Packet Watermarking With ECG Biological Feature

Kuo-Kun Tseng[1], Xialong He[1], Xiaoxiao An[1], Chin-Chen Chang[2], Chao Wang[1], Xiangmin Guo[3]
(Corresponding author: Chin-Chen Chang)
School of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), China[1]
Department of Information Engineering and Computer Science, Feng Chia University, Taiwan[2]
School of Architecture, Harbin Institute of Technology (Shenzhen), China[3]
(Email: alan3c@gmail.com)
(Received Feb. 7, 2018; Revised and Accepted Oct. 18, 2018; First Online Sept. 21, 2019)

Abstract

In this paper we proposed a novel security authentication mechanism, which is a secure authentication mechanism for network transmission with an ECG biological feature. The theory of this authentication mechanism can be applied within various network identification and authentication systems. In addition, the algorithm needs to strengthen the safety and performance for watermarking. In addition, experimentation on the packet watermarking of ECG is conducted. The criteria has two parameters, one is the SNR (signal-to-noise ratio) and the other is BER, to evaluate the overall performance. Not only that, we have also considered noise attack. According to our obtained results, our algorithm has proven to be robust, and it thus worth considering in the application.

Keywords: Authentication; Biological Feature; ECG Signal; Packet Watermarking; Secure Transmission

1 Introduction

The emergence of communication networks has made enormous changes to people's lives. The network has enabled the communication between people to become more concise, has greatly improved the quality of human life, and sped up the process of social development. But it also carries a variety of risk [14]. Nowadays, all over the world, all aspects of the military, economy, society, culture and so on, are increasingly dependent on computer networks. The dependence on computer networks of human society has achieved an unprecedented record [4]. However, at the same time, the scale of attacks and threats to computer networks are also unprecedented. Many kinds of attack continually emerge, which can sometimes quickly cause large-scale network debacles. For today's society, the impact is definitely not less than a natural disaster, and may even be worse than. Therefore the protection of network security is imperative. The threats to networks may be from computer virus, worm and hacker attacks. These security problems are commonly introduced due to negligence and careless management and cause a large adverse impact. For example, hosting on an exposed environment, supervision of staff not being strict and so on, also gives attackers attacking space.

Therefore a more powerful mechanism to identify authorized data or users is essential. In this paper a new kind of the network authentication technology with transmission watermarking is proposed. We hope that the use of the personal ECG characteristic to assist with network transmission, and then providing a feature sequence as a watermark will protect the transmission process. The watermark operation is on the transmitting end, and a de-watermark operation is at the receiving end. Through the negotiation of the two parties we can confirm the security of the network transmission. Currently, we propose a security authentication mechanism based on the packet size with the ECG feature to achieve a transmission security authentication mechanism. In this research we also examine the feasibility and security of our proposed approach.

The structure of the paper is as follows: In the second section the applications of this mechanism in real life are firstly proposed. Of course this is only a hypothesis; and the application of secure transmission is very broad and not just limited to this hypothesis.

In the third section, we introduce relevant studies, especially highlighting research on watermarks. The proposed algorithm belongs to a new type of secure transmission.

In the fourth part we focus on the relevant content, as well as the algorithm, including the network transmission principle, ECG data acquisition methods and sources, and the principle of digital watermarking. Of course, the most important part is the changes that apply to digital watermarking in this architecture, and the algorithm used.

The fifth part undertakes the key evaluation of the watermark. It not only implements our methods, but also those of related research according to our ideas. As can

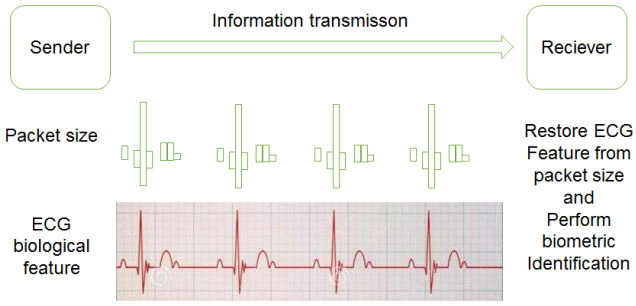

Figure 1: Application concept

be seen by comparing the data, the method has a certain advantage. In this method, the two assessment parameters of SNR and BER are mainly used as the evaluation criteria.

The final section of this paper provides a summary of the entire experiment, and comments on the literature review.

2 Application

As shown in Figure 1, we present a scheme of the proposed mechanism. It can work together with traditional biometric identification systems, such as fingerprint recognition or face recognition, distance certification, which can be applied to this authentication mechanism to enhance the safety performance of the authentication systems. Firstly, at the sender, is the extraction of the ECG, fingerprints or facial image as the biological features. Before transmission, the packet sizes of the network transmission are formed by biological features, such as the ECG waveform. In this, the series of packet size values has been formed as a sequence of waveforms, and then the data transmitted to the receiving end. After which the recipients receive these data, and decode the data packets. The correct sequence is obtained and the value of packet size extracted, and then compared with the ECG data to ensure that the transmission process is safe. Sequentially the extracted fingerprint or face images can also be converted to the related feature for identification and authentication.

Of course, this is just one kind of application of our proposed technology. The authentication mechanism can also be applied to many other applications, and requires further discussion in other research.

3 Background and Realted Work

3.1 Related Research

Articles on digital watermarking have been published continuously since 1994. Over time, the number of articles has presented a rapid increase, and several highly influential international conferences (such as IEEE ICIP, IEEE ICASSP, ACM Multimedia, *etc.*) as well as some international authoritative journals (such as the Proceedings of IEEE, Signal Processing, IEEE Journal of Selected Areas on Communication, Communications of ACM). "A digital watermark" [25] published by Van Schyndel for the ICIP'94 conference is the first article on digital watermarking published at major conferences [19]. May 30–June 6, 1996 saw the assembly of the first international symposium on information hiding (IHW) [22]. SPIE and IEEE International Conferences also featured related topics.

