IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 9, Issue.2, February 2021 E-ISSN: 2347-2693

Biometric Finger Knuckleprint based Authentication System using Sobel Edge Detection & Emboss

Sonali Patel[1*], Arun Jhapate[2]

[1, 2]Computer Science & Engineering, Sagar Institute of Research & Technology Bhopal, Madhya Pradesh, India

[*]*Corresponding Author: 11sonalipatel@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v9i2.2328 | Available online at: www.ijcseonline.org

Received: 13/Feb/2021, Accepted: 16/Feb/2021, Published: 28/Feb/2021

***Abstract*—** Researchers are always on the move to innovate something new from their side. Such a work by researchers in the field of biometrics has led to identify the finger knuckle print as a biometric trait with distinct features. There are certain biometric parts such as fingerprint, iris, palm print and now knuckle print. Knuckle contains rich texture that is distinct for each fingers it selves. Knuckle has potential information that can differentiate persons uniquely. System is intended to acquire the knuckle image and process it for data acquisition and generate code map. Code map is a template that localized in database and compare with input code maps. The proposed system is able to extract information from knuckle image with high precision using different kind of filters and image enhancement techniques such as Gabor, Spatial filters and Sobel that facilitate SURF (Speeded Up Robust Feature). Proposed system possess low error rate with zero false recognition recall. If a system has false acceptance rate then the precision does not follow ideal system. System should have zero false acceptance and high false rejection rate along with true acceptance. Precision is based on high quality feature extraction that could be made by some image enhancement techniques that proposed system follows.

***Keywords*—** Knuckle Print, Sobel Edge Detection, SURF, Gabor Filter, Biometric and Binary Localization

I. INTRODUCTION

Finger knuckles can be played as a strong contender among competent features used in biometric system due to its characteristics. Fundamentally, surface of finger knuckle is considered as a unique shape created on the finger joints at their back region of the hands. As there are three phalangeal joints exists on the back region of fingers. Metacarpophalangeal joint is a region where finger joints with the surface of the hands. Proximal Inter Phalangeal (PIP) joint is the section which is considered as the middle joint of a finger. Distal joint is the portion refer to the joint at the tip surface of the finger at the back region. So, the first joint from the tip of the finger is known as Distal joint, middle joint is considered as the Proximal Inter Phalangeal (PIP) joint and the last joint on the finger is known as Metacarpophalangeal joint. The existence of these joints in the back portion of a finger generates shrinks on the outer area of the skin, which forms a cutaneous shape comprising of lines, wrinkles, shapes, etc. So, the shape or pattern formed at the joint of PIP on the finger is taken as the finger knuckle print. Disparate to the finger prints, knuckle patterns are hard to scuffle due to its distillates on the inside surface of the region. Characteristics acquired by the knuckle prints are tremendously inimitable which can be an ideal option for a biometric system [1]. Knuckle print based authentication system is a system where identification is conformed through finger knuckle. Knuckles are having distinct features or textures that can be used for developing a biometric system which is also useful for crime scene investigation where knuckle print found in place of fingerprint. The traditional approach for extracting features from finger knuckle is based on binary patterns.

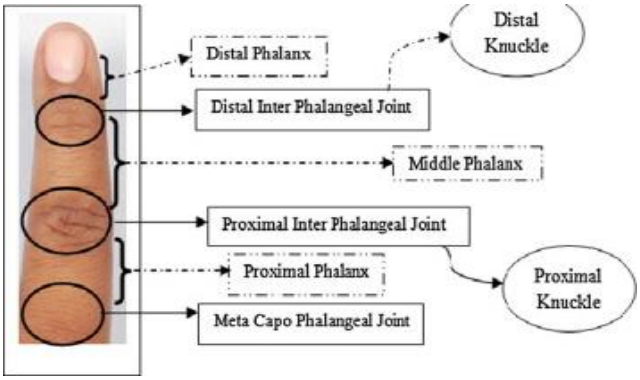


Figure 1. Finger Knuckle Print Sections [1]

