A Highly Secure Authentication Scheme Using Text and Integrated Biometrics Technique

Ephin M

Lecturer

Abstract – Biometrics is the measurement of physical characteristics such as fingerprints, palm print, retina, iris, face etcetera. Integrated biometric mechanism is meant for combining more than one biometric mechanism for example fingerprint and palm print, for better authentication. Existing single modal biometric system has more error rate and provides less security than the combined one[1][2]. Single modal finger print authentication fails in situations like usage of fake finger print, presence of scars in the finger print etcetera[3]. This paper presents a highly secure authentication scheme using text and combined biometrics technique which can increase the security of the system and offers better authentication whereas the error rate is less. Moreover it enables the user to select the level of authentication for various applications considering different factors in view of user behavior and threat[4]. Further, the combination of text and multimodal biometric system achieves significantly better performance than either of the individual schemes.

Keywords - Biometrics, Authentication, Security, Fingerprint, Palm print.

1. INTRODUCTION

Authentication is the first step of security requirement for accessing the resources of any kind of application in the real world. Traditionally password and user id is used for authentication. Now a day's biometric mechanism is becoming more and more popular for identification and verification all over the world[4][5]. Since biometrics are unique, measurable, difficult to forge and cannot be stolen or forgotten, Biometric system offers a precise, irreplaceable, appropriate and high secure alternative to identify individuals. Biometric identifiers are based upon physiological and behavioral characteristics. Physical characteristics contain fingerprints, retinas, irises, facial patterns and hand measurements whereas behavioral characteristics comprise signature, gait and typing patterns.

As biometric systems are distinctive to individuals, they are more consistent in authenticating individuality than token and knowledge-based identification methods. Biometric data cannot be replaced by passwords or keys as it is personal privacy information which is individually and permanently related with a person. However, biometric systems offer privacy protection which has become the concern of public.

2. EVALUATION OF BIOMETRIC METHODS

A brief appraisal on different biometric methods is done based on universality, distinctiveness, permanence, acceptability, accuracy and performance[6][7][8][9]. Universality is meant for every person using a system should possess the peculiarity. Permanence relates the manner in which trait changes over time. Acceptability checks whether the system is user friendly and ease to access. Performance indicates completion of a given task measured against preset known standards of accuracy, completeness, cost, speed etc. It is based on Equal Error Rate (EER), False Accept Rate (FAR) and False Reject Rate (FRR).

False Accept Rate: The prospect that the system imperfectly ties the input pattern to a non-matching pattern in the database. It processes the per cent of unacceptable inputs which are falsely assumed. False Reject Rate: the prospect that the system flops to identify a match between the input pattern and a matching pattern in the database. It processes the per cent of effective inputs which are falsely excluded. Equal Error Rate: the proportion at which both consent and discard errors are alike. Table 1 shows the evaluation of Biometric methods.

Table-1: Evaluation of Biometric Methods

Biometric methods	Uty	Dts	P	A	Pr	Acc	EER
Fingerprint	M	H	H	M	H	M	2%
Face	H	L	M	L	H	M	12.70%
Iris	H	H	H	L	H	H	0.01%
Palm Print	M	H	H	M	H	M	1%
Heartbeat	H	H	L	L	M	L	13.66%

Where Uty = Universality, Dts = Distinctiveness, P = Permanence, A = Acceptability, Pr = Performance, Acc = Accuracy, H = High, M = Medium, L = low

3. THE PROPOPSED SYSTEM

Factors to Improve Biometric Authentication

This section points out various factors to be considered while implementing biometric authentication system. They

are (i) Sensitivity of Data: Any data can be either classified as sensitive or non-sensitive data or semi-sensitive data. Sensitivity demands of users vary not only from Data to Data but also from application to application. For instance, loss of password for accessing bank account is more dangerous than loss of e-mail password. (ii) Complexity Acceptance Level: Not many users can tolerate the increase in complexity, anything would be a success if it is user friendly. (iii) Ability to Wait: Waiting time against robust security is a key factor to study, because adding complex security methods to improve the robustness depends on the answer to the question. How long the customers can wait to get access to that application? (iv) Affordability: This is another area where the user behavior can be studied by asking a question. How much a user affords to spend on authentication equipment's or software? (v) Priority: This is very intuitive than other parameters, because how a user priorities a system is necessary.

