Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Biometrics authentication techniques: A comparative study

Noor Alyanis, Shukor Razak *, Arafat Al-Dhaqm

Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia

ARTICLE INFO

Article history:
Received 20 December 2019
Received in revised form
7 June 2020
Accepted 7 June 2020

Keywords:
Biometric
Cryptosystem
Palm vein
Fuzzy vault scheme

ABSTRACT

Literature confirms that the biometric system lacks security and has numerous limitations and weaknesses. The disadvantages of this system come from the distinctness of biometric signals and the way it collects data and represents individuals, which is dependent on the method adopted to gather data, surroundings, the way users interact with the device, as well as the pathophysiological phenomena that arise due to variations in traits. In addition, this system has many problems in regard to forgery since, for instance, people's voices can be captured when they are expressing their passwords, the camera is able to take the photo of an iris from across the room, and fingerprints on surfaces can be removed. As a result, a key feature with a high strength against any attacks is needed to be utilized in a way to maximize the biometric system security. To this end, numerous techniques for biometric authentication have been proposed. The present study attempts to introduce different biometric authentication techniques like biometric cryptosystem and palm vein cryptosystem.

1. Introduction

In definition, biometric machines establish an individual's identity on the basis of his/her physical, chemical, or behavioral characteristics (Jain et al., 2004). Ali and Gaikwad (2016) maintained that biometrics is a certain technology measuring and studying the features of the human body to be applied to user authentication processes, and its work is entirely dependent upon two concepts: Uniqueness and permanence. The former guarantees that there will not be any similarity between the same biometric information of two individuals, while the latter guarantees that the biometric characteristic never changes over time. Biometric features must be distinctive, universally-applicable, and obtainable (Jain et al., 2004). Thus, any pair of human beings do not have a similar biometric feature, even in the case of twins. In this research, a number of concepts related to biometric technologies are discussed, i.e., biometric authentication, biometric cryptosystem, palm vein cryptosystem, and hand biometrics.

The rest of the paper is organized as follows. Section 2 reviews and discusses the literature. Section 3 introduces biometric authentication. Section 4 presents the biometric cryptosystem. Section 5 explains the concepts related to hand biometric. Section 6 introduces the palm vein cryptosystem. Section 7 introduces biometrics authentication systems strengths, and weaknesses and finally, Section 8 concludes the whole study.

2. Literature review

As reported by the Healthcare Financial Management Association (HFMA, 2016), hospitals are still dependent upon manual processes during care experience. Such processes involve identifying the patients at registration and then the use of modalities like armbands and barcodes. In addition, lots of protocols have been established to follow, for instance, the use of two patient identifiers at the time of drawing blood, giving medication, etc. Despite the presence of such protocols, these methods do not offer high reliability because human errors are always probable along with these processes, which may lead to mistakes (some of them can be deadly) inpatient identification processes (HFMA, 2016). As a dependable way to address such challenges, a number of health organizations have started some investments on biometric technology to be applied to patient identification processes. It has been found an effective way to minimize the patient

* Corresponding Author.
Email Address: shukorar@utm.my (S. Razak)
https://doi.org/10.21833/ijaas.2020.09.015
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-8824-6069

misidentification-related problems and also to decrease medical records duplication. In biometric technology, unique biological identifiers are applied to matching the patients with their correct identity. Biometric systems are capable of measuring different physiological characteristics, such as palm print, palm vein, handprint, fingerprint, iris, etc.

Andalib and Abdulla-Al-Shami (2013) and Tome and Marcel (2015) argued that biometric systems are also vulnerable to various system attacks. These attacks generally make use of the weakness in the system infrastructure or administration. It could be because of the limited liveliness detection capability of the commonplace system, which can, in turn, reduce the security of the system. Attacks performed against the systems can be categorized into two main groups: direct attacks and indirect ones. Adversaries attack the sensor with the use of artificial biometric samples with no particular knowledge about the framework. On the other hand, for indirect attacks, the adversaries need to hold additional information in regard to the internal structure, and they have to gain direct access to some components of the application (Ratha et al., 2001). Ngadi et al. (2012) proposed a mechanism that utilizes the dependency relationship among items to detect and prevent malicious data by calculating a number of relations among data items.

