Efficient palm vein authentication encryption technique in wireless implantable medical devices

Ahlam Almukhlifi, Saad M. Almutairi
Master of Information Security, Department of Information Technology, Faculty of Computers and Information Technology, University of Tabuk, Tabuk, Saudi Arabia

Article Info

Article history:

Received Dec 22, 2022
Revised Jan 14, 2023
Accepted Jan 19, 2023

Keywords:

Biometric encryption
Hashing
Implantable medical device security
Palm vein authentication
Wireless security
Zero-watermarking

ABSTRACT

Implantable medical devices (IMD) are commonly utilized to treat chronic illnesses. Many IMD communicate in wireless mode using an external programmer, which raises security concerns. Security of IMD is a critical issue which assaults direct harm to patients. Many researches are carried out on IMD security and challenges when the patient is not in a critical situation. Still, it would be a major issue while the patient is unconscious. In this research, a novel scheme for emergency secure access control of IMD was proposed to improve the security of biometric-based IMD schemes. The proposed authentication scheme uses a combination of palm vein and zero-watermark to generate encrypted credential data for IMDs. Using quantitative assessment for evaluating images, such as the peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), and the mean squared errors (MSE), the suggested framework is shown to be superior to existing methods. Two other study goals are improved efficiency and image quality at a lower computational cost.

Corresponding Author:

Saad M. Almutairi
Master of Information Security, Department of Information Technology
Faculty of Computers and Information Technology, University of Tabuk
Tabuk, Saudi Arabia
Email: s.almutairi@ut.edu.sa

1. INTRODUCTION

Wireless communication technology is progressive, when it is being integrated into healthcare and medical devices. It will be more effective in real-time medical based applications by providing prompt replies to patients on time. The quality of life of many people has improved dramatically as a result of these advancements [1]. Wireless communication is available on all contemporary implantable medical devices (IMD), together with cardiac pacemakers, implantable cardioverter-defibrillators (ICDs), neurostimulators, and insulin pumps. Modern IMDs have a radio transmitter that allows them to interconnect with a "programmer," an exterior device. An approved IMD systems analyst is able to carry out instructions to change IMD arrangement locations and therapy-related parameters, as well as obtain critical information for health observation [2]. However, some researchers have shown that effective attacks on IMDs not only conciliation the privacy of therapeutic information but can also trigger malevolent actions in the IMD, potentially harming or even killing a patient [3], [4]. So, it's critical to keep sensitive data safe from adversaries [5]. A key difficulty in the IMD security design is balancing security and accessibility [5], [6]. This study aims to rise the security of the IMD in emergency medical situations, which constitutes one example: decision making, devices with more computing, and message competences. Some examples of IMD are shown in Figure 1. Figure 1(a) shows an artificial pacemaker, Figure 1(b) shows a Medtronic InterStim neuro-stimulation device, Figure 1(c) shows a semi-implanted insulin pump monitor and Figure 1(d) shows a cochlear implant.

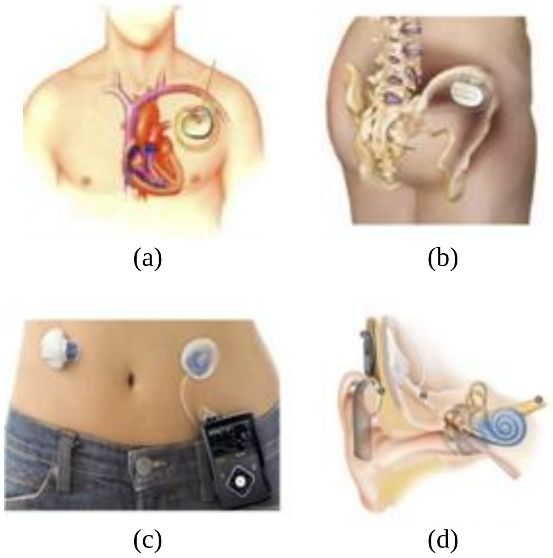


Figure 1. Implantable medical devices [6] (a) artificial pacemaker, (b) Medtronic InterStim neuro-stimulation device, (c) semi-implanted insulin pump monitor, and (d) a cochlear implant

