Middle-East Journal of Scientific Research 24 (4): 1355-1361, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.04.23373

Enhancing Security in Mobile Devices Through Multimodal Biometrics

[1]N. Krishnaraj, [2]P. Ezhilarasu, [3]S. Karthick and [2]J. Manoj Prabhakar

[1]SRM Valliammai Engineering College, Kattangulathur, Chennai, Tamilnadu, India -603203
[2]Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India -641032
[3]Hindusthan Institute Technology, Coimbatore, Tamilnadu, India -641032

Abstract: In recent years, dependency upon the mobile devices has increased rapidly, as we can store sensitive information in them, perform business transactions, etc.. Hence it becomes necessary to protect mobile devices from impostors. To develop better solutions, in order to secure mobile devices, is one of the major research work across the world. Authentication is an added security measure, which is used to prove that someone or something is who they're before they're allowed to access any confidential data. Usually, PIN/password protection mechanism is used for protection of mobile devices. But its major drawback is that, it can be disabled by the users owing to its inconvenience. Therefore, in order to provide security to these devices in an even easier and efficient manner, biometric authentication is proposed.

Key words: Biometrics · Keystroke Dynamics · Fingerprint Recognition · Palm recognition · Feature extraction · Feature subset · SVM

INTRODUCTION

Authentication [1], is an added security measure used to prove that someone or something is who or what they say, they're, in order to allow then access to confidential information. There exists several authentication technologies that verify the identity of a user before granting access. Flow ever, most of these technologies offer protection at different levels and hence no single security measure provides complete security. An individual is mostly identified based on username and password. In security systems, authentication differs from authorization, which is the process of giving individuals access to system objects based system.

With the growing reliance upon mobile devices over recent years, it has widened the gap between the degree of user trust and the level of information security that these devices provide. More expensive and technologically advanced devices are more prone to theft during the fewer significant devices greater possibility of getting lost. Biometric information [2] proposed as a solution to many of the authentication and security needs in mobile devices, but owing to the high cost, greater size, weight, consumption of battery power [3] etc., It's ideally suited for mobile devices such as telephones due to its potential implementation overheads. In response to modern device security options, such as PIN protection [6], which's often disabled by users, due to an inconvenience, biometric is proposed for the devices that require higher security. Moreover, its offers minimal inconvenience to the user. The major drawback of biometric systems its costs and cannot be implemented in modern applications. Hence, the need for a biometric system, that require minimal cost and is easy to implement arises.

In this paper, a model to secure mobile devices using keystroke dynamics through soft computing techniques has been proposed.

Biometric Authentication: Biometric authentication is an scientific method that identifies a user or verifier his/her identify based on physiological traits (fingerprints, face, hand or palm geometry, retina etc.,) [4] or behavioral characteristics(voice, gait, signature keystroke dynamic etc.,). Physiological biometrics [5] is a biological/chemical trait that’s innate or naturally grown and behavioral biometrics is mannerisms or traits that's learned or acquired.

Corresponding Author: N. Krishnaraj, SRM Valliammai Engineering College, Kattangulathur , Chennai, Tamilnadu, India -603203.

Advantages of Biometric Approach:

- The biometric trait is unforgettable.
- It cannot be lost.
- It cannot be shared and uniqueness.
- It prevents identity theft.
- Uniqueness.

The other biometrics techniques[8] are not efficient because

- Additional hardware device for mobile phones.
- Cost.
- Low computational power.
- Limited storage.
- Difficult to Implement.
- Design Constraints [9]

Keystroke Dynamics: The current keystroke dynamics studies choose either static or dynamic text entry as a basis for comparing a typing pattern with a pattern captured during enrollment. Static text [7] entry requires the user to type a predefine text string as their PIN and compares the keystroke patterns to those gathered at an enrollment using the same predefined PIN. Authentications based on static text entry are significantly easier to implement and provide much more acceptable error rates. Dynamic text entry is a much better approximation of real world situations, however and allows the authentication based on keystroke dynamics to take place in a transparent manner, which increases the likelihood of general user acceptance.

True dynamic text entry means that the text entered should not be constrained in any way, including allowing the user to choose what text they wish to enter as well as allowing errors, pauses and other breaks in the flow of text entry. Keystroke dynamics based authentication system shown in Fig 2.1 requires users to register their details. The features are extracted from the user inputs and most dominant features were selected in feature subset selection. The matcher in the application device identifies the user, whether he is genuine or not.

