Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 1, January 2021, pp. 224~232
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v21.i1.pp224-232

Intelligent multimodal identification system based on local feature fusion between iris and finger vein

Enas Abbas Abed, Rana jassim mohammed, Dhafer Taha Shihab
Departmet of Computer Engineering, University of Diyala, Diyala, Iraq

Article Info

Article history:

Received Apr 3, 2020
Revised Jul 8, 2020
Accepted Jul 30, 2020

Keywords:

Finger vein identification system
Iris identification system
Multi-model biocentric system
Pattern recognition
SIFT

ABSTRACT

Biometric identification systems, which use physical features to check a person's identity, ensure much higher security than password and number systems. Biometric features such as the face or a fingerprint can be stored on a microchip in a credit card, for example. A single modal biometric identification system fails to extract enough features for identification. Another disadvantage of using only one feature is not always readable. In this article, a smart multimodal biometric verification model for identifying and verifying a person's identity is recommended based on artificial intelligence methods. The proposed model is identified the iris and finger vein unique patterns each individual to overcome many challenges such as identity fraud, poor image quality, noise, and instability of the surrounding environment. Several experiments were performed on a dataset containing 50 people by using many matching methods. The results of the proposed model were provided a higher accuracy of 98%, with FAR and FRR of 0.0015% and 0.025%, respectively.

Corresponding Author:

Enas Abbas Abed
Departmet of Computer Engineering
University of Diyala
Diyala, Iraq
Email: enasabbas1111@gmail.com

1. INTRODUCTION

There are four general methods used to identify people through different systems and can be used through single system or combined system. The first method is the traditional method in which a person relies on his memory, such as a username and password, personal identification number, or answers to some questions. In this way, there are many challenges and faults, such as being stolen or forgotten. The second method, which depends on something the person owns, such as smart cards or keys, etc., but it also faces many challenges and problems such as theft, damage or counterfeiting [1]. Now, there are modern methods that depend on the biometric and vital measurements of a person that any person possesses and cannot be easily counterfeited, stolen or forgotten. The contributions in this article are divided into four main categories and can be summarized as follows:

a) Smart multi-modal identification system is proposed and tested in various environment settings
b) Effective preprocessing and segmentation techniques are used to overcome the noise and poor-quality images.
c) Smart and fast extracting and selecting features algorithm (Fast-SIFT) is used to select distinct features among samples.
d) Hamming distance as template matching algorithm and support vector machine (SVM) is used in final process to accept or reject the user in identification process.

Now, there are modern methods that depend on the biometric and vital measurements of a person that any person possesses and cannot be easily counterfeited, stolen or forgotten. There are many problems and challenges in the traditional and modern identification types that we will overcome in this article. These challenges are discussed as the following: Traditional identification models such as username and password and can be easily counterfeited, stolen or forgotten. Modern single biometric identification model fails to extract enough features for identification and verification. In single biometric models cannot individually extract unique and distinctive patterns that characterize people. Also, it is not sufficiently accurate, as it can increase the percentage of false rejection of a genuine person or false acceptance of an impostor person. Our proposed model contains two main operations, namely the enrollment process and the identification process. Firstly, the enrollment or registration operation is divided into four sub-processes. The first subprocess is taking a sample from the person using some types of sensors and this sample is often an image of the fingerprint or iris. The second sub-process is the preprocessing stage, in which the problems of sample quality and noise treatment are overcome. The third sub-process is extracting and selecting the distinctive patterns of the person via using the extraction and selecting algorithms such as scale invariant feature transform (SIFT), speedup robust feature (SURF), fast SIFT [2], principal component analysis SIFT (PCA-SIFT), canny edge detection, etc. The final sub-process is storing these selected features in the database. Secondly, the identification process, which is a process that also contains sub-processes such as taking a sample and matching it with the sample stored in the database. This operation is similar to the registration process, but instead of storing the sample, it works to match it with the sample previously stored [3–5]. This article is formed in the subsequent parts. A survey of the previous related works was in part II. The proposed framework has been described in detail in part III. Test results and performance analysis were discussed in part IV. Finally, the conclusions were presented in part V.

