HUMAN IDENTIFICATION BASED ON THINNING MINUTIAE OF FINGERPRINT

[1]OMED HASSAN AHMED, [2] *JOAN LU,* [3] MUZHIR SHABAN AL-ANI

[1]University of Huddersfield, The School of Computing and Engineering, UK
[1]University of Human Development, College of Science and Technology, Department of Information Technology, Sulaimani, KRG, Iraq
E-mail: omed.hassan@uhd.edu.iq

[2]University of Huddersfield, The School of Computing and Engineering, UK
E-mail: j.lu@hud.ac.uk

[3]University of Human Development, College of Science and Technology, Department of Information Technology, Sulaimani, KRG, Iraq
E-mail: muzhir.al-ani@uhd.edu.iq

ABSTRACT

The rapid growth in the development of biometric applications causes human identification as an important issue. In addition fingerprint as a part of biometrics leading to an efficient method of human identification. Many problems appears in fingerprint patterns such as noisy patterns, confused patterns, unclear patterns displacement of patterns, spread of ink … etc. The main objective of this paper is to design and implement an efficient and effective approach for human identification using human fingerprint. The main operation of this approach after preprocessing is to localize and recognize the minutiae in fingerprint image. This approach depends on the thinning operation that is so important to prepare the image to recognize the minutiae. Good results have been achieved via implementing this approach, where the obtained similarity ratio is approximately 90%.

Keywords: *Multi-Biometrics; Human Identification; Fingerprint Recognition; Biometric Recognition.*

1. INTRODUCTION

Security is very important part in our life [1]. The traditional approach of security is very similar to the sequential approach in software engineering [1],[2]. First identify all the requirements through a systematic risk assessment, then design your security and decide what controls you will use to reduce the identified risk [3]. Then, after the implementation phase, during which it creates its security policy and implements its controls, it starts the test phase [3].

It is no secret that preserving information has been important for a long time [4]. Where the person began to draw drawings and symbols when writing messages and have certain meanings known to the recipient of the message [5]. As the technology developed, the password, digital signature and other devices were used to preserve data and information [6]. All this can be stolen and entered into data because it is about the possibilities and how to get to solve the mystery [7]. The large amount of data and information owned by individuals and institutions has become a burden in terms of maintaining them because in itself is the great value of that institution or company [8]. The revolution of communications, the Internet, Internet of things and mobile phones opened many doors in front of the thieves and intruders to access data in illegal ways due to the development of their abilities as well [9] [10].

Man encounters hundreds of people every day and can recognize people by their faces, which is one of the physical biological characteristics of human [11]. Fingerprints have been used for a long time ago to identify criminals and wanted persons, where there are mismatch of fingerprints approaching a million cases [12]. Before introducing the characteristic of using biometric approaches in security, there are some drawbacks of the traditional security systems concentrated on: it can be forgotten easily, it can be stolen easily, it can be broken easily, and it can be lost easily [13]. Therefore it is better to introduce other way of security that offers powerful security, this is available with biometric security that eliminates most of the drawbacks appeared with the traditional security [14] [15].

This work tries to implement an efficient approach for human identification using fingerprint recognition via minutiae recognition method. So, this addressed the research question in this work.

2. BIOMETRICS

Traditionally, passwords and identification cards have been used to restrict access to systems [16]. However, security can easily be violated in these systems when a password is revealed to an unauthorized user or a card is stolen by an imposter; In addition, simple passwords are easy to guess and passwords are hard to remember [17]. The emergence of biometrics has solved the problems plaguing traditional verification methods. Biometrics refers to the automatic identification of an individual who uses certain physiological or behavioral traits associated with the person [18].

Biometrics refers to the study of automated methods for uniquely recognizing humans based on one or more intrinsic physical or behavioral characteristics [19]. The physical characteristics including fingerprint recognition, face recognition, iris recognition, hand geometry, DNA, retina recognition, ear recognition, skin reflection, lip motion, vein pattern, brain wave pattern and body odor [20]. The behavioral characteristics including signature verification, speaker recognition gait recognition, and keystroke [21].

Although biometric systems have their limitations, they have an advantage over traditional security methods in which it is very difficult to lose, steal or fragment biometric features; In addition, they facilitate human recognition at a distance [22]. Biometric systems also present a practical aspect for the user that may not be possible using traditional security techniques [23]. Users who keep different passwords for different applications may have difficulty remembering the password associated with a specific application [24]. A typical biometric system works by acquiring biometric data from an individual, extracting a set of characteristics from the acquired data and comparing that set of characteristics with the set of characteristics of the model in the database [25].

In an identification platform, the comparison is made with the models corresponding to all registered users to recognize the individual means one-to-many correspondence [26]. In a verification platform, the comparison is made only with the models corresponding to the identity claimed to verify the claim means one-to-one correspondence [27]. Therefore, the identification (whose are the biometric data?) And the verification (does this biometric data belong to them?) Are two different problems with different inherent complexities [28]? The templates are generally created at the time of registration and depending on the application, may or may not require staff intervention [29]. Figure 1 shows the general biometric system with both enrollment and verification [30]. This biometric system has four important parts including biometric acquisition (responsible of capturing biometric data and convert it into digital form), feature extraction (responsible of generating features from the digital biometric data), feature matching (responsible of comparing the feature values with the template and generating a matching score) and decision making (responsible of generating a decision for accept or reject depending on the matching score) [31].

