www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 8 August, 2013 Page No. 2348-2354

Biometric Based Web Security Using Ridges of Fingers

***Md. Majharul Haque*[1]*, R. H. M. Alaol Kabir*[2]*, Md. Shakil Ahamed Shohag*[3]*, Dr. Zerina Begum*[4]**

[1]Dhaka University, Department of Computer Science & Engineering,
Dhaka, Bangladesh
mazharul_13@yahoo.com

[2]Dhaka University, Institute of Information Technology,
Dhaka, Bangladesh
alaol_kabir@yahoo.com

[3]University of Development Alternative, Department of Computer Science & Engineering
Dhaka, Bangladesh
shakilshohag@gmail.com

[41]Dhaka University, Institute of Information Technology,
Dhaka, Bangladesh
zerinabegum@gmail.com

Abstract: ***Web security is in general taken as providing safeguard at the borders of an organization by keeping out impostors. For this purpose password based verification system with public key cryptography is a common standard. Passwords however have their own weaknesses; not only weak passwords can be easily guessed but the strong ones can be broken through too. Sometime people use access cards or identity cards for authentication purpose which can easily be stolen or forged. So designing a high security using passwords, identity cards or access cards still remain an open problem. Biometric characteristics of an individual however are unique and do not change over time that makes biometrics well suited for authentication. There are a large number of applications of biometric system for authentication based on finger prints, hand geometry, iris and voice exist, such as forensics, driver license and passport control etc. Since the internet growth is increasing rapidly, restricted access to sensitive data on the Web to unauthorized users is needed. A hand geometry based system has been proposed here to authenticate users for imposing access restriction to web. This method has been tested on 100 individuals. This technique can be used for e-commerce, e-banking applications etc.***

Keywords: Hand geometry, biometrics, authentication, Web pages, FAR, FRR.

1. Introduction

Security on the World Wide Web is now the most talked of topics where vulnerability is as usual. The technical terminology of the day is information warfare and network security, and there are valid reasons for their rise in importance. Throughout the evolution of networking and the Internet, the threats to information and networks have risen dramatically. Many of these threats have become cleverly exercised attacks causing damage or committing theft. There is a huge amount of sensitive commercial, personal, military and governmental information on the internet that needs to be secured so that only authorized people can gain access, the public has become more conscious of the need for network security and so too has the government. Generally web services depend on Internet Protocol (IP) name service [1]. That is why the name service based access should be secured from imposter accesses. Otherwise an intruder can easily gain access to the name service and the security based on correlating names and network addresses will fail. Username and password is required for authentication in the traditional methods which transmit information openly through the network. The risk of password eavesdropping can be reduced by the use of encryption technologies. The techniques for automatically identifying an individual based on his physical or behavioral characteristics are called biometrics. It is an emerging technology which authenticates users by their physical and behavioral characteristics and obviates the need to remember a password.

For Web access and e-commerce, biometrics along with encryption is capable of providing foolproof security. Some of the biometric sensors such as camera and microphone are becoming low-price standard options on PCs. Stamp-size solid state fingerprint capture devices are expected to become very cheap (~$10) and may soon be available on laptops [2]. Since the price of biometric readers is dropping, biometric authentication is becoming very popular day by day.

The personal attributes used in a biometric identification system can be physiological, such as facial features, fingerprints, iris, retinal scans and hand geometry; or behavioral, such as voice print, gait, signature, and keystroke style.

