International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 011 | November 2019 www.irjet.net p-ISSN: 2395-0072

STEGANOGRAPHIC SCHEME FOR OUTSOURCED BIOMEDICAL TIME SERIES DATA USING AN INTELLIGENT LEARNING-A RESEARCH

Harshala Pundkar[1], Dr. Atul Joshi [2]

[1]ME Student, Dept of Electronics and Telecommunication
[2]Associate Professor, Sipna College of Engineering and Technology, Amravati.

Abstract: Sharing outsourced data between owners and data mining experts is becoming a challenging issue in biomedical and healthcare fields. Watermarking has been proved as a right-protection mechanism that can provide detectable evidence for the legal ownership of a shared dataset, without compromising its usability. However, the main disadvantage of these conventional techniques is unintelligent, rule-based and they do not directly deal with the data synchronization. Therefore, decoding performance reduces significantly when the watermarked data is transmitted through a real communication channel. This paper proposes an intelligent learning-based watermark scheme for outsourced biomedical time series data. The scheme carries out embedding of watermark data based on modifying mean modulation relationship of approximation coefficients in wavelet domain.. Experimental results on electroencephalography (EEG) data with lifting wavelet transform shows that the proposed scheme provides good imperceptibility and more robust against various signal processing techniques and common attacks.

***Key Words:** ECG, Steganography, watermarking, time series data.*

1. INTRODUCTION

In Medical field images play a crucial role in tele-surgery, tele-diagnosis, tele-conferencing, and many other tele-medicine applications. The ease of copying, manipulation, exchange, and distribution of images across the vulnerable public networks have brought for the importance of providing security to exchanged medical images. To provide safe transmission of medical images, there exists some security requirements that must be met. These requirements are confidentiality, authenticity, and integrity. Confidentiality states that only authorized users have access to the exchanged image, authenticity allows verification of the origin and owner of the exchanged image, and integrity ensures that the exchanged image has not been modified or tampered with. Two technologies have been in common use to achieve the above security requirements: steganography and digital watermarking. Steganographic techniques scramble the medical image to achieve confidentiality, and use digital signatures to provide authenticity and integrity. However, with encryption only it is impossible to monitor how a legitimate user handles the content after decryption, thus making it possible to illegally redistribute or manipulate the content. The science which deals with the hidden communication is called Steganography. There are different kinds of steganographic techniques which are complex and which have strong and weak points in hiding the invisible information in various file formats. The innocent carriers are the possible cover carriers which will hold the hidden communication. A Steganography method is admirably secure only when the statistics of the cover information and the steganographic information are similar with each other.

2. LITERATURE REVIEW

Trung Pham [1] proposed the scheme that adopts a blind digital watermarking detection method based on intelligent learning for outsourced biomedical time series data and this proposed method can extract the embedded watermark without any information from the original watermark. In the embedding scheme, the original signal is divided into a set of frames, and these frames are selected according to a secret key. These selected frames are then separated into two sets of sub-frames by a down-sampling technique. After that four-level wavelet is performed on each of these sub-frame sets. Finally, the watermark data is embedded in to these sub-frames based on modulating mean value relationship of their coefficients in wavelet domain. At extraction scheme Noise, lossy compression and signal processing can modify the watermarked biomedical data and the modification can be viewed as the corruption to the biomedical data by different noise types.

Elisa Bertino [2] implemented demand for the secondary use of medical data is increasing steadily to allow for the provision of better quality health care. Two important issues pertaining to this sharing of data have to be addressed: one is the privacy protection for individuals referred to in the data; the other is copyright protection over the data. In this scheme, they present a unified framework that seamlessly combines techniques of binning and digital watermarking to attain the dual goals of privacy and copyright protection. Our binning method is built upon an earlier approach of generalization and suppression by allowing a broader concept of generalization. To ensure data usefulness, they propose constraining Binning by usage metrics that define maximal allowable information loss, and the metrics can be enforced off-line. This watermarking algorithm watermarks the binned data in a hierarchical manner by leveraging on the very nature of the data. The method is resilient to the

generalization attack that is specific to the binned data, as well as other attacks intended to destroy the inserted mark. They prove that watermarking could not adversely interfere with binning, and implemented the framework. Experiments were conducted, and the results show the robustness of the proposed framework. Two important issues inherent to the outsourcing of medical data are the protection of individual privacy and copyright protection over the data

