IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 10, 2018, accepted May 24, 2018, date of publication June 5, 2018, date of current version July 25, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2844182

Securing Mobile Healthcare Data: A Smart Card Based Cancelable Finger-Vein Bio-Cryptosystem

WENCHENG YANG[1], SONG WANG[2], JIANKUN HU[3], GUANGLOU ZHENG[1], JUNAID CHAUDHRY[4], (Senior Member, IEEE), ERWIN ADI[3], AND CRAIG VALLI[1]

[1]Security Research Institute, Edith Cowan University, Joondalup, WA 6027, Australia
[2]Department of Engineering, La Trobe University, Bundoora, VIC 3086, Australia
[3]School of Engineering and Information Technology, University of New South Wales at Canberra, Campbell, ACT 2612, Australia
[4]College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ 86301-3720, USA

Corresponding author: Wencheng Yang (w.yang@ecu.edu.au)

This work was supported by the Defence Science and Technology Group (DST) of Australia under Project CERA 221.

ABSTRACT Most existing biometric systems designed for healthcare applications only use biometrics for authentication/access control without considering its other function—data encryption. In this paper, we propose a cancelable finger-vein-based bio-cryptosystem, which not only can provide authentication but also can encrypt sensitive healthcare data through a biometric cryptographic technique, fuzzy commitment scheme (FCS). The proposed bio-cryptosystem stores both the encrypted version of healthcare data and the biometric template on a smart card for the reason that it is safer if the biometric data never leaves the card. The employment of the cancelable biometrics further enhances the system security. The experimental results and security analysis show the validity of the proposed scheme.

INDEX TERMS Biometrics, security, healthcare, data security.

I. INTRODUCTION

Health Insurance Portability and Accountability Act (HIPAA) [1] and Australia Privacy Principles Act (APPA) [2] have requirements for protecting patients' privacy and personal information, which may contain treatments received, life style details, family medical history, medications prescribed and lots of other information pertinent to the patients' health [3]. Moreover, health data can be shared among different health information systems within one organization or across different healthcare organizations [4]. The information exchange/sharing process increases the risk of disclosing patients' healthcare data. This needs to be taken into account during the development of an electronic health record system, because some patients are concerned that their electronic healthcare data might be easily accessed or compromised by unauthorized individuals for inappropriate or even unlawful purposes rather than for proper medical use. Hence, the protection of patients' privacy as well as safe access and retrieval of patients' information is vitally important in the design of a modern healthcare information system.

In an information sharing scenario, controlling who is accessing the information is a time-consuming and complex task. Accurate patient authentication/identification is the most critical step in this task [5], since it is the key to ensuring right care delivered to the right patient and that the patient's medical records are up to date, accurate and properly shared across systems [3]. Traditional authentication in the healthcare sector is through passwords. Passwords are simple to use and deploy; however, passwords are also considered to be an extremely poor form of protection. It is reported that 80% of security incidents are related to poorly chosen passwords [6]. For example, some passwords are simple combinations of well-known numbers, e.g., 123456, or date of birth, or telephone extension, which are easy to guess and breach [7].

In comparison to passwords, biometrics, which is a biological measurement technology, uses the unique nature of some physical or behavioral traits of human beings for verification and/or identification1. Biometric technology is being pushed forward to replace traditional ways of authentication, such as passwords and tokens, which are physical devices for authentication [8] 1. The fact that biometric traits cannot be forgotten or lost and are hard to forge enables them to be more secure than traditional authentication. Many biometric traits can be defined from a human body. Examples of biometric traits include fingerprint, face, iris, voice and so on. They can be generally classified into two categories, physiological traits and behavior traits, as shown in Figure 1. Each of them has its strengths and weaknesses, and plays a unique role in some specific applications [9], [10].

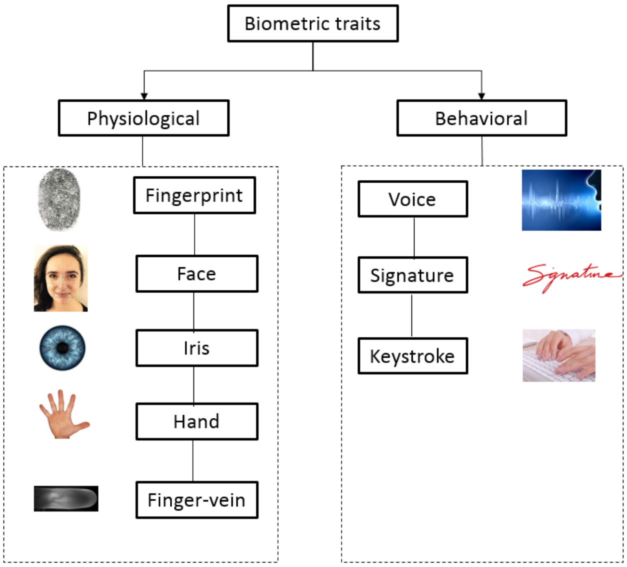


FIGURE 1. Classification of biometric traits (adapted from [15]).

Among all the biometric recognition systems, fingerprint-based recognition systems are the most extensively studied and most widely deployed. On the surface of a finger, the pattern of ridges and valleys has been determined in the first few months and even identical twins own different patterns [8]. The recognition performance, measured by equal error rate (EER) [11], of fingerprint-based recognition systems has been reported to be pretty good [11]. Finger-vein is another unique trait related to one's fingers and can be used to identify individuals. Finger-vein develops inside fingers and the collection of finger-vein images is touch-less, therefore it is not prone to external distortion suffered by fingerprint during the image acquisition process. Also, finger-vein does not leave latent prints on any object surface like fingerprint. Moreover, a finger-vein recognition model can come with liveness detection that senses flow of blood in veins [12]–[14], which makes finger-vein a promising trait for biometric systems.

