Egyptian Informatics Journal xxx (xxxx) xxx

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Iris based cancelable biometric cryptosystem for secure healthcare smart card

Firdous Kausar *

Department of Electrical and Computer Engineering, College of Engineering, Sultan Qaboos University, Muscat, Oman

ARTICLE INFO

Article history:
Received 30 March 2020
Revised 19 January 2021
Accepted 31 January 2021
Available online xxxx

Keywords:
Biometric cryptosystem
Authentication
Key binding
Healthcare
Cancelable biometric

ABSTRACT

Health related information of an individual is very sensitive and demands a high level of security and privacy. Healthcare providers have the responsibility to ensure that patient information is secure and accessible only to authorized users. Healthcare systems are using biometrics since long for authentication and/or access control purposes. Biometrics can also be used for healthcare data security and privacy. This paper proposes an iris based cancelable biometric cryptosystem to securely store the healthcare data of patients on the smart card. It employs symmetric key cryptography to encrypt the healthcare data and store it on the smart card in encrypted form. We use the fuzzy commitment scheme to bind the secret encryption key with the cancelable iris template of the patient. Our proposed scheme provides user authentication as well as the decryption of healthcare data when needed by using the iris template of the owner of the healthcare smart card. The implementation results show that our proposed scheme provides better performance as compared to other schemes. It can generate an encryption key of a maximum of 252 bits from the input iris template with a false acceptance rate (FAR) of 0 and a false rejection rate (FRR) of 0.07. The generated key can be used for encrypting the health care data of patients using a symmetric encryption algorithm, e.g. Advance Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Blowfish, etc. As compared to a conventional encryption system where the security of the system depends on keeping the key secret, our proposed scheme binds the encryption key with the iris - template of the patient impeccably without the need to store it securely. The security analysis demonstrates that it is not possible for an attacker to retrieve the secret key or healthcare data of the patient from the stolen healthcare card.

1. Introduction

The protection of sensitive data from unauthorized access is one of the greatest challenges in today's world. This becomes a more important requirement in the healthcare industry where the security and privacy of patients' healthcare data is prone to breach. Health Insurance Portability and Accountability Act Rules (HIPPA) outline the privacy and security rules that need to follow for accessing the patient healthcare data. Any healthcare provider company must obey those rules by implementing the proper risk management policy to ensure the security and privacy of patients' healthcare data for compliance with HIPPA. In some cases, there is a need to share the patients' data among different healthcare providers or different departments within the same provider. The process of data transfer may leak the personal sensitive information which can be further utilized for some unlawful activity instead of personal medical use. Therefore, healthcare information systems should be designed to provide the patients' privacy and secure access or exchange of patient sensitive health related data.

Patient/user authentication is critical to prevent unauthorized access to confidential data or systems. Passwords are one of the most widely used methods for user authentication, but it has many deficiencies. Poorly chosen passwords are considered to be the most common reason for system intervention [1]. A password based system requires the exact recall of choosing a secret password which is hard for human cognition. The token based authentication system requires holding tokens for authentication purposes which can be easily misplaced, lost, or misuse by anyone. Biometric authentication is an alternative method of user authentication, which relies on the unique biological characteristics of human beings. These biological characteristics include both physical and behavioral traits of humans, for example, fingerprint, face, iris, hand, finger vein, voice, signature, gate, keystrokes, etc. Bio-

* Corresponding author.
E-mail address: firdous@squ.edu.om

https://doi.org/10.1016/j.eij.2021.01.004
1110-8665/

Please cite this article as: F. Kausar, Iris based cancelable biometric cryptosystem for secure healthcare smart card, Egyptian Informatics Journal, https://doi.org/10.1016/j.eij.2021.01.004

metric authentication systems are more secure than conventional authentication based on password/PIN or token because it cannot be forgotten or lost and are hard to forge.

Biometric authentication systems consist of the enrollment and identification/authentication phase. During the enrollment phase, the biometric trait is given as input to the system to generate the biometric template which is stored in the database along with other user's details. During the authentication phase, the biometric trait of the user is given as input to the system to generate the biometric template which is matched against the stored template in the database. The matching process depends on statistical algorithms and is not 100% accurate. Different biometric traits provide a different level of accuracy. The Iris based authentication system is considered to be more accurate as compared to other biometric systems.