Traditional security, such as knowledge-based and object-based solutions, is not applicable here because of the use of security keys or credentials to authenticate programmers to IMDs. So, quickly recovering credentials or keys in an emergency is very difficult. This authentication is normally accepted by requesting a person who claims they are to supply one or more of three components that based on: knowledge-based (like a password, personal identification number (PIN)), object-based (like a physical key, identification (ID) cards), or body characteristics based (like a fingerprint, palm vein) [7]. Otherwise, biometric methods are recommended in an emergency due to biometrics are permanent, universal and inherent (every person is carrying), cannot be lost or forgotten, are unique, efficient, have a higher perceived degree of security, recordable and measurable [8]. Various biometric-based resolutions have been projected to handle the particular difficulty of balancing security and accessibility for the IMD during an emergency. Security schemes based on scanning a patient's fingerprint [9], electrocardiogram (ECG) signals [10], utilizing patients' iris data [11], using the patient fingerprint to unlock their smart-phone [12]. The collaborative design approaches, including minimizing peel and cleavage-loading circumstances, should expand to accommodate the ever-shrinking device sizes. Biometrics technologies have played a significant role in gaining access to secure places and simplifying the identifying process of people in comparison to traditional techniques such as cards, passwords, and so on [13]. Among the various biometrics, fingerprint is more feasible for developing a secured solution towards a system [14]. The author comes with finger-to-heart (F2H) IMD authentications mechanism in this work to address the security-accessibility trade-off [15]. All biometrics mentioned above have issues and are inappropriate to use with IMD:

- The drawbacks of fingerprint are: fingerprint is more exposition to change with time because it is exposed to the elements and is subject to cuts and damage. Cuts and scrapes on the finger might cause fingerprint scanners to fail to recognize a valid user, resulting in IMD rejecting access (false reject); some users are unable to enrolling the system, and the accuracy and operation of the system are influenced by people's skin problems.
- While the drawback of an Iris scan is that it can't utilize a normal camera, and visible light must keep to a minimum for the best accuracy, it is affected by some diseases such as cataracts and require cooperation from the user. That means if an unconscious patient, doctors cannot access the IMD.
- The drawback of ECG signals is that the IMD must detention and progression biometric characteristics each time a secure get-to attempt is made, which requires many resources within the IMD. Hence, resource consumption is the major concern when implementing the security based on ECG to the IMD [16].

Salt generation for hashing approaches using electrocardiogram reading for immediate accessibility to IMD was developed by Belkhouja *et al*. [17]. Here, the patient's current heartbeat serves as the verification key. These details will be fed into a method to produce a hash tail for use in exchanging data in between IMD and the future healthcare system. Electrocardiogram (ECG) signal-based safety systems, in which a physician brings attention to the patients IMD through analyzing patient's actual ECG signals, have also been investigated in some papers [18], [19].

Hei and Du [11] comes with biometrics-based two-levels protected accesses controls for IMD during emergency [20]. In this paper, the researchers introduce a unique biometrics-based two-levels secured access control (BBS-AC) method for IMDs in emergencies in this work (e.g., in an Unconscious). Ahmad *et al.* [20] develop light weight and privacy-preserving templates generations for palm vein-based human recognitions [21] and proposed a wave atoms transforms (WAT) based palm vein recognitions method that is both efficient and privacy-preserving. Mishra *et al.* [21] comes with a lossless model for the identification of biometric images for the generation of unique digital code [22]. Although the admirable attempts created by the academic communities, there were still problems that need to be solved, including insufficient fundamental capabilities, higher communications and computational overheads, and formal lag in security verifications [23]. Dorsal hand vein (DHV) biometrics, one of the newest biometrics technologies, has drawn a lot of attention lately [24]. This study develops a hybrid verification method that was depended on biometrics and encryptions technologies. This study uses sophisticated standards of encryption as the reliable encryption systems and fingerprint as a biometric technology for achieving stronger and reliable techniques [25]. The multi-biometric systems that identify people using hand-based modalities are the subject of this work. Additionally, it discusses alternative feature extraction strategies and analyses their effectiveness using one of the biometric systems' performance indicators [26]. The proposed bio-cryptosystem maintains cancellable feature vectors online in encrypted form, which was utilised to identify or validate the subjects following decryptions [27]. The research gap table is given in Table 1 with advantages and disadvantages.

