ISSN 2394-739X

IJRSET

International Journal for Research in Science Engineering and Technology

AN EFFECTIVE SWARM INTELLIGENCE BASED PASSIVE BIOMETRIC CONTINUOUS AUTHENTICATION SYSTEM

[1] **K. Juliana GnanaSelvi,**
[1] Head of the Department,
[1] Department of Information Technology,
[1] Rathinam College of Arts and Science,
[1] Coimbatore, Tamil Nadu – 641 021.

Abstract:-

Swarm intelligence (SI) is the collective behavior of decentralized, self-organized systems, natural or artificial. Systems consist typically of a population of simple agents or boids interacting locally with one another and with their environment. The inspiration often comes from nature, especially biological systems. The agents follow very simple rules, and although there is no centralized control structure dictating how individual agents should behave, local, and to a certain degree random, interactions between such agents lead to the emergence of "intelligent" global behavior, unknown to the individual agents. Examples in natural systems of SI include ant colonies, bird flocking, animal herding, bacterial growth, fish schooling and microbial intelligence.

1. INTRODUCTION

Biometrics refers to the identification of persons by their individuality or behavior. Biometrics is mainly used in various fields as an outline of recognition and access control. Also it is used to identify each person in groups that are under observation. Biometric identifiers are exclusive, significant characteristics used to tag and illustrate individuals. Biometric identifiers are frequently sort as physiological against behavioral characteristics. Physiological biometric would recognize by one's voice, DNA, hand print or behavior and the behavioral biometrics are typing rhythm, walk, voice etc. Researchers have introduced the word called behavior metrics to explain the other class of biometrics. Further conventional approaches of access control comprise of token-based identification systems, such as a driver's license, passport, voter id and knowledge-based identification system such as a password or personal identification number etc. Even though biometric identifiers are distinctive to each person, they are consistent in verifying identity than the other methods. Hence, the collection of biometric identifiers raises privacy concerns about the vital use of this information.

2. ORIGIN OF THE RESEARCH PROBLEM

Conventional security and authentication systems have been developed largely by various researchers. The Conventional authentication system simply needs the user to give the authorized account and password to log into the system once they start to use a computer or a terminal. Though, under this authentication support, the machine can only be familiar with the user's identity from the login information. It does not have the data to identify who is using it. Disadvantage of the one-time authentication system is that if a person use the system in daily life, when the user leaves the place for a break like to get some documents or have a drink, that time anybody can steal up to the computer and pretend to be the authorized user to access their data, or do anything under a fake identity.

Afterward if the system is on, no one will know who used the computer. This type of security fault is not tolerable in some applications with the sensitive data, for instance, the banking financial record, the military industry and the business confidentiality.

Interdisciplinary relevance

This study can be conducted with the interdisciplinary manner with the following departments of computer science, government, Forensic applications etc.

Significance of the study

Security and Authentication by means of biometrics has become an active area of research in the present decade. A biometric device that determines fingerprints, voice, irises and facial images are offered. All biometric devices need initial registration of the user's attribute that are calculated by the sensors of the biometric device. These devices necessitate training, are time consuming, can be hard to use, can require extra equipment, can be expensive and are so inconvenient that user identity authentication is done only upon initial use.

A multi-sensor biometric system would have many of one type of sensor. The problem with this type of system is that if there is a general environmental factor that causes problems in one sensor, most likely all of the sensors will have the same problem.

For example, poor lighting will reduce the efficacy of a multi-camera facial recognition system. A multi-modal sensor system would use several different modes of sensing biometric data. For example, sensing temperature, pulse rate & eye tracking, would be multimodal and less impacted by a single environmental problem. Continuous Authentication is essential in online examinations where the user has to be continuously verified during the entire session.

It can be used in many real time applications, when accessing a secure file or during the online banking transactions where there is need of highly secure continuous verification of the user. A number of biometric characteristics exist and are used in various applications.

Each biometric has its own strengths and weaknesses, and the choice depends on the application. To avoid this disadvantage under the conventional authentication system, the user can only log off from the terminal or lock up the screen manually before leaving, and log in again when coming back to continue the work. This causes an inconvenience to the user, especially when the user is busily coming and going, and doing other things. Sometimes, the user may skip the log-off process just to keep away from the annoyance caused by repeating the log-off and re-login processes. Hence, the leak of the information security appears. Nevertheless, these situations will not happen in a passive Continuous Authentication (CA) system.