This paper focuses on the design of a finger-vein based bio-cryptosystem built for smart cards. The proposed bio-cryptosystem considers not only the security of healthcare data but also the security of the biometric template itself. In addition, the proposed scheme strikes a good balance between security and matching performance. The rest of this paper is organized as follows. In Section II, biometric applications in the healthcare industry are reviewed and comparatively analyzed. In Section III, the new cancelable finger-vein, smart card based bio-cryptosystem is proposed. In Section IV, the experimental results and security analysis of the proposed system are provided. The conclusions and future research directions are given in Section V.

II. RELATED STUDY

A. INTRODUCTION OF EXISTING WORK

A patient's healthcare data should be available to all medical professionals who have the right to access the data so that they can perform their duties. Healthcare data security and patients' privacy are the major concerns in an information sharing process, where the healthcare data are operated by multiple users and may be corrupted in the sharing channels. The maintenance of healthcare data security is costly and complex. To achieve a good balance between the security requirement and the availability of healthcare data, when designing a security mechanism, we should consider such factors as security, efficiency and user friendliness [4].

Biometric recognition techniques provide reliable user authentication to ensure that only authorized personnel can access patients' healthcare data [16]. Biometric systems can also facilitate remote access to healthcare data [17] by using biometric features as a tool of authentication. For example, in [18], Bao *et al.* introduced a physiological signal, heart rate variability (HRV) based entity authentication scheme specific for a body area sensor network (BASN), which is a basic component in the healthcare systems. In [19], Krawczyk and Jain designed and implemented an authentication system based on voice and signature data. The proposed system helps medical facilities comply with the HIPAA standards regarding protection and privacy of medical records. The voice and signature modalities are combined at the matching score level and the weighted sum rule are utilized. Garson and Adams [7] developed a system architecture for data encryption and access control in an e-hospital environment. In this architecture, a two-factor authentication mechanism is introduced for improving security. One factor is the username and password system, and the other factor is fingerprint biometrics. However, the cost of a two-factor authentication mechanism may be higher than a single-factor authentication mechanism. In [20], the authors proposed to use both encryption and authentication for tele-healthcare communication. The benefits of combining static biometrics, e.g., fingerprint, and dynamic biometrics, e.g., electrocardiogram (ECG), are discussed. In [4] and [21], the authors analyzed the advantages and disadvantages of using biometric technology in the healthcare industry. The biometric technology is compared with traditional identification methods, e.g., passwords, to determine the core benefits and shortcomings. Andreeva [22] first discussed the problem of human authentication in the BASN (body area sensor network), and then proposed the heart sound based biometric technique as an authentication solution. Díaz-Palacios *et al.* [23] gave an insight on how to combine hardware and software methodologies with biometrics to preserve patients' privacy while retrieving the health information of the patients. Specifically, a mobile device embedded with a fingerprint reader is designed to capture and send the fingerprint of the patient from an emergency scene to a central database. If biometric matching is successful, the patient's health information will be returned to the mobile device. Being token-free is the obvious advantage of this approach, while other methods require the patient to carry a token. He *et al.* [24] proposed a tri-factor to achieve user authentication for the BASN for healthcare application. In the tri-factor method, the user's password, smart card and ECG, are utilized as three factors to enhance the security and accuracy of identity authentication. In [25], Azeta *et al.* designed a CareMed Hospital Information System (HIMS), which uses PIN and fingerprint as two-factor authentication to secure patients' health records. In [26], to safeguard the cloud based electronic health record (EHR), the authors provided a comprehensive solution with a cryptographic role based technique. It distributes session keys to establish communications and with location and ECG based biometrics, it authorizes users. Apart from being used for authentication, ECG is treated as the host to embed the HER data securely by steganography.

B. COMPARATIVE ANALYSIS OF EXISTING WORK

In the aforementioned systems, most of them use biometrics as a single factor or one of multiple factors, e.g., fingerprint, passwords and smart card, to offer authentication and access control. In these systems, the role of the biometric modality is to conduct matching between the template and query, to generate a verdict of success or failure. If matching is successful, the user is granted the right to access the corresponding healthcare data. We illustrate a general framework of such a biometric based authentication system in Figure 2.

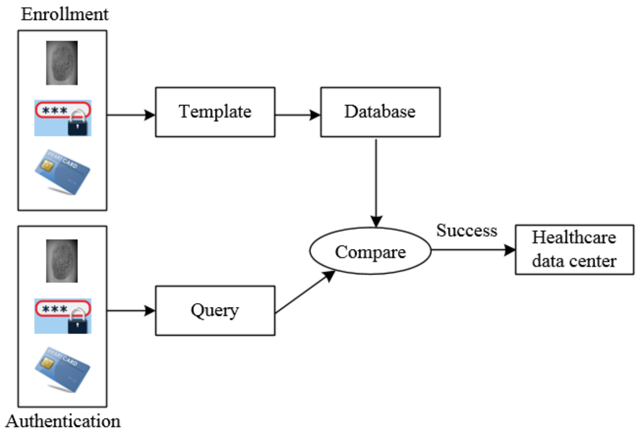


FIGURE 2. A general framework of a basic biometric based authentication system.

A fundamental drawback of this framework is that the biometric modality only allows the user to gain system access based on the matching result, but it does not provide further protection to healthcare data. In [4], the idea of biometric cryptography is proposed to further increase the security of sensitive information. The biometric modality is used to generate or release a cryptographic key for encrypting sensitive healthcare data. Therefore, the biometric modality can be utilized not only for access authorization or identity verification but also for protecting sensitive health related information.

C. MOTIVATION AND CONTRIBUTION

The idea of biometric encryption for healthcare data proposed in [4] can obviously increase the security of sensitive information compared with the existing biometric systems, e.g., [18]–[26], which are only designed for authentication/access control purposes. However, the concept proposed in [4] did not aim to include design details and experimental tests to validate the idea. Existing biometric systems in healthcare applications do not consider the security of the biometric modality itself. It is well known that losing one's biometric data can have serious consequences of identity abuse and privacy invasion. There is a gap in literature to examine issues such as feature selection, performance and security analysis of biometric encryption for healthcare data.

