Haitham Salman Chyad *et al*, International Journal of Computer Science and Mobile Applications,
Vol.10 Issue. 7, July- 2022, pg. 8-15 **ISSN: 2321-8363**
Impact Factor: 6.308
(An Open Accessible, Fully Refereed and Peer Reviewed Journal)

Subject Review: Palm Print Biometric Authentication System for Security Applications

Haitham Salman Chyad[1]; Raniah Ali Mustafa[2]
[1,2]Computer Science Department, Collage of Education, Mustansiriyah University, Baghdad, Iraq
dr.haitham@uomustansiriyah.edu.iq
rania83computer@uomustansiriyah.edu.iq

DOI: 10.5281/zenodo.6874686

Abstract
Biometric authentication offers an authoritative and accurate approach in access control to identifying or verifying the identity of the individual using the system, through their behavioural and physical traits such as palm print, face, finger print, voice, iris etc. The field of Security, Forensics, and Banking pays great attention to biometrics. Individual traits cannot be forget or missing as compared passwords to and keys. They are also being much complicated to copy. For this reason biometric security systems are considered to be safer and very secure than conventional security systems. But every trait has its own disadvantages and advantages. In this paper, we propose a detailed background review for several techniques, methods and approaches used in the palm print authentication system with many various methods and procedures. A comparison of these security application technologies (dataset, pre-processing, feature extraction, Authentication/ security applications techniques and result) is also presented.

Keywords: Palm print, Feature Extraction (FA), Region of interest (ROI), Authentication, security applications, Gaussian Distribution (GD), Euclidian distances (ED).

1. Introduction
Personal security and authentication are increasingly important in applications like access control (cc), banking, issuance of visas etc. Biometrics rely on authentication is emerging as a mentor to the fore due to its ingrained presence and increased thoroughness. Biometrics is the measuring of a person's physiological characteristics like their iris, palmprints, fingerprints, etc., and/or behavioral characteristics such as their keystrokes, gait etc., in order to identify them (Pankanti, Bolle, & Jain ,2000). Biometrics researchers work on most of those characteristics and their combinations to low error rates, augmentation thoroughness, and lower cost to attain comprehensive performance improvements (Jain, Ross & Pankanti, 2006). In recent years, there has been an increasing important of biometric security and palmprint recognition solutions. As biometrics technology is still relatively new, it looks promising. Referring to the authoritative and precise person recognition, palm prints (palm's inner superficies) carry several identifying similarity traits. Similar to fingerprints, palm prints have always distinctive traits, detailed patterns of valleys and ridges, minutiae, as well as high-resolution images (over1000 dpi) (Zhang, Zuo, & Yue,2012; Mandeel, Ahmad, & Anwar ,2019; Al-Nima, Al-Ridha &Abdulraheem,2019).

In recent years, scientists have begun to utilize palmprint information to identify a person and authenticate a person. Several researches are presented in the palmprint such as enhancement, segmentation, feature extraction (FE) and matching. The palmprint processing is categorized under biometrics, pattern matching, and image processing. There are many biometrics obtainable in the humans. Such as retina features, palmprint, facial features, fingerprint etc. Fingerprints are generally utilized in mobile phones, laptops, and other security applications to identify people and authenticate. The retina matching and face matching are still begin researched and utilized in a few applications. The success rate of retina and face based on security systems are less in precision and the hardware costs higher.

Among every these biometric authentication schemes, the palmprint is the simplest and easiest to handle. A palmprint can be captured utilizing any simple camera. Currently every mobile phone that have built-in camera. Palmprint can be obtained with the assist of mobile phone camera without physical interaction from a person. The palmprint is unique from individual to individual and from hand to hand. Palm print plays a significant role in the security systems of the future (Chandran,2015)

2. Literature Survey

In the past last few years, several techniques and methods related to the biometric authentication system for palm prints has been proposed. In this section, some of these techniques will be discussed.

Mohamed A. El-Sayed (El-Sayed, 2015) Suggested a multi-modal authentication technicality rely on palmprint utilizing Shannon and Tsallis entropies. The first stage, we presented a biometric authentication technicality. The characteristics of palm veins/ palm print are utilized to augmentation the precision of security authentication in this scheme. Where the suggested approach for techniques to identifying verification. Tsallis q coefficient could be utilized as an amenable value and could play a significant part as a tuning parameter in the image processing concatenation for the similar class of images. We utilized in the suggested technique, the characteristics of the kinds of entropy in following stage.