Responding to the need of heightened security applications, different CA systems have been proposed in the past five years.

This study is an urgent need to explore the impact and issues related to the security issues influences during continuous authentication.

3. OBJECTIVES

- To improve the continuous authentication process during online process of various real time application.
- To authenticate and memorize both the user's hard and soft biometric information, and continuously authenticating whether the person using the terminal is as the same valid user as the one login at the beginning.
- To improve Continuous user authentication without requiring active interaction through the use of behavioral biometric modalities.
- To provide an understanding of the different behavioral biometric modalities for continuous authentication.
- To implement a cost-effective and efficient continuous authentication system to substantially reduce the risk of fraud.
- To examine on resistance against spoofing

4. EFFICIENT PASSIVE CONTINUOUSAUTHENTICATION USING PSO WITH ABC

A new method called passive continuous authentication (CA) system is introduced is based on biometrics. The biometrics is of two types they are soft biometrics and the hard biometrics. The facial features of the humans are used as hard biometric information for the verification process and the color of the users clothes are with soft biometric information. For verifying the system continuously without interrupt the user the passive CA system is used. Also that it gives the capability for the machine to identify who is in front of the terminal, reduces the potential security leaks, and deny access to the attacker with the stolen account and password. In this system, the face recognition core is applied to not only by the Eigen face method, but also it is supported by the improved swarm intelligence techniques. By this proposed algorithm the weighting mask is trained for assisting the face recognition process. Artificial Bee Colony (ABC) optimization algorithm