To fill the above gap, in this paper we propose a cancelable finger-vein, smart card based bio-cryptosystem to encrypt sensitive healthcare data while securing the original biometric data themselves. The main contributions of the proposed system are summarized below:

1. The proposed system is equipped with the functions of both authentication and data encryption via a cryptographic key which is bound and secured by the biometric template. This is a clear improvement over the existing biometric systems in healthcare industry applications, because existing systems only have the function of user authentication.
2. We propose to store both sensitive healthcare data and biometric template data on a smart card. With healthcare data and biometric template data stored centrally in a database and shared in multiple systems, sensitive data misuse and theft is a growing concern for the healthcare industry. To resolve this problem, the smart card can be designed to store as well as match the biometric data on the card. Since the biometric template never leaves the card, access to it is prevented during transmission, which greatly helps to reduce the risk of information leakage.
3. The cancelable template technique is employed in the proposed system. One major concern over the use of biometrics is the permanence of a biometric trait. When biometrics in one application is compromised, any other applications in which the same biometrics is enrolled are exposed. With the properties of revocability and diversity, cancelable biometrics employed can effectively protect biometric template data across various applications.

III. PROPOSED CANCELABLE FINGER-VEIN, SMART CARD BASED BIO-CRYPTOSYSTEM

To secure sensitive healthcare data and finger-vein biometric features, we develop a finger-vein, smart card based cancelable bio-cryptosystem. The system includes two phases: the data encryption phase and data decryption phase. In the setup process, three types of data: the helper data, hash value of secret key and the encrypted healthcare data, are first

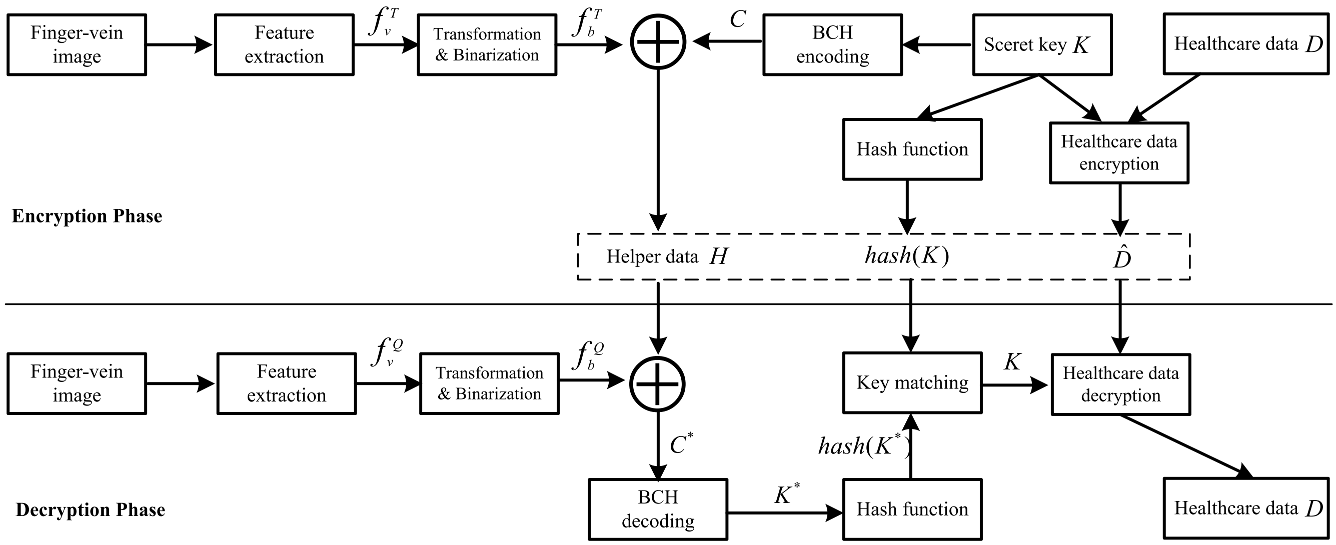


FIGURE 3. The proposed cancelable finger-vein, smart card based bio-cryptosystem.

generated in the data encryption phase. Specifically, sensitive healthcare data is encrypted by using a secret key. To protect the secret key, template finger-vein features are extracted and transformed to establish the transformed template, which is technically bound with the secret key by the well-known biometric cryptography technique, fuzzy commitment scheme (FCS). In the data decryption phase, query finger-vein features are extracted and transformed in the same way as the template. The query is further input to the decoder of FCS to retrieve the secret key. If the query is close enough to the template, key retrieval will be successful. With the retrieved secret key, healthcare data can be correctly decrypted. The proposed system is shown in Figure 3. Also some parameters and their descriptions used in this paper are listed in Table I.

TABLE 1. Some parameters and their descriptions.

Parameters	Descriptions
f_v	Original finger-vein feature
f_c	Transformed finger-vein feature in format of real value
f_b	Transformed finger-vein feature in format of binary value
N_v	Feature length before transformation
N_b	Feature length after transformation
K	Secret key
D	Original healthcare data
$\hat{D}$	Encrypted healthcare data

A. FINGER-VEIN FEATURE EXTRACTION

1) FEATURE EXTRACTION

Finger-vein feature extraction has been extensively researched. The same steps used in [12] are applied in our system for the detection and enhancement of the finger-vein image region of interest (ROI) area. The ROI is cropped into the size of 256×96 pixels. The technique of Gabor filter has been proven to be a powerful tool for image-based feature extraction [27]. According to [27], a family of 40 (=5×8) Gabor filters of five scales and eight orientations are constructed; refer to [27] for the details of the Gabor filter construction. The 256×96 pixel finger-vein image is processed by all the 40 filters. Each Gabor filter (GF) generates a feature string $f_g(i)$ and by concatenating all the 40 feature strings, we obtain a full Gabor feature vector $f_g = f_g(1)\|f_g(2)\| \ldots \|f_g(39)\|f_g(40)\|$ of length 983040 (=256×96×40). It can be seen that this feature vector f_g resides in a high-dimensional space. A mature dimensionality reduction technique, Principal Component Analysis (PCA) [28], is employed. PCA is capable of generating a subspace of an original vector and retaining most information about the original vector [29]. After the dimension reduction with PCA, a finger-vein feature vector f_v of length N_v is generated. The process of the finger-vein feature extraction is demonstrated in Figure 4.

