This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSE.2021.3063174, IEEE Transactions on Network Science and Engineering

SIP: An Efficient and Secure Information Propagation Scheme in E-health Networks

Liping Zhang, Zhen Wei, Wei Ren, *Member, IEEE,* Xianghan Zheng, Kim-Kwang Raymond Choo, and Neal N. Xiong

***Abstract*—Electronic healthcare (e-health) networks are increasingly popular, particular during pandemics such as COVID-19. This reinforces the importance of ensuring security and privacy for data-in-transit. One such solution is steganography-based schemes that utilize biological signals (e.g., ECG) as cover signals to preserve the privacy of patient personal information without affecting the diagnostic features. There are various limitations in existing steganography-based schemes, and in this study we present an effective privacy protection scheme leveraging both multidimensional steganography and shared keys. To enhance security and accelerate signal processing in our design, the Fast Walsh-Hadamard transform (FWHT) is employed to decompose ECG signals into a set of coefficients, of which the less-significant coefficients are used to construct the multidimensional space. The negotiated shared keys facilitate the embedding of encrypted data in the constructed space. We then evaluate the proposed scheme using different categories of ECG signals in the MIT-BIH database. It is observed that the signal distortion is minimal (i.e., less than 1%), even if the embedded data reaches the maximum embedding capacity. The security analysis also demonstrates that unauthorized retrieval of hidden information is not practical, within a short period of time.**

***Index Terms*—E-health Networks, Privacy Protection, Privacy Preservation Steganography, Key Management.**

I. Introduction

Telemedicine has been studied in the last decade or two, and its importance (or benefits) is more prominent in the recent COVID-19 pandemic, where society is locked down due to the stay-at-home orders. Specifically, telemedicine platforms allow patients to consult medical and allied healthcare practitioners from their home or other locations, via their Internet-connected smart mobile devices (e.g., teleconferencing software on their Android or iOS phones) – see also Fig. 1. In such a system, the users (e.g., medical practitioners and patients) are connected wirelessly, and intelligent embedded or wearable low-power sensor devices can be used to collect and monitor the user / patient (e.g., blood pressure, glucose level, temperature, Photoplethysmogram — PPG, Electroencephalograph — EEG, Electrocardiogram — ECG) periodically [1]. Such data (e.g., patient medical and identity information) are typically relayed by the smart mobile devices to a remote medical server, which can facilitate medical diagnosis and inform treatment strategy.

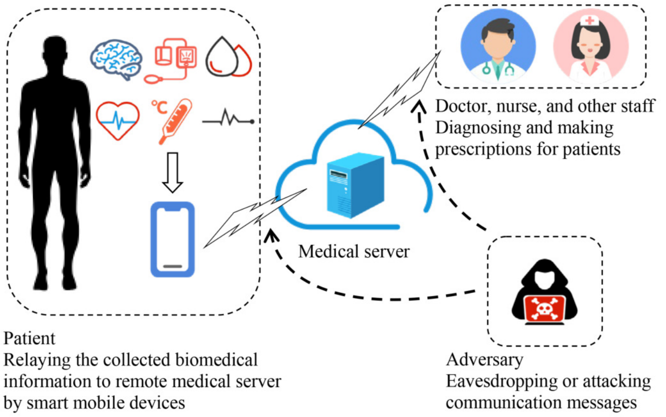

Doctor, nurse, and other staff
Diagnosing and making prescriptions for patients
Medical server
Patient
Relaying the collected biomedical information to remote medical server by smart mobile devices
Adversary
Eavesdropping or attacking communication messages

Fig. 1. An e-health example.

It is clear that such sensitive information (e.g., different types of biological data such as EEG, PPG, and ECG) needs to be secure. For example, intentional or unintentional modifications to patient information transmitted through insecure channels can have serious or fatal consequences [2, 3]. Hence, there have been a large number of security solutions designed to provide security and privacy for data-in-transit, including over insecure channels [4–6].

One potential approach is steganography, which can be used to hide the existence of private information during the transmission process. There exist, however, limitations in existing schemes such as significant storage overheads [7, 8]. Biomedical carriers such as Magnetic Resonance Imaging (MRI) and PPG, have also been explored in steganography-based approaches [9, 10], but these biomedical images are not typical of transmitted biomedical information in e-health environments. ECG, on the other hand, is more common and hence suitable to be used as a cover carrier. In addition, the embedded privacy information such as patient identity can

Liping Zhang is with the School of Computer Science, China University of Geosciences, Wuhan, China 430074; and Hubei Key Laboratory of Intelligent Geo-Information Processing, China University of Geosciences, Wuhan, China 430078.

Zhen Wei is with the School of Computer Science, China University of Geosciences, Wuhan, China 430074.

Wei Ren is with the School of Computer Science, China University of Geosciences, Wuhan, China; Guangxi Key Laboratory of Cryptography and Information Security, Guilin, P.R. China 541004; and Key Laboratory of Network Assessment Technology, CAS, (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, P.R. China 100093); e-mail: weirencs@cug.edu.cn.

Xianghan Zheng is with Fuzhou University, Fuzhou, China; Mingbyte Technology, QingDao, China.

Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA.

Neal N. Xiong is with Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, OK 74464, USA.

Corresponding author: Wei Ren.

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSE.2021.3063174, IEEE Transactions on Network Science and Engineering

be used to authenticate the ECG itself. Although there are benefits associated with ECG-based steganography methods, there are few studies to explore its utility in privacy protection and authentication. As sensitivity is the most crucial factor in the diagnosis [11], it is challenging and complex to employ ECG as a cover carrier in steganography. If the stego ECG is distorted (i.e., differs from the genuine ECG signal), it may result in misdiagnosis or fatalities.

A number of ECG-based steganography schemes have been proposed to guarantee privacy protection of medical data [11–14]. Using wavelet transform technology, some schemes [12, 13] have achieved effective hiding of privacy information in ECG data (signals). However, these solutions require two communication parties to have some pre-shared information, and we observe that the signal processing's performance can be further improved. To enhance security, the security key is adopted in the design of a number of ECG-based steganography schemes [11, 14] to encrypt private patient information. However, the security key used in [11] is a pre-shared key, and the leakage of the shared key can result in the successful attack of the steganography scheme. Furthermore, the scheme of [14] fails to provide sufficient embedding capacity since not all parts of the ECG signal are used for concealment.

ECG as a carrier is more sensitive than other traditional carriers since it is also an important diagnostic data. This characteristic requires that the visual difference between the stego ECG signal and the genuine one to be ignored during diagnosis, so that the stego ECG signal can be directly used for the diagnosis. Such a requirement complicates the design of the steganography scheme. Furthermore, sufficient embedding capacity, security, and efficiency also need to be considered, which further compounds the challenges in designing such schemes. In other words, how to achieve privacy protection using ECG-based steganography in e-health networks is still challenging in practice.

In this paper, a novel steganography-based scheme is proposed to achieve secure communication in e-health networks by using multidimensional steganography and shared keys. The main contributions of our paper are summarized as follows:

- To minimize the risk of unauthorized retrieval, we construct a multidimensional space using ECG signals to strengthen the hiding process. In our design, the multidimensional space is established using the less significant coefficients decomposed by Fast Walsh-Hadamard Transform (FWHT). Then, using both templates generated by the shared keys, the patient sensitive information can be randomly embedded in the constructed multidimensional space. The mathematical analysis demonstrate that our design of multidimensional space increases the complexity of illegitimate retrieval, and it is computationally expensive to crack the proposed steganography algorithm.
- In our design, a dynamical key negotiation method is presented to generate three different shared keys for each steganography process. One shared key is used to encrypt patient sensitive information, and the other two are used in the embedding phase to find the embedding position at the bit level. Since the three shared keys involved in our security scheme are negotiated in each communication, such a dynamic feature of the shared keys further enhances the security of steganography.
- To optimize the performance of the signal processing issue, FWHT is employed in our security scheme to accelerate the signal transform. Furthermore, the large number of less significant coefficients decomposed by FWHT are adopted in our design to maximize the embedding capacity with high imperceptibility. Since the visual difference between the stego signals and the genuine one can be ignored during diagnosis, in our scheme, the doctors can use stego signals to obtain accurate diagnoses without performing retrieval operations. This ensures ECG sensitivity.

The rest of our paper is organized as follows. In the next two sections, we will introduce the related literature and relevant background materials (e.g., system and adversary models), respectively. In Section IV, we will present our proposed steganography-based scheme, followed by its performance and security evaluation in Section V. In Section VI, we present the comparative summary and discuss potential application scenarios. Finally, we conclude this work in the last section.

II. Related Work

In e-health networks, a number of techniques such as cryptography, steganography, and watermarking have been applied to provide privacy protection for a broad range of transmitted data [4, 5]. Cryptographic primitives, for example, can be leveraged to establish a shared shared key that can be subsequently used to encrypt and decrypt medical data. Despite their functional advantages, cryptographic-based approaches may have high computational complexity. The security of the encrypted medical data is mostly determined by the secrecy of symmetric keys, hence the management of keys is crucial.