5. EXPERIMENTAL RESULTS

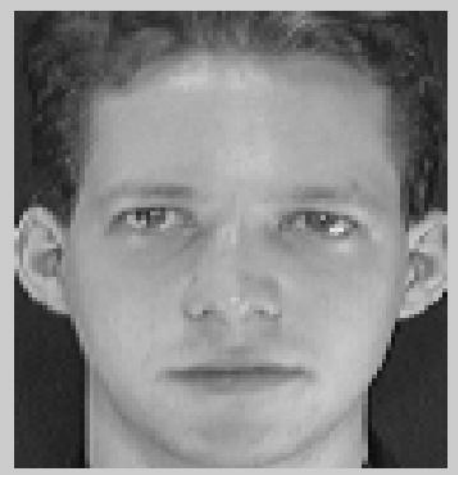


Figure 1: Input image

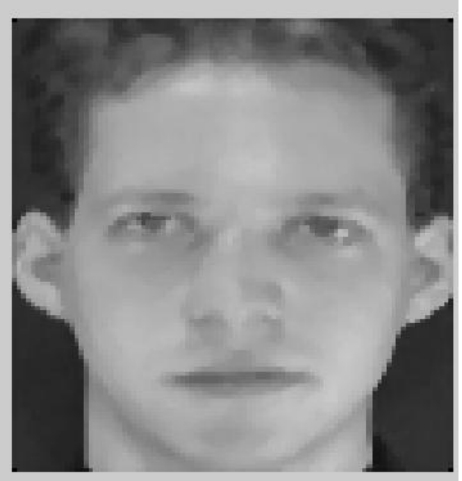


Figure 2: Preprocessing image

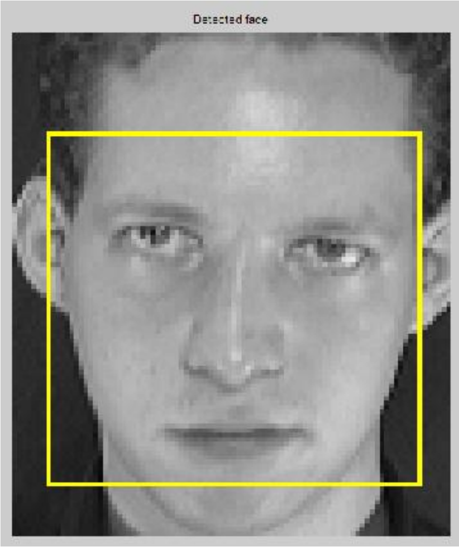