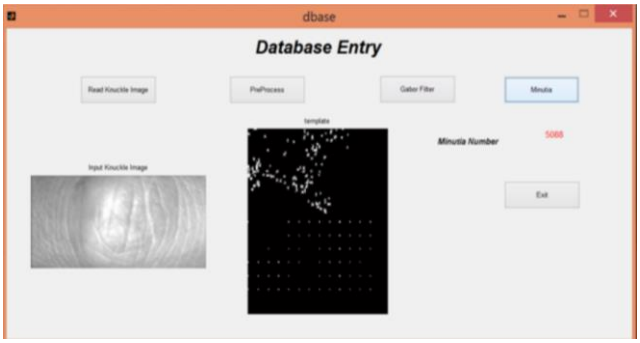


Figure 2. Finger Knuckle Print Authentication System [2]

Fig.2 shows the GUI of finger knuckle print authentication system that prefabricated in previous works.

II. RELATED WORK

Amine AMRAOUI et al. [3] proposed a concept of Compound Local Binary Patterns (CLBP) where patterns are extracted by encoding all corresponding to a neighbor of local neighborhood in order to construct the compound and robust feature. System uses PolyU database for storing binary templates that intended to compare while authentication. Author used distance-based classifier for reducing the computational time. The accuracy trails to 98.71 % for authenticating the legitimate and illegitimate users. Jooyoung Kim et al. [4] proposed a finger knuckle print system based on difference between the images with respect to the Euclidean distance comparison. Here the difference image operation has been performed to enhance the knuckle-print lines on the image matrix. The difference operation has been achieved by shifting the complete image by one to many pixels followed by a subtraction operation between two images. Subsequently, features are extracted by transforming the disparity image into frequency domain using a discrete Fourier transform. Finally, matching is achieved through the Euclidean distance between the extracted features of input image and the stored one. Arulalan. V et al. [5] proposed a combinational biometric system of two traits Iris and Finger knuckle print; it means that the score will be captured on the basis of two distinct features. Here Haar Wavelet has been used for Iris feature extraction and Linear Discriminant Analysis for finger knuckle print. Combining two biometric features do not met the desirable system because single system should be liable to attain the true acceptance and false rejection instead of combining two biometric systems. Two levels verification always return an ideal authentication but the complexity level of attaining the feature become higher and computational time get increases. Farzam Kharaji Nezhadian et al. [6] proposed a system which is based on inner knuckle print instead of outer one. In this system the inner surface of finger has been used authentication that may possess less features or texture. Gabor wavelet filter has been used for enhancing the inner knuckle print and feature extraction has been done using K-Nearest neighbor fuzzy classifier. Forward Feature Selection is an algorithm that pertain scores as per the features matched and return result accordingly. Wavelets are powerful tools that generally used for feature extraction in the field of authentication that deals with horizontal, vertical and diagonal matrix. Inner knuckle print contains very less feature as compare to the outer most knuckle of a finger. E. O. Rodrigues et al. [7] proposed a system which is based on image filter and Similarity measures. It is an edge detection technique that finding edges or lines from finger knuckle and preprocess for noise reduction if it contains. System is intended to capture the knuckle print from folded knuckle that forms less creases or principal lines which results low feature extraction. Wafa El-Tarhouni et al. [8] proposed a system which is based on Local Binary Patterns that measures local binaries value of knuckle print texture and compare with the threshold value. Local Binary Pattern (LBP) is widely used to analyze local texture features of an image. An extension of LBP based texture descriptors has been proposed and focusing on improving noise strengthening using different encoding or threshold plans where the most widely known Median Binary Pattern (MBP), Fuzzy LBP (FLBP), are Local Accurate Pattern (LAP), and Shift LBP (SLBP). LBP based Descriptors rarely apply in Finger-Knock-print (FKP) not recognized and specially, SLBP-based descriptors not yet reported. Iman Sheikh Oveisi et al. [9] proposed a system which is based on Multimodal approach that combines two biometric system i.e. palm print and knuckle print using AdaBoost classifier. AdaBoost classifier is employed to address the problem of restricted number of training data in unimodal systems. System uses Dual Tree-Complex Wavelet Transform (DT-CWT) for feature extraction for both finger knuckle prints as well as palm print. But combining two features raises two biometric level that may consumes computational time as well as the complexity level of acquisition.