Unlike typical cryptographic-based approaches, steganography does not require one to convert the transmitted data into an encrypted format, thus reducing the costs associated with encryption / decryption and in some sense minimize the exposure of content hidden using steganography, especially in the presence of passive attackers [11]. Steganography is first introduced in the field of multimedia, and the carriers are usually images [15, 16], audios [17, 18], and videos [19, 20]. A large number of approaches to protect these multimedia carriers have been proposed. In the context of e-health, steganography can also be used to conceal medical data (e.g., in multimedia carriers), although using irrelevant multimedia carriers may result in unnecessary storage overheads [8, 19]. Therefore, in recent years, different steganography approaches have been designed to protect the transmitted medical data using medical data as the carrier (instead of multimedia carriers) [7–14]. For example, Khari et al. [7] presented a scheme based on both cryptography and steganography to protect transmitted medical video data in Internet of Things (IoT) settings. In their design, the elliptic Galois cryptography is applied to encrypt secret data from different medical sources, and a matrix XOR encoding technique is employed to embed the encrypted data into some blocks of a cover image or video with the Adaptive

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

Firefly Optimization. However, this solution is not suitable in e-health networks, since the transmitted carriers are simply images or videos that are irrelevant to the patients; thus, incurring additional communication and storage overheads.

Biomedical data can also be used as the carrier to hide private patient information, as demonstrated in the proposed approaches of [9–14]. Brain MR images, for example, are used in the scheme of [9] to conceal patient medical information. Specifically, private information is embedded in the spatial domain of MRI using the Least Significant Bits (LSB) substitution. Their scheme ensures that the retrieval of embedded bits is lossless, and the stego images do not affect the accuracy of classifying the pathological brain. However, their solution lacks a user-defined security key and once the steganography algorithm is compromised, there is a high risk to patient privacy. Mukhopadhyay et al. [10] proposed a steganography scheme for the PPG signal and its compression. Specifically, they used the optimum truncation of singular values to hide private information in the truncated left-singular matrix coefficients of PPG signals and used ASCII character encoding to realize lossless compression of stego PPG signals. However, since private information is not embedded in the PPG signal, the security of their scheme mainly relies on compression rather than steganography.

Compared with MRI and PPG, ECG is a more suitable carrier in steganography scheme design due to its universal use of daily diagnosis in e-health networks [11–14]. For example, Ibaida and Khalil [12] proposed a 2-D five-level wavelet-based steganography scheme by decomposing the host ECG signal to 32 sub-bands of coefficients, in which the secret information is embedded and scrambled by the given matrix and level vector. Although their scheme employs the 2-D hiding order as the security key, it is static and cannot be updated in each communication. To reduce the storage overheads, an ECG steganography scheme based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) was proposed by Jero et al. [13]. However, this scheme does not have a security key and tnd the storage for the SVD matrix incurs additional overheads. More recently in 2019, Neetika et al. [14] employ a dynamic security key to design a data-embedding algorithm using the chaotic map. In their design, private information is encrypted by performing XOR operations on the chaotically generated values and then embedded in the non-QRS regions of ECG signals using the Optimum Location Selection algorithm. However, compared with algorithms that utilize both non-QRS regions and QRS regions to embed private information (e.g., [12, 13]), the embedding capacity of Neetika et al.'s scheme is not sufficiently large.

Although efforts have been made to achieve privacy protection during the steganography process, existing ECG steganography-based schemes generally do not meet the require security, efficiency, and payload requirements of e-health networks. Schemes such as those of [12, 13] either lack a security key or adopt a static one, and several wavelet-based schemes (e.g., [12–14]) involve time-consuming operations. Also, several non-QRS complex based schemes (e.g., [14]) do not meet the embedding capacity needs. These ECG-based steganography schemes are also not carried out on some special conditions when the ECG signal is pathological. That is, patients who suffer from arrhythmia or other heart diseases will have an irregular ECG, and hence these schemes may not work well under such conditions.

III. Preliminaries

A. Walsh-Hadamard Transform

Walsh-Hadamard Transform (WHT) is a non-sinusoidal orthogonal transform that decomposes a signal from its time domain to its frequency domain [21]. After decomposition, a set of basis functions named Walsh function is obtained. The transform is a $2^m \times 2^m$ square matrix containing only +1 and -1 elements. The lowest order Hadamard transform matrix and the fundamental recursion relations are shown in (1). Each Walsh function has a unique sequency value, and the signal frequency of the original signal can be estimated using the sequency value returned by the transform.

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, H_{2m} = \begin{pmatrix} H_m & H_m \\ H_m & -H_m \end{pmatrix} \tag{1}$$

Walsh-Hadamard transform is widely used in signal processing, language processing, filtering, power spectrum analysis, and other scenarios, which reduce bandwidth storage requirements and spread spectrum analysis. By changing the storage order of the Walsh function, the corresponding application scenarios can be matched. For example, the Walsh function applied to the signal processing adopts a default sequence, while the Walsh function applied to the control system utilizes a Hadamard sequence.

B. Fast Walsh-Hadamard Transform

The fast Walsh-Hadamard transform is a rapid version of WHT, which uses the idea of the divide-and-conquer algorithm to simplify the complex transform process and decompose it into several add and subtract operations [22]. By significantly reducing the complexity of the algorithm from the original $O(n^2)$ to $O(n \log n)$, the FWHT requires less storage space. Its operation expression is shown as

$$y_n = \frac{1}{N} \sum_{i=0}^{N-1} x_i FWHT(n,i), n = 1, 2, ..., N-1 \tag{2}$$

Here, x_i denotes the original signal, $FWHT(n,i)$ represents the process of the transform, N denotes the length of the signal that is transformed by WHT, i is an integer from 0 to $N-1$, and y_n denotes the coefficients obtained after the transform. The transform only works on signals of which the length is equal to a power of two. If the length of the signal does not meet the condition, it will be automatically filled to a power of two with zero before the transform.

C. Fast Walsh-Hadamard transform reconstruction

The FWHT reconstruction is shown as follows. The stego coefficients together with the original significant coefficients are reconstructed to form a stego signal.

$$x_n = \frac{1}{N} \sum_{i=0}^{N-1} y_i FWHT(n,i), n = 1, 2, ..., N-1 \tag{3}$$

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

D. *Key Agreement Scheme*

The shared keys are critical to the steganography scheme. If the shared keys are lost or compromised by adversaries, the sensitive information of the patient could be easily obtained. Therefore, the shared keys should be negotiated during the communicating process to provide uniqueness in each run.

Key agreement schemes are widely used to establish a shared key between two communication parties. During the key negotiation process, the communication parties exchange some key materials to generate a shared key through an insecure channel. Each run of a key agreement scheme generates a unique shared key and this shared key is not known by anyone but only the two communication parties.

E. *System and Adversary Models*

1) System Model: The e-health networks mainly contain three entities, namely: the bio-sensors, the control unit and the medical server. Usually, the bio-sensors are deployed on a user's body or in surrounding environment collecting and transmitting physiological signals, etc, to the control unit. In e-health networks, the bio-sensors are comparatively low-energy and inexpensive devices with limited computational resources.

A control unit collects and forwards various physiological signals from multiple bio-sensors to the associated medical server, as per the specification of health monitoring. The control unit is more powerful than the bio-sensors, for example in terms of computation, communication and storage capabilities. The medical server provides physiological feature extraction and analysis, health information storage and management services. It is also tasked with security, for example to achieve authentication and privacy protection. The proposed security scheme is used to protect the communication between the control unit and the medical server.

2) Adversary Model: As observed in [23], the Dolev and Yao adversary model [24] is one of the most widely used adversary models in applied security research. Similarly, in this paper we adopt the Dolev and Yao adversary model, where the adversary is assumed to have control over the communication channel in the wireless sensor networks. In other words, the adversary can perform the following activities:

- Interception: The adversary can be a passive eavesdropper who has the ability to intercept physiological information between the control unit and the medical server.
- Modification / Tampering: The adversary can also be an active adversary who has the ability to modify and transmit modified data to a medical server.
- Inference: Based on the information obtained, the adversary can learn which signal-processing algorithm(s) is/are used in the security scheme, as well as obtaining the transmitted stego signal.

The adversary's purpose is to obtain the patient privacy by retrieving the hidden secret bits from stego ECG signals.

IV. Our Proposed SIP Scheme

In this paper, we present an innovative steganography scheme that achieves a delicate balance between security and efficiency in e-health environments. Multidimensional steganography and shared keys are designed in the proposed steganography algorithm to achieve high security. In addition, the fast Walsh-Hadamard transform adopted in our security scheme speeds up the signal transform process and meanwhile provides sufficient embedding capacity.

Our proposed scheme consists of three main phases: shared key negotiation phase, embedding phase, and retrieval phase. In the shared key negotiation phase, three shared keys are negotiated between the communication parties using a key agreement scheme. Next, the embedding phase will be performed to realize the secure embedding of secret information. During this process, the original ECG signal is first decomposed into a set of coefficients by FWHT, and a multidimensional space is constructed using the less significant part. Then the secret information is encrypted and embedded in this space using the generated keys. After that, the retrieval process is executed to extract the secret information from the reconstructed stego ECG signal. The holistic view of our proposed security scheme is shown in Fig. 2, and the detailed procedures of our security scheme are explained in the subsequent sections.

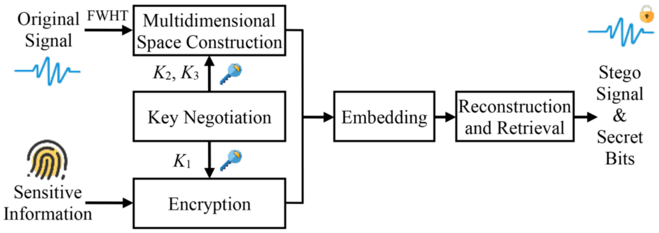


Fig. 2. The holistic view of our proposed scheme.