The research presented was ordered as shown in: section 2 provides system architecture of the research method. Section 3 provides a description of the scientific procedures that have been followed in a proposed work. The experimental setup, output and the discussions are represented in section 4. Section 5 concludes the work.

Table 1. Research gap with their advantages and disadvantages

Method	Advantages	Disadvantages
Hashing schemes [17]	This approach sought to resolve the problem of granting access to the IMD for medical care in an urgent situation, even without the user's participation.	Nevertheless, IMDs are vulnerable to hacking with such wireless technologies.
H2H [18-20]	Not even like what's needed for urgent access, these procedures save resources.	But suppose an incapacitated patient with this IMD is transported to an unknown emergency department. In that case, any doctors who don't have the right security permissions won't be able to access the IMD.
Finger-to-Heart (F2H) [15]	With this, concerns for the patient's well-being and the need for a high-security level are addressed.	The fingerprint picture will not be taken if the glass area where the finger stays during the detection phase has been scratched, which is a problem, especially for older persons with a heritage of forced work.
BBS-AC [21]	There is a risk that the implant, and the patient's health, might be compromised in this way.	The criminals may easily steal the fingerprint and use it to make a false one.
WHAT [22]	Particularly useful for low-capacity authentication systems, this technique solves the problems of pattern storage, calculation, the privacy of identity features, and efficiency reliability.	Because of their size and location, these IMD have limited resources, including power, memory, and processing speed, that must be included in any proposed security measures.
Zero watermarking approaches [23]	This ID is a meaningless piece of paper devoid of personal or identifying information about the owner.	In addition, a protection solution's viability depends on its ability to handle crises and everyday situations.

2. PROPOSED SECURE AN IMD WITH PALM VEIN METHOD

Figure 2 depicts a system architecture to encourage the implementation of palm vein-based security techniques in an IMD. IMD is a medical device that is entrenched into the body of a patient. An external reader (programmer) could use the wireless communication channel to connect with the IMD. The IMD system comprises the IMD and the programmer that goes with it. IMD will extract the palm vein features and store it with an associated person for future use. Figure 3 depicts the outline of the proposed work. The functionalities and hardware following must add to the existing IMD systems to deploy the palm vein-based IMD security models.

- Process-A is palm vein acquisition-> ROI->feature exaction ->PVC.
- Process B generates a digital binary of personal identity/zero-watermark.
- V1. Ensuring integrity and authentication using correlation coefficient.

