The XORed value is then hided in the same iris image and a template is created which is then sent for authentication request .During authentication at the backend the system will separate the hidden data from the iris image. (Sabarigiri, 2012; MojtabaNajafi, 2010) The password will be extracted from the xored value. The password and iris image will be checked with the one in the database for match. Similarly a match score for the iris recognition step will be generated.

Both the match score will be fused and the system will decide whether the user is authorized or not and access will be provided to the system.

***Collaboration Diagram:***

A collaboration diagram show the objects and relationships involved in an interaction, and the sequence of messages exchanged among the objects during the interaction. The collaboration diagram can be a decomposition of a class, class diagram, or part of a class diagram. it can be the decomposition of a use case, use case diagram, or part of a use case diagram.

The collaboration diagram shows messages being sent between classes and object (instances). A diagram is created for each system operation that relates to the current development cycle (iteration).

***Proposed system analysis:***

***A. Registration of the User:***

The first module begins with the registration phase with basic details of the user. The registration (enrollment) phase contains three stages of details collection from the user in order to verify all basic details of the user.

The registration phase first gathers about the personal information like first name, date of birth, gender, email ID, last name, mobile number, pan card no. for verification purpose and then blood group. After this account details of the user is collected this asks for the account number and bank details from the user. The summit is clicked after filling the details of the user. The system verifies whether it is authorized bank and account number and details of the customer, pan card and then valid email id and then authorize the user to go on with the further process of registration.

Next comes the password details which ask for the user to enter the password and another text box to repeat the same. The summit is clicked after filling all the details .if all the details of the user is furnished correctly then the system moves on with next stage of process. Otherwise the error mentions by means of alert message.

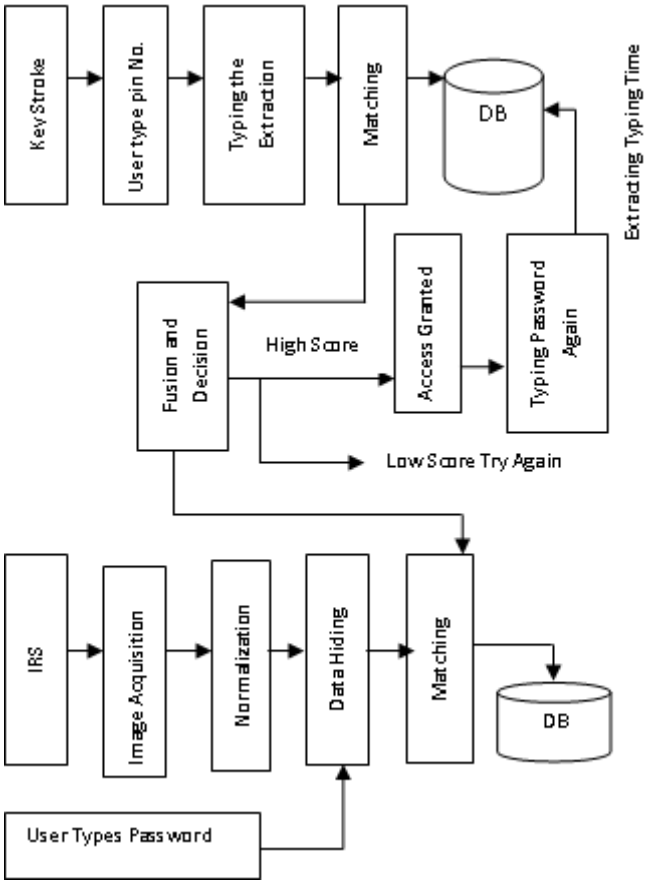


**Fig. 3:** Authentication phase.

***B. Keystroke Computation and Iris Capturing:***

In this module the keystroke behaviour of user will be extracted. The second module starts with the name of the user with "hi_username"if the user has filled the previous page successfully. The system provides text box and as soon as the user enters the pin no, he is expected to select the create button and the system shows the time taken by the user to enter the pin number. A reset button is set to do the process once again. The methodology here is the system calculates the Dwell time which is the time duration that a key is pressed and Flight time, the time duration in between releasing a key and pressing the next key. The important thing in keystroke computation is the key code which is nothing but the string which user types and three time-features down-down (DD), down-up (DU), and up-down (UD) time. In the iris computation, the iris of the user is taken by the system and iris computation begins here. Then iris acquisition, localization, normalization takes place.