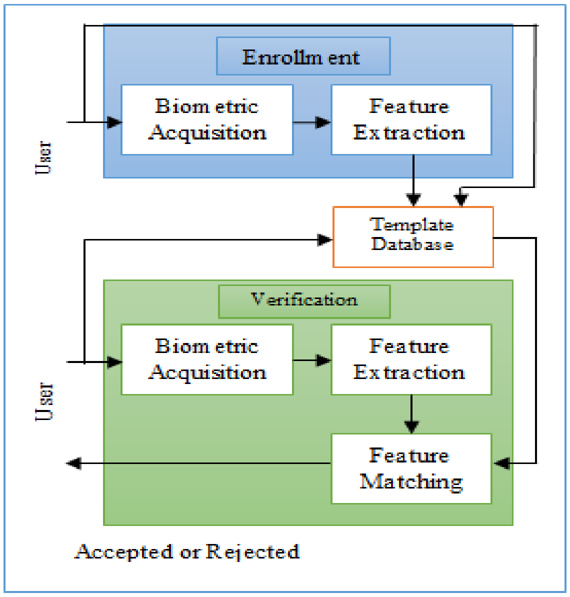

Figure 1 Enrollment of biometric system

3. FINGERPRINT

There are records of fingerprints taken centuries ago, although they were not as sophisticated as they are today [32]. The ancient Babylonians pressed their fingertips on the clay to record commercial transactions [33]. The Chinese used fingerprints on paper for business and to help identify their children [34]. However, fingerprints were not used as a method of identifying criminals until the 19th century [35].

Among all the biometric elements, fingerprints have one of the highest levels of reliability and have been widely used by forensic experts in criminal investigations [36]. Fingerprint refers to the number of peak patterns at the tip of the finger [37]. The flow of this peak anomalies in the local regions of the finger (Figure 2) and is the position and orientation of these anomalies that are used to represent and match fingerprints [38]. Although they have not been scientifically established, fingerprints are considered unique among individuals and among individuals of the same person [39]. Even identical twins who have similar DNA are assumed to have different fingerprints [40]. Traditionally, fingerprint heads were extracted by creating an inked impression of fingertip on paper [41]. Electronics has been used in a wide range of compact sensors that provide digital images of these models [42]. These sensors can be easily integrated into existing computer peripherals such as mouse or keyboard, which makes the identification mode very attractive [43]. This has led to increased use of automatic fingerprint authentication systems based on civil applications and their application.

Fingerprints provide a reliable means of personal identification [44]. This is the essential explanation of the fingerprints that replaced other methods to establish the identities of people reluctant to admit previous arrests [45]. Other visible human characteristics, such as facial features, tend to change significantly with age, but fingerprints are relatively persistent [46]. Except for traumatic injuries or surgery that causes deep scars, or diseases such as leprosy that damage the layers of skin that form the friction of the friction crest, it has never been shown that fingerprints and palms displace or change their relationship unity throughout a person's life [47] [48].

The Department of Homeland Security's Office of Biometric Identity Management (OBIM was formerly US-VISIT), contains over 120 million persons' fingerprints, many in the form of two-finger records [49]. The US Visit Program has been migrating from two flat (not rolled) fingerprints to ten flat fingerprints since 2007 [50]. Fast capture technology currently enables recording of ten simultaneous fingerprint impressions in as little as 15 seconds per person [51].

The biometric identity management office of the Department of Homeland Security (formerly US-VISIT) contains more than 120 million fingerprints, many of which are in the form of two-finger records [52]. The US touring program has gone from two flat fingerprints (unprinted) to ten fingerprints since 2007 [53]. The "fast capture" technology currently allows ten simultaneous fingerprints in just 15 seconds per person [54].

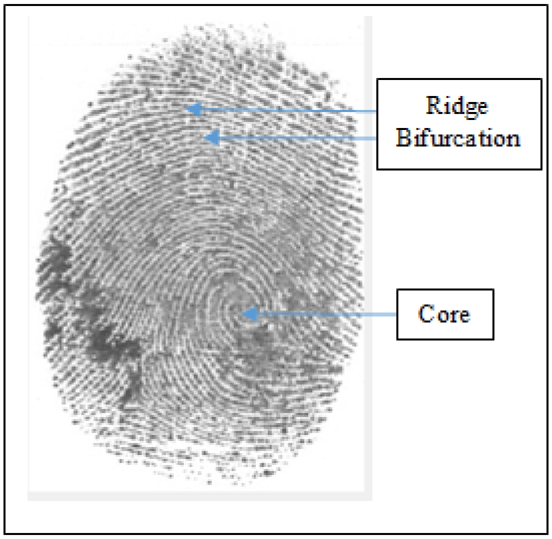

Figure 2 fingerprint image with core and minutiae

4. LITERATURE REVIEWS

Wide range of biometric measures are available, also different types of biometrics are existing, in addition there are big amount of biometric application. So for these huge amount of papers and literatures are published treating this area of research. This literature is concentrate on the latest published articles on this field.

B.S. Akhmetov et al. (2015) examined the problems of testing the quality of teaching biometric transformers, since much attention is now being paid to the development of biometric technologies. The given systems have transformed not only the principles and forms of collection, processing and transfer, but have begun to sufficiently influence all aspects of the life of society to become one of the key factors to maintain their sustainable development. After the tests of students in higher education in real time as part of the work carried out by the interprofessional laboratory on biometric devices and technology tests, some results were obtained [55].

Hao Zhang et al. (2015) focused on soft biometry versus extended attributes and presents the results of three experiments that quantify performance gains in a difficult task of facial recognition when standard facial recognition algorithms are augmented using soft biometry. These experiments include the best case analysis using perfect knowledge of gender and race, flexible biometric vectors based on support machines, and shape of the face expressed by a shape model. All three experiments indicate that small improvements can be made when soft biometry increases the existing algorithm [56].