Figure 3: Face detection

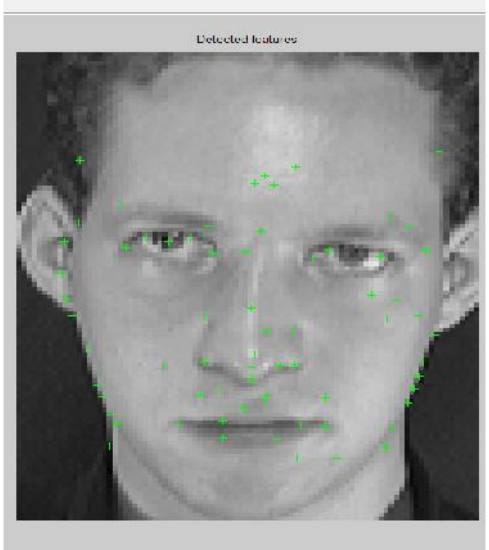


Figure 4: Facial feature selection

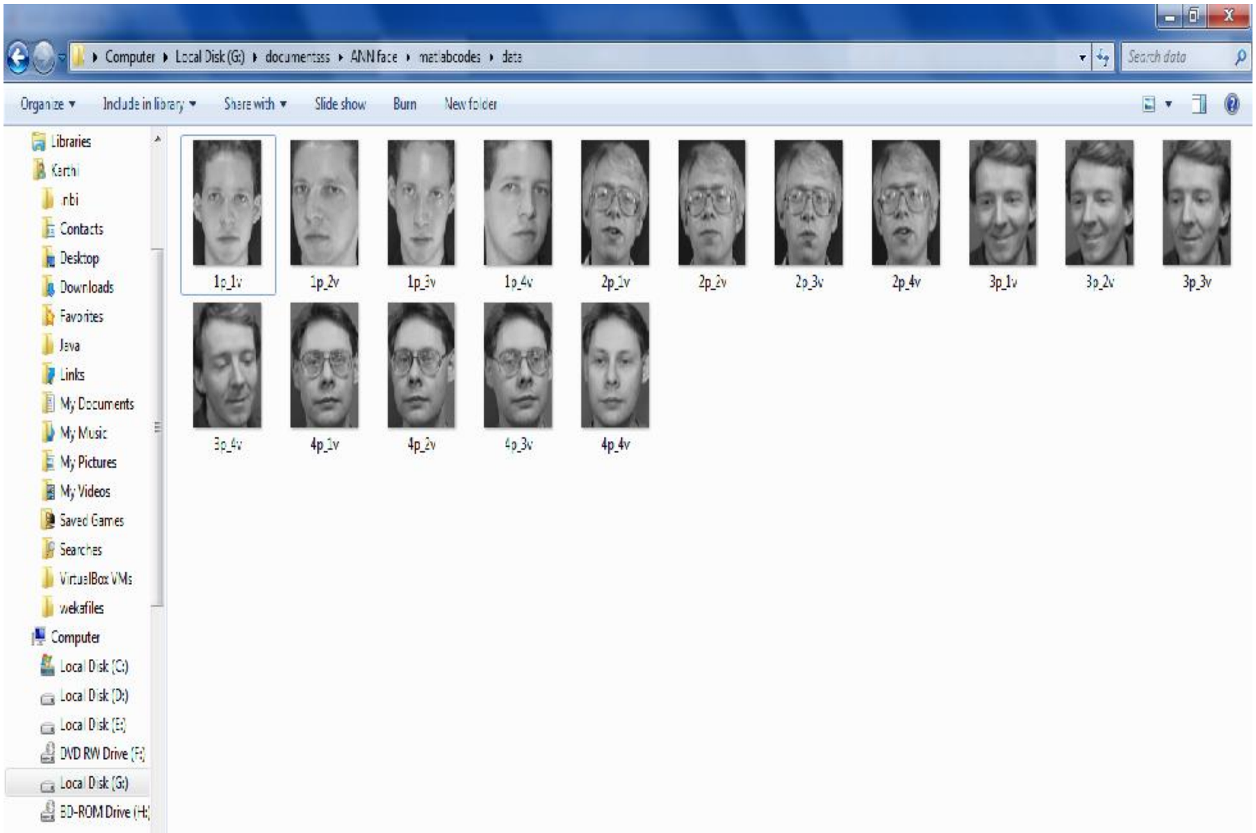
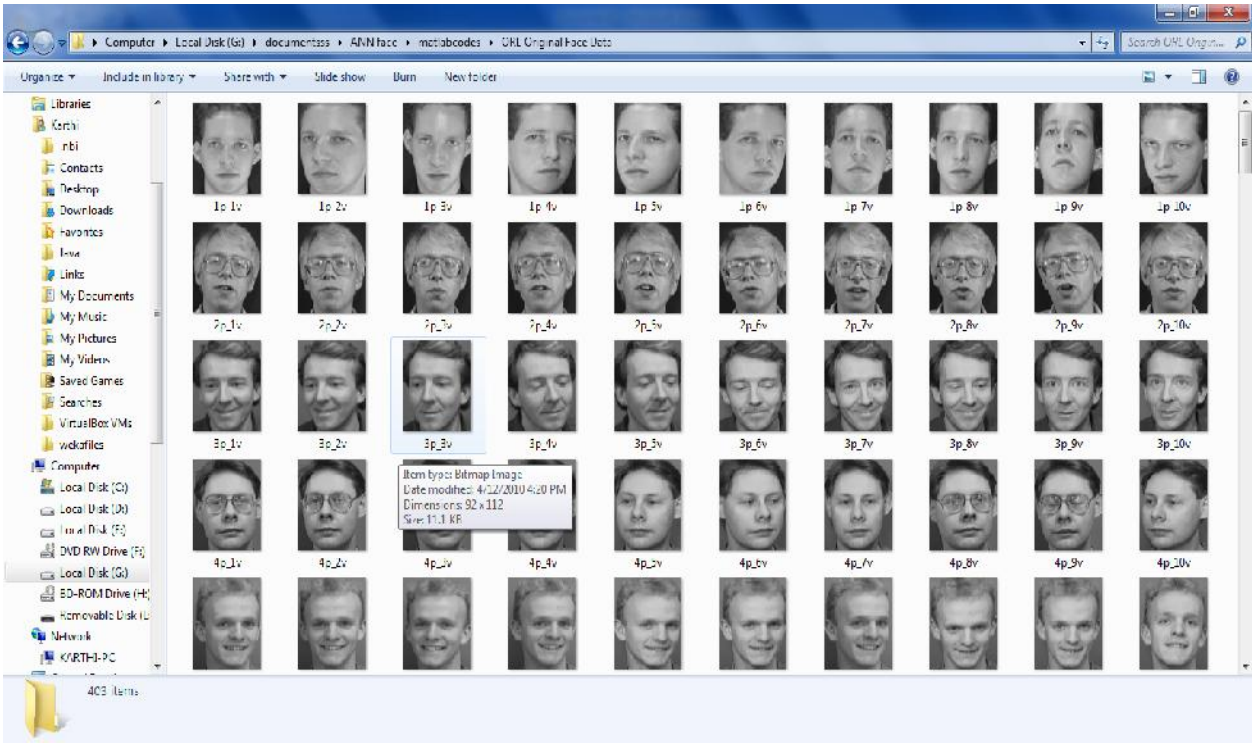