In the United States, a number of research institutions and enterprises represented by the MIT Media Lab have already applied for patents on digital watermarking. Digital watermarking has been supported or research conducted by government departments, universities and well-known enterprises, including the United States Finance Committee, United States Copyright Working Group, United States Air Force Institute, United States Army Research Laboratory, German National Information Technology Research Center, Japan NTT Information and Communications System Research Center, MIT, Illinois University, Minnesota University, and Cambridge University, Switzerland Lausanne Federal Institute of Technology, Vigo University, IBM Thomas J. Watson Research Center, Microsoft Research Cambridge, Lucent Technologies, Bay Networks, CA, Sony, NEC Research Institute and the Philips [25].

Chinese academic research on digital watermarking technology is not lagging behind compared to other countries. A number of famous scientific research institutions are already devoted to research in this area. In order to promote the research and application of digital watermark technology and other information hiding, by the end of 1999 several experts in the field of information security and related applied research units jointly held the first symposium on information hiding [22]. In early 2000, the national "863" intelligent machine expert group and the CAS Institute of Automation Pattern Recognition State Key Laboratory organised a symposium on digital watermarking, and reported the results of their own research.

Compared with the level of the rest of the world, the relevant Chinese academic field is not far off, and contains unique research ideas. So far, from the view of research, digital watermarking mainly relates to image, video, audio, text, and 3D grid data watermarking and so on, among which most of research and papers on watermarking focus on images. The reason for this is that the image is the most basic of multimedia data, and the development of the Internet provides large direct applications for image watermarking [13].

In addition, video watermarking has also attracted some researchers. Because video can be seen as a continuous image sequence, in a sense this is very similar to the principle of image watermarking, and many image watermarking research results can be directly applied to video watermarking. But there is an important difference between the two with respect to the magnitude of signal processing. In particular, the problem of real-time is considered in the study of video watermarking.

The research in this paper is similar to audio water-

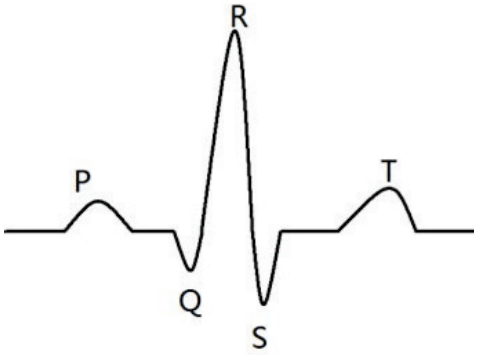

Figure 2: ECG schematic diagram

marking, because there are many similarities between ECG and audio. In this respect, the number of related studies at home and abroad is not extensive, but is in a gradually improving state. Simple watermarking technology has some shortcomings. Such as the watermark cannot be applied to images or signals with high accuracy, because watermarking causes some damage to the receptor and cannot fully recover during the restoration process.

The current watermarking applications have certain limitations, mostly used for copyright protection [7], adding fingerprinting [2], anti-tampering [9] and other aspects. The method proposed in this paper can guarantee transmission security with the adoption of watermark technology. Not only using ECG which is a kind of biological feature, but also establishing connections between the ECG feature and packet size, forming a relatively novel authentication mechanism. Whilst not exactly the same issue, the functionality of the authentication mechanism has yet to be further explored.

At present, it is undeniable that research on ECG information protection is still in its infancy, which is lack of related studies. The existing research may consist of the following categories:

1) Digital Watermarking Technology for Medical Imaging Area [5, 20];

2) ECG Monitoring Systems based on Sensor Network;

3) ECG Digital Watermarking Technology by Wavelet Transform;

4) ECG Transmission in Wireless Networks. Wavelet transform based digital watermarking encryption technology is mainly use for watermarking of the ECG signal. Thereby, our research provides great potential for researchers.

3.2 ECG Data Preparation

As shown in Figure 2, an electrocardiogram refers to the pacemaker, atrium and ventricle in each cardiac cycle, which continuously stimulates the electrocardiogram and the bioelectrical changes in the electrocardiogram. ECG traces are graphs of various forms of potential changes from the surface (referred to as ECG). An electrocardiogram is an objective indicator of the process of cardiac activation, transmission and recovery. ECG is an electrical activity in which the heart excites, and it has significant reference value for the basic functions of heart and pathology research. ECG can be used to analyze, even to identify a series of arrhythmias; it can also reflect the extent and development of myocardial injury and atrial and ventricular function as well as structural conditions. It provides the reference value for guiding cardiac surgery and advising on the necessary drug treatment.

The standard ECG lead to electrocardiogram waves, named by the Dutch physiologist William Einthoven (the inventor of the ECG). He divided one cardiac cycle into P, Q, R, S, T-waves.

P wave: P waves are generated by atrial depolarization, which is the excitement of the heart originates from the sinus node and then reaches the atria. This is the first wave of each wave group. In left and right atrium, p wave reflects the depolarization process. The front half of the P wave represents the right atrium, and the back half of the P wave reflects the left atrium.

QRS complex: Usually, A QRS complex consists of three closely connected waves. The first downward wave which is the Q-wave, along with a high-tip-Q-wave vertical wave called the R-wave. The downward wave followed by the R wave is called an S-wave. Science they are closely connected, and they reflect the excitement of the ventricular electrical process, it is collectively referred to as the QRS complex. This wave group reflects the left and right ventricular depolarization process.

T-wave: The T-wave is located in followed ST segment. It is relatively low and occupies much longer wave, which is produced by ventricular repolarization.

According to the above description, the ECG diagnosis mainly depends on the PQRST wave. Therefore, when we add a watermark, it is very indispensable to maintain the shape of these waveforms.