2) FINGER-VEIN FEATURE TRANSFORMATION AND BINARIZATION

Raw finger-vein features need protection. Security and privacy concerns arise to both biometric template data and sensitive healthcare data when raw finger-vein features are compromised. To protected raw finger-vein features, we resort to cancelable biometrics, which is initiated by Ratha *et al.* [30]. The core idea of cancelable biometrics is to transform the original biometric template with a non-invertible transformation function into a new version, so that the transformed biometric template instead of the original one is generated and stored [31], [32]. If the transformed template is compromised, the original template will not be recovered and the transformed template can be revoked and replaced

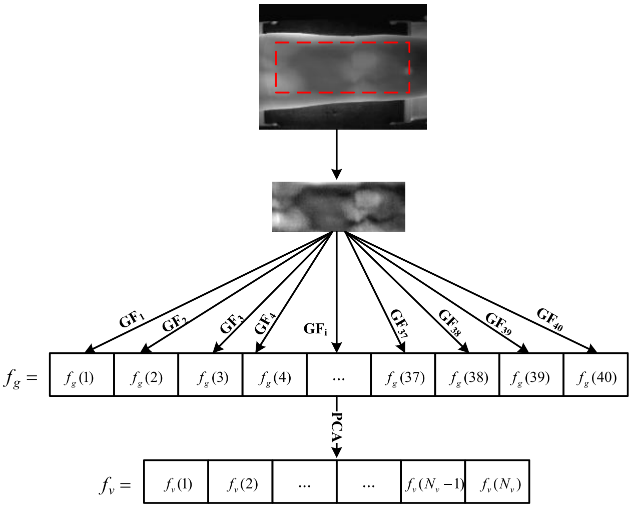


FIGURE 4. The process of finger-vein feature extraction.

by just changing a parameter key. By doing so, the original biometric template and the associated system are safe [33].

To irreversibly transform the extracted finger-vein feature vector f_v of length N_v, the random projection based transformation is used. Specifically, the feature vector f_v is projected onto a random space with the guidance of the random projection matrix $\mathbf{M}$ of size $N_b \times N_v$, where $N_b < N_v$. The non-invertible transformation process can be compactly expressed as:

$$f_c = \mathbf{M} \times f_v \quad (1)$$

where f_c is the inner product of $\mathbf{M}$ and f_v. Equation (1) makes the dimension of the transformed feature vector f_c reduced from N_v to N_b. In our application, N_v is set to be 399 and $N_b \in \{255, 63\}$ by considering the system performance and security.

The elements of f_c are real-valued and therefore unsuitable for the subsequent processing of the FCS (fuzzy commitment scheme) [34], [35], which requires the input to be in the binary format. To convert the feature vector f_c into the binary format, each element $f_c(i), i \in [1, N_b]$, is converted to a binary value $f_b(i)$ by:

$$f_b(i) = \begin{cases} 1 & \textit{if } f_c(i) > \delta \\ 0 & \textit{if } f_c(i) \leq \delta \end{cases} \quad (2)$$

where δ is a threshold and is set to be 0 in our application. Using Equation (2), we get the binary feature vector $f_b = [0, 0, 1, \ldots, 1, 1, 0]$ of length N_b. The process of feature transformation and binarization is demonstrated in Figure 5.

B. SECRET KEY BINDING AND RETRIEVAL

Obviously, both the sensitive healthcare data D and the biometric template feature vector f_b^T (the superscript T stands for 'template') contain crucial information, so they cannot be stored on a smart card without protection. In traditional cryptography, D can be protected by a secret key K together with a data encryption function, as $\hat{D} = F_e(D, K)$. However, the secret key K itself needs protection since it plays the most important role in the protection of D. We apply the FCS (fuzzy commitment scheme) [34] to the protection of both the secret key K and the biometric template feature vector f_b^T by technically binding them together. Fuzzy commitment scheme is a combined technique of error-correction code and cryptography. It can conceal and bind a secret in a way that makes it is infeasible for an adversary to learn the secret. With its error correction characteristic, it is useful in biometric authentication systems, in which the biometric data is subject to random noises/errors. By using FCS in biometric application, it is hard to restore either the secret key or the biometric template without any knowledge of the user's biometric data [35]. In this way, both the healthcare data D and the biometric template feature vector f_b^T are secured. Hence, the secret key binding and retrieval procedures are the critical steps, which are detailed below.

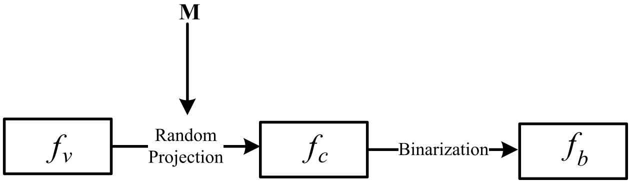


FIGURE 5. The process of finger-vein feature transformation and binarization.

1) SECRET KEY BINDING

The healthcare data encryption is provided by the FCS based on the error correction code, "Bose-Chaudhuri-Hocquenghem" (BCH) code [36], with (n, k, t) parameter settings, where n is the codeword length, k is the secret key length and t is the correctable error length. The BCH encoder (Enc) module converts the secret key K into its corresponding codeword $C \in \{0, 1\}^{\mathrm{n}}$, as $C = Enc(K)$, where $K \in \{0, 1\}^{\mathrm{k}}$ is the secret key and is as long as k bits. The codeword C is then bound with the binary template vector f_b^T through the XOR operation creating the offset H as helper data, $H = C \oplus f_b^T$, where $\oplus$ is the XOR operation [37]. The helper data H together with the hash value $hash(K)$ of K are stored on the smart card.

2) SECRET KEY RETRIEVAL

The healthcare data decryption relies on whether the secret key used for encryption can be retrieved correctly. The secret key retrieve process equals to the authentication process. If the secret key can be retrieved successfully, the authentication is passed and the user can correctly decrypt the encrypted healthcare data.