If a password has been compromised, it can be changed, but if the biometric template is compromised it cannot be changed. Also, biometrics are not secret. A biometric template can be protected by using a cancelable biometric system [2] which stores the irreversible transformed version of biometric templates. As the transformation is one-way, so leakage of the cancelable template does not reveal information about the original biometric template. Biometric cryptosystems [3] combines biometric and cryptography to get the best of both worlds. Biometric cryptosystems (BCSs) are used to either bind or generate an encryption key to biometric data. In key binding schemes, the helper data is generated by the fusion of the biometric data and secret encryption key. Helper data is then used to generate or retrieve the secrete key/password from the given biometric data which eliminate the user to memorize password or hold tokens. Fuzzy commitment schemes (FCS) use the combination of error correcting codes and cryptography to perform key binding [26].

The main contribution of this paper is the successful integration of the cancelable biometrics system and FCS based key binding scheme in order to authenticate and securely store the patient healthcare data on the smart card. The helper data is generated by combining the Reed Solomon (RS) encoding of the secret key and cancelable transformation of the iris biometric template of the patient. The novelty of this contribution is that we solved the major problem of key management with symmetric key encryption algorithms by allowing the patients and healthcare providers to share the encryption key without saving it anywhere The patients or healthcare providers do not need to store or memorize the encryption key to decrypt the data stored on the healthcare card. It is generated on the go when needed from the patient's iris image. Further, the irreversibility and unlikability of biometric data are provided by using the cancelable biometric system. The attacker can't retrieve any information about the secret key or healthcare data of the patient from the stolen healthcare smart card.

The rest of the paper is organized as follows. Section 2 presented the related work in the field of secure health care data solutions and biometric cryptosystems. In Section 3, the new cancelable Iris-based biometric cryptosystem scheme is proposed. The experimental results and security analysis is provided in Section 4. In the end, the conclusion and future work are presented in Section 5.

2. Related work

The healthcare data of the patient should be properly secured and make available anytime when needed for legitimate use by healthcare professionals. There is a need to design security mechanisms that provide the efficient availability of data while maintaining a high level of security. Biometric based access control mechanisms provide a solution to secure access to the healthcare data of patients. Garson et al. [12] proposed an e-hospital architecture based on two factor authentication for data security and access control. They are using the combination of password along with fingerprints as two factor authentication mechanism. It required an additional overhead of securely managing the passwords of users along with fingerprint.

Zhang et al. [13] proposed an ECG-based authentication method for the smart healthcare system. They used a hybrid ECG feature extraction method for patient recognition. The proposed scheme performance is affected in case of alteration in ECG signals because of the effect of cardiac disease in patients.

Li et al. [14] developed an authentication protocol and privacy preserving mechanism for cloud-assisted telecare medical information systems. Peng et al. [15] proposed fingerprints based biometric cryptosystem. It employed three different error correcting codes, i.e. Bose–Chaudhuri–Hocquenghem (BCH), Reed-Solomon (RS), and Lower Density Parity Check (LDPC) for successful key recovery from the fingerprint template. It showed that LDPC based codes provide better performance for longer codewords as compared to the BCH and Reed-Solomon codes.

Shakil et al. [16] presented a signature-based authentication scheme and data management for cloud-based healthcare systems. It attained an equal error rate (EER) of 0.12, a sensitivity of 0.98, and a specificity of 0.95. Adamovic et al. [17] proposed an iris based fuzzy commitment scheme to generate cryptographic keys from the high entropy region of iris images that can be used for encryption or authentication purposes in different applications. It used Reed-Solomon codes for error correction, resolution in inter, and intraclass iris images. It only concentrates on the information present in a high resolution area of the iris to get the maximum entropy.

Yang et al. [9] proposed a cancelable finger-vein based biometric cryptosystem for securely storing the healthcare data of patients on a healthcare card. It binds the finger-vein template with the encryption key by using BCH error correcting codes. The maximum key length that can be achieved is 63 bits only which is insufficient to use in modern cryptographic algorithms e.g. AES [11].

Hao et al. [18] presented a method to generate a cryptographic key from iris code and for error correction purposes they use the combination of Hadamard and Reed-Solomon codes. The cryptographic key cannot be generated either with an iris template or auxiliary data alone.

Ruthgeb et al. [19] developed a two-factor authentication system based on iris biometric. They performed the XOR operation between a random number and iris code to generate an iris template during the enrollment phase, and the same random number is used during the matching/authentication phase. The security of the system depends on the secrecy of a random number.

The biometric recognition system security mainly depends on the protection of biometric templates. The biometric cryptosystem based on the iris is proposed in [20,21] which utilizes the digital modulation paradigm to provide iris template protection. The access control mechanism utilizing the biometric iris and fingerprint matching on the smart card is proposed in [22,23]. The main constraints of low storage and limited processing power on the smart card are resolved by efficient translation of biometric templates.