3.3 Principles of Network Transmission and Control

In this paper, we propose an architecture to ensure transmission security based on the control packet size. This will involve changes to the underlying network transmission. We need a control packet size for each transmission in a TCP/IP network protocol. Network transmission is a

communication process using a series of lines (such as optical fibres and twisted pairs) through the circuit changes and in accordance with the network transmission protocol [16]. Network transmission requires a medium, which is the network's physical path between the sender and the recipient, and has a certain influence on the data communication of the network. Common transmission media are optical fibers, twisted pair, coaxial cable and coaxial cable wireless transmission media. The network protocol is a specification for communicating and managing information in a network, including the Internet. Since the interaction between people needs to follow certain rules, the mutual communication between computers needs to comply with certain rules, which are called network protocols. Network protocols are usually divided into several levels, and communicating parties can only be connected to each other at in common level.

Common protocols are: TCP/IP, IPX/SPX, NetBEUI, *etc.* IPX/SPX is very usual in LAN. If the user wants to access the Internet, the TCP/IP protocol must be added to the network protocol. In this task, we mainly use the TCP/IP protocol [24]. TCP/IP is an abbreviation of "Transmission Control Protocol/Internet Protocol". TCP/IP is a network communication protocol that standardizes all communication devices on the network, especially the data format and transmission mode between the two parties.

TCP/IP is the basic protocol of the INTERNET, which is the standard method of data packing and addressing. In the process of data transmission, it could be represented as two envelopes with TCP and IP being like the envelope, the message is spliced into a number of segments, and each segment is delivered into a TCP envelope, and the envelope records the segment number information, then the TCP envelope is delivered in the IP envelope, and finally sent over the Internet.

At the receiving end, the TCP package collects envelopes, extracts data and restores the order. If an error is found, TCP will issue a repeat request. Therefore, TCP/IP on the Internet provides almost error-free data transmission. Ordinary users only need to know the IP address format, regardless of the entire structure of the network protocol, and then they can communicate with the rest of the world.

3.4 Principles of ECG Digital Watermarking

A common understanding of digital watermarking technology is that some identification information is directly embedded in a digital carrier (including multimedia, software, documents) or indirectly (modification of a specific area of the structure), which does not affect the use value of the original carrier, and is not easy to detect and modify, but can be identified by the producer. The hidden information in the operator can calculate the content creator and the purchaser, and can send out the secret information to find out whether the operator has been tampered with. As an effective means of copyright protection, digital watermarking is an important branch and research direction of information hiding technology research. Digital watermarking systems must have certain conditions to become a trusted application system for digital product copyright protection and integrity identification. A safe and reliable watermarking system should generally meet the following requirements:

- Concealment: Also known as imperceptibility. For an invisible watermark system, the watermarking embedding algorithm should not produce appreciable data modifications, namely the watermark in the normal viewing conditions should not be visible, and watermarking should not affect the visual effects of works.

- Robustness:

  Watermarking must be difficult to get rid of (hopefully impossible to remove). Of course, in theory any watermark can be removed as long as sufficient understanding of the process of watermark embedding is held. But if only a partial understanding of the watermark embedding process is held, any attempts to destroy or eliminate the watermark should lead to carriers of severe degradation, resulting not available.

- Tamper resistance:

  Uulike robustness, tamper resistance means that once the watermark is embedded in the carrier it is difficult for attackers to change or forge. Applications demanding high robustness usually require a strong tamper resistance. It is more difficult to achieve a good tamper resistance in copyright protection.

- Watermark capacity:

  Embedded watermark information must be sufficient to represent the multimedia content creator or owner of the flag, or the serial number of the purchaser. So when copyright disputes occur, the information of the creator or copyright owner is available, and the sequence number is used to indicate the users who have breached the agreement and provide multimedia data for piracy [15].

- Safety:

  The embedded information should ensure confidentiality and a low false detection rate. Watermarks can be any form of data, such as numeric, text, images, and so on. All watermarking embedded systems contain a watermark and watermark recovery system.

- Low error rate:

  Even in the case of attack or signal distortion, the probability of not detecting a watermark (undetected, false-negative) and detecting a watermark (false detection, false-positive) where the is none should be very small.

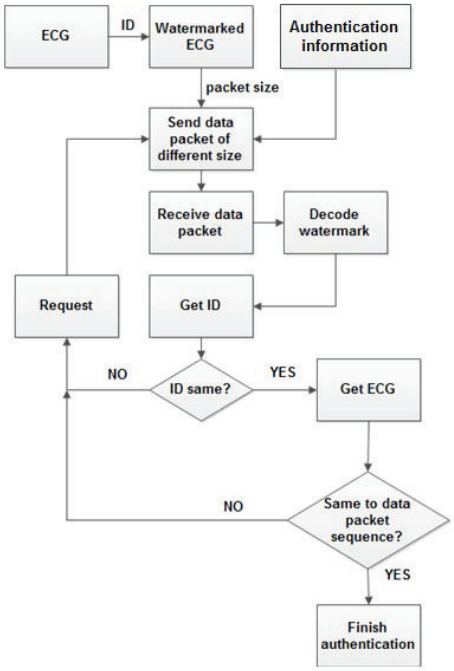

Figure 3: Overall flow of proposed algorithm

4 Proposed Algorithm

Our idea is like that at the transmitting end of the network we control the size of the transmission packet according to the ECG feature of the sender. Then we select a value calculated by the coefficient as the interval, to meet the range of packet sizes. Subsequently, senders send the designed packet, and at the same time the ECG sequence is transmitted as a key.

As shown in Figure 3, in the process of transmission the ECG sequence is watermarked, and the watermark is an ID number. The receiver receives the data, orders in accordance with the sequence, obtains the size of the packets, and puts them into a sequence. At the receiving end, the received ECG is de-watermarked to get the ID number and ECG sequence. According to the comparison of the ID number, the first step in the confirmation is obtained. If the ID number changes, or is beyond a certain range, it can detect that the information has be tampered with or suffered other attacks. And then the ECG signal, if the changes in the ECG signal do not exceed the threshold value, the network transmission can be identified as secure. Regardless of the kind of change to the network packet, its packet size will be changed, resulting in the export sequence being different to the original sequence. So we have to set the threshold standard. This is the preliminary idea of the authentication mechanism. This mechanism can be applied in various types of network identity authentication system, and can also be applied in a variety of network security transmissions.

