A Model to Secure Mobile Devices using Keystroke Dynamics through Soft Computing Techniques

M. Karnan, N. Krishnaraj

***Abstract**: In this mobile world, there are more mobile phones in than computers. Everyday more of these phones becomes smart phones. Nowadays, mobile devices functions like a mini computer, it becomes more attractive target for thieves. A reliable security application is needed to safeguard data and protect against theft. As mobile devices become more pervasive in our lives, there is a greater need to protect the data on such devices. The current PIN (Personal Identification Number) authentication in mobile device is weak and there is a demand of strong authentication. Biometrics adds an additional authentication and it provides most significant improvement in mobile security. In this research work, we proposed a hybrid authentication mechanism (keystroke, finger print and palm print) where biometric data's are captured and user template can be generated. The template is used to check whether the user is authenticated person or an imposter.*

***Index Terms**: PIN, Template, Keystroke dynamics, Finger print, palm print.*

I. INTRODUCTION

Authentication [5,13] is the process of verifying whether the digital identities of computers and the physical identities of people are authentic. Now a day the mobile phone usage has made revolutionary changes in our day to day life. Mobile devices are extremely useful for storing sensitive documents, manage email, delivering presentation, mobile banking.

In India most of the adults have been victims of mobile phone loss or theft. Only four in ten Indians have a password protecting their services. Traditional security system prompts a user to provide a 4 or 6 digit PIN to access protected data. It is not sufficient to protect the mobile devices. So ,there is a need of secure authentication method which protect sensitive data present in the mobile device.

The most common is authentication based on something know(usually a password). The second category is something has(ATM, Smartcard) and third category is based on something that a person is(Fingerprint, Palm print)[7,8].

In this paper , we concentrate on three things (i) keystroke dynamics (ii) Finger print recognition and (iii) palm recognition . Keystroke dynamics is a widely accepted biometric technique it can be easily implemented in mobile devices without need of any external hardware. Second finger print ,it requires special hardware to capture finger print[1], now a day's all the mobile phones have the capability to acquire finger print images. Example [GI100 – the first mobile phone with finger print recognition[21] technology] Third , palm recognition is a new physiological biometric technique provides reliable performance due to its stable and unique characteristics. It provides better results because , size of the image is large than finger print image. So, palm print is more unique than finger print. We concentrate on Physical security, Content Security and Device Management. So, reliable performance is assured in mobile devices.

In the proposed mobile user authentication system Fingerprint, Palmprint and Keystroke dynamics are combined in a single model in Fig2. The proposed system is implemented using Matlab7.0 and it shows reliable performance when compared with other unimodal and bimodal biometric authentication system.

II. BIOMETRICS

A. Definition

Biometric authentication [16] is an automatic method that identifies a user or verifies the identity based upon the measurement of his or her unique physiological traits or behavioral characteristics. Biometrics for mobile user authentication is becoming convenient and considerably more accurate[8,11,12]. Multibiometric is becoming socially acceptable because it is convenient (nothing to carry on remember), accurate (provides for positive authentication), and can provide better efficiency[14].

B. Keystroke Dynamics

Keystroke dynamics is a behavioral measurement and it aims to identify users how they type[8], such as duration of a keystroke or key hold time, latency of keystrokes (inter-keystroke times) [7,8]. The analogy is made to the days of telegraphy when operators identify each other by recognizing "the fist of the sender" [9]. Both the National Science Foundation (NSF) and National Institute of Standards and Technology (NIST), United States of America have conducted studies establishing that typing patterns are unique for the person [5].

C. Fingerprint & Palmprint

Palm and finger reader recognition systems measure and analyze the overall structure, shape and proportions of the hand, e.g. length, width and thickness of palm, fingers and joints[17,18]; characteristics of the skin surface such as creases and ridges.

Manuscript received on July, 2012.

Dr.M.Karnan, Department of Computer Science and Engineering, Tamilnadu College of Engineering, Coimbatore, Tamilnadu, India.