D. Jagadiswary et al. (2016) proposed multimodal merged systems that offered several advantages over non-biometric systems, such as improved verification accuracy, a larger space to accommodate more subjects and greater security against counterfeiting. The proposed enhanced multimodal authentication system based on feature extraction (using fingerprint, retina and finger vein) and key generation. The experimental evaluation implemented using MATLAB, illustrates the significant improvement in the performance of multimodal biometrics with Genuine Acceptance Rate of 95.3% and FAR of 0.01% [57].

Changhee Hahn et al. (2016) offered an efficient and respectful privacy fingerprinting system that uses cloud computing systems. The proposed scheme makes great use of the computational power of a cloud for the cloud service provider to perform the most thorough calculations. Based on the obtained experimental results in an Amazon e-commerce cloud, the proposed scheme is faster than existing schemes and guarantees client confidentiality by exploiting symmetric homomorphic encryption. The security analysis showed that during identification, the customer's fingerprint data is not disclosed to the cloud service provider or the fingerprint database server [58].

Fernando Alonso-Fernandez et al. (2016) studied the periocular research work found in the literature. They provided a comprehensive framework that covers various aspects, from existing databases to algorithms for the detection of the periocular region and characteristics for recognition. The databases used include databases of faces and irises, as well as new databases that specifically capture the periocular area. Although the initial studies used annotated data, the detection and segmentation of the periocular region became a research objective in itself. This research provided an overview of the most relevant topics in periocular biometrics, providing complete coverage of existing literature and the current state of the art [59].

Alessandra Lumini et al. (2017) reviewed several systems and architectures related to the combination of biometric, unimodal and multimodal systems, classifying them according to a determined taxonomy. In addition, they discussed the problems of evaluating the biometric system, both performance indicators and existing benchmarks. Provided a case study on the combination of biometric couplers, then explain an experimental comparison of many different pairing approaches at the scoring level, conducted in three very different scoring databases. The experiments showed that the most valuable performance is obtained through mixed approaches, based on the merging of scores. The source code of the entire method implemented for this research is available for free for future comparisons [60].

Ahmed Mahfouz et al. (2017) provided a review of active biometric authentication systems. They presented the components and the operating process of active authentication systems in general, followed by a general description of the advanced biometric behavior characteristics that were used to develop an active authentication system and its evaluation in smartphones. They explained the problems, strengths and limitations associated with each biometric behavioral trait. In addition, they presented a comparative summary between them. Then they explored the challenges and research problems in this area of research [61].

Neyire Deniz Sarier (2018) described the first generic construct for multimodal encryption based on biometric identity when considering two distance measures at the same time. The current protocols for biometric Identity Based Encryption (BIE) are designed for the superposition of sets or for the Euclidean distance in unimodal biometry. However, the measures of similarity for biometric models can be very different from those considered in the theoretical works. In fingerprint template usually consists of a set of minutiae, and two models are considered similar if more than a number of minutiae in one model are close to the minutiae separated in the other. So, the measure of similarity must take into account both the Euclidean distance and the adjustment difference at the same time. Similarly, multimodal systems designed to meet the limitations of unimodal systems may involve two different characteristics that require different distance measurements for each modality [62].

Kien Nguyen et al. (2018) examined the next-generation super resolution approaches proposed for four main biometric modalities: face, iris, fingerprints and gait. They addressed the problem of super resolution in biometrics from several different angles, including spatial and frequency domains, single and multiple input images, learning-based approaches and reconstruction. Also they highlighted two special categories: the superdomain resolution that performs a superresolution directly in the feature space to improve recognition performance and the super-deep learning resolution that deals with the most advanced functions. Then, they explained the current and open research challenges and make recommendations for the improved use of super resolution in biometrics [63].

Marta Gomez-Barrero et al. (2018) presented an efficient methodology to estimate the main parameters of multi-biometric systems, based on a statistical analysis of non-protected models. In addition, to increase the accuracy of the audit and the protection of confidentiality, a general approach to a feature-protected merger is proposed. In order to avoid biased results, the robustness of the estimation methods is confirmed for the face, the iris, the fingerprint and the fervor in two sets of databases completely accessible to the public. In addition, they showed how the weighted entity level merger preserved the accuracy of unprotected score level merger, while adding confidentiality protection to the implemented system [64].

The above literatures concentrated on applying recognition and identification using single and multi-model biometrics, in addition of combination of different methods using standard fingerprint dataset. The proposed approach is concentrated on building the fingerprint dataset and apply all the required operation to extract the minutiae.

5. STATEMENT OF THE PROBLEM

Fingerprint recognition and identification becomes an important field of research because it related to multidirectional area of processing. The main challenge in this field is how localize and recognize certain points to identify the identical person within minimum time. This paper try to address an efficient approach of human identification based on fingerprint feature extraction.

6. METHOGOLOGY

The implemented methodology inn this paper is divided into three main parts: dataset collection that concentrated on fingerprint images, proposed fingerprint recognition approach that concentrated on the structure of the implemented system and minutiae recognition that deals with extraction of features from minutiae.

This approach concentrated on the traditional fingerprint images (ink stamp) that may have many problems during the collection procedure. So after collection of fingerprint images, these images must be cleaning and refining to be adequate for storing and processing. As a test sample 10 fingerprint images are collected from each individual (5 fingerprint image for left thumb and 5 fingerprint image for right thumb) as shown in figure 3. Some of these fingerprint images are used for enrollment and others are used for verification.

6.1 Dataset Collection

This approach concentrated on the traditional fingerprint images (ink stamp) that may have many problems during the collection procedure. So after collection of fingerprint images, these images must be cleaning and refining to be adequate for storing and processing. As a test sample 10 fingerprint images are collected from each individual (5 fingerprint image for left thumb and 5 fingerprint image for right thumb) as shown in figure 3. Some of these fingerprint images are used for enrollment and others are used for verification.