From anatomical point of view, human hand can be characterized by its length, width, thickness, geometrical composition, shapes of the palm, and shape and geometry of the fingers. It is generally accepted that fingerprint, retinal and iris patterns can uniquely define each member of an extremely large population which makes them suitable for large-scale recognition (establishing a subject's identity). However, in many applications, because of privacy or limited resources, we only need to authenticate a person (confirm or deny the person's claimed identity). Moreover, suitability of a particular biometric to a specific application depends upon several factors [3]. In these situations, we can use different distinguishing features with less discriminating power such as face, voice or hand shape. One distinct advantage the hand modality offers is that its imaging conditions are less complex, for example a relatively simple digital camera or flatbed scanner would be sufficient. Consequently, hand-based biometry is user-friendlier and it is less prone to disturbances and more robust to environmental conditions and to individual anomalies. Moreover, hand geometry has long been used for biometric verification and identification because of its acquisition convenience and good verification and identification performance [4, 5, 6]. Hand geometry measurement is non-intrusive and the verification involves a simple processing of the resulting features [7]. Almost all of the working population has hands and exception processing for people with disabilities could be easily engineered [8]. In contrast, face modality is known to be quite sensitive to pose, facial accessories, expression, and lighting variations; iris or retina-based identification requires special illumination and is much less friendly; fingerprint imaging requires good frictional skin etc., and up to 4% of the population may fail to get enrolled [9].Therefore, authentication based on hand shape can be an attractive alternative due to its unobtrusiveness, low-cost, easy interface, and low data storage requirements. Some of the presently deployed access control schemes based on hand geometry range from passport control in airports to international banks, from parents' access to child daycare centers to university student meal programs, from hospitals, prisons, to nuclear power plants [10]. In fact, there exist a number of patents on hand information-based personnel identification, using either geometrical features or on hand profile [10].

The features will be used to construct the template data. In this paper we address the issue of biometric-based access to the Web. The feasibility of such a system is demonstrated by designing a prototype system which uses hand geometry [10, 12] to verify a user and give him access to particular files on the Web. Any other biometric [16] (e.g., fingerprint and speech) may be used in similar way.