A. *Negotiation of Three Shared Keys*

In our design, the three keys are generated using a lightweight key agreement scheme, which ensures that the shared keys are different in each communication. Generally, a key agreement scheme can use to establish a shared key between the two communication parties at the end of the key negotiation process. However, in our design, three shared keys need to be constructed that are required in the further embedding stage. So, the existing key agreement schemes need to be improved to generate three shared keys K_1, K_2, and K_3, so that meet the requirements of our design.

Since several authenticated key agreement schemes, such as [25, 26], achieve high security and low consumption, these schemes can be applied to generate three shared keys by modifying the key construction phase after mutual authentication is finished. However, using the generated shared key to construct the other two shared keys may lead to an association among the shared keys. So, we focus on how to break the links among the generated shared keys and provide three unrelated shared keys. Next, we describe the process of three shared keys' negotiation, as shown in Fig. 3.

The construction of the shared key can be designed as $SK = h(A, B, C)$, which is widely used in key agreement schemes [25, 26]. Here $h(\cdot)$ is a collision-free hash function.

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSE.2021.3063174, IEEE Transactions on Network Science and Engineering

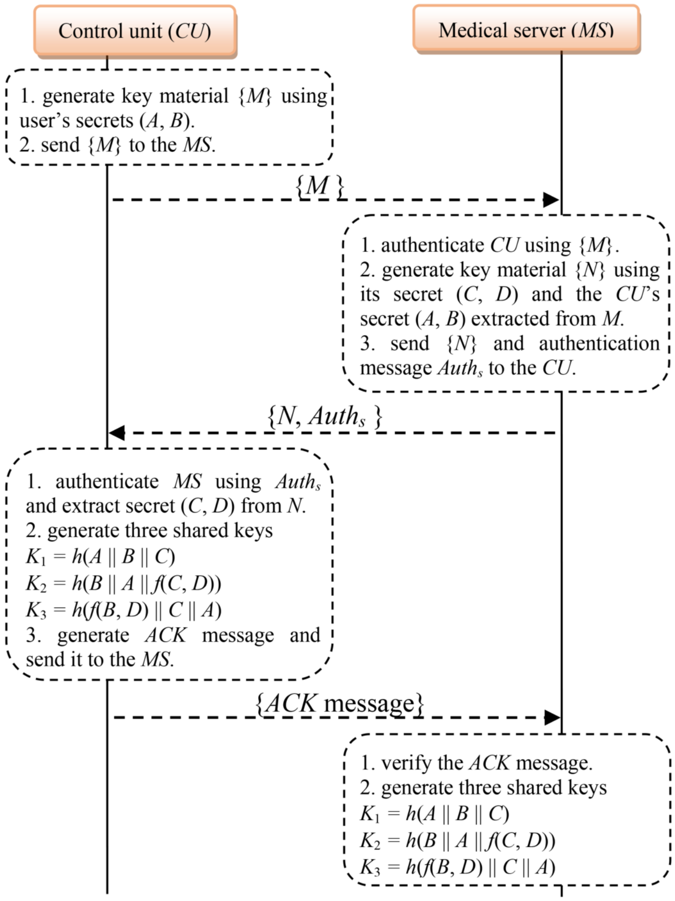

Control unit (*CU*)
Medical server (*MS*)
1. generate key material {*M*} using user's secrets (*A*, *B*).
2. send {*M*} to the *MS*.
{*M* }
1. authenticate *CU* using {*M*}.
2. generate key material {*N*} using its secret (*C*, *D*) and the *CU*'s secret (*A*, *B*) extracted from *M*.
3. send {*N*} and authentication message *Auth_s* to the *CU*.
{*N*, *Auth_s* }
1. authenticate *MS* using *Auth_s* and extract secret (*C*, *D*) from *N*.
2. generate three shared keys
$K_1 = h(A \| B \| C)$
$K_2 = h(B \| A \| f(C, D))$
$K_3 = h(f(B, D) \| C \| A)$
3. generate *ACK* message and send it to the *MS*.
{*ACK* message}
1. verify the *ACK* message.
2. generate three shared keys
$K_1 = h(A \| B \| C)$
$K_2 = h(B \| A \| f(C, D))$
$K_3 = h(f(B, D) \| C \| A)$

Fig. 3. Negotiation of three shared keys.

B and C denote the privacy information (i.e., identity) of two parties, respectively. The notation A represents the secret generated during the key negotiation process. To resist known attacks and provide security features such as perfect forward secrecy, the secret A usually contains two high entropy random integers that are chosen freely by the two communication parties respectively in each run. To ensure the three shared keys are unrelated, the structure of each shared keys need to be changed. According to the above analysis, the three shared keys in our scheme are designed as follows.

$$K_1 = h(A \| B \| C) \tag{4}$$

$$K_2 = h(B \| A \| f(C, D)) \tag{5}$$

$$K_3 = h(f(B, D) \| C \| A) \tag{6}$$

Where $f(\cdot)$ can be a computationally invertible function or a simple operation such as XOR, and the D denotes the secret information only can be obtained by the communication parts using the transmitted messages. This secret information is used to authenticate the identity of the communication parties. Since the three shared keys are designed with different constructions, the linkages among them are broken. Furthermore, this design ensures that if K_1 is a secure shared key, then the shared keys K_2 and K_3 are also secure.

After the keys are generated, they will be used in subsequent processes. In the embedding and retrieval process, the shared key K_1 is adopted to encrypt/decrypt the patients' sensitive information, and the other two shared keys K_2 and K_3 are used to generate the embedding templates.

B. Embedding Process

In this process, the original signal is first decomposed by the Fast Walsh-Hadamard Transform (FWHT) to obtain a set of coefficients. Then, parts of the coefficients are reshaped to construct a multidimensional space. Finally, encrypted secret bits are embedded in the constructed space.

1) ECG signal processing

Compared with other transforms used in signal-processing fields, the fast Walsh-Hadamard transform requires less computation and energy consumption since it only contains addition and subtraction operations. Accordingly, it has better real-time performance and is suitable for the transmission of biological signals [27]. The above advantages of FWHT motivate us to apply it to ECG signal processing. Therefore, we explore the possibility of employing the FWHT technique to construct a secure space for hiding secret information. Experiments have been performed on the original ECG signals, and we observed that the reconstruction of the ECG signal only depends on the low sequency values of the decomposed coefficients. That means a large percentage of coefficients can be modified without affecting the overall visual quality of the reconstructed signal.

Fig. 4 shows an example of ECG signals that are reconstructed using the low sequency values of coefficients. The low sequency values contain most of the ECG signal energy but account for less than approximately 20% of the total ECG signal. Conversely, the high sequency values of coefficients contain less energy so that a certain amount of sensitive information can be embedded therein without affecting the visual quality after signal reconstruction. These interesting observations inspire us to adopt FWHT and use the high sequency values of coefficients to construct a multidimensional space that can embed more secret information effectively.

2) Encryption for secret information

To enhance security, the secret information needs to be encrypted before it is embedded in the multidimensional space. The secret information can be the patients' identity information (name, ID, address, geometric location, etc.), unique biological information (fingerprint signature, iris images, etc.), and diagnostic results (body temperature, blood pressure, blood glucose level, etc.) [11, 28].

In this step, we use the negotiated key K_1 from Section IV-A to encrypt the above secret information. Legitimate entities in the e-health networks share the negotiated key K_1 and the coding method (e.g., ASCII) before transmission. As shown in Fig. 5, the patients' sensitive information such as his/her name is encrypted using a lightweight symmetric algorithm (e.g., AES) with K_1. Then the ciphertext is converted into bits for the next steganography process.

3) Construction of the multidimensional space

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

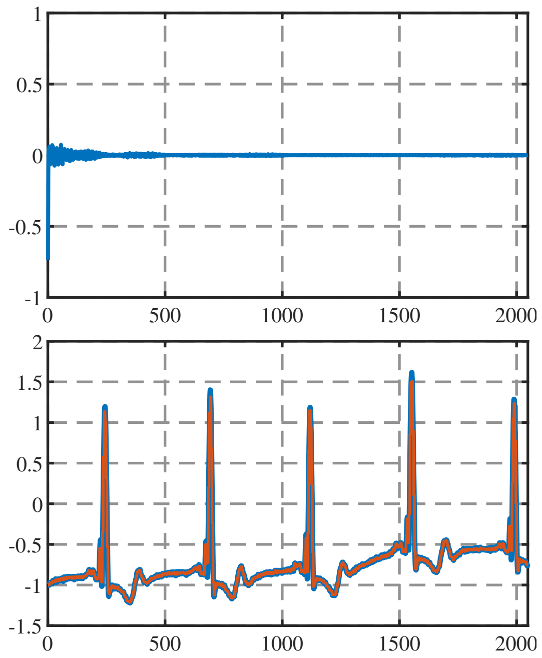


Fig. 4. Reconstructed signal (depicted in yellow) using just low sequency values of FWHT coefficients and the original signal (depicted in blue). Loss of peaks occurs.

