IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010
ISSN: 1793-8236

3D Signature for Efficient Authentication in Multimodal Biometric Security Systems

P. M. Rubesh Anand, Gaurav Bajpai, and Vidhyacharan Bhaskar

***Abstract*— Unimodal biometric systems rely on a single source of biometric trait information for recognition of individuals. These systems are highly vulnerable to spoof attacks as imposters easily imitate the particular biometric trait of any genuine user. The impact of circumvention is reduced by combining the functions of different unimodal biometric systems to perform as a multi-biometric system. The multimodal biometric systems operate in two or more ways to authenticate individuals by their biometric traits. This paper proposes a multimodal biometric security model for efficient authentication. The model deals with multi-biometrics in first two phases for identification, verification followed by the decision making as third phase. The first phase employs physiological biometric traits for identification by exhibiting the liveliness of individual. The second phase uses 3D handwritten signature for verification of the claiming identity. The 3D handwritten signature records the pressure information on the special signature pad during the signing process. The pressure information recorded on different layers of the signature pad provides distinct information for verification of the individuals based on their signatures. This unique pressure information raises the level of difficulty in the forgery of signatures. The individual matching score is calculated in identification phase and verification phase. The fusion is performed on the obtained matching scores and compared with threshold value in the decision phase to provide efficient authentication of the individual. The threshold value in the decision phase is varied according to particular application for combating the problem of circumvention in biometric security systems. The preliminary results show the viability of using 3D handwritten signature in biometric security.**

***Index Terms*— 3D Signature, Authentication, Multimodal Biometrics, Spoof Attacks.**

I. Introduction

Biometrics refers to the method of recognizing individuals based on their physiological or behavioural traits. The physiological recognition is based on the biological individuality of users, like, fingerprint, face, hand geometry, vein patterns, retina and iris. The behavioural biometric recognition considers voice, handwritten signature [1]. Biometric systems are widely used for authentication, identification, and verification of any individual. Any human physiological and/or behavioural characteristic can be used as a biometric characteristic as long as it satisfies the requirements like universality, distinctiveness, permanence, collectability and acceptability [2]. Human handwritten signature is used as a traditional way of authentication in banking, business transactions, acknowledgment of goods/services received due to its acceptance in legal and social levels. The static (off-line) and dynamic (real-time) signature verification for the paper-based document is done by humans. The challenges faced in that verification are: any signature can be learnt; it can be changed by the owner and has several versions of the signature depending on the level of importance or intent of the signer [3]. The unimodal 2D signature verification systems are vulnerable to spoof [4], [5].

Most of the commercially available biometric recognition systems work with single biometric identifier. These unimodal biometric systems use any one of the physiological or behavioural biometric identifiers. Unimodal systems contend with a variety of problems such as noise in sensed data, intra-class variations, inter-class similarities, non-universality and spoof attacks [6]. The noise, intra-class variations, non-universality is overcome by selecting a high quality sensor with appropriate biometric trait, whereas, the inter-class similarities, spoof attacks pose the danger for the system being compromised. The circumvention in unimodal biometric recognition systems exhibit the ways of deceiving the system by fraudulent methods are of main concern in security and privacy. The well trained imposters perform high attempt to forge a particular biometric trait in the unimodal biometric systems. Improving the method of analysis and tightening the threshold for recognition reduces the issue of circumvention but instead, they will increase the false rejection rate and failure to enroll rate. The appropriate solution for this problem is to use multi-biometric traits working in serial with suitable fusion method to decide upon the credentials of the individual under question. The multimodal biometric system is also forged by expert forgers but fusion of matching scores decides the result.

This paper proposes a multimodal biometric security model for efficient authentication against expert forgers. The model deals with three phases for identification, verification and decision. The first phase employs physiological biometric traits for identification, second phase uses 3D handwritten signature for verification, the third phase decides from the fusion of the obtained matching scores compared with the threshold value. The application of this model is to use in access control, contract/agreement execution, banking services, financial transactions, and acknowledgment of goods/services received.

Manuscript received September 9, 2009.

P. M. Rubesh Anand is a Ph.D. research scholar in the Department of Electronics and Communication Engineering, SRM University, Kattankulathur – 603203, Tamil Nadu, India. (Phone: +91-44-27454646; fax: +91-44-2745 2343; e-mail: rubesh.anand@gmail.com).

Gaurav Bajpai is with the Department of Computer Engineering and Information Technology, Faculty of Engineering, Kigali Institute of Science and Technology, B.P.3900, Kigali, Rwanda. (e-mail: gb.bajpai@gmail.com).

Vidhyacharan Bhaskar is with the Department of Electronics and Communication Engineering, SRM University, Kattankulathur – 603203, Tamil Nadu, India. (e-mail: vcharan@gmail.com).