The use of a biometric system may cause two significant effects: Refusal of service and intrusion (Jain et al., 2008). The former takes place in case a legal user fails to obtain services s/he is completely qualified for because the infrastructure is attacked, and the user is kept deprived of gaining access to the system. On the other hand, the latter (intrusion) happens in case an attacker has obtained access to the system illegally, which could be due to low security and/or loss of private data. The big problem is that when a biometric template is utilized, it cannot be easily canceled, which is because of the absence of a revocation mechanism (Dhamija and Tygar, 2005); the template will then be rendered as unusable (Beng et al., 2008). Furthermore, according to Lalithamani and Sabrigiriraj (2014), the use of biometric information in situation identity attributes authentication to deliver a few nonminor tasks, which is because of the nature of biometric information. For instance, two successive analyses of specified biometrics do not bring about precisely the biometric template as matching against the stored template is probabilistic. In addition, storing biometric templates within a database together with more personally distinct data may lead to security/privacy hazards (Dhamija and Tygar, 2005). This is because the database can be highly susceptible to attacks that may set by insiders or outside adversaries, and also the database may be searched without justified reasons. In cryptographic, a significant issue related to the security system is key management. In case the key is selected too short or simple, attackers can simply break it, and if the key is stored in, for instance, a database, it can be lost or stolen, which causes threats for the system (Panchal and Samanta, 2016). If biometric data are leaked, it may result in significant privacy-related problems since biometric features are completely unique and stable for each person.

In random sequences, the key demonstrates the highest level of security; however, it is not easy to produce and memorize such keys rapidly. In addition, in case the key is disclosed, unauthorized parties are capable of determining the key producer or the person to whom the key is assigned (Ogiela and Ogiela, 2011). The process of biometric key authentication can also be subjected to different attacks, e.g., presentation of false biometrics, the matching unit corruption, attacking the channel between the template stored and the matching unit, tampering with the biometric feature presentation, etc. (Kannan and Asthana, 2012).

Apart from that, digital forensics has a relationship along with biometric systems to detect who the attacker is? How did the attack happen? And when did the attacking happen? For example, Ikuesan and Venter (2019) established an attribution approach based on heuristics built on traditional machine learning algorithms, with stress on the possibility of interactive mining constancy from the stochastic information of human performance. Digital investigation, explicitly in computer and network forensic, stands to increase much care from such social attribution process (Al-Dhaqm et al., 2017a). Several articles have been proposed for database forensics to detect and identify attackers or malicious activities (Al-Dhaqm et al., 2014; 2016; 2018; 2017b). Thus, biometric systems can be used with database forensic to detect and recognize database crimes.

3. Biometric authentication

In general, a biometric system creates a unique profile of the physical, chemical, or interactive characteristics of a certain individual (Jain et al., 2004). Biometric machines verify the individuals' identity in order to provide secure access to a certain system (Lalithamani and Sabrigiriraj, 2014). Biometrics can provide dependable tools to overcome the difficulty of individuals identified through the use of individuals' unique features (Jain et al., 2004). It proposes a strategy of high simplicity and security in a way to exactly verify people's identity, and also it assures the use of some identification tools that cannot be stolen, lost, or forgotten (Lalithamani and Sabrigiriraj, 2014). With the use of biometrics, individuals cannot make false denial claims since this system needs the individual to be present when the authentication process is being done (Jain et al., 2004). It also prevents unauthorized access (Adler, 2004).

According to Ali and Gaikwad (2016), biometrics is dependent upon two modes: Enrolment and recognition. At the enrolment step, biometric information is obtained by means of sensors and stored within a certain database together with the individual personal information to be used for

recognition purposes. After that, at the recognition step, the biometric information is obtained by means of the sensors, and then the information is compared to the previously-stored information to exactly determine the individual's identity. The enrolment and authentication processes are depicted graphically in Fig. 1.

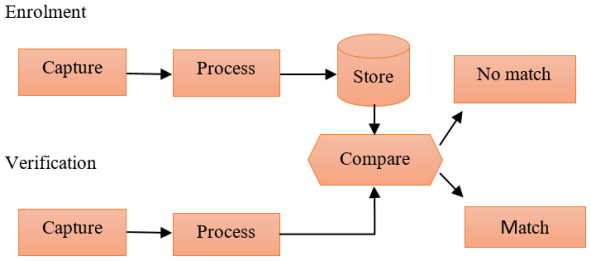

Fig. 1: The enrolment and authentication processes (Kothavale, 2004)

4. Biometric cryptosystem

Based on definitions proposed by Chafia et al. (2010) and Uludag et al. (2005), a biometric cryptosystem refers to a combination of the biometric components and cryptographic keys, which is typically known as a crypto-biometric system. Cryptography provides a high and adjustable level of security; it makes available non-repudiation and eliminates the need for memorization of the password or conveying tokens (Arul and Shanmugam, 2009).