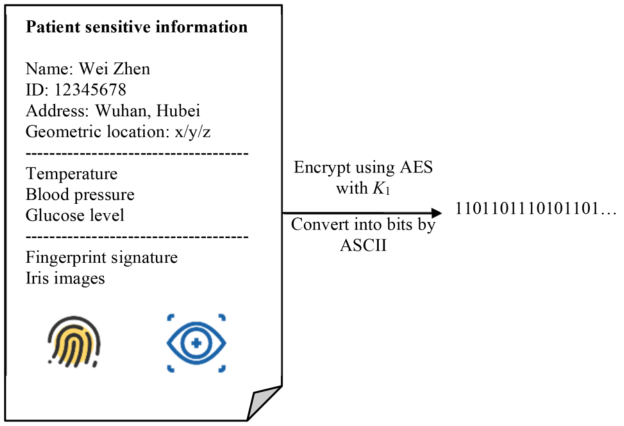


Fig. 5. The operation of encrypting and converting confidential information to bits before embedding process.

In the proposed steganography scheme, the high sequency values of the coefficients are used to construct the multidimensional space. These coefficients are shuffled and then reshaped to form several small cubes, which can be identical or different in terms of their shape. To enhance the embedding complexity, we arrange these small cubes to create a large one. The formation and usage of the constructed multidimensional space are fully illuminated by the following three procedures.

Coefficients shuffling: The values of the insignificant coefficients are expanded from a decimal form to a positive integral one by shifting and scaling operations, where the least significant bits can be replaced with the encrypted bits generated in the previous encryption step.

Formation of small cubes: The shuffled coefficients are separated into several sections, whose number is at least eight in order to constitute a cube-shaped 3-D space. After that, each section is reshaped to a small cube from 1-D to 3-D.

Formation of multidimensional space: The reshaped cubes are numbered in turn, and then they are randomly arranged as a large cube to form a multidimensional space.

Fig. 6 shows an example of how the multidimensional space is constructed. The number of low and high sequency values are 512, 1536 separately. For clarity, the number of sections we presume is eight, so each of eight small cubes contains 192 coefficients. The created cubes are adjusted to the same shapes ($8 \times 8 \times 3$). Finally, eight small cubes are reshaped to a $2 \times 2 \times 2$ multidimensional space.

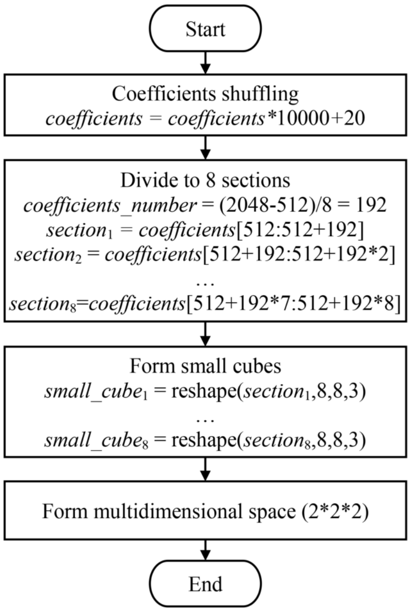
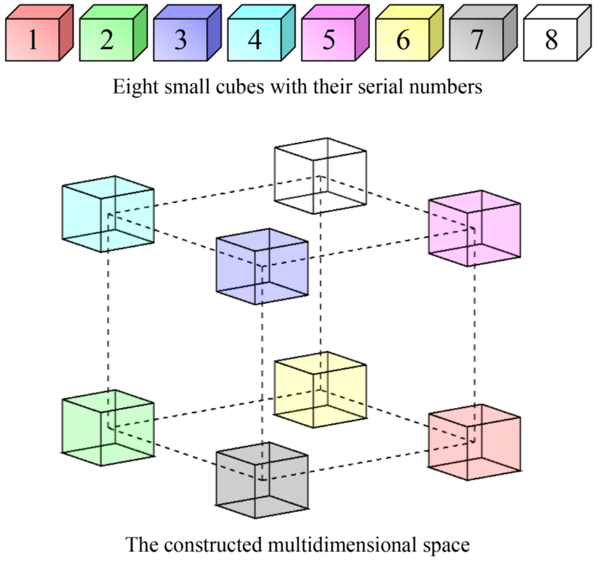

Start
Coefficients shuffling
$coefficients = coefficients$*10000+20
Divide to 8 sections
$coefficients\_number$ = (2048-512)/8 = 192
$section_1 = coefficients$[512:512+192]
$section_2 = coefficients$[512+192:512+192*2]
…
$section_8$=$coefficients$[512+192*7:512+192*8]
Form small cubes
$small\_cube_1$ = reshape($section_1$,8,8,3)
…
$small\_cube_8$ = reshape($section_8$,8,8,3)
Form multidimensional space (2*2*2)
End

Fig. 6. An example of the construction of the multidimensional space.

As shown in Fig. 7, eight cubes in different colors are numbered from one to eight, and they represent the small cubes. Then the eight small cubes are jointly assembled to establish a multidimensional space, as signified by the dashed lines. As a whole, the large cube consisting of eight small cubes forms a multidimensional space.

In the above steps, the serial number is used to determine different stego scales and rearrange the separated sections. The embedded bits in each cube (i.e., stego scale) varies according to its serial number by performing modulo operation. Presume the serial number is denoted by n, and the maximum stego scale is denoted by b. If n is divisible by b, then the coefficients of the corresponding cube are embedded with the lowest b bits; if not, the embedded bits of the corresponding cube is the remainder after division of n by b. As later analyzed in Section IV-D, cubes with different serial numbers are embedded with one to b encrypted bits, respectively, and b can be any integer from one to five. For example, the maximum embedding bits is three, and the serial number of the located cube is eight, then the calculated stego scale is two. Besides, the serial number in each cube facilitates the restoration of the cubes in their original order so that the modified coefficients can be

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.



Eight small cubes with their serial numbers

The constructed multidimensional space

Fig. 7. Construction of the multidimensional space composed of eight small cubes.

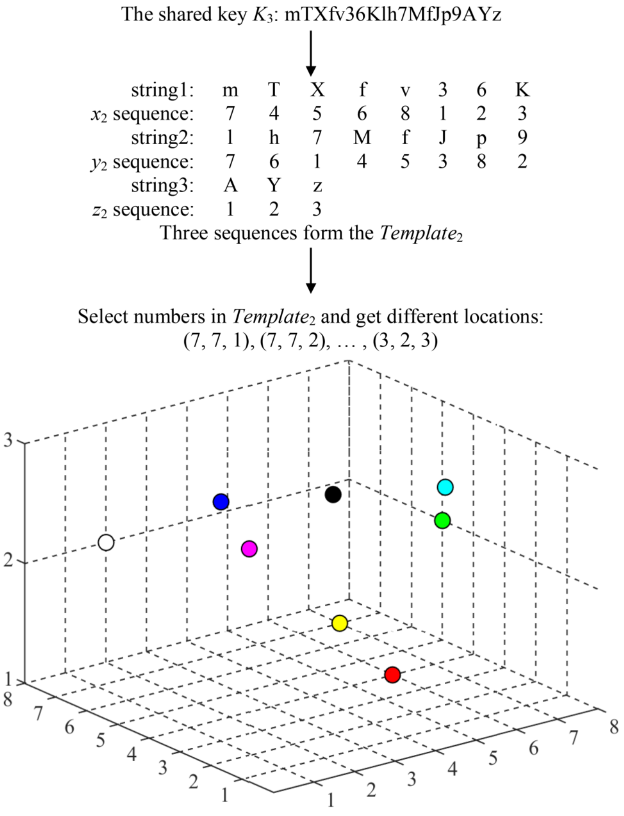
retransformed to the genuine signal by inverse FWHT in the reconstruction process.

The idea of dynamically changing the maximum embedding bits enhances the embedding complexity even with the same constructed multidimensional space. Compared with the related schemes where the stego scale is usually fixed in their embedding process, our method provides enough variability to ensure higher security. Therefore, it is infeasible for adversaries to retrieve the embedded bits accurately in our security scheme.

4) Embedding

After the construction of the multidimensional space, the encrypted bits will be embedded therein. The whole embedding procedure includes three steps: (a) locate one small cube in the large cube using $Template_1$, (b) locate one coefficient value in the certain small cube using $Template_2$, and (c) embed secret bits in the determined coefficient value. These steps will be performed repeatedly until all encrypted bits are embedded in the multidimensional space. In steps (a) and (b), $Template_1$ and $Template_2$ are two templates that are used to determine the locations in the constructed multidimensional space. Each template is formed by three sequences: x sequence, y sequence, and z sequence, which are generated by shared keys. By selecting numbers in these three sequences respectively, different locations can be found in the embedding space to hide the secret information. And such locations can be separately denoted by two ternary coordinates (x_1, y_1, z_1) and (x_2, y_2, z_2).

In our design, $Template_1$ and $Template_2$ are separately generated from the two shared keys K_2 and K_3 during steps (a) and (b) processes. Since both templates are constructed in the same way, we take the generation of $Template_2$ as an example to illustrate the whole location process. Firstly, three different character strings with different lengths are drawn from K_3, and the lengths of these strings are determined according to the three dimensions of the small cubes. Then, adopting one generated string, a sequence is constructed in the order of the characters' ASCII values. Note that the characters in one string of fixed length should be different from each other. By using the above method, three sequences are generated and then form the $Template_2$. After that, different numbers will be selected from $Template_2$ to generate the ternary coordinates (x_2, y_2, z_2), which is used to locate the coefficient values in one small cube. The above procedures are illustrated in Fig.8, and the dots in different colors represent the precisely located positions of coefficient values.