Further, this paper is organised into six sections. Following an introduction to unimodal biometric system in section I, section II covers the introduction to multimodal biometrics, section III describes the proposed authentication model, section IV explains the 3D signature analysis, section V shows the results and discussions, and section VI presents the conclusion.

II. Multimodal Biometrics

Multimodal biometric systems use more than one physiological and/or behavioural biometric trait for recognition of individuals. The physiological biometric authentication methods like fingerprint, iris, voice, face recognition can be spoofed by a duplicate or when the person is in an unconscious state of mind. The behavioural biometric authentication like voice, handwritten signature possess strong barrier for such spoofing even when the individual is in medicated state due to the need for memory [7]. The balance between "no need for memory" and "need for memory" is obtained by considering one biometric trait from each of physiological and behavioural biometric traits. The proposed model considers one biometric trait from physiological for identification (finger print, face recognition, iris recognition) and one from behavioural for verification (3D handwritten signature). The biometric identifiers considered individually have exhibited some drawbacks [2] whereas fusion exhibit some merits as shown in Table I.

TABLE I Comparison of Unimodal and Multimodal Biometric Identifiers Based on the Perception of the Authors - High, Medium and Low are Denoted by H, M, and L, Respectively

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Iris	H	H	H	M	H	L	L
3D Handwritten Signature	L	M	L	H	M	H	L
Fusion (Fingerprint + 3D Handwritten Signature)	M	H	M	H	H	H	L
Fusion (Face + 3D Handwritten Signature)	M	M	M	H	M	H	M
Fusion (Iris + 3D Handwritten Signature)	M	H	M	H	H	M	L

A. Fingerprint

Human fingerprints are unique to each person and even the fingerprints of twins are not exactly the same [8]. Fingerprint is the pattern of ridges that make loops, arches or whorls. In each fingerprint, there are regions where changes in ridge are noticed, like, a ridge ends, splits into two ridges, join another ridge or create an island; these features are called minutia [9]. It is these features that are extracted and compared for determining a match. The comparison of two fingerprints is performed through feature-based/minutia-based matching methods [10]. Different fingerprint matching algorithms use different types of information extracted from the input fingerprints for matching. Automatic identification methods based on fingerprint provide positive identification with a very high accuracy [11], [12].

B. Face Recognition

Face recognition measures, analyzes the overall structure, shape and proportions of the face. The features extracted from the face images are used in comparison with face database for identification [13]. The commonly used features are distances between individual organs (like eye, nose, mouth) located on a face, length of the organs, area, angle made between two organs. Automated face recognition system is capable of capturing face images from a distance using camera, extract features and compare with database for recognizing individuals [14], [15].

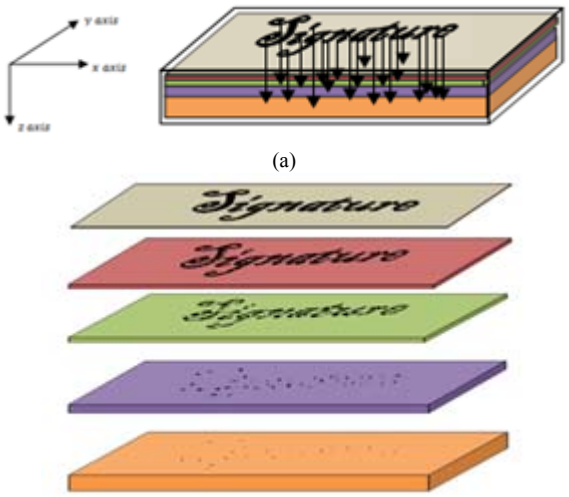
C. Iris Recognition

The iris is the annular region of the eye bounded by the pupil and the sclera on either side. The complex iris texture carries very distinctive information different for every individual [2]. Iris recognition is the process of recognizing the random pattern of the iris. It has higher consistency and uniqueness compared to fingerprint or face [16]. Automated algorithm for iris recognition is available which works by locating iris using landmark features. The landmark features and the distinct shape of the iris allow for imaging, feature extraction and identification [17].

D. 3D Handwritten Signature

Handwritten signatures are usually recognized in 2D. The writing pad with dedicated pen for 2D handwriting is commercially available for email signing and handwriting recognition [18], [19]. The handwritten signatures in 2D are easily forged, thus their impact in biometric security is quite low.

The features that are considered usually in signature verification are velocity, acceleration, pressure, direction, pen ups/downs, total time taken, and length of the signature. The handwritten signature considered with z-axis pressure information is termed as 3D signature. Every handwritten signature considered in 3D has a distinct feature of pressure applied on the signature pad. This pressure information in 3D makes the imposters difficult to forge the signature of the genuine user. A special signature pad of non-linearly spaced layers is considered for recording the signature with 3D pressure feature [20]. The z-axis pressure variation is measured by non-linearly spaced layers of the signature pad as in Fig. 1(a). The non-linearity is considered in the model for the reason of capturing the minute pressure variations in z-axis which normally remains with the upper layers. The lower layers are widely spaced to record the details of the heavy pressure variations during the process of signing as in Fig. 1(b). The hard to forge property of behavioural biometric 3D signature fused with other physiological biometric trait decreases the problem of circumvention.