III. PROBLEM IDENTIFICATION

Previously proposed system is based on Local Binary Patterns and PolyU database. Since the method uses predefined algorithm which limits the practical implementation of system as slight illumination can affect the accuracy of knuckle print scanner. Binary values may differ on different light occurrence that resulted inaccurate precision. If a single false acceptance made among 1000 of users then system get failed to provide ideal authentication system. Fig.4 shows the binary code representation of an image. Binary code based template matching affects the accuracy directly because of lightness or luminance and does not work with poor image. Local binary pattern has been used by several researchers but do not met desirable accuracy. It is a widely used effect in graphics software, typically to reduce image noise. Less pattern details extracted that possesses less accuracy rate.

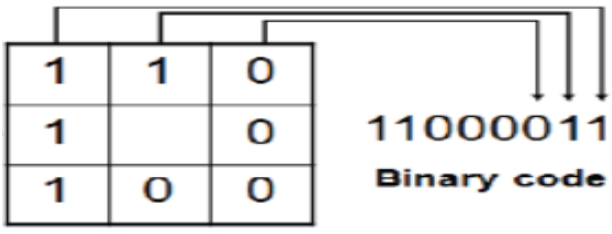


Figure 3. Binary Code Extraction

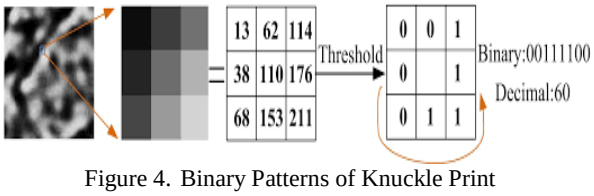


Figure 4. Binary Patterns of Knuckle Print

Fig.5 shows finger knuckle pixel binarization that matches with the templates for feature valuation. A finger knuckle can be affected by luminance that resulted inaccurate authentication. As shown in the Fig.6, a region of finger knuckle represent the gay level with different densities.

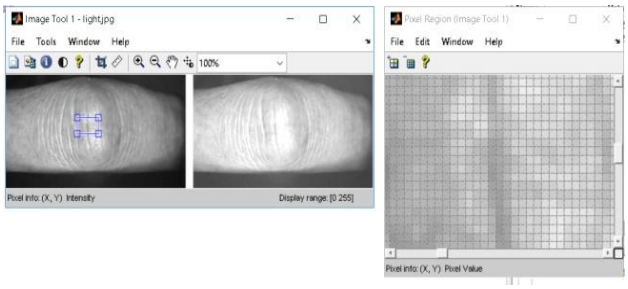


Figure 5. Finger Knuckle gray level Extraction for original knuckle

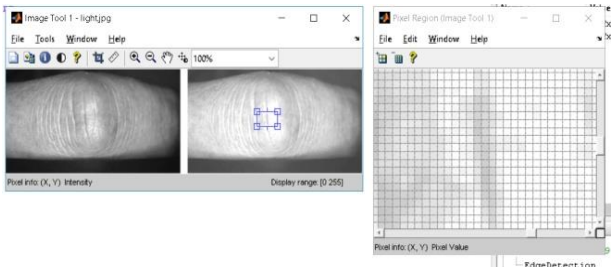


Figure 6. Finger Knuckle gray level Extraction for distinct luminance

IV. PROPOSED WORK AND METHODOLOGY

The proposed system is able to provide better authentication approach towards knuckle print. It acquires user's knuckle in the form of frame and later processes it for feature extraction that can be compared with the stored template. The true acceptance rate of proposed method is bit higher as compare to the earlier implemented system with minimal error rate. The system has been implemented in MATLAB with Sobel Edge Detection that extract feature for matching with templates. Once the feature has been extracted, it matches with the stored templates and if the matching feature is greater than the threshold value or key points; the referential result will be returned with holder's detail. System is capable to return true positive results with minimal false or fake results. System has been tested with many enrollments and system observed as effective biometric authentication system.