N.Krishnaraj, Research Scholar, Manonmaniam Sundaranar University, Tirunelveli,Tamilnadu , India.

The palm and finger scanner/reader devices still maintain accuracy even when hands are dirty, which are good in construction areas Palm and finger scanner recognition systems[19] are best used for verification due to less accurate detection compared to fingerprint detection and can be more expensive than these devices. Some drawbacks, Minor injuries to palm may occur, and weight fluctuations can prevent the device from working properly. Sometimes systems need to be updated regularly to accommodate these changes.

D. Performance of the Biometric System

The performance of the biometric system has been measured using (i) False Alarm Rate (FAR) and (ii) Imposter Pass Rate (IPR) [1]. FAR is the percentage of genuine users incorrectly categorized as imposters and IPR is the percentage of imposters incorrectly matched to a genuine user's reference template. Equal Error Rate (EER) is the rate of setting at which both false alarm and imposter pass errors are equal. EER is also known as the crossover error rate (CER). The lower the ERR (or CER), more accurate is the system. The overall performance of a biometric system is assessed in terms of its accuracy, speed, storage, cost and ease-of use.

III. EXISTING SYSTEM

In this paper, we proposed keystroke dynamics with finger print and palm recognition. As for our survey there is no researchers developed a model combined the above three things (keystroke , finger print and palm print). But finger print and palm print recognition [17,18] were developed and it produces better results.

IV. FEATURE EXTRACTION

In keystroke dynamics Various features can be extracted from the keystroke dynamics[8] are (i) Duration (Amount of a time a key is pressed), (ii) Latency (Differences of time between two key events), (iii)Mean, standard deviation (Mean and standard deviation value of each type of PIN), (iv) Press–Release (Latency between pressing and releasing the key), (v) Digraph . All the above features are used to create template for the particular user. In Fig1 the duration of the first letter T is the time between T_2 (key Release time) – T_1 (key press time), and latency between the letters T and H is T_3 (next key press) – T_2 (key release), the time between the two key-press B and H is T_5 and T_3 i.e. the duration of the first key with latency between the keys is the digraph, where T_1, T_2, T_3, T_4 and T_5 is the time when a key-release or key-press event occur.

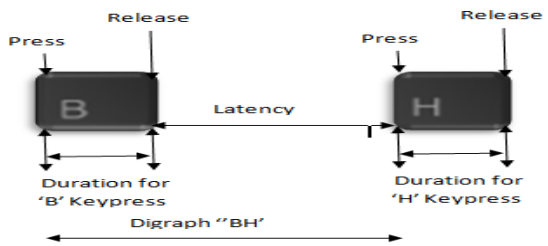

Fig 2 Duration, Latency and Digraph for the word "BH"