The steps of the scheme are listed below:

1) Adding a watermark to the ECG;
2) Extracting number ID as the packet size;
3) Sending data as different sized packets;
4) Receiver open the packet;
5) Packet sizes are selected;
6) Decoding of watermark to get ID;
7) Checking of the size sequence (ID).

4.1 ECG Data Acquisition

In this research we use the MIT-BIH ECG data [12]. An ECG recording is composed of three parts:

1) Head files [.hea], which store the ASCII code character.
2) Data files [.dat], binary storage, each three bytes store two numbers, a number is 12 bit.
3) Notes file [.art], binary storage, format definition is more complex.

In the early stage of research, the methods of reading and the application of ECG data should be learnt and mastered [6].

4.2 ECG Watermarking Algorithm

We proposed a self-synchronous ECG digital watermarking encryption technology to achieve the protection of the transmission data. In addition, a series of ECG data is embedded in synchronous code, so that this data is self-synchronous. Further, some hidden data is embedded into DWT low frequency coefficients. Finally, the SNR (signal-to-noise ratio) and BER (bit error rate) are used for the analysis and evaluation of the overall effects. SNR measures the transparent of embedded data. The BER test after the addition of Gaussian noise, assesses the performance of the design algorithm.

In this process we use the mechanism of synchronous code. Next, we introduce the principle. It can be used to locate hidden information in order to prevent unpredictable attacks [26]. Supposing $\{a_i\}$ is a set of source-synchronous code, and $\{b_i\}$ is the location code which has the same length as A. If the difference between $\{a_i\}$ and $\{B_i\}$ is less than the set threshold, then $\{b_i\}$ will be recognised as a synchronisation code. Also there will be a fault-tolerance rate. Our formula is shown below. Assume that P_1 is a positive error rate, P_2 is a negative error rate, l is the length of the synchronisation code, and e is the threshold value we have set.

$$P_1 = \frac{1}{2^l} \cdot \sum_{k=l-e}^{l} C_l^k \tag{1}$$

$$P_2 = \sum_{k=e+1}^{l} C_l^k \cdot (BER)^k \cdot (l - BER)^{l-k} \tag{2}$$

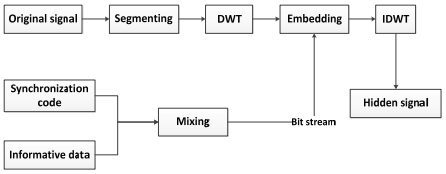

Figure 4: Embedding model

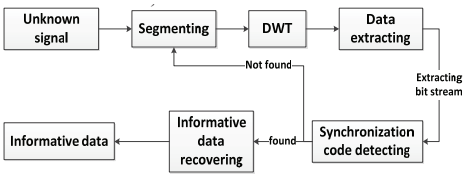

Figure 5: Extracting model

Taking into account the low-pass filtered improved robustness, the synchronisation code and the watermark is embedded in the low frequency sub-band coefficients of the seventh stage, which are the lowest frequency wavelet coefficients in our system. Then the synchronisation code and embedded information is mixed, when the watermarking ECG data is embedded in the low-frequency sub-band of the DWT factor, and then after the inverse transform, we obtained the watermarked ECG data. The detailed process model of embedment is shown in Figure 4.

In the data extraction section, data is firstly processed by the Wavelet transform which is the opposite to the embedding. It extracts binary data from the low frequency sub-band of wavelet coefficients. From these data, we can restore the synchronous code. In the signal analysis process, the selected action is repeated until the synchronous code is detected. The details of the process description are shown in Figure 5. After determining the location of the synchronisation code, we can extract the hidden information.

In this step, the ECG signal is segmented, and each segment executes the DWT transform. Then the sequence {MI} is embedded in each frequency band. The length of the signal segment depends on the size of the wavelet decomposition level. Of course, this length should be at least capable of accommodating a synchronous code and a number of data information. The embedded rules are as follows:

$$X_k^{'} = \begin{cases} \lfloor X_k/\alpha \rfloor \cdot \alpha + 3\alpha/4 & W_k = 1 \\ \lfloor X_k/\alpha \rfloor \cdot \alpha + \alpha/4 & W_k = 0 \end{cases} \quad (3)$$

In this equation, X_k is the original DWT transform coefficient, $X_k^{'}$is the watermarking DWT transform coefficient, and α is the embedding strength.

In addition to the synchronous code, when embedding the watermark in the ECG, we use the concept of payload that the number of bits, to measure the rate of each unit (bit per second). And as B are used in the following formula. Supposing the sampling rate is R(Hz), the wavelet decomposition level is K. And the formula is as follows:

$$B = R/2^K bps \quad (4)$$

During data extraction, the signal of the ECG embedded watermark is similarly segmented. These fragments include at least one synchronous code segment. Then each segment executes wavelet transformation. Assuming $X_k^{'}$ is the coefficient of the low-frequency sub-band, the sequence of W_k^* is extracted from $X_k^{'}$ using the rules shown below.

$$W_k^* = \begin{cases} 1, & if\ X_k^{'} - \left\lfloor X_k^{'}/\alpha \right\rfloor \cdot \alpha \geq \alpha/2 \\ 0, & if\ X_k^{'} - \left\lfloor X_k^{'}/\alpha \right\rfloor \cdot \alpha < \alpha/2 \end{cases} \quad (5)$$

5 Evaluation

In this section, our data are selected from the MIT-BIH ECG database. Under such conditions, the embedded data transmission rate of the synchronisation code is evaluated, and the payload adopting this method tested. The SNR and BER are mainly used in the assessment. SNR and BER have been introduced in the previous section, and their formulas are given as Equations (6) and (7). Of course, the characteristics of the watermark are transparent to the user, and the presence of the watermark does not affect the user. Therefore we should as far as possible ensure that the watermark signal is consistent with the original signal [1].