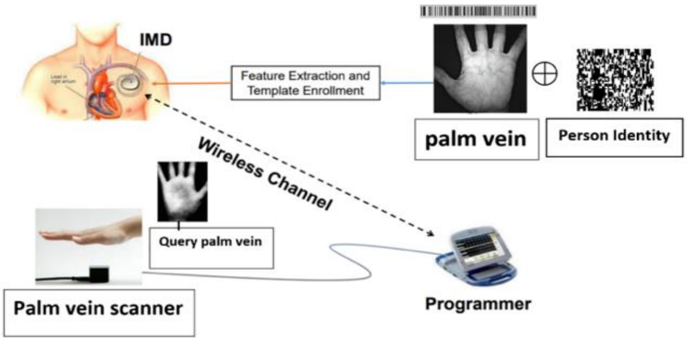


Figure 2. Palm vein-based IMD security architecture

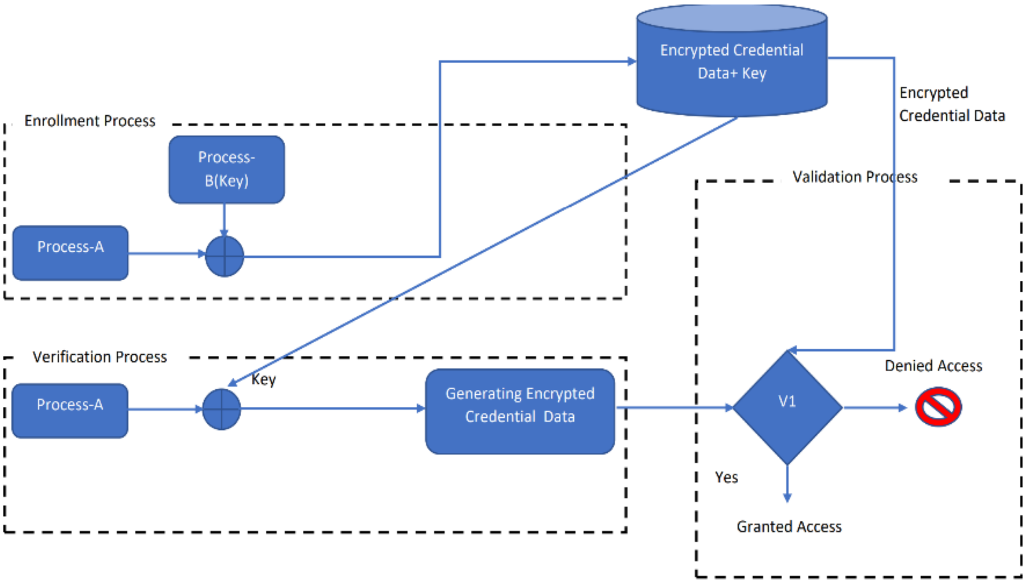


Figure 3. Outline of the work

2.1. Zero watermark generation

Assuming the user's palm vein image is PV with the dimensions is $N \times N$, and the corresponding two-fold watermark palm vein image is BPV, $BPV = \{BPV(i,j) \in \{0,1\}, 0 \leq i < I, 0 \leq j < J\}$, and the size is $I \times J$. The detailed phases of the zero-watermark production stage are given as:

- Calculating the coefficients of PVCs: in this phase, compute the maximum order x_{max} [24] PVCs of the host PV image and have total $T = (X_{max} + 1)^2$ features, where a T- length vector of the amplitudes is created.
- Feature selection (FS) is constructed on the typical assortment criteria in [25] and retaining a secret key, $SK_1, I \times J$ quantity, which is the watermark image dimensions, the accurate and precise premature ventricular contractions (PVCs) coefficient set, M would be $M = \{|PVC_{i,j}|, j \neq 4m, m \in N\}, i,j = 1,2,\ldots,N$.
- Feature vector generation, where the $I \times J$ of PVCs constants produced in FS is used for the feature image creation. The $I \times J$ amount PVCs instants is arbitrarily designated from the designed PVCs moments (set M), where compute the bounties and yield the vector $V = \{v(i), 0 \leq i < I \times J\}$.
- Binary feature vector generation: the two-fold feature categorization $BPV = \{BPV(i), 0 \leq i < I \times J\}$ is obtained from the feature direction/sequence V, is shown in (1):

$$BPV_i = \begin{cases} 1 & if\ V_i \geq Th \\ 0 & if\ V_i < Th \end{cases} \tag{1}$$

where Th is the threshold that depends on mean value of V, the binarized direction/sequence BPV was rearranged into a 2D binary feature image, T, with the size of $I \times J$.

- Watermark palm vein image generation: the achieved XOR process is used in scrambling the watermark image, $WPVC$ [24] and the image's feature T to produce the zero-watermark as given in (2).

$$WPVC_{zero}: WPVC_{zero} = T \oplus WPVC \tag{2}$$

2.2. Recognition of the watermark

Here mostly detect, the palm vein image's watermark data in the recognition phase, autonomous of the original images. Extraction of watermark image: the contrary procedure of scrambling can excerpt and visually vacate the watermark, and $WPVC^*$ is reversely scrambled using the key, $SK_2$of 1D-Chebyshev map to get the retrieved watermark, $WPVC^*$ denoted as $WPVC^* = \{WPVC^*\ (i,j) \in \{0,1\}, 0 \le i < I, 0 \le j < J\}$.

2.3. Palmvein authentication

The IMD authentication technique has been classified into two different phases. In the first phase, the user personal details are enrolled, and it is called enrolment process. The acquired information from the person is validated in the second phase of verification process, as shown in the Figure 2.