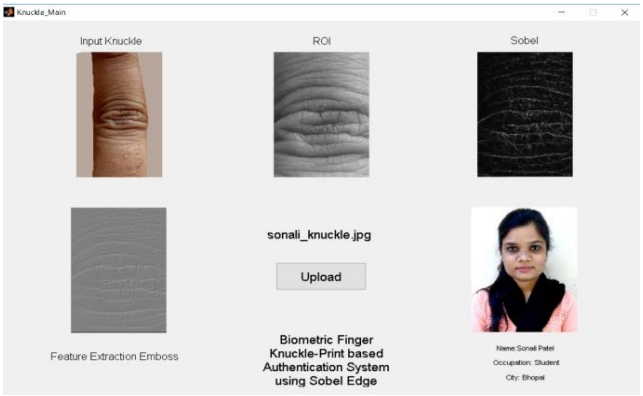


Figure 7. Proposed GUI

Fig. 8 represents the graphical user interface where an authentic user gets accessed with her knuckle image and Fig. 9 is a demonstration of denying illegitimate user. All the images are real and taken manually for better authenticity.

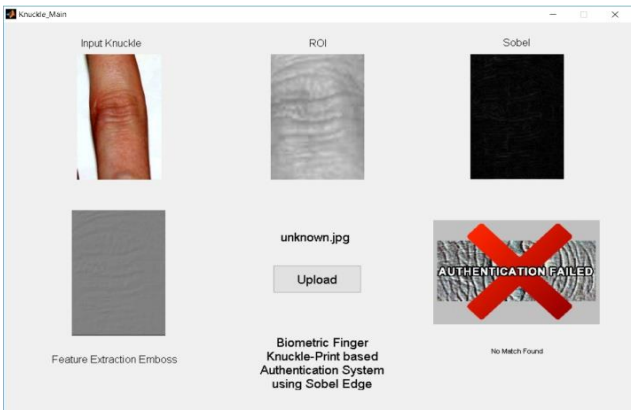


Figure 8. False User Denying

System is capable to reject false user at all that strongly affect the precision of the system. Here the system is based on Sobel Edge Detection with Emboss, sobel extract the features edges and emboss makes it highlight from the background and stored it as feature texture as templates. These templates are stored in the database that later compare with the input one, comparison is based on key points extracted and the amount of key points matched. If key points are greater than the threshold value then it will authenticate the user and if it is less than the threshold value then system will deny the user and score will be printed over the screen. A standard matching amount is 20%, if is stated as if a user may have 20% similar features then he belongs to that feature. If a true user get denied, no causality count but if a false user get accessed then the whole system get failed and error rate shallow the precision.