3. Proposed scheme

We propose a scheme to secure healthcare data by using an iris based cancelable biometric cryptosystem. The overall architecture of the system is shown in Fig. 1.

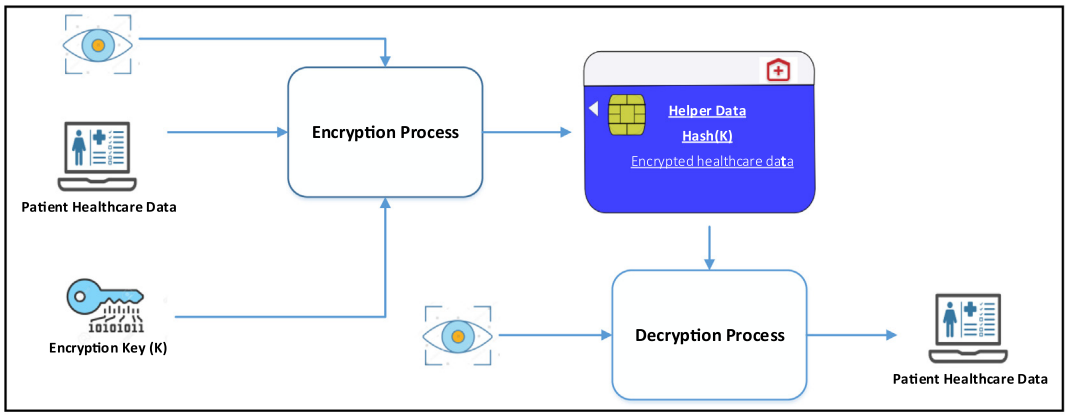

Fig. 1. Iris based Cancelable Biometric Cryptosystem System Architecture.

Our scheme performs its function in two phases, including data encryption and data decryption as shown in Fig. 1. The encryption process takes as input the iris image, encryption key, and healthcare data of the patient. It generates the helper data, a cryptographic hash of the encryption key, and encrypted healthcare data of a patient and stores this information on the healthcare smart card of the patient. The decryption process is used to retrieve the encrypted healthcare data of a patient from the smart card without providing an encryption key. It takes as input only the iris image of the patient and healthcare smart card data. It generates the decryption key from this input information and uses it to decrypt the encrypted healthcare data saved on the smart card. The secret encryption key is neither stored on the healthcare smart card nor being provided by the user. It is generated from the input iris image and helper data stored on the healthcare smartcard.

During the encryption process as shown in Fig. 2(a), we generate the helper data, cryptographic hash of encryption key, and encrypted healthcare data. The encryption key is protected by binding it with a cancelable transform of iris-template by using the fuzzy commitment scheme of biometric cryptosystems. During the decryption process as shown in Fig. 2(b), from the input query iris image the cancelable template is generated which then combined with helper data, and output is decoded to generate the decryption key. The cryptographic hash of the generated decryption key is matched against the cryptographic hash of the encryption key to verify the successful retrieval of the decryption key. If both are the same then the generated decryption key can be used for the decryption of encrypted healthcare data stored on the card. Some of the notations used in this section are described in Table 1.

3.1. Encryption process

We divide the encryption process further into four phases: 1) Iris code generation phase 2) Cancelable template generation phase 3) Key binding phase 4) Encryption phase.

3.1.1. Iris code generation phase

The iris code is generated by adopting the method described in [4]. The process of iris code generation is shown in Fig. 3. First, on an input eye image, a Hough transform based segmentation method is applied to segment the circular region of the iris and pupil. Then a normalization process is applied to the extracted iris region based on Daugman's rubber sheet model. The normalized iris pattern is convolved with a 1D log-Gabor wavelet to perform the feature encoding. In the end, the distinct iris model is encoded into a bit-wise biometric template by applying four level quantization on phase data from 1D Log-Gabor filters.

3.1.2. Cancelable template generation phase

A cancelable iris template is generated by using the Indexing-First-One (IFO) hashing scheme [5]. The generated iris code of length $(n_1 \times n_2)$ is given as input to the IFO hashing algorithm. The 'P' number of random permutations is applied to each row of the iris code. Hadamard product code is generated by multiplying together all the randomly permuted iris code. Then a k size window is defined to search the occurrence of the first binary '1′ in each row of the product code and its index is recorded. A modulo threshold function is applied to get the hash code value. The same procedure is iterated 'm' number of times to generate an IFO hash code of length $(n_1 \times m)$.