2. LITERATURE REVIEW

In any biological scheme, especially in biometrics, the individual biological characteristics of each person are stored in a template and then the template presented in the identification process is compared to the template stored before that. Therefore, not every biological measure is a biometric measure unless it contains some important properties such as universality (UV), distinctiveness (UQ), permanence (PM), and vulnerability. Universality factor (UV) means that this type of biometrics can be applied to all users. Uniqueness factor (UQ) means that any two people cannot have or possess the same patterns for these biometric measurements. Permanence factor (PM) means that this type of pattern or biometrics cannot change over time. Hair color or body weight are examples of biological measures, but they change over time, so we cannot consider them as biometrics measures approved. The compression between different types of biometrics according to some important characteristics are conducted in Table 1. According to Table 1, we found that Iris and Finger vein had very qualified characteristics to be integrated into a multimodal system [3, 6–11].

Table 1. Compression between different types of biometrics according to usability factors

Factors	Finger Print	Face	Iris	Finger Vein	Voice
Universality	H	H	H	M	H
Distinctiveness or Uniqueness	H	H	H	H	M
Permanence	H	L	H	H	L
Performance or Accuracy	L	M	H	M	L
Vulnerability (Spoofing)	H	M	L	L	H
Security	L	M	H	H	L

H – High L – Low M – Medium

2.1. Single-modal finger print identification systems

Hoyle et al. [12] suggested methodologies utilize minutiae triplet-based patterns in a hierarchical order, where not only minutia circumstances are utilized, but ridge data is applied to maintain associations between minutiae. Kumar et al. [13] introduced a novel strategy for individual identification by utilizing finger back outside imaging. This article proposed pegfree imaging technique. Finger images are normalized to reduce their scaling, rotation, and interpretation variations in knuckle images. Test results gained encouraging outcomes, an error rate of 1.39%.

2.2. Single-modal face identification systems

Face identification has a lot of in-depth, high-quality study outcomes. Jiménez et al. [14] suggested a feature spread design to distribute with the artificial distinction in face identification. Eigenvectors and pose factors are used to integrate pose reconstructed images based on thin-plate splines-based warping. Apple originated face identification (ID) in 2017, which provides a provocation to the business of facial identification [15]. Face identification system utilizes machine learning to increase its identification accuracy constantly. IPhone X has used the implemented version of this approach, and it is extremely trusted by users.

2.3. Single-modal iris identification systems

Pillai et al. [16] introduced a combined structure-based on stochastic projections and sparse descriptions. Its method can deal with a basic deformity in an iris image acquisition. This approach can produce high efficiency, over 96%. System running performance is not specified in this paper. Thavalengal et al. [17] directed on significant circumstances for practice implementation, such as image quality, and iris size. They presented system specifications for unconstrained acquisition in smart devices. They gave various design plans. Two of these designs have achieved high efficiency, over 97%. Moreover, they have medium-level usability and safety. Rigas et al. [18] utilized the distinction between the artificial iris and an actual eye iris to introduce a procedure based on the detection of eye movement to deal with the fake iris threat. The experiment results based on a dataset, involving 200 individuals, proved that the system could obtain a typical classification rate of 96.5% with FAR equal 3.4% and FRR equal 3.5%. Bodade et al. [19] suggested an approach to identify the internal side of iris-based on pupil size disparity. Since pupil size variations with various light levels, its variety can be used to discover the aliveness of iris. Samples using 380 images of 64 individual subjects were used in laboratory tests. The efficiency of iris localization from eye samples was 98.48%.

2.4. Single-modal finger vein identification systems

K. R. Park et al. [20] have introduced a novel method for finger vein identification that possesses three pros and participation compared to earlier works. Firstly, local information of the finger veins based on local binary pattern (LBP) without segmenting was extracted. In the second step, the extracted pattern of the finger veins based on the Wavelet transform method was obtained. In the third step, LBP score values were fused by the SVM method. A robust feature extraction procedure for finger vein was implemented by N. Miura et al. [21]. They have introduced a process of individual verification based on finger-vein patterns. Vein sample is taken using infrared light technology includes occasional shading generated by the different densities of the finger bones, tissues, and muscles. Jadhav et al. [22] demonstrated that a finger vein biometric identification framework is more useful than other biometric schemes since it has a higher performance and lower fabrication rate. They included an image processing method, and executed Field. programmable gate array (FPGA) to deal with template matching. Test outcomes explained that its efficiency can equal 96% with 4% FRR.