***C. Login: First Step of Authentication:***

Whenever the user needs to use the system he must login. In this module the first step of authentication is done. The first step is keystroke behavior checking. The user first enters the PIN number and as he enters it the behavior is extracted and it will be checked with the template in the database which was pre-computed in the second module. Then the user will be directed to the next step of authentication. (Zhong, 2012; Deepak Sharma, 2011; Epp, 2011)

***D. Login: Second Step of Authentication:***

In this module the second step of authentication is used. Here the iris image uploading and data hiding takes place. First the user needs to enter the password given by him during the registration phase. Then user must upload his iris image. The process that happens in back end is first the iris feature will be extracted then this feature will be hidden in the user uploaded iris image. At the database while checking the data will be separated from the image and the image and password will be checked for match. (Sabarigiri, 2012)

**Fig. 4:** Localization of iris from user image.

For the first step and the second step of authentication a match score will be generated. This match score will be combined and a fused match score for the authentication will be generated .after the user has finished the two steps the list of match scores will be displayed to him. If the match score is up to a maximum level the user is authenticated as legal user and he is permitted to use the system or if the match score is not up to a maximum or is very low then the user isa illegal or illegitimate and he will be intimated with a error message.

***E. Transaction:***

To demonstrate the secured authentication in this system a transaction module has been used as a transaction deals with money it needs to be more secure. The transaction here can be done only when a user clears the two steps of the authentication. In this module a user can transfer money from his account to another and also can check the amount deposited, transferred etc.

***F. Keystroke Re Computation:***

After the transaction is over the user needs to logout of the system, before the user logs out the user must reenter his PIN number ,again the keystroke behavior will be calculated and the time taken will be displayed to the user .This time will be stored as the new keystroke time taken in the database. This will be used for checking the user behavior the next time he logs into the system so the user must remember this time. The method that is adopted here is different from the conventional keystroke computation where samples are stored. If sample storing is used then there is a chance of attacker to take advantage of it .So here instead of sample storing the keystroke is re computed and intimated to user.

**Fig. 5:** Edge detection.

***Proposed algorithms analysis:***

***A.canny edge detection*:**

Canny edge detection algorithm is used in this system for feature extracting while doing data hiding. This algorithm gives more accurate detections which enhances the efficiency of the system. Detection is done when condition:

$\nabla^2 G*f = 0$ and

$\nabla G*f$ reaches a maximum. Is satisfied

$\nabla G$ is the first derivative of the Gaussian defined (in 1-D) as:

$$\nabla G(x) = -\frac{x\exp(-x^2)}{\sqrt{2\pi\sigma_2^3}\,2\sigma_2^2} \quad (1)$$

***B. Background Subtraction Algorithm:***

This algorithm is used to remove the unwanted parts or regions in the iris image after the iris feature have been extracted using the Canny edge detection algorithm.

***C. Converting Iris Feature into Values:***

After extracting the feature from the iris image of the user, it is then converted into values based on the intensity of the extracted image .The conversion technique used here is RGB to Gray scale conversion. The feature extracted from the iris image when subjected to this technique it gets converted into a gray scale image. A grayscale or grayscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of grey, varying from black at the weakest intensity to white at the strongest. The intensity of a pixel is expressed within a given range between a minimum and a maximum, inclusive. This range is represented in an abstract way as a range from 0 (total absence, black) and 1 (total presence, white), with any fractional values in between.

To convert a color from a color space based on an RGB color model to a grayscale representation of its luminance, weighted sums must be calculated in a linear RGB space, that is, after the gamma compression function has been removed first via gamma expansion.

