International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||

Hand Geometry Biometric Identification and Authentication System: A Review

Sangeeta Dey[1], A. K. Kapoor[2]

Research Officer, Sports Authority of India, Delhi, India[1]

Professor, Department of Anthropology, University of Delhi, Delhi, India[2]

ABSTRACT: In this modernized era, identification of individual's has been replaced by human biological characteristics such as fingerprint, iris scan, etc. instead of password, pin codes and ID Cards which comes under the domain of biometrics. The geometric structure of human hand possesses unique characteristics that can serve as a biometric feature that can be efficiently used for identification and authentication. In this paper, an attempt has been made to investigate the process and techniques of hand geometry biometrics which has emerged as a biometric solution in the applications where low to medium security is required due to its universality, acceptance, permanence, measurability, reliability, and comparability. Previous works on hand geometry biometrics has been compared on the basis of recognition method. It is concluded that in order to make hand geometry biometrics more reliable for identification and verification purposes, it should be infused with other biometric features like fingerprint, palm prints, hand vein patterns which can able to give more accurate and better results. Researchers in this field should orient their focus in this direction to further improve its applicability.

KEYWORDS: Hand Geometry, Biometric Modules, Personal Identification and Authentication, FRR, FAR, Anthropological Significance.

I.INTRODUCTION

The term "Biometrics" is a general term, comes from the Greek word 'bios' meaning life and 'metrics' meaning measurements, used alternatively to describe a characteristics or a process. As a characteristic, a biometric is a measurable biological & behavioural characteristic that can be used for automated recognition whereas as a process, a biometric is an automated method of recognizing an individual based on measurable biological and behavioural characteristics [1,2]. Thus, Biometrics refers to the identification and verification of individuals based on their biological and behavioural characteristics [3,4].

Human beings develop several unique biological and behavioural characteristics that can serve as biometric features or identifiers. The various biological characteristics that are generally used are face, facial thermo grams, iris and retina pattern, DNA, fingerprint, palm-print, hand vein thermo grams and hand geometry whereas the behavioural characteristics include signatures, handwriting pattern, keystroke pattern, gait, odour and voice [1,5-9]. The biological characteristics are more stable than behavioural characteristics as behavioural methods has high variation due to influences such as stress, fatigue or illness [4].

Human identification and authentication through biometric technologies is gaining more and more privilege in recent years [10,11] as biometric technologies are becoming the foundation of extensive array of highly secure identification and personal verification solutions [12,13]. With the increase in fraud in today's world, there is a need for highly secure identification system and biometrics emerged as an advanced automated identification and verification system based on human characteristics [5,14]. The humans can either be recognized by the password or pin which he knows or by Voter ID, Smart card or Aadhaar card etc. which he owns or by his human characteristics. Identification by means of his own characteristics is more beneficial and secure than the other conventional identification systems as the possessions can be lost, stolen or easily duplicated and the knowledge can be forgotten and shared whereas human characteristics cannot be misplaced or forgotten [4,8].

Each biometric feature has its own advantages and disadvantages according to user acceptance, cost and performance etc. [1]. The attributes required to be a good biometric characteristics are

- *universality* – every person must possess the characteristics; uniqueness – the characteristics should be as unique as possible;
- *permanence* – the characteristics should be constant over a long period of time;

- *measurability* – the characteristics should be easily obtained and captured;
- *acceptance* – the characteristics can be collected from large percentage of population;
- *reducibility* – the characteristics should be capable of being reduced to a file which is easy to handle;
- *reliability and tamper resistance* – the characteristics should be impractical to manipulate;
- *privacy* – the characteristics should not violate the privacy of the person; and
- *comparable* – the characteristics should be digitally comparable and matching can be processed for more authoritative identification [15].

Hand Geometry based biometric technologies emerged as an efficient biometric solution in the applications where low to medium security systems is required. The present paper aims to conduct an extensive survey on the process, techniques, advantages and disadvantages of Hand Geometry Biometric System.