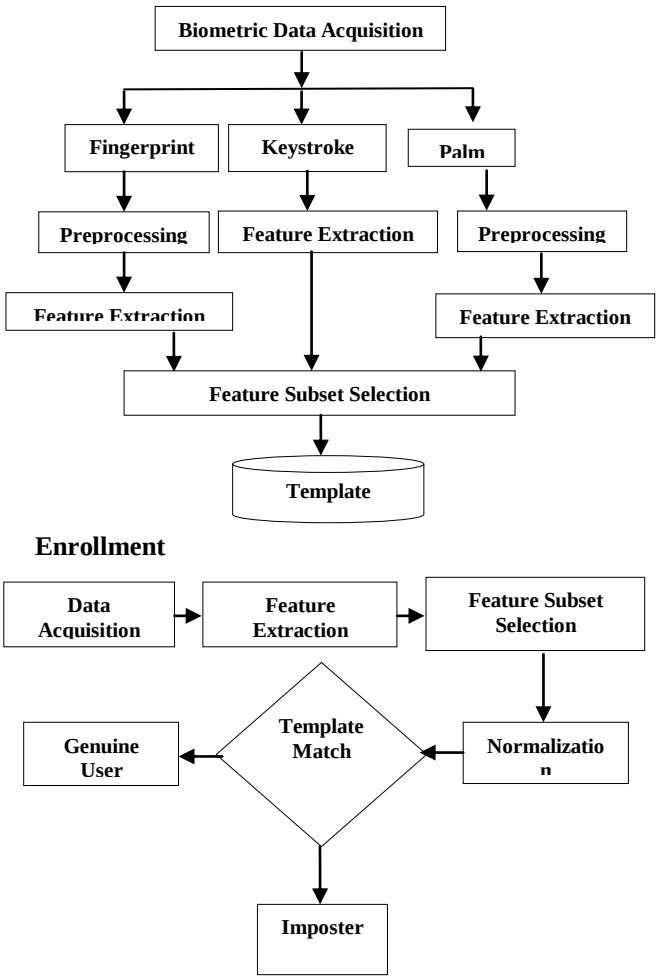

Fig1. Proposed Mobile Authentication system

A. Feature Extraction in Fingerprint Biometric System

The original finger print must be preprocessed in order to achieve high classification ratio. In the proposed system, original image is binarized, then the image is thinned using Bock filter technique, finally set of interest lines, ridge endings and ridge bifurcations from the input finger print images, minutiae are extracted [4,6], and spurious elements in the original image were eliminated. The template has been created based on the feature extracted from the original finger print image.

For each fingerprint image the following values are stored in the user template (i) a and y coordinates of the minutiae (ii) the orientation angle of the ridge containing the minutiae

B. Feature Extraction in fingerprint and Palmprint Biometric System

In recognition, the Gabor filter is used for feature extraction, where mean and standard deviation of the palmprint has been extracted. The palmprint images are preprocessed before extracting the features.

The aim of preprocessing is to eliminate the unwanted components in the input images.

The palmprint recognition based on the principal lines, wrinkles and ridges on the surface of the palm[2]. The line structures are stable and remain unchanged throughout the life of an individual.

V. F EATURE SUBSET SELECTION

Feature selection is used to remove irrelevant features. The aim of feature selection is to reduce the quantity of data and speed up the computation time, and also to improve the performance of the system. Several Optimization techniques like Particle Swam Optimization (PSO), Ant Colony Optimization (ACO) and Bacteria Foraging Algorithm (BFOA) was used for selecting subset features [3,10]. The selected features in the finger print and palm print is given as the input to the BFOA algorithm, to find out the dominant subset features.

The selected features will be given as the input the classification. The dominant features improve the classification accuracy. In the proposed system each biometric techniques can be implemented separately and it combinations are implemented, their performance are measured.

A. Bacteria Foraging Optimization Algorithm

The Bacteria Foraging Optimization Algorithm (BFOA) has been widely accepted as a global optimization algorithm[10], inspired by social foraging behavior of E-coli described in the algorithm.

Chemotaxis :

It simulates the E-coli movement through swimming and tumbling via flagella.

Swarming :

All E-Coli groups organized in such a way that travelling a ring by moving to nutrient gradient.

Reproduction :

The least health bacteria eventually die, and healthier bacteria split into two and placed in same location.

Assumptions :

S_p – Dimension of Search Space
N_b –Total number of bacteria in the population
C_s – Number of chemotatic steps
S_l –Swimming length
N_{re} – Number of reproduction steps
N_{ed} –Number of elimination Dispersal Events
P_{ed} – Probability of Elimination Dispersal Events