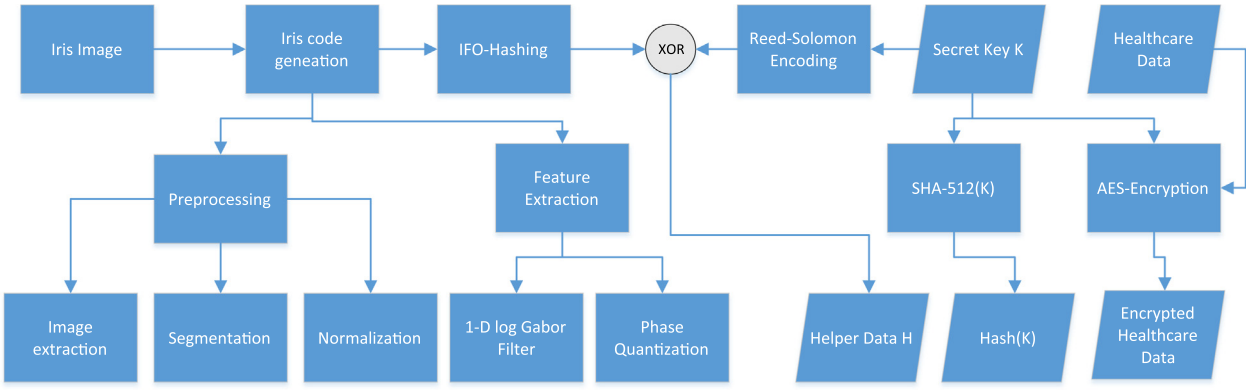

Fig. 2a. Encryption Process.

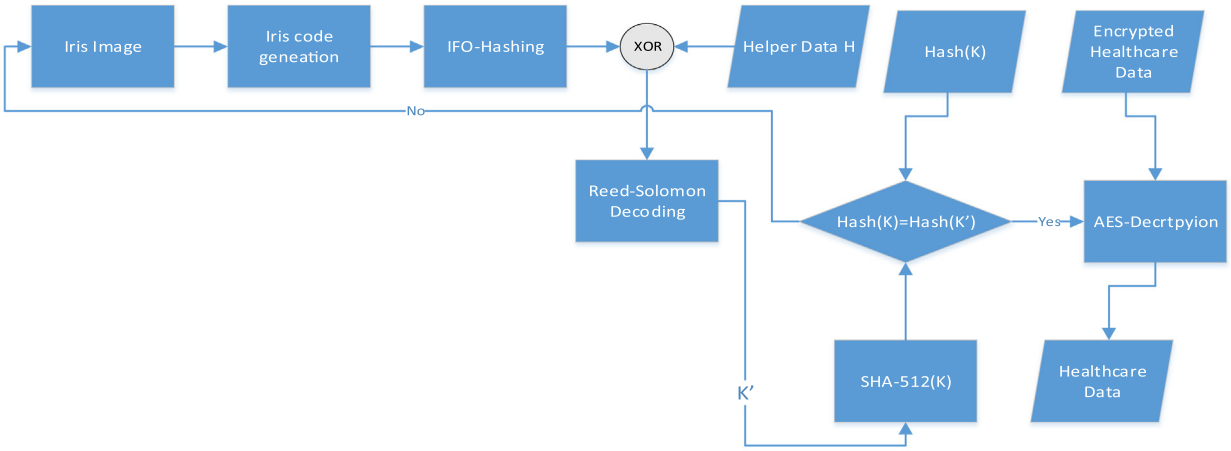

Fig. 2b. Decryption Process.

Table 1
Notations and description.

Notations	Description
K	Secret Key
I_p^T	template iris code of patient P
C_p^T	IFO hash code of patient P
H	helper data
E	encrypted healthcare data
I_p^Q	Query Iris code of patient P
C_P^Q	query IFO hash code of patient P