Duy, Dat Tran, and Wanli Ma [3] proposed copyright protection for multimedia data owners is of crucial importance as the duplication of multimedia data has become easily with the advent of Internet and digital multimedia technology. Current digital watermarking techniques for preserving the product ownership are rule-based and not directly deal with the data synchronization, therefore their decoding performance reduces significantly when the watermarked data is transmitted through a real communication channel. This paper proposes a pattern recognition framework to build a new blind watermark scheme for electroencephalography (EEG) data. Embedding a watermark is based on modifying mean modulation relationship of approximation coefficient in wavelet domain. Retrieving this watermark is done effectively using Support vector data description (SVDD) models trained with the correlation between modified frequency coefficients and the watermark sequence in wavelet domain.

M. Kamran and Muddassar Farooq [4] stated that the data is an important asset for its owner. Digital data sharing is becoming an emerging trend both at the personal and organization level. Information and communication technology (ICT) systems generate and use enormous amount of data that contains useful knowledge which needs to be extracted by using different data mining and warehousing techniques. In a collaborative environment, individuals and organizations need to share their data using different resources. The shared data must adhere to secrecy (for preventing unauthorized disclosure of data), integrity (malicious data modifications), and availability (error recovery). The digital data can be copied, altered and may be redistributed for different purposes, and this fact may violate the copyrights of the data owner. In their work, a comprehensive review of the database watermarking and fingerprinting techniques, proposed to date, has been presented. The classification of techniques has been done on the basis of watermarking technique and the orientation of the inserted watermark. Using this nomenclature, three types of top level classes are presented: BRT, DSMT, and CDCMT.

Xinyue Cao, Zhangjie Fu, and Xingming Sun [5] Cloud storage has been recognized as the popular solution to solve the problems of the rising storage costs of IT enterprises for users. However, outsourcing data to the cloud service providers (CSPs) may leak some sensitive privacy information, as the data is out of user's control. So how to ensure the integrity and privacy of outsourced data has become a big challenge. Encryption and data auditing provide a solution toward the challenge. In this scheme, they propose a privacy-preserving and auditing-supporting outsourcing data storage scheme by using encryption and digital watermarking. Logistic map-based chaotic cryptography algorithm is used to preserve the privacy of outsourcing data, which has a fast operation speed and a good effect of encryption. Local histogram shifting digital watermark algorithm is used to protect the data integrity which has high payload and makes the original image restored losslessly if the data is verified to be integrated.

Roopam Bamal, Singara Singh Kasana [6] Watermarking techniques are widely used for copyright protection, confidentiality and integrity issues in medical field. Reversibility, robustness, embedding capacity and invisibility are the essential requirements of a watermarking technique. Cogitating the need of security for medical images, this paper proposes a reversible high embedding capacity, high image fidelity, a hybrid robust lossless data hiding technique by using both transform and spatial domains. Proposed technique alters the mean of the selected non-overlapping slantlet transformed blocks of the host image whereas RS vector considers flipping factor for data embedding. The optimum thresholds to select the blocks are calculated through PSO technique and watermark is generated by using patient details, biometric id and region of interest (ROI) blocks of host image.

Hongjun Liu, Abdurahman Kadir, Xiaobo Sun [7] proposes a chaos-based colour image encryption scheme, the highlight is that the randomly sampled noise signal is applied to serve as the initial values of a chaotic system. The 256-bit hash value of noise is transformed into the one-time initial values of the Liu system. The sequences generated by Liu system are subjected to three batteries of TestU01. Exclusive OR, the only operation, is applied to diffuse the pixels, and some measures are taken to speed up the encryption process. Finally, some statistical tests are performed to assess reliability and efficiency of the proposed cryptosystem in terms of time complexity and security. Also introduces a chaos-based colour image encryption scheme, and the main novelty is the generation of one-time keys by the common hash value of the randomly sampled environmental noise. The initial values and control parameter of the Liu system are true random numbers from a noise array, and their subscripts in noise array are determined by the hash value. Three state variable sequences of Liu system are applied to diffuse the red, green and blue components through bitwise XOR operation. The running speed is effectively improved by some time-saving operations, such as effectively determine iterative times according to image size, faster integer operations, exactly amplification factor of state variables, matrix calculation and pre-allocated memory.