(a)

(b)

Fig. 1 (a) Special signature pad (b) z-axis pressure variations in the

E. Fusion

Fusion combines multiple sources of information to form a single value for comparison. The fusion can be performed at different levels in the multimodal biometric systems, like, fusion at feature level, match score level or decision level [6], [21]. Feature level fusion is difficult as the features extracted from the multi-biometric traits are of different types [22]. Decision level feature is like majority voting which depends on the winning results from different biometric traits that can be spoofed by imposters. The only viable way for fusion between different features of the various biometric traits is matching score fusion [23].

III. Proposed Model

The proposed authentication model involves three phases, namely, identification phase, verification phase and decision phase. The simple block diagram of the model with direction flow is shown in Fig. 2 and the detailed block diagram of the multimodal biometric authentication model with feedback is shown in Fig. 3.

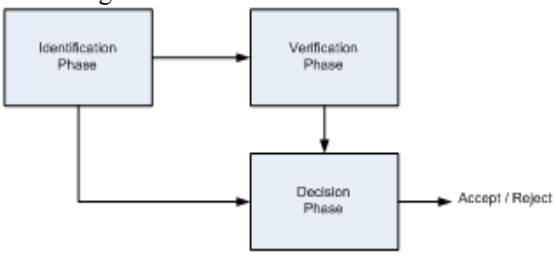


Fig. 2. Simple block diagram of the proposed model.

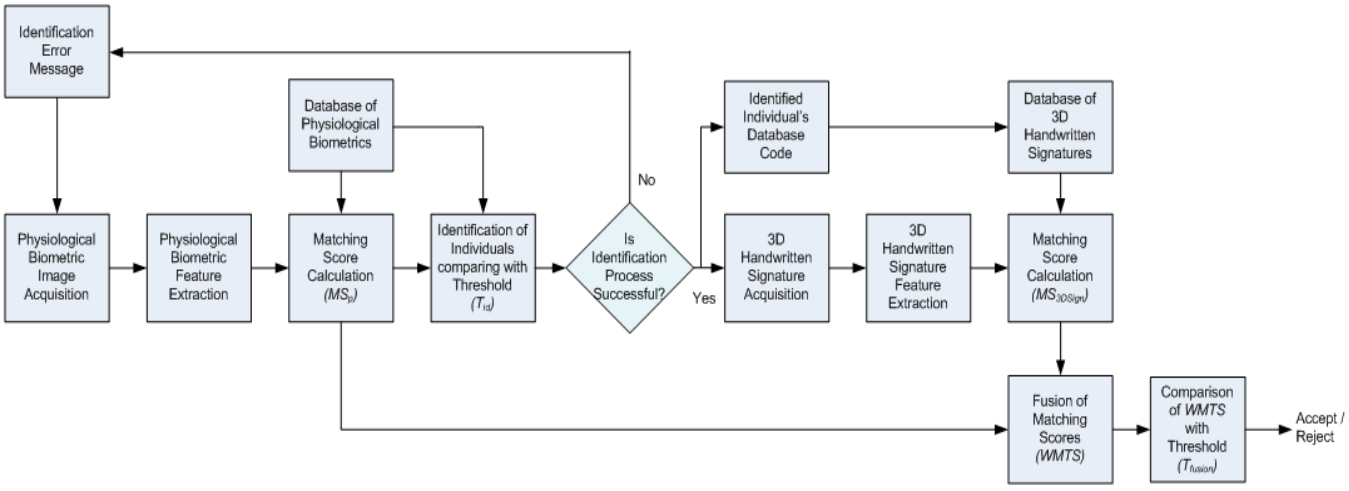


Fig. 3. Block Diagram of the Multimodal Biometric Authentication Model

A. Identification Phase

The physiological biometric traits like, fingerprint, face or iris is used for identifying the individuals. These biometric traits can be used independently or in combined mode depending on the applications for identification. Initially, the physiological biometric image acquisition is made for a clear and perfect image. Then the features are extracted from the obtained image. Once the required features are acquired, the physiological matching score (MS_p) is calculated by comparing the features with the available database as in (1); f_{match} is the number of matched features and f_{total} is the total number of features considered. The calculated matching score is sent for identification and fusion.

$$MS = \frac{f_{match}}{f_{total}}. \quad (1)$$

In the identification process, *1:N* matching is done by comparing the matching score with identification threshold (T_{id}) to identify the individual from *N* individuals in the database. The identification threshold is chosen from the scale depending upon the application. Once the identification process is successful, the identified individual's database code is transferred to the database of the verification phase along with an indication to the next phase to proceed. When the identification process ends in failure without identifying any individual, then an error message is sent along with an indication to repeat the

identification phase.