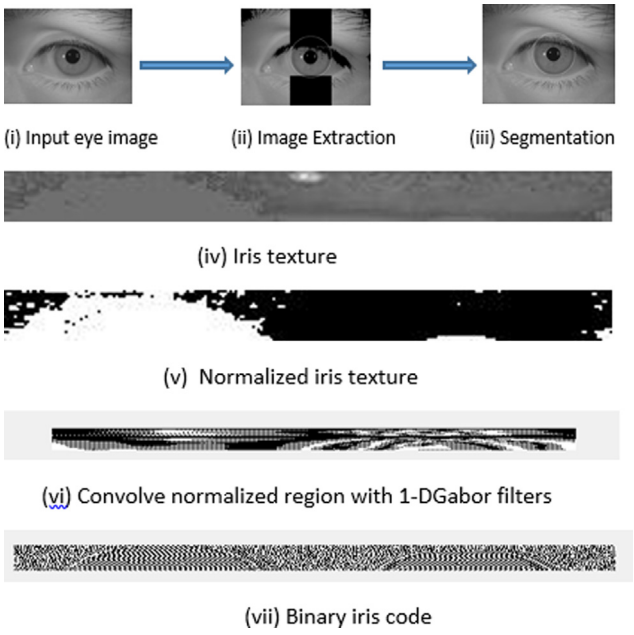

Fig. 3. Iris code Generation Process.

3.1.3. Key binding phase

Our encryption process is based on symmetric key encryption where the same key is used for encryption as well as decryption. Healthcare data of the patient is encrypted by using the secret key K.

The input eye image of the patient (p) is used to generate the template iris code I_p^T as described above in Section 3.1.1. Template Iris code I_p^T is given as input to the IFO hashing function to generate the cancelable template IFO hash code $C_p^T$of the patient (p).

$$C_p^T = IFOHashing(I_p^T)$$

The secret encryption key, K is encoded by using the Reed-Solomon encoding scheme (n, k, m) [10]. The output of the Reed-Solomon encoder is XORed with the IFO hash code to generate the helper data H.

$$H = RSEncoder(K) \oplus C_p^T$$

3.1.4. Encryption phase

The healthcare data of the patient is encrypted using *AES* algorithm [11] with the secret key K as shown below.

$$E = AES(K,\ HelathcareData)$$

Also, the cryptographic hash code of the secret key K is generated by applying the SHA512 algorithm [6] on the secret key K.

The output of the encryption process consists of helper data$H$, a cryptographic hash of the secret encryption key$K$, and encrypted healthcare data E.

3.2. Decryption process

To decrypt data, the first step is to retrieve the secret key from helper data H and query eye image. The decryption process is also divided into three phases: 1) Iris code generation phase 2) Cancelable template generation phase 3) Key unbinding phase.

Iris code generation phase and cancelable template generation phase are the same as in the encryption process discussed above in Section 3.1.1 and Section 3.1.2. Query Iris code I_p^Q of patient p, is generated from the query eye image and then corresponding query IFO hash code C_P^Q is produced by applying cancelable IFO hashing function on the query iris code I_p^Q.

$$C_p^Q = IFOHashing(I_p^Q)$$

3.2.1. Key unbinding phase

Exclusive OR (XOR) operation is performed on helper data and IFO hash code. The output of this operation is decoded by the same block code used in the encoding process. The decoded message is a potential secret key K.

$$K' = RSDecoder(C_p^Q \oplus H)$$

The cryptographic hash of K' is performed and compared with the stored hash of key K.

$$SHA512(K) = SHA512(K^{'})$$

If both are the same then K' can be used to decrypt the encrypted healthcare data E stored on the card.

$$HealthCareData = AES(K^{'}, E)$$

4. Experimental results and security analysis

This section presents the experimental results and security analysis of the proposed scheme.

4.1. Experimental results

We performed the experiment to evaluate the performance of our proposed iris based cancelable biometric cryptosystem. We use a CASIA-IrisV3-Lamp database. This database consists of twenty iris images of each left and right eye of 411 users with a total of 16,440 iris images. Our experiments are conducted only on left eye iris images. We use the first iris image of the left eye from 100 users for training purposes and the third image of the left eye from the same 100 users for testing.

For measuring the false rejection rate (FRR), the first iris image of each user is considered as a template and third iris images of the same user are utilized as a query. On the other hand, to measure the value of false acceptance rate (FAR), the first iris image of each user is considered as a template while the third iris image of every other user is utilized as a query which results in a total of 505,000 imposter comparisons. The accuracy of the proposed scheme is measured by calculating the equal error rate (EER) where FAR is equal to FRR.

The FAR and FRR values are calculated in order to measure the performance of our proposed system. RS code is defined by the three parameters (n, k, m), where n is the block length, k is the message length and m is the number of bits in each message symbol. Different RS codes (n, k, m) are implemented to investigate the performance of the system as shown in Table 2. It can be seen that for smaller key lengths that the value of FRR is low but FAR is high. On the other hand, for larger key lengths the value of FAR is low but FRR is high. For RS n = 127, k = 36, and m = 7 by having a key of length 252 the theoretical maximum error correcting capability is t = n-k/2 = 45.5 bits and a minimum distance, d_{min} = 2 t + 1 = 92bits. Our testing shows that it gives us a maximum value of t = 38 bits. As shown in Fig. 4 the FRR and FAR are computed for different values of t by fixing the n = 127. It can be observed that for smaller values of t, the FRR is high while FAR is low.