2.3.1. Palm vein authentication algorithm using zero-watermark

The entire procedure could be functioned in two steps: the first is to produce the encrypted credential template to guarantee confidentiality, and the second is to validate the integrity and authentication of the patient and the Pseudocode 1:

Pseudocode 1. The proposed zero-watermarking approach

```
Input: Palm vein image
Output: Secure palm vein image
Procedure call key generation ()
original image $PV$ in square size $N \times N$;
begin
calculating the coefficients of PVC and calculating $T = (X_{max} + 1)^2$;
$Sk_1$ =average value of 64 pixels of resulting $I \times J$ coefficient;
Calculation of feature vector and generate PVCs coefficients
Compute vector $V$;
Generate binary feature sequence $BPV$;
Perform XOR operation and generate watermark image, $WPVC$;
End
Reverse watermark generation $WPVC^*$ using $SK_2$
Produce the result of a secure PV image.
A. Production of encrypted credential data:
   1. Read entered image (Palm Vein).
   2. Generate a unique palm vein design from the palm vein image.
   3. Generate encrypted palm vein code from unique palm vein pattern of Palm vein image.
   4. Generate a digital binary of personal identity.
   5. Encrypted Credential Data =XOR (PVC, person ID).
   6. stored the encrypted credential data + key (binary person identity)
B. Validation process:
   1. Read the Acquired PV.
   2. Generate a unique palm vein design from the palm vein image.
   3. Generate encrypted palm vein code from unique palm vein design of Palm vein image.
   4. Retrieve the key
   5. Generating encrypted credential data by XOR retrieve key and encrypted PVC.
   6. IF (login successful) by verifying Reference encrypted credential data == Acquired
      encrypted credential data.
        THEN access IMD
        ELSE the access to IMD is a block
      END IF;
```

3. RESULTS AND DISCUSSION

System model: the proposed system will ensure integrity, confidentiality and authentication. Guarantee integrity and authentication during the validation/verification process, and guarantee confidentiality that the encrypted credential template stored in IMD is cancellable, which is absolutely uninformative and does not reveal biometric information. Three factors were applied to quantify the efficacy of the suggested method (PV with zero-watermark), such as mean squared errors (MSE), structural similarity (SSIM) and peak signal-to-noise ratio (PSNR) (dB).

Table 2. The numerical results of existing and proposed methods based on PSNR (dB), MSE and SSIM

Number of images	PSNR (dB)			MSE			SIM		
	Hashing	zero watermarking	PV with zero-watermark	Hashing	zero watermarking	PV with zero-watermark	Hashing	zero watermarking	PV with zero-watermark
4	26.21	28.56	30.25	0.019	0.017	0.015	0.7321	0.7541	0.8358
8	27.56	30.14	31.48	0.018	0.015	0.013	0.7841	0.7956	0.8567
12	29.63	31.56	32.69	0.017	0.012	0.012	0.8014	0.8452	0.8789
16	31.25	32.59	39.65	0.015	0.01	0.008	0.8241	0.8564	0.8896
20	32.15	33.54	49.95	0.012	0.009	0.0025	0.8362	0.8741	0.9289

- PSNR: this is extensively used to measure the watermarked image's quality. The constraint was described as the peak signal ratio authority to the level of noises in the reversed watermarked medical data $WPVC^*$ as stated in (3). A higher PSNR value indicates a better denoising ability of the scheme.
- MSE: this is a usually used falsification measure and evaluates the average of the square of errors as shown in (4). The MSE is nonnegative, and standards nearer to zero are healthier.

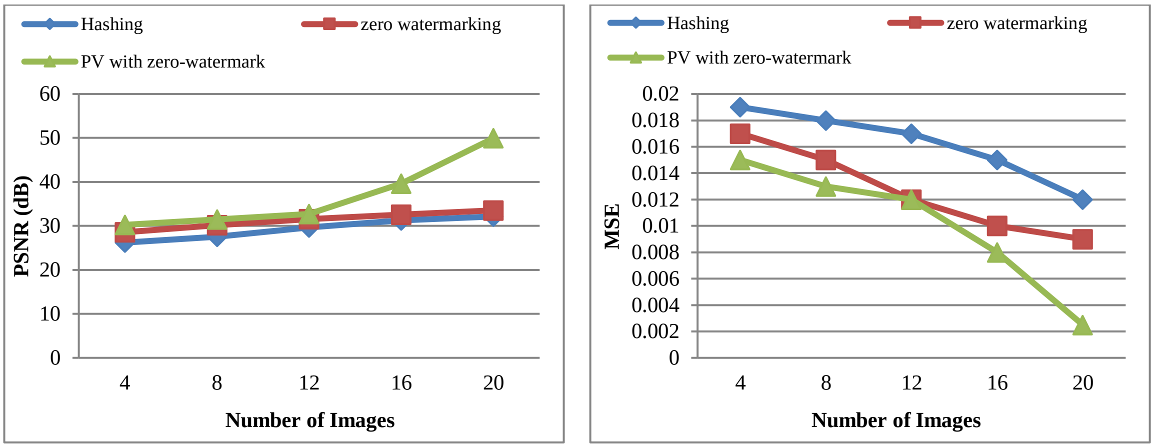
$$PSNR = \log_{10}\frac{WPVC^{*2}_{max}}{MSE} \tag{3}$$