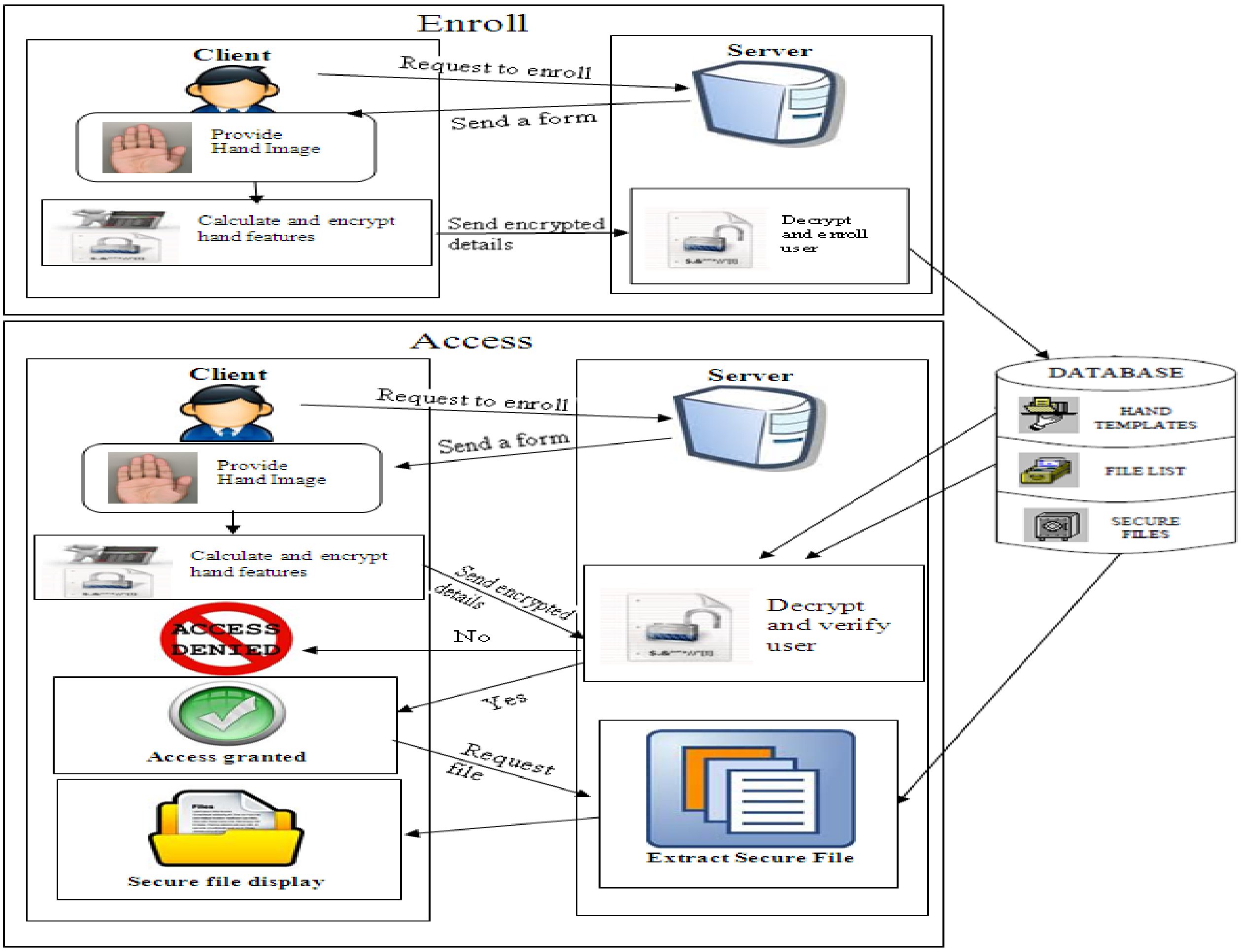


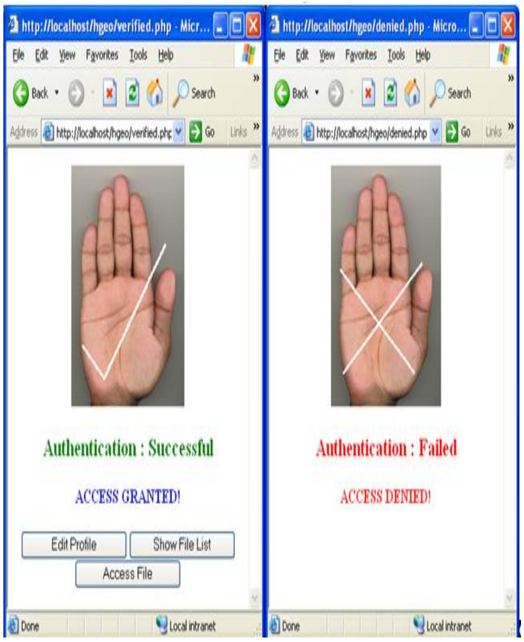
Figure 1: Flow diagram of client-server interaction

ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 8 August, 2013 Page No. 2348-2354

1.1 Restricting Access on Web and Flow Diagram

Our access mechanism uses the NCSA's (National Center for Supercomputing Applications) standard Basic Authentication [17] to restrict access to a web directory. Figure 1 shows the client/server interaction for the enrollment and access of secure files. Only one file (e.g., index.php) is allowed to access in the directory. This file, when downloaded to the client side, prompts the user to provide his hand geometry for authentication. The dialog box which provides live feedback of the hand geometry is an ActiveX control which can access system resources. This control captures the hand geometry image, calculates the feature vector and sends it to server along with other information about the user without storing it on the client's disk. This way, transmission of the feature vector is transparent to the user and the user has to be present at the point of authentication. This Protective tools and techniques exist to combat security threats; nevertheless, only with the proper implementation will they succeed. If the authentication fails, the client is denied access to the files and this information is conveyed to the client (Figure 2(b)). If the access is allowed (Figure 2(a)), then the server retrieves all the filenames accessible to this user and displays them as a list. The client can then access these files by clicking on their names in the browser. The secure files do not reside in a world readable directory and hence cannot be accessed through a URL. The server reads the users' requested file(s) and dynamically generates an HTML file with the contents.


http://localhost/hgeo/verified.php - Micr...

Address http://localhost/hgeo/verified.php

Authentication : Successful

ACCESS GRANTED!

http://localhost/hgeo/denied.php - Micro...

Address http://localhost/hgeo/denied.php

Authentication : Failed

ACCESS DENIED!

Figure 2: Authentication GUI. (a) Access is granted. (b) Access is denied.

2. Methodology

Feature mining may be unsuitable when the input data is fed into the biometric system. This is due to the several noise elements which may sneak into the data. After removing blast the resized image is used to extract and accumulate features. The final module of the biometric scheme is matching.

2.1 Conscription

A. Image Attainment and Resizing

The images are incarcerated using a flatbed scanner with 24 bit color and 200 dpi resolution. The input image is a colored image of the right palm (fingers are combined together) without any deformity. The captured image, shown in Figure 3(a) is stored in *tif* format. In cases of standard deformity such as a missing finger the system expresses its inability to process the image.

For resizing and cropping the captured image a photo editor is required such as Microsoft paint. The hand image will be converted to 25% of the original image. By cropping eliminate the unnecessary portion of the hand and stored in *bmp* file format as shown in Figure 3(b).