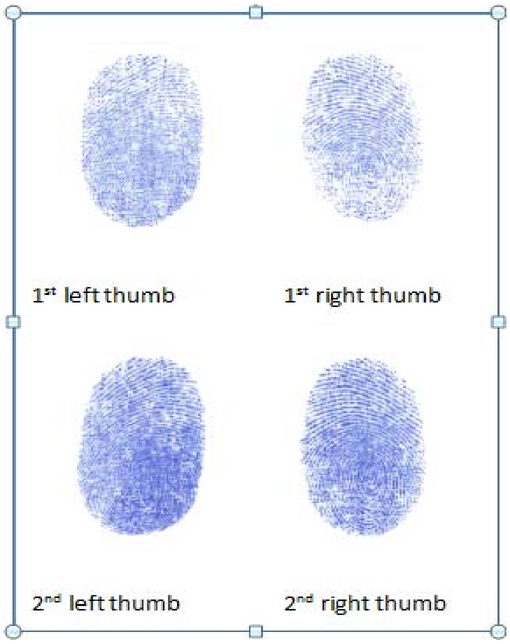

Figure 3 fingerprint dataset

6.2 Proposed Fingerprint Recognition Approach

The proposed fingerprint recognition approach passed into many stages starting from data acquisition up to decision making that identify the person. This approach consider that each stage is important because an improvement will introduce in each stage to achieve good performance in the overall approach. The proposed approach composed of the following stages (figure 4):

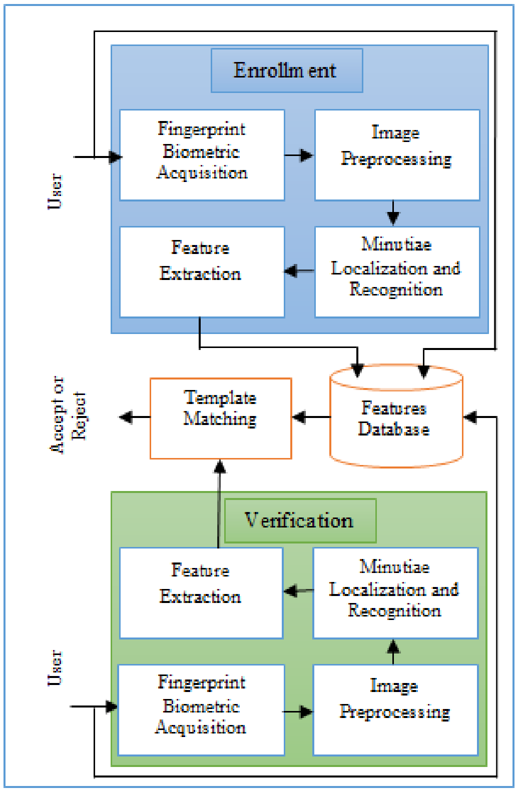

Figure 4 proposed fingerprint recognition approach

Fingerprint recognition approach has two main phases (enrollment and verification) and each phase consist of the following stages:

- **Fingerprint Acquisition**: this is represented the first stage of the overall system that can be performed using traditional (ink stamp) method or electronic method (scanner device). This approach used the ink stamp in order to illuminate and avoid any distortion appear in this method.
- **Image preprocessing**: this is an important stage in this approach because this stage prepare the image to the feature extraction stage. This stage including, converting color image into gray scale image, noise reduction, fingerprint image enhancement, fingerprint image resizing and converting gray image into binary image.
- **Minutiae Localization and Recognition**: this stage is the most important stage in which it can generate the positions of the important features in the pattern. There are two types of minutiae these types are ridge bifurcation (crossing) and ending line. After preprocessing stage, the minutiae must be enhanced in order to localize so it is easy to catch their pattern. The enhanced step is concentrated on the thinning process in which the minutiae can be find easily.
- **Feature Extraction**: This stage is the last stage for both enrollment and verification and it organize number of values (features) into a certain database. These features are used later for decision making.
- **Template Matching**: This stage is a decision making operation that decide accept or reject of the individual to the system depending on a certain threshold.

6.3 Minutiae Recognition

As it is mentioned previously it is very important to find and recognize the minutiae in the fingerprint image. This operation is implemented via many steps as shown in figure 5.

- Converting image into binary image step, after getting the gray scale fingerprint image it must be converted into binary images in which reduce the important part (dark part) into minimum values so it can be find that points.
- Thinning step: in this step convert the fingerprint image into narrow lines that represents the ridge lines.
- Minutiae Extraction: this step including localize and extract the minutiae. At this step the bifurcation well be find via the crossing lines that represents the bifurcation finding and the ridge line that represents the ridge end finding.

7. RESULTS AND DISCUSION

According to the designed approach for fingerprint recognition that implemented for a certain dataset of fingerprint images in order to recognize these fingerprints for human identification. Figures 5 and 6 show the implementation of the proposed approach on different types of fingerprint images. Figure 5 shows original image, binary image, thinned image and minutiae image that applied on first left thumb image. The final step of this figure demonstrates the drawing of fingerprint minutiae that realize each part of fingerprint. Figure 6 shows original image, binary image, thinned image and minutiae image that applied on first right thumb image. The final step of this figure demonstrates the drawing of fingerprint minutiae that realize each part of fingerprint.