In the decryption step, a query finger-vein vector, f_b^Q (the superscript Q stands for 'query') is generated by the same steps as the template feature vector f_b^T. Hereafter, the helper data H is XOR-ed with f_b^Q, resulting in the possible compromised codeword $C^* = H \oplus f_b^Q = C \oplus (f_b^T \oplus f_b^Q) = C \oplus e$, where the hamming distance $\varepsilon = d(f_b^T, f_b^Q) = \|e\|$ is the number of errors compromising the codeword C [37]. By using the decoder (Dec) module of FCS, a candidate key K^* is recovered, as $K^* = Dec(C^*)$. If the hash value $hash(K^*)$ of K^* is equal to the hash value $hash(K)$ of K, it means that K is equal to K^*. This happens only when the hamming distance between the template feature vector f_b^T and query feature vector f_b^Q is smaller or equal to the error correcting capability of the BCH code, i.e., $\varepsilon = d(f_b^T, f_b^Q) \leq$ t, where $d(\cdot)$ is a function calculating the hamming distance. Therefore, to successfully retrieve the secret key K, the query feature vector f_b^Q must be close enough to the template feature vector f_b^T within t bits of difference.

After the secret key K is retrieved correctly, it is further supplied into the data decryption function $F_d(\cdot)$, of which the encrypted healthcare data $\hat{D}$ can be decrypted to D, as $D = F_d(\hat{D}, K)$.

IV. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

A. EXPERIMENTAL RESULTS

We carry out experiments to evaluate the proposed cancelable finger-vein, smart card based bio-cryptosystem by using a public finger-vein database included in the Homologous Multi-modal Traits Database (FV-HMTD) [38]. The chosen finger-vein database involves finger-vein images from 106 users. Six images are acquired from each of six fingers (index finger, middle finger and ring finger of both hands) of each user. So a total of 106×6=636 different fingers with six finger-vein images per finger are collected. Each finger-vein image is of size 320×240 pixels. In our experiments, the first four finger-vein images of each finger from the first 100 fingers are used for training and the remaining two finger-vein images of each finger are used for testing.

The evaluation of the proposed system is based on three indices, False Acceptance Rate (FAR), False Rejection Rate (FRR) and the Equal Error Rate (EER), which is the error rate when the FAR is equal to FRR. To obtain the value of FRR, the fifth image is considered as the template and the sixth image from the same finger is used as the query. To obtain the value of FAR, the fifth image of each finger is considered as the template and the fifth image from other fingers is used as the query. To avoid correlation, if an image a has been compared with an image b, then the symmetric comparison, e.g., b against a, is not performed. Therefore, a total of 100 genuine matching tests and 4950 (=100×99÷2) imposter matching tests are performed [39].

We first evaluated the system performance before and after cancelable transformation. The finger-vein feature vector f_v, which is extracted from a finger-vein image by the Gabor filter and PCA techniques, is set to be $N_v = 399$ in length before cancelable transformation. After random projection based cancelable transformation, the resulting finger-vein feature vector is f_c with a length of N_b. As mentioned in Section III, two different parameter values $N_b \in \{255, 63\}$ are applied in our experiments.

Template-query matching tests are conducted by using the feature vectors before and after cancelable transformation, respectively. Since the feature-vein feature vectors f_v and f_c are in the format of real-value, the similarity between them can be calculated to see if the template and query data match. Assume $f^T = f_v^T$ or f_c^T is the feature vector extracted from a template image, and $f^Q = f_v^Q$ or f_c^Q is the feature vector extracted from a query image. The similarity score between f^T and f^Q is calculated as follows

$$S_{T_Q} = 1 - \frac{\|f^T - f^Q\|_2}{\|f^T\|_2 + \|f^Q\|_2} \tag{3}$$

where $\|\cdot\|_2$ represents 2-norm and the similarity score S_{T_Q} is in the range [0, 1]. 0 means that two feature vectors are totally different and 1 means they are exactly the same. The corresponding system performance under different parameter settings is shown in Figure 6.

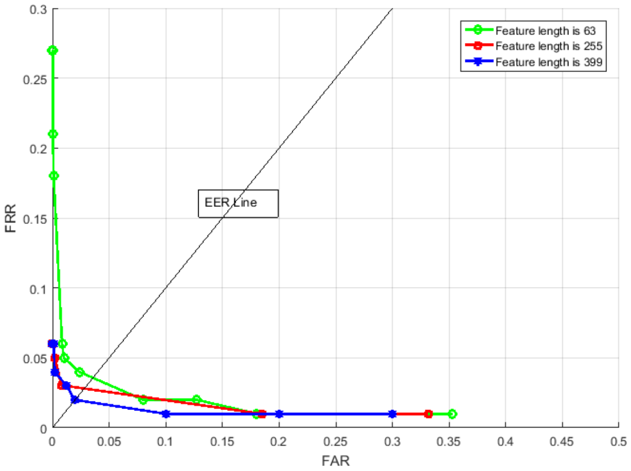


FIGURE 6. The system performance before and after cancelable transformation.

From Figure 6, we can see that matching performance decreases after cancelable transformation. The feature vector length before cancelable transformation is $N_v = 399$, which corresponds to the matching performance of EER=2%; after random projection based cancelable transformation, the performance decreases to be EER=3% with the feature vector length $N_b = 255$, and further decreases to be EER=3.77% with the feature vector length shortened to $N_b = 63$. Different values of N_v and N_b determine the size of random projection matrix $\mathbf{M}$, which is of size $N_b \times N_v$. The random projection based cancelable transformation is a many-to-one projection, the smaller the N_b value is, the less information from the original feature vector is kept after transformation. In this situation, the discriminative power of the feature vector will decrease and cause poorer matching performance, as verified by the experiments above. However, with less information kept from the original feature vector, it is harder for the adversary to reverse from f_c to f_v, which translates into higher security of the template.