This image acquisition setup is simple and neither the employs require any special illumination nor uses any peg to cause any inconvenience to users. Only the users will be requested to place their hands on the surface of the scanner in such a manner that their fingers touch neighbor fingers. If the quality of the image is not satisfactory then the image is rejected. As a result, the database contains only good quality templates and the system accuracy improves.

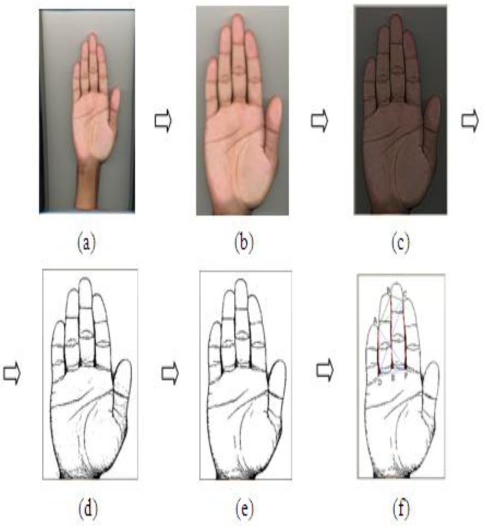


Figure 3: Process of features extraction (a) Original image, (b) Resized image, (c) Filtered image using 5x5 high pass filter, (d) Monochromic image, (e) Monochromic noise free image, (f) Extracted features.

B. Preprocessing

In this section, a moderated edge detection algorithm, based on high pass filer is applied to extract contour of hand. The first step of this edge detection algorithm is translating the hand image in such a way that all edges become black, shown in Figure 1(c). Then extract only edges by applying a threshold a value as shown in Figure 1(d). Noise exists between the fingers, the inside of the palm perimeter or in background. A convolution filter is applied which checks if a black pixel is surrounded on all sides by white pixels. If that is found will be considered as noise and is converted to a white pixel, shown in Figure 1(e). The size of the convolution filter is variable. First the filter uses a 3*3 template, then a 5*5, after that a 7*7 and finally a 9*9. This progressively removes larger and larger noise elements from the image.

C. Feature Extraction

Initially the coordinate values of the six points are detected from the acquired and preprocessed image. Three points of them are the three joining (valley) points- one point is between little and ring named A, the second one is between ring and middle named B and the last one is between middle and index fingers named C. The other three points are the three bottom joining points- one bottom point is that between little and ring named D, the second one is between ring and middle named E and the last one is between middle and index fingers named F marked in Figure 4.

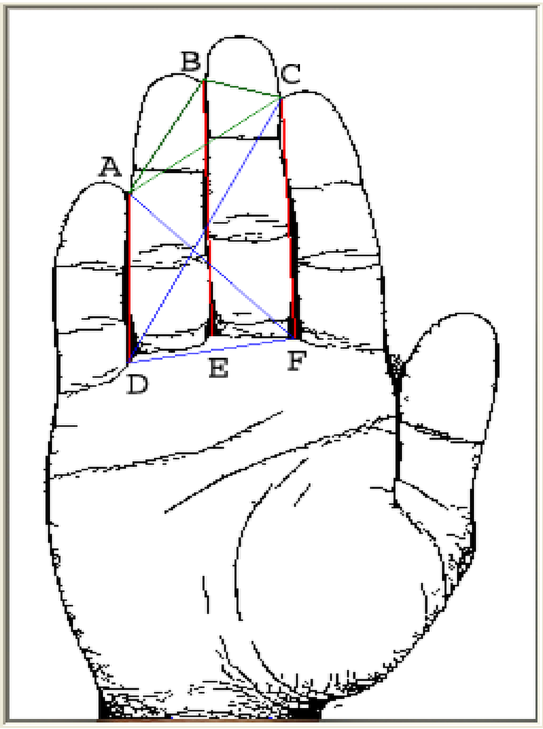


Figure 4: Joining points

Using these six points, features of hand geometry verification are extracted. At first, possible distances are considered. There are nine possible distances are taken by using these six points. The distances are AB, BC, AC, AD, BE, CF, DF, AF, and CD.