First of all, define SNR and BER.

$$SNR = -10\log_{10}\left[\left(\sum\nolimits_i \left(f_i^{'} - f_i\right)^2 \Big/ \left(\sum\nolimits_1 f_i^2\right)\right)\right] \quad (6)$$

$$BER = \frac{Number\ of\ error\ bits}{Number\ of\ total\ bits} \times 100 \quad (7)$$

In the above formula, f_i and $f_i^{'}$ represent the original signal and the modified signal.

Firstly we selected four sets of data from the MIT-BIH database. Then we tested the running of the algorithms using these four groups of data. The first step is to contrast an improved method with the original method which was applied to audio. In the last part of the experiment, the white noise attack multiplication factor was set to control the different degrees of attack. A total of four values were obtained: 1,50,500,1000. The table 1 is the contrast effect for the SNR value before and after modification.

From the above table it can be seen that after our modification the value of SNR has been improved to some extent. This shows that after our modifications this method is more suitable for the application of the ECG data encryption, and by using this method we can get a better result.

In Figure 6 the blue curve represents the original signal, and the green curve shows the watermarked signal.

From Figure 7 we can see that the difference between the original signal and watermarked signal is very small,

Table 1: Comparison of SNR before and after modification

Data	Before modification SNR	After modification SNR
Class 1	27.2382	30.4968
Class 2	25.6382	30.6291
Class 3	29.7743	31.7761
Class 4	28.3629	32.0753

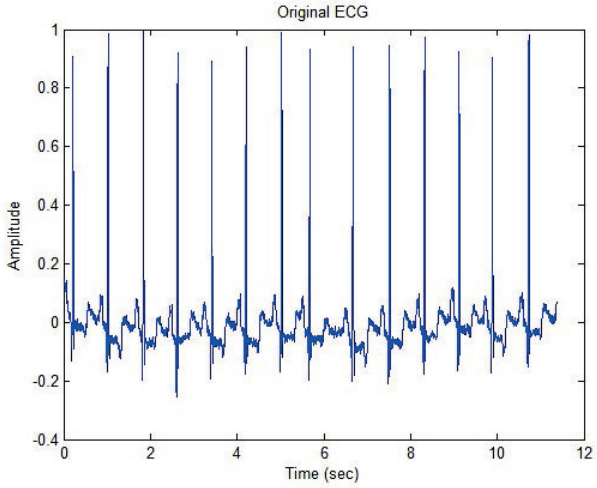

Figure 6: Original ECG signal

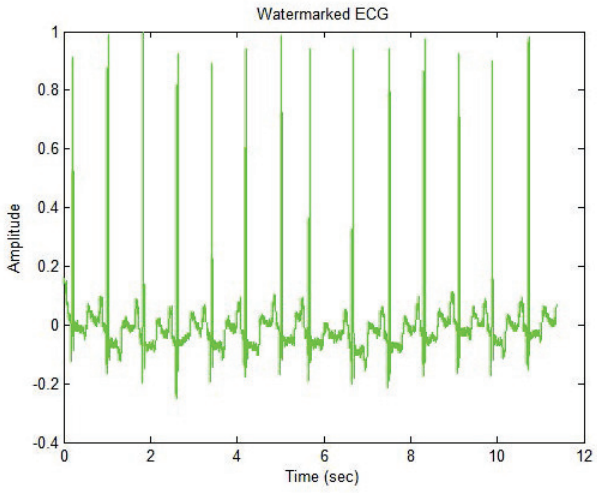

Figure 7: Merger of watermarked and original ECG signal

Table 2: Watermark basic parameters

Data	Fs	Time	SNR	level
Class 1	360	10	30.4968	7
Class 2	360	10	30.6291	7
Class 3	360	10	31.7761	7
Class 4	360	10	32.0753	7

Table 3: Watermark robustness test

Data	WhiteNoise	BER	Error	SNR_noise
Class 1	1	0	0	72.6337
Class 1	50	0	0	38.6543
Class 1	500	0	0	18.6543
Class 1	1000	21.8750	7	12.6337
Class 2	1	0	0	71.8875
Class 2	50	0	0	37.9081
Class 2	500	0	0	17.9081
Class 2	1000	21.8750	7	11.8875
Class 3	1	0	0	73.9786
Class 3	50	0	0	39.9992
Class 3	500	0	0	19.9992
Class 3	1000	21.8750	7	13.9786
Class 4	1	0	0	73.7127
Class 4	50	0	0	31.3995
Class 4	500	0	0	19.7333
Class 4	1000	21.8750	7	13.7127

and with the naked there is almost no difference. In the above test, the ECG sampling rate is 360. In each of the data signals, the fragments whose length is 4096 were chosen to test. Using a synchronous code whose length is 63, and a 256 bit watermark sequence. In the third chapter, the threshold is defined as 21. The Haar wavelet transform has eight layers of decomposition level, which is also mentioned in the previous section.

Table 2 is a test of four groups of data, for which different SNR values are obtained. In this table we can see that the SNR value is over 30, which is able to meet the accuracy demand. Under such conditions, it does not affect the diagnosis of the doctor for the ECG image.

Subsequently, white noise attack is tested on the watermarked signal. Thus we can better understand the robustness of watermark [21]. After the signal is watermarked, the white noise is added. They can be used to simulate transmission channel noise and possible attack. The specific data are shown in Table 3.