Hand Geometry Biometrics

Hand Geometry as the name suggests, refers to the geometric structure of the hand [1]. Hand Geometry based biometric system has been widely and most commonly used with respect to other biometric characteristics such as face, iris, retina which require special illumination setup[16-22].

The Hand Geometry Biometrics in comparison to other techniques are –

- User acceptance or User friendlier, it is rarely rejected by the user as it doesn't hamper their privacy;
- Ease of acquisition of data, it is relatively easy to collect;
- Cost effective, it requires only a low cost CCD camera or a low cost document scanner;
- Low template size, it greatly reduces the need of the memory,
- Low computational needs, it requires low computational complexity algorithms that leads to fast results;
- Lesser error, it produces relatively lesser error and has better performance and accuracy [10].

The typical human hand features recognized as a characteristic for Hand Geometry Biometrics can be divided into five different categories –

1. Widths: The width of each finger at various locations, width of the palm through various reference points, width of the wrist;
2. Lengths/heights: The height or length of each finger from finger bases to the middle of the fingertips and the palm through reference points on the wrist base line to the finger valley points, the thickness of the hand and perimeter of the hand and fingers;
3. Deviations: Distance between a middle point of respective finger and the middle point of the straight line between the interfinger point and the height measured at the minimum width of the finger towards the fingertip;
4. Ratio: aspect ratio of the palm and various fingers;
5. Angles: between the interfinger points and the horizontal [10].

II.THE PROCESS

The typical process of all biometric systems generally consists of two phases – Enrollment phase and the Verification phase [1,4,9,14].

Enrollment Phase:

In the phase of enrollment, it involves one of the following two tasks – add a new user to the database; and update a current user's feature vector [1]. The phase involves three Modules or Steps – Image Acquisition; Image Pre-Processing; and Feature Extraction Module. For example, with respect to hand geometry biometrics, several images of the human hand are captured from the user in succession. These images, called templates are then pre-processed to be used to compute the feature vector of the given hand. Re-computing the feature vector is done by averaging the individual feature values. Feature extraction involves a set of measurements to be performed which are most distinctive and stable and are extracted and encoded into a biometric reference or template that is the mathematical representation of the individual's biometric feature which is stored in the system database.

Verification Phase:

In the phase of verification, the process involves matching a given hand to an individual previously enrolled in the system database. The phase involves all the five modules of biometric system as depicted in the Fig. 1. For verification,

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||

a single image or template is taken, pre-processed and features are extracted. The given feature vector (Let Y = y1, y2, y3,….,yd) are then compared with the feature vector stored in the database associated with the claimed identity (Let X = (x1, x2, x3,……, xd). The verification is positive or authenticated if the distance between X and Y is below the threshold value. The distance metrics used in biometric and the mathematics behind the threshold value is discussed in the matching and decision module later in the section.