D. Template Construction

Templates are only data representing key or distinctive features of a biometric and are not a complete image or record of the original biometric (such as a fingerprint, voice recording or digital image). In this work, the template will be generated from three snapshot of each person. At first, we calculate distances for individual snapshot. Four distance metrics [11] are used for verification. Two of them need only mean values another one needs both mean values and standard deviation and the rest one needs both mean values and variance of individual distances. Thus mean values, variance and standard deviations of individual distances are calculated. The mean values will be used to construct the template for each person. That means,

Template $F = (d_1, d_2, \ldots\ldots\ldots, d_i)$

Where d_i average value of individual distance

i=1, 2, 3 number of features.

2.2 Verification

A. Matching

Matching is the process of calculating a similarity and dissimilarity between current feature representation of the biometrics data of a user and the respective reference data set. Snapshot of the hand are taken and the feature vector is computed. The given feature vector is then compared with the feature vector stored in the database associated with the claimed identity. Let $F = (f_1, f_2, \ldots\ldots, f_d)$ represent the d-dimensional feature vector in the database associated with the claimed identity and $Y = (y_1, y_2, \ldots\ldots, y_d)$ be the feature vector of the hand whose identity has to be verified. The size of the feature vector dimension is nine. The verification is positive if the distance between F and Y is less than a threshold value. Four distance metrics i) absolute, ii) weighted absolute, iii) Euclidean and iv) weighted Euclidean corresponding to the following four equations were explored [12].

$$\text{i)}\ \sum_{j=1}^{d} |y_i - f_i| < \varepsilon_a \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

$$\text{ii)}\ \sum_{j=1}^{d} \frac{|y_i - f_i|}{\sigma_j} < \varepsilon_{wa} \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

$$\text{iii)}\ \sqrt{\sum_{j=1}^{d} (y_i - f_i)} < \varepsilon_e \ \ldots\ldots\ldots\ldots\ldots\ldots(3)$$

$$\text{iv)}\ \sqrt{\sum_{j=1}^{d} \frac{(y_i - f_i)^2}{\sigma_j^{\ 2}}} < \varepsilon_{we} \ \ldots\ldots\ldots\ldots\ldots(4)$$

where σ_j^2 is the feature variance of the j_{th} feature and ε_a, ε_{wa}, ε_e, and ε_{we} are threshold values for each respective distance metric.

3 Experimental Result

One of the tasks to be studied for the enrollment process is the number of feature vectors that form the user's template. It is obvious that the bigger the number of samples used the better the calculated template will be created.

The hand geometry authentication system was trained and tested using a database of 18 users. At least four images of each user's hand were captured over different sessions. Total 125 images were made available. Out of 125 images, only 100 were used for testing our hand geometry system. The remaining 25 images were discarded due to incorrect placement of the hand by the user. Thus, user adaptation of this biometric is necessary. Three images of each user's hand were randomly selected to compute the feature vector which is stored in the database along with the user's name.

3.1 FAR-FRR Analysis

The performance of a biometric system is measured in certain standard terms. These are given below:
False Acceptance Rate (FAR) is the ratio of the number of unauthorized (unregistered) users accepted by the biometric system to the total of identification attempts made.

$$\text{FAR } (\lambda) = \frac{\text{Number of False Attempts}}{\text{Number of Impostor Accesses}}$$

(λ) = Security Level
False Rejection Rate (FRR) is the ratio of the number of number of authorized users rejected by the biometric system to the total number of attempts made.

$$\text{FRR } (\lambda) = \frac{\text{Number of False Rejects}}{\text{Number of Client Accesses}}$$