Deepika, C. L. and et al. (Deepika et al., 2010) Suggested palmprint verification scheme utilizing two dimensions Legendre moments (LM) are described as a linear combination of geometric moment invariants (GMI) that non-uniform scaling, rotation and invariant to translation. The improved Legendre moments are utilized for feature extraction (FE) and the weighted fusion method is utilized to integrate the matching results of the sub-images. The results gained utilizing a Baye's classifier elucidate an impressive prognosis precision of (98%), validating the select of lower arranging Legendre moment for efficient palmprint verification.

Mustafa, R. A. and et al. (Mustafa et al., 2021) Proposed a novel palm print recognition system rely on a harmony search algorithm (HAS) where the Gaussian Distribution (GD) is used to compute the distance. First stage in this system is preprocessing, where includes the segmentation, the region of interest (ROI) of the palmprint has been cut. Second stage in this system is to extract features of the palm print images using the harmony search algorithm (HSA) utilizing several parameters of the harmony search algorithm (HSA). Final stage in this system using is Gaussian Distribution (GD) to compute the distance among features to recognize the palm print images of individuals. The system utilizing palmprint databases was obtained through the Hong Kong Polytechnic University (HKPU) and the results showed that the proposed recognition system for palm print achieved a recognition rate of reach 92.60%.

Awate and Dixit (Awate & Dixit, 2015) Conducted a study to identify to user depended on unique biological feature. The proposed system has achieved an excellent level of security for the users and the scheme also achieved authentication in the least possible time. The results showed that the proposed system for palm print images recognition obtains of high accuracy up to 99 % and a precision of 91% also a high sensitiveness of 76 % and a specificity of 99 %.

Li, H., and L. Wang (Li & Wang, 2012) Suggested a cancelable palmprint authentication scheme rely on chaotic stream cipher (CSC). Firstly, a new two dimension anisotropic filter (AF) is utilized to obtain binary direction co-occurrence vector (BOCV, that can effectively apply in various directions for a local region of palmprint images. After that the binary encrypt the palmprint images through a chaotic stream cipher rely on feedforward–feedback nonlinear dynamic filter (FFNDF) to generate the feature for cancelable palmprint, which has huge re-issuance efficiency and could be performed very rapid for actual implementations. It also has best robustness--- even in the robbed-symbol issue, the result only iterates to the real achievement without lost in achievement and it could still performed state-of-the-art authentication precision, i.e., the EER is 0.07%. The experiments with on PolyU palmprint database emphasize the efficiency of the suggested scheme.

Bhasker Dappuri (Dappuri et al., 2020) Implemented a novel palm print identification scheme based on a hybrid model by utilizing a morphological process for elimination from region of interest (ROI) and utilize an un-decimed biorthogonal wavelet (UDBW) to utilized to extract low level features (LLF) that have been utilized to make feature vector (FV). The implemented model achieved accuracy 100% for many test images acquisition in real time environment.

Indu Priya and et al. (Priya et al., 2019) Presents an efficient scheme for presenting similarities of right and left palmprint along with the integrated image of right and left palmprint by utilize the Principle Component Analysis (PCA), Set Partitioning in Hierarchical Trees (SPHIT) and MDC. Palmprint is promising biometric feature for utilize in forensic and access control applications. However, for feature extraction (FE) and recognition, most of present schemes are making utilize of two-dimension image, that could be easily forged rather than three-dimension palmprints are more competitive in anti-counterfeiting. In these three-dimension images data is taken. It is than converted into two-dimension images in preprocessed and fused. By this system, a two-dimension palm print database is established, and verification identification experiments are performed. This method is more efficient, faster, and accurate. The palmprint recognition scheme suggests a 70% achievement for our database

Tamije Selvy and et al. (Selvy et al., 2017) Implementation of the palmprint recognition scheme. The scheme uses Gray level co-occurrence matrix (GLCM) to extract the characteristics for palm print images as it uses the orientation features and also comprise second order features like homogeneity, contrast, energy and correlation for recognition and comparative. The support vector machine (SVM) for recognition. The CASIA database (version2) used in this suggested scheme. Whereas experiments executed on the dataset demonstration that the proposed technique gives best results than the existent orientation techniques. The suggested technique enhances the accuracy and also it minimizes the average error rate (AER) in recognition.

Jong-Hyuk and et al. (Im et al., 2016) Suggested a palm print authentication system. The suggested scheme extracts data for palm print images and then stores it in a distant server in an encrypting form. The method used to compute the likeness of user input to the recorded biometric data is the RP technique and homomorphic encryption (HE). The performance of the suggested scheme was evaluated with an application on an i7- rely server and android (smartphone).