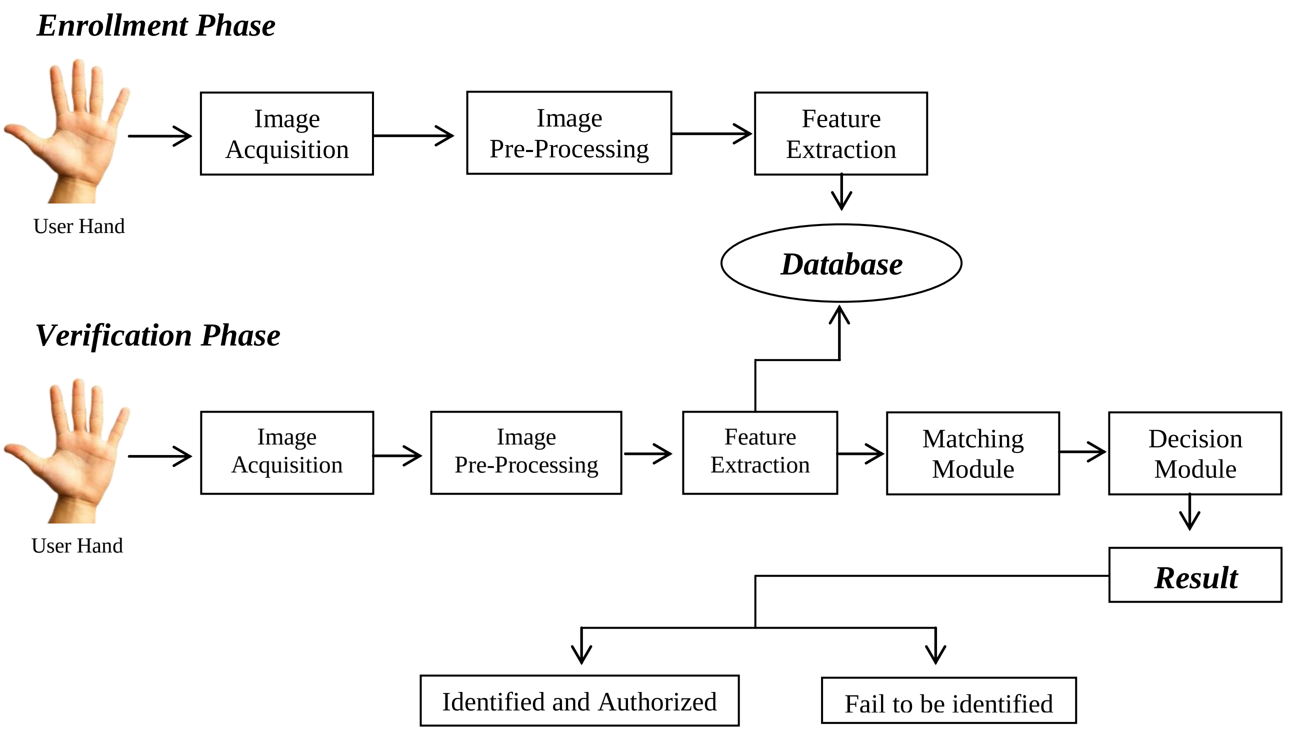


Fig. 1: Block Diagram of the Process of Biometric Systems

III. THE MODULES OF BIOMETRIC SYSTEM

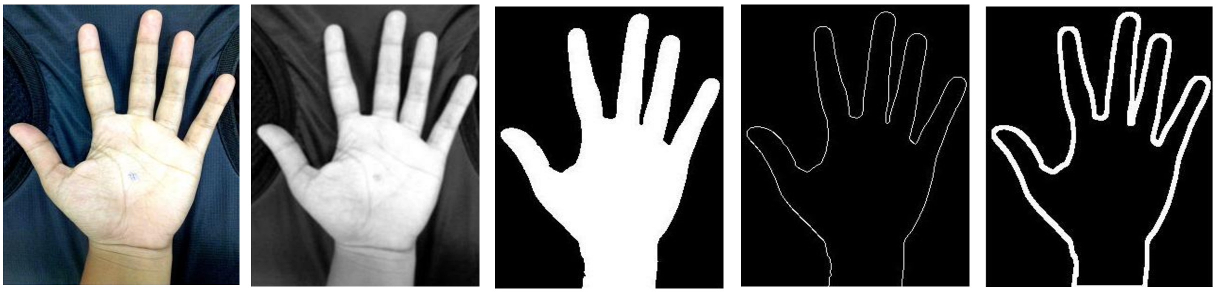
A biometric identification and authentication system comprises of five important modules – image acquisition, image pre-processing, feature extraction, matching and decision module [10,11,23,24].

Image Acquisition Module comprises of a light source and a camera or scanners which captures a sample of the user's biological data [10]. A number of templates or images of the biological data are generally captured during this module or enrolment process in order to create a truly representative template [9]. These captured templates are stored in a database or on a smart card in various formats such as .jpeg, .tiff, .bmp and .gif on the computer for possible image processing.

Image Pre-processing Module - after the image is captured, it is pre-processed to obtain only the area of information [4]. Image pre-processing step is important because the input data is unsuitable for feature extraction as only monochromatic image is required for further analysis and due to the several noise elements which may present or creep into the data inadvertently [25].