(λ) = Security Level

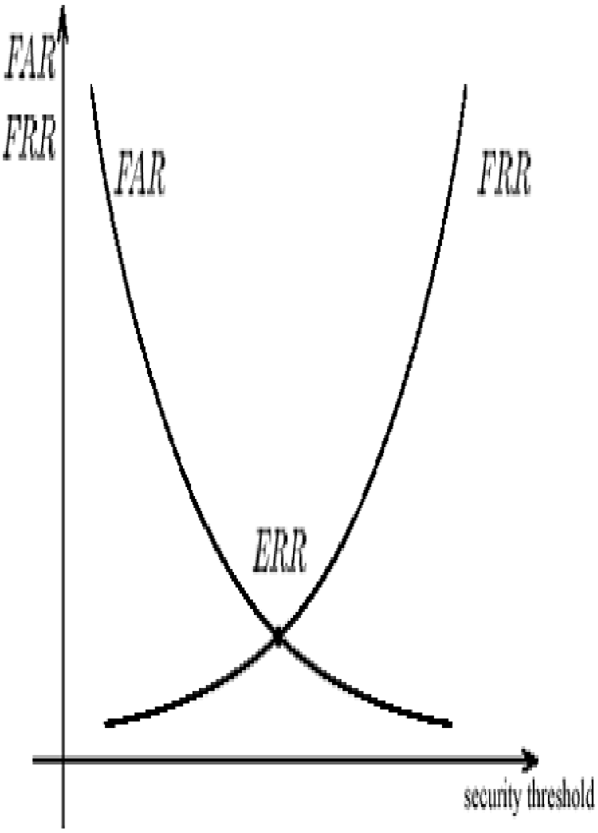


Figure 5: FAR-FRR Rate

False acceptance poses much more serious problem than false rejection. It is therefore desired that the biometric system keep the FAR to the minimal possible limit. This can be achieved by setting a high threshold so that only very near matches are recognized and all else are rejected. The higher the security requirement from the system the higher the threshold required to maintain it.
Now FAR-FRR analysis is going to be conducted for each of the distances used in this study.
During these tests the match-score for each false acceptance has been noted. Also the match-score for each false rejection are noted The FAR-FRR curve is shown in Figure 6 depict the performance of the system for the Absolute, Euclidean, Absolute, Weighted Euclidean distance.

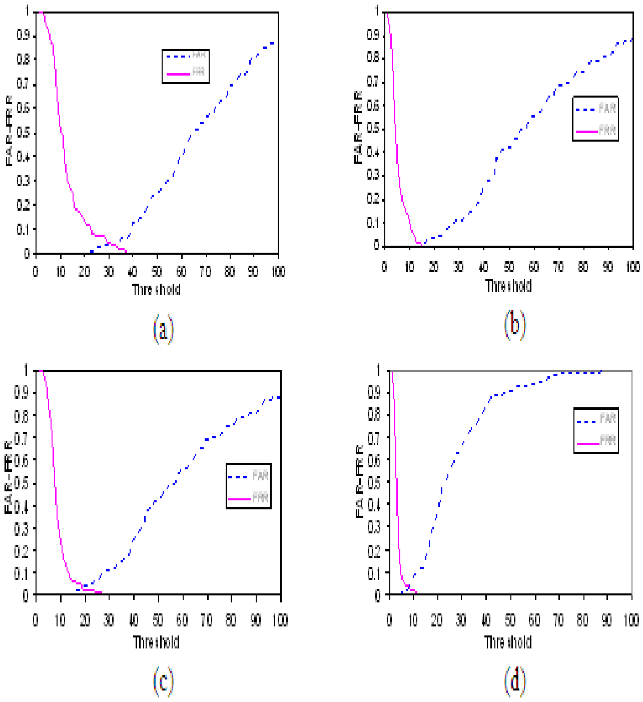


Figure 6: FAR - FRR curve for (a) Absolute Distance, (b) Euclidean Distance, (c) Weighted Absolute Distance, and (d) Weighted Euclidean Distance.

From the above curves we get best performance of FAR-FRR by Euclidean distance.

3.2 ROC Curve Analysis

The Receiver Operating Characteristic (ROC) is used instead of thresholds for this purpose. The ROC is a plot depicting the genuine acceptance rate along the Y-axis and the false acceptance rate along the X-axis. Time in some cases is of crucial importance in the performance of a biometric system. In an offline system it is not crucial but in the case of online systems it is of importance that the system works fast enough so as not to cause the user unnecessary annoyance.
The ROC curves shown in Figure 7 depict the performance of the system for the Absolute, Euclidean, Absolute, Weighted Euclidean distance.