Advantageous of Keystroke Dynamics: The advantages of keystroke authentication are;

- Additional hardware not needed.
- Very less cost.
- Computational power & Storage.

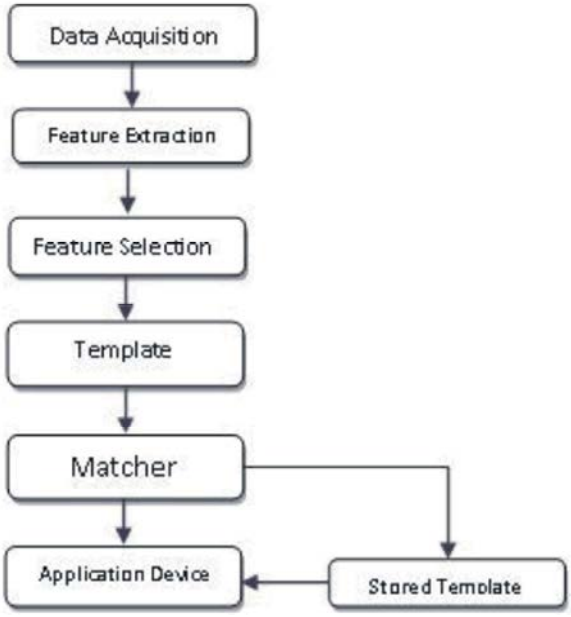


Fig. 2.1: Keystroke Dynamics Analysis Framework

Fingerprint: Fingerprint is the biometric authentication technique used to identify the people by using their impressions [10]. The user impression is captures using the fingerprint scanner; then the features are extracted from the input image. The Fig. 1.5 Shows the different parts of fingerprint impression.

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints [11]. Fingerprint is a kind of biometrics used to identify individuals and verify their identity. Fingerprint recognition [12] technology for mobile devices is posed as a preferred user authentication solution in terms of security.

Advantages of Using Finger Recognition:

- Require less space to store the fingerprint biometric data.
- Efficient biometric technique, widely used in the world for all security applications.
- Fingerprint patterns are unique for everyone. The twins also have different fingerprint patterns.

Palm Recognition: Palm Recognition is a kind of biometric technique used for user authentication. The palmprint recognition is similar to fingerprint recognition [13]. The major difference between fingerprint and palmprint is, the palmprint area is larger in size. Now a days all the

Smartphone's have the capability of capturing palmprint images. So, the palmprint [14] can be implemented in mobile phones as an additional security measure to protect the sensitive data from the thieves. Palm prints are relatively easy to capture and measure with a typical camera equipped with smartphones. Like fingerprint, palm print also contains sufficient information [15] to personals and principle lines of a palm image likely to remain stable over time [16]. Thus, palmprint matching typically focuses on matching these principle lines.

Palm Print Recognition vs Fingerprint Recognition: Several aspects of palm vein recognition make it more reliable and easier to use than fingerprint recognition. Palm print patterns are imperceptible and near impossible to falsify, to make the system more secure.

Advantages of Palmprint Recognition:

- Palm area is larger when compared to fingerprint area.
- High resolution is not required.
- Not sensitive to noise
- More distinctive features can be extracted from palmprint images.
- High reliability.
- Universally acceptable.

Intelligent System to Secure Mobile Devices: The proposed mobile user authentication system shown in Fig 3.1 has major four phases namely,

- Feature Extraction
- Feature Subset Selection
- Classification
- Performance Evaluation

The feature extraction, the user, has to type their Password/ PIN for the specified number of times. From the user, keystroke data feature vector has been created. [17]. Different keystroke features (Duration (D), Latency (L), Digraph (DI), Duration & Latency, Latency & digraph, Digraph & duration and Digraph & Duration and Latency) and their combinations are calculated which is given as input to the feature subset selection phase[18].

To acquire fingerprint [19] and palm print data, the user's finger and palm images are acquired through the scanner device that is inbuilt in the mobile devices. In this paper, the static enrollment process is used. The feature extraction [20] extracts the features of the system. There are many types of feature that can be gathered during a user's typing session.

In this paper feature's duration, latency, digraph and their combination of each user keystrokes are used in the extraction phase. The ridge endings, Bifurcations and minutiae points are extracted from the Fingerprint of the user. Similarly in palm print principal lines, ridges and wrinkles are extracted.

