IJASRM International Journal of Advanced Scientific Research and Management, Vol. 1 Issue 6, June 2016.
www.ijasrm.com
ISSN 2455-6378

# Performance Enhancement Security Technique of a Personal Multimodal Identification System Using Fusion of Keystroke Dynamics and Palm print Biometrics

**[1]Gaurav Kumar Singh,[2]Arjit Bansal,[3]Avinandan Nandi, [4]Chaitanya Bhat and [5]Dr. S. Venkatesan**

[1] Computer Science and Engineering, Dayananda Sagar College of Engineering,
Bangalore-560078, Karnataka, India

[2]Computer Science And Engineering, Dayananda Sagar College of Engineering,
Bangalore-560078, Karnataka, India

[3]Computer Science And Engineering, Dayananda Sagar College of Engineering,
Bangalore-560078, Karnataka, India

[4] Computer Science And Engineering, Dayananda Sagar College of Engineering,
Bangalore-560078, Karnataka, India

[5] Computer Science And Engineering, Dayananda Sagar College of Engineering,
Bangalore-560078, Karnataka, India

## Abstract

In this implementation, the objective of thesystem is to provide a multi-modal user authentication system, forincreased system security and efficient authentication for secure user login by a combination oftwo single-modal biometric systems, Keystroke Dynamics and Palmprint Recognition.This is done by comparing values of the registered keystroke timings and key values with thevalues that are obtained when the user enters the secure text during login time. The values arerecorded by calling a built-in MATLAB function for keystroke recording. After the Keystroke timings are recorded, theuser is prompted to place his palm in front of the camera, which captures the palm print image.After various pre-processing functions, comparison is done.

***Keywords:****Biometrics, palmprint recognition, keystroke dynamics, authentication, comparison.*

## 1. Introduction

Keystroke Dynamics is a behavioral biometric which uses the manner and rhythm in whichan individual types characters on a keyboard or a keypad. It is basically used in authenticationsystems, such as user login to an email account, database login and so on. In such systems,the keystroke rhythms and characters are recorded to develop a unique biometric template ofthe users typing pattern for future authentication. The manner in which the individual types isrecorded by timings between eachkey-press. Such a system requires low computational powerand is easy to implement.Palmprint Verification is a biometric system, where the user’s palm-print is used forauthentication. The authentication systems include user-login, authentication for entry intoareas of high security and authorization in an organization, etc. Specific features of the palm,such as principal lines, wrinkles and ridges, which are unique for each person, provide amethod for unique user verification. These unique features are extracted through dedicatedfeature extraction algorithms, after the palmprint image undergoes pre-processing.

### 1.1 User Registration:

User registration is the process of registering the user into the database of the system, for futureauthentication. The keystroke registration is done by prompting the user to enter a secure textthat is generated based on the users name three times, where the key pressed and the timingbetween each press is stored in a specific file in the user's database.For palmprint registration, the user is prompted to place his/her palm in a black box, wherethe palm print image of the user is captured three times to provide greater efficiency. Thepalm print images are stored in a specific location in the database unique to the user, for futureauthentication.

## 2. Proposed System

The outline of the Two-Way Authentication System is as follows:

### 2.1 Keystroke Implementation

The user, while registering, will have to type-in the automatically generated string thrice to increase the accuracy of the system of processesthat evaluate the dynamic values of the keystrokes typed in.Keystroke data obtained during the registration phase is processed in this phase. The timing for each keystroke is recorded and a normalizedvalue of each of the strings is evaluated. This value is then used for comparisonduring the user login. During login, authorization of the user takesplace. The user will have to type in the generated string during login. The wholeevaluation process is carried on this string and the evaluated value is compared to the value obtained during registration.

### 2.2Palmprint Recognition

Here, the image of the user's palm is first captured through a camera. Then, the image is converted to gray scale and canny algorithm is applied to it, which is an edge detection technique and it produces abinary image. This binary image consists of black and white pixels, wheretheblack pixels are discarded and the white pixels are evaluated for their intensityinformation.The evaluated information from the users palm is compared with theimages stored in the database. The total number of black pixels and white pixelsare calculated and their pixel intensities are compared with the already presentinformation.

## 3. System Requirements

The implementation of the proposed system will require a standard keyboard and webcamconnected to a computer for accepting the key patterns and the palm image during theregistration phase and also during the authorization phase. However, the software requirementsfor performing the implementation will be:

i. The software chosen for the implementation of this project is MATLAB R2015b.

ii. The operating system used will be either Microsoft Windows 7, 8, 8.1, 10.

## 4. Results and Discussion

Keystroke dynamics is implemented on the string generated by the system; typed the same bythe user at the specified field. Keystroke pattern is recorded thrice during registration of the user. This is used as a training setfor the system. Later on during login, same string is again typed by the user.Based on algorithm explained earlier, this login keystroke pattern is used to check the ingenuity of the user.

Further, for palmprint recognition, extensive research has been performed. During registration, user is asked for palm image input. Here, the system requires to capture 3 palm images, which would be essential for the training set. At the timeof login, user is asked to input another image. Through image-pixel comparisonmethod, matching is done and result is generated.