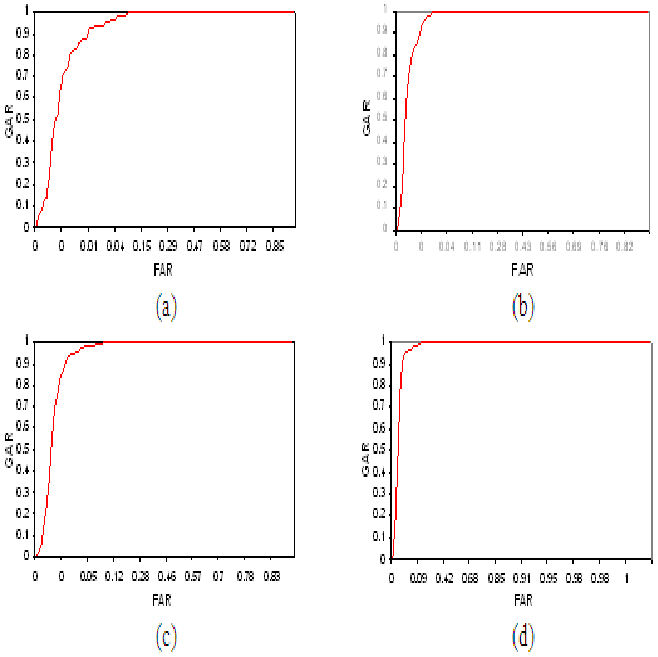


Figure 7: ROC curve for (a) Absolute Distance, (b) Euclidean Distance, (c) Weighted Absolute Distance, and (d) Weighted Euclidean Distance.

From the above curves we get best hit ratio against the false acceptance rate by Euclidean distance.

3.3 Comparison Analysis

To evaluate the system performance, experimental results of proposed technique using 100 images are taken and three well-known measurements are used, such as False Rejection Rate (FRR), False Acceptance Rate (FAR) and Total Success Rate (TSR). The system performance could be significantly improved by having habituated users.

Relatively a comparison is made based on the outcomes of Absolute, Euclidean, Weighted Absolute and Weighted Euclidean distance of proposed system and shown in Table I. In Table II, a comparison is made among the results of the proposed method and the results of the existing methods.

Table 1: Comparison Study of Four Distance Matrices

Feature Vector Dimension	Name of the Distance Metrics	Decision Threshold	FAR %	FRR %	TSR % [11]
9	Absolute	26	0.03	0.07	99.95
	Euclidean	14	0	0.02	99.99
	Weighted Absolute	15	0.01	0.06	99.96
	Weighted Euclidean	7	0.02	0.04	99.97

Table 2: Comparison among Proposed Method and Existing Methods

Name of the Paper	Techniques Applied for Verification	Feature Vector Dimens-ion	Classif-ication Success Rate (%)
Biometric Identification through Hand Geometry Measurement [11]	Euclidian distance metric	15	86
A prototype Hand Geometry Based Verification System [12]	Absolute Distance Metric	14	94.99
Hand Reorganization using Implicit Polynomial and Geometric Features [13]	Geometry	16	89
Personal Verification using Palm-print and Hand Geometry Biometric [14]	Normalized Correlation	16	91.66
Peg-Free Hand Geometry Recognition Using Hierarchical Geometry and Shape Matching [15]	Gaussian Mixture Models (GMMs)	16	96
Personal Authentication Using Hand Geometry [18]	Absolute without mean	15	99.71
A Simple and Effective Technique for Human Verification with Hand Geometry [19]	Distance Based Nearest Neighbor (DBNN)	15	99.11
Authentication of Individuals Using Hand Geometry Biometrics: A Neural Network Approach [20]	Multi layer perception (MLP)	10	99.62
Proposed System	Euclidean distance Metric	9	99.99

It can be observed evidently that the performance of the proposed system is better than existing systems.

4 Conclusion

On the Web, like the knowledge-based authentication (e.g., passwords and PIN), Biometric is increasingly used in conjunction with other technologies. This approach stated that restricting access to web pages can be imposed using hand geometry-based authentication. This study is based on new features selection for hand geometry based personal verification systems which is very much user friendly and convenient to implement. This method is peg free and images can be captured by a normal scanner. Organizer need not to manage a high image captured instrument or pegged scanner so it can be put in practice in anywhere and anytime. User can place his/her hand in any orientation less than 45 degree along vertical axis. Generally a large number of feature decrease the performance of computation [21] here as only one set of feature vector (nine features) are used which improves the computational efficiency. The remarkable achievement obtained from the proposed method is the result of verification, which is the best among the prevailing techniques of hand geometry based verification system. It showed promising results with accuracy around 99.99% which support our claim that our system is secure.

References

[1] A. K. Jain, A. Ross and S. Prabhakar, “Biometrics-Based Web Access”, MSU Technical Report TR98-33, 1998.