2.5. Multi-modal identification systems

Prabhakar et al. [23] presented the signal acquiring features of iris and fingerprint biometrics-two of the most universally used biometric characteristics. Individual identification of people is needed to handle many everyday and commercial exercises. Besides visual identification of associations, checking an individual's government-issued photo ID is the most traditional method. Saevanee et al. [24] denoted out that remarkably finger stress pressure provides more discriminative information than dynamic keystroke does. There must be a press sensor in the tube to assemble the stress signals. The dynamic keystroke verification normally uses a two-class classifier. Both positive samples and negative ones train the classifier.

2.6. Comparison between existing biometric identification system

In Table 2 we scoring the global famous biometric system according to essential factors such as false acceptance rate (FAR): the probability of recognizing fake registration as an authorized registration. False rejection rate (FRR): the probability of recognizing an authorized registration as an impersonator. Equal error rate (EER): introduces the point when the FAR line intersects to the line of FRR. Different usability factors such as UV, UQ, PM and EE. Security: Biometric identification systems are exposed to a list of threats.

Table 2. Comparison Summaries between different types of biometric systems according to various characteristics [5]

Ref.	System Type-Applied Biometric	Accuracy (S)			Usability (S)				Suppo
		FAR score	FRR score	FER score	UV score	UQ score	OM score	EE score	securi (S)
[12]	Singel modal-Finger print	1	1	1	2	2	1	2	0
[13]	Singel modal-Finger knuckle	3	3	3	2	3	3	3	0
[14]	Singel modal-Face	1	1	1	3	1	1	3	1
[15]	Singel modal-Face	2	2	2	3	1	1	3	3
[16]	Singel modal-Iris	3	3	3	2	3	3	1	2
[17]	Singel modal-Iris	3	3	3	2	3	3	1	2
[18]	Singel modal-Iris	2	2	2	2	3	3	1	2
[19]	Singel modal-Iris	3	3	3	2	3	3	1	2
[20]	Singel modal-Finger vein	2	2	2	2	3	3	3	3
[21]	Singel modal-Finger vein	3	1	2	3	2	2	2	2
[22]	Singel modal-Finger vein	3	2	2	2	3	3	3	3
[23]	Multimodal-Finger print and Iris	2	2	2	3	3	3	2	3
[24]	Multimodal-Keystroke and Finger pressure	3	3	3	2	1	1	1	3

3. PROPOSED MULTIMODAL BIOMETRIC MODEL

The suggested system is a multimodal fusion biometric model between finger vein and iris, as shown in Figure 1. The proposed system is divided into three distinct phases. The first phase is the iris identification phase, which includes three stages such as preprocessing, feature extracting process, and storing template in the database. The second phase is the finger vein identification phase, which also includes the same stages of iris model system. The objective of the recommended model is to obtain higher accuracy that may not be possible using a single modal of the biometric system. The third final phase is the fusion phase at score -level. The suggested combined system provides anti-spoofing propositions by using multiple biometric traits simultaneously. Scores generated from personal features are combined at a matching score level using a weighted aggregate of score procedure.