In fact, the biometric cryptosystem makes a new integrated form combining biometrics and cryptography, aiming at exploiting the advantages of both fields. Cryptographic keys are generated through direct use of biometrics features (Balakumar and Venkatesan, 2012), which is consisted of long pseudo-random keys that cannot be memorized (Ayoub and Singh, 1984). Such characteristic controls and enhances the system security level for a long time (Balakumar and Venkatesan, 2012). The biometric cryptosystem combines biometric features and encryption (Sadkhan et al., 2016). In this combination, the biometric features play the role of individuals' authentication, while the standard key generation scheme addresses the other components related to controlling (Balakumar and Venkatesan, 2012). Fig. 2 displays the structure of a biometric system. Encoding the original data is performed by means of any key in a way to make it more and more complex. Then, it can be decoded whenever needed by means of the same key (Balakumar and Venkatesan, 2012). Two different levels can be observed in a biometric cryptosystem: Biometric-based key generation and biometric matching between input and enrolled biometric signal by means of the secret key (Verma and Jain, 2015). According to Arul and Shanmugam (2009) and Juels and Sudan (2006), the biometric cryptosystem comprises three modes: Key release, key binding, and key generation.

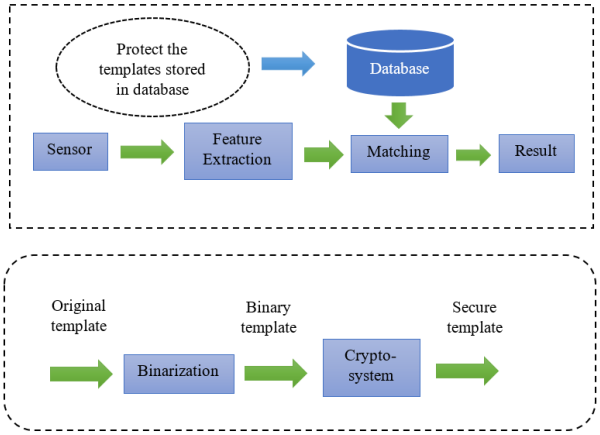

Fig. 2: Structure of a biometric system (Sadkhan et al., 2016)

5. Hand biometrics

The hand plays a fundamental role in the body of any human being. It is the most used part amongst other parts of the body during a day. Thus, in the field of biometrics, the hand is highly accepted by people to be used (Hao et al., 2006). Generally, hand biometrics is divided into three categories: Skin surface-based modality, internal structure-based modality, and global structure-based modality. Two recognized instances of the skin surface-based modality are palm print and fingerprint, in which the information related to the skin surface is explored and stored. An instance of the internal structure-based modality is the veins pattern, where the information related to the veins structure under the skin surface is used for recognizing purposes. The vein pattern is highly unique and consistent. Finally, hand geometry is an example of the global structure-based modality. This is an acceptable choice in the case of small-scale applications and high-performance price ratio (Hao et al., 2006). As indicated by Ali and Gaikwad (2016), the surface of fingertips contains some ridge and valleys that hold a high uniqueness for each individual; the fingerprint features remain unchanged throughout one's life. In addition, no two individuals can be found with the exactly similar fingerprints even in case of twins. In a fingerprint system, the ridges are marked by black lines, whereas the valleys are marked by white lines. The image of a fingerprint is depicted in Fig. 3.

Palm is another part of the hand that comprises ridges and valleys with a high uniqueness. Palm consists of flexion creases, secondary creases, and ridges (George et al., 2014). In a palm print, there are some important characteristics, namely the palm geometry, principle lines (life, heart, and head), wrinkles, minutiae, and delta point (Ali and Gaikwad, 2016). They comprise information required for accurate identification of an individual (Awate and Dixit, 2015) since they hold unique information (Nie et al., 2019). Fig. 4 displays the features in a palm print.