To further evaluate the system performance, the FRR and FAR values are examined. Recall that the BCH code used in FCS is described by the triplet (n, k, t). To strike a balance between security and performance, we choose the BCH codes from a list of possible triplet values. System performance is investigated with different BCH codes. For a fixed n, which is set to be the same as N_b, FAR and FRR for different values of t are computed and shown in Figure 7 and Figure 8. It is straightforward to observe that for the same n value, e.g., n=63 or 255, when t is small, the FAR is small, but FRR is high. Some of the (n, k, t) BCH codes and their corresponding FAR and FRR are listed in Table II. A smaller value of t corresponds to a longer key length k of secret key K. For example, if the key length is k=13, the system performance is FRR=8% with FAR=0. When the key length is increased to be k=47, the system performance is FRR=24% with FAR=0.

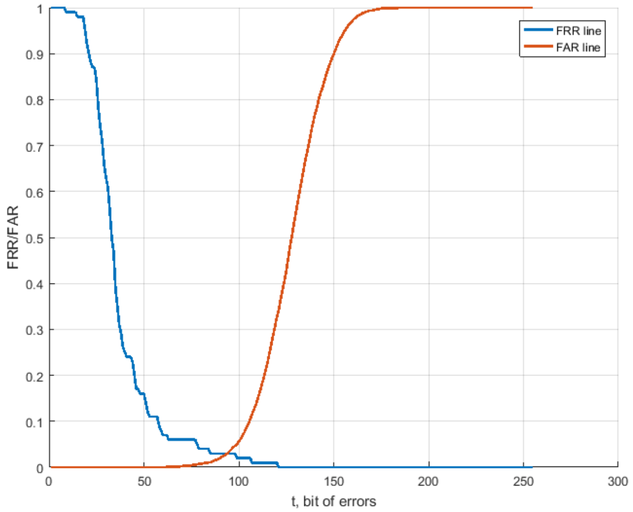


FIGURE 7. The system performance under different t when n=255.

TABLE 2. The system performance with different parameter settings.

n (bits)	k (bits)	t (bits)	FRR/FAR (%)
63	7	15	5/0.46
	18	10	32/0.04
	30	6	53/0
	36	5	62/0
255	13	59	8/0
	37	45	20/0
	47	42	24/0
	63	30	63/0

B. SECURITY ANALYSIS

The main objective of the proposed bio-cryptosystem is to protect sensitive healthcare data stored on the smart card. In contrast to the traditional key-based cryptographic scheme, in which healthcare data protection relies on keeping the key secret, our proposed system seamlessly bound the key with the template finger-vein features by FCS. Without the query features from the same user, it is difficult to retrieve the secret key.

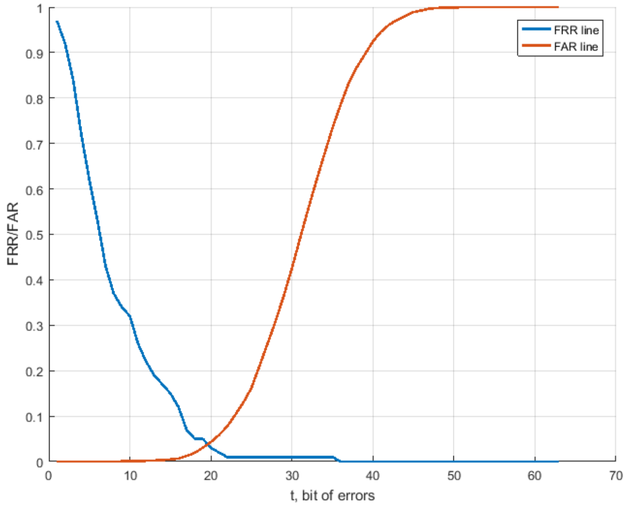


FIGURE 8. The system performance under different t when n=63.

One way to retrieve the key is through brute force attack. Its computational complexity equals to the key length k, which is a variable in the range of 7-63 bits, Different k values imply different system performance. In our testing, we chose the (n, k, t) BCH code to be (255, 47, 42) BCH code, which can provide protection to a 47 bit secret key with the system performance of FRR=24% when FAR=0.

Another way to compromise the secret key is by attacking the FCS. In FCS, the k bit secret key K is mapped to a n bit codeword C of an (n, k, t) BCH code. The template finger-vein feature vector f_b^T and the codeword C are XOR-ed to generate helper data H, as $H = C \oplus f_b^T$. When the smart card is stolen, all the internal data inside the smart card including the helper data H can be revealed. Given the (n, k, t) BCH code, by the sphere-packing bound [40], the rough lower bound on the difficulty facing the adversary, who has obtained the helper data H and attempts to reconstruct the feature vector f_b^T, is equal to the entropy of f_b^T by a given H. This is expressed in Equation (4).

$$H_\infty(f_b^T|H) = \log_2\left(2^{\mathrm{n}}/\binom{\mathrm{n}}{\mathrm{t}}\right) \tag{4}$$

If feature vector f_b^T is known, then the key K is no longer deemed secret. With a specific BCH code, e.g., (255, 47, 42) BCH code, of which n=255, t=42, the security provided by FCS to the feature vector f_b^T is 94 bits calculated by Equation (4). We can see that in this case, the adversary actually requires more effort than directly brute force attacking the secret key K, whose computational complexity is only 47 bits under the (255, 47, 42) BCH code.

One motivating reason for an adversary to capture the feature vector f_b^T is that if the same feature vector f_b^T from the same user is used for different applications, then the adversary can use the restored feature vector f_b^T to launch cross matching attacks to the user's private data in other applications. However, it is impossible in the proposed system thanks to the cancelable template design we adopt. The reason is that the feature vector f_b^T is a transformed, non-invertible version of the original feature vector f_v^T. Under the guidance of transformation matrix $\mathbf{M}$, a different feature vector f_b^T can be easily generated by just changing the seed for $\mathbf{M}$. Through this method, the possibility of launching cross matching attacks can be eliminated.

V. CONCLUSION AND FUTURE DIRECTIONS

Due to their advantages, biometric authentication systems have increasingly become the preferred means to identity authentication in the healthcare sector. In this paper, we have proposed a cancelable finger-vein, smart card based bio-cryptosystem. The proposed system not only can perform authentication but also provide data encryption to sensitive healthcare data, which has not previously been proposed in the existing biometric systems for healthcare industry. Also, the idea of storing both the biometric template and sensitive healthcare data on the smart card can avoid information leakage during data exchange or biometric template transformation, because biometric template data never leaves the card. Moreover, the employment of cancelable biometrics further enhances system security.