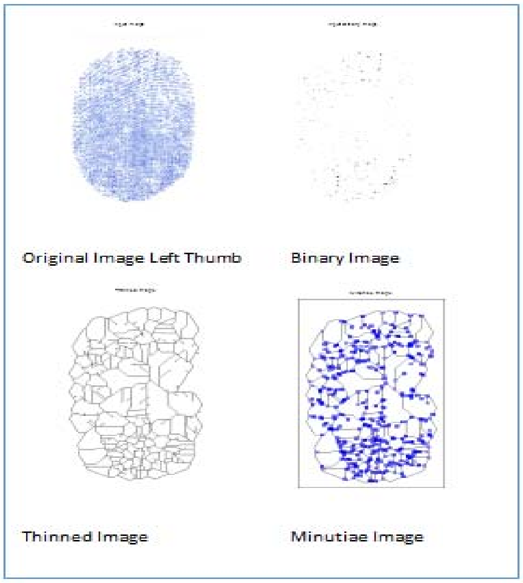

Figure 5 first left thumb

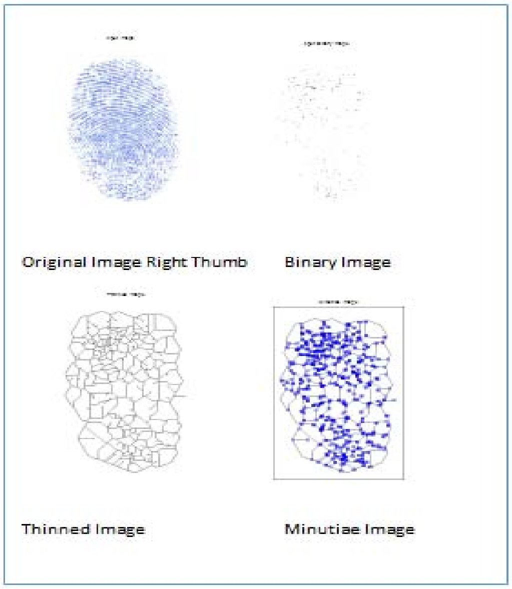

Figure 6 first right thumb

The implemented approach leading to significant results, these results is concerned with the last step of the minutiae operation. The obtained minutiae images are obtained from different types of fingerprints. These fingerprint images are concerned with left and right thumbs. To compare these images, many parameters are measured:

- **PSNR** is the peak signal to noise ratio in decibels (dB). The PSNR is only meaningful for data encoded in terms of bits per sample, or bits per pixel. For example, an image with 8 bits per pixel contains integers from 0 to 255.
- **MSE** is the mean square error that represents the squared norm of the difference between the data and the approximation divided by the number of elements.
- **MAXERROR** is the maximum absolute squared deviation of the data, from the approximation.
- **RATIO** is the ratio of the squared normalizing of the signal or image approximation to the input signal or image.

Table 1 demonstrate five sets of comparisons between PSNR, MSE, MAXERROR and RATIO. For example, L11 represents the first left thumb, L21 represents the second left thumb, L31 represents the third left thumb, L41 represents the fourth left thumb and L51 represents the fifth left thumb. In order to check all the five thumbs with each other, it is better to make cross comparison.
The measured values of the indicated parameters are including in the final results excluding that values for the same identity. PSNR in table 1 indicates their values with in the average of 5.9051, so this value is near to that values in the table. On other hand the overall mean values of MSE is 1.6719e+04 that is near to most of the measured MSE. The expected ratio of the square normalized image to the original image is about 1 but the obtained result is 1.0155 which is so near to most of the measured values. This ratio is demonstrated in figure 7 in which there is a very small variations in these values.
Table 1 values of PSNR, MSE, MAXERROR and RATIO

Ref. Thumb	Test Thumb	PSNR	MSE	MAXERROR	RATIO
L11	L11	Inf.	0	0	1
L11	L21	5.4850	1.8390e+04	255	0.8930
L11	L31	6.0124	1.6287e+04	255	0.8547
L11	L41	5.4520	1.8530e+04	255	0.8869
L11	L51	5.9475	1.6532e+04	255	0.8423
Average		**5.7242**	**1.7435e+04**	**255**	**0.8954**
L21	L11	5.4850	1.8390e+04	255	1.2610
L21	L21	Inf.	0	0	1
L21	L31	6.0922	1.5990e+04	255	1.0777
L21	L41	6.1521	1.5771e+04	255	0.9923
L21	L51	5.9223	1.6628e+04	255	1.0621
Average		**5.9129**	**1.6695e+04**	**255**	**1.0786**
L31	L11	6.0124	1.6287e+04	255	1.1700
L31	L21	6.0922	1.5990e+04	255	0.9279
L31	L31	Inf.	0	0	1
L31	L41	5.9332	1.6587e+04	255	0.9207
L31	L51	6.1020	1.5954e+04	255	0.9855
Average		**6.0350**	**1.6205e+04**	**255**	**1.0008**
L41	L11	5.4520	1.8530e+04	255	1.2708
L41	L21	6.1521	1.5771e+04	255	1.0078
L41	L31	5.9332	1.6587e+04	255	1.0861
L41	L41	Inf.	0	0	1
L41	L51	5.9519	1.6515e+04	255	1.0703
Average		**5.8723**	**1.6851e+04**	**255**	**1.0870**
L51	L11	5.9475	1.6532e+04	255	1.1873
L51	L21	5.9223	1.6628e+04	255	0.9416
L51	L31	6.1020	1.5954e+04	255	1.0147
L51	L41	5.9519	1.6515e+04	255	0.9343
L51	L51	Inf.	0	0	1
Average		**5.9809**	**1.6407e+04**	**255**	**1.0156**