Evaluation of Levels and Block diagram of Integrated Biometric Scheme

Integrated Biometric is meant for combination of more than one biometric mechanism for better authentication. The proposed scheme considers finger print and palm print along with traditional password. Finger print and palm print mechanisms are more practical to use rather than the other biometric mechanisms [11][12]. Moreover it has less error rate and integration of these two mechanism offer better authentication and high security. If the password is lost, we can easily generate a new one. But the stolen biometric template will have more impact as it is unique and it cannot be replaced. So there must be efficient way to protect the biometric template. Considering all these factors and behavior of user and threats, three levels have been evaluated for our proposed authentication scheme. Table 2 shows how three levels are evaluated for our proposed authentication scheme

Table-2: Levels of Proposed Scheme

Level	AC	Degree
LLA/TBA	PW	0
MLA/TIA	FP	1
HLA/TAIIA	FP, PP	2

Where AC = Authentication Channel, LLA = Low Level Authentication, TBA = Text Based Authentication, MLA = Medium Level Authentication, TIA = Text Image Authentication, HLA = High Level Authentication, TAIIA = Text and Integrated Image Authentication, Pwd = Password, FP = Finger Print, PP = Palm Print.

Password is used for entry level authentication and the level is termed as LLA (Low Level Authentication). The degree of this level is defined as "0". Here degree denotes the number of biometric mechanism used in the level for authentication. For low level application the user is authenticated using password ie., Text Based Authentication(TBA). The next one is MLA (Medium Level Authentication) and the degree of this level is defined as "1" as there is only one biometric mechanism is considered along with user id ie., Text Image Authentication(TIA).

And the last one is HLA(High Level Authentication) and the degree of this level is defined as "2" as there are two biometric mechanism used along with user id ie., Text and Integrated Image Authentication(TAIIA). LLA is for common resources like ordinary web sites. HLA is for highly confidential resources like bank account is also considered. Block diagram of the proposed highly secure authentication scheme is depicted in Fig.1. Table 3 shows LLA, MLA and HLA authentication procedures.

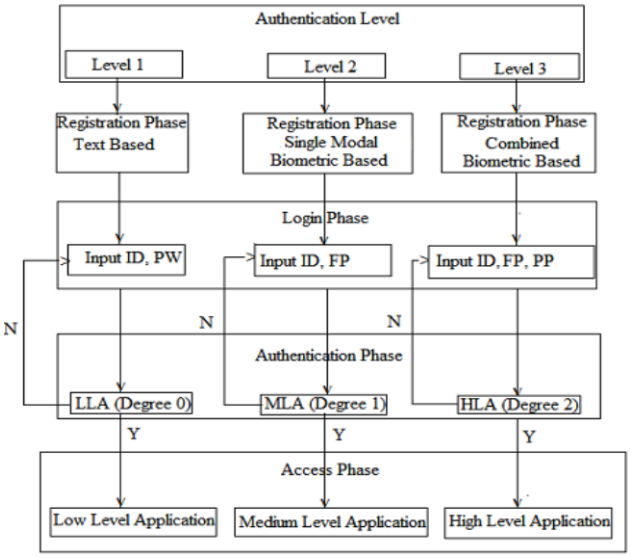

Fig.1. Text and Integrated Biometric Authentication.

Table-3: Authentication Procedures at Three Levels

LLA	MLA	HLA
1. Input the ID and Password.	1. Input the ID and Fingerprint.	1. Input the ID, Fingerprint and Palmrprint.
2. Encrypt the Password.	2. Encrypt Fingerprint.	2. Enhancement of Finger print & Palmprint.
3. XOR previous output with Random Number.	3. XOR previous output with Random Numer.	3. Extract features of Finger print and Palmprint .
4. Encrypt the XOR value.	4. Encrypt the XOR value.	4. Integrate them by fusion.
5. Decrypt it at Verification Phase.	5. Decrypt it at Verification Phase.	5. Store it in Database as template.

6. Decrypt the same from Database.	6. Decrypt the same from Database.	6. Do steps 1 to 4 for verification.
7. Compare the output of step 5 with that of 6.	7. Compare the output of step 5 with that of 6.	7. Retrieve stored template.
8. If matching occurs then Access phase is executed.	8. If matching occurs then Access phase is executed.	8. Compare the output of step 6 with that of 7.
		9. If matching occurs then Access phase is executed.