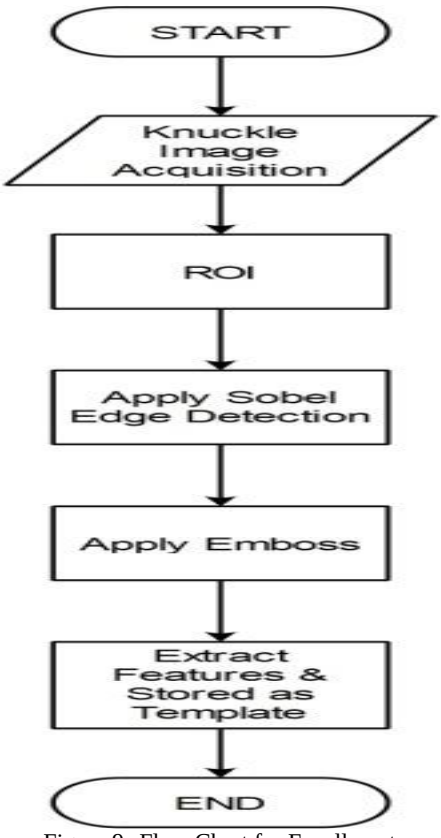


Figure 9. Flow Chart for Enrollment

First of all, an enrollment is required to create feature templates for matching score levels for results. Here in the enrollment phase, first of all a knuckle image has to be captured or acquired, then region of interest has been targeted where the useful information exists. Then sobel is to be applied for detecting edges and after that Emboss the extracted edges that highlight the features and store the features as templates for future matching. These features are stored in database that later comparing with the input knuckle image.

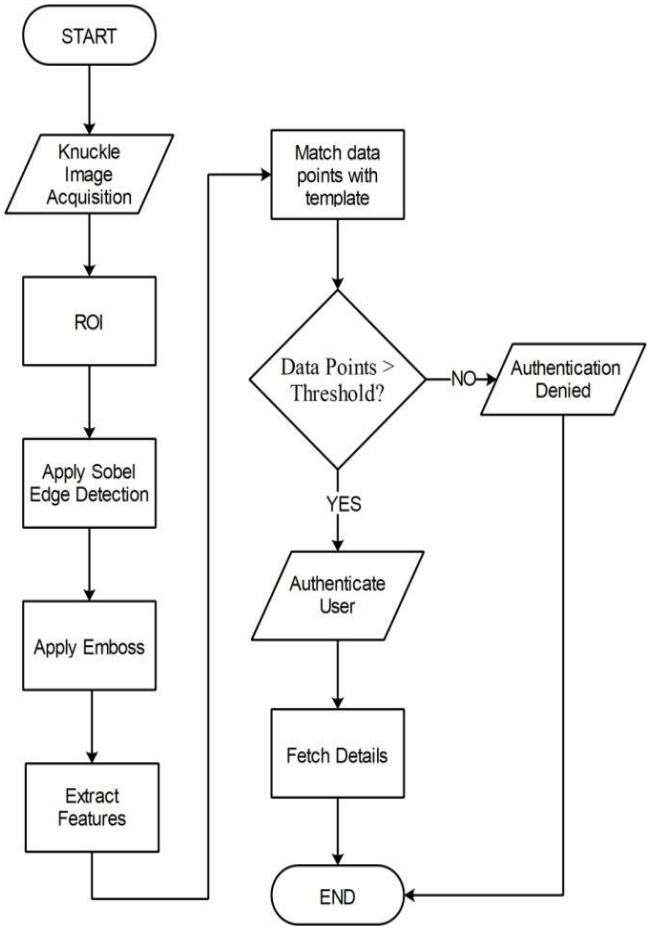


Figure 10. Flow Chart for Authentication

After successful enrollments, authentication is to be checked, for that knuckle image has to be acquired for feature extraction like enrollment phase. First of all a knuckle image has been acquired then ROI targeted then apply Sobel and emboss for feature extraction, once the feature has been extracted then it will compare with the stored templates, the acquired data points are comparing with the stored data points and if it is greater than the threshold value then it will authenticate the user otherwise it will deny the user at all. Threshold is value where a condition has been applied for accepting or rejecting user on the basis of amount of similarities. The Sobel operator, sometimes called the Sobel-Feldman operator or Sobel Filter, is used in image processing and computer vision, especially within the Edge Detection Algorithm where it creates an emphasis on the edges. It is named after Irwin Sobel and Gary Feldman who are co-workers of the Stanford Artificial Intelligence Laboratory (SAIL). Sobel and Feldman presented the idea of an "isotropic 3x3 image gradient operator" in a dialogue in SAIL in 1968. Technically, it is a discrete discrimination operator, computing an estimate of the gradient of the image intensity function. At each point of the image, the result of the Sobel-Feldman operator is either the respective gradient vector or the ideal of this vector. The Sobel-Feldman operator is based on conveying the image in a horizontal and vertical direction with a small, detachable and integer-valuable filter, and therefore is relatively inexpensive in terms of calculations. On the other hand, this gradient produces approximation, it is relatively raw, especially for high-frequency variations in the image.