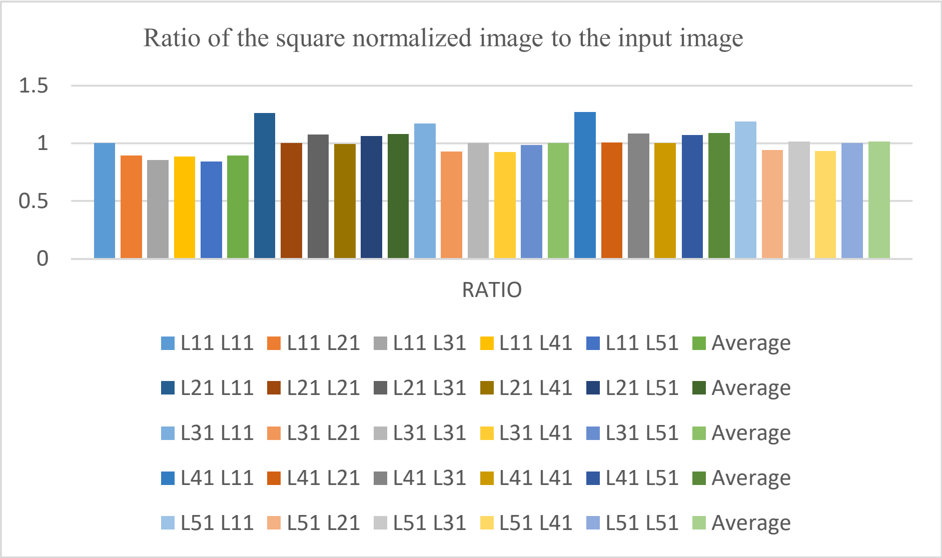

Figure 7 the ratio of the square normalized image to the input image

8. CONCLUSIONS

As it is mentioned previously there are very huge applications of human biometrics. On the other hand there is a strong relationship between biometrics human biometrics and security. Many researchers applied different biometric characteristics as human identification. This using fingerprint biometric in a simple procedure to recognize specific features to be used for human identification. The implemented approach concentrated on thinning and recognizing the minutiae via many steps to generate certain features that used later for human identification. This approach measured many parameters such as PSNR, MSE, MAXERROR and RATIO that can be used for comparing of different fingerprint images. The obtained similarity ratio is approximately 90% according to the required threshold. The minutiae localization leading more powerful issue to the recognition process. The obtained result leading to significant finding in which indicated a good decision can be taken according to the similarity of the tested fingerprint images.

REFRENCES:

[1] Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Tiago J. Cruz (2018) Cyber security of critical infrastructures, ICT Express, In press, accepted manuscript, Available online 21 February 2018.

[2] Yu-Chih Wei, Wei-Chen Wu, Ya-Chi Chu (2018) Performance evaluation of the recommendation mechanism of information security risk identification, Neurocomputing, Volume 279, 1 March 2018, Pages 48-53.

[3] Kamel Adi, Lamia Hamza, Liviu Pene (2018) Automatic security policy enforcement in computer systems, Computers & Security, Volume 73, March 2018, Pages 156-171.

[4] José M. de Fuentes, Lorena González-Manzano, Juan Tapiador, Pedro Peris-Lopez (2017) PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing, Computers & Security, Volume 69, August 2017, Pages 127-141.

[5] Sashank Dara, Saman Taghavi Zargar, VN Muralidhara (2018) Towards privacy preserving threat intelligence, Journal of Information Security and Applications, Volume 38, February 2018, Pages 28-39.

[6] Edlira Martiri, Artur Baxhaku (2012) Monotone digital signatures: an application in software copy protection, Procedia Technology, Volume 1, 2012, Pages 275-279.

[7] N. Houmani, A. Mayoue, S. Garcia-Salicetti, B. Dorizzi, C. Vivaracho-Pascual (2012) BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures, Pattern Recognition, Volume 45, Issue 3, March 2012, Pages 993-1003.

[8] K. Govinda, E. Sathiyamoorthy (2012) Identity Anonymization and Secure Data Storage using Group Signature in Private Cloud, Procedia Technology, Volume 4, 2012, Pages 495-499.

[9] Dhvani Shah, Vinayak haradi (2016) IoT Based Biometrics Implementation on Raspberry Pi, Procedia Computer Science, Volume 79, 2016, Pages 328-336.

[10] Tracey Caldwell (2015) Market report: healthcare biometrics, Biometric Technology Today, Volume 2015, Issue 1, January 2015, Pages 5-10.

[11] John S. Torday (2018) Pleiotropy, the physiologic basis for biologic fields, Progress in Biophysics and Molecular Biology, In press, corrected proof, Available online 9 February 2018.

[12] Curtis Matherne, Brian Waterwall, J. Kirk Ring, Keith Credo (2017) Beyond organizational identification: The legitimization and robustness of family identification in the family firm, Journal of Family Business Strategy, Volume 8, Issue 3, September 2017, Pages 170-184.

[13] Daniel Mellado, Carlos Blanco, Luis E. Sánchez, Eduardo Fernández-Medina (2010) A systematic review of security requirements engineering, Computer Standards & Interfaces, Volume 32, Issue 4, June 2010, Pages 153-165.

[14] Anshul Kumar Singh, Charul Bhatnagar (2015) Biometric Security System for Watchlist Surveillance, Procedia Computer Science, Volume 46, 2015, Pages 596-603.

[15] Gaurav Bhatnagar, Q.M. Jonathan Wu, Balasubramanian Raman (2010) Biometric Template Security based on Watermarking, Procedia Computer Science, Volume 2, 2010, Pages 227-235.

[16] Richa Singh, Mayank Vatsa, Arun Ross, Afzel Noore (2010) Biometric classifier update using online learning: A case study in near infrared face verification, Image and Vision Computing, Volume 28, Issue 7, July 2010, Pages 1098-1105.