Fig. 3: Features on a fingerprint (Ali and Gaikwad, 2016)

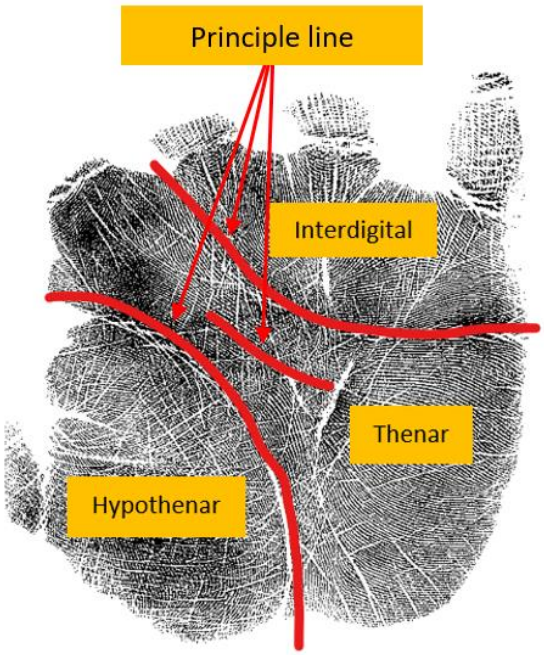

Fig. 4: Features of a palm print (Ali and Gaikwad, 2016)

When recorded, the palm print is shown as a set of dark lines. It represents a high peaking portion of the friction ridge skin, whereas the valleys that exist between the ridges are shown as white space and is with a low shallow portion friction ridge skin (Fig. 5) (George et al., 2014).

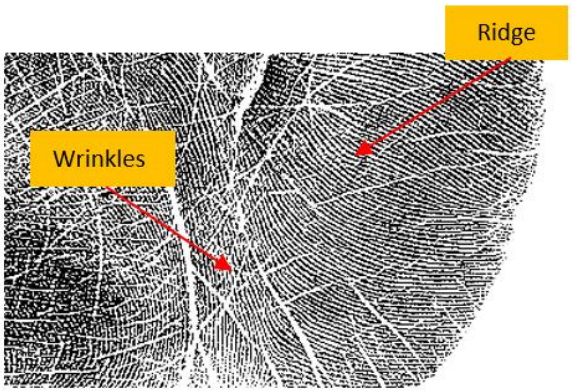

Fig. 5: Ridges in palm print (George et al., 2014)

In the palm vein authentication system, the individuals' palm vascular patterns are used as identification sources (Mahto and Yadav, 2013), as seen in Fig. 6. During the last decade, extensive studies have been carried out into the palm vein structure (Kumar and Prathyusha, 2009; Wu et al., 2008). The vein pattern of an individual is established in utero, and any two persons cannot be found with the same patterns of palm vein (Mahto and Yadav, 2013). Within the vein vessels, there is deoxidized hemoglobin that absorbs the light of the wavelength of roughly (7.6*10.4mm) in the near-infrared area (Miura et al., 2007). This way, we can observe some dark lines of blood vessel pattern that contains deoxidized hemoglobin molecules. The vein authentication device indeed translates the palm blood vessel pattern as black lines of infrared ray image (Mahto and Yadav, 2013).

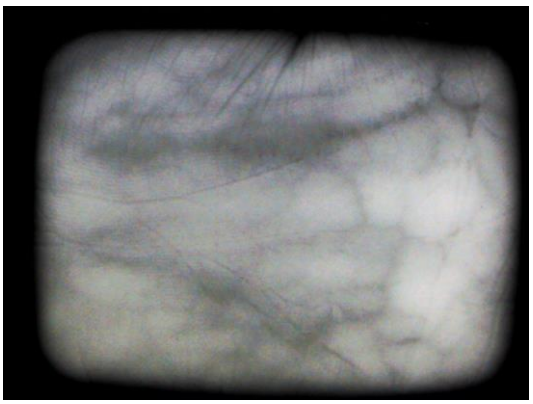

Fig. 6: Palm vein image (Mahto and Yadav, 2013)

6. Palm vein cryptosystem

The innovative technique of palm vein cryptosystem is used for identification purposes by means of the blood vessels that exist under individuals' palm skin (Zhou and Kumar, 2011). Palm vein is within the subcutaneous layer of palm skin; it is completely unique even in twins (Athale et al., 2015). Fig. 7 displays the cross-section anatomy of palmer skin.