Figure 11. Sobel Edge Detection [10]

A. ***Edge Magnitude Sobel Emboss Algorithm –***

Require: Horizontal gradient mask G_x, Vertical gradient mask G_y, threshold T, Absolute magnitude G, template F_t

INPUT: A ← 2 dimensional image arrays.
OUTPUT: Gradient ratio for edge detection

Step 1: Acquire the input knuckle image.
Step 2: Function Sobel (A)
G_x = [-1 0 1; -2 0 2; -1 0 1]
G_y = [-1 -2 -1; 0 0 0; 1 2 1]
Step 3: Apply gradient mask G_x and G_y to input image
$S_1 = G_x * A$
$S_2 = G_y * A$
Step 4: Separate mask manipulation for G_x and G_y as S_1 an d S_2 resp.
Step 5: Combine the results to find out the absolute magnit ude of the gradient.

$$|G| = \sqrt{S_1^2 + S_2^2}$$

Step 6: Apply Emboss w.r.t . θ direction-

$$\theta = \begin{pmatrix} 0 & +1 & 0 \\ 0 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

Step 7: Store key points as F_t
Step 8: if $F_t > T$ **then**
Authenticate user;
else
Denying user;
end else
end if
Step 9: End

Here the input is a 2 dimensional image array and output is gradient ratio for edge detection. First of all a knuckle image is to be acquired for further process and once it has been acquired then sobel function will be applied for calculating gradient values. Once the gradient value has been calculated in x and y axis the gradient magnitude is to be calculated. After this, Emboss is applied with θ angle of direction after all this; a feature has been extracted as key points that can be stored in database for future matching. While performing authentication, feature extraction process is similar to the enrollment process. If extracted feature is greater than the threshold value then it will authenticate the user otherwise deny. Similarities are based on key point extracted from input image and the image stored in the database.

V. RESULTS AND DISCUSSION

The result has been analyzed on the basis of true acceptance, true rejection, false acceptance and false rejection. Here the total number of 25 true knuckle image tested that belongs to stored templates. All true users get accessed with true authentication and there is no true rejection at all, similarly 25 false users are also tested for error computation. There are no false users get accessed, all are denied by the system.

Table 1. Result Analysis

Holders	Key points Found	Key points Matched	Score %
1	1070	1070	100%
2	302	302	100%
3	1211	1186	97.93%
4	589	587	99.66%
5	785	781	99.49%
6	799	799	100%
7	877	877	100%
8	1040	1040	100%
9	691	680	98.40%
10	547	547	100%
			Overall = 99.54 %

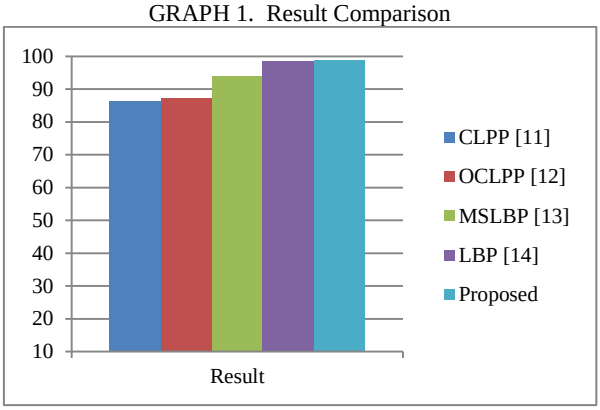
Table I represent the key points extracted from input image and key points that are stored in database. Accuracy is computed on the basis of score level and matching key points.

Table 2. Result Comparison

	Accuracy
CLPP [11]	86.26 %
OCLPP [12]	87.42 %
MSLBP [13]	93.87 %
LBP [14]	98.71%
CGF [15]	99.33 %
Proposed	99.54%

Table II represent the comparison over the last decades researches on knuckle print based authentication system. As per the accuracy computed is higher than the previous one. The accuracy of successful key points matching is 99.03% along with 100% false rejection rate and true acceptance rate as per the samples tested. The accuracy is calculated over the 10 score levels or key points, the ratio for deriving precision is based on key points found on an image and how many key points matched. There is no false acceptance that shows an ideal system with minimal error rate.