[17] Muzhir Shaban AL-Ani (2014) Biometrics: Identification and Security, Source title: Multidisciplinary Perspectives in Cryptology and Information Security, 2014, DOI: 10.4018/978-1-4666-5808-0.ch014. IGI Global, Pennsylvania (USA).

[18] Silvia Venier (2010) Global mobility and security, Biometric Technology Today, Volume 2010, Issue 5, May 2010, Pages 8-10.

[19] Matthew Field, David Stirling, Zengxi Pan, Montserrat Ros, Fazel Naghdy (2015) Recognizing human motions through mixture modeling of inertial data, Pattern Recognition, Volume 48, Issue 8, August 2015, Pages 2394-2406.

[20] Muzhir Shaban AL-Ani (2015) Biometric Security, Source title: Handbook of Research on Threat Detection and Countermeasures in Network Security, 2015, DOI: 10.4018/978-1-4666-6583-5.ch011, IGI Global, Pennsylvania (USA).

[21] Koki Takagaki, Yasumasa Okamoto, Ran Jinnin, Asako Mori, Shigeto Yamawaki (2014) Behavioral characteristics of subthreshold depression, Journal of Affective Disorders, Volume 168, 15 October 2014, Pages 472-475.

[22] Rohit Thanki, Komal Borisagar (2015) Sparse Watermarking Technique for Improving Security of Biometric System, Procedia Computer Science, Volume 70, 2015, Pages 251-258.

[23] Chhaya Sunil Khandelwal, Ranjan Maheshewari, U.B. Shinde (2016) Review Paper on Applications of Principal Component Analysis in Multimodal Biometrics System, Procedia Computer Science, Volume 92, 2016, Pages 481-486.

[24] Gianluca Dini, Lanfranco Lopriore (2015) Password systems: Design and implementation, Computers & Electrical Engineering, Volume 47, October 2015, Pages 318-326.

[25] Kamel Aloui, Amine Nait-Ali, Mohamed Saber Naceur (2017) Using brain prints as new biometric feature for human recognition, Pattern Recognition Letters, In press, corrected proof, Available online 3 October 2017.

[26] Athira Nambiar, Alexandre Bernardino, Jacinto Nascimento (2015) Shape Context for soft biometrics in person re-identification and database retrieval, Pattern Recognition Letters, Volume 68, Part 2, 15 December 2015, Pages 297-305.

[27] Doroteo T. Toledano, Rubén Fernández Pozo, Álvaro Hernández Trapote, Luis Hernández Gómez (2006) Usability evaluation of multi-modal biometric verification systems, Interacting with Computers, Volume 18, Issue 5, September 2006, Pages 1101-1122.

[28] Rafael M. Luque-Baena, David Elizondo, Ezequiel López-Rubio, Esteban J. Palomo, Tim Watson (2013) Assessment of geometric features for individual identification and verification in biometric hand systems, Expert Systems with Applications, Volume 40, Issue 9, July 2013, Pages 3580-3594.

[29] Marius Iulian Mihailescu (2014) New Enrollment Scheme for Biometric Template Using Hash Chaos-based Cryptography, Procedia Engineering, Volume 69, 2014, Pages 1459-1468.

[30] Gianni Fenu, Mirko Marras, Ludovico Boratto (2017) A multi-biometric system for continuous student authentication in e-learning platforms, Pattern Recognition Letters, In press, corrected proof, Available online 2 April 2017.

[31] Mark Crego, Janice Kephart (2017) Top 10 must-haves for biometric ID systems, Biometric Technology Today, Volume 2017, Issue 5, May 2017, Pages 8-11.

[32] M.D. Freeman, F. Franklin (2016) Chapter 15: Criminal Investigation, Book chapter, Forensic Epidemiology, 2016, Pages 371-394.

[33] Karla D. Wagner, Lin Liu, Peter J. Davidson, Jazmine Cuevas-Mota, Richard S. Garfein (2015) Association between non-fatal opioid overdose and encounters with healthcare and criminal justice systems: Identifying opportunities for intervention, Drug and Alcohol Dependence, Volume 153, 1 August 2015, Pages 215-220.

[34] Adrian Palmer (2016) Cracking the code: identifying criminals using communication patterns, Computer Fraud & Security, Volume 2016, Issue 5, May 2016, Pages 5-7.

[35] Sotarat Thammaboosadee, Bunthit Watanapa, Nipon Charoenkitkarn (2012) A Framework of Multi-Stage Classifier for Identifying Criminal Law Sentences, Procedia Computer Science, Volume 13, 2012, Pages 53-59.

[36] Richard Clodfelter (2010) Biometric technology in retailing: Will consumers accept fingerprint authentication?, Journal of Retailing and Consumer Services, Volume 17, Issue 3, May 2010, Pages 181-188.

[37] Yu-Qiong Wu, Yu-Qiang Gou, Jing Han, Ying-Yan Bi, Chun-Ming Wang (2011)

Evaluation preparation technology of Xiaochaihu granules using fingerprint-peak pattern matching, Journal of Pharmaceutical Analysis, Volume 1, Issue 2, May 2011, Pages 119-124.

[38] Wonjune Lee, Sungchul Cho, Heeseung Choi, Jaihie Kim (2017) Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners, Expert Systems with Applications, Volume 87, 30 November 2017, Pages 183-198.

[39] Li Zhang, KengTeck Ma, Hossein Nejati, Lewis Foo, Dong Guo (2014) A talking profile to distinguish identical twins, Image and Vision Computing, Volume 32, Issue 10, October 2014, Pages 771-778.

[40] Si Chen, Shirong Ge (2017) Experimental research on the tactile perception from fingertip skin friction, Wear, Volumes 376–377, Part A, 15 April 2017, Pages 305-314.