B. Verification Phase

Once an individual is identified, the credential of the individual is verified through behavioural biometric trait in the verification phase. The behavioural biometric trait considered is 3D handwritten signature. Once the 3D signature is acquired through the special signature pad, dynamic features like, velocity, acceleration, pressure, direction, pen ups/downs, and total time taken are extracted as f_d along with the pressure information from each layer as f_{layer}. The obtained individual features are compared with the identified database of the individual for dynamic feature matching score (MS_d) and layers matching score (MS_{layer}) as in (1). The 3D signature weighted mean matching score (MS_{3DSign}) is calculated by considering the dynamic and layer matching scores with weight factors a and b respectively as in (2).

$$MS_{3DSign} = \frac{\left[a \times \sum_{i=1}^{q} MS_{d_i} \right] + \left[\sum_{j=1}^{r} \left(b_j \times MS_{layer_j} \right) \right]}{\left[a + \sum_{j=1}^{r} b_j \right]}. \quad (2)$$

The number of dynamic features considered is q whose combined matching score is multiplied by a common weight factor a. In the consideration of layer matching scores, the weight factor b for each layer is assigned individually with more weightage to the lower layers as the pressure information is distinct for individuals. The weight factor b gradually increases from the upper layer towards the lower layers with the total number of layers as r. The calculated weighted mean matching score is transferred to the decision phase for fusion and authentication.

C. Decision Phase

The identification phase acts as a user ID, verification phase acts as a password, and decision phase provides the authentication result for the user ID and password like, the general authentication method used in the internet applications. In this model, individuals are safe from attacks as physiological biometric is used along with 3D signature by fusion. The fusion is performed in the matching score level from the identification phase and verification phase matching scores as in (3) for calculating the weighted mean total score (*WMTS*) with α_p, β as the weight factor depending upon the applications,

$$WMTS = \frac{\left[\sum_{p=1}^{n} \alpha_p \times MS_p \right] + \left[\beta \times MS_{3DSign} \right]}{\left[\sum_{p=1}^{n} \alpha_p + \beta \right]}. \quad (3)$$

When more than one physiological biometric trait is considered, then the individual weight factor α_p is assigned for each biometric trait with n being the total number of physiological biometric traits considered. The summation of the weight factor with their respective matching scores gives the total physiological biometric matching score. The 3D handwritten signature matching score is emphasized by the weight age factor β. The calculated weighted mean total score is compared with the preset threshold of fusion (T_{fusion}) for deciding upon the accept/reject condition. The fusion threshold (T_{fusion}) is chosen from scale depending upon the application. The authentication depends on the weight factor and threshold of fusion for efficient result.

IV. 3D Signature Analysis

Samples of 140 handwritten signatures are collected from 140 individuals. Among them, 100 genuine signatures are forged by 20 imposters. Individuals acting as genuine signers are given with five layers of paper to sign on the layer 1 with their usual pressure applied on the paper.

The imposters are then trained and allowed to imitate the genuine signatures with reasonable time limit. From the sample of 100 genuine signers, 25 individuals are selected to repeat their signature at different intervals of time in 10 days period. A sample signature of genuine user compared with imposter in five layers is shown in Fig. 4. The pressure information recorded on each layer shows the distinct variation in the signatures of the genuine user and the imposter.

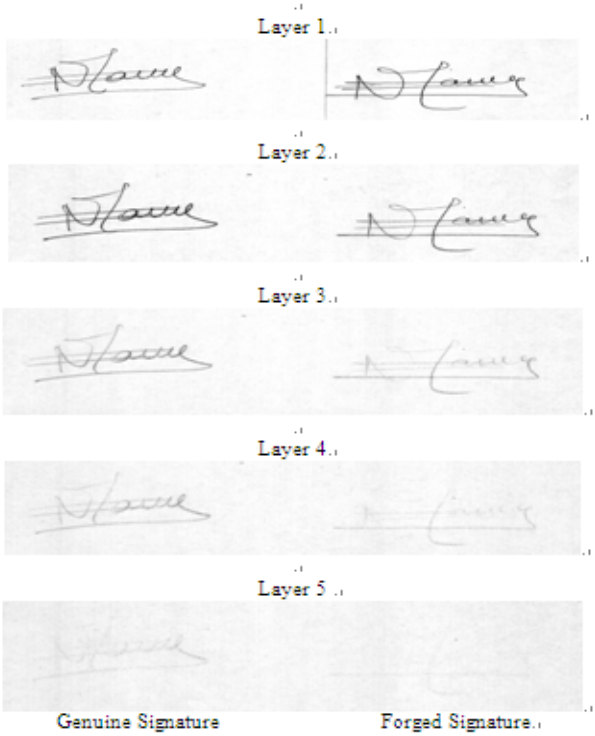


Fig. 4. A sample signature of genuine user compared with imposter shown for each layer