Algorithm

1. Initialize ($S_p, N_b, C_s, S_l, N_{re}, P_{ed}$)
2. Elimination dispersal loop i=i+1
3. Reproduction loop k=k+1
4. Chemotaxis loop p=p+1
   - 4.1 for i=1,2..n, take chemotatic step for n bacterium i
   - 4.2 compute fitness function $B_b(I,p,k,l)$
   - 4.3 Assign $B_{last} = B_b(I,p,k,l)$
   - 4.4 Tumple
   - 4.5 Move
   - 4.6 Compute fitness function $B_b(I,p+1,k,l)$
   - 4.7 Swim
     - 4.7.1 m=0 (swim length counter)
     - 4.7.2 while m< S_l then m=m+1
     - 4.7.3 if $B_b(I,p+1,k,l) < B_{last}$ $B_{last} = B_b(I,p+1,k,l)$ else m= S_l
   - 4.8 Go to next bacterium (i+1)
5. if p< C_s go to step 4
6. Reproduction
   - 6.1 Compute health of each bacteria $P^I_{health} = \sum_{p=1}^{Cs+1} p(i,p,k,l)$
   - 6.2 The bacteria with lowest health die, and highest health slit into two , and palced in same location.
7. If k< N_{re} , goto step3
8. Elimination – Dispersal
   For I = 1,2 … n , with probability p_{ed}eliminate & disperse each bacterium
9. If l< N_{ed} then goto step2.
   Else end.

VI. CLASSIFICATION

Classification is the main task for different applications like voice recognition, text classification, data classification and image classification.etc. Support Vector Machine (SVM) [7] is used to classify the features. Each user's individual template is given as the input to the input layer of SVM after normalization. The network is trained to produce the target value assigned for each user and the results from the output layer are stored in the database inorder to find classification accuracy. The SVM classification produces better performance with BFOA. The network is trained to produce output value of 0.9 for genuine user and 0.1 for imposter. The time required to train and test the data with SVM shown in Table1.

Table 1 : Training time and Testing time required for biometric techniques

Biometric Techniques	Algorithm	Training (ms)	Testing (ms)
Keystroke	BFOA	28	0.62
	PSO	30	0.70
	ACO	20	0.65
Fingerprint	BFOA	28	0.62
	PSO	35	0.71
	ACO	23	0.68
Palmprint	BFOA	36	0.84
	PSO	27	0.92
	ACO	24	0.86
Keystroke & Fingerprint	BFOA	24	0.51
	PSO	32	0.59
	ACO	19	0.54
Keystroke & Palmprint	BFOA	28	0.62
	PSO	26	0.70
	ACO	20	0.63
Fingerprint & Palmprint	BFOA	32	0.73
	PSO	30	0.81
	ACO	23	0.77
Keystroke & Fingerprint & Palmprint	BFOA	21	0.41
	PSO	30	0.48
	ACO	15	0.40

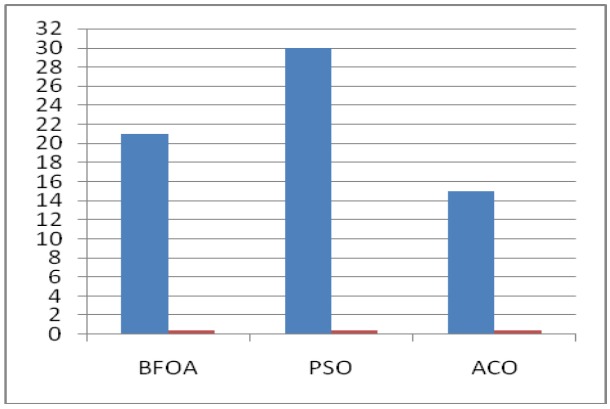

Fig3. Time Required to train and test data

VII. PERFORMANCE EVALUATION

FAR is used to determine the classifier performance.FRR, is used to determine how many incorrect positive results occur among all positive samples during the test. The proposed hybrid system was tested on 200 samples of keystroke features, 100 finger print and 100 palm print features to verify the classification accuracy. As computational time and classification accuracy BFOA provides better performance than other existing methods, shown in fig4.

From the experiments and results, the proposed hybrid authentication system (Fingerprint, Palmprint and Keystroke dynamics), produces 92.8% of accuracy in detecting imposters is shown in Table2 and the error rate is 0.063 shown in Fig5.