The shared key K_3: mTXfv36Klh7MfJp9AYz

string1:	m	T	X	f	v	3	6	K
x_2 sequence:	7	4	5	6	8	1	2	3
string2:	l	h	7	M	f	J	p	9
y_2 sequence:	7	6	1	4	5	3	8	2
string3:	A	Y	z					
z_2 sequence:	1	2	3					

Three sequences form the *Template*$_2$

Select numbers in *Template*$_2$ and get different locations: (7, 7, 1), (7, 7, 2), … , (3, 2, 3)

Fig. 8. Locating positions in a determined space using the templates.

The generations of $Template_1$ and $Template_2$ are just the same. With the help of these two templates, all the coefficient values in the corresponding small cube can be located. Then the secret bits can be embedded in the determined coefficient value. Repeat the above steps until all encrypted bits are embedded in the multidimensional space. And the whole embedding process is complete.

Here follow the specified procedures with an instance. With a 2048-bit sample, the 1536 bits of the high sequency values are equally divided into eight sections. After shuffling operations, the 192 bits of coefficients in each section are reshaped into small cubes so that eight identical cubes are obtained. Each small cube is numbered from one to eight and then arranged to form a large cube. The dimensions of the small cubes and the large cube are $8 \times 8 \times 3$ and $2 \times 2 \times 2$, respectively. Then, locate one small cube in position (x_1, y_1, z_1) of the large cube using $Template_1$, whose serial number is eight. Next, choose one coefficient value in position (x_2, y_2, z_2) of the determined small cube

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

using $Template_2$, select the maximum embedding bits to be three, and calculate the stego scale to be two. After that, the encrypted bits are embedded in the lowest three bits of the chosen coefficient value. Repeatedly, if one small cube's total coefficient values are all embedded with secret bits (576 bits in detail), another small cube with a different serial number will be adopted subsequently. Finally, the above processes are executed continually until all encrypted bits are embedded.

After the above embedding process is finished, the stego coefficients will be reconstructed to obtain the stego signal that will be later transmitted in the e-health networks safely. Since the visual difference between the stego signal and the genuine one can be ignored, the stego signal can be directly used in the diagnosis without getting the genuine signal via the steganography scheme. Furthermore, the negligible difference avoids the attention of adversaries and makes it impossible to distinguish the stego signals from the genuine ones.

C. Reconstruction and Retrieval

In this section, stego coefficients will first be retransformed by inverse FWHT to obtain the stego signal, which will be later transmitted to the authorized parties in the e-health networks. Finally, the receiver can precisely retrieve total hidden bits without any error.

1) Reconstruction of signal

This step explains the signal reconstruction process. Firstly, the multidimensional space is reshaped into an original vector format. Next, the multidimensional space is deconstructed into several small cubes, whose serial numbers are employed to arrange the sequence to the original order. Then, the small cubes are reshaped from 3-D to 1-D format using the Reshape function. In the end, the stego coefficients (80%) and the unmodified coefficients (20%) are spliced together as a whole to reconstruct the stego signal by performing the inverse FWHT. The reconstruction process of ECG signals is as fast as the decomposition process. In addition, the reconstructed ECG signals with hidden secrets are almost the same as the original ECG signals, which preserves high visual fidelity.

The entire embedding process (including signal processing, bits embedding, and signal reconstruction) is shown in Algorithm 1, and the retrieval process is simply its reverse.

2) Retrieval of embedded bits

To accurately extract and decrypt the hidden bits in the stego signal, the receiver should share some security messages in advance, which are the shared keys (K_1, K_2, and K_3), maximum embedding bits (i.e., the value of *b*), and coding method. These messages are shown in red in Fig. 9. Only legal users sharing these messages can retrieve the secret information and authenticate the sender's identity.

The extraction of the secret information is the inverse process of the embedding. Its total operations are almost the same as the embedding process, apart from extracting the least significant bits instead of replacing them. As shown in Fig. 9, after receiving the stego ECG signal, the receiver applies FWHT to obtain the high sequence coefficient part. Then, this part is adopted to establish an identical multidimensional space using the same construction methods in Section IV-B-3). The negotiated keys K_2 and K_3 are utilized to generate two templates for locating. Then the hidden information can be extracted from the least significant bits following the same steps in Section IV-B-4). At last, the retrieved secret bits are decrypted using the AES algorithm with key K_1, and then the decrypted messages are decoded to plaintext by ASCII.

Algorithm 1 The embedding algorithm

```
$ecg$: the host ECG signal
$secg$: the stego ECG signal
$coef$: coefficients generated by FWHT and only less significant part is modified
$k$: the key of a symmetric encryption algorithm (e.g., AES)
$m$: patient's sensitive information
$b$: the secret bits generated by $m$ as shown in Fig. 5
$bl$: the length of $b$
$bc$: the index of the current character in $b$
$n$: the number of small cubes (as shown in Fig. 6, the value is 8)
$x$: the index (serial number) of one small cube
$s$: the embedded bits per coefficient determined by $x$
$sm$: the maximum embedded bits per coefficient without visual distortion
$l$: the location set generated by selecting numbers in $Template_2$ (as shown in Fig. 8, the number of locations is 192)
$b \leftarrow ascii(f_e(k, m))$
$coef \leftarrow fwht(ecg)$
$coef \leftarrow coef + 20$
$coef \leftarrow coef \times 10000$
Reshape the coefficients to construct a multidimensional space as shown in Fig. 6 and Fig. 7
$bc \leftarrow 1$
for $i = 1 \rightarrow n$ do
    Select a small cube and get its index $x$
    if $mod(x, sm) == 0$ then
        $s \leftarrow sm$
    else
        $s \leftarrow mod(x, sm)$
    end if
    for $j \in l$ do
        $coef(j) \leftarrow bitset(coef(j), s, b(bc))$
        $bc \leftarrow bc + 1$
        if $bc > bl$ then
            break
        end if
    end for
end for
$coef \leftarrow coef/10000$
$coef \leftarrow coef - 20$
$secg \leftarrow ifwht(coef)$
```

V. Performance and Security Evaluation

To evaluate our proposed scheme, we will perform experiments for different categories of ECG signals, focusing on common security attributes (e.g., imperceptibility, embedding capacity / payload, and availability [28–31]). Computational

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSE.2021.3063174, IEEE Transactions on Network Science and Engineering

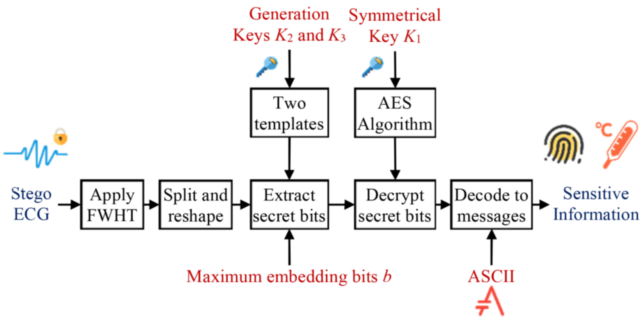


Fig. 9. The process of retrieval process with shared keys.

efficiency will also be analyzed to evaluate efficiency. Specifically, the proposed scheme was implemented on two different computers to simulate the communication of the control unit and the medical server. The control unit has an Inter(R) Core(TM) i5-3337U CPU with a clock speed of 1.80 GHz and 4 GB random-access memory (RAM), and the medical server has an Inter(R) Core(TM) i5-4210M CPU with a clock speed of 2.60 GHz and 8 GB RAM. The control unit and medical server are connected via the Internet at a bandwidth speed of 100 Mbps. The programming platform used is MATLAB R2019b.

The ECG experimental dataset adopted used is the MIT-BIH Arrhythmia dataset [32, 33], as well as three other popular databases as shown in Table II. In general, ECG signals can be broadly separated into five categories [34–36]. A limited number of beats containing one or more types make up one segment, and the majority type in that segment determines the signal category. Five types of cardiac beats are listed, namely: normal beat (N), left bundle branch block beat (L), right bundle branch block beat(R), aberrated atrial premature beat (A), and premature ventricular contraction (V) [37–39]. The definite type of each beat is manually annotated, which is stored in the annotation file of a segment [32]. From the file, we can determine a segment specific category of a fixed time or length.

In our experiments, selected leads were used in one type of ECG signal, as this is composite. The time of a segment was fixed to 10 seconds, which contains a length of 3600 bits. To meet the input requirements of the fast Walsh-Hadamard transform, we picked the first 2048 bits of different segments as the samples. The first 512 bits were employed as the low sequence part to remain unmodified, which accounts for less than 25% of the total coefficients. The last 1536 bits were reshaped to construct the proposed multidimensional space to hide the secret information of the patients.