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||



Captured Image (Coloured) | Gray Scale Image (*im2bw*) | Binarized & Normalized (*imfilter*) | Edge Detected Image | Smoothed Image for Feature Extraction

Fig. 2: Image Pre-processing Module

The first step in image pre-processing is transforming the input colored image into gray scale image using various functions such as rgb2gray or im2bw from software MATLAB. The red, green and blue (RGB) values of each pixel of the image are extracted. Since a monochromatic image is required for the proposed system a threshold is determined. The next step in which the grayscale image is converted into binary image by thresholding is called binarization as shown in Fig 2. The threshold level or value is automatically computed using Ostu method [26] to minimize the intra-class variation of the black and white pixels. The binary image has a clear distinction in intensity between the biological data and the background because it has values of 0 (black) for all the pixels of the input image with RGB values below the threshold level and 1 (white) for the pixels which has RGB values above the threshold level. Therefore, the histogram of the image is bimodal. Then noise removal is done to remove the fake pixels in the image. The process is called normalization. MATLAB function imfilter or median filters or are used to remove those pixels which computes the value of each output pixel using double-precision and floating-point arithmetic. The last step in pre-processing module is edge detection. The edge detection algorithm converts all the pixels to black (0) except those which are present at the boundary of black and white regions to localize the pixel intensity transition. Detecting boundaries of an image also filters out the useless information while preserving the important structural properties of an image [7]. Algorithm also ensures that the thickness of the boundary is as low as possible [27] as thick boundary will affect the accuracy of the feature detection module. The edge or boundary is then smoothed using morphological operators to be used effectively for further analysis. So, the primary task of the image processing module is to prepare the captured image or input data for feature extraction.

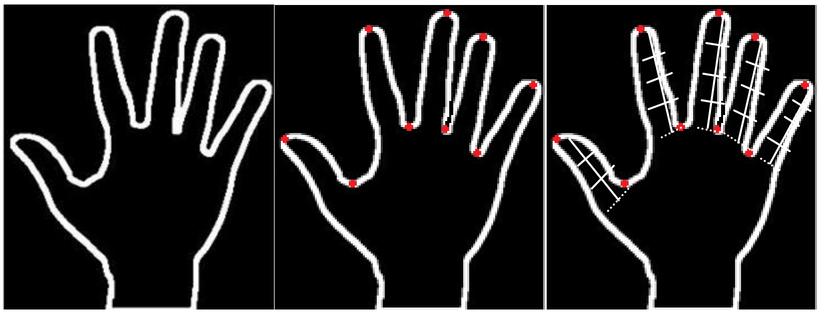


Fig. 3: Hand Geometry Feature Extraction Module

Feature Extraction Module is the most important module in a biometric system as it enables us to extract the peculiar features of the biological data and transforms the input data into the set of features. An algorithm for the feature extraction was created using programming environment MATLAB which is based on counting pixel [18]. For example, in Hand Geometry Biometric System, typical features include length and width of the fingers (as depicted in Fig 3), aspect ratio of the palm or fingers, perimeter of the hand and fingers, thickness of the hand etc. The reference points for these features are fixed and the landmark points such as fingertips, finger valley points have to be located. For this purpose, the algorithm looks for white pixels between two given points and computes a distance using geometrical

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 5, May 2020||

principles [28]. The result is the vector of all the features. The feature vector so obtained registered in the database as user model.

Matching and Decision Module is the last module of biometric system which determines the degree of similarity between the user feature vector and claimed feature vector. The matching process may be divided into two types based on the application - Verification and Identification. Verification is one to one matching which involves confirming or denying the claimed identity of an individual by comparing with the stored template of the claimed person and measuring the degree of similarity. On the other hand, identification is one to many matching where an individual's identity is compared with all the stored templates of feature set in database and degree of matching is calculated by a matching score [24]. So, essentially the feature vector obtained from the input image is matched against the feature vector of the images in the database. Distance functions or various classifiers are used for this purpose such as Euclidian distance, Hamming distance, Gaussian mixture model (GMMs), Radial basic function neural networks (RBF), Bayes classifier, k-nearest Neighbour (k-NN), geometric classifiers etc. [5,10,29]. The matching algorithm produces the closest match and match score. The match score represents the closeness of the input image to the image present in the database. This however creates a problem that is in cases when an individual is not registered with the system, the system may return the closest match to that individual and thus the system becomes useless as both registered and unregistered individuals are recognized. To overcome or to prevent this problem, a threshold is decided based on experimentations. The threshold is a value which lies in the range of match score. Decision for positive identification and verification is made as either accepted to be genuine or rejected as an imposter by comparing the distance value obtained from the matching score to a predefined threshold. For any image, if the match score is below the threshold then that image is rejected as a match to the database image specified. However, if the match scores of an image is higher or above the threshold then it is said to match the image in the database. Thus, only those matches which are above the certain threshold are said to be valid and accepted whereas other are rejected. So, the output of the matching module is a match score and the judgment of whether it is higher or lower than the threshold [27].