Rizki Arif, Sastra K. Wijaya, Prawito, and Hendra Saputra Gani [8] This study demonstrates the feasibility of identifying and quantifying pathological changes in brain electrical activity with a portable eight-channel data acquisition system based on Raspberry Pi 3 and MATLAB-based Graphical User Interface (GUI) to perform analyses on Electroencephalogram (EEG) signal including Fast Fourier Transform (FFT), Power Spectral Density (PSD), Relative Power Ratio (RPR), and Brain Symmetry Index (BSI). These parameters are important for analyzing various electrical brain activities including confirmation of acute ischemic stroke and EEG biofeedback analysis for stroke rehabilitation. The data acquisition system is using Raspberry Pi 3 and Front-End Analog to Digital Converter (ADC) ADS1299EEG-FE to stream the data that will be processed and displayed in the MATLAB-based GUI.

Hiba Abdel-Nabi [9] proposed that in this scheme an efficient crypto-watermarking algorithm is proposed to secure medical images transmitted in tele-medicine applications. The proposed algorithm uses standard encryption methods and reversible watermarking techniques to provide security to the transmitted medical images as well as to control access privileges at the receiver side. The algorithm jointly embeds two watermarks in two domains using encryption and reversible watermarking to avoid any interference between the watermarks. The authenticity and integrity of medical images can be verified in the spatial domain, the encrypted domain, or in both domains. The performance of the proposed algorithm is evaluated using test medical images of different modalities. The algorithm preforms well in terms of visual quality of the watermarked images and in terms of the available embedding capacity. Further A separable joint crypto data hiding algorithm has been proposed in this work.

Tamás Ferenci [10] many biomedical data are available as time series, especially in the field of public health and epidemiology, where indicators are usually collected over time. Clinical studies with long follow-up are also sometimes best analyzed with time series methods. The analysis of administrative health care data often gives rise to time series problems too, as events are frequently converted to counts over a given interval. Finally, some biomedical measurements also may be viewed as time series, such as ECG recordings. The methods of time series analysis can be very broadly divided into two categories: time-domain and frequency domain methods. Frequency-domain methods are based on converting the time series, classically using Fourier transform, to a form where the time series is represented as the weighted sum of sinusoids. This so-called spectral analysis allows us to get insight into the periodic components of the time series, making it possible to investigate cyclicity/seasonality of the original data. Fourier transform, however, does not allow the spectrum to evolve over time, so methods were developed which make a trade-off between time resolution and frequency resolution, such as wavelet analysis. In addition to the investigation of periodicity in epidemiologic data, these methods are also widely used in biomedical signal analysis, such as the analysis of ECG recordings

3. ARCHITECTURAL SYSTEM

This scheme adopts a blind digital watermarking detection method based on intelligent learning for outsourced biomedical time series data shown in Fig. 1 and Fig. 2, and this proposed method can extract the embedded watermark without any information from the original watermark. A. Watermark embedding procedure in the embedding scheme, the original signal is divided into a set of frames, and these frames are selected according to a secret key. These selected frames are then separated into two sets of sub-frames by a down-sampling technique four-level wavelet is performed on each of these sub-frame sets. Finally, the watermark data is embedded in to these sub-frames based on modulating mean value relationship of their coefficients in wavelet domain.

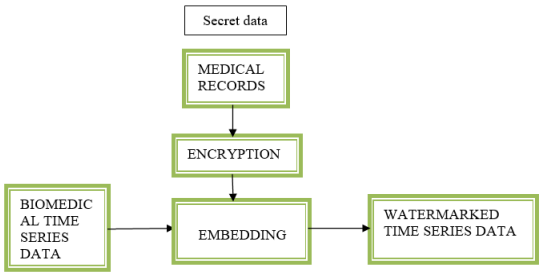

Fig 1. Embedding watermark scheme

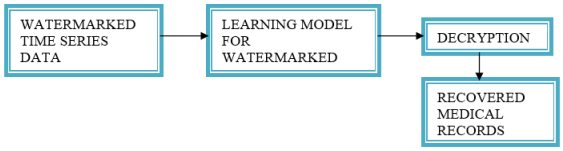

Fig.2 Watermarked extraction scheme

Fig -1: Architectural system

System's architecture basically consists of two phases namely Embedding phase and Extraction phase.

EMBEDDING PHASE-

STEP 1-Biomedical time series data-

In this method, ECG images of patient are taken through online standard websites to create the required database. This database has different types of images which comprises of different patient ECG data images and images are stored in jpeg format. Validation of images are done by experts thus making the training as accurate as possible. To collect this database we are taking help from some of the online websites.

STEP 2- medical records-

It contains the file of patient data which include basic information regarding patients. These files are the set of information of different patient which is the form of .txt file. the concern of this work is to encrypt this file and safely delivered to the destination.

STEP 3-Encryption-

Hiding the patient information into certain code which is unpredicatble to third party is the encryption.

Step 4- Embedding-

An embedding is one instance of some mathematical structured contained within another instance , such as a group that is sub group .when some object X is said to be embedded in another object Y, the embedding is given by some injective and structure preserving map. We can add objects such as file, an image or an audio file to word document.

Step 5- watermarked time series data-

A watermark stored in a data file refers to a method for ensuring data integrity which combines aspects of the data hashing and digital watermarking. Originally a watermark is a more or less transparent image or text that has been applied to a piece of paper, another image to either protect the original image, or to make it harder to copy the item.

EXTRACTION PHASE-

STEP 1-learning model for watermark-

Researchers have developed a technique that embeds watermarked into machine learning models. It uses a digital watermarking technique- embedding and detection, to identify stolen models.

STEP 2-decryption-

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of unencrypting the data.

STEP 3-recoverd medical records-

In this stage we get the original medical records of the patients without any loss of data.

4. EMBEDDING

A. *Watermark embedding procedure*:
In the embedding scheme, the original signal is divided into a set of frames, and these frames are selected according to a secret key. These selected frames are then separated into two sets of sub-frames by a down-sampling technique. After that four-level wavelet is performed on each of these sub-frame sets. Finally, the watermark data is embedded in to these sub-frames based on modulating mean value relationship of their coefficients in wavelet domain. Details of the embedding procedure are as follows:

1) Watermark creation:

The watermark W consists of two components which are reference information T with length n and owner signature I of a binary logo image with size $m = m_1 \times m_2$.

• Step 1a: The binary watermark image I is scrambled by watermarking scrambling algorithm (Arnold transformation) with transform key denoted as K_A in order to dispel the pixel space relationship of the binary watermarking image and to improve the security performance of the whole digital watermarking system. The transformed image is then converted to binary sequence R.

• Step 1b: Combining the reference information *T*, a pseudo-random binary sequence, is used to train learning model during watermarking extraction with binary sequence R to create the watermark represented as $W = TR = w_1,w_2,...,w_n,w_{n+1},...,w_{n+m} = t_1,t_2,...,t_n,r_1,r_2,...,r_m$.

2) *Embedding frame selection*:

• Step 2a: Splitting host biomedical signal S with length L into Si frames ($i = 1, 2,..., M$) with length $2D$, where $M = L/2D$.

• Step 2b: Selecting $(n + m)$ biomedical frames from the above biomedical frames according to a secret key KR to embedded water mark. These biomedical frames consist of two parts where the first part contains reference frames, which are used to embed the reference information T, and the second part contains watermark frames, which are used to embed the owner signature R.

3) *Selected frame modification*:

• Step 3a: Calculating two sub-frames of Si using down-sampling technique, as follows

$$\begin{cases} S_i^1 = s_i(1), s_i(3), \ldots, s_i(2L-1) \\ S_i^2 = s_i(2), s_i(4), \ldots, s_i(2L) \end{cases} \quad (1)$$

• Step 3b: Calculating four-level DWT from sub-frames $\{S^1_k, S^2_k\}$ with $i = 1, 2,..., M$. Let A^1_k and A^2_k denote approximation coefficients of four-level DWT for odd sub-frames and even sub-frames, respectively. We have:

$$\begin{cases} A_i^1 = \{a_i^1(j)\}, \quad \text{and} \quad A_i^2 = \{a_i^2(j)\} \\ j = 1, 2, \ldots, D/16 \\ i = 1, 2, \ldots, M \end{cases} \quad (2)$$

• Step 3c: Computing mean values of approximation coefficients in sub-frames using the following relation:

$$\begin{cases} \mu_i^1 = \dfrac{16}{D}\sum_{j=1}^{D/16} |a_i^1(j)|^2, \quad \text{and} \quad \mu_i^2 = \dfrac{16}{D}\sum_{j=1}^{D/16} |a_i^2(j)|^2 \\ i = 1, 2, \ldots, M \end{cases} \tag{3}$$

4) *Watermark embedding*:

A mean value modulation technique which modulates mean value relationship between two biomedical data sub-frames is employed to carry out watermark embedding. The following modulation strategy will be used to achieve watermark embedding:

1) For each biomedical data frame, only one watermark bit (1 or 0) is embedded.

2) Either 1 or 0 is embedded and fulfilled by modulating all coefficients A^1_i *and* A^2_i such *as* $\mu^1_i \geq \mu^2_i$ or $\mu^1_i \leq \mu^2_i$. The method is called mean relationship modulation in this research.

• Step 4a: Embedding watermark with the following condition: According to mean relationship modulation, let $\Delta\mu = |\mu^1_i - \mu^2_i| + \Delta$ where Δ is a constant

$$\begin{cases} \mu_i^1 \geq \mu_i^2, & \text{if } w_i = 1 \\ \mu_i^1 \leq \mu_i^2, & \text{if } w_i = 0 \end{cases} \tag{4}$$

If the condition is not satisfied we modify it with the following rule:

$$\begin{cases} \bar{\mu}_i^1 = \mu_i^1 + \Delta\mu_i/2,\ \bar{\mu}_i^2 = \mu_i^2 - \Delta\mu_i/2 & \text{if } w_i = 1 \\ \bar{\mu}_i^1 = \mu_i^1 - \Delta\mu_i/2,\ \bar{\mu}_i^2 = \mu_i^2 + \Delta\mu_k/2 & \text{if } w_i = 0 \end{cases} \tag{5}$$

• Step 4b: Modifying all coefficients A^1_i and A^2_i by the following expression

$$\begin{cases} \bar{a}_i^1(j) = \dfrac{a_i^1(j) \times \bar{\mu}_i^1}{\mu_i^1} \\ \bar{a}_i^2(j) = \dfrac{a_i^2(j) \times \bar{\mu}_i^2}{\mu_i^2} \end{cases} \tag{6}$$

where j =1 ,2,...,L/16, i =1 ,2,...,M

5*) Biomedical Signal Reconstruction*:

• Step 5: Applying inverse DWT transform for each biomedical sub-frame to reconstruct and then combining all biomedical frames into the final watermarked biomedical signal S'.

5. EXTRACTION

B. Watermark extraction procedure:

Noise, lossy compression and signal processing can modify the watermarked biomedical data and the modification can be viewed as the corruption to the biomedical data by different noise types. Therefore, from the view of signal processing, watermark extraction problem can be regarded as the problem that watermark signal is extracted from the corrupted biomedical data. In this work, we will present a learning-based watermark detector for biomedical watermarking. Since learning machine has a high capacity of recognition, classification and generalization, it can solve many problems related to watermark extraction process, such as capturing correlation and learning dynamic threshold values. Details of the proposed watermark decoder are presented as follows:

1) *Locating watermark embedded frames*:

• Step 1a: Splitting the received signal S' into S'_i frames (i =1 ,2,...,M) with length 2D.

• Step 1b: Selecting (n + m) biomedical frames from the watermarked biomedical signal according to the same secret key KR as seen in the above embedding procedure. These selected biomedical frames consist of two parts: reference frames (first n biomedical frames) and watermark frames (last m biomedical frames).

2) *Calculating the approximate coefficients*:

• Step 2a: Using down-sampling technique in Eq. (14) to calculate two sub-frames of S'_i frame (S'^1_i and S'^2_i).

• Step 2b: The two sub-frames of each selected biomedical frame are transformed by the four-level DWT decomposition to obtain their approximate sub-band A^1_i and A^2_i, respectively, where *i =1 ,2,...,M.*

3) *Model training*:

We construct a training set T from the first n biomedical frames in which the reference information *R* is embedded. In the training set *T*, an input is composed of all coefficients in $\hat{A}^1_i$ and $\hat{A}^2_i$ while the corresponding output is class label, i.e., reference information bit r_i in R. For convenience, $r_i = 0$ is denoted as $r_i = -1$.

• Step 3a: We construct the training set T from the n reference frames whose reference information $t_1, t_2, \ldots, tn$ has been embedded:

$$\begin{aligned} T &= \{(x_i, y_i) | i = 1, 2, \ldots, n\} \\ &= \{(\tilde{a}_i^1(1), \tilde{a}_i^1(2), \ldots, \tilde{a}_i^1(L/2), \tilde{a}_i^2(1), \tilde{a}_i^2(2), \\ &\ldots, \tilde{a}_i^2(L/2)), r_i | i = 1, 2, \ldots, n\} \end{aligned} \tag{7}$$

where $\tilde{a}_i^1(j) \in \tilde{A}_i^1$, $\tilde{a}_i^2(j) \in \tilde{A}_i^2$, $j = 1, 2, \ldots, L/2$, $i = 1, 2, \ldots, n$

• Step 3b: Machine learning algorithm will be trained using the training set T. In this paper, SVDD will be used with the RBF kernel function as follows:

$$K(x,x_i)=e^{-\gamma||x-xi||2} \quad (8)$$

and the decision function of SVDD can be expressed as follows:

$$y = f(x) = sign\ (R^2 - (K(x,x_i)-c)^2) \quad (9)$$

4) Watermark extraction:
Step 4a: Based on biomedical frames where the owner signature is embedded, we construct an input set as follows

$$\begin{aligned} T' &= \{(x_i'|i = 1, 2, \ldots, n\} \\ &= \{(\widetilde{a}_i^1(1), \widetilde{a}_i^1(2), \ldots, \widetilde{a}_i^1(L/2), \widetilde{a}_i^2(1), \widetilde{a}_i^2(2), \\ &\ldots, \widetilde{a}_i^2(L/2))|i = 1, 2, \ldots, m\} \end{aligned} \quad (10)$$

We then use the well-trained SVDD model in Eq. (8), we can calculate their corresponding output, denoted by $y_i'|i = 1, 2, .., m$.
• Step4b:The embedded owner signature is extracted using the following rules

$$r_i = \begin{cases} 1 & \text{if } \widetilde{y}_i = +1 \\ 0 & \text{if } \widetilde{y}_i = -1 \end{cases} \quad i = 1, 2, \ldots, m \quad (11)$$

5) Binary Image Reconstruction:

• Step 5a: The one-dimensional sequence $r_1, r_2, ..., r_m$ with $m = m_1 \times m_2$ of the owner signature is converted into a two-dimensional encrypted watermark image.

• Step 5b:Then, the watermark image is retrieved by inversely shuffling the image using the same key KA in chaotic encryption

6. RESULTS AND DISCUSSION

The proposed work is implemented on Intel Core processor i5, 4GB RAM Laptop configuration and operating system is windows 7. MATLAB R2016a software is used to write the programming code. In this we used Image processing toolbox and the database of patient data images is collected by taking help from different records of patients.

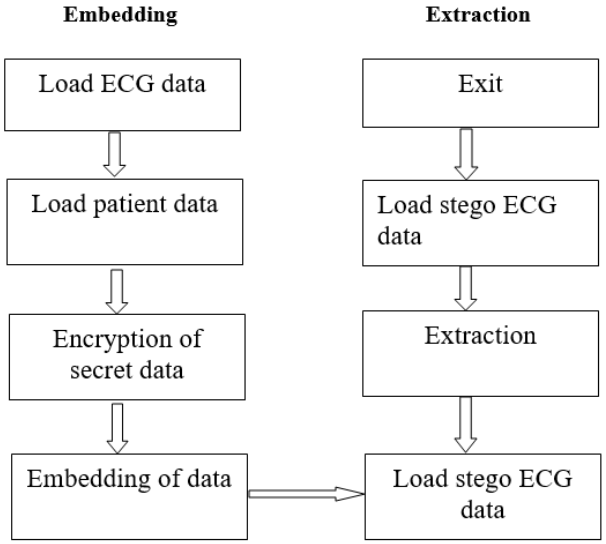

Fig -1: System Flowchart

Table -1: parameters measured from different patient files.

Serial no.	Input data	Stego data	Parameter 1 MSE	P2
Case 1	101.dat	Patient.1 file	0	∞
Case 2	102.dat	Patient.2 file	0	∞
Case 3	103.dat	Patient.3 file	0	∞
Case 4	104.dat	Patient.4 file	0	∞

7. CONCLUSION

An intelligent learning-based watermarking scheme for biomedical data can be develop. The watermark embedding and watermark extraction issues can be treated as a classification problem involving binary classes, and the machine learning algorithm is used to realize watermark extraction. The watermark detector achieved watermark extraction by learning mean modulation relationships in biomedical sub-frames. Due to powerful learning ability and good generalization ability of machine learning, watermark can be exactly recovered under several common attacks. In addition, our watermark scheme possesses the characteristic of blind extraction which does not require the original 8biomedical signal in extraction. The experimental results on ECG data using Arnolds algorithm could be conclude that the proposed watermarking scheme can achieves good imperceptibility and strong robustness against common signal processing.

8. FUTURE SCOPE

Our research can be used in e-healthcare application which need to share and transmit the biomedical data via network with ownership protection purpose. Since information can

be extracted exactly, health information such as patient's data can be embedded in biomedical signal, reducing the consequences of health information thefts, increasing the data security, and saving storage space and bandwidth requirement for transmission of biomedical data. It is obvious that our study is also preferable to facilitate data management in health information management systems

REFERENCES

1. Trung Pham Duy, Dat Tran, and Wanli Ma Faculty of Education, An intelligent learning-based watermarking scheme for outsourced biomedical time series data Science, Technology and Mathematics University of Canberra, ACT 2601. ©2017 IEEE.
2. Elisa Bertino Purdue University bertino@cs.purdue.edu Beng Chin Ooi National University of Singapore ooibc@comp.nus.edu.sg . Privacy and Ownership Preserving of Outsourced Medical Data.
3. Duy, Dat Tran, and Wanli Ma A Proposed Pattern Recognition Framework for EEG-Based Smart Blind Watermarking System 2016 23rd International Conference on Pattern Recognition (ICPR).
4. M. Kamran and Muddassar Farooq A Comprehensive Survey of Watermarking Relational Databases Research arXiv:1801.08271v1 [cs.CR] 25 Jan 2018.
5. XinyueCao,1 ZhangjieFu,1,2 andXingmingSun1,2 A Privacy-Preserving Outsourcing Data Storage Scheme with Fragile Digital Watermarking-Based Data Auditing. Hindawi Publishing Corporation Journal of Electrical and Computer Engineering Volume 2016.
6. Roopam Bamal1 ·Singara Singh Kasana1 Slantlet based hybrid watermarking technique for medical images Received: 9 December 2016 / Revised: 10 April 2017 / Accepted: 1 June 2017 © Springer Science+Business Media, LLC 2017.
7. Hongjun Liu1,2 , Abdurahman Kadir3, Xiaobo Sun4 Chaos-based fast colour image encryption scheme with true random number keys from environmental noise ISSN 1751-9659 Received on 22nd January 2016 Revised 29th December 2016 Accepted on 5th February 2017.
8. Rizki Arif, Sastra K. Wijaya, Prawito, and Hendra Saputra Gani Design of EEG Data Acquisition System based on Raspberry Pi 3 for Acute Ischemic Stroke Identification. 978-1-5386-5689-1/18/$31.00 ©2018 IEEE
9. Hiba Abdel-Nabi Efficient Joint Encryption and Data Hiding Algorithm for Medical Images Security. 978-1-5090-4243-2/17/$31.00 ©2017 IEEE.
10. Tamás Ferenci Biomedical applications of time series analysis. 2017 IEEE 30th Jubilee Neumann Colloquium • November 24-25, 2017.
11. Hadi Latifpour1 • Mohammad Mosleh1 • Kheyrandish1 An intelligent audio watermarking based on KNN learning algorithm Int J Speech Technol (2015) 18:697–706 DOI 10.1007/s10772-015-9318-0.
12. Dat Tran. Ownership protection of outsourced biomedical time series data based on optimal watermarking scheme in data mining. Journal of Information Systems Duy, Tran & Ma 2017, Vol 21, Selected Papers from AusDM.
13. Saman Iftikhar1*, M. Kamran 2 and Zahid Anwar1 A survey on reversible watermarking techniques for relational databases. SECURITY AND COMMUNICATION NETWORKS S e c u rit y C o m m . N e t wo r k s 2015; 8:2580–2603 Published online 28 January 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1196.
14. Ram Pal Singh,IEEE member On Extreme Learning Machine for Watermarking of an Images in Discrete Wavelet Transform Domain. 978-1-4799-5390-5/14 $31.00 © 2014 IEEE DOI 10.1109/IIH-MSP.2014.47.
15. 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.