A total number of 25 individuals are selected from the categories of simple signatures, normal signatures, and difficult signatures. The selected 25 individuals are allowed to repeat their signatures at different timings. A sample signature of genuine user compared with his signature for layer 1 and layer 5 at different timings is shown in Fig. 5. The comparison of the signatures of the same individual shows equal impression on layer 5 for different attempts at different timings. A sample signature of genuine user compared with the imposter as shown in Fig. 6 for layers 1 and 5. The signature of genuine user and imposter shows exact matching at layer 1 with less matching at layer 5.

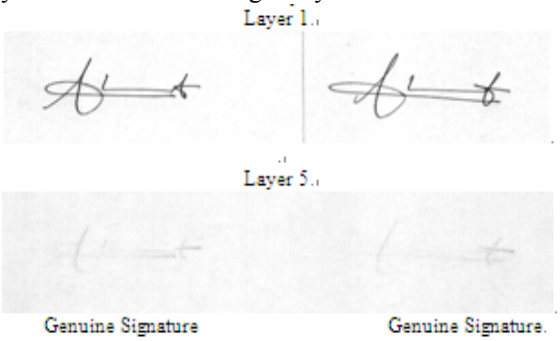
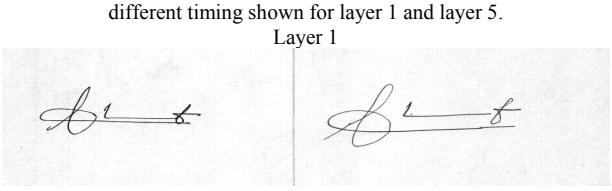


Fig. 5. A sample signature of genuine user compared with his signature at different timing shown for layer 1 and layer 5.



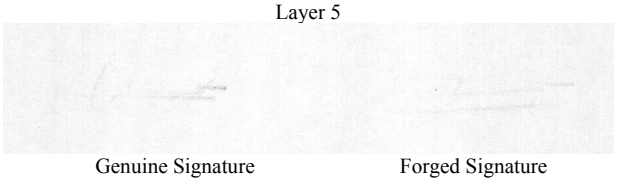


Fig. 6. A sample signature of genuine user compared with imposter shown for layer 1 and layer 5.

V. Results And Discussions

The collected signature samples are verified off-line by three human judges; out of them, two are experienced in signature verification and the third is an amateur signature verifier. The judges are given reasonable time limit to verify the signature and award matching score, varying in the matching scale of 0 to 5, 0 being the point for no matching and 5 being the point for exact matching. Points 1, 2, 3, and 4 denote 20%, 40%, 60% and 80% matching between two signatures under test.

TABLE II Matching Scores from the Mean of Sample Genuine Signatures with Forged Signatures is Given in 0-5 Scale Denoting with 0 Being No matching and 5 Being Exactly Matching

Layers / Judges	Layer 1	Layer 2	Layer 3	Layer 4	Layer 5
Judge 1	3.42	2.80	2.05	0.77	0.01
Judge 2	3.81	3.38	2.51	1.07	0.09
Judge 3	3.40	3.06	2.31	1.06	0.14
Average	**3.54**	**3.08**	**2.29**	**0.97**	**0.08**

The results of the human judgment are shown in Table II. The results show that the expert forger can replicate the genuine signature in the 2D surface easily at upper layers, namely, layer 1 and layer 2. When the hidden information of the pressure is considered for the verification of genuine and forged signatures, it is observed that the expert forgers are unable to replicate the exact pressure that is applied by the genuine user as shown in layer 4 and layer 5 matching scores. The matching scores between the genuine and forged signatures decrease while considering the pressure of the signatures from layer 2 to layer 5. The mean of the matching scores of the three judges for 100 signature samples compared with imposter in layer 1, layer 3, and layer 5 is shown in Fig. 7. Layer 5 matching scores between genuine user and imposter are low due to the different matching points of the signatures recorded. Fig. 8 shows the mean of the matching scores between genuine user and imposter for 25 signature samples showing huge difference in the matching scores between layer 1 and layer 5. The results of signature matching score from the same user compared with his/her own signature has high values even in the lower layers, like, layer 4 and layer 5. The matching score differences between layer 1 and layer 4 are quite low as shown in Fig. 9.