In Feature subset selection Bacteria Foraging Optimization Algorithm (BFOA) is used. The best subset used to identify the imposter is calculated from the set of features. The accuracy and time requirement are calculated. The proposed BFOA technique is computationally more efficient in finding the dominant features.

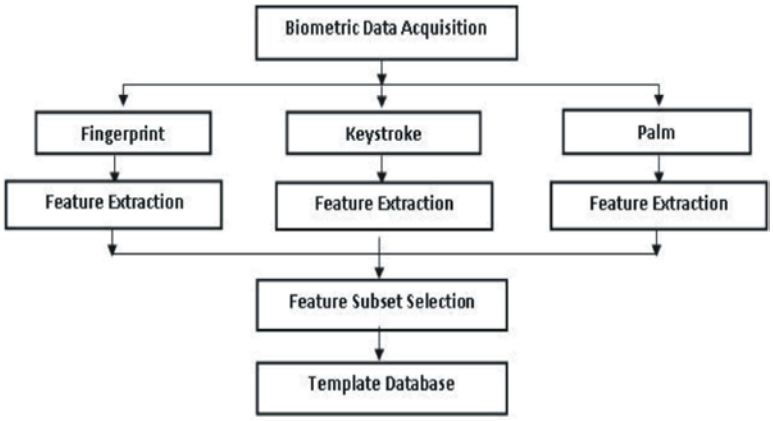
Feature subset selection algorithms search for the optimal subset of features for the problem at hand. In classification problems, it is assumed that a small number of features is sufficient to solve the problem for that greedy sub-optimal solution is used.

In Classification Support Vector Machine, (SVM) is used to classify the features. During the enrollment, user biometric data is acquired, processed and stored as templates.

There is several classification methods used in keystroke dynamics research. The historical favorite has been pattern classifiers, which is come under statistical classifier. Commonly used statistical classifier Bayes (including Naïve Bayes), Mahalanobis distance, Hamming distance, Euclidean distance, etc. Most recent studies have begun to use neural networks as a pattern classification method. Common neural network approaches include Feed Forward Multilayered Perceptron Networks (with or without back propagation), Radial base function networks and Generalized Regression Networks. The neural networks are superior classification method, but the mobile devices lacking in computing power necessary to employ a neural network in a situation where the processing is done on the device itself.

Classification is the process that identifies the best class among others. Support Vector Machine (SVM) classify the features in the classification phase. The network is trained based on the target value. Then the network is tested to classify the users feature as valid or invalid feature.

Enrollment



Verification

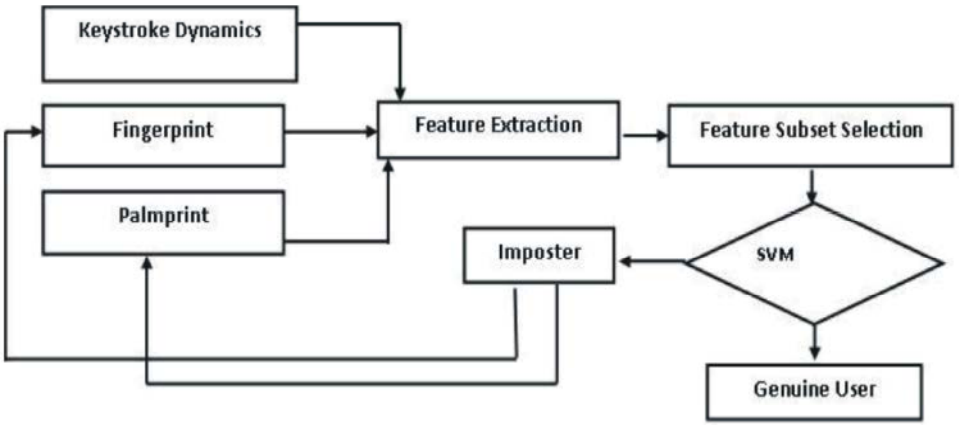


Fig. 3.1: Intelligent system to Secure Mobile Devices

Classification: In classification, Support Vector Machine (SVM) is proposed to identify the imposter. The classifier is trained on the dataset acquired from the users. The best feature selected, using BFOA is fed to the SVM classifier. Based on the input, the classifier decides whether the user is genuine or an imposter.