Figure 5: Training data base



Item type: Bitmap Image
Date modified: 4/12/2010 4:20 PM
Dimensions: 92 x 112
Size: 11.1 KB

Figure 6: Test images

S.NO	**Algorithm**	**Feature selection points**
1	pso	980
2	aco	900
3	E(pso+aco)	820

TABLE 1: Feature selection comparison for yaleb data base

S.NO	**Algorithm**	**Time period**
1	pso	230(sec)
2	aco	200(sec)
3	E(pso+aco)	166 (sec)

TABLE 2: Training time: for yaleb data base

S.NO	**Algorithm**	**Feature selection points**
1	pso	1000
2	aco	970
3	E(pso+aco)	900

TABLE 3: Feature selection comparison for ORL data base

S.NO	**Algorithm**	**Time period**
1	pso	330(sec)
2	aco	300(sec)
3	E(pso+aco)	230 (sec)

TABLE 4: Training time: for Orl data base

S.NO	Algorithm	Recognition rate
1	pso	89.4
2	aco	93.4
3	E(pso+aco)	96.4

TABLE 5: Recognition rate: yaleb

S.NO	Algorithm	Recognition rate
1	pso	87.3
2	aco	92.5
3	E(pso+aco)	97.2

TABLE 6: Orl data base

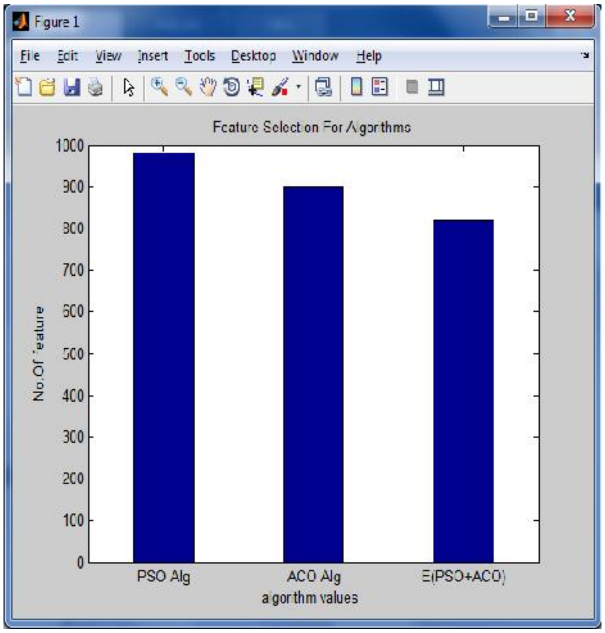


Figure 7: Yaleb data base

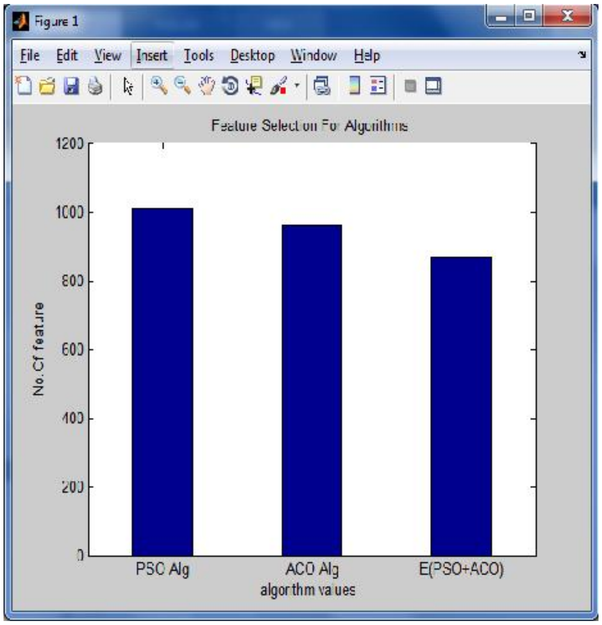


Figure 8: ORl data base