$$MSE = \frac{1}{N}\sum_{i=0}^{N}[WPVC(x_i,y_i) - WPVC^*(x_i,y_i)]^2 \tag{4}$$

- SSIM: the parameter is computed to find the comparation between the encrypted and decrypted palm vein images as given in (5). Its rate would be within [0, 1]. An advanced rate designates a better-watermarked image. Where μ is the average of the image and σ are the discrepancies of the images and v_1 and v_2 are two variables for alleviating the frail denominator.

$$SSIM = \frac{(2\mu_{WPVC}\cdot\mu_{WPVC^*}+v_1)(2\sigma_{WPVC}\cdot\mu_{WPVC^*}+v_2)}{(\mu^2_{WPVC}+\mu^2_{WPVC^*}+v_1)(\mu^2_{WPVC}+\mu^2_{WPVC^*}+v_2)} \tag{5}$$

PSNR and MSE-based comparison of several existing methods with the proposed work is shown in Figure 4. Figures 4(a) and (b) compared to other techniques like hashing and zero watermarking, the PSNR of the suggested method is the greatest at 49.95 dB. PSNR values for various signal kinds and measurement techniques are displayed in next section and the preceding techniques have yielded PSNR values between 32.15 and 33.54 decibels. When compared to alternative techniques like hashing and zero watermarking, the MSE value of the suggested approach, 0.0025, is rather small. Reduced MSE values suggest more accurate picture registration. As shown from the outcomes, PV with zero-watermark-based approaches is efficient in generating medical data security. Although prior approaches achieved low MSE, their performance was restricted by computational complexity.



(a) (b)

Figure 4. Comparison of (a) PSNR and (b) MSE of different methods compared with the proposed framework

For an example of how the suggested model and SSIM might be used to compare and contrast various methods, see Figure 5. Associated to other approaches, the SSIM value produced using the recommended framework is higher. Compared to alternative techniques like hashing and zero watermarking, the SSIM of the suggested method, 0.9289, is the greatest. Gains in SSIM using existing approaches fall between 0.8362 and 0.8741.

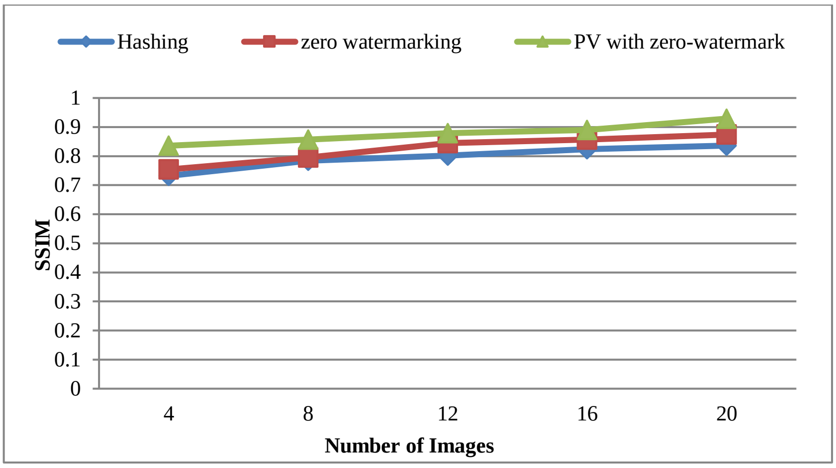


Figure 5. SSIM of different methods compared with the proposed framework

4. CONCLUSION

Since the attacks on IMDs might directly harm patients, their security is crucial. When the patient is not in an emergency, IMD operate in a normal situation and several research organizations have looked into IMD security concerns in this case. These security schemes would be ineffective in an emergency because they require the patient's cooperation. The proposed system recommends a scheme for securing IMD access control in emergencies and preventing illegal access to IMDs by combining encrypted PVC and zero-watermark (personal identity) to generate encrypted credential data. Before implantation surgery, the encrypted credential data and key will be stored in the IMD. The proposed system will ensure integrity, confidentiality and authentication. In future a computational approach based on a rapid fourier transform will be used to improve the computation precision and agility of the feature abstraction process in medical images. Also, a new chaotic map and deep learning-based encryption algorithms will be integrated with the proposed system to boost security.