From Table 3 it can be seen that the ordinary size of noise cannot affect the watermark. From the data, when the noise factor is 1, 50 and 500, the values of BER are all 0. Even under the influence, the error rate is 0. When the white noise coefficients were 1 and 50, the SNR with noise is greater than 30. Today's popular ADSL broadband network basically does not produce much noise [3]. According to industrial regulations, if the network noise reaches 30–50 dB then the network is largely as unusable. When the noise size is about 5 dB, the network has begun

to enter an unstable state. In this state many failures and errors can occur in the network. Only when the noise is sufficiently large, such as a coefficient of more than 500 times, will some deviations appear. However, such a large noise is very rare in the real environment. Therefore the watermark robustness of this method is good.

In this section we conduct an in-depth study of some of the papers on ECG watermarking, and select a number of representative methods for comparison. Then, according to our understanding these methods are implemented and compared. According to the various parameters listed in the literature, an attempt is made to make the test data consistent with the original experiment. So the results and the original intention of the author are not too different. After testing it can be seen that the difference between the obtained data and the original data is not too large, and is basically the same. Although there is a little deviation, overall it is still in an acceptable range. The experimental results listed below have basically achieved the desired results [8].

One of these studies is "Wavelet Transformation Based Watermarking Technique for Human Electrocardiogram (ECG)", whose authors are Mehmet Engin, Oğuz Çıdam and Erkan Zeki Engin. The main idea of the article bears some similarities with our approach. Therefore there is value in contrasting it. Firstly, the ECG signal is decomposed into 8 sub-bands through discrete wavelet transform. Then they calculate the average power of each sub-band. Finally, the random sequence is inserted into the watermark signal and the selected low frequency subband. In the process they use the Daubechies Wavelet function (DB2) and bi-orthogonal functions (bior5.5) [23].

In the process of watermark embedding they use a random Gaussian noise and Theravada as the coefficients for generating a random sequence. However the embedding process is only a simple process of summation. In the watermark extraction process, they need to use the original ECG to calculate the watermarked sequence. In such a case, the significance of network security will be lost. And, in this way we cannot guarantee the security of the transmission. If the original ECG signal and watermarked ECG signal is modified at the same time, they may not be detected. In terms of data, they selected four typical data sets, including a normal ECG and diseased ECG. Their data are also from the MIT-BIH database [18]. After this method was studied we implemented it. In the original article they have compared the two methods of DB2 and bior5.5 [18], and proven that the effect of bior5.5 is worse than DB2, so we only tried the DB2 method.

Compared with their method, the most obvious difference with ours is the ability of self-synchronisation. Furthermore, in the process of watermark extraction, we do not require the use of the source ECG. The following table shows the implementation of the two methods, and their testing using the same data. It compares the SNR values of the two methods with watermark.

As can be seen from the table above, the SNR value using our methods are significantly higher. This shows

Table 4: SNR comparison

Data	Our SNR	Their SNR
Class 1	30.4968	20.9100
Class 2	30.6291	20.3561
Class 3	31.7761	21.2650
Class 4	32.0753	24.9800

Table 5: The robustness of their method

Data	WhiteNoise	BER	Error	SNR_noise
Class 1	1	28.1250	9	72.6197
Class 1	50	31.2500	10	38.6403
Class 1	500	37.5000	12	18.6403
Class 1	1000	50.0000	16	12.6197
Class 2	1	56.2500	18	71.9227
Class 2	50	53.1250	17	37.9433
Class 2	500	53.1250	17	17.9433
Class 2	1000	71.8750	23	11.9227
Class 3	1	62.5000	20	73.9056
Class 3	50	62.5000	20	39.9262
Class 3	500	56.2500	18	19.9262
Class 3	1000	53.1250	17	13.9056
Class 4	1	56.2500	18	73.6919
Class 4	50	56.2500	18	39.7125
Class 4	500	65.6250	21	19.7125
Class 4	1000	65.6250	21	13.6919

that after the watermark embedding process the use of our method produces less noise.

On the table 5, we can know the robustness with adding white noise when embed watermark [10]. The SNR values are listed in the table. After finishing the extraction of the watermark, BER was used to assess the robustness of this approach [11]. From the comparison of the data obtained with the data from Table 5, it can be seen that the error rate of extracting the watermark sequence is relatively low when using our method, and the noise coefficient increases.

As shown in Figure 8 this is a discount figure. It visually shows the effect of the BER comparison of the two methods. The error rate of the sequence watermark obtained using our method is significantly lower

In the end we tested 48 sets of data, are all from the

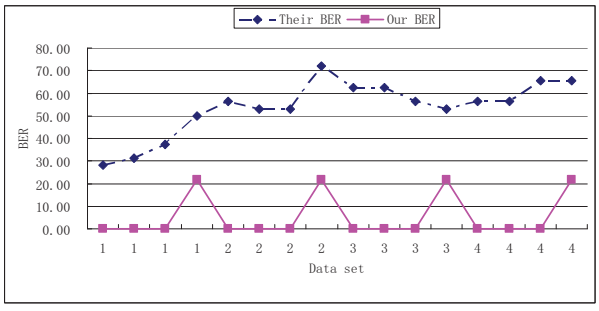

Figure 8: BER comparison of the two methods

MIT-BIH database. Using our method the data obtained is presented in Table 6. SNR represent the signal-to-noise ratio without noise [17]. SNR_noise represents the signal-to-noise ratio with noise attacks. The noise factor is 500.

Table 6: 48 datasets

	SNR	SNR_noise		SNR	SNR_noise
100	30.4968	18.6543	201	33.2101	20.1639
101	29.0157	17.9081	202	32.2859	19.8937
102	29.7	19.9992	203	34.9532	23.9485
103	31.3995	19.7333	205	29.9598	19.3858
104	30.9927	20.0396	207	36.2762	25.0338
105	32.6936	21.8737	208	36.3481	24.5461
106	33.5246	21.0478	209	31.0114	20.4217
107	37.5646	26.2966	210	34.9704	22.3635
108	32.534	22.831	212	33.2044	22.7276
109	34.7681	24.9335	213	33.9076	23.0179
111	33.3272	21.1172	214	34.4189	23.0512
112	33.4805	22.0718	215	34.3245	23.216
113	31.5873	21.0054	217	38.1804	25.8837
114	31.9882	21.6256	219	33.7499	21.7806
115	30.249	18.4942	220	30.6738	19.4284
116	33.6845	21.1607	221	32.2778	21.4587
117	34.5648	23.0738	222	30.3614	19.8714
118	36.1235	24.1986	223	35.0769	21.4536
119	31.5782	20.8796	228	33.4002	23.0628
121	34.9675	21.7999	230	31.2626	20.7424
122	33.9329	22.6893	231	31.627	19.9292
123	28.8724	18.2877	232	32.2554	20.3259
124	30.5468	19.9755	233	34.9552	24.7316
200	32.9446	22.4092	234	29.8672	20.7317

The overall trend of the data in Table 6 is shown in Figure 9.