The SVM classify function uses results from strain to classify vectors x according to the following equation.

$$c = \sum_i \alpha_i k(s_i x) + b,$$

where $_{Si}$ is the set of support vectors, α are the weight value, b is the bias value and k is a kernel function. In linear kernel, k is the dot product. If $c = 0$, then x is a member of a first group, otherwise it is classified as a member of the second group.

Support Vector Machine (SVM) is seemed to be much more suitable for pattern classifier than Back Propagation Neural Network (BPNN) because it can solve a non-linear problem and for its ability to classify pattern and it is better in generalization. The input values of Mean, Standard deviation and Median of a duration value sample of User is given to SVM for training shown in Table 4.1.

The weight of the support vectors and bias are initialized. After applying the SVM Learning, the calculations are done. The objective function and accuracy of the classifier are calculated. The SVM classifies the input as two groups based on the Class:

Class I - Genuine
Class II - Imposter

In the SVM Classification, the Pbest value is fed to the classifier, based on the training samples, the classifier has to decide whether the user is " Genuine" or "Imposter".

Table 4.1: Dataset for SVM Training

Duration-Mean		Duration - SD		Duration -Median	
Class I	Class II	Class I	Class II	Class I	Class II
Genuine	Imposter	Genuine	Imposter	Genuine	Imposter
1.4077	1.3418	-0.3010	-0.3416	1.0385	1.1560
1.1381	1.1953	0.0656	0.3416	1.2400	2.5486
1.2823	1.7038	0.1739	0.1544	1.3400	2.3456
1.3220	1.4029	0.3123	0.3909	1.6450	1.1560
1.3476	1.9448	0.3446	0.3045	1.0389	1.6650

The following steps explains the SVM Classification

Step 1: The classification Function is;

$$c = \sum_i \alpha_i k(s_i x) + b,$$

where Si – Support Vector, ái - Weight, b - Bias

Kernel function

K=tanh(p1*U*V+p2)
where, p1 =1 & P2=-1
KKT Violation Level - [0]

Step 2: The first Pbest value is fed as the input to the classifier

Pbest = 1.0478

Step 3: The number of support vector that support the input = 0
Step 4: Set U, V =1, because first we take a first column and first-row value of Pbest among 21 features.
Step 5: The value of U, V[1, 1] =1.0477
Step 6: Calculate the Kernel Value

K = 0.0976
Step 7: Assign weight ái = 0.5
Step 8: Set b=0
Step 9: Compute the Class Value

$$c = \sum_i \alpha_i k(s_i x) + b,$$

C = 1.0488
Step 9: The class value does not match with the trained dataset.
Step 10: The classifier decides the user is "Imposter."

Classification Accuracy: In the proposed mobile user authentication system, the classification accuracy and error rate are discussed in this chapter. The classification accuracy of an optimization algorithm is shown in Table 5.2 and the graphical representation shown in Fig. 4.1 and Fig. 4.2. From the experiments and results, the single biometric authentication does not provide as much security in mobile devices. But the combination of multi-biometric system shows reliable performance. Finally, it is concluded that the combination of fingerprint, keystroke and palm shows excellent performance in identifying imposters.

False Acceptance and False Rejection Rate: FRR of verification system gives an indication of how often an authorized individual will not be properly recognized. FAR of verification system gives an indication of how often an authorized individual will be properly mistakenly recognized. FAR and FRR are important intrinsic characteristics of a matcher. The goal of the proposed authentication system to have a low False acceptance rate (FAR) and low False rejection rate (FRR) .FAR and FRR of the proposed system is shown in Fig. 4.3.

Table 4.2: Accuracy and Error rate of Proposed Biometric Techniques

S.NO	Biometric Techniques	Accuracy	Error Rate
1	Keystroke	92.6	0.069
2	Fingerprint	98.4	0.076
3	Palmprint	94.2	0.083
4	Keystroke & Fingerprint	94.6	0.074
5	Keystroke & Palmprint	92.4	0.077
6	Fingerprint & Palmprint	93.8	0.081
7	Keystroke & Fingerprint & Palmprint	95.9	0.059

Table 4.3 Error Rate of SVM Classifier

S.No	Biometric Technique	FAR	FRR
1	Keystroke Dynamics	0.618	0.412
2	Fingerprint	0.508	0.234
3	Palmprint	0.562	0.248
4	Keystroke Dynamics & Fingerprint	0.522	0.295
5	Keystroke Dynamics & palmprint	0.590	0.33
6	Fingerprint & Palmprint	0.535	0.279
7	Keystroke Dynamics & Fingerprint & Palmprint	0.494	0.213