REFERENCES

[1] A. F. Demir *et al.*, “In Vivo communications: steps toward the next generation of implantable devices,” *IEEE Vehicular Technology Magazine*, vol. 11, no. 2, pp. 32–42, Jun. 2016, doi: 10.1109/MVT.2016.2520492.

[2] L. Wu, X. Du, M. Guizani, and A. Mohamed, “Access control schemes for implantable medical devices: a survey,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1272–1283, Oct. 2017, doi: 10.1109/JIOT.2017.2708042.

[3] B. Rios and J. Butts, “Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies,” WhiteScope, 2017, [Online]. Available: https://www.ledecodeur.ch/wp-content/uploads/2017/05/Pacemaker-Ecosystem-Evaluation.pdf.

[4] C. Li, A. Raghunathan, and N. K. Jha, “Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system,” in *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2011*, Jun. 2011, pp. 150–156, doi: 10.1109/HEALTH.2011.6026732.

[5] G. Zheng *et al.*, “Finger-to-heart (F2H): authentication for wireless implantable medical devices,” *IEEE Journal of Biomedical and Health Informatics*, vol. 23, no. 4, pp. 1546–1557, Jul. 2019, doi: 10.1109/JBHI.2018.2864796.

[6] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, and K. Saleem, “Ideas and challenges for securing wireless implantable medical devices: a review,” *IEEE Sensors Journal*, vol. 17, no. 3, pp. 562–576, Feb. 2017, doi: 10.1109/JSEN.2016.2633973.

[7] M. Darji and B. H. Trivedi, “Emergency aware, non-invasive, personalized access control framework for IMDs,” in *SNDS 2014: Recent Trends in Computer Networks and Distributed Systems Security*, 2014, pp. 370–381. doi: 10.1007/978-3-642-54525-2_33.

[8] R. Srividya and B. Ramesh, “Design of biometric authentication technique for MANET based emergency response system,” in *Proceedings of 2015 IEEE International Conference on Electrical, Computer and Communication Technologies, ICECCT 2015*, Mar. 2015, pp. 1–5, doi: 10.1109/ICECCT.2015.7226138.

[9] G. Zheng *et al.*, “Fingerprint access control for wireless insulin pump systems using cancelable delaunay triangulations,” *IEEE Access*, vol. 7, pp. 75629–75641, 2019, doi: 10.1109/ACCESS.2019.2920850.

[10] M. Rostami, A. Juels, and F. Koushanfar, “Heart-to-heart (H2H): authentication for implanted medical devices,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2013, pp. 1099–1111, doi: 10.1145/2508859.2516658.

[11] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in *Proceedings - IEEE INFOCOM*, Apr. 2011, pp. 346–350, doi: 10.1109/INFCOM.2011.5935179.

[12] H. Chi, L. Wu, X. Du, Q. Zeng, and P. Ratazzi, "E-SAFE: secure, efficient and forensics-enabled access to implantable medical devices," in *2018 IEEE Conference on Communications and Network Security, CNS 2018*, May 2018, pp. 1–9, doi: 10.1109/CNS.2018.8433213.

[13] H. Wasmi, M. Al-Rifaee, A. Thunibat, and B. Al-Mahadeen, "Comparison between proposed convolutional neural network and KNN for finger vein and palm print," in *2021 International Conference on Information Technology, ICIT 2021 - Proceedings*, Jul. 2021, pp. 946–951, doi: 10.1109/ICIT52682.2021.9491737.

[14] "RF wireless world," *GSM network architecture*, 2012, (accessed Jan. 1, 2023), [Online]. Available: https://www.rfwireless-world.com/Tutorials/gsm-architecture.html.