For future work, we will explore other more stable biometrics, e.g., iris, to obtain high-quality biometric features for better data protection. We will also investigate the fusion of multiple biometric traits so as to design multi-biometric systems for the healthcare sector, which will provide stronger security and better recognition accuracy.

REFERENCES

[1] J. Hu, H.-H. Chen, and T.-W. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations," *Comput. Standards Interfaces*, vol. 32, nos. 5–6, pp. 274–280, 2010.

[2] D. Wright and C. Raab, "Privacy principles, risks and harms," *Int. Rev. Law, Comput. Technol.*, vol. 28, pp. 277–298, 2014.

[3] O. F. Segun and F. B. Olawale, "Healthcare data breaches: Biometric technology to the rescue," *Int. Res. J. Eng. Technol.*, vol. 4, no. 11, pp. 946–950, 2017.

[4] A. E. F. Zuniga, K. T. Win, and W. Susilo, "Biometrics for electronic health records," *J. Med. Syst.*, vol. 34, no. 5, pp. 975–983, 2010.

[5] B. Spence. (2011). *Hospitals can Finally Put a Finger on Biometrics*. Accessed: Jun. 22, 2018. [Online]. Available: http://www.securityinfowatch.com/article/10473265/hospitals-can-finally-put-a-finger-on-biometrics

[6] G. C. Kessler. Disponível por, MAIO. (1999). *Passwords-Strengths and Weaknesses*. http://www.hill.com/library/staffpubs/password.html

[7] K. Garson and C. Adams, "Security and privacy system architecture for an e-hospital environment," in *Proc. 7th Symp. Identity Trust Internet*, 2008, pp. 122–130.

[8] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*. New York, NY, USA: Springer-Verlag, 2007.

[9] W. Yang, J. Hu, J. Yang, S. Wang, and L. Shu, "Biometrics for securing mobile payments: Benefits, challenges and solutions," in *Proc. 6th Int. Congr. Image Signal Process. (CISP)*, 2013, pp. 1699–1704.

[10] W. Yang, J. Hu, C. Fernandes, V. Sivaraman, and Q. Wu, "Vulnerability analysis of iPhone 6," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, 2016, pp. 457–463.

[11] *FVC-onGoing*. Accessed: Jun. 22, 2018. [Online]. Available: https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/Home.aspx

[12] S. J. Xie, S. Yoon, J. Yang, Y. Lu, D. S. Park, and B. Zhou, "Feature component-based extreme learning machines for finger vein recognition," *Cogn. Comput.*, vol. 6, no. 3, pp. 446–461, 2014.

[13] S. J. Xie, Y. Lu, S. Yoon, J. Yang, and D. S. Park, "Intensity variation normalization for finger vein recognition using guided filter based singe scale retinex," *Sensors*, vol. 15, no. 7, pp. 17089–17105, 2015.

[14] W. Yang, J. Hu, and S. Wang, "A finger-vein based cancellable bio-cryptosystem," in *Network and System Security*. Berlin, Germany: Springer, 2013, pp. 784–790.

[15] S. R. Kodituwakku, "Biometric authentication: A review," *Int. J. Trend Res. Develop.*, vol. 2, no. 4, pp. 113–123, 2015.

[16] W. Atkins, "A bill of health for biometrics?," *Biometric Technol. Today*, vol. 8, no. 9, pp. 8–11, 2000.

[17] Y. Shin, Y. Lee, W. Shin, and J. Choi, "Designing fingerprint-recognition-based access control for electronic medical records systems," in *Proc. 22nd Int. Conf. Adv. Inf. Netw. Appl.-Workshops (AINAW)*, 2008, pp. 106–110.

[18] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," in *Proc. IEEE-EMBS 27th Annu. Int. Conf. Eng. Med. Biol. Soc.*, Jan. 2005, pp. 2455–2458.

[19] S. Krawczyk and A. K. Jain, "Securing electronic medical records using biometric authentication," in *Audio- and Video-Based Biometric Person Authentication*. Berlin, Germany: Springer, 2005, pp. 435–444.

[20] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, "A biometrics based security solution for encryption and authentication in tele-healthcare systems," in *Proc. 2nd Int. Symp. Appl. Sci. Biomed. Commun. Technol. (ISABEL)*, 2009, pp. 1–4.

[21] H. Jhaveri, H. Jhaveri, and D. Sanghavi, "Biometric security system and its applications in healthcare," *Int. J. Tech. Res. Appl.*, vol. 2, no. 6, pp. 15–20, 2014.

[22] E. Andreeva, "Alternative biometric as method of information security of healthcare systems," in *Proc. 12th Conf. FRUCT Assoc.*, Oulu, Finland, 2011, p. 5.

[23] J. R. Díaz-Palacios, V. J. Romo-Aledo, and A. H. Chinaei, "Biometric access control for e-health records in pre-hospital care," in *Proc. Joint EDBT/ICDT Workshops*, 2013, pp. 169–173.

[24] C.-G. He, S.-D. Bao, and Y. Li, "A novel tri-factor mutual authentication with biometrics for wireless body sensor networks in healthcare applications," *Int. J. Smart Sens., Intell. Syst.*, vol. 6, no. 3, pp. 910–931, 2013.

[25] A. A. Azeta, D.-O. A. Iboroma, V. I. Azeta, E. O. Igbekele, D. O. Fatinikun, and E. Ekpunobi, "Implementing a medical record system with biometrics authentication in E-health," in *Proc. IEEE AFRICON*, Sep. 2017, pp. 979–983.

[26] U. Premarathne *et al.*, "Hybrid cryptographic access control for cloud-based EHR systems," *IEEE Cloud Comput.*, vol. 3, no. 4, pp. 58–64, Jul./Aug. 2016.