The system willgenerate authentication result to be true only when both the systems have cleared the threshold(threshold set for keystroke dynamics is 85% and for palmprint it is 90%).

## 5. Tables, Figures and Equations

### 5.1 Tables and Figures

The below table shows accuracy results and cases where the user is either accepted or rejected.

Table 1: Decision of Multimodal Approach

| KD Pass | Palm Pass | Deny/Grant |
|---|---|---|
| FALSE | FALSE | DENY |
| FALSE | TRUE | DENY |
| TRUE | FALSE | DENY |
| TRUE | TRUE | GRANT |

Table 2: Experimental result of Keystroke Dynamics

| S.No | Key Value during Login | Key Value1 | Key Value 2 | Key Value 3 | Error (E%) | Decision (P:pass,E <15%,F: fail,Otherwise) |
|---|---|---|---|---|---|---|
| 1 | 106.71 | 69.83 | 70.34 | 73.61 | 35.48 | F |
| 2 | 73.03 | 174.78 | 100.54 | 100.17 | 62.83 | F |
| 3 | 60.11 | 59.71 | 70.22 | 61.89 | 5.93 | P |
| 4 | 57.39 | 63.12 | 57.86 | 54.04 | 3.84 | P |
| 5 | 83.6 | 81.51 | 79.41 | 79.01 | 3.78 | P |
| 6 | 57.02 | 67.41 | 55.91 | 60.14 | 6.29 | P |
| 7 | 80.55 | 70.68 | 74.24 | 88.57 | 8.19 | P |
| 8 | 71.24 | 91.5 | 73.93 | 70.56 | 11.80 | P |
| 9 | 70.31 | 71.43 | 89.86 | 73.21 | 11.42 | P |
| 10 | 78.23 | 60.08 | 67.95 | 68.7 | 13.24 | P |
| 11 | 64.13 | 74.2 | 63.31 | 63.17 | 5.85 | P |
| 12 | 78.2 | 81.73 | 1.1 | 1.01 | 63.02 | F |
| 13 | 60.7 | 69.18 | 0.38 | 1.06 | 49.21 | F |
| 14 | 77.31 | 98.1 | 83.13 | 93.68 | 15.64 | F |
| 15 | 69.4 | 69.53 | 66.29 | 61.56 | 4.87 | P |
| 16 | 91.51 | 73.28 | 87.69 | 55.52 | 23.39 | F |
| 17 | 71.52 | 72.23 | 23.93 | 71.92 | 27.48 | F |
| 18 | 76.84 | 74.01 | 77.45 | 73.8 | 2.42 | P |
| 19 | 81.33 | 66.8 | 80.78 | 79.9 | 8.43 | P |
| 20 | 76.56 | 77.99 | 71.89 | 76.77 | 2.82 | P |

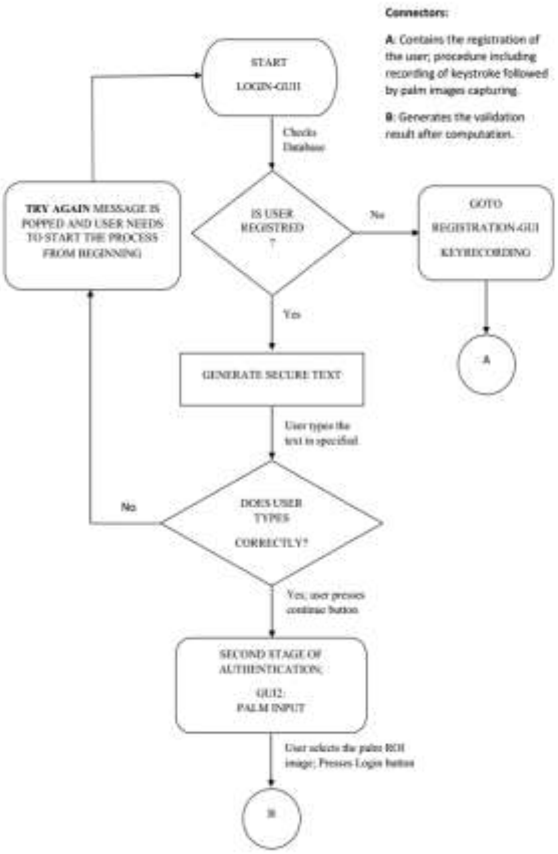
Connectors:
A: Contains the registration of the user; procedure including recording of keystroke followed by palm images capturing.
B: Generates the validation result after computation.
START
LOGIN-GUI1
Checks Database
TRY AGAIN MESSAGE IS POPPED AND USER NEEDS TO START THE PROCESS FROM BEGINNING
IS USER REGISTRED ?
No
GOTO REGISTRATION-GUI KEYRECORDING
A
Yes
GENERATE SECURE TEXT
User types the text in specified
No
DOES USER TYPES CORRECTLY?
Yes; user presses continue button
SECOND STAGE OF AUTHENTICATION;
GUI2:
PALM INPUT
User selects the palm ROI image; Presses Login button
B

Fig. 1. Dataflow control diagram of proposed system.