The experiments were carried out by embedding and retrieving the patient privacy information. For example, the sender can be the patient or a doctor who wishes to hide some secret messages via the ECG signals through the public channel. The receiver is usually the corresponding medical institution tasked with recording, analysis, and/or diagnosis. Our scheme can prevent unauthorized third parties from accessing any useful patient-related information, and provide easy verification of the senders for legitimate users such as medical institutions. Different categories of ECG signals were tested with different sizes such as 512, 1024, 2048, 4096, and all less-significant coefficient values were used to embed the secret bits. Since the results were consistent for all tests, we chose a segment of No. 124 ECG signal to act as an example. As shown in Fig. 10, it is difficult to distinguish the stego ECG signal from the genuine one, indicating that the embedded secret bits have minimal influence on visual effect using our proposed scheme. Therefore, our proposed approach allows the use of stego signals to facilitate medical diagnosis.

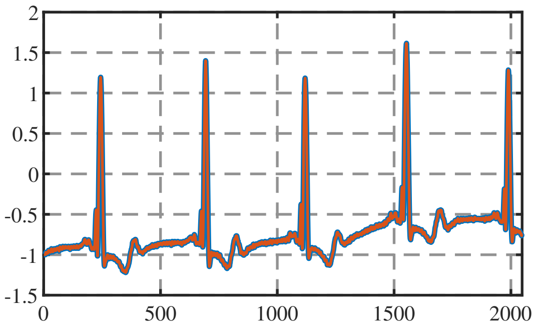


Fig. 10. Stego ECG sample (depicted in blue) is almost the same as the genuine one (depicted in yellow).

A. Imperceptibility

Operations on ECG signals may cause a certain degree of distortion that will attract the attention of adversaries. Therefore, the stego signals should be free of noticeable visual modifications to provide high imperceptibility. To measure the quantitative visual impact of the proposed steganography method, PRD and PSNR, as two statistical indicators, were adopted to analyze the exact deformation [28].

PRD (Percentage Residual Difference) is employed to quantify the difference between the genuine signal and the stego one [28], which is also known as the distortion rate brought by steganography operations. The calculation formula is shown in

$$PRD = \sqrt{\frac{\sum_{i=1}^{N}(X_i - Y_i)^2}{\sum_{i=1}^{N} {X_i}^2}} \times 100\% \tag{7}$$

Where X_i and Y_i represent the genuine signal and the stego one, respectively, and N represents their length. The magnitude of the PRD value indicates the extent to which the embedded secret information affects the genuine signal. In general, an amount of less than 1% means that the original signal is less affected.

The normalized PRD (PRDN) is also calculated, and the formula is shown in

$$PRDN = \sqrt{\frac{\sum_{i=1}^{N}(X_i - Y_i)^2}{\sum_{i=1}^{N} (X_i - S_{mean})^2}} \times 100\% \tag{8}$$

Where S_{mean} denotes the mean of signal value.

PSNR (Peak Signal-to-Noise Ratio) values quantify the similarity between the genuine signal and the stego one [28].

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSE.2021.3063174, IEEE Transactions on Network Science and Engineering

Equation (8) defines the mathematical representation of the PSNR.

$$PSNR(dB) = 20\lg\frac{max(X_c)}{\frac{1}{N}\sum_{n=1}^{N}(X_c - X_w)^2} \tag{9}$$

Here, the genuine signal and the stego one are denoted by X_c and X_w, respectively, and N represents their length. The numerator is the peak value of the genuine signal. The higher the PSNR value is, the better the visual fidelity performs.

To obtain impartial results, in our experiments, we selected several categories of ECG samples in the database mentioned above, and all selected segments were embedded with secret bits of the same length. In addition, the stego scale was fixed to the lowest (1 bit) in each less-significant coefficient. Table I shows the results of seven ECG segments that we selected. As shown in Table I, the PRD values are all less than 1%, and the corresponding PSNR values are all large enough (i.e., close to 100) for different categories of ECG samples.

TABLE I
EXPERIMENTAL RESULTS FOR DIFFERENT CATEGORIES OF ECG IN MIT-BIH DATABASE

Sample No.	Category	PRD(%)	PSNR(dB)
100	N	0.00629	92.8583
101	N	0.00613	92.8213
109	L	0.00352	92.9843
111	L	0.00922	93.1819
118	R	0.00218	92.7237
124	R	0.00274	92.8789
208	V	0.00438	92.7755

Table II summarizes the comparative performance of the proposed algorithms on three other datasets.

The result indicates that the values of PRD and PSNR in our proposed scheme are all in the appropriate range mentioned above, which meet the imperceptibility requirement. Therefore, the proposed scheme has minimal impact on the genuine signal while achieving high visual fidelity.

B. Embedding Capacity

Embedding capacity is defined to measure the actual number of secret bits that can be embedded in a certain segment of ECG signals. Its value should be as large as possible while keeping the visual fidelity of the stego signal [28, 40, 41]. To calculate the exact number of embedded bits in our scheme, a mathematical equation is used to calculate the total volume as

$$v = R \times C \times D \times n \times b \tag{10}$$

TABLE II
EXPERIMENTS BASED ON VARIOUS DATABASES

Dataset	PRD(%)	PSNR(dB)
MIT-DB	0.0078	91.97
CU-VT	0.0053	98.58
BIDMC-CHF	0.0077	91.30
PTB	0.0157	81.78

Where v represents the embedding capacity, R, C, and D denote the length, width, and height of the reshaped small cube, n represents the number of small cubes in the multidimensional space, and b represents the number of embeddable bits per value.

The embeddable bits at the coefficient level are also known as the stego scale. According to the previous sections, the maximum embeddable bits in one coefficient value are limited. Therefore, to maximize the embedding capacity without a noticeable impact on the host signal, several experiments have been done to obtain an optimal upper value of the stego scale, which determines the exact number of the coefficient value's lowest bits to be replaced by the secret bits.

In our experiment, one fixed signal sample No. 124 was chosen with a length of 256 bits, and the stego scale varied from one to seven, to which this length of secret bits was adjusted. From Table III, we can conclude that up to five of the least significant bits can be embedded per coefficient value, and the distortion of the stego signal is still within an acceptable range. Therefore, the parameter b in Equation (6) can vary from one to five in integer.

TABLE III
PRD VALUES OF EMBEDDING DIFFERENT BITS

Stego scale	Bits embedded	PRD(%)
1 bit	192	0.00343
2 bits	384	0.00720
3 bits	576	0.01363
4 bits	768	0.02693
5 bits	960	0.05302
6 bits	1152	0.12
7 bits	1344	0.22

For clarity, suppose a biological ECG sample of 10-s length was applied to our steganography scheme. The first 2048 bits of values were selected for implementing FWHT, where the dimension of the eight identical reshaped small cubes is 8*8*3. It was presumed that each coefficient value could be replaced by five secret bits. Then the embedding capacity was 7680, which means around 7680 bits of patients' privacy information could be embedded in the sample.

C. Availability

Availability consists of two parts: clinical validation and lossless retrieval. For clinical validation, the diagnosis should be able to perform on stego covers directly without extracting the hide messages via the steganography scheme. On the other hand, the BER is introduced to evaluate lossless retrieval [28].

Our previous analysis of imperceptibility explains that the stego signals are almost the same as the genuine signals. That means doctors can directly use the stego ECG signals for diagnosis, while authorized entities can retrieve patient privacy information from the stego signals. Furthermore, the stego ECG signals do not affect the accuracy of the classification of arrhythmia. These advantages ensure clinical validation.

To evaluate retrieval reliability of the retrieved secret information, BER (Bit Error Ratio) was employed in our scheme to calculate the percentage of the erroneous bit number in the

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

retrieved bits to the sent total bit number [28]. BER values can well indicate the accuracy of the signal transmission within a specified time. In general, the more data is lost, the more BER value increases. The calculation formula of BER is shown in (10).

$$BER = \frac{error\ bits\ received}{total\ bits\ sent} \times 100\% \qquad (11)$$

When BER is used to reflect the reliability, the interference of the communication channel should be taken into account. Generally, BER value is only meaningful in the lossless channel.

From Table I, the BER values are all zero, meaning that the extracted secret bits are error-free. Therefore, in our design, the secret information can be restored after decrypting and decoding operations.

D. Security Analysis

In this part, we analyzed the security of our proposed scheme by discussing the complexity of illegitimate retrieval with/without the proposed steganography algorithm.

1) illegitimate retrieval without steganography algorithm

Suppose that an adversary has the following knowledge: (a) the employed signal-processing algorithm is FWHT, (b) the transmitted stego signal. Then he/she try to retrieve the hidden secret bits from the insignificant part of the transformed coefficients. Consider the following embedding situations: (a) the length of the hidden secret bits is as long as that of the insignificant coefficient values, (b) the lowest one bit of each insignificant value is replaced by one secret bit. In this case, if an adversary obtains a transmitted stego signal with a length of 2048 bits and the insignificant part is 25% (1536 bits), he/she needs to try $1536! \approx 1.63 \times 10^{4229}$ times to get the secret bits. Since the secret bits that can be embedded in every insignificant value are varied from zero to five, our proposed scheme is much more complex than the presumed situations. Therefore, this exhaustive search is not feasible in practice.

2) illegitimate retrieval with steganography algorithm

As previously introduced in Section IV-B-4), two shared security keys K_2 and K_3 are used in our scheme. Suppose that an adversary that has obtained the transmitted stego signal (a) can directly use our scheme without knowing its principle, or (b) cannot use it but know its principle. In case (a), the adversary will launch an exhaustive key search in a certain keyspace to obtain the shared keys. When the keyspace is ASCII characters, and the lengths of K_2 and K_3 are 6 and 19 respectively, the adversary needs to try $6^{128} + 19^{128} \approx 4.79 \times 10^{163}$ times to obtain the right secret bits. So, it is highly infeasible for adversaries to obtain the secret bits through correctly guessing the two shared keys. In case (b), for the adversary, since the selected parts of all insignificant coefficients that are used to form the large cube cannot be determined, and the number and the shape of all small cubes also cannot be determined in the large cube, he/she has no ability to extract the secret bits by exhaustive searching in such uncertain space.