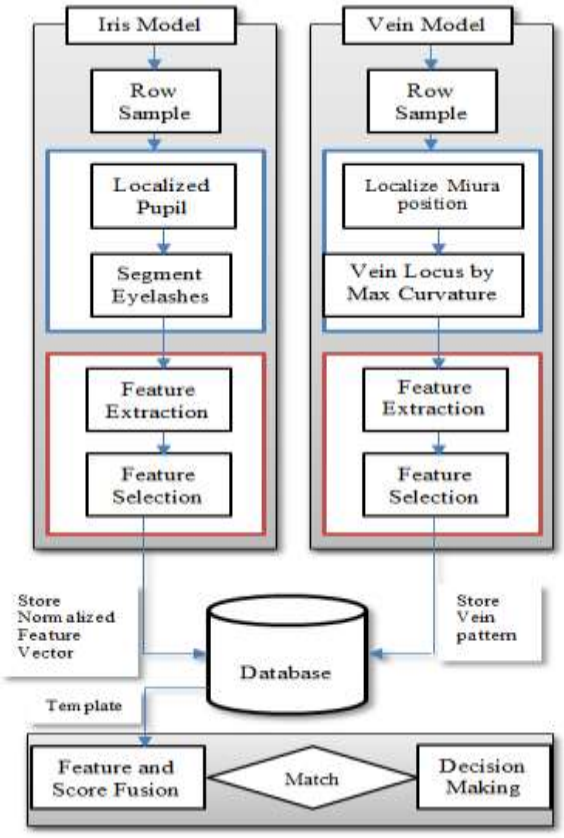


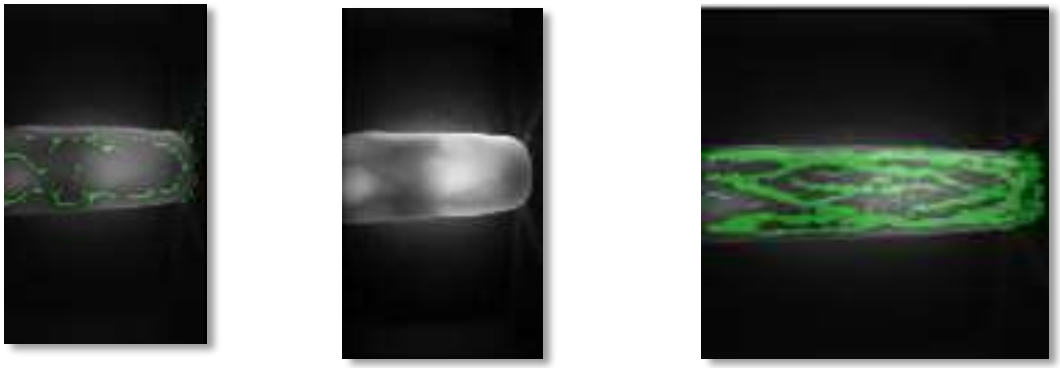
Figure 1. Multimodal proposed identification system

4. METHODS

This phase contains four combined stages such as preprocessing, feature processing, storing template in database, and matching template with the tested image. Process in iris identification system is shown in Figure 2. The result of each process in finger vein identification system is shown in Figure 3.

(a) Original row sample (b) Localized iris image (c) Segmented iris image

Figure 2. Iris preprocessing results



(a) Original sample (b) Localized locus position (c) Repeat the vein tracking method using max curvature method

Figure 3. Finger vein preprocessing results

4.1 Preprocessing stage

In this stage, iris identification model has two main processes such as localization and segmentation processes. Also, finger vein identification mode has two main process to detect locus position. The result of each process in iris identification system is shown in Figure 2. The result of each process in finger vein identification system is shown in Figure 3.

4.2 Feature processing stage

In this stage, there are also two main processes such as feature extraction and selection processes. The result of the normalized feature extraction and selection process of iris and vein is shown in Figure 4 and Figure 5 respectively. The result of each process is shown in Figure 4 We use different feature extraction algorithms such as SIFT, SURF, PCA, canny edge detection and fast SIFT [2] algorithm to extract and select primary distinct features. This algorithm covers the most of the following noise challenges in sampling image such as:

a) Scaling challenge: the registered or tested image are taken in different scale.
b) Orientation challenge: the registered or tested image are rotated with respect to each other.
c) Occlusion challenge: the registered or tested image are partially covered or interference with another object.

Illumination challenge: the registered or tested image are taken in a failure environmental setting such as taking a sample in high light, or darkness.

Figure 4. Iris feature normalization results

Figure 5. Binarized normalized vein patterns

The Gaussian scale space $L(x, y, \sigma)$ of an image is represented as the convolution method $G(x, y, \sigma)$ of varying widths ¾ with the input image $I(x, y)$:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \quad (1)$$

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma) \quad (2)$$

Where k is a fixed multiplicative parameter in range space. The DoG are utilized for various purposes. Initially, it is an effective function that requires minimum calculation power to measure: The smoothed images $L(x, y, \sigma)$ require to be calculated for scale space pattern description and therefore, D can be calculated by simple subtraction. Every image sample within a 16x16 window around each key point, the gradient magnitude, m, and its orientation, θ, are computed using pixel differences:

$$\theta(x, y) = \arctan\frac{L(x,y+1) - L(x,y-1)}{L(x+1,y) - L(x-1,y)} \quad (3)$$