## 5.2 Equations

The following are equations used to calculate Keystroke Values:

$$\text{keyvalue} = 100*\sum(\text{time btw keys})*(\text{ASCIIvalue}) \qquad \text{Eq. (1)}$$

$$\text{Maxkeyvalue}=(\text{keyvalue0}-\text{keyvalue1})^2+(\text{keyvalue0}-\text{keyvalue2})^2+(\text{keyvalue0}-\text{keyvalue3})^2 \qquad \text{Eq. (2)}$$

$$\text{Finalkeyvalue} = \sqrt{}(\text{Maxkeyvalue}/3) \qquad \text{Eq. (3)}$$

## 6. Conclusions

We have proposed to implement a two-way authentication system, with the first level ofauthentication using Keystroke Dynamics, which records the timing pattern of the way keysare pressed on the keyboard, along with key values, and the second level using Palmprintverification, where the palm feature lines are extracted and used as a basis for comparisonduring future authentication.

First, for a new user, a registration GUI pops up, where he/she is first asked to type in the securetext generated, multiple times, so that the key timing and key values are recorded and stored for future authentication.

Second, the palmprint image of the user is captured multiple and various pre-processingtechniques, such as conversion to grayscale, extraction of ROI and conversion to binary foredge detection and future comparison, is applied. These registration parameters are stored in adatabase specific to the user for future authentication.

Finally, during the login process, the user is asked to type in the generated text to record thetimings and values of the keys pressed. Then, the palm image of the user to be compared isloaded and compared with a pre-loaded image of the user in the background, using the pixelmatching technique, after the image is fully pre-processed. If both authentication processes aresuccessful, the user is allowed entry into the system. If any one of the authentication processesfail, user access is denied.

### Acknowledgments

We thank Dr. S. Venkatesan, Professor, Dept. of CSE, Dayananda Sagar College of Engineering, for his constant guidance and encouragement to make this implementation a success.

We would also like to thank Dr. D.R. Ramesh Babu, Vice-Principal and H.O.D, Dept. of CSE, Dayananda Sagar College of Engineering, for his relentless support in making this implementation a success.

## References

[1] Wei Shu and David Zhang. Palmprint verification: an implementation of biometrictechnology. In Pattern Recognition, 1998. Proceedings. Fourteenth InternationalConference on, volume 1, pages 219–221. IEEE, (1998).

[2] Alen Peacock, Xian Ke, and Matthew Wilkerson. Typing patterns: A key to useridentification. IEEE Security & Privacy, (5):40–47, (2004).

[3] MM Khan, RK Subramanian, and NA Mamode Khan. Low dimensional representationof dorsal hand vein features using principle component analysis (pca). World Academy of Science, Engineering and Technology, 49:1001–1007, (2009).

[4] R Raghavendra, Mohammad Imran, Ashok Rao, and G Hemantha Kumar. Multimodalbiometrics: Analysis of handvein & palmprint combination used for person verification.In Emerging Trends in Engineering and Technology (ICETET), 2010 3rd InternationalConference on, pages 526–530. IEEE, (2010).

[5] Wei Li, Bob Zhang, Lei Zhang, and Jingqi Yan. Principal line-based alignment refinementfor palmprint recognition. Systems, Man, and Cybernetics, Part C: Applications andReviews, IEEE Transactions on, 42(6):1491–1499, (2012).

[6] Swarna Bajaj and Sumeet Kaur. Typing speed analysis of human for password protection(based on keystrokes dynamics). no, 2:88–91, (2013).

[7] Poonam RangnathDholi and KP Chaudhari. Typing pattern recognition using keystrokedynamics. In Mobile Communication and Power Engineering, pages 275–280. Springer,(2013).

[8] Muhammad Imran Ahmad, MohdZaizuIlyas, MohdNazrinMd Isa, RuzelitaNgadiran,and Abdul Majid Darsono. Information fusion of face and palmprint multimodalbiometrics. In Region 10 Symposium, 2014 IEEE, pages 635–639. IEEE, (2014).

[9] VisheshRaimugia, Naman Patel, AkshayPawar, and KhushaliDeulkar. Feature extractiontechniques for palmprint identification: A survey International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-2, Issue-11, November (2014).

[10] MithunaBehera and VK Govindan. Palm print authentication using pca technique. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 3638-3640, (2014)

[11] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, SoumikMondal,and Patrick Bours. Keystroke dynamics performance enhancement with soft biometrics.In Identity, Security and Behavior Analysis (ISBA), 2015 IEEE International Conferenceon, pages 1–7. IEEE, (2015).

[12] Shanmukhappa A Angadi and Sanjeevakumar M Hatture. A graph theoretic approachfor user identification using palmprint biometrics. In Next Generation ComputingTechnologies (NGCT), (2015) 1st International Conference on, pages 419–425. IEEE,(2015).