2016 23rd International Conference on Pattern Recognition (ICPR)
Cancún Center, Cancún, México, December 4-8, 2016

A Proposed Pattern Recognition Framework for EEG-Based Smart Blind Watermarking System

Trung Pham Duy, Dat Tran, and Wanli Ma
Faculty of Education, Science, Technology and Mathematics
University of Canberra, ACT 2601, Australia
Email: dat.tran@canberra.edu.au

***Abstract*—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. Experimental results show that the proposed scheme provides good imperceptibility and more robust against various signal processing techniques and common attacks such as random cropping, noise addition, low-pass filtering, and resampling.**

I. Introduction

Digital watermarking techniques have been used to embed copyright information into the multimedia data without any perceptible differences compared with the original data, and more importantly the embedded information cannot be removed [14]. Since the multimedia data can be duplicated very easily without any quality degradation, copyright protection is of crucial importance [14]. The digital watermarking techniques provide an efficient tool to ensure that the product ownership of the multimedia data is preserved even if the data is processed by such attackers [5].

Current digital watermarking techniques are focused on presenting new modulations in special domains and locating optimal insertion regions to improve the trade-off between imperceptibility and robustness. A watermark is detected using simple correlation-based decision rules [12]. Specific predefined rules for embedding and/or extracting watermark data are used because of their simplicity and low complexity [11]. However, the main disadvantage of these techniques is that they are unintelligent and rule-based, thus they are called non-learning-based watermarking scheme. In these methods, the watermark detection and decoding are often considered separately and mostly decoding performance is declared. One of the major deficiencies of these detectors is that they are dependent on decision threshold and use a series of specific rules but lack of intelligence that undermines their performance. The difficulty in the specification of reasonable detection threshold is a challenge. The detectors are not usually used to directly deal with the data synchronization. Therefore, decoding performance reduces significantly when the watermarked data is transmitted through a real communication channel.

Pattern recognition approach to watermark decoding and/or detection has been recently used to overcome the drawbacks of the correlation-based techniques. These efforts have taken advantage of machine learning and soft computing techniques to conquer those problems, thus designing more robust and intelligent watermarking techniques. These techniques are formed a learning-based watermarking scheme. In [18], a watermark decoding process based on neural network is presented. An watermark is extracted by learning characteristics of the embedded watermark in an audio. Kribiz et al. [9] propose an audio watermark method based on support vector machine (SVM). Watermark decoding and detection problems are combined into a single classification problem.

Electroencephalography (EEG) is a neuroimaging technique for recording the brain's electrical potentials, which are commonly used to study the dynamics of neural information processing in the brain, and diagnose brain disorders and cognitive processes [1]. EEG is also used in telemedicine and brain-computer interface (BCI) applications. The widespread emergence of computer networks and the popularity of electronic managing of medical records have made it possible for digital medical data to be shared across the world for services such as telemedicine, teleradiology, telediagnosis, and teleconsultation [3]. However, there are multiple danger zones like copyright and integrity violations of digital objects [7]. It is well known that the integrity and confidentiality of medical data including EEG data are critical issues for ethical as well for legal reasons. Preliminary research in watermarking or information hiding techniques has been developed for embedding text, images, audio or video in a host signal. However, techniques developed for these data do not transpose well to other data modalities for some reasons such as: 1) The redundancy in a time series of biomedical signals such as EEG and ECG that is less compared with an image or audio. Therefore, embedding data in time series data such as EEG or ECG which has a low redundancy is much more difficult due to the reduced redundancy limiting possibilities of hiding data and has not been investigated; and 2) audio signal has slow time-varying feature while EEG signal is the fast changing-time series.

978-1-5090-4846-5/16/$31.00 ©2016 IEEE

In this paper, we propose a blind watermarking scheme based on pattern recognition network which performs a support vector data description (SVDD)-based supervised learning followed by a blind decoding for 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 SVDD models trained with the correlation between modified frequency coefficients and the watermark sequence in wavelet domain. The main contributions of this research are as follows:

1) An appropriate efficient watermarking algorithm suitable for time series biomedical data such as EEG.
2) Overcoming the limitation of existing watermarking schemes that is based on rule-based without intelligent. The novelty of this method lies in its interpretation of the mean value relationship. Unlike the conventional watermarking methods, in this research, the watermarking embedding and extraction problems are integrated into a unique classification problem and supervised learning of the embedded watermark data in wavelet domain is introduced
3) A new adaptive EEG watermarking detection algorithm based on SVDD learning machine, and this algorithm can extract the watermark without original EEG signals (blind watermarking scheme).
4) Effectively improving robustness of watermarking algorithm under different attacks using learning ability and generalization performance of SVDD.