[41] Bartosz Czaplewski, Mariusz Dzwonkowski, Roman Rykaczewski (2014) Digital fingerprinting for color images based on the quaternion encryption scheme, Pattern Recognition Letters, Volume 46, 1 September 2014, Pages 11-19.

[42] Chia-Hung Lin, Jian-Liung Chen, Chiung Yi Tseng (2011) Optical sensor measurement and biometric-based fractal pattern classifier for fingerprint recognition, Expert Systems with Applications, Volume 38, Issue 5, May 2011, Pages 5081-5089.

[43] Marcela Espinoza, Christophe Champod, Pierre Margot (2011) Vulnerabilities of fingerprint reader to fake fingerprints attacks, Forensic Science International, Volume 204, Issues 1–3, 30 January 2011, Pages 41-49.

[44] Anthony J. Palmer (2010) Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA), Computers & Security, Volume 29, Issue 7, October 2010, Pages 785-806.

[45] S. Gino, M. Omedei (2011) Effects of the most common methods for the enhancement of latent fingerprints on DNA extraction from forensic samples, Forensic Science International: Genetics Supplement Series, Volume 3, Issue 1, December 2011, Pages e273-e274.

[46] Simona Crihalmeanu, Arun Ross (2012) Multispectral scleral patterns for ocular biometric recognition, , Pattern Recognition Letters, Volume 33, Issue 14, 15 October 2012, Pages 1860-1869.

[47] Leila Lopes Mizokami, Lara Rosana Vieira Silva, Selma Aparecida Souza Kückelhaus (2015) Comparison between fingerprints of the epidermis and dermis: Perspectives in the identifying of corpses, Forensic Science International, Volume 252, July 2015, Pages 77-81.

[48] Juan S. Arteaga-Falconi, Hussein Al Osman, Abdulmotaleb El Saddik (2018) ECG and Fingerprint Bimodal Authentication, Sustainable Cities and Society, In press, accepted manuscript, Available online 3 January 2018.

[49] Rahul Bhaskar, Bhushan Kapoor (2014) Chapter 7: Homeland Security, Book chapter, Cyber Security and IT Infrastructure Protection, 2014, Pages 179-203.

[50] Paul H.P. Yeow, Y.Y. Yuen, W.H. Loo (2013) Ergonomics issues in national identity card for homeland security, Applied Ergonomics, Volume 44, Issue 5, September 2013, Pages 719-729.

[51] Torin Monahan, Jennifer T. Mokos (2013) Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks, Geoforum, Volume 49, October 2013, Pages 279-288.

[52] Coulier, P.-J. Les vapeurs d'iode employees comme moyen de reconnaitre l'alteration des ecritures. In L'Annee scientiJique et industrielle; Figuier, L. Ed.; Hachette, 1863; 8, pp 157-160 at http://gallica.bnf.fr/ark:/12148/bpt6k7326j (as of March 2010).

[53] Margot, Pierre and Quinche, Nicolas, "Coulier, Paul-Jean (1824-1890): A Precursor in the History of Fingermark Detection and Their Potential Use for Identifying Their Source (1863)", Journal of forensic identification, 60 (2), March-April 2010, pp. 129-134, (published by the International Association for Identification).

[54] Mark Crego, Janice Kephart (2017) Top 10 must-haves for biometric ID systems, Biometric Technology Today, Volume 2017, Issue 5, May 2017, Pages 8-11.

[55] B.S. Akhmetov, A.I. Ivanov, T.S. Kartbayev, A.U. Kalizhanova, G.S. Nabiyeva (2015) Testing the Quality of Teaching the Biometrical-code Transformers, Procedia - Social and Behavioral Sciences, Volume 191, 2 June 2015, Pages 2261-2266.

[56] Hao Zhang, J. Ross Beveridge, Bruce A. Draper, P. Jonathon Phillips (2015) On the

effectiveness of soft biometrics for increasing face verification rates, Computer Vision and Image Understanding, Volume 137, August 2015, Pages 50-62.

[57] D. Jagadiswary, D. Saraswady (2016) Biometric Authentication Using Fused Multimodal Biometric, Procedia Computer Science, Volume 85, 2016, Pages 109-116.

[58] Changhee Hahn, Junbeom Hur (2016) Efficient and privacy-preserving biometric identification in cloud, ICT Express, Volume 2, Issue 3, September 2016, Pages 135-139.

[59] Fernando Alonso-Fernandez, Josef Bigun (2016) A survey on periocular biometrics research, Pattern Recognition Letters, Volume 82, Part 2, 15 October 2016, Pages 92-105.

[60] Alessandra Lumini, Loris Nanni (2017) Overview of the combination of biometric matchers, Information Fusion, Volume 33, January 2017, Pages 71-85.

[61] Ahmed Mahfouz, Tarek M. Mahmoud, Ahmed Sharaf Eldin (2017) A survey on behavioral biometric authentication on smartphones, Journal of Information Security and Applications, Volume 37, December 2017, Pages 28-37.

[62] Neyire Deniz Sarier (2018) Multimodal biometric Identity Based Encryption, Future Generation Computer Systems, Volume 80, March 2018, Pages 112-125.

[63] Kien Nguyen, Clinton Fookes, Sridha Sridharan, Massimo Tistarelli, Mark Nixon (2018) Super-resolution for biometrics: A comprehensive survey, Pattern Recognition, Volume 78, June 2018, Pages 23-42.

[64] Marta Gomez-Barrero, Christian Rathgeb, Guoqiang Li, Raghavendra Ramachandra, Christoph Busch (2018) Multi-biometric template protection based on bloom filters, Information Fusion, Volume 42, July 2018, Pages 37-50.