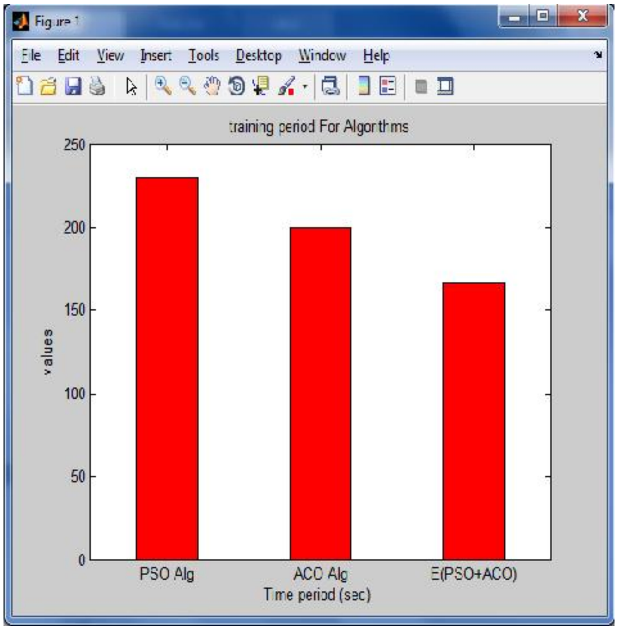


Figure 9: Yaleb data training time period

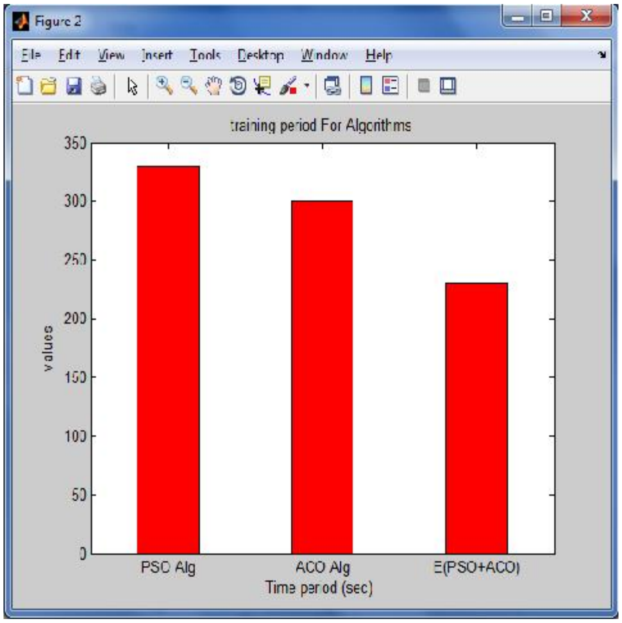


Figure 10: ORL data set

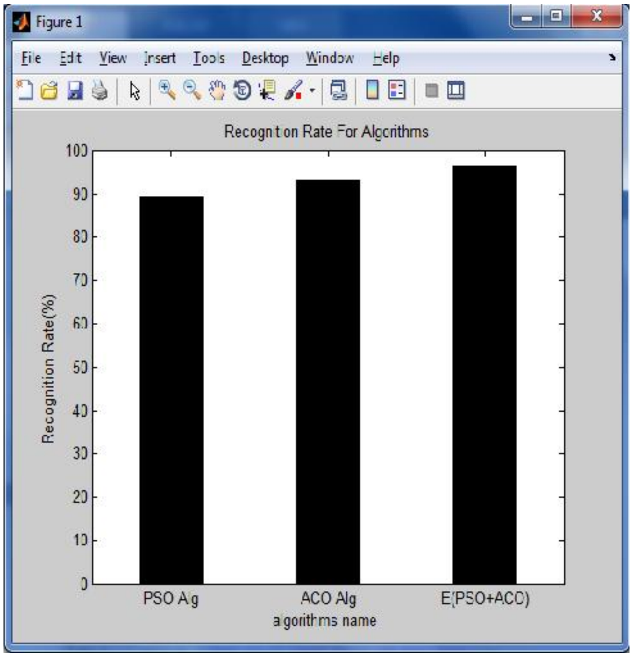


Figure 11: Recognition rate

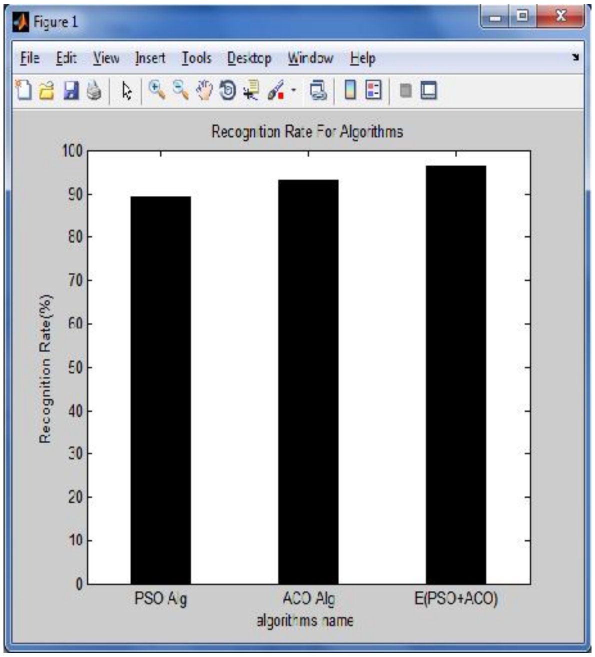


Figure 12: OR data base

CONCLUSIONS

The Experimental result demonstrates the ceaseless authentication process amid online procedure of different ongoing application. The Experimental result validate and retain both the client's hard and delicate biometric data, and consistently confirming whether the individual utilizing the terminal is as the same substantial client as the one login toward the starting and enhance Continuous client authentication without requiring dynamic connection using behavioral biometric modalities. The study gives a comprehension of the diverse behavioral biometric modalities for nonstop authentication. To execute a savvy and proficient constant authentication framework to significantly decrease the danger of extortion. To look at on resistance against ridiculing.