For the sRGB color space, gamma expansion is defined as

$$C_{linear} = \begin{cases} C_{srgb}/12.92 & C_{srgb} \le 0.04045 \\ (C_{srgb}+0.055/1.055)^{2.4} & C_{srgb} > 0.04045 \end{cases} \quad (2)$$

where $C_{srgb}$ represents any of the three gamma-compressed sRGB primaries ($R_{srgb}$, $G_{srgb}$, and $B_{srgb}$, each in range [0, 1]) and $C_{linear}$ is the corresponding linear-intensity value (R, G, and B, also in range [0, 1]). Then, luminance is calculated as a weighted sum of the three linear-intensity values. The sRGB color space is defined in terms of the CIE 1931 linear luminance Y, which is given by

$$Y=0.2126R+0.7152G+0.0722B \quad (3)$$

The coefficients represent the measured intensity perception of typical trichroma thumans, depending on the primaries being used; in particular, human vision is most sensitive to green and least sensitive to blue. To encode grayscale intensity in linear RGB, each of the three primaries can be set to equal the calculated linear luminance Y (replacing R,G,B by Y,Y,Y to get this linear grayscale). Linear luminance typically needs to be gamma compressed to get back

to a conventional non-linear representation. For sRGB, each of its three primaries is then set to the same gamma-compressed $Y_{srgb}$ given by the inverse of the gamma expansion as:

$$Y_{srgb} = \begin{cases} 2.92Y, & Y \leq 0.0031308 \\ 5Y^{1/2.4} - 0.055, & Y > 0.0031308 \end{cases} \quad (4)$$

In practice, because the three sRGB components are then equal, it is only necessary to store these values once in sRGB-compatible image formats that support a single-channel representation. Web browsers and other software that recognizes sRGB images will typically produce the same rendering for a such a grayscale image as it would for an sRGB image having the same values in all three color channels.

### *D. Hiding Secret Message Into The Iris Image:*

In order to enhance security, the secret message is hided into iris image of the user using stegnographic approach. The value obtained from the feature of the iris image as a result of RGB to Grayscale conversion is then XORed with password of the user. This XORed value is considered as the secret message which is then hided into the same iris image using stegnography. (Amritha, 2013; Sabarigiri, 2012; Mojtaba Najafi, 2010)

## RESULTS AND DISCUSSIONS

From the snapshot of the implementation of this work, we can understand that how the system is implemented and working in the expected ways. And also, we can understand that how far it is more efficient. Few of the snapshot are given below to understand the quality of the work.

**Fig. 6:** Keystroke time computation.

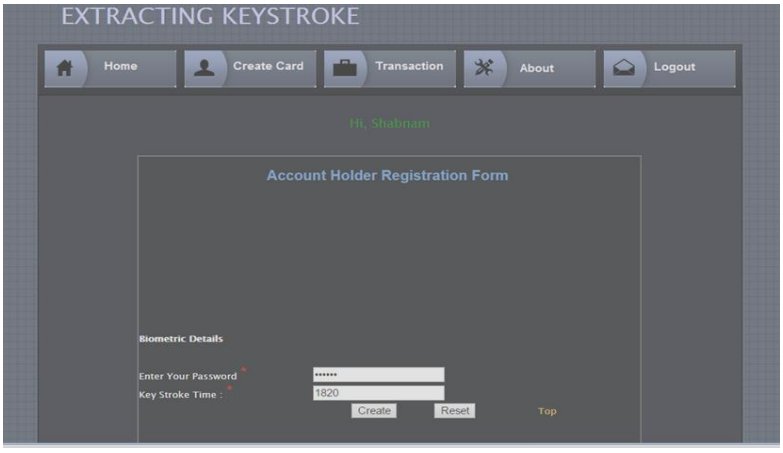


**Fig. 7:** Iris matching for authentication.

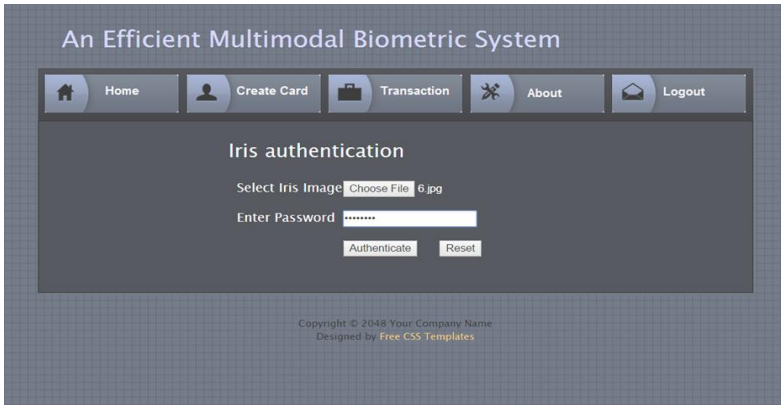


**Fig. 8:** Keystroke time recomputation for next transaction.

From the above implementation snapshot, we can understand that the new proposed technique giving more accuracy and time consuming transaction, and the proposed system giving fast transactions process and providing more efficiency also. The security and the unique features of the system are also improved to the maximum extent.