Hossein Javidnia and et al. (Javidnia et al., 2015) Conducted a study on the potential of biometrics embedded in smartphone authentication schems as a way to improve cyber security. Palmprint authentication is authoritative and could be utilized on each smartphone, provides it has a posterior camera. The study suggested as solutions to the hand segmentation phase, suggested color thresholding and compared the results. Initial method, the YCbCr color space is utilized to evaluation the allocation of the skin pixels in the central point of the image and then force that period on the full Cb and Cr channels. Other skin detection methods comprise the utilize of the HSI color spaces, that explore various methods of representing color information. Then, Harris

corner detection technique utilized to detect the central part of the hand and the ROI extracting rely the calculated point.

S. M. Prasad and et al. (Prasad et al., 2009) Suggested palmprint authentication system based on fusion of Wavelet. The system suggested a new method for feature extraction. Modernity lies in the extraction of two distinguishing features, where (dominant wrinkles and principal lines) and energy characteristics utilizing the same wavelet decomposition of the palmprint region of interest (ROI).Experimental showed that the integrate of these characteristics could minimize the EER significantly through (39.38%) at minimum computational encumbrance. Integrate obtained a comprehensive EER of 1.37, that is superior to the precision performances of another state of the art wavelet rely on and fusion relies on approaches. This showed the efficiency of our system. Estimation the suggested system on huge database with more number of testing experiments, in order to as assured the appropriateness of the suggested approach for huge population covering.

Pallavi D. Deshpande and et al. (Deshpande et al., 2016) Presented a multimodal biometric identification scheme rely on the integrate of palm vein and palm print of the hand. The scheme passes three modules. The first module pre-processing for hand images. The second module is extracted the features for palm print through utilizing wavelet decomposition technique and extracted features for palm vein utilizing matched filter technique. Final module is utilized separate matcher for recognition. Decisions that are gained through both the matchers are rationally ANDed jointly to recognized the individual. Module one presentes 96% precision with zero FAR. The next module, a rough-to-fine hierarchical feature matching is done for effective hand recognition. Module two presentes 97.25% precision with very lower FAR.

Arulalan and et al. (Arulalan et al., 2016) Suggested a new idea, the main idea is to encrypt digital documents generated by a multimodal biometric scheme through the use of a 256-bit cryptographic key. The scheme uses two biometrics (Fingerprint and Palmprint) as traits. The feature was extracted for both biometrics by merging at the characteristic level. Biometric rely on cryptographic key is unpredictable to a meddler as the meddler lacks the knowing of physical characteristics of the user. In this suggested scheme is achieved the integrity, availability techniques and confidentiality. Biometric rely on cryptographic security could be merging to e-health and e-governance for effective management.

Ankit Kumar (Kumar et al., 2020) presented the zero-bit watermarking approach for palm-print image. Much work has already been done with regard to iris and fingerprint and troubling concerns are growing. Essential seniority of accepting novel data set confers us to figure out new and privileged characteristics of palmprint that restriction on unauthorized access. The digital pattern is acquired of unrivalled characteristics of the palmprint image without causing any deformation on it. In this approach uses SVD and DWT for the investigation of zero watermarking since this technique is much essential inversion to diversified image processing menace. The features of palmprint are unrivalled, so the duality of data is extirpated through this suggested technique.

Lu Leng and et al. (Leng et al., 2013) suggested as a reversible multimodal biometric is the Conjugate two dimension PalmHash Code (CTDPHC), which was generated by two dimension PalmHash Codes (2DPHCs). To define the appropriate fusion technique of 2DPHCs of palmvein/ palmprint, diverse fusion rules at score level are comparative and explained. Comparative with 2DPHC, CTDPHC relishes high-verification precision and stronger anti counterfeit efficiency, while trades neither computational complication nor storage cost.

3. Comparison of Systems

Table 1 demonstrates the comparison of prior research studies based on the study of the dataset, pre-processing, feature extraction and authentication, security applications techniques used in study, and results.