IV.PERFORMANCE PARAMETERS OF BIOMETRIC SYSTEMS

The performance and accuracy of the biometric systems can be measured using certain standard parameters – FRR (False Rejection Rate), FAR (False Acceptance Rate) and EER (Equal Error Rate).

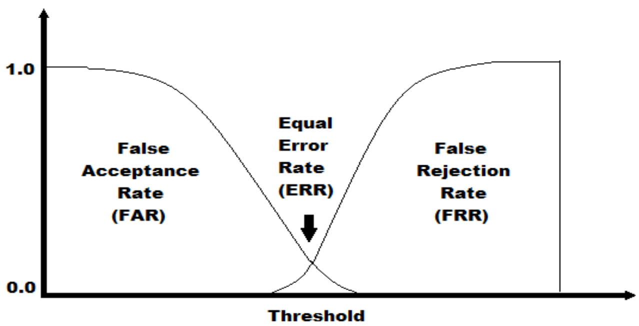
False Rejection Rate (FRR) is the ratio of the number of times the authorized users rejected by the biometric system to the total number of attempts made [9].

$$FRR\ (\lambda) = \frac{Number\ of\ False\ Rejection}{Total\ Number\ of\ Attempts}$$

False Acceptance Rate (FAR) is the ratio of the number of unauthorized users accepted by the biometric system to the total number of attempts made.

$$FAR\ (\lambda) = \frac{Number\ of\ False\ Attempts}{Total\ Number\ of\ Attempts}$$

Equal Error Rate (ERR) is a point on the ROC (Receiver Operating Characteristics) or DET plot where FRR and FAR are equal. It indicates how accurate the system is and lower the value of EER, the more accurate or better will be the biometric system.



Both the FRR and FAR are functions of system threshold that is if the threshold is increased then FAR will decrease but FRR will increase and vice versa. So, for a given biometric system both the errors cannot be decreased simultaneously by varying the threshold.

Comparison of Related Literatures of Hand Geometry Biometric Systems

In this Section, Comparison was made based on the work done by the researchers on hand geometry biometrics on the basis of recognition method, features extracted, size of database, performance indicators as depicted in Table 1.

Table 1: Comparative Analysis of Hand Geometry Biometric Recognition Methods

Recognition Method	Features Extracted	Size of Database	FAR/FRR (Success Rate)	Reference
Euclidean distance, Hamming distance, Gaussian Mixture Model (GMM)	21 Features: 3 Finger Widths at each finger except thumb with 2 FW; 5 Finger Heights; and 2 Palm size	408 hand images	Best Result by using GMM with FAR = 0,1812% FRR = 14,583%	Varchol and levicky, 2007 [4]
Gaussian Mixture Model (GMM), Hamming distance, Radial basis Function Neural Networks (RBF), Multi Layer Perception (MLP), k-Nearest Neighbor (k-NN), Bayes Method	31 Features: 10 area and length of fingers, 21 width of multiple parts	200 hand images	Best results with GMM 85% and RBF 91%.	Hashemi and Fatemizadeh, 2005 [5]
Euclidean distance, Hamming distance, Gaussian Mixture Model (GMM), Radial basis Function Neural Networks (RBF)	31 Features: 21 widths, 3 heights, 4 deviations, and 3 angles.	200 hand images	GMM shows the best result with 97% success rate	Sanchez-Reillo et al., 2000 [10]
Neural Net Classifier, Radial basis Function Neural Networks (RBF)	9 Features	220 hand images	Nearest Neighbor 73.64% and RBF 90%	Faundez-Zanuy and Mérida, 2005 [30]
Euclidean distance and absolute distance	24 Features: Length and width of four fingers except thumb	500 hand images	Best results by Absolute distance classifier EER = 0,1743%	Aghili and Sadjedi, 2010 [31]
Support Vector Machine Classifier	34 Features	60 images / person	FAR = 1,85%	Guo et al., 2012 [32]