According to the above analysis, it is highly impractical for adversaries to retrieve the hidden secret bits from stego ECG signals, and the proposed scheme can prevent illegitimate retrieval effectively.

Furthermore, even if the adversary has retrieved the secret bits, without the knowledge of the shared key K_1 and the coding method, he/she still cannot obtain the patients' privacy information. Therefore, the proposed scheme can provide high security in e-health environments.

VI. Discussion

A. Comparative Summary

Here, we will present the performance of our proposed scheme with those of Ibaida and Khalil [12] and Neetika et al. [14], since all three schemes use biological ECG signals as the transmitted carriers to hide private information during steganography. The performance metrics considered are the statistical results, embedding capacity, runtime, overhead, complexity and security. The performance evaluations were carried out using the No. 101 sample of MIT-BIH database, and the duration was 10s and 1min.

As shown in Table IV, the PRD and PRDN values of our scheme (0.0078% and 0.01% for 10s, 0.0241% and 0.04% for 1min) are lower than those in [12] (0.0582% and 0.11% for 10s, 0.0617% and 0.10% for 1min) and [14] (0.0761% and 0.13% for 10s, 0.0823% and 0.17% for 1min). In addition, one can observe that the PSNR value of our scheme is 91.97dB for 10s and 85.46dB for 1min, which is higher than that those of [12] (76.17dB for 10s and 77.30dB for 1min) and [14] (77.56dB for 10s and 75.91dB for 1min). These results imply that our scheme outperforms the other two schemes [12, 14], in terms of imperceptibility. The BER value of all three schemes is 0%, which implies reliability of the extracted bits. In summary, our scheme outperforms the other two schemes with respect to the statistical results.

Furthermore, when using ECG signals of the same duration, our scheme provides more embedding capacity (13500 for 10s and 81000 for 1min) than that of [14] that only uses the non-QRS regions of ECG signals (2400 for 10s and 17266 for 1min), and the embedded bits are slightly lower than that of [12] (19250 for 10s and 118125 for 1min). By utilizing FWHT, the runtime of our scheme (0.0608s for 10s and 0.1219s for 1min) is less than that of [12] that employs wavelet transforms (0.4589s for 10s and 2.8354s for 1min). We also observe that the scheme of [14] has the longest runtime (2.8307s for 10s, 16.4263s for 1min) because finding non-QRS complex incurs significantly more time than the other two schemes. The overhead of our scheme (14.12KB for 10s, 84.45KB for 1min) is lower than those of [12] (30.07KB for 10s and 100.30KB for 1min) and [14] (219.81KB for 10s, 347.19KB for 1min). In other words, our scheme requires less storage space and is more suitable for resource-limited environments (e.g., those involving medical IoT devices).

The embedding complexity of our scheme and the scheme of [12] is $O(kl \times wl)$, where kl is the length of security key, and wl is the length of embedded bits. The embedding complexity of the scheme of [14] is $O(l)$, where l is the length of generated chaotic sequence. Therefore, the embedding complexity of our scheme and the scheme of [12] is

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSE.2021.3063174, IEEE Transactions on Network Science and Engineering

TABLE IV
PERFORMANCE OF OUR PROPOSED SCHEME AND TWO OTHER SCHEMES FOR ECG SIGNALS ON THE MIT-BIH DATASET: A COMPARATIVE SUMMARY

Duration	Scheme	PRD(%)	PRDN(%)	PSNR(dB)	BER(%)	Bits embedded	Runtime(s)	Overhead(KB)	Embedding complexity	Dynamic key
10s	[12]	0.0582	0.11	76.17	0	19250	0.4589	30.07	$O(kl \times wl)$	N
	[14]	0.0761	0.13	77.56	0	2400	2.8307	219.81	$O(l)$	N
	Ours	0.0078	0.01	91.97	0	13500	0.0608	14.12	$O(kl \times wl)$	Y
1min	[12]	0.0617	0.10	77.30	0	118125	2.8354	100.30	/	/
	[14]	0.0823	0.17	75.91	0	17266	16.4263	347.19	/	/
	Ours	0.0241	0.04	85.46	0	81000	0.1219	84.45	/	/

lower than that of [14]. In FWHT, the input signal is divided into two parts of the same length, and in each loop, only addition and subtraction operations are used with the factor values of +1 and -1. Thus, no division or multiply is used in FWHT [27, 42]. In wavelet transform, a coefficient tree is built with a set number of layers. In each layer, two sets of coefficients (approximation coefficients and detail coefficients) are sent to convolve with a low-pass filter and a high-pass filter, respectively. In this process, these coefficients (stored as *double* type) will be operated using multiplication operations [43, 44]. Since only additions and subtractions are adopted in the FWHT mathematical model [27, 42], FWHT incurs less computation, memory, and power in comparison to wavelet transform. Therefore, our scheme is more efficient than the wavelet-based scheme [12].

In terms of security, both schemes presented in [12, 14] do not provide a dynamic key for users. Consequently, these schemes suffer from security issues associated with the use of static keys. On the contrary, in our design, dynamic keys are adopted in each run to provide robustness, which enhances the security of the steganography scheme.

In addition, we performed several experiments in which the section number is varied. From the experiment findings, one can observe that the runtime increases with the section number. For example, when the section number is 8, the runtime calculated is 0.06081s. When the number reaches 16 and 24, the runtime also increases to 0.06563s and 0.06714s, respectively. Furthermore, based on our security analysis, when the number increases, so does the security. In other words, we can adjust the section number to achieve the required balance between security and performance, where a large section number can be chosen to enhance the security and a small section number can be used to achieve low consumption.

Therefore, our scheme meets the requirements of real-time transmission of ECG signals, and it is more suitable for the e-health networks compared to the schemes of [12, 14].

B. Potential Application Scenarios

E-health services have been increasingly promoted on a global scale, and particularly at the time of this research due to COVID-19. Since such services rely on e-health networks, it is important to protect real-time submission of private information such as physiological data (heart rate, blood pressure, blood sugar, etc.) between the users and other devices / systems (e.g., servers). By using our proposed SIP scheme, users (e.g., patients) can send their identity information and physiological data collected by medical or consumer IoT devices to the specified server with our ECG-based multidimensional steganography method, from remote locations (e.g., homes or workplaces). The generated Electronic Medical Record (EMR) can be accessed by patients, family members, and doctors using the negotiated dynamic keys. Even during emergency (e.g., the patient suffers a stroke or has a fall), the medical IoT device can immediately send the stego ECG data to the server, from which the medical staff can extract relevant information (e.g., patient identity and current status) to facilitate decision-making (e.g., sending an alert to the nearest medical resource).

Fig. 11 shows an application scenario in e-health networks. For example, we assume that Alice is sick at home and her condition is being monitored by various medical IoT devices in real-time. Using our proposed SIP scheme, her physiological data will be hidden in the ECG signal at the set time interval, and then sent to the specified server. The server first authenticates Alice's identity by extracting the hidden identity information, then finds her EMR, and stores her physiological data in it. As a result, her family member, say Bob, can monitor Alice's health condition on his mobile device (via an application). In addition, her physician can also monitor her health status and dispatch appropriate medical resources, as needed (e.g., based on an analysis of the physiological data in her EMR). Considering the open nature of the communication and resource limitations of e-health networks and devices, our secure transmission scheme minimizes the risks of open channel attacks (e.g., eavesdropping, and data tampering). At the same time, it does not require additional storage space.

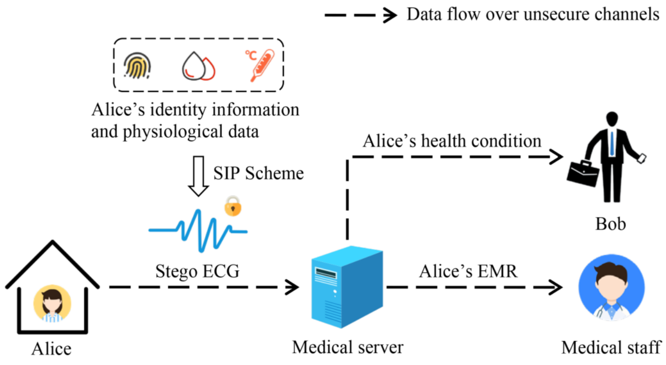


Fig. 11. An application scenario in e-health networks.

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSE.2021.3063174, IEEE Transactions on Network Science and Engineering

VII. Conclusion

In this paper, we proposed a steganography-based scheme to achieve privacy protection in e-health networks by dynamically embedding encrypted data in the transmitted biological signals at the bit level. In order to enhance embedding complexity while providing sufficient embedding capacity, a multidimensional space is constructed using the less-significant coefficients that are decomposed by a fast signal-processing algorithm named FWHT. In addition, three shared keys are adopted in our design to help achieve secure embedding. One shared key is used to encrypt patients' personal information into secret bits, and two other shared keys are employed to generate two different templates that help to locate the embedding coefficient values in the constructed space. For different categories of ECG signals, the performance of the proposed scheme is assessed by various statistical measures, such as PRD, PSNR, and BER, whose results indicate that our scheme achieves high imperceptibility (PRD less than 1%) and provides retrieval reliability (BER=0). Furthermore, the security analysis demonstrates that illegitimate retrieval in our design is infeasible. Therefore, the proposed scheme is a successful steganography scheme for e-health environments.