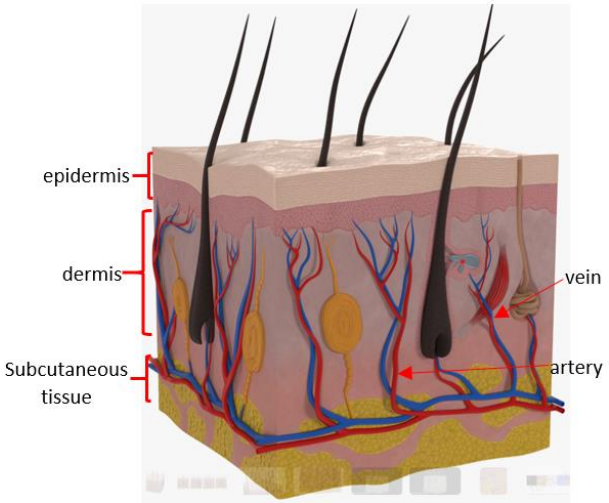

Fig. 7: Cross-section anatomy of palmer skin (Zhou and Kumar, 2011)

The most reliable and secure biometric modality is a palm vein since this cannot be easily copied and faked. This is because palm vein cannot be observed directly by eyes under ordinary light (Athale et al., 2015). This unique feature will remain unchanged during an individuals' lifetime (Zhou and Kumar, 2011). Thus, it offers an accurate, reliable, and cost-efficient tool for identification (Athale et al., 2015).

The palm vein cryptosystem involves four steps: Acquiring an image, preprocessing, extracting features, and producing a key. Numerous low-cost vein acquisition systems have been proposed in the literature to take the image needed for the above-mentioned processes (Raghavendra et al., 2014). During the acquisition step, the image of the palm vein is obtained by means of a near-infrared (NIR) illumination since it is not possible to penetrate with ordinary light. The volume of hemoglobin within the individual's blood affects the penetration of light; therefore, the visibility of different veins is different in infrared light.

Then, the obtained image is subjected to preprocessing steps for smoothing and enhancement purposes in a way to make the image completely suitable for the following processes. Through the image preprocessing process, blur, noise, and background are eliminated (Chavez-Galaviz et al., 2015). This step also involves cropping and scaling of the image to discard the undesirable parts and achieve the region of interest (ROI) and then improving the sharpness/smoothness of ROI. On the one hand, the ROI size should not encroach into the background areas, and on the other hand, it needs to be wide enough to preserve the pattern texture (Harmer and Howells, 2012).

After that, the image is transformed into a grey-scale format to extract the required features, where the image contains grey shades ranging between white and black colors. Then, the global threshold segmentation method is used to convert the image into a binary format (Chavez-Galaviz et al., 2015). This format comprises only two digits, i.e., 0 and 1. After that, the obtained binary image is exposed to the thinning algorithm for the aim of obtaining the vein skeleton that is applicable to the feature extraction process (Chavez-Galaviz et al., 2015). As the binary image has a noise that comes from the threshold segmentation, it needs to be subjected again to the enhancement process by means of, at first, the Guided Filtering and then the Gabor filtering (Harmer and Howells, 2012). Segmentation noise is decreased using the morphological operation.

Then, it turns to perform the key production process through which the feature already extracted is encrypted in order to create a unique key. Literature consists of numerous approaches to the production of the unique key or the cryptosystem; the approaches include RSA algorithm, Blowfish cryptographic algorithm, Fuzzy commitments, etc. (Athale et al., 2015). As stated by (Nagar et al., 2011), the Fuzzy commitment scheme is applied to biometric encryption. It operates based on binary vectors. The Blowfish cryptographic algorithm makes use of a single key for both encryption and decryption (Balakumar and Venkatesan, 2012). RSA is known as a public cryptography algorithm offering a system for not only encryption but also authentication.

7. Strengths and weaknesses

The proposed biometrics authentication systems have strengths and weaknesses, as shown in Table 1.