Table 1: Comparison of previous research studies

Reference	Dataset	Pre-processing	Feature Extraction	Authentication/ security applications techniques	Result
(El-Sayed, 2015)	Collected images for 30 individuals, palm vein images & utilizing "M2-PalmVein™ Reader"	enhancement Image, insert salt and pepper noise with various factors like : 0.01, 0.1, and 1 % noise, different noises utilizing the filters (Speckle, Pepper & Salt, and Gaussian) with 1% , 2% , and 3%	Statistical Features Set (SFS) such as ("Mean, Variance, Smoothness, Skewness, Kurtosis, Uniformity, and Entropy")	Shannon & Tsallis entropies	recognition rates (99.4 %)
(Deepika et al., 2010)	PolyU palmprint database	ROI Extraction (Gaussian smoothing, Binary image, calculate the centroid of an palmprint,…), Contrast enhancement (histogram equalization)	Legendre Moments	Bayes Net or Bayesian Belief Networks (BBN)	accuracy of 98%
(Mustafa et al., 2021)	the Hong Kong Polytechnic University (HKPU), college of engineering pune (COEP)	(segmentation, ROI image) & edge detector (Kirsch filter))	Harmony Search Algorithm (HS)	Gaussian Distribution (GD)	rate of recognition 92.60%
(Awate & Dixit, 2015)	PolyU palmprint database	draw rectangle on palm, Canny edge detection, Max Circle in Palm Print,	Stockwell transform	Support Vector Machine (SVM)	accuracy of 99% and precision 91%
(Li & Wang, 2012)	PolyU Database(DB)		anisotropic filter(AF) is create on Gaussian functions (GF)	cancelable BOCV code & the BOCV Code & chaotic stream cipher (CSC) rely on the FFNDF by specific OR process, Hamming distance (HD)	precision, i.e., the EER is 0.07%.
(Dappuri et al., 2020)	a chimeric multimodal database	region of interest (ROI), distance transform	3-level UDBW transform, relevant features (FV)	Euclidean distance	100% accuracy

(Priya et al., 2019)	criminal database	Gray scale conversion& Image Resize& Image enhancement (Histogram equalization (HE) & Noise elimination utilizing & wiener filter &Linear contrast modification, Median filtering (MF)& Unsharp mask filtering& Contrast-limited adaptive histogram equalization(CLAHE))	SPIHT(Set Partitioning in Hierarchical Trees) algorithm, discrete wavelet transform (DWT), PCA(Principle Component Analysis) & MDC (Minimum Distance Classifier) extracted feature	comparing the between the test image with the save database.	70% achievement
(Selvy et al., 2017)	CASIA database (version2)	Input image of Hand ,Obtain Binary hand image from the Input, Extracted Palm print Image, Palm print Image in Gray scale density Format	energy, correlation, contrast, homogeneity & (GLCM)	Support vector machine (SVM)	99.95%
(Im et al., 2016)	Collected images from smartphone	region of interest (ROI image)	RP technique is utilizied to extract a biometric feature vector (FV)	homomorphic encryption, Euclidean distance	
(Javidnia et al., 2015)		Harris Corner Detection & Central Point, region of interest & Extracted ROI & LBP Pattern descriptor & SIFT Descriptors	LBP & SIFT Features	matching using SIFT	
(Prasad et al., 2009)	PolyU online palmprint database	Segmentation& location of invariant points& alignment and extracting of ROI	discrete wavelet transform (DWT), HVD subbands, Line feature extraction, Fusion Strategy	score level (create sum rule & rule) fusion	39.38%
(Deshpande et al., 2016)	Collected images (Logitech C310 webcam (5MP))	Enhanced Palm Print Images, Enhanced Palm Veins	wavelet decomposition technique	Euclidean distance	Module one presentes (96%) precision, Module two presentes (97.25%) precision

(Arulalan et al., 2016)	IITD Touchless Palmprint	ROI of Palmprint	two dimension Gabor filter, Fourier transform	k-bit cryptographic key is generated from multimodal biometric template BT	97.78%
(Kumar et al., 2020)	IIT Delhi palm-print	Normalize for the palm-print, Watermark ID	divide LL wavelet band into non collapsing equivalent size blocks and SVD is practiced on every block.	Match primary singular values of every fix-size block to generate 'tm' matrix, Arnold Cat map (ACM)	
(Leng et al., 2013)		color ROI, gray ROI,	2DPHCs of palmprint along four θτ, 2DPHCs of palmvein along four θτ	Two-DPHC, CTDPHC, convenient CTDPHC	

4. Conclusion

In this review study, we highlighted a major works discussion of the different methods used in the authentication system for palm print based security applications for the period 2009 to 2021. Individual authentication plays an important role in the forensic, access control, public security and e-banking. The palmprint of individual person differs in patterns and size and thickness of valleys and ridges. The palmprint of person from different ethnical groups differs. Palm print recognition has been recognized as an efficient biometric identifier due it is more authoritative and user friendly. This study uses authentication system for palm print based security applications. In this study is focusing through use better dataset, where the systems pass many phase such as pre-processing, feature extraction, Authentication/ security applications techniques. Those systems of authentication are thoroughly investigated and analysed in order to improvement the authentication and recognition efficiency by extract features best for region of interest (ROI) and to ensure Efficiency performance also an algorithm for compressing the large database of palmprints has to be advanced and the database of the feature vectors (FV) have to be coded to provide a simpler database structure to minimize the complexity in computations. Today, novel authentication and recognition are being developed on a daily basis, and the newly, proposed authentication system for palm print based security applications has increased security. Each technology has a set of advantages and disadvantages; thus, novel technologies are becoming more and more advanced.