V. HAND GEOMETRY BIOMETRICS ADVANTAGES AND DISADVANTAGES

Hand Geometry Biometrics, like all other Biometrics systems has its own set of advantages as well as disadvantages. These include:

Advantages of Hand Geometry Biometrics –

- HG (Hand Geometry) Biometric technology is relatively simple, accurate, inexpensive and easy to use.
- It is considered less intrusive than other biometric modalities like fingerprint, retinal and iris scans due to sufficient dexterity for the users in HG Biometrics to access the HG devices which further reduces the error rates.
- Performance of the HG Biometric systems doesn't vary with the environmental conditions such as dry weather or extreme heat or cold where other biometric systems may fail or with the conditions of the skin surface such as skin texture, wet/dry skin, smudged skin or excessive scars etc.

- HG Biometric System is hard to circumvent and resistant to spoofing as it would require the entire 3D replica or cast or latex model of the users hand and thus it is difficult to execute and more likely to be rejected.
- Requirement of memory is relative less for HG Biometrics as it has small template size comparatively which allows fast processing and a single device (for e.g. magnetic stripe cards) can accommodate over 40,000 HG biometric template of different users and thus it can be used in warehouses and factories, where large volumes of individuals are processed.
- It doesn’t require special lighting like in retinal scans and are thus reliable and have high level of public acceptance as compare to other biometric technologies.

Disadvantages of Hand Geometry Biometrics –

- HG Biometrics characteristics or features is not sufficiently unique or distinctive enough to allow high security or one-to-many searches but limited to one-to-one authentication and thus its applications are limited to verification rather than identification of an individual from an database.
- Performance of HG Biometric systems can be affected by the medical conditions of the hand like swelling, injuries, arthritis that obscure or changes the basic structure of the hand and cause recognition difficulties.
- The geometric structure of the hand is affected with respect to weight and aging and thus affects HG biometric recognition.
- HG biometric systems require re-enrollment once or twice for the users who are under growth and thus possess hindrance in verification.
- HG scanners are relatively large and hygiene concerns are associated with it as multiple users place their hands on the scanning plate. However, to overcome this issue, manufacturers uses silver Nano-technology on the scanning surface which has anti-microbial properties making the biometric system suitable and hygiene sensitive.

VI.CONCLUSION

Biometrics systems provide three kinds of services – Verification; Classification and Identification. Biometric system procedures are gaining more and more privilege for security purposes. Researchers used simple classifier – nearest box classifier and verifier, as well as novel classifier – minimum enclosing ball classifier for verification, classification and identification of individuals. However, Gaussian Mixture Model (GMM) has been revealed as the one with the best performance and provided better results as compared to other methods but with more features and less populations.

Anthropologists and researchers in the field of biometrics found that human hand contains characteristics that can be used for identification in forensic domain [33-35] and it is the source for a number of physiological biometric features such as fingerprints, the palm print, the geometry of the hand, the geometry of the fingers and the vein pattern on the back of the hand [5,6]. Hand Geometry Biometrics include the geometric structure of the hand that is length of the hand and the fingers, width of the fingers at various locations, width of the palm, thickness of the palm, perimeter of the hand and fingers, area of the hand and fingers etc. It is also well known fact that hand geometry system cannot be applied to individuals with severe arthritis who cannot spread their hands.