Acknowledgment

The research was financially supported by National Natural Science Foundation of China (No.61303237, No.61972366), the Open Research Project of the Hubei Key Laboratory of Intelligent Geo-Information Processing (No. KLIGIP-2019B09), the Foundation of Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences (No. KFKT2019-003), the Foundation of Guangxi Key Laboratory of Cryptography and Information Security (No. GCIS201913), and the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (No. 2018BDKFJJ009, No. 2019BDKFJJ003, No. 2019BDKFJJ011). K.-K. R. Choo was supported only by the Cloud Technology Endowed Professorship.

References

[1] B. Liu, J. Li, C. Chen, W. Tan, Q. Chen, and M. Zhou, "Efficient motif discovery for large-scale time series in healthcare," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 3, pp. 583–590, 2015.

[2] F. Sufi, Q. Fang, I. Khalil, and S. S. Mahmoud, "Novel methods of faster cardiovascular diagnosis in wireless telecardiology," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 537–552, 2009.

[3] Y. Sang, H. Shen, Y. Tan, and N. Xiong, "Efficient protocols for privacy preserving matching against distributed datasets," in *International Conference on Information and Communications Security*. Springer, 2006, pp. 210–227.

[4] X. Luo, J. Sun, Z. Wang, S. Li, and M. Shang, "Symmetric and nonnegative latent factor models for undirected, high-dimensional, and sparse networks in industrial applications," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3098–3107, 2017.

[5] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Systems*, vol. 21, no. 1, pp. 49–60, 2015.

[6] Y. Liu, M. Ma, X. Liu, N. Xiong, A. Liu, and Y. Zhu, "Design and analysis of probing route to defense sinkhole attacks for internet of things security," *IEEE Transactions on Network Science and Engineering*, 2018.

[7] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in internet of things (iot) using cryptography and steganography techniques," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 73–80, 2019.

[8] S. Balu, C. N. K. Babu, and K. Amudha, "Secure and efficient data transmission by video steganography in medical imaging system," *Cluster Computing*, vol. 22, no. 2, pp. 4057–4063, 2019.

[9] S. Devi, M. N. Sahoo, K. Muhammad, W. Ding, and S. Bakshi, "Hiding medical information in brain mr images without affecting accuracy of classifying pathological brain," *Future Generation Computer Systems*, vol. 99, pp. 235–246, 2019.

[10] S. K. Mukhopadhyay, M. O. Ahmad, and M. Swamy, "Compression of steganographed ppg signal with guaranteed reconstruction quality based on optimum truncation of singular values and ascii character encoding," *IEEE Transactions on Biomedical Engineering*, vol. 66, no. 7, pp. 2081–2090, 2018.

[11] A. Abuadbba and I. Khalil, "Walsh–hadamard-based 3-d steganography for protecting sensitive information in point-of-care," *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 9, pp. 2186–2195, 2016.

[12] A. Ibaida and I. Khalil, "Wavelet-based ecg steganography for protecting patient confidential information in point-of-care systems," *IEEE Transactions on biomedical engineering*, vol. 60, no. 12, pp. 3322–3330, 2013.

[13] S. E. Jero, P. Ramu, and S. Ramakrishnan, "Discrete wavelet transform and singular value decomposition based ecg steganography for secured patient information transmission," *Journal of medical systems*, vol. 38, no. 10, p. 132, 2014.

[14] N. Soni, I. Saini, and B. Singh, "A morphologically robust chaotic map based approach to embed patient's confidential data securely in non-qrs regions of ecg signal," *Australasian Physical & Engineering Sciences in Medicine*, vol. 42, no. 1, pp. 111–135, 2019.

[15] Y. Wang, W. Zhang, W. Li, X. Yu, and N. Yu, "Non-additive cost functions for color image steganography based on inter-channel correlations and differences," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2081–2095, 2020.

[16] X. Liao, Y. Yu, B. Li, Z. Li, and Z. Qin, "A new payload partition strategy in color image steganography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 3, pp. 685–696, 2019.

[17] J. Wu, B. Chen, W. Luo, and Y. Fang, "Audio steganography based on iterative adversarial attacks against con-

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSE.2021.3063174, IEEE Transactions on Network Science and Engineering

volutional neural networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2282–2294, 2020.

[18] W. Lu, L. Li, Y. He, J. Wei, and N. N. Xiong, "Rfps: A robust feature points detection of audio watermarking for against desynchronization attacks in cyber security," *IEEE Access*, vol. 8, pp. 63 643–63 653, 2020.

[19] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in internet of things (iot) using cryptography and steganography techniques," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 73–80, 2020.

[20] Z. Wan, N. Xiong, N. Ghani, A. V. Vasilakos, and L. Zhou, "Adaptive unequal protection for wireless video transmission over ieee 802.11 e networks," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 541–571, 2014.

[21] H. F. Harmuth, "Applications of walsh functions in communications," *IEEE spectrum*, vol. 6, no. 11, pp. 82–91, 1969.

[22] Y. A. Geadah and M. Corinthios, "Natural, dyadic, and sequency order algorithms and processors for the walsh-hadamard transform," *IEEE Transactions on Computers*, vol. C-26, no. 5, pp. 435–442, 1977.

[23] Q. Do, B. Martini, and K. R. Choo, "The role of the adversary model in applied security research," *Computers & Security*, vol. 81, pp. 156–181, 2019.

[24] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[25] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1900–1910, 2016.

[26] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended chebyshev chaotic maps," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4815–4828, 2018.

[27] B. J. Fino and V. R. Algazi, "Unified matrix treatment of the fast walsh-hadamard transform," *IEEE Transactions on Computers*, vol. C-25, no. 11, pp. 1142–1146, 1976.

[28] H. Sajedi, "Applications of data hiding techniques in medical and healthcare systems: a survey," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 7, no. 1, p. 6, 2018.

[29] C.-C. Lai and C.-C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Transactions on instrumentation and measurement*, vol. 59, no. 11, pp. 3060–3063, 2010.

[30] S. D. Lin and C.-F. Chen, "A robust dct-based watermarking for copyright protection," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 415–421, 2000.

[31] X. You, L. Du, Y.-m. Cheung, and Q. Chen, "A blind watermarking scheme using new nontensor product wavelet filter banks," *IEEE Transactions on Image Processing*, vol. 19, no. 12, pp. 3271–3284, 2010.

[32] G. B. Moody and R. G. Mark, "The impact of the mit-bih arrhythmia database," *IEEE Engineering in Medicine and Biology Magazine*, vol. 20, no. 3, pp. 45–50, 2001.

[33] A. L. Goldberger, L. A. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, and H. E. Stanley, "Physiobank, physiotoolkit, and physionet: components of a new research resource for complex physiologic signals," *circulation*, vol. 101, no. 23, pp. e215–e220, 2000.

[34] P. De Chazal, M. O'Dwyer, and R. B. Reilly, "Automatic classification of heartbeats using ecg morphology and heartbeat interval features," *IEEE transactions on biomedical engineering*, vol. 51, no. 7, pp. 1196–1206, 2004.

[35] B. Hou, J. Yang, P. Wang, and R. Yan, "Lstm-based auto-encoder model for ecg arrhythmias classification," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 4, pp. 1232–1240, 2019.

[36] J. Shi, I. Alikhani, X. Li, Z. Yu, T. Seppänen, and G. Zhao, "Atrial fibrillation detection from face videos by fusing subtle variations," *IEEE Transactions on Circuits and Systems for Video Technology*, 2019.

[37] B. Pourbabaee, M. J. Roshtkhari, and K. Khorasani, "Deep convolutional neural networks and learning ecg features for screening paroxysmal atrial fibrillation patients," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 12, pp. 2095–2104, 2018.

[38] S. Kiranyaz, T. Ince, and M. Gabbouj, "Real-time patient-specific ecg classification by 1-d convolutional neural networks," *IEEE Transactions on Biomedical Engineering*, vol. 63, no. 3, pp. 664–675, 2015.

[39] S. Raj and K. C. Ray, "Ecg signal analysis using dct-based dost and pso optimized svm," *IEEE Transactions on instrumentation and measurement*, vol. 66, no. 3, pp. 470–478, 2017.

[40] J. Tian, "Reversible data embedding using a difference expansion," *IEEE transactions on circuits and systems for video technology*, vol. 13, no. 8, pp. 890–896, 2003.

[41] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[42] K. G. Beauchamp, *Applications of Walsh and related functions: with an introduction to sequency theory*. Academic press, 1984.

[43] S. G. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," *IEEE transactions on pattern analysis and machine intelligence*, vol. 11, no. 7, pp. 674–693, 1989.

[44] Y. Meyer, *Wavelets and Operators: Volume 1*. Cambridge university press, 1992, no. 37.

2327-4697 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Cape Town. Downloaded on May 20,2021 at 00:21:15 UTC from IEEE Xplore. Restrictions apply.