Table 2 : Accuracy and Error Rate of Biometric Techniques

Biometric Techniques	Algorithm	Accuracy	Error Rate
Keystroke	BFOA	90.6	0.069
	PSO	86.9	0.088
	ACO	84.6	0.073
Fingerprint	BFOA	88.4	0.076
	PSO	83.5	0.081
	ACO	85.2	0.086
Palmprint	BFOA	88.2	0.083
	PSO	84.6	0.080
	ACO	86.7	0.078
Keystroke & Fingerprint	BFOA	83.2	0.074
	PSO	85.8	0.086
	ACO	85.9	0.082
Keystroke & Palmprint	BFOA	88.3	0.077
	PSO	84.8	0.086
	ACO	86.4	0.077
Fingerprint & Palmprint	BFOA	86.9	0.081
	PSO	82.7	0.072
	ACO	85.4	0.059
Keystroke & Fingerprint & Palmprint	BFOA	92.8	0.059
	PSO	86.6	0.078
	ACO	88.9	0.063

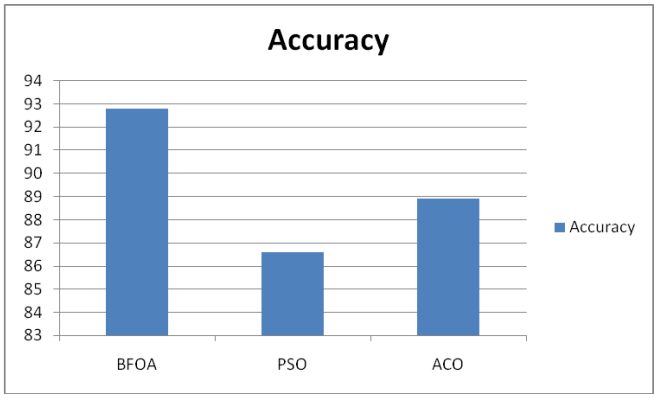

Fig4: Accuracy of Fingerprint, Palmprint and Keystroke Dynamics

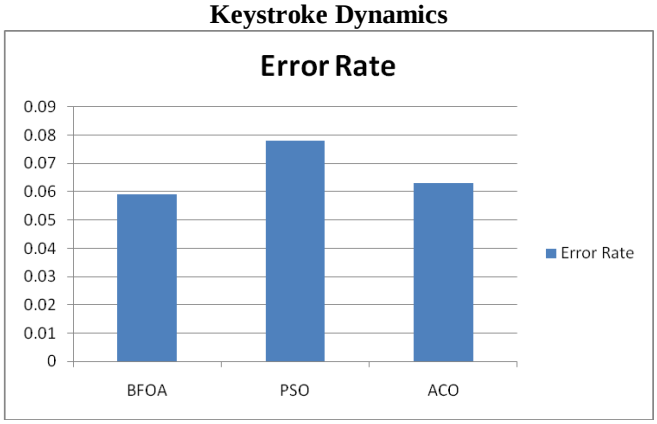

Fig5: Error rate of Fingerprint, Palmprint and Keystroke Dynamics

REFERENCES

1. Chandran GC, Rajesh RS (2009). Performance Analysis of Multimodal Biometric System Authentication, Int. J. Comput. Sci. Network Security, 9: 3.
2. Chin YJ, Ong TS, Goh M K O, Hiew B Y (2009). Integrating Palmprint and Fingerprint for Identity Verification, Third International Conference on Network and System Security.
3. Das, S., Biswas, A., Dasgupta, S. & Abraham, A.2009b.Bacterial foraging optimization algorithm: Theoretical foundations, analysis, and applications. In Foundations of Computational Intelligence (3), 23–55.
4. De-Song Wang, Jian-Ping Li, A New Fingerprint -Based Remote User Authentication Scheme Using Mobile Devices , Apperceiving Computing And Intelligence Analysis, 2009. ICACIA 2009. **Page(S):** 65 – 68 , Chengdu, China
5. Duane Blackburn, Chris Miles, Brad Wing, Kim Shepard, Biometrics Overview,National Science and Technology Council (NSTC) Committee on Technology Committee on Homeland and National Security, 2007.
6. Jea.T.Y and Govindaraju V, "A minutia-based partial fingerprint recognition system," *Pattern Recognition*, vol.38, pp. 1672-1684, 2005.
7. Karnan.M, ,Akila,M and Krishnaraj.N Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*, 1(2):1565–1573, March 2011.
8. Karnan.M, , Krishnaraj.N ,Bio password—keystroke dynamic approach to secure mobile devices. In *IEEE International Conference on Computational Intelligence and Computing Research*, pages 1–4, December 28–29, 2010, Tamilnadu, India, 2010.
9. Kenneth Revett , *Behavioral Biometrics: A Remote Access Approach* , John Wiley & Sons, Ltd. ISBN: 978-0-470-51883-0 , 2008
10. Kim, D. H., A. Abraham, and J. H. Cho, "A hybrid genetic algorithm and bacterial foraging approach for global optimization," *Information Sciences*, Vol. 177, 3918-3937, 2007.
11. Kumar, A., Zhang, David, (2006). Combining Fingerprint, Palmprint and Hand-shape for User Authentication, 18th Internation Conference on Pattern Recognition, ICPR 2006, 4, pp. 549 - 552.