References

[1] Pankanti, S., R. M. Bolle, & A. Jain ,2000, Biometrics: The future of identification [guest eeditors' introduction], Computer, 33(2): 46-49.
[2] Jain, A. K., A. Ross, & S. Pankanti, 2006, Biometrics: a tool for information security, IEEE transactions on information forensics and security, 1(2): 125-143.
[3] Zhang, D., W. Zuo, & F. Yue,2012, A comparative study of palmprint recognition algorithms, ACM computing surveys (CSUR), 44(1): 1-37.
[4] Mandeel, T. H., M. I. Ahmad, & S. A. Anwar ,2019, A multi-instance multi-sample palmprint identification system, Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 13(2): 825-830.
[5] Al-Nima, R. R., M. Y. Al-Ridha, & F. H. Abdulraheem, 2019, Regenerating face images from multi-spectral palm images using multiple fusion methods, TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(6): 3110-3119.
[6] Chandran, S. ,2015, Touchless Palmprint Authentication System Using Harris Operator, paper presented at International Conference on IT, Architecture and Mechanical Engineering (ICITAME'2015) May.

[7] Mohamed A. El-Sayed, 2015, Proposed System of Biometric Authentication Using Palm Print/Veins with Tsallis Entropy, International Journal of Computer Science And Technology, 6(2): 9-14.
[8] Deepika, C. L., A. Kandaswamy, C. Vimal, & B. Satish,2010, Palmprint authentication using modified legendre moments, Procedia Computer Science, 2, 164-172.
[9] Mustafa, R. A., H. S. Chyad, & R. A. Haleot 2021, Palm print recognition based on harmony search algorithm, International Journal of Electrical & Computer Engineering, 11(5) :2088-8708.
[10] Awate, I., and B. Dixit ,2015, Palm print based person identification, paper presented at 2015 International Conference on Computing Communication Control and Automation, IEEE.
[11] Li, H., & L. Wang ,2012, Chaos-based cancelable palmprint authentication system, Procedia Engineering, 29, 1239-1245.
[12] Dappuri, B., V. Srija, & B. Dhanne ,2020, Palm print Biometric Authentication System for Security Applications, paper presented at IOP Conference Series: Materials Science and Engineering, IOP Publishing.
[13] Priya, N. I., K. Y. Reddy, M. Rishika, K. K. Reddy, S. Senbagakuzhalvaimozhi, & R. Partheepan, 2019, PALMPRINT RECOGNITION FOR HIGH SECURITY, 14(6):185-191.
[14] Selvy, P. T., A. Anjugam, & P. A. Begum, 2017, Authentication Using Palm Print Recognition System, International Journal of Engineering Development and Research, 5(1):642-646.
[15] Im, J.-H., J. Choi, D. Nyang, & M.-K. Lee ,2016, Privacy-preserving palm print authentication using homomorphic encryption, paper presented at 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), IEEE.
[16] Javidnia, H., A. Ungureanu, and P. Corcoran, 2015, Palm-print recognition for authentication on smartphones, paper presented at 2015 IEEE International Symposium on Technology and Society (ISTAS), IEEE.
[17] Prasad, S., V. Govindan, and P. Sathidevi, 2009, Palmprint authentication using fusion of wavelet based representations, paper presented at 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC), IEEE.
[18] Deshpande, P. D., A. S. Tavildar, Y. H. Dandwate, & E. Shah, 2016, Fusion of dorsal palm vein and palm print modalities for higher security applications, paper presented at 2016 Conference on Advances in Signal Processing (CASP), IEEE.
[19] Arulalan, V., K. S. Joseph, & V. Premanand ,2016, Securing digital data using 256-bit multimodal biometrics based cryptographic key, paper presented at 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), IEEE.
[20] Kumar, A., A. Dwivedi, & M. K. Dutta, 2020, A zero watermarking approach for biometric image security, paper presented at 2020 International Conference on Contemporary Computing and Applications (IC3A), IEEE.
[21] Leng, L., M. Li, & A. B. J. Teoh, 2013, Conjugate 2DPalmHash code for secure palm-print-vein verification, paper presented at 2013 6th International congress on image and signal processing (CISP), IEEE.