GRAPH 1. Result Comparison



Graph I shows the precision comparison among various researches made over biometric knuckle print based authentication system.

VI. CONCLUSION AND FUTURE SCOPE

Thus the currently proposed system is able to recognize knuckle region along with its features that correctly authenticate the user and rejecting the false on. Precision is calculated over the key points matching scores and error rate is computed as per the false acceptance, false rejection, true acceptance and true rejection. So, the accuracy rate of proposed work is 99.54% along with 100% false rejection and true acceptance rate. Sobel Edge Detection and Embossing are liable to acquire the accuracy rate which is bit higher from previous works. Knuckle print based authentication system can be implemented with bit higher precision in future and applicable in various fields of authentication. Knuckle biometric authentication is a touch-less system that allows users to interact without any hygienic disease. This biometric feature cannot be stolen

and no unauthorized users get access. This system can be implemented in various fields that may replaces existing one.

REFERENCES

[1] K.Usha, M.Ezhilarasan, "Fusion of geometric and texture features for finger knuckle surface recognition" , Science Direct, **Volume 55, Issue 1, Pages 683-697, March 2016.**

[2] Neerja Deogaonkar , Harshada Kahar ,Bhagyshri Parab ,Snehal Rajpure , Disha Bhosle, "Biometric Authentication Using Finger Knuckle Print" IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) **Volume 6, Issue 1, Ver. I, PP 55-59. Jan. -Feb. 2016.**

[3] Amine AMRAOUI*, Youssef FAKHRI and Mounir AIT KERROUM, " Finger Knuckle Print Recognition System using Compound Local Binary Pattern", 3rd International Conference on Electrical and Information Technologies **ICEIT'2017**, IEEE.

[4] Jooyoung Kim, Kangrok Oh, Andrew Beng-Jin Teoh and Kar-Ann Toh, "Finger-Knuckle-Print for Identity Verification Based on Difference Images" **2016** IEEE 11th Conference on Industrial Electronics and Applications (ICIEA).

[5] Arulalan. V and Dr. K.Suresh Joseph, "Score Level Fusion of Iris and Finger Knuckle Print", 2016 10th International Conference on Intelligent Systems and Control (ISCO), IEEE.

[6] FarzamKharajiNezhadian and Saeid Rashidi, "Inner-knuckle-print for human authentication by using ring and middle fingers", ICSPIS 2016, **14-15 Dec. 2016,** Amirkabir University of Technology, Tehran, Iran, IEEE.

[7] E. O. Rodrigues, T. M. Porcino, A. Conci and A. C. Silvah, "A simple approach for biometrics: Finger-knuckle prints recognition based on a Sobel filter and similarity measures," 2016 International Conference on Systems, Signals and Image Processing (IWSSIP), Bratislava, **pp. 1-4, 2016.**

[8] Wafa El-Tarhouni1, Larbi Boubchir2 and Ahmed Bouridane1, "Finger-Knuckle-Print Recognition Using Dynamic Thresholds Completed Local Binary Pattern Descriptor", 2016 39th International Conference on Telecommunications and Signal Processing (TSP), IEEE.