The effectiveness of the proposed scheme is qualified using metrics like Peak Signal Noise Ratio (PSNR), Normalized Correlation (NC) and Bit Error Rate (BER) to analyze the watermarked signal in terms of imperceptibility and robustness. Experimental results show that our proposed watermarking scheme yields a good imperceptibility and more robust against various signal processing and common attacks.

II. Background

A. Chaotic encryption

Chaotic maps have been used frequently in digital watermarking. Watermark scrambling is used to dispel the pixel space relationship of the binary watermark image and improve the robustness of the whole digital watermark system. Chaotic encryption of the watermark image is performed using Arnold transform [20] also called Cat Face transfer and is given by

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N) \tag{1}$$

where (x, y) is the pixel of the watermark image, (x', y') is the pixel of the watermark image after scrambling. N is order of watermark image matrix. Since the Arnold transform is periodic, the number of scramblings can be considered as the key to enhance the security. In this research, the key for Arnold transform is denoted as Γ_A.

B. Discrete wavelet transform (DWT)

DWT employs extensive time window for low frequencies and short time window for higher frequencies. DWT is widely used for the time-frequency analysis of biomedical signals [13], [8], especially in an EEG signal analysis due to its non-stationary characteristics. As EEG signal is the fast changing-time series with continuous random changes, we use the Haar wavelet which is more suitable for such fast changing time-series compared to Daubechies wavelets, Mexican Hat wavelets and Morlet wavelets which are better suited for smoothly changing time series [15]. In addition, the Haar wavelet is also simple, fast and exactly reversible which is necessary to reconstruct cover signal in digital watermarking. Each wavelet decomposition of the original signal halves the frequency and length of the signal. The Haar function Ψ used as the mother wavelet generates a set of wavelets as follows:

$$C_{a,b} = \sum_{N_{samp}} c(t)\Psi_{a,b}(t) \tag{2}$$

where $\Psi_{a,b}(t) = \frac{1}{\sqrt{s}}\Psi(\frac{t-\tau}{s})$, a denotes the dilation index, b the translation index, s the scale factor and τ the displacement. DWT is basically an application of set of filters resulting in and approximate C_a and fine detailed C_b representation of c.

III. Proposed EEG Watermarking Scheme

Our scheme adopts a blind digital watermarking detection method based on SVDD for EEG data. The proposed method can extract the embedded watermark without any information from the original watermark. Watermarking scrambling algorithm is first used in order to dispel the pixel space relationship of the binary watermarking image and to improve the whole digital watermarking system.

A. Watermark embedding

A watermark W consists of two components which are reference information T with length n and owner signature R of a binary logo image with size $m = m_1 \times m_2$. This binary logo image is scrambled by Arnold transformation with key Γ_A. The reference information T is used to train SVDD during watermarking extraction. Thus the watermark to be embedded can be represented as $W = TR = w_1, w_2, ..., w_n, w_{n+1}, ..., w_{n+m} = t_1, t_2, ..., t_n, r_1, r_2, ..., r_m$.

In the embedding scheme, the original signal is divided into a set of frames and then a down-sampling technique is performed to separate every frame into two sub-frames. Next, four-level wavelet is performed on each sub-frame. Finally, the watermark data is embedded in to the sub-frame based on modulating mean value relationship of their coefficients in wavelet domain. Details of the embedding procedure are as follows:

1) Step 1: Splitting host EEG signal S with length L into S_k frames $(k = 1, 2, ..., K)$ with length $2D$, where $K = L/2D$.