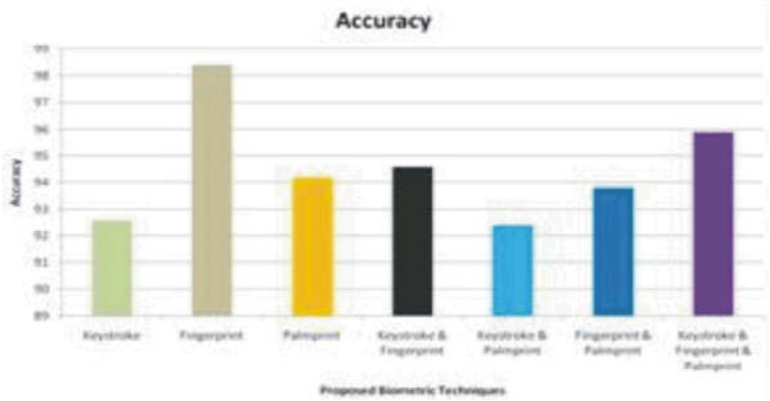


Fig. 4.1: Accuracy of Proposed Biometric Techniques

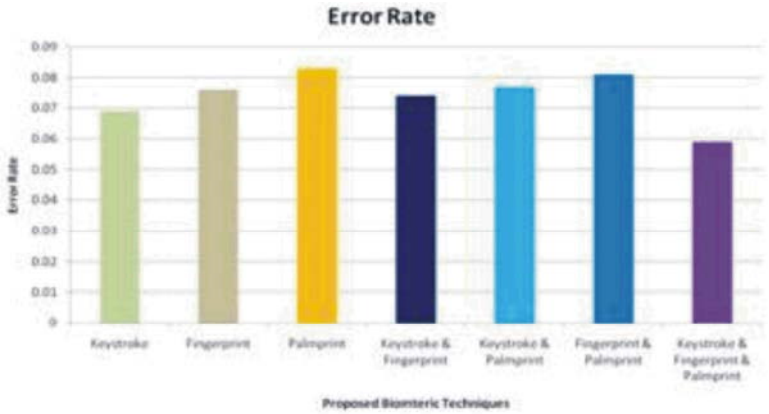


Fig. 4.2: Error Rate of Proposed Biometric Techniques

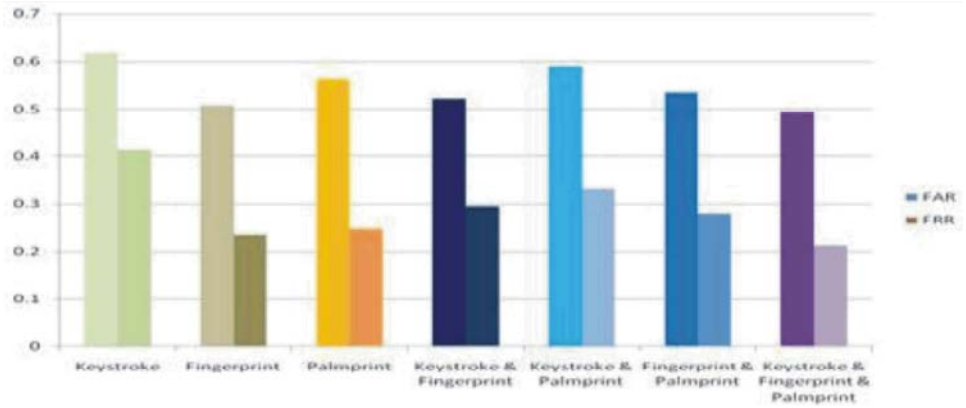


Fig. 4.3: FAR and FRR of SVM Classifier

CONCLUSION

This paper aims at developing new intelligent system to secure mobile devices, using soft computing algorithm. Bacteria Foraging Optimization Algorithm (BFOA) is proposed. This particular piece of work consist of four major phases, namely Feature extractions, features subset selection, classification and Performance Evaluation. In feature subset selection, the most dominant features are selected from the keystroke, fingerprint and palmprint features. It's used to improve the classification accuracy when detecting the imposter. The BFOA is used to select the subset features from the set of features. The results so obtained, shows BFOA showing better performance in selecting the dominant feature from the set of features. In performance analysis, the single biometric and multi-

biometric systems are analyzed separately and also the accuracy and error rate of the BFOA is analyzed. The accuracy and error rate of the combination of keystroke, fingerprint and palmprint is 95.9 and 0.059.To conclude, the single biometric system does not provide reliable performance, while in contrast, the combination of the keystroke, fingerprint and palmprint biometric techniques provides reliable security for mobile user authentication and also BFOA is found to give a better performance in feature selection and classification.