4.3 Matching phase

In the matching phase, 200 iris samples were picked from 50 persons; every individual has four images in the training stage. While in the testing stage, fifty iris samples for 50 persons were used. These samples are collected from the CASIA-v1 database. Hamming, cosine, and euclidean distance methods are used and processed for performing the matching. The smallest distance should be investigated; if it is smaller than the threshold condition, that indicates it is from the same classification class. We can also use the proposed matching ranking algorithm introduced by El-Gayar [25]. Otherwise, if it is larger than the threshold value, that shows it is from the other classification class. The applied distance methods are [26]:

a) Euclidean Distance method equation

$$d(x, y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad (4)$$

b) Cosine Distance method equation

$$d(x, y) = 1 - \frac{\sum_{i=1}^{n}(x*y)}{\sqrt{\sum_{i=1}^{n} x^2 * \sum_{i=1}^{n} y^2}} \quad (5)$$

c) Hamming Distance method equation

$$d(x, y) = \sum_{i=1}^{n} \delta(x_i, y_i) \quad (6)$$

Example of iris matching process as shown in Figure 6.

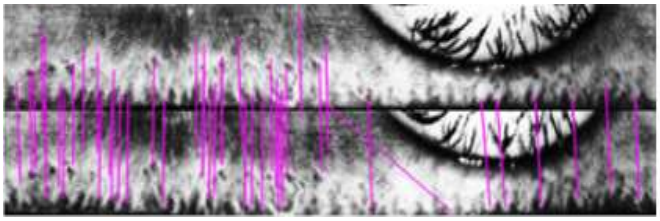


Figure 6. Example of iris matching proces

5. RESULTS AND DISCUSSION

In this part, the testing of recommended system is required to prove its reliability, accuracy and efficiency. We applied different feature processing and matching algorithms to conduct experiments. Experiments are done out on windows 10, processor core i7 and 8 GB RAM to gain high accuracy and performance. We use MATLAB and Apache server to conduct the experiments. MATLAB is a high-performance language for technical computing. MATLAB is used to perform Iris and miura localization, normalization, feature extraction and selection. Apache server is used to store template in database and perform matching techniques. Iris CASIA-V1 and finger vein (MLA) datasets are used to estimate the results. The dataset consists of fifty persons, and each person has five samples captured in two sessions. We use four samples for each module for training and one sample for testing. All samples are stored in JPG format with dimensions 320*280. Dataset and machine specification are presented in Table 3.

Table 3. Dataset and machine spesification

Platform	Windows 10
Mircoprocessor	Intel core-i7
Main memory	8BG
Dataset	Casia-V1 for IRIS From Center of biometrics and security research MLA for Finger vein
Dimension	320*280
File format	Image JPG
Data size	5 images for each person We have 5 persons

5.1. Evaluation metrics

FAR: the probability of recognizing fake registration as an authorized registration.

$$\text{FAR} = \frac{\text{Number of Falsely accepted images}}{\text{Total number of imposter}} * 100\% \quad (7)$$

FRR: the probability of recognizing an authorized registration as an impersonator.

$$\text{FRR} = \frac{\text{Number of Falsely reject images}}{\text{Total number of genuine}} * 100\% \quad (8)$$

EER: introduces the point when the FAR line intersects to the line of FRR.

5.2. Evaluation results

Serval experiments are conducted using different feature extraction algorithms such as canny edge detection, SIFT, SURF, PCA and FSIFT. In each experiment, we used different distance matcher algorithms. The evaluation results for each experiment are presented in Table 4. FAR and FRR charts for each distance matcher algorithm are presented in Figure 7, 8 and 9 respectively. Time consuming chart for each experiment are represented in Figure 10.