An efficient biometric system which utilizes the fulfilled multimodal biometrics is proposed. This system also makes use of the biometric fusion which combines the measurements from different biometric traits to enhance the different parameter strength in various levels to fulfill the requirement. This system uses the biometric technologies keystroke dynamics and iris recognition.

Finally, we conclude that the proposed approach giving better security, efficiency and flexibility in handling and maintaining the system for various purposes. The given screenshot will help you to understand the implementation of An Efficient Multimodal Biometric System for Secured Authentication

***Conclusion and future enhancement:***

We have presented a new system for authentication purposes where login is based on the biometric characteristics such as keystroke dynamics (behavioral biometric) and iris recognition (physiological biometric) combined with hiding password. The keystroke dynamics can be used to secure PINs against the case when the imposter gets hold of the secret user PIN. Similarly data hiding taking place at the background of the iris image make it difficult for an illegitimate user to break the authentication.

The system mainly focuses on providing increased security and also overcomes the disadvantages in the existing multimodal biometric system. The biometrics used such as keystroke dynamics and iris recognition both are equally efficient. As iris feature is unique for every individual, password hiding also adds additional security. Likewise keystroke dynamics method does not negatively affect the legitimate user .The PINs of length 4 digits with which the imposter would fail in at least 72% of trials. Further research is needed to test the case when keyboard is displayed on the touch screen.

## REFERENCES

Amritha, G., Meethu Varkey, 2013. ”Biometric Steganographic Technique Using DWT and Encryption”,International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 3.

Anil Jaina, Karthik Nandakumara, Arun Rossb, 2005. ”Score normalization in multimodal biometric systems”,The Journal of the Pattern Recognition Society.

Arvind Kumar, Km Pooja, 2010. “Steganography- A Data Hiding Technique” ,International Journal of Computer Applications, Vol. 9-7.

Battista Biggio, Giorgio Fumera, Fabio Roli, 2014. ”Security evaluation of pattern classifiers under attack” B. Sabarigiri1 ,T.Karthikeyan, IEEE Transactions On Knowledge And Data Engineering, VOL. 26, NO. 4.

Deepak Sharma, Ashok Kumar, 2011. “Iris Recognition-An Effective Human Identification”, International Journal of Computing and Business Research, volume 2 Issue 2.

Epp, C., M. Lippold and R.L. Mandryk, 2011. “Identifying Emotional States using Keystroke Dynamics”, Proc. 2011 annual conf. on Human factors in computing systems.

Fabian Monrose, D. Aviel, B. Rubin, 2000. “Keystroke dynamics as a biometric for authentication”, Future Generation Computer Systems, 16: 351–359.

Lívia Araújo, C.F., H.R. Luiz Sucupira Jr., G. Miguel Lizárraga, L. Lee Ling and B.T. João Yabu-Uti, 2005. “User Authentication Through Typing Biometrics Features”IEEE Transactions On Signal Processing, Vol. 53, No. 2.

MojtabaNajafi, SedighehGhofrani, 2010. “A new iris identification Method Based on

RidgeletTranform", The 3rd International Conference on Machine Vision (ICMV).

Sabarigiri, B., T. Karthikeyan, 2012. "Acquisition of Iris Images, Iris Localization, Normalization, and Quality Enhancement for Personal Identification",International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),V.olume 1, Issue 2.

Zhong, Yu., Yunbin Deng, K. Anil Jain, 2012. "Keystroke Dynamics for User Authentication",IEEE Computer Society Conference onComputer Vision and Pattern Recognition Workshops (CVPRW).

Trupti, S. Indi, D. Suhas Raut Phd, 2012. CSE Orchid College of Engineering & Technology Solapur University "Biometric Feature based Person Unique Identification System" International Journal of Computer Applications (0975 – 8887) Volume 51– No.13.