It is concluded that Hand Geometry Biometric System can be used for medium security applications. On the basis of literature review, it is also suggested that hand geometry biometrics can be effectively and efficiently used as a good technique for verification than identification and in order to make hand geometry biometrics more reliable for identification and verification purposes, it should be infused with other biometric features like fingerprint, palm prints, hand vein patterns which can able to give more accurate and better results. Hand geometry biometrics have found sustainable market niche in national and international security and has been widely used in applications such as physical access, attendance tracking, dual custody application, cash vault application, parking lot application, immigration, border control, interactive kiosks, security application in airports, at entrance of nuclear power points, in Olympic games etc. and personal identification, verification authentication and recognition.

VII. ACKNOWLEDGEMENT

SD is grateful to Department of Anthropology, University of Delhi for the infrastructural support and University Grant Commission for providing UGC-SRF financial assistance under which the present study was conducted.

REFERENCES

[1] Anil K. Jain, Arun Ross, SharathPankanti, "A Prototype Hand Geometry-based Verification System." *Proc. of 2nd Int'l Conference on Audio and Video-based Biometric Person Authentication (AVBPA), Washington D.C.*, pp.166-171, March 22-24, 1999.

[2] MuzhirShaban Al-Ani, MahaAbd Rajab, "Biometrics hand geometry using discrete cosine transform (DCT)."*SciTechnol*, vol. 3, no. 4, pp. 112-117, 2013.

[3] A. K. Jain, R. Bolle, S. Pankanti(Eds).,"Biometrics: Personal identification in Networked Society."*Kluwer Academic Publishers*, pp. 1-41, 1998.

[4] P. Varchol, D.Levicky, "Using of hand geometry in biometric security systems."*Radioengineering*, vol. 16, no. 4, pp. 82-87, 2007.

[5] J. Hashemi, E.Fatemizadeh, "Biometric identification through hand geometry."*The International Conference on Computer as a Tool*, vol. 2, pp. 1011-1014, 2005.

[6] T. Fotak, P. Koruga, M. Baca,"Trends in hand geometry biometrics". *In Central European Conference on Information and Intelligent Systems*, pp. 319-324, 2012.

[7] P. Das, S. Meshram, "An efficient handgeometry system for biometric identifications.*" IOSR Journal of Electronics and Communication Engineering*, vol. 4, no. 4, pp.17-19, 2013.

[8] N. Saxena, V.Saxena, N. Dubey, P. Mishra, "Hand geometry: A new method for Biometric recognition."*International Journal of Soft Computing and Engineering*, vol. 2, no. 6, pp. 192-196, Jan. 2013.

[9] R.C.Bakshe, A.M. Patil, "Hand geometry techniques: A review."*International Journal of Modern Communication Technologies and Research*, vol. 2, no. 11, pp. 14-20, Nov. 2014.

[10] R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos, "Biometric identification through hand geometry measurements."*IEEE Transactions on pattern analysis and machine intelligence*, vol. 22, no. 10, pp. 1168-1171, Oct. 2000.

[11] A.K. Jain, A. Ross, 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

[12] A.K. Jain, N. Duta, "Deformable Matching of Hand for Verification."*IEEE International Conference on Image Processing*, vol. 2, pp.857–861, Oct. 1999.

[13] V. Roy, C. V. Jawahar, "Feature Selection for Hand-Geometry based Person Authentication."*IEEE Transactions on Image Processing*, vol. 17, no. 4, pp. 594-607, 2008.

[14] M.K. Ahuja, A. Singh, "A Survey of Hand Geometry Recognition."*International Journal of Advance Research in Computer Science and Management Studies*, vol. 3, no. 3, pp. 312-318, 2015.

[15] P. Sareen, "Biometrics – Introduction, characteristics, basic techniques, its types and various performance measures." *International Journal of Emerging Research in Management & Technology*, vol. 3, no. 4, pp. 109-119, 2008.

[16] R.S. Choras, M. Choras, "Hand shape geometry and palmprint features for the personal identification."*Proc. of Sixth International Conference on Intelligent Systems Design and Applications, IEEE Explore Press*, vol. 2, pp. 1085-1090, Oct. 2006.