[27] V. Štruc and N. Pavešic, "The complete Gabor-Fisher classifier for robust face recognition," *EURASIP J. Adv. Signal Process.*, vol. 2010, p. 26, May 2010.

[28] K. Delac, M. Grgic, and S. Grgic, "Independent comparative study of PCA, ICA, and LDA on the FERET data set," *Int. J. Imag. Syst. Technol.*, vol. 15, no. 5, pp. 252–260, 2005.

[29] M. Turk and A. Pentland, "Eigenfaces for recognition," *J. Cognit. Neurosci.*, vol. 3, no. 1, pp. 71–86, 1991.

[30] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[31] S. Wang, G. Deng, and J. Hu, "A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognit.*, vol. 61, pp. 447–458, Jan. 2017.

[32] S. Wang and J. Hu, "A blind system identification approach to cancelable fingerprint templates," *Pattern Recognit.*, vol. 54, pp. 14–22, Jun. 2016.

[33] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia Pairs," *Pattern Recognit.*, vol. 66, pp. 295–301, Jun. 2017.

[34] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur.*, 1999, pp. 28–36.

[35] A. Teoh and J. Kim, "Secure biometric template protection in fuzzy commitment scheme," *IEICE Electron. Exp.*, vol. 4, no. 23, pp. 724–730, Dec. 2007.

[36] R. Chien, "Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 4, pp. 357–363, Oct. 1964.

[37] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis, "Preventing the decodability attack based cross-matching in a fuzzy commitment scheme," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 107–121, Mar. 2011.

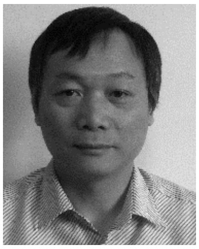
[38] Y. Yin, L. Liu, and X. Sun, "SDUMLA-HMT: A multimodal biometric database," in *Proc. Chin. Conf. Biometric Recognit.*, 2011, pp. 260–268.

[39] W. Yang, J. Hu, S. Wang, and M. Stojmenovic, "An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures," *Pattern Recognit.*, vol. 47, no. 3, pp. 1309–1320, 2014.

[40] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: Elsevier, 1977.

WENCHENG YANG is currently a Post-Doctoral Researcher with the Security Research Institute, Edith Cowan University, Australia. His major research interest is in biometric security and pattern recognition. He has published several high-quality papers in high ranking journals and conferences, such as the IEEE Transactions on Information Forensics and Security, and *Pattern Recognition*.

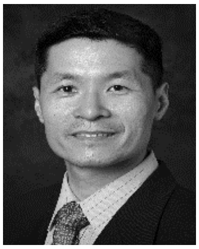
SONG WANG received the Ph.D. degree from the Department of Electrical and Electronic Engineering, The University of Melbourne, Australia. She is currently a Senior Lecturer with the Department of Electronic Engineering, La Trobe University, Australia. Her research areas are biometric security, blind system identification and wireless communications.



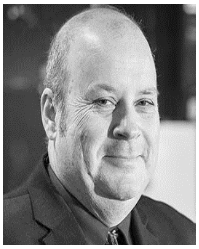
JIANKUN HU is currently a Full Professor with the School of Engineering and IT, University of New South Wales, Canberra, Australia. His main research interest is in the field of cyber security, including image processing/forensics and machine learning, where he has authored many papers in high-quality conferences and journals, including the IEEE Transactions on Pattern Analysis and Machine Intelligence. He has served on the Editorial Board of up to seven international journals, including the top venue IEEE Transactions on Information Forensics and Security and served as the Security Symposium Chair of IEEE flagship conferences of the IEEE ICC and the IEEE Globecom. He has received seven Australian Research Council (ARC) Grants and has served at the prestigious Panel of Mathematics, Information and Computing Sciences, ARC The Excellence in Research for Australia Evaluation Committee.

GUANGLOU ZHENG was a telecommunication system R&D engineer with the Nanjing R&D Center, ZTE Corporation, Nanjing, China. He is currently a Post-Doctoral Research Fellow with the Security Research Institute, Edith Cowan University, Perth, WA, Australia. His research interests include wireless network security, medical system security, biometrics, IoT security, ECG signal processing, spacecraft orbit determination, GPS/GNSS, and precise navigation and positioning technologies.

JUNAID CHAUDHRY (SM'17) is currently an Assistant Professor with the College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ, USA. He has authored three books, over 50 research papers, and holds several patents. He is a Senior Member the High Technology Crime Investigation Association, the Australian Computing Society, and the Australian Information Security Association, and frequently volunteers his time for public speaking events, conference organization, and editing of scientific journals.



ERWIN ADI received the B.Sc. degree in computer science from The State of New York at Stony Brook, NY, USA, in 1992, the M.Sc. degree in communications technology from the University of Strathclyde, Glasgow, U.K., in 1998, and the Ph.D. degree in computer science from Edith Cowan University, Perth, Australia, in 2017. He served for six years giving lectures in network and Web security with Bina Nusantara University, Jakarta, Indonesia, where his students went to the final stage of a national hacking competition. He is currently a Post-Doctoral Researcher with the University of New South Wales, Australia, under the Australian Centre for Cyber Security research group. One of his publications proposed a novel method that adapts the architecture of human immune system to detect cyber attacks. He received the Dean's List Award (top 2% student of the university) from The State of New York at Stony Brook for 3 semesters and was invited to join the Golden Key National Honor Society.



CRAIG VALLI is currently the Director of the Security Research Institute, Edith Cowan University, and a Professor of Digital Forensics. He is also the current Research Director of the Australian Cyber Security Research Institute. He has over 30 years of experience in the ICT industry and consults to industry and government on cyber security and digital forensics issues. He has over 100 peer-reviewed academic publications in cyber security and digital forensics. His main research and consultancy is focused on securing networks and critical infrastructures, detection of network borne threats and forensic analysis of cyber security incidents. He is also a fellow of the Australian Computer Society. He is the Director of the Australian Computer Society Centre of Expertise in Security at ECU. He is also the Vice President of the High Tech Crime Investigators Association (Australian Chapter) and a member of the INTERPOL Cyber Crime Experts Group.