12. Kumar.A, Wong D.C.M, Shen H.C, and Jain A.K, "Person verification using palmprint and hand geometry biometric*" Proc. Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pp.668-675, 2003.
13. Matyas S.M, Stapleton J, A biometric standard for information management and security, Computers & Security 19 (n. 2) (2000) 428–441.
14. Ross.A, Nandakumar.K, and Jain.A.K, Handbook of Multibiometrics, Springer Verlag, 2006.
15. Saevanee. H and Bhatarakosol P. User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device. In ICCEE 2008, pages 82–86, December 20– 22, 2008, Phuket, Thailand, 2008. IEEE Computer Society, Los Alamitos, CA.
16. Samir Nanavati, Michael Thieme, Raj Nanavati, Biometric's Identity Verification in a Networked World, John Wiley and Sons Inc./Wiley Computer Publication,2003.
17. Yao YF, Jingb XY, Wong HS (2007). Face and palmprint feature level fusion for single sample biometrics recognition, Neurocomputing, 70: 1582-1586.
18. Zhou J, Su G, Jiang C, Deng Y, Li C (2007). A face and fingerprint identity authentication system based on multi-route detection, Neurocomputing, 70: 922-931.
19. www.findbiometrics.com/hand-and-finger/
20. www://subhb.org/2012/01/26/palm-recognition- technology -to-enable-mobile-biometrics/
[21] www.mobilemag.com/2004/11/30/pantech-gi100-
22. mobile-phone-with-biometric-fingerprint- recognition/

AUTHORS PROFILE

Dr.M.Karnan received the PhD Degree in Computer Science and Engineering in 2007 from Gandhigram Rural University (fully funded and controlled by Government of India), Dindigul, Tamilnadu, India. He obtained the Master of Engineering Degree in Computer Science and Engineering in 2000 from Government College of Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India. He received the Bachelor of Engineering Degree in Electrical and Electronics Engineering from Government College of Technology Bharatiar University, Madurai, Tamilnadu, India.Currently he is working as Professor in Department of CSE , TCE, Coimbatore, Tamilnadu, India. His area of interest is Biometrics in Pattern Recognition, Neural Networks, Pattern Recognition, Data Mining, etc..

N. KRISHNARAJ received the B.Tech in Information Technology in 2005 from Anna University, Chennai, Tamilnadu, India. He obtained the Master of Engineering Degree in Software Engineering in 2007 from Anna University,Chennai, Tamilnadu, India. Currently he is working as Assistant Professor in Department of Information Technology, Hindusthan College of Engineering and Technology,, Coimbatore, Tamilnadu, India. Her area of interest is Biometrics in Pattern Recognition. He is a Research Scholar in Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India.