Table 1: Strengths and weaknesses of proposed biometrics authentication systems

Features	Strengths	Weaknesses	Reference
Fingerprint	Fingerprint characteristic does not change along with life	Fingerprint is exposed to cuts	(Ali and Gaikwad, 2016)
Palm print	Greater surface area and contain more minutiae compared to fingerprint. More deformable than fingerprint. Ridges present in palms are unique and persistent. More distinctive than a fingerprint. Vary in quality of discrimination power and skin distortion	Appearance is sensitive to illumination condition, aging, skin disease and abrasion	(Banerjee et al., 2018; George et al., 2014; Hao et al., 2006)
Finger vein	Cannot be forged. Ensure the vitality of the authorized person. Characteristic does not change along a lifetime. Unique and no two people have the same vein pattern	Small region of interest	(Banerjee et al., 2018; Ali and Gaikwad, 2016)
Palm vein	Has broader and more complicated vascular pattern. Contain a wealth of differentiating features for personal identification. Less susceptible to change in skin color, unlike finger or back of the hand. Offer contactless authentication. Provides hygienic and non-invasive solution thus promoting a high level of user acceptance. Difficult to forged and contributes to a high level of security because it measures the hemoglobin flow through veins internal of the body. Cannot be stolen by photographing, tracing, and recording. Not susceptible to minor trauma, cuts and etc. because the vein is inside hand, so they are protected. Has no hair, thus eliminates an obstacle to capturing the vein pattern	Acquisition device is expensive	(Mahto and Yadav, 2013)

8. Conclusion

The previous works of the biometrics authentication systems discovered that biometric systems have several limitations and weaknesses. The disadvantages of this system come from the distinctness of biometric signals and the way it collects data and represents individuals, which is dependent on the method adopted to gather data, surroundings, the way users interact with the device, as well as the pathophysiological phenomena that arise due to variations in traits. In addition, this

system has many problems in regard to forgery since, for instance, people's voices can be captured when they are expressing their passwords, the camera is able to take the photo of an iris from across the room, and fingerprints on surfaces can be removed. As a result, a key feature with a high strength against any attacks is needed to be utilized in a way to maximize the biometric system security. To this end, numerous techniques for biometric authentication have been proposed. The present study attempts to introduce different biometric authentication techniques like biometric cryptosystem and palm vein cryptosystem. Future work will include developing a cryptographic key generation from palm vein using a fuzzy vault scheme to detect and prevent the privacy of data.

Acknowledgment

This work was supported by the Ministry of Education Malaysia through TRGS under Grant R.J130000.7813.4L844.

Compliance with ethical standards

Conflict of interest

The authors declare that they have no conflict of interest.

References

Adler A (2004). Images can be regenerated from quantized biometric match score data. In the Canadian Conference on Electrical and Computer Engineering, IEEE, Niagara Falls, Canada, 1: 469-472.

Al-Dhaqm A, Abd Razak S, Othman SH, Nagdi A, and Ali A (2016). A generic database forensic investigation process model. Jurnal Teknologi, 78(6-11): 45-57. https://doi.org/10.11113/jt.v78.9190

Al-Dhaqm A, Razak S, and Othman SH (2018). Model derivation system to manage database forensic investigation domain knowledge. In the IEEE Conference on Application, Information and Network Security, IEEE, Langkawi, Malaysia: 75-80. https://doi.org/10.1109/AINS.2018.8631468

Al-Dhaqm A, Razak S, Othman SH, Choo KKR, Glisson WB, Ali A, and Abrar M (2017a). CDBFIP: Common database forensic investigation processes for internet of things. IEEE Access, 5: 24401-24416. https://doi.org/10.1109/ACCESS.2017.2762693

Al-Dhaqm A, Razak S, Othman SH, Ngadi A, Ahmed MN, and Mohammed AA (2017b). Development and validation of a database forensic metamodel (DBFM). PloS One, 12(2): e0170793. https://doi.org/10.1371/journal.pone.0170793 **PMid:28146585 PMCid:PMC5287479**

Al-Dhaqm AMR, Othman SH, Razak SA, and Ngadi A (2014). Towards adapting metamodelling technique for database forensics investigation domain. In the International Symposium on Biometrics and Security Technologies, IEEE, Kuala Lumpur, Malaysia: 322-327. https://doi.org/10.1109/ISBAST.2014.7013142

Ali MMH and Gaikwad AT (2016). Multimodal biometrics enhancement recognition system based on fusion of fingerprint and palmprint: A review. Global Journal of Computer Science and Technology, 16(2): 1-15.