[17] J.J. Fuertes, C.M. Travieso, M.A. Ferrer, and J.B. Alonso, "Intra-modal biometric system using hand-geometry and palmprint texture."*In 44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, pp. 318-322, 2010.

[18] A. Kumar, D.C.M. Wong, H.C. Shen, A.K. Jain, "Personal verification using palmprint and hand geometry biometric."*In proceedings International Conference on Audio-and Video-Based Biometric Person Authentication(AVBPA)*, pp. 668-678, 2003.

[19] V. Kanhangad, A. Kumar, D. Zhang, "Combining 2D and 3D hand geometry features for biometric verification."*In 2009 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp. 39-44, 2009.

[20] B. Mathivanan, V. Palanisamy, S. Selvarajan, "Multi-dimensional hand geometry based biometric verification and recognition system."*International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 7, pp. 348-354, 2012.

[21] C. Oden, A. Ercil, V.T. Yoldoz, H. Kormozotas, B. Buke, "Hand recognition using implicit polynomials and geometric features." *In proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication*, vol. 2091 of Lecture Notes in Computer Science, pp.336–341, June 2001.

[22] E. Yoruk, H. Dutagaci, B. Sankur, B, "Hand biometrics."*Image and vision computing*, vol. 24, no. 5, pp. 483-497, 2006.

[23] G. Boreki, A. Zimmer, "Hand geometry: a new approach for feature extraction."*In proceedings of 4^{th} IEEE Workshop on Automatic Identification Advanced Technologies*, pp. 149-154,Oct. 2005.

[24] G. Seshikala, U. Kulkarni, M.N.Giriprasad, “Biometric Parameters & Palm Print Recognition. *International Journal of Computer Applications*, vol. 46, no. 21, pp. 31-34, May 2012.
[25] S. Ashish, “Design of a hand geometry based recognition system.”*Indian Institute of Technology, Kanpur, Department of Computer Science & Engineering*, M.Sc. Thesis, Jan 2007.
[26] N.A. Ostu, “Threshold Selection Method from Gray-scale Histogram.” *IEEE Transaction on Systems, Man and Cybernetics*, vol. 9, no. 1, pp. 62-66, 1978.
[27] J. Jobin, J. Joseph, Y.A. Sandhya, S.P. Saji, P.L.Deepa, “Palm biometrics recognition and verification system.”*International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 1, no. 2, pp. 41-47, August 2012.
[28] P. Varchol, D. Levicky, “Access security based on biometric.”*In proceedings Research in Telecommunication Technology*, 2006.
[29] Y. Bulatov, S.Jambawalikar, P. Kumar, S.Sethia, “Hand recognition using geometric classifiers.”*In International Conference on Biometric Authentication*, pp. 753-759, July2004.
[30] M. Faundez-Zanuy, G.M.N.Mérida, “Biometric identification by means of hand geometry and a neural net classifier.”*In International Work-Conference on Artificial Neural Networks*, pp. 1172-1179,June 2005.
[31] B. Aghili, H.Sadjedi, “Personal identification/verification by using four fingers.”*In 2010 3rd International Congress on Image and Signal Processing*, vol. 6, pp. 2619-2623, Oct. 2010.
[32] J.M. Guo, C.H. Hsia, Y.F. Liu, J.C. Yu, M.H. Chu, T.N. Le, “Contact-free hand geometry-based identification system.” *Expert Systems with Applications*, vol. 39, no. 14, pp. 11728-11736, 2012.
[33] S. Dey, A.K. Kapoor, “Ethnicity Identification from Hand Dimension: A Study in North India.”*European Journal of Biomedical and Pharmaceutical Sciences*, vol. 5, no. 3, pp. 323-334, 2018.
[34] S. Dey, A.K. Kapoor, “Relevance of Extra Digital Flexion Creases: A Study in North India.”*Journal of Forensic Science and Criminology*, vol. 5, no. 4, pp. 404, 2017.
[35] S. Dey, A.K. Kapoor, “Digit ratio (2D:4D) – A forensic marker for sexual dimorphism in North Indian population.”*Egyptian Journal of Forensic Sciences*, vol. 6, no. 4, pp. 422-428, 2016.