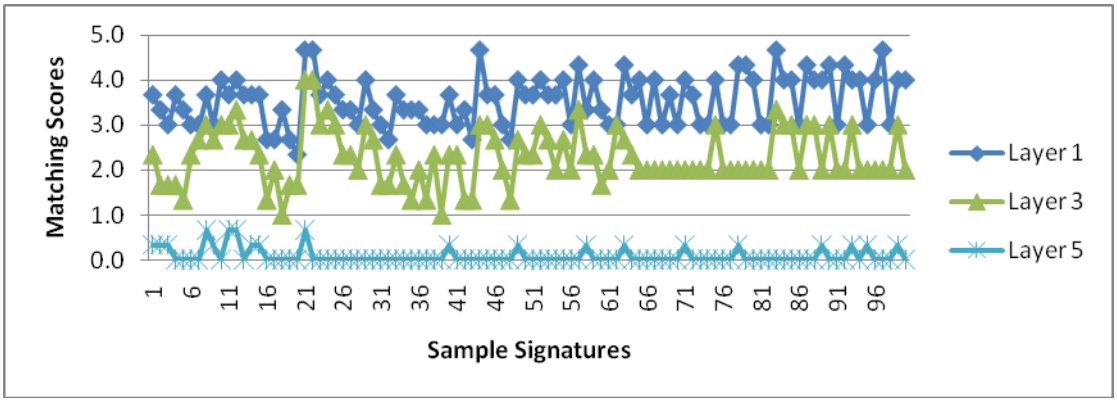


Fig. 7. Matching scores between genuine users and imposters for the sample of 100 signatures given as the mean of the three judges for layer 1, layer 3, and layer 5.

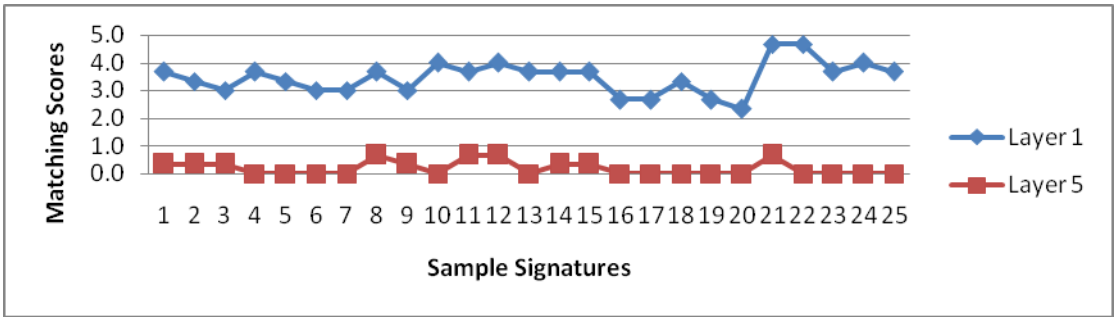


Fig. 8. Matching scores between genuine users and imposters for the selected 25 signature samples given as the mean of the three judges for layer 1 and layer 5.

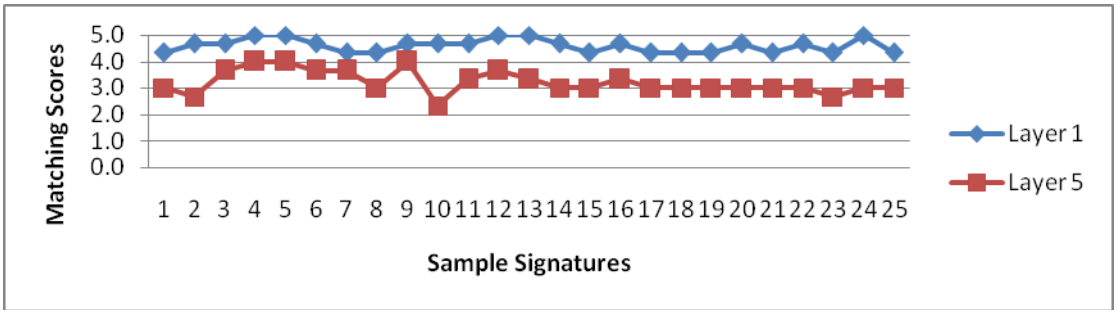


Fig. 9. Matching scores between genuine users with his/her own signature for the selected 25 individuals given as the mean of the three judges for layer 1 and layer 5.