[15] "Iris recognition - Bometrics make use of our most unique physical features," (accessed Jan. 1, 2023), [Online]. Available: https://www.aware.com/iris-recognition.

[16] R. C. Rahul, M. Cherian, and M. C. M. Mohan, "Literature survey on contactless palm vein recognition," *International Journal of Computer Science Trends and Technology (IJCST)*, vol. 3, no. 5, pp. 250-255, 2015.

[17] T. Belkhouja, A. Mohamed, A. K. Al-Ali, X. Du, and M. Guizani, "Salt generation for hashing schemes based on ECG readings for emergency access to implantable medical devices," in *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, Jun. 2018, pp. 1–6, doi: 10.1109/ISNCC.2018.8530897.

[18] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: securing implantable medical devices with the external wearable guardian," in *Proceedings - IEEE INFOCOM*, Apr. 2011, pp. 1862–1870, doi: 10.1109/INFCOM.2011.5934987.

[19] G. Zheng, G. Fang, M. A. Orgun, R. Shankaran, and E. Dutkiewicz, "Securing wireless medical implants using an ECG-based secret data sharing scheme," in *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, Sep. 2014, pp. 373–377, doi: 10.1109/ISCIT.2014.7011935.

[20] F. Ahmad, L. M. Cheng, and A. Khan, "Lightweight and privacy-preserving template generation for palm-vein-based human recognition," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 1, pp. 184–194, 2020, doi: 10.1109/TIFS.2019.2917156.

[21] M. Mishra, A. Bhattacharya, A. Singh, and M. K. Dutta, "A lossless model for generation of unique digital code for identification of biometric images," in *International Conference on Computational Intelligence and Communication Technology*, Feb. 2018, pp. 1–5, doi: 10.1109/CIACT.2018.8480297.

[22] Q. Wen, T. F. Sun, and S. X. Wang, "Concept and application of zero-watermark," *Tien Tzu Hsueh Pao/Acta Electronica Sinica*, vol. 31, no. 2, pp. 214–216, 2003.

[23] D. G. Duguma, I. You, Y. E. Gebremariam, and J. Kim, "Can formal security verification really be optional? Scrutinizing the security of imd authentication protocols," *Sensors*, vol. 21, no. 24, Dec. 2021, doi: 10.3390/s21248383.

[24] W. Jia *et al.*, "A survey on dorsal hand vein biometrics," *Pattern Recognition*, vol. 120, Dec. 2021, doi: 10.1016/j.patcog.2021.108122.

[25] M. A. Hossain and M. A. Al Hasan, "Improving cloud data security through hybrid verification technique based on biometrics and encryption system," *International Journal of Computers and Applications*, vol. 44, no. 5, pp. 455–464, May 2022, doi: 10.1080/1206212X.2020.1809177.

[26] A. Aftab, F. A. Khan, M. K. Khan, H. Abbas, W. Iqbal, and F. Riaz, "Hand-based multibiometric systems: state-of-the-art and future challenges," *PeerJ Computer Science*, vol. 7, Oct. 2021, doi: 10.7717/peerj-cs.707.

[27] A. Sardar, S. Umer, R. K. Rout, and M. K. Khan, "A secure and efficient biometric template protection scheme for palmprint recognition system," *IEEE Transactions on Artificial Intelligence*, pp. 1–13, 2022, doi: 10.1109/TAI.2022.3188596.

BIOGRAPHIES OF AUTHORS

Ms. Ahlam Almukhlifi is doing her Master of Information Security in Faculty of Computers and Information Technology, University of Tabuk, Kingdom of Saudi Arabia. Her research interests arecyber security, and steganography. She can be contacted at email: 421009277@stu.ut.edu.sa.

Dr. Saad M. Almutairi is Member, IEEE received the B.Sc. degree from Al-Ahliyya Amman University, Jordon, and the M.Sc. and Ph.D. degrees from De Montfort University, U.K. He is currently working as an Associate Professor in Faculty of Computers and Information Technology, University of Tabuk, Saudi Arabia. His research interests are software engineering, context aware systems, cloud computing, cyber security, and steganography. He has published ample of articles in international refereed journals and conferences in his research areas. He can be contacted at email: s.almutairi@ut.edu.sa.