REFERENCES

[1] Hong L, Jain A .& Pankanti S., Can Multibiometrics Improve performance, Proceedings of AutoID 99, pp. 59-64, 1999.

[2] Ross A.& Jain A.K , Information Fusion in Biometrics, Pattern Recognition Letters, 24 (13), pp. 2115-2125, 2003.

[3] Ross.A. A, Nandakumar.K, Jain.A.K. Handbook of Multibiometrics. Springer-Verlag, 2006.

[4] J. Fierrez-Aguilar, Ortega-Garcia J.,Garcia-Romero D., and Gonzalez Rodriguez J, —A comparative evaluation of fusion strategies for multimodal biometric verification,‖in Proc. 4th Int , Conf, Audio-video-based Biometric PersonAuthentication , J. Kittler and M. Nixon, Eds., 2003 vol. LNCS 2688, pp. 830–837

[5] Hong L. and Jain A. K , —Integrating faces and fingerprints for personal identification,‖ IEEE Trans. Pattern Anal. Mach. Intell. , vol. 20, no. 12, pp. 1295– 1307, Dec. 1998

[6] Kumar A. , Wong, Shen1 H. C. , and Jain A. K, — Personal verification using palmprint and hand geometry biometric, ‖in Proc. 4th Int. Conf. Audio- Video-Based Biometric Person Authentication , J. Kittler and M Nixon, Eds., 2003 vol. LNCS 2688, pp 668–678

[7] Frischholz R. and Dieckmann U., —BiolD: A multimodal biometric identification system,‖ Computer, vol. 33,no. 2, pp.64-68,Feb,2000

[8] Chandran GC, Rajesh RS (2009). Performance Analysis of Multimodal Biometric System Authentication, Int. J. Comput. Sci. Network Security, 9: 3.

[9] Toh K. A , Jiang X.D, and Yau W. Y, Exploiting global and local decisions for multi-modal biometrics verification,‖ IEEE Trans. Signal Process. , vol. 52, no. 10, pp. 3059–3072, Oct. 2004

[10] Poinsot A, Yang F, Paindavoine M (2009). Small Sample Biometric Recognition Based on Palmprint and Face Fusion, Fourth International Multi-Conference on Computing in the Global Information Technology.

[11] Shahin MK, Badawi AM, Rasmy ME (2008). A Multimodal Hand Vein,Hand Geometry and Fingerprint Prototype Design for High Security Biometrics, CIBEC'08.

[12] A. Zramdini, "Study of optical font recognition based on global typographical features", PhD thesis, University of Fribourg, 1995.

[13] H. Nezam, S. Nezam Abadipour, and V. Saryazdi and Ebrahimi, "Font recognition based on Gabor filters" (in Farsi), in 9th Iranian Computer Conference , pp. 371-378, 2003.

[14] E. Rashedi, H. Nezamabadi-pour, and S. Saryzadi, "Farsi font recognition using correlation coefficients" (in Farsi), in 4th Conf. on Machine Vision and Image Processing , (2007): Iran.

[15] A. Borji and M. Hamidi, "Support vector machine for Persian font

recognition", International Journal of Computer Systems Science and Engineering , Vol.2 (3), 2007.

[16] H. Khosravi and E. Kabir, "Farsi font recognition based on Sobel-Roberts features", Pattern Recognition Letters, Vol.31, p. 75-82, 2010

[17] J. Yang and V. Honavar, "Feature subset selection using a enetic algorithm", IEEE Intelligent Systems and their Applications, Vol.13, p. 44-49, 1998.

[18] X. Wang, et al., "Feature selection based on rough sets and particle swarm optimization", Pattern Recognition Letters, Vol.28, pp. 459-471, 2007.

[19] M. Dorigo, "Optimization, learning and natural algorithms", in Dipartimento di Elettronica, Ph.D. dissertation, Politecnico di Milano: Italy, 1992

[20] M. Dorigo and T. Sttzle, "Ant colony optimization", MIT press, 2004.