Andalib AS and Abdulla-Al-Shami M (2013). A novel key generation scheme for biometric cryptosystems using fingerprint minutiae. In the International Conference on Informatics, Electronics and Vision, IEEE, Dhaka, Bangladesh: 1-6. https://doi.org/10.1109/ICIEV.2013.6572670

Arul P and Shanmugam A (2009). Generate a key for AES using biometric for VOIP network security. Journal of Theoretical and Applied Information Technology, 5(2): 107-112.

Athale SS, Patil D, Deshpande P, and Dandawate YH (2015). Hardware implementation of palm vein biometric modality for access control in multilayered security system. Procedia Computer Science, 58: 492-498. https://doi.org/10.1016/j.procs.2015.08.013

Awate I and Dixit BA (2015). Palm print based person identification. In the International Conference on Computing Communication Control and Automation, IEEE, Pune, India: 781-785. https://doi.org/10.1109/ICCUBEA.2015.156

Ayoub F and Singh K (1984). Cryptographic techniques and network security. IEE Proceedings F-Communications, Radar and Signal Processing, 131(7): 684-694. https://doi.org/10.1049/ip-f-1.1984.0103

Balakumar P and Venkatesan R (2012). A survey on biometrics based cryptographic key generation schemes. International Journal of Computer Science and Information Technology and Security, 2(1): 80-85.

Banerjee A, Basu S, Basu S, and Nasipuri M (2018). ARTeM: A new system for human authentication using finger vein images. Multimedia Tools and Applications, 77(5): 5857-5884. https://doi.org/10.1007/s11042-017-4501-8

Beng A, Teoh J, and Toh KA (2008). Secure biometric-key generation with biometric helper. In the 3rd IEEE Conference on Industrial Electronics and Applications, IEEE, Singapore, Singapore: 2145-2150. https://doi.org/10.1109/ICIEA.2008.4582898

Chafia F, Salim C, and Farid B (2010). A biometric crypto-system for authentication. In the International Conference on Machine and Web Intelligence, IEEE, Algiers, Algeria: 434-438. https://doi.org/10.1109/ICMWI.2010.5648101

Chavez-Galaviz J, Ruiz-Rojas J, García-González A, and Fuentes-Aguilar RQ (2015). Embedded biometric cryptosystem based on finger vein patterns. In the 12th International Conference on Electrical Engineering, Computing Science and Automatic Control, IEEE, Mexico City, Mexico: 1-6. https://doi.org/10.1109/ICEEE.2015.7357994

Dhamija R and Tygar JD (2005). The battle against phishing: Dynamic security skins. In the Symposium on Usable Privacy and Security, Association for Computing Machinery, Pittsburgh, USA: 77-88. https://doi.org/10.1145/1073001.1073009

George A, Karthick G, and Harikumar R (2014). An efficient system for palm print recognition using ridges. In the International Conference on Intelligent Computing Applications, IEEE, Coimbatore, India: 249-253. https://doi.org/10.1109/ICICA.2014.60 **PMid:25208960**

Hao F, Anderson R, and Daugman J (2006). Combining crypto with biometrics effectively. IEEE Transactions on Computers, 55(9): 1081-1088. https://doi.org/10.1109/TC.2006.138

Harmer K and Howells G (2012). Direct template-free encryption key generation from palm-veins. In the 3rd International Conference on Emerging Security Technologies, IEEE, Lisbon, Portugal: 70-73. https://doi.org/10.1109/EST.2012.20

HFMA (2016). The value of precise patient identification. Healthcare Financial Management Association, Illinois, USA.

Ikuesan AR and Venter HS (2019). Digital behavioral-fingerprint for user attribution in digital forensics: Are we there yet? Digital Investigation, 30: 73-89. https://doi.org/10.1016/j.diin.2019.07.003

Jain AK, Nandakumar K, and Nagar A (2008). Biometric template security. EURASIP Journal on Advances in Signal Processing, 2008: 113. https://doi.org/10.1155/2008/579416

Jain AK, Nandakumar K, Lu X, and Park U (2004). Integrating faces, fingerprints, and soft biometric traits for user recognition. In the International Workshop on Biometric Authentication, Springer, Prague, Czech Republic: 259-269. https://doi.org/10.1007/978-3-540-25976-3_24

Juels A and Sudan M (2006). A fuzzy vault scheme. Designs, Codes and Cryptography, 38(2): 237-257. https://doi.org/10.1007/s10623-005-6343-z

Kannan PM and Asthana A (2012). Secured encryption algorithm for two factor biometric keys. International Journal of Latest Research in Science and Technology, 1(2): 102-105.