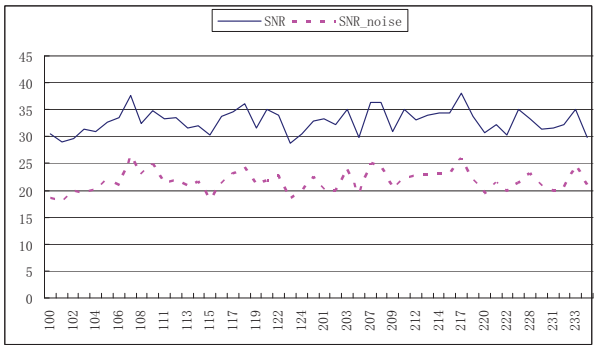

Figure 9: Overall trend

Now, in order to verify our search result we developed a system. The algorithm of the watermarking and decoding are implemented by Matlab, and the sender and receiver, which can send and receive the package, are coded by C code. We have built the project to transmit a message by TCP/IP packet size based on the ECG biological feature for a security network.

The execution screen can be viewed in Figure 10 for the sender (left widow) and for the receiver (right widow).

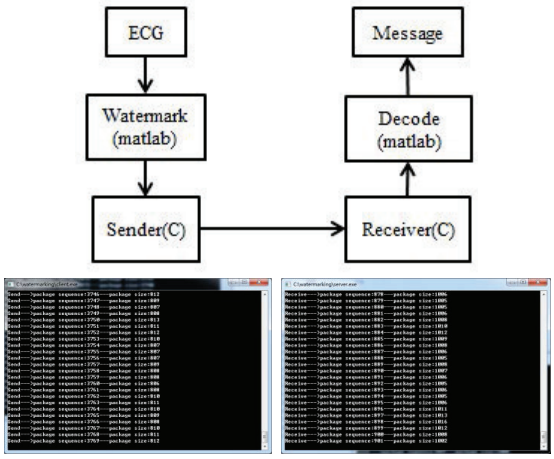

Figure 10: Execution screens for the implemention code

And we have shared the code on Google Code. If needed you can download the source code from website: `https://code.google.com/p/my-watermarking-ecg/`. If you want to run the system, you can refer to the process below. The system contains the programs: Watermarked.m, client.exe, server.exe and Decode_watermark.m. Firstly run Watermarked.m, with ecg_embed.dat, which contains the watermarked ECG. Next you can run client.ext and server.exe which will send and receive the package. The server will receive the message and place the message in ecg_embed_recv.dat and ecg_recv.data. ecg_embed_recv.data contains the package size message, and ecg_recv.data contains the receiving data. Finally, run Decode_watermark.m, which decodes the data of ecg_recv.data, and obtains the watermarked message.

6 Conclusion

In this paper we firstly discussed the security issues in network transmission, and presented a new secure transmission scenario, packet watermarking with ECG signal. Then we provided further discussion on the proposed algorithm, especially that on transmission watermarking research. This proposed an idea for secure watermarking transmission with an ECG feature to control the packet size. In order to guarantee the security of the watermarked transmission, we adopted the ECG feature and self-synchronisation technology, this focused on the idea of a self-synchronised watermark. The next detailed describe the specific steps about how the texts uses the self-synchronous wavelet watermark with ECG signal. In the end, we evaluated our system and compared it with some other methods.

In our proposed algorithm, the self-synchronous ECG digital watermark technology is used in security transmission to protect the key link. In order to enhance the robustness, the synchronisation code sequence and the watermark sequence are embedded into the lowest frequency wavelet coefficients. To improve efficiency, in the process of synchronisation code searching the time frequency of

the wavelet transform is used to to locate the code .

From the experimental results, we can see that the watermarked ECG signals have high SNR values; it can resist common attacks, and is robust to changes in the waveform. In the experiment, a number of representative ECG signals were selected to obtain a general conclusion. However, it is just a small part compared to the larger ECG database. At the same time, we think the experimental results can be improved, and better result obtained through different approaches. We also hope this technology can be applied to other fields, such as brain waves and hand signatures, which may need further study and research.

References

[1] D. Anand and U. C. Niranjan, "Watermarking medical images with patient information," in *Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 703–706, Nov. 1998.

[2] N. Bousnina, S. Ghouzali, M. Lafkih, O. Nafea, M. Mikram, W. Abdul, and D. Aboutajdine, "Watermarking for protected fingerprint authentication," in *International Conference on Innovations in Information Technology*, pp. 1–5, 2017.

[3] S. T. Chen, H. N. Huang, J. S. Pan, K. K. Tseng, and S. Y. Tu, *Audio Watermarking Quantization Based on Minimum-length Scaling Scheme*, National Science Council, TAIWAN, under the NSC grant: NSC 98-2115-M-029-006-MY2, 2009.

[4] G. P. Feng, "computer network unsafe factor analysis and countermeasures," *Shanxi Coking Coal Science and Technology*, vol. 11, no. 11, pp. 30–31, 2005.

[5] J. J. Garciahernandez, W Gomezflores, and J Rubioloyola, "Analysis of the impact of digital watermarking on computer-aided diagnosis in medical imaging," *Computers in Biology & Medicine*, vol. 68, pp. 37–48, 2016.