[9] I. S. Oveisi and M. Modarresi, "A feature level multimodal approach for palmprint and knuckleprint recognition using AdaBoost classifier," 2015 International Conference and Workshop on Computing and Communication (IEMCON), Vancouver, BC, **pp. 1-7, 2015.**

[10] Steve, https://blogs.mathworks.com/steve/2016/05/16/image-binarization-new-r2016a-functions/, Published on **April 16th, 2016.**

[11] D. Zhang, and M. S. Kamel, "An analysis of iriscode," IEEE transactions on image processing, **vol. 19, no. 2, pp. 522–532, 2010.**

[12] S. Agarwal and P. Gupta, "Identification of human through palmprint: A review," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), **vol. 1, no. 10, pp. pp–19, 2012.**

[13] X.-Y. Jing and D. Zhang, "A face and palmprint recognition approach based on discriminant dct feature extraction," IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), **vol. 34, no. 6, pp. 2405–2415, 2004.**

[14] D. Zhang, Z. Guo, G. Lu, L. Zhang, and W. Zuo, "An online system of multispectral palmprint verification," IEEE transactions on instrumentation and measurement, **vol. 59, no. 2, pp. 480–490, 2010.**

[15] Nigam, Aditya & Gupta, Phalguni. (2016). Finger-Knuckle-Print ROI Extraction using Curvature Gabor Filter for Human Authentication. 364-371. 10.5220/0005724103640371.

[16] W. K. Kong, D. Zhang, and W. Li, "Palmprint feature extraction using 2-d gabor filters," Pattern recognition, **vol. 36, no. 10, pp. 2339–2347, 2003.**

[17] D. I. Devi and B. T. G. Sampantham, "An efficient security system based on gabor feature detector," in Control, Automation, Communication and Energy Conservation, 2009. INCACEC 2009. 2009 International Conference on, **pp. 1–6, IEEE, 2009.**

[18] W. Li, D. Zhang, and Z. Xu, "Image alignment based on invariant features for palmprint identification," Signal Processing: Image Communication, **vol. 18, no. 5, pp. 373–379, 2003.**

[19] W. Jia, R.-X. Hu, J. Gui, Y. Zhao, and X.-M. Ren, "Palmprint recognition cross different devices," Sensors, **vol. 12, no. 6, pp. 7938–7964, 2012.**

[20] D. Zhang, V. Kanhangad, N. Luo, and A. Kumar, "Robust palmprint verification using 2d and 3d features," Pattern Recognition, **vol. 43, no. 1, pp. 358–368, 2010.**

[21] K. Krishneswari and S. Arumugam, "A review on palm print verification system," International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM) ISSN, **pp. 2150–7988, 2010.**

[22] Z. Guo, W. Zuo, L. Zhang, and D. Zhang, "Palmprint verification using consistent orientation coding," in Image Processing (ICIP), 2009 16th IEEE International Conference on, **pp. 1985–1988, IEEE, 2009.**

[23] W. Li, B. Zhang, L. Zhang, and J. Yan, "Principal line-based alignment refinement for palmprint recognition," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), **vol. 42, no. 6, pp. 1491–1499, 2012.**

[24] M. Mu, Q. Ruan, and Y. Shen, "Palmprint recognition based on discriminative local binary patterns statistic feature," in Signal Acquisition and Processing, 2010. ICSAP'10. International Conference on, **pp. 193–197, IEEE, 2010.**

[25] S.S. Khot, V.A. Mane and K.P. Paradeshi, "Real Time Palm print Identification Technique-Effective Biometric Identification Technique", International Journal of Societal Applications of Computer Science, **Vol. 1, Issue 1, November 2012.**

[26] Wenxin Li, David Zhang and Zhuoqun Xu, "Image alignment based on invariant features for Palm print identification", Signal Processing: Image Communication, **Vol. 18, pp. 373-379, 2003.**

[27] Wei Jia, Rong-Xiang Hu, Jie Gui, Yang Zhao and Xiao-Ming Ren, "Palm print Recognition across Different Devices", Sensors, ISSN: 1424-8220, **Vol. 12, pp. 7938-7964, 2012.**

[28] David Zhang, Vivek Kanhangad, Nan Luo and Ajay Kumar, "Robust Palm print Verification Using 2D and 3D Features", Pattern Recognition, **Vol. 43, No. 1, pp. 358-368, January 2010.**

[29] K. Krishneswari and S. Arumugam, "A Review on Palm Print Verification System", International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM), ISSN: 2150-7988 **Vol. 2, pp. 113–120, 2010.**