Kothavale M, Markworth R, and Sandhu P (2004). Computer security SS3: Biometric authentication. Available online at: https://bit.ly/3fBvuHU

Kumar A and Prathyusha KV (2009). Personal authentication using hand vein triangulation and knuckle shape. IEEE Transactions on Image Processing, 18(9): 2127-2136. https://doi.org/10.1109/TIP.2009.2023153 **PMid:19447728**

Lalithamani N and Sabrigiriraj D (2014). Technique to generate a face and palm vein-based fuzzy vault for a multi-biometric cryptosystem. Machine Graphics and Vision, 23(1/2): 97-114. https://doi.org/10.1179/1743131x14Y.0000000090

Mahto D and Yadav DK (2013). Network security using ECC with Biometric. In the International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Springer, Greader Noida, India: 842-853. https://doi.org/10.1007/978-3-642-37949-9_73

Miura N, Nagasaka A, and Miyatake T (2007). Extraction of finger-vein patterns using maximum curvature points in image profiles. IEICE Transactions on Information and Systems, 90(8): 1185-1194. https://doi.org/10.1093/ietisy/e90-d.8.1185

Nagar A, Nandakumar K, and Jain AK (2011). Multibiometric cryptosystems based on feature-level fusion. IEEE Transactions on Information Forensics and Security, 7(1): 255-268. https://doi.org/10.1109/TIFS.2011.2166545

Ngadi M, Al-Dhaqm R, and Mohammed A (2012). Detection and prevention of malicious activities on RDBMS relational database management systems. International Journal of Scientific and Engineering Research, 3(9): 1-10.

Nie W, Zhang B, and Zhao S (2019). Discriminative local feature for hyperspectral hand biometrics by adjusting image acutance. Applied Sciences, 9(19): 4178. https://doi.org/10.3390/app9194178

Ogiela MR and Ogiela L (2011). Image based crypto-biometric key generation. In the 3rd International Conference on Intelligent Networking and Collaborative Systems, IEEE, Fukuoka, Japan: 673-678. https://doi.org/10.1109/INCoS.2011.102

Panchal G and Samanta D (2016). Comparable features and same cryptography key generation using biometric fingerprint image. In the 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics, IEEE, Chennai, India: 691-695. https://doi.org/10.1109/AEEICB.2016.7538381

Raghavendra TVS, Arudhra N, Amaranath K, Raviteja B, and Sreekar G (2014). Humanitarian supply chain model for flood relief-a case study analysis. International Journal of Engineering Research and Technology, 3(1): 3538-3547.

Ratha NK, Connell JH, and Bolle RM (2001). An analysis of minutiae matching strength. In the International Conference on Audio-and Video-Based Biometric Person Authentication, Springer, Halmstad, Sweden: 223-228. https://doi.org/10.1007/3-540-45344-X_32

Sadkhan ESB, Al-Shukur BK, and Mattar AK (2016). Survey of biometrie based key generation to enhance security of cryptosystems. In the Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications, IEEE, Baghdad, Iraq: 1-6. https://doi.org/10.1109/AIC-MITCSA.2016.7759942

Tome P and Marcel S (2015). On the vulnerability of palm vein recognition to spoofing attacks. In the International Conference on Biometrics, IEEE, Phuket, Thailand: 319-325. https://doi.org/10.1109/ICB.2015.7139056

Uludag U, Pankanti S, and Jain AK (2005). Fuzzy vault for fingerprints. In the International Conference on Audio-and Video-Based Biometric Person Authentication, Springer, Rye Brook, USA: 310-319. https://doi.org/10.1007/11527923_32

Verma I and Jain SK (2015). Biometrics security system: A review of multimodal biometrics based techniques for generating crypto-key. In 2nd the International Conference on Computing for Sustainable Global Development, IEEE, New Delhi, India: 1189-1192.

Wu X, Wang K, and Zhang D (2008). A cryptosystem based on palmprint feature. In the 19th International Conference on Pattern Recognition, IEEE, Tampa, USA: 1-4. https://doi.org/10.1109/ICPR.2008.4761117

Zhou Y and Kumar A (2011). Human identification using palm-vein images. IEEE Transactions on Information Forensics and Security, 6(4): 1259-1274. https://doi.org/10.1109/TIFS.2011.2158423