TABLE III CALCULATION OF FAR AND FRR BASED ON THE HUMAN JUDGES' PERCEPTION FOR 3D SIGNATURE

S. No.	Threshold Value (T)	FAR	FRR
1	0.5	4%	0%
2	1	0%	0%
3	1.5	0%	0%
4	2	0%	0%
5	2.5	0%	4%
6	3	0%	12%
7	3.5	0%	72%
8	4	0%	88%

False Acceptance Rate (FAR) denotes the percentage of accepting an imposter as a genuine user. False Rejection Rate (FRR) denotes the percentage of rejecting the genuine user deciding the user as an imposter. The percentages of FAR and FRR solely depends on the threshold value set for a particular application. Table III shows the threshold value (T) set for the 3D signature verification matching points, and its effect on FAR and FRR. The mean value of the three judges are considered to decide upon FAR and FRR. When the threshold value is set at a high value, FAR is fully eliminated and FRR increases, exponentially. FAR increases whereas leaving FRR to 0% for the less threshold value. The increasing values of FRR for high threshold are mainly due to image quality in the layer 4 and layer 5 of the samples. The FAR and FRR values are plotted against the threshold values as shown in Fig. 10. The Equal Error Rate (EER) denotes the lowest point where the values of FAR and FRR are considered to be equal. EER helps in setting the optimum value of the threshold. As per the values obtained, the EER is at the threshold values of 1 to 2. The image quality obtained down to layer 2, namely, layer 3 to layer 5 made some signatures to be difficult for judgment. The automated system with dedicated hardware for 3D signature acquisition can show better results. The calculated values of FAR, FRR, and ERR exhibit an encouraging preliminary results for the deployment of 3D signature verification hardware.

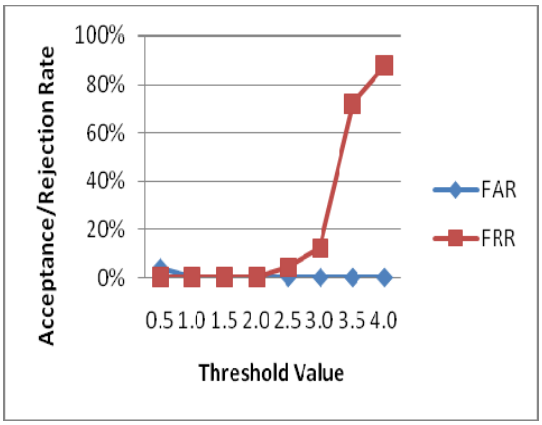


Fig. 10. FAR and FRR corresponding to the threshold values.

VI. Conclusion

Multimodal biometric systems are tolerable for the circumvention than the unimodal biometric systems. The preliminary results reveal that the 3D information of handwritten signature is acting as a distinct hidden factor and shows positive sign for consideration of 3D handwritten signature as a unique biometric identifier. The large set of samples indicates that the expert forgers are unable to imitate the pressure variation of the genuine signer even though the forgers are able to exactly replicate the signature in 2D. The fingerprint forms the superior combination with 3D handwritten signature compared to face recognition and iris recognition as many governmental agencies, like, passport office, immigration, registration office can easily deploy them. The threshold value in the decision phase is decided based on the security level that is needed for any application to overcome the problem of circumvention in biometric security systems. The proposed authentication model increases the security in access control, contract/agreement execution, banking services, financial transactions, and acknowledgment of goods/services received. The apt selection of weight factor and threshold depending upon the application efficiently eliminates the imposters.

References

[1] K. W. Boyer, V. Govindaraju, and N. K. Ratha, Eds., "Introduction to the special issue on recent advances in biometric systems," IEEE Transactions on Systems, Man, and Cybernetics, vol. 37, no. 5, pp. 1091–1095, Oct. 2007.

[2] A. K. Jain, Arun Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004.

[3] S. J. Elliott and A. R. Hunt, "The challenges of forgeries and perception of dynamic signature verification," Proceedings of the 6th International Conference on Recent Advances in Soft Computing (RASC 2006), pp. 455-459, 2006.

[4] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," Pattern Recognition, vol. 35, no. 12, pp. 2963–2972, 2002.

[5] L. Lee, T. Berger, and E. Aviczer, "Reliable on-line human signature verification systems," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, no. 6, pp. 643–647, June 1996.

[6] A. Ross and A.K. Jain, "Multimodal Biometrics: An Overview," Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, Sep. 2004.

[7] M. Kam, K. Gummadidala, and R. Conn, "Signature authentication by forensic document examiners," Journal of Forensic Science, vol. 46, 2001.

[8] A. K. Jain, S. Prabhakar, and S. Pankanti, "On the Similarity of Identical Twin Fingerprints," Pattern Recognition, vol. 35, no. 11, pp. 2653-2663, 2002.

[9] Alfred C. Weaver, "Biometric Authentication," Computer, vol. 39, no. 2, pp. 96-97, Feb. 2006.

[10] A. K. Jain, S. Prabhakar, and S. Chen, "Combining Multiple Matchers for a High Security Fingerprint Verification System," Pattern Recognition Letters, vol. 20, no. 11-13, pp. 1371-1379, 1999.

[11] A. Ross, A. K. Jain, and J. Reisman, "A Hybrid Fingerprint Matcher," Pattern Recognition, vol. 36, no. 7, pp. 1661-1673, 2003.