REFERENCES

1. Marcus, Karnan and N. Krishnaraj, 2010. "Biopassword – A Keystroke Dynamics Approach to Secure Mobile Devices", in IEEE International Conference on computational Intelligence and Computing Research (ICCCIC), pp: 1-4.
2. Marcus, Karnan and M. Akila, 2010. "Personal Authentication based on Keystroke Dynamics using Soft Computing Techniques The 2010 International Conference on Communication Software and Networks (ICCSN 2010) 26 - 28, February 2010, Singapore.
3. Marcus Karnan, M. Akila and N. Krishnaraj, 2011. " Biometric Personal Authentication using Keystroke dynamics – A Review", in International Journal of Applied soft Computing, 11(2): 1565-1573.
4. Marcus, Karnan and N. Krishnaraj, 2012. "A Model to Secure Mobile Devices Using Keystroke Dynamics through Soft Computing Techniques" in International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012
5. Leggett, J. and G. Williams, 1988. " Verifying Identity via Keystroke Characteristics", International Journal of Man-Machine Studies, 28-1, 67-76.
6. Rajkumar Janakiraman and Terence Sim, " Keystroke Dynamics in a General Setting", dvances in Biometrics, Lecture Notes in Computer Science, 4642: 584-592.
7. Sajjad Haider, Ahmed Abbas and Abbas K. Zaidi, 2000. A multi-technique approach for user identification through keystroke dynamics, Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, 2: 1336-1341.
8. David Cooper, Secure Biometric Match-on-Card Feasibility Report, National Institute of Science and Technology, U.S Department of Commerce , NIST Interagency Report 7452. Gaithersburg , MD, 2007.
9. Duane Blackburn, Chris Miles, Brad Wing and Kim Shepard, 2007. Biometrics Overview, National Science and Technology Council (NSTC) Committee on Technology Committee on Homeland and National Security, 2007.
10. Hong, L., Y. Wan and A.K. Jain, 1998. "Fingerprint image enhancement:Algorithm and performance evaluation," IEEE Trans. Patt. Anal. Machine Intell., 20: 777-789.
11. Jing, X.Y., Y.F. Yao, D. Zhang, J.Y. Yang and M. Li, 2007. "Face and palmprint pixel level fusion and Kernel DCV-RBF classifier for small sample biometric recognition", Pattern Recognition, 40: 3209-3224.
12. Matyas, S.M. and J. Stapleton, 2000. A biometric standard for information management and security, Computers & Security, 19(2): 428-441.
13. Fronthaler, H., K. Kollreider and J. Bigun, 2006. "Automatic image quality assessment with application in biometrics," in Proc.Workshop Biometrics, Assoc. CVPR, pp: 30-35.
14. Jiuqiang, Han and Fenghua Wang, 2008. Robust Multimodal Biometric Authentication Integrating Iris, Face and Palmprint, Information Technology and Control, 37(4).
15. Savic, T. and N. Pavesic, 2007. "Personal recognition based on an image of the palmar surface of the hand", Pattern Recognition, 40: 3252-3163.
16. David Zhang, Wai-Kin Kong, Jane You and Michael Wong, 2003. Online Palmprint Identification IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(9).
17. Jain, A.K. and A. Ross, 2004. Multibiometric Systems. Communications of the ACM, Special Issue on Multimodal Interfaces, 47(1): 34-40.
18. Jain Anil, K. *et al*., 1999/ Biometrics: Personal Identification in Networked Society. Springer.
19. Samir Nanavati, Michael Thieme and Raj Nanavati, 2003. "Biometrics Identity Verification in a Networked World" , John Wiley and Sons Inc., Wiley Computer Publication.
20. Seong-Seob Hwang, Hyoung-joo Lee and Sungzoon Cho, 2009. "Improving Authentication Accuracy Using Artificial rhythms and cues for Keystroke Dynamics based Autentication", Expert system with Applications: An International Journal, 36(7): 10649-10656.