Table 4. Accuracy and security results when applying various feature extraction methods using different matcher algorithms

Method	Distance Measure	FAR%	FRR%	Accuracy%	Required Time (sec)
	Eculidren	0.069	0.0813	91	180
Cany edge detection	Cosine	0.339	0.533	89	192
	Hamming	0.039	0.132	92	176
	Eculidren	0.0039	0.036	96	228
SIFT	Cosine	0.0244	0.434	94	280
	Hamming	0.0019	0.031	97	216
	Eculidren	0.0052	0.93	95	178
SURF	Cosine	0.0113	0.152	93	202
	Hamming	0.0022	0.044	96	158
	Eculidren	0.0071	0.081	94	188
PCA	Cosine	0.0250	0.362	90	212
	Hamming	0.0058	0.088	92	195
	Eculidren	0.0042	0.032	97	118
Fast SIFT	Cosine	0.0093	0.0073	95	130
	Hamming	0.0015	0.025	98	103

Figure 7. FAR and FRR evaluation results for each feature extraction algorithm based on Euclidean distance matcher algorithm

Figure 8. FAR and FRR evaluation results for each feature extraction algorithm based on Cosine distance matcher algorithm

Figure 9. FAR and FRR evaluation results for each feature extraction algorithm based on Hamming distance matcher algorithm

Figure 10. Time consumption results for each feature extraction algorithm

6. CONCLUSION

In this article, a smart multimodal pattern identification system for identifying a person's identity is proposed based on different feature extraction and distance matcher algorithms. This system is identified the iris and finger vein unique patterns and features for each individual to overcome many challenges such as identity fraud, poor image quality, noise and instability of the surrounding environment. This system provides an effective fusion scheme based on the incorporation of different features of each biometric system and thus increase the efficiency that cannot be achieved in a single-modal identification system. Several experiments were performed on a dataset containing 50 people and using the Hamming distance algorithm to measure the similarity between a person and previously entered data. The results of the proposed system were provided a higher accuracy of 98%, with false accept rate and false reject rate of 0.0015% and 0.025%, respectively.

REFERENCES

[1] Stallings William, Brown Lawrie, *Computer security: principles and practice / William Stallings, Lawrie Brown, UNSW Canberra at the Australian Defence Force Academy*, Fourth edi., New Jersey: Pearson Education, Inc Hoboken, 2018.
[2] El-Gayar MM, Soliman H, Meky N., "A comparative study of image low level feature extraction algorithms," *Egyptian Informatics Journal*, vol. 14, no. 2, pp. 175–181, 2013.
[3] Delac K, Grgic M., "A survey of biometric recognition methods," *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine*, Zadar, Croatia, 2004, pp. 184-193.
[4] Chauhan S, Arora AS, Kaul A., "A survey of emerging biometric modalities," *Procedia Comput Sci*., vol. 2, pp. 213–8, 2010.
[5] Rui Z, Yan AZ, Yan Z., "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," *IEEE Access*, vol. 7, pp. 5994-6009, 2019.
[6] Bharadwaj S, Vatsa M, Singh R., "Biometric quality: a review of fingerprint, iris, and face," *Eurasip J. Image Video Process*., vol. 34, pp. 1–28, 2014.
[7] Nixon MS., *Handbook of Biometric Anti-Spoofing*, Springer, 2019.
[8] Masyn S, Vuchelen A, Santermans E, Rasschaert F, Bangura A, Parys W, *et al*., "Overcoming the challenges of iris scanning to identify minors (1-4 years) in the real-world setting," *BMC research notes*, vol. 12, pp. 1–6, 2019.
[9] Hoyle K. "Minutiae triplet-based features with extended ridge information for determining sufficiency in fingerprints," Master dissertation, Virginia Tech, 2011.
[10] Kumar A, Ravikanth C., "Personal authentication using finger knuckle surface," *IEEE Trans Inf Forensics Secur*., vol. 4, no. 1, pp. 98–110, 2009.
[11] Gonzalez-Jimenez D, Alba-Castro JL., "Toward Pose-Invariant 2-D Face Recognition Through Point Distribution Models and Facial Symmetry," *IEEE Trans Inf Forensics Secur*., vol. 2, no. 3, pp. 413–429, 2007.