[6] K. Ibrahim I. Ayman and S. Ron van, "A low complexity high capacity ecg signal watermark for wearable sensor-net health monitoring system," in *Computing in Cardiology*, pp. 393–396, Sep. 2011.

[7] A. Jadhav and M. Kolhekar, "Digital watermarking in video for copyright protection," in *in Proceedings of the International Conference on Electronic Systems, Signal Processing and Computing Technologies*, pp. 140–144, Dec. 2014.

[8] Y. L. Kan, "Digital audio watermark technology based on fourier transform," *Journal of Beijing Broadcasting Institute*, vol. 01, 2005.

[9] Z. Ling, "Anti-tampering technology of digital watermarking in dynamic web page images," *Agro Food Industry Hi Tech*, vol. 28, no. 1, pp. 2195–2199, 2017.

[10] K. D. Manab P. Dipti and P. Smita, "Integration of FCM, PCA and neural networks for classification of ecg arrhythmias," *IAENG International Journal of Computer Science*, vol. 3, 2010.

[11] J. Mehrdad, E. Reza, S. Atena, F. Soheil, and Z. Shokoufeh, "Improving ecg classification accuracy using an ensemble of neural network modules," *Plos One*, vol. 6, no. 10, pp. e24386, 2011.

[12] M. S. Nambakhsh, A Ahmadian, M Ghavami, R. S. Dilmaghani, and S Karimi-Fard, "A novel blind watermarking of ecg signals on medical images using EZW algorithm," in *International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 3274–3277, 2006.

[13] J. Peng, "On the computer network security," *Sichuan University of Arts and Science Journal*, vol. 20, no. 9, pp. 73, 2010.

[14] F. Qin and C. L. Shi, "Authenticated encryption schemes: Current status and key issues," *Computer Knowledge and Technology*, vol. 6, no. 5, pp. 4118–4119, 2010.

[15] S. Riya, K. Suneet, F. Omar and S. A. Bhavneet, "Watermarking for protected fingerprint authentication," in *Proceedings of the 12th International Conference on Innovations in Information Technology (IIT'10)*, pp. 140–144, Mar. 2010.

[16] X. Shen, C. Lin, Y. Sun, J. Pan, P. Langendoerfer, and Z. Cao, "Wireless network security," *Wireless Communications & Mobile Computing*, vol. 6, no. 3, pp. 269–271, 2006.

[17] P. Singh and P. K. Mann, "Fast fourier transformation based audio watermarking using random sample," *ResearchGate*, 2011. (`https://www.researchgate.net/publication/268184106_Fast_Fourier_Transformation_Based_Audio_Watermarking_using_Random_Sample`)

[18] L. W. Tang, K. M. Zheng and X. Qian, "Watermarking technology for electrocardiogram signal certification," *Computer Engineering and Applications*, vol. 45, no. 20, pp. 231–233, 2009.

[19] A. Z. Tirkel R. G. van Schyndel and C. F. Osborne, "A digital watermark," in *Proceedings of 1st International Conference on Image Processing*, pp. 86–90, Nov. 1994.

[20] C. S. Tsai N. I. Wu, C. M. Wang and M. S. Hwang, "A certificate-based watermarking scheme for coloured images," *The Image Science Journal*, vol. 56, no. 6, pp. 326–332, 2008.

[21] D. H. S. Wu, J. Huang and Y. Q. Shi, "Efficiently self-synchronized audio watermarking for assured audio data transmission," *IEEE Transactions on Broadcasting*, vol. 51, no. 1, pp. 69–76, 2005.

[22] Y. Wu, "digital watermark technology research matlab simulation," *Technology Applications*, pp. 37, 2005.

[23] H. Y. Yang, X. Y. Wang, and H. Zhao, "Digital audio watermarking algorithm based on adaptive quantization," *Technical Acoustics*, vol. 02, 2004.

[24] F. Zhang, and J. F. Ma, "Authentication mechanisms, performance and security analysis," *Xi'an University of Electronic Technology*, vol. 4, 2004.

[25] J. M. Zhang, *Digital Watermarking Technology and Computer Application Technology*, Shandong University of Science and Technology, Master's Degree Thesis, 2005.

[26] K. M. Zheng, and Q. Xu, "Reversible data hiding for electrocardiogram signal based on wavelet transforms," in *In Proceedings of the International Conference on Computational Intelligence and Security*, pp. 295–299, Dec. 2008.

Biography

Kuo-Kun Tseng, is an associate Professor and Shenzhen Peacock B-level talent, born in 1974, received his doctoral degree in computer information and engineering from National Chiao Tung University of Taiwan in 2006. Since 2004 he has many years of research and development experience, long engaged in biometric systems and algorithms research. The current research results, published more than 70 articles, of which about 30 is a high impact factor of the SCI or the famous ACM / IEEE series of journals.

Xialong He, was a graduate student at Harbin University of Technology (Shenzhen), and now is a senior software engineer. His expertise is watermarking and biometric processing.

Xiaoxiao An was a graduate student at Harbin University of Technology (Shenzhen), and now is a senior software engineer in Alibaba Corporation. His expertise is machine learning and biometric processing.

Chin-Chen Chang received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Taiwan. He was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the College of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From July 1998 to June 2000, he was the director of Advisory Office of the Ministry of Education of the R.O.C. Since February 2005, he has been a Chair Professor of Feng Chia University. He is currently a Fellow of IEEE and a Fellow of IEE, UK. He also published several hundred papers in Information Sciences. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression and data structures.

Chao Wang is a master student at Harbin University of Technology (Shenzhen), his interested in the deep learning algorithm and bio-signal processing.

Xiangmin Guo is the deputy dean of Shenzhen Branch of Urban Planning & Design Institute of Harbin Institute of Technology (HIT), and associate professor in Harbin Institute of Technology, Shenzhen Graduate School.