We compare the results of our proposed scheme with W. Yang et al. [9] as shown in Table 3. Our proposed scheme provides a better value of FAR and FRR with larger key lengths for practical use with different cryptographic algorithms e.g. AES. The maximum key length provided by our proposed scheme is 252 bits with FAR of 0%, while FRR of 7% as compared to Yang et al. [9] which provides the key length of 63bits with FAR of 0% and FRR of 63%.

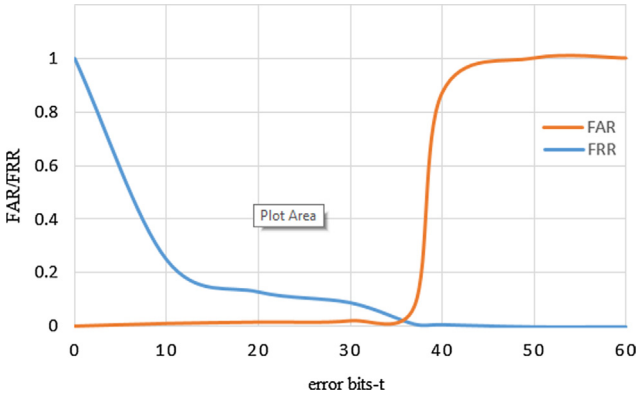

Fig. 4. Error correcting capability of the system for n = 127.

4.1.1. Time complexity

Our proposed scheme uses the AES algorithm to encrypt the patient healthcare data and the SHA512 algorithm to compute the hash of the encryption key. AES operates on a fixed block size of 128 bits. If our message consists of *'m'* number of plain text blocks then the time complexity of the AES algorithm is O(m). Calculation of the hash value using the SHA512 algorithm takes approximately the same time when the input sizes are fixed, thus they are O(1).

4.2. Security analysis

This section describes that the proposed scheme is resilient to various security attacks and provides user authentication and privacy.

4.2.1. Stolen smartcard attack

Data stored on the healthcare smart card can lead to a different type of data level security attacks on confidentiality, integrity, and availability of the patients' healthcare information [24,25]. In our proposed scheme we store the following data on the healthcare smart card: 1) cryptographic hash of the encryption key 2) encrypted healthcare data of the patient 3) helper data.

The first information stored on the healthcare smart card is a cryptographic hash of the encryption key. If the card is stolen, the attacker would not be able to find the encryption key from its hash value because SHA-512 is a one-way hash algorithm [6]. The attacker cannot get the key from the SHA512 hash value of the key [7].

The second information stored on the healthcare smart card is encrypted healthcare data by using the AES algorithm. The possible length of the encryption key can be a maximum of 252 bits with FAR 0% and FRR 7%. So, if an attacker performs the brute force attack on encrypted healthcare data, it would not be possible to get the key or the original message from it in a reasonable amount of time [8].

The third information stored on the healthcare smart card is helper data. The attacker cannot retrieve the key from the stolen card unless it has a query iris image of the patient. As we are not

Table 2
System performance.

Coding Scheme	Key length(bits)	RS codeword length (bits)	FAR %	FRR%
RS (31,9,5)	45	155	0.8	2
RS(63,11,6)	66	378	0	3.5
RS (63,17,6)	102	378	0	5
RS (127,36,7)	252	889	0	7

Table 3
Performance Comparison.

Our Proposed Scheme			W. Yang et al. [9]		
Key Length	FAR (%)	FRR (%)	Key Length	FAR (%)	FRR (%)
45	0.8	2	13	0	8
66	0	3.5	37	0	20
102	0	5	47	0	24
252	0	7	63	0	63

storing the iris image of the patient or corresponding iris template anywhere in the database so the attacker won't be able to get the patient iris image in any case from the system.

4.2.2. Cross-matching attack

The advantage of integrating the cancelable biometric with a biometric cryptosystem is to prevent the cross-matching attacks. It is possible that an adversary got access to the user iris template from a different application and can use it for a cross-matching attack as well as retrieving the secret key from the healthcare data card. However, in our proposed scheme, it is not possible because we perform a non-invertible cancelable IFO hashing function on the iris template before using it to generate helper data. In case of any breach, we can always generate the new iris template by giving different input parameters to the cancelable IFO hashing function. Therefore, an adversary cannot launch the cross-matching attack on the patients' private data in any other application.