[12] Bud A., "Facing the future: the impact of Apple FaceID. Biometric Technol Today," *Biometric Technology Today*, vol. 2018, no. 1, pp. 5–7, 2018.
[13] Pillai JK, Patel VM, Chellappa R, Ratha NK, "Secure and robust Iris recognition using random projections and sparse representations," *IEEE Trans Pattern Anal Mach Intell*., vol. 33, no. 9, pp. 1877–1893, 2011.
[14] Thavalengal S, *et al*., "Proof-of-concept and evaluation of a dual function visible/NIR camera for iris authentication in smartphones," *IEEE Trans Consum Electron*, vol. 61, no. 2, pp. 137–143, 2015.
[15] Rigas I, Komogortsev O V., "Eye movement-driven defense against iris print-attacks" *Pattern Recognit Lett*., vol. 68, pp. 316–326, 2015.
[16] Bodade R, Talbar S., "Dynamic iris localisation: A novel approach suitable for fake iris detection," *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 2. pp.163-173,2010.
[17] Lee HC, Kang BJ, Lee EC, Park KR., "Finger vein recognition using weighted local binary pattern code based on a support vector machine," *J Zhejiang Univ Sci C*., vol. 11, no. 7, pp. 514–524, 2010.
[18] Miura N, Nagasaka A, Miyatake T., "Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification," *Machine Vision and Applications*, vol. 15, pp. 194–203, 2004.
[19] Jadhav M, Nerkar PM., "Implementation of an embedded hardware of FVRS on FPGA," *2015 International Conference on Information Processing (ICIP)*, Pune, 2015, pp. 48-53.
[20] Prabhakar S, Ivanisov A, Jain A., "Biometric recognition: Sensor characteristics and image quality," *IEEE Instrumentation & Measurement Magazine*, vol. 14, no. 3, pp. 10–16, 2011.
[21] Saevanee H, Bhattarakosol P., "Authenticating user using keystroke dynamics and finger pressure," *2009 6th IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, 2009, pp. 1-2.
[22] El-Gayar MM, Mekky NE, Atwan A, Soliman H., "Enhanced search engine using proposed framework and ranking algorithm based on semantic relations," *IEEE Access*, vol. 7, pp. 139337-139349, 2019.
[23] Al-Taie I, Azeez N, Basbrain A, Clark A., "The effect of distance similarity measures on the performance of face, ear and palm biometric systems," *2017 International Conference on Digital Image Computing: Techniques and Applications (DICTA*), Sydney, NSW, 2017, pp. 1-7.
[24] S. Arora and M. P. S. Bhatia, "A computer vision system for Iris recognition based on deep learning," *2018 IEEE 8th International Advance Computing Conference (IACC)*, Greater Noida, India, 2018, pp. 157-161.
[25] N. Jagadeesh and C. M. Patil, "Development of a new methodology for iris algorithm in biometric authentication using hamming distance concepts," *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, 2017, pp. 3362-3365.
[26] Q. Zhang, H. Li, Z. Sun and T. Tan, "Deep feature fusion for Iris and periocular biometrics on mobile devices," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2897-2912, 2018.

BIOGRAPHIES OF AUTHORS

Enas Abbas Abed Msc. University of Diyala, enasabbas1111@gmail.com. Enas A. Abed received his B.E. degree in Computer Engineering from the University of Diyala in 2005, his M.Sc. degree in Information System from Egypt/Banha University in 2018. She is currently a lecturer in Diyala University, Iraq. His current research interests Information Retrieval, image processing, and Artificial intelligence. Email: enasabbas1111@gmail.com.

Rana Jassim Mohammed Msc. University of Diyala. Rana J. Mohammed received his B.E. degree in computer science from the University of Diyala in 2006, his M.Sc. degree in computer science from the University of Diyala in 2019. She is currently a lecturer in Diyala University, College of science, Department of computer science, Diyala, Iraq. His current research interests cover image pre-processing, security, and authentication in mobile. Email: ad.ranamohammed@uodiyala.edu.iq.

Msc. Dhafer Taha Shihab. University of Diyala/college of engineering, Dhafer T. Shihab, got a bachelor's degree in computer engineering from the University of technology, Iraq in 2006 and got a master's degree in Computer Engineering and information from Bulgord State Technical University, Russia in 2014. Currently teaching as Assistant Lecture at the Faculty of Engineering/Diyal. Email: dhafershihab@gmail.com.