[2] Solid-state fingerprint capture devices from Veridicom. [Online] Available: http://www.veridicom.com (Accessed: August 19, 2013)

[3] A. Jain, L. Hong, S. Pankanti, R. Bolle, “Online identity-authentication system using finger-prints”, Proceedings of IEEE, vol. 85, pp. 1365-1388, September 1997.

[4] J. Ashbourn, Biometrics: Advanced Identity Verification, Springer-Verlag, New York, November 2000.

[5] R. Sanchez-Reillo, “Hand geometry pattern recognition through Gaussian mixture modeling”, In Proceedings of the 15th International Conference on Pattern Recognition, vol.2, pp. 937-940, September 2000.

[6] A.K. Jain, N. Duta, “Deformable matching of hand shapes for verification”, In IEEE International Conference on Image Processing, pp. 857-861, October 1999.

[7] J. R. Young, H. W. Hammon, “Automatic Palmprint Verification Study”, Rome Air Development Center, RADC-TR-81-161 Final Technical Report, June 1981.

[8] R. Zunkel, Hand Geometry Based Authentication, In Biometrics: Personal Identification in Networked Society, A. Jain, R. Bolle, and S. Pankanti (Eds.), Kluwer Academic Publishers, 1998.

[9] A. K. Jain, A. Ross, S. Prabhakar, “An introduction to biometric recognition”, IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4-20, Feb. 2004.

[10] R. L. Zunkel, Hand geometry based verification, In Biometrics, A. Jain, R. Bolle, and S. Pankanti (Eds), Norwell, MA: Kluwer, pp. 87-101, 1999.

[11] R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos, “Biometric identification through hand geometry measurements”, IEEE Trans. Pattern Anal. Mach. Intell., vol. 22, no. 10, pp. 1168-1171, Oct. 2000.

[12] A. K. Jain, A. Ross, S. Pankanti, “A prototype hand geometry based verification system”, In Proc. 2nd Int. Conf. Audio and Video-Based Biometric Person Authentication, pp. 166-171, March. 1999.

[13] C. Öden, A. Erçil, B. Büke, “Combining implicit polynomials and geometric features for hand recognition”, Pattern Recognit. Letter, vol. 24, pp. 2145-2152, 2003.

[14] Y. A. Kumar, D. C.M.Wong, H. C. Shen, A. K. Jain, “Personal verification using palm-print and hand geometry biometric”, In Proc. 4th Int. Conf. Audio Video-Based Biometric Person Authentication, Guildford, U.K., pp. 668-678, Jun. 9-11, 2003.

[15] Alexandra L.N. Wong, Pengcheng Shi, “Peg-Free Hand Geometry Recognition Using Hierarchical Geometry and Shape Matching”, Department of Electronic and Electrical Engineering, Hong Kong University of Science and Technology.

[16] Anil K. Jain, R. Bolle, S. Pankanti, BIOMETRICS: Personal Identification in Networked society, Kluwer Academic Publishers, 1998.

[17] NCSA HTTPD Mosaic User Authentication Tutorial. [Online] Available: http://kh.hd.uib.no/httpddoc/info/authtut.htm (Accessed: August 20, 2013)

[18] Aghili, B., “Personal Authentication Using Hand Geometry”, Conference on Computational Intelligence and Software Engineering, Dept. of Electr. Eng., Shahed Univ., Tehran, Iran, 2009.

[19] Rahman, A.; Anwar, F.; Azad, S., “A Simple and Effective Technique for Human Verification with Hand Geometry”, In Proceedings of the International Conference on Computer and Communication Engineering, ICCCE ’08, Kuala Lumpur, Malaysia, pp. 1177-1180, May 13-15, 2008.

[20] Marcos Faúndez-Zanuy, David A. Elizondo, Miguel Angel Ferrer-Ballester, Carlos Manuel Travieso-González, “Authentication of Individuals using Hand Geometry Biometrics: A Neural Network Approach”, Neural Processing Letters 26(3): 201-216, 2007.

[21] Yan Li, Jia-Xiong Peng, “Remote sensing Texture Analysis Using Multi-Parameter and Multi-Scale Features”, Photogrammetric Engineering & Remote Sensing, vol. 69, no. 4, pp. 351-355, April 2003.