4.2.3. Masquerade attack

The integration of biometric cryptosystem with cancelable biometrics makes it more resilient to masquerade attacks. Since the adversary can't reconstruct the original biometric template from the compromised cancelable biometric template of the user [27]. In traditional biometric systems, biometrics cannot be revoked in case of compromise. In our proposed scheme it is possible to revoke the compromised biometric template and can generate the new template by just changing the input parameters to the cancelable IFO hashing function.

4.2.4. Brute force attack

The helper data stored on the smartcard is XORed with the IFO hash code of the iris template to retrieve secrete key *K*. There are two possibilities of brute force attack in our proposed scheme. Firstly, the attacker can get the secrete key by a successful generation of the IFO hash code of the user's iris template. As the IFO hash code of the iris template is not stored on the card and is calculated on runtime, the attacker cannot launch the brute force attack on it.

Secondly, a brute force attack can be launched on the SHA512 hash value of the secrete key stored on the card. A brute attack on the SHA512 algorithm is equivalent to find the collision in it such that SHA512(K') = SHA512(K) which is called birthday attack and its complexity is $O(2^{n/2})$ where n is the length of the output of the hash function. In our proposed scheme discovering a collision in SHA512 will take $O(2^{256})$ time. If the attacker can calculate 1 million SHA512 hashes in 1 msec, it would take him 2^{236}msec $\approx 3.5 \times 10^{60}$ years to find the secrete key. Even if the computation power of the attacker is increased to a much larger extend this would still make brute force attack impractical.

4.2.5. Attack via record multiplicity (ARM)

ARM is a security attack on the cancelable biometric systems which requires the attacker to gain access to several transformed biometric templates and the transformation parameters or keys which are usually not kept secret and are used in generating the transformation matrix. In our proposed scheme we don't save the transformed iris template of the user on the smart card but instead, the helper data which is generated by XORing the transformed iris template with the RS encoded secret key as shown in Fig. 2(a). To perform an ARM attack the attacker first has to acquire the transformed iris template from the helper data. If we assume that the attacker manages to reconstruct the transformed iris template for the helper data still ARM attack is not possible because we used IFO hashing method to generate the transformed iris template which is secure against ARM [5].

4.2.6. User authentication

The proposed scheme also provides user authentication because only the legitimate user with a valid query iris template is able to retrieve the secret key, hence decrypt the encrypted patient healthcare data stored on the card.

4.2.7. User privacy

The privacy of the patient's data is intact in our proposed scheme because no personal information about the patient is stored in clear on the healthcare smart card. It also does not store any biometric data of the patient on the smart card.

4.2.8. Cryptographic smart cards

We can use cryptographic smart cards that are in compliance with ISO/IEC 7816-15:2016 standard for implementation of our proposed scheme [28]. These cards are equipped with a special crypto-processor and capable of performing different cryptographic algorithms e.g. AES, triple DES, RSA, SHA512, etc. It also provides the amenities of storage, retrieval, and use of the cryptographic information on the smart cards.

5. Conclusion

This paper proposes a secure and authenticated iris-based cancelable biometric cryptosystem to provide user authentication and secure encryption of healthcare user data. In the proposed scheme, there is no need to store the cryptographic key use for the encryption of healthcare data. It can be retrieved at run time after successful iris-based biometric authentication of the user. We utilize the Reed-Solomon codes to bind the cancelable iris template with the secret key. The experimental results show that we can successfully get a key of maximum 252bits with the FAR of 0% and FRR of 7% from the input iris template as compared to [9] where the maximum key length is 63bits with FAR of 0% and FRR of 63%. The security analysis indicates that the adversary is not able to get the secret key from the data stored on the smart healthcare card. A non-invertible cancelable transform function application on the iris template before biding it with a secrete key prevents the attacker to perform cross-matching attack or get a secret key from the stolen iris template of the user.

As future work, we would like to extend our proposed scheme to the multimodal fusion of different biometrics e.g. iris, fingerprint, finger vein, face, etc. to attain better accuracy and larger

key lengths. We would also extend our work to investigate the efficiency of the proposed scheme in terms of execution time and memory consumption on different types of smartcards.

Conflict of interest

There is no conflict of interest.