4. RESULT ANALYSIS

Result analysis of the novel scheme presented in this paper has been done with text, single modal biometric and integrated biometric images. Text is used for "Level 1" authentication. Single modal biometric is used for "Level 2" authentication. And combination of images used for "Level 3" authentication. Table-4: Existing Scheme Error Rate and Security

Scheme	Level	EER	FAR	FRR	Security
FP	NA	2%	2%	2%	M
PP	NA	1%	0%	2%	M

Level 3 is the integrated biometric authentication. Here encryption and decryption is done using the same key. Preprocessing of images using low pass filter, feature extraction by Gabor linear filter[12], Integration of images using wavelet fusions[13] and Image matching is done in the ratio of 1:1 as each user has unique id with biometric[14]. From the results it can be concluded that the proposed authentication scheme provides good performance, high level security and less error rate.

Table-5: Proposed Scheme Error Rate and Security at Different Levels

Level	AC	EER	FAR	FRR	Sec	EU	A
0^{th} Degree	PW	NA	NA	NA	M	H	H
1^{st} Degree	FP	2%	2%	2%	H	H	H
2^{nd} Degree	FP, PP	0.75%	1.50%	1.50%	H	H	H

Where AC = Authentication Channel, Sec = Security, EU = Ease of Use, A = Acceptability

To identify the levels of various applications, pilot study has been conducted on various classes of users and the result is given in Table 6.

Table-6: Various Applications at Three Levels

LLAP	MLAP	HLAP
E-Learning	E-booking	Online Payment
E mail	File Sharing	E-Banking
Website Login	Online Reservation	E-Voting
Online Library	Online Shopping	
CMS		
LMS		

5. CONCLUSION

To overcome the drawbacks of traditional password authentication and single modal biometric authentication, this paper presents a highly secure authentication scheme using text and integrated biometrics technique. The result analysis shows that the proposed authentication scheme based on text and combined biometrics technique offers better authentication and increase the security of the system while maintaining the acceptable efficiency and less error rate. The choice of different levels of authentication enables the one to select the best level authentication suitable and applicable for various applications. It can be used for common resources like ordinary web sites to highly confidential resources like bank account.

REFERENCES

[1] Jain A.K, Ross A, Pankanti, Biometrics: a tool for information security. IEEE Transactions on Information Forensics and Security, Vol 2, Pp. 125-143, June 2006

[2] A.K Jain, P. Flynn and A. Ross, Handbook of Biometrics, Springer, 2007

[3] Krishneswari, K. and S. Arumugam, "Multimodal Biometrics using Feature Fusion", Journal of Computer Science, Pp: 431-435, 2012

[4] Robert Richardson, "Computer Crime and Security Survey," Computer science Institute, 2010/2011

[5] Chun-Ta Li and Min-Shiang Hwang,"An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards," Journal of Network and Computer Applications, Pp.1-5, 2010

[6] Netto, D.B.S. Fornazin, M. Cavenaghi, M.A. Spolon, R. Lobato, R.S. "A practical approach for biometric authentication based on smartcards," 5th Iberian Conference on Information Systems and Technologies (CISTI), Pp. 1, Jun 2010

[7] Khurram, "Fingerprint Biometric-based Self-Authentication and Deniable Authentication Schemes for the Electronic world," IETE, Vol. 26, Pp.191-195, Jun 2009

[8] D. Zhang and W. Shu, "Two novel characteristics in palm print verification: datum point invariance and line feature matching," Pattern Recognition, vol. 32, no. 4, pp. 691-702, Apr. 1999

[9] M. Turk and A. Pentland, "Eigen faces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, Mar. 1991

[10] Palmer, L.R.; "Efficient fingerprint feature extraction: Algorithm and performance evaluation," IEEE Communication Systems Networks and DSP, pp. 581 - 584, 2008

[11] Ito, K.; Morita, A.; Aoki, T.; Higuchi, T.; Nakajima, H.; Kobayashi, K., "A Fingerprint Recognition Algorithm Using Phase-Based Image Matching for Low-Quality Fingerprints," IEEE Transactions on Image Processing, pp. II - 33-6, 14 November 2005

[12] Wais Kin Kong, David Zhang, Wenxin Li, "Palmprint feature extraction using 2-D Gabor Filters", Elsevier Journal of the Pattern Recognition Society, Pp:2339-2347, 2003

[13] R. Gayathri, P. Ramamoorthy, "A Fingerprint and Palmprint Recognition Approach Based on Multiple Feature Extraction", European Journal of Scientific Research, Vol 76, Pp: 514-526, 2012

[14] W. Shu and D. Zhang, "Automated personal identification by palm print," Opt. Eng., vol. 37, no. 8, pp. 2359-2362, Aug. 1998