[12] A. K. Jain, Y. Chen, and M. Demirkus, "Pores and Ridges: High Resolution Fingerprint Matching Using Level 3 Features," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 1, pp. 15-27, Jan. 2007.

[13] R.-L. Hsu, Mohamed Abdel-Mottaleb, and A. K. Jain, "Face Detection in Color Images," IEEE Transactions on PAMI, vol. 24, no.5, pp. 696-706, May 2002.

[14] R.-L. Hsu and A. K. Jain, "Semantic face matching," Proc. IEEE Int'l Conf. Multimedia and Expo (ICME), Switzerland, Aug. 2002.

[15] X. Lu, Y. Wang, and A. K. Jain, "Combining Classifiers for Face Recognition," Proc. ICME 2003, IEEE International Conference on Multimedia & Expo, vol. 3, pp. 13-16, Baltimore, MD, July, 2003.

[16] J. Daugman, "Recognizing persons by their Iris patterns," Biometrics: Personal Identification in a Networked Society, A. K. Jain, R. Bolle, and S. Pankanti, Eds. Norwell, MA: Kluwer, 1999, pp. 103–121.

[17] John Daugman, "How iris recognition works," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[18] Intuos Pen Tablets, Wacom, [Online]. Available: http://www.wacom.com/intuos/index.php

[19] Interlink Electronics, eSign, [Online] Available: http://www.interlinkelectronics.com/esign/index.html

[20] P. M. Rubesh Anand, Gaurav Bajpai, and Vidhyacharan Bhaskar, "Online Multi-Parameter 3D Signature Verification through Curve Fitting," International Journal of Computer Science and Network Security, vol. 9, no. 5, pp. 38-44, May 2009.

[21] A. Rattani, D. R. Kisku, M. Bicego, M. Tistarelli, "Feature Level Fusion of Face and Fingerprint Biometrics," IEEE International Conference on Biometrics: Theory, Applications, and Systems, (BTAS 2007), pp. 1-6, Sep. 2007.

[22] A. Ross and A. K. Jain, "Information Fusion in Biometrics," Pattern Recognition Letters, vol. 24, no. 13, pp. 2115-2125, 2003.

[23] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification," Pattern Recognition, vol. 35, no. 4, pp. 861–874, 2002.

P. M. Rubesh Anand received the B.E. degree in Electronics and Communication Engineering from Periyar University, India in 2002, and M.Tech. degree in Advanced Communication Systems from SASTRA University, India in 2004. Since 2005, he is working as a Lecturer in the Faculty of Engineering, Kigali Institute of Science and Technology, Rwanda. Currently, he is pursuing his Ph.D. research at SRM University, Kattankulathur, India. His research interests include communication networks, cryptography and network security.

Gaurav Bajpai received the B.Tech. degree in Computer Science & Engineering from SRMSCET Rohilkhand University, India in 2000, M.Tech. degree in Software Engineering from Motilal Nehru National Institute of Technology, Allahabad, India and Ph.D. degree from Uttar Pradesh Technical University, Lucknow, India in 2006. He was an assistant Professor in the Department of Computer Science and Business Administration, Academy of Medical Sciences and Technology, Khartoum, Sudan from April

2006 to March 2007. Since March 2007, he is working as a Senior Lecturer in the Department of Computer Engineering and Information Technology, Faculty of Engineering, Kigali Institute of Science and Technology, Rwanda. His research interests include software engineering, network routing, network hardware security and bio-medical engineering. He has published more than 30 International Journal and conference papers.

Vidhyacharan Bhaskar received the B.Sc. degree in Mathematics from D.G. Vaishnav College, Chennai, India in 1992, M.E. degree in Electrical & Communication Engineering from the Indian Institute of Science, Bangalore in 1997, and the M.S.E. and Ph.D. degrees in Electrical Engineering from the University of Alabama in Huntsville in 2000 and 2002 respectively. During 2002-2003, he was a post-doc fellow with the Communications research group at the University of Toronto. From Sep. 2003 to Dec. 2006, he was an Associate Professor in the Département Génie des systèmes d'information et de Télécommunication at the Université de Technologie de Troyes, France. Since January 2007, he is a Professor and Associate Dean of the School of Electronics and Communication Engineering at S.R.M. University, Kattankulathur, India. His research interests include wireless communications, signal processing, error control coding and queuing theory. He has published 33 International Journal papers, presented 11 Conference papers in various International Conferences, and co-authored a book on MATLAB. He is also an active reviewer of refereed Journals like the IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, IEEE Communication Letters, IEEE Transactions on Vehicular Technology, Wireless Personal Communications Journal, International Journal of Network and Computer Applications, International Journal of Computer Communications, International Journal of Applied Mathematical Modeling, and International Journal of Computers and Electrical Engineering.