References

[1] Cheswick B, Bellovin S. Firewalls and internet security: repelling the wily hacker; 1994.
[2] Patel VM, Ratha NK, Chellappa R. Cancelable biometrics: a review. IEEE Signal Process Mag 2015;32(5):54–65.
[3] Uludag U, Pankanti S, Prabhakar S, Jain AK, Biometric cryptosystems: issues and challenges. In: Proceedings of the IEEE, vol. 92, no. 6; June 2004, pp. 948–960.
[4] Masek L. Recognition of human Iris patterns for biometric identification; 2003.
[5] Lai Y, Jin Z, Teoh A, Goi B, Yap W, Chai T, et al. Cancellable iris template generation based on Indexing-First-One hashing. Pattern Recogn 2017;64:105–17.
[6] FIPS PUB 180-4, Secure Hash Standard (SHS), <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf> [accessed online: Feb 24, 2020].
[7] Dobraunig C, Eichlseder M, Mendel F. Analysis of SHA-512/224 and SHA-512/256. In: Proceedings, Part II, of the 21st International Conference on Advances in Cryptology, ASIACRYPT 2015 – vol. 9453; 2015, pp. 612–630.
[8] How secure is AES against brute force attacks?. EE Times. Retrieved Feb 26, 2020.
[9] Yang W, Wang S, Hu J, Zheng G. Securing mobile healthcare data: a smart card based cancelable finger-vein bio-cryptosystem. IEEE Access 2018;6:36939–47.
[10] Plank JS. A tutorial on Reed-Solomon coding for fault-tolerance in RAID-like systems; 1997.
[11] FIPS PUB 197, Advanced Encryption Standard (AES), <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf> (accessed online: March 1, 2020).
[12] Garson K, Adams C. 'Security and privacy system architecture for an e-hospital environment. In: Proc. 7th Symp. Identity Trust Internet; 2008, pp. 122–130.
[13] Zhang Y, Gravina R, Lu H, Villari M, Fortino G. PEA: parallel electrocardiogram-based authentication for smart healthcare systems. J Netw Comput Appl 2018;117:10–6.
[14] Li C, Shih D, Wang C. Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Comput Methods Programs Biomed 2018;157:191–203.
[15] Li P, Yang X, Qiao H, Cao K, Liu E, Tian J. An effective biometric cryptosystem combining fingerprints with error correction codes. Expert Syst Appl 2012;39(7):6562–74.
[16] Shakil K, Zareen F, Alam M, Jabin S. BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. J King Saud Univ, Comput Inf Sci 2020;32(1):57–64.
[17] Adamovic S, Milosavljevic M, Veinovic M, Sarac M, Jevremovic A. Fuzzy Commitment scheme for generation of cryptographic keys based on iris biometrics. IET Biom 2017;6(2):89–96.
[18] Hao F, Anderson R, Daugman J. Combining Crypto with biometrics effectively. IEEE Trans Comput 2006;55(9):1081–8.
[19] Rathgeb C, Uhl A. Two-factor authentication or how to potentially counterfeit experimental results in biometric systems. In: Proc. of the Int. Conf. on Image Analysis and Recognition; 2010, pp. 296–305.
[20] Maiorana E, Campisi P, Neri A. IRIS template protection using a digital modulation paradigm. In: 2014 IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), Florence; 2004, pp. 3759–3763.
[21] Álvarez Mariño R, Hernández Álvarez F, Hernández Encinas L. A crypto-biometric scheme based on iris-templates with fuzzy extractors. Inf Sci 2012;195:91–102.
[22] Nedjah N, Wyant RS, Mourelle LM, Gupta BB. Efficient yet robust biometric iris matching on smart cards for data high security and privacy. Future Gener Comput Syst 2017;76:18–32.
[23] Nedjah N, Wyant R, Mourelle L, Gupta B. Efficient fingerprint matching on smart cards for high security and privacy in smart systems. Inf Sci 2019;479:622–39.
[24] Gupta B, Quamara M. A taxonomy of various attacks on smart card-based applications and countermeasures. Concurr Comput: Pract Exp 2018. doi: https://doi.org/10.1002/cpe.4993.
[25] Gupta B, Quamara M. Smart Card Security Applications, Attacks, and Countermeasures; 2019. https://doi.org/10.1201/9780429345593.
[26] Juels A, Wattenberg M. A fuzzy commitment scheme. In: 6th ACM Conference on Computer and Communications Security. p. 28–36.
[27] Cavoukian A, Stoianov A. Biometric encryption: the new breed of untraceable biometrics. Biometrics: fundamentals, theory, and systems. London: Wiley; 2009.
[28] ISO/IEC 7816-15:2016 Identification cards — Integrated circuit cards — Part 15: cryptographic information application, <https://www.iso.org/standard/65250.html>