2) Step 2: Calculating two sub-frames of S_k using down-sampling technique is as follows

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

3) Step 3: Selecting EEG frames to embed watermark. To be secure, we randomly select $(n+m)$ EEG frames from K EEG frames according to a secret key Γ_R. The selected EEG frames consist of two parts where the first part is called reference frames, which are used to embed the reference information T, while the second part is called watermark frames, which are used to embed the owner signature R.
4) Step 4: Calculating four-level DWT from sub-frames $S_k^i (i = 1, 2$ and $k = 1, 2, \ldots, K)$. Let A_k^i denote approximation coefficients of four-level DWT, we have:

$$\begin{cases} A_k^i = \{a_k^i(j)\} \\ i = 1, 2 \\ j = 1, 2, \ldots, D/16 \\ k = 1, 2, \ldots, K \end{cases} \quad (4)$$

5) Step 5: Computing mean values of approximation coefficients in sub-frames using the following relation:

$$\mu_k^i = \frac{16}{D} \sum_{j=1}^{D/16} |a_k^i(j)|^2 \quad (5)$$

where $i = 1, 2$, $k = 1, 2, \ldots, K$. A mean value modulation technique which modulates mean value relationship between two EEG sub-frame is employed to carry out watermark embedding. The following modulation strategy will be used to achieve watermark embedding:
   a) For each EEG frame, only one watermark bit (1 or 0) is embedded
   b) Either 1 or 0 is embedded and fulfilled by modulating all coefficients A_k^1 and A_k^2 such as $\mu_k^1 \geq \mu_k^2$ or $\mu_k^1 \leq \mu_k^2$. The method is called mean relationship modulation in this research.
6) Step 6: Embedding watermark with the following condition: According to mean relationship modulation, let $\Delta\mu = |\mu_k^1 - \mu_k^2| + \Delta$ where Δ is a constant

$$\begin{cases} \mu_k^1 \geq \mu_k^2, & \text{if } w_k = 1 \\ \mu_k^1 \leq \mu_k^2, & \text{if } w_k = 0 \end{cases} \quad (6)$$

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

$$\begin{cases} \bar{\mu}_k^1 = \mu_k^1 + \Delta\mu_k/2,\ \bar{\mu}_k^2 = \mu_k^2 - \Delta\mu_k/2 & \text{if } w_k = 1 \\ \bar{\mu}_k^1 = \mu_k^1 - \Delta\mu_k/2,\ \bar{\mu}_k^2 = \mu_k^2 + \Delta\mu_k/2 & \text{if } w_k = 0 \end{cases} \quad (7)$$

7) Step 7: Modifying all coefficients A_k^1 and A_k^2 by the following expression

$$\bar{a}_k^i(j) = (a_k^i(j) \times \bar{\mu}_k^i)/\mu_k^i \quad (8)$$

where $j = 1, 2, \ldots, L/16$, $i = 1, 2$, $k = 1, 2, \ldots, K$
8) Step 8: Each EEG sub-frame is reconstructed through applying inverse DWT transform and all EEG frames are then combined into the final watermarked EEG signal $\widetilde{S}$.

B. Watermark extraction

Since machine learning 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. In watermark extraction procedure, we firstly select $(n+m)$ EEG frames from the watermarked EEG signal according to the same secret key Γ_R as seen in the above embedding procedure. Next, we construct a training set T from the first n EEG frames in which the reference information R is embedded. In the training set T, an input is composed of all coefficients in $\widehat{A}_k^1$ and $\widehat{A}_k^2$ while the corresponding output is class label, i.e., reference information bit r_k in R. For convenience, $r_k = 0$ is denoted as $r_k = -1$. SVDD will be trained using the training set T. Finally, the well-trained SVDD model is used to extract watermark bits. The proposed watermark decoder is presented as follows:

1) Step 1: Splitting the received signal $\widetilde{S}$ into $\widetilde{S}_k$ frames $(k = 1, 2, \ldots, K)$ with length $2L$.
2) Step 2: Using down-sampling technique in Eq.(3) to calculate two sub-frames of $\widetilde{S}_k$ frame $(\widetilde{S}_k^i,\ i = 1, 2)$.
3) Step 3: Selecting EEG frames. According to the same secret key Γ as seen in the above embedding procedure, we select $(n+m)$ EEG frames from all EEG frames. These selected EEG frames consist of two parts: reference frames (first n EEG frames) and watermark frames (last m EEG frames). The two sub-frames of each selected EEG frame are transformed by the four-level DWT decomposition to obtain their approximate subband $\widetilde{A}_k^1$ and $\widetilde{A}_k^2$, respectively, where $k = 1, 2, \ldots, K$.
4) Step 4: Training SVDD
   a) We construct the training set T from the n reference frames whose reference information $t_1, t_2, ..., t_n$ has been embedded:

$$\begin{aligned} T &= \{(x_k, y_k) | k = 1, 2, \ldots, n\} \\ &= \{(\widetilde{a}_k^1(1), \widetilde{a}_k^1(2), \ldots, \widetilde{a}_k^1(L/2), \widetilde{a}_k^2(1), \widetilde{a}_k^2(2), \\ &\quad \ldots, \widetilde{a}_k^2(L/2)), r_k | k = 1, 2, \ldots, n\} \end{aligned} \quad (9)$$

   where $\widetilde{a}_k^1(j) \in \widetilde{A}_k^1$, $\widetilde{a}_k^2(j) \in \widetilde{A}_k^2$, $j = 1, 2, \ldots, L/2$, $k = 1, 2, \ldots, n$
   b) The following RBF kernel is used in SVDD:

$$K(x, x_k) = e^{-\gamma ||x - x_k||^2} \quad (10)$$

   c) The decision function can be expressed as follows

$$y = f(x) = sign(R^2 - (K(x, x_i) - c)^2) \quad (11)$$

5) Step 5: Watermark extraction. Based on EEG frames where the owner signature is embedded, we construct an input set as follows

$$\begin{aligned} \widetilde{T} &= \{(\widetilde{x}_k | k = 1, 2, \ldots, n\} \\ &= \{(\widetilde{a}_k^1(1), \widetilde{a}_k^1(2), \ldots, \widetilde{a}_k^1(L/2), \widetilde{a}_k^2(1), \widetilde{a}_k^2(2), \\ &\quad \ldots, \widetilde{a}_k^2(L/2)) | k = 1, 2, \ldots, m\} \end{aligned} \quad (12)$$

We then use the well-trained SVDD model in Eq. (8) to can calculate their corresponding output, denoted as $\widetilde{y}_k|k = 1, 2, .., m$. Finally, the embedded owner signature is extracted using the following rules

$$r_k = \begin{cases} 1 & \text{if } \widetilde{y}_k = +1 \\ 0 & \text{if } \widetilde{y}_k = -1 \quad k = 1, 2, \ldots, m \end{cases} \tag{13}$$

6) Obtaining watermark image. The one-dimensional sequence $r_1, r_2, ..., r_{m=m1\times m2}$ of the owner signature is converted into a two-dimensional encrypted watermark image. Then, the watermark image is retrieved by inversely shuffling the image using the same key Γ_A in chaotic encryption.

IV. Experimental Results and Discussion

In our experiments, the DEAP dataset (Dataset for Emotion Analysis using Electroencephalogram, Physiological and Video Signals) which is an open database proposed by Koelstra et al. [10] was used as the original EEG signals. The 8 channels (FP1, AF3, F3, FC5, FC1 C3 and T7) of 32 subjects were chosen randomly to test. A binary logo image with size 32x32 will be used as the watermark image shown in Fig.1 (a). The owner signature R is generated from the watermark image by permuting and reshaping into line order, thus $m = 1024$. We carried on several experiments to obtain necessary parameters for our watermarking scheme as follows:

1) Reference information is a pseudo-random binary sequence with length $n = 512$.
2) The length of EEG sub-frame is $D = 64$, and the factor $\Delta = 0.5$.
3) The RBF kernel function $K(x, \widehat{x}) = e^{-\gamma||x-\widehat{x}|^2}$ was used. The parameters for SVDD training are γ and υ, where γ was searched in $\{2^k : k = 2l + 1, l = -8, -7, \ldots, 2\}$ and υ was searched in $\{0.001, 0.01, 0.1\}$. The best parameters found are $\upsilon = 0.1$ and $\gamma = 2^{-3}$.

The performance of the proposed watermarking method is investigated by measuring its imperceptibility and robustness.

An acceptable watermarking technique needs to satisfy two main requirements: imperceptibility and robustness [17]. Imperceptibility refers to perceptual quality of the data being protected. Robustness is the resistance of watermark signal against common signal processing and malicious attacks.

Similar to digital image watermarking, biomedical data such as EEG is based on human visual system (HVS) and is typically analyzed in two ways: 1) Visual inspection by human experts and 2) automatic analysis using processing algorithms. Watermarking techniques need to reconstruct biomedical data without introducing any errors in such analyses. According to [16], biomedical data is mainly used for diagnosis, thus the imperceptibility of the watermark should be as high as possible. Distortions to the original due to the watermark may result in wrong interpretation of the data. Medical signals are not likely to be subject to the same type of malicious attack as downloaded image, audio or video files. However, attacks such as pre-processing signals, or downsampling of large data files to allow more efficient data transmission could be an issue. The robustness of the watermark is verified against different attacks such as low pass filtering, addition of Gaussian noise, different sampling rate, and cropping. It is sufficient if the embedded data is robust to simple signal processing techniques necessary for efficient transmission.

TABLE I: Performance metrics on average for different EEG signal channels of 32 subjects

EEG Channel	PSNR (in dB)	NC	BER
Fp1	70.61	1	0
AF3	65.29	1	0
F3	68.57	1	0
F7	66.18	1	0
FC5	69.46	1	0
FC1	63.16	1	0
C3	64.32	1	0
T7	64.81	1	0
Average	**66.55**	**1**	**0**

A. Imperceptibility

For imperceptibility, PSNR were employed to evaluate the differences between original EEG signals and watermarked EEG signals. It should be noted that the larger PSNR, the better imperceptibility. A larger PSNR value indicates that the watermarked EEG signal more closely resembles its original signal, meaning that watermarked EEG signal has better imperceptibility. According to Chen et al. [4], PSNR above 40 dB indicates a good perceptual fidelity. The PSNR (in dB) of the watermarked EEG are shown in Table 1, all of them are higher than 40 dB, thus this indicates that diagnosability is not lost and degradation to the overall signal is acceptable. It also shows that our watermarked EEG signal is near identical to the original EEG signal (Fig.2).

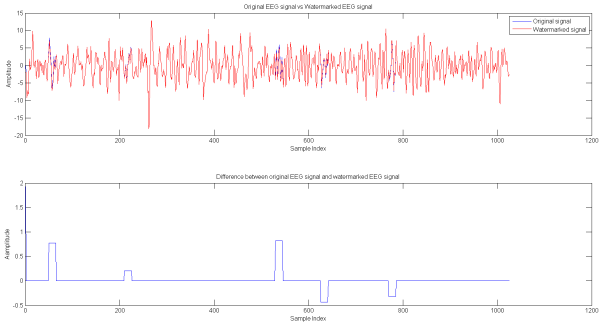
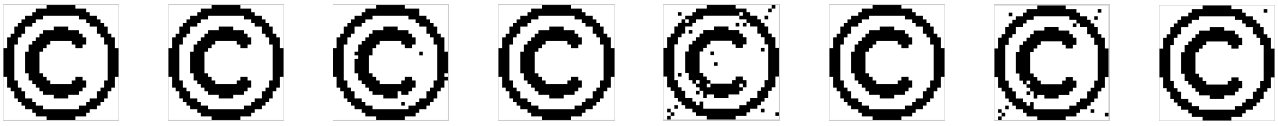


Fig. 2: Original EEG signal vs Watermarked EEG signal (above), Difference between original EEG signal and watermarked EEG signal (below) in channel Fp1, subject 01

B. Robustness

In order to evaluate the robustness of the proposed method against the common signal processing attacks, we used BER



(a) (b) (c) (d) (e) (f) (g) (h)

Fig. 1: Result of watermark extraction at channel Fp1 of subject 01: (a) Original watermark, (b) Free attack, (c) Noise addition, (d) Random cropping at front, (e) Random cropping at middle, (f) Random cropping at end, (g) Low-pass filtering, and (h) Re-sampling.

and NC measures. The following signal attacks were performed in Matlab:

1) Noise addition: Additive white Gaussian noise (AWGN) was added to the watermarked EEG signal with 20dB.
2) Random cropping: In our experiment, 10% samples were removed at each of three randomly selected positions (front, middle and back) of the watermarked signal and then these samples were replaced by the watermarked sample attacked with AWGN.
3) Low-pass filtering: The low-pass filter with cut-off frequency of 40Hz was applied to all watermarked EEG signals.
4) Re-sampling: The original EEG signals were sampled with a sampling rate of 128 Hz. Watermarked EEG signals were resampled at 64 Hz and then restored by sampling again at 128 Hz.

In attack-free case, we extracted watermark from watermarked EEG signals using the proposed watermark extraction algorithm. Table 1 shows $BER = 0$, $NC = 1$ in case of no attack, meaning that watermark can be accurately extracted from the watermarked EEG signal. In addition, the proposed watermarking scheme uses the trained SVDD model to extract the watermark without the original EEG signal, thus our proposed watermarking scheme is blind. As seen from Table 2, after applying MATLAB attacks on watermarked EEG signals, it is observed that the values of BER is very low (less than 3%) while the values of NC is very high (close to one), which implies extracted watermark is very similar to the original watermark. Therefore, this indicates that the robustness of the proposed scheme is very good. In addition, $BER < 3\%$ could be corrected with the use of error correcting codes [19].

The strong robustness of the proposed method benefits from powerful learning ability and good generalization ability of machine learning alogrithm. It is assumed that the watermarked EEG signal may suffer distorted from different signal processing operations or attacks. This results in the change of DWT coefficients of an EEG signal after attacking. Therefore, the requirement of the designed detector should have high ability to detect the watermark under this contaminated environment. In the machine learning point of view, the watermark detection can be realized as an ability of generalization. The EEG watermarking scheme based on pattern recognition using SVDD has good generalization ability, thus improving the robustness of watermarking system.

C. Security

To enhance the security, the proposed method utilizes chaotic encryption. The embedding and extraction processes in the watermarking scheme depends on the secret key Γ_A and Γ_R, it is impossible to malicious attack to detect the watermark without these keys. In addition, the proposed method possesses the high robustness which against attack is very important for a secured watermarking scheme.

D. Error Analysis

The performance of a watermarking system is generally characterized by two types of errors [6], the false-positive error and false-negative error. The the false-positive error is the probability that an unwatermarked EEG signal declared as watermarked by the decoder, while false-negative error is the probability that a watermarked EEG signal declared as unwatermarked by the decoder. The probability of false-

TABLE II: Performance metrics for different EEG signal channels under different attacks

EEG Channel	**Noise Addition**		**Random Cropping**						**Low-pass Filtering**		**Resampling**	
			Front		**Middle**		**End**					
	BER (%)	***NC***	***BER (%)***	***NC***	***BER (%)***	***NC***	***BER (%)***	***NC***	***BER(%)***	***NC***	***BER(%)***	***NC***
Fp1	0.39	0.9969	0	1	0	1	0	1	4.20	0.9662	0.11	0.9905
AF3	0.59	0.9953	0	1	0	1	0	1	3.51	0.9718	3.71	0.9703
F3	0.39	0.9969	0	1	0	1	0	1	0.49	0.9961	0.59	0.9953
F7	0.49	0.9961	0	1	0	1	0.2	0.9992	3.42	0.9726	0.68	0.9945
FC5	0.68	0.9945	0.1	0.9992	0	1	0	1	2.05	0.9836	3.52	0.9717
FC1	0.98	0.9921	0	1	0	1	0	1	2.93	0.9762	2.54	0.9796
C3	0.88	0.9929	0	1	0.2	0.9984	0.17	0.9987	0.10	0.9992	2.44	0.9802
T7	0.49	0.9961	0	1	0	1	0	1	2.68	0.9834	0.39	0.9969
Average	**0.61**	**0.9951**	**0.0125**	**0.9999**	**0.025**	**0.9998**	**0.046**	**0.9997**	**2.42**	**0.9811**	**1.75**	**0.9849**

positive error P_{FP} and probability of false-negative error P_{NE} can be computed as:

$$P_{FP} = 2^{-m} \sum_{h=\lceil \rho m \rceil}^{m} \binom{m}{h} \tag{14}$$

$$P_{FN} = \sum_{h=0}^{\lceil \rho m \rceil - 1} \left[\binom{h}{m} P^h (1-P)^{m-h} \right] \tag{15}$$

where $\binom{m}{h}$ is the binomial coefficient, m is the total number of watermark bits, h is the total number of matching bits, and P is probability of difference between extracted watermark and original watermark ($w \neq w'$). According to [2], the desired false alarm error must be smaller than 10^{-6} order of magnitude. We have $h = \lceil (1 - BER) \times m \rceil$, therefore BER less than 20% meets this demand. If we set $BER = 20\%$, then $\rho = 0.8$. In our method, $m = 1024$, Eq.(14) gives $P_{FP} = 2.6209 \times 10^{-88}$, hence the false positive is close to 0.

In Eq.(15), the approximate value of P can be obtained from the BER under different attacks. As can be seen from Table 1 and Table 2, the average of BER is less than 3%, so P can be taken as 0.97. By substituting the values of m, ρ, and P, Eq. (15) gives $P_{FN} = 1.5286 \times 10^{-102}$. In summary, our experimental results show that the proposed blind watermarking scheme based on pattern recognition for biomedical data has good imperceptibility and strong robustness against several different attacks.

V. Conclusion

A novel blind watermarking scheme based on pattern recognition framework for EEG data has been developed. The watermark embedding and watermark extraction issues can be treated as a classification problem involving binary classes, and the SVDD is used to realize watermark extraction. The watermark detector achieved watermark extraction using SVDD to learn mean modulation relationships in EEG sub-frames. Due to powerful learning ability and good generalization ability of SVDD, 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 EEG signal in extraction. The experimental results have showed clearly that the proposed watermarking scheme achieves good imperceptibility and strong robustness against common signal processing. In the future work we will consider the following problems:

1) Machine learning approach to pattern recognition frameworks has high computation complexity. We will develop a simple learning algorithm and lower computation complexity to improve the performance of the proposed watermarking technique.
2) Implementing the error coding code in watermark extraction.
3) Automatically searching the location which indicates presence of watermark based on BER and NC with some threshold, and secret key Γ_R will be removed, thus improving the convenience for the scheme.

References

[1] Hafeez Ullah Amin, Aamir Saeed Malik, Rana Fayyaz Ahmad, Nasreen Badruddin, Nidal Kamel, Muhammad Hussain, and Weng-Tink Chooi. Feature extraction and classification for eeg signals using wavelet transform and machine learning techniques. *Australasian Physical & Engineering Sciences in Medicine*, 38(1):139–149, 2015.

[2] Vivekananda Bhat, Indranil Sengupta, and Abhijit Das. An adaptive audio watermarking based on the singular value decomposition in the wavelet domain. *Digital Signal Processing*, 20(6):1547–1558, 2010.

[3] Gaurav Bhatnagar and QM Jonathan Wu. Biometrics inspired watermarking based on a fractional dual tree complex wavelet transform. *Future Generation Computer Systems*, 29(1):182–195, 2013.

[4] Tung-Shou Chen, Chin-Chen Chang, and Min-Shiang Hwang. A virtual image cryptosystem based upon vector quantization. *Image Processing, IEEE Transactions on*, 7(10):1485–1488, 1998.

[5] Ingemar J Cox and Matt L Miller. The first 50 years of electronic watermarking. *EURASIP Journal on Advances in Signal Processing*, 2002(2):1–7, 2002.

[6] Mingquan Fan and Hongxia Wang. Chaos-based discrete fractional sine transform domain audio watermarking scheme. *Computers & Electrical Engineering*, 35(3):506–516, 2009.

[7] Akshya Kumar Gupta and Mehul S Raval. A robust and secure watermarking scheme based on singular values replacement. *Sadhana*, 37(4):425–440, 2012.

[8] Pari Jahankhani, Vassilis Kodogiannis, and Kenneth Revett. Eeg signal classification using wavelet feature extraction and neural networks. In *Modern Computing, 2006. JVA'06. IEEE John Vincent Atanasoff 2006 International Symposium on*, pages 120–124. IEEE, 2006.

[9] Serap Kirbiz and Bilge Gunsel. Robust audio watermark decoding by supervised learning. In *Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings. 2006 IEEE International Conference on*, volume 5, pages V–V. IEEE, 2006.

[10] Sander Koelstra, Christian Mühl, Mohammad Soleymani, Jong-Seok Lee, Ashkan Yazdani, Touradj Ebrahimi, Thierry Pun, Anton Nijholt, and Ioannis Patras. Deap: A database for emotion analysis; using physiological signals. *Affective Computing, IEEE Transactions on*, 3(1):18–31, 2012.

[11] Hadi Latifpour, Mohammad Mosleh, and Mohammad Kheyrandish. An intelligent audio watermarking based on knn learning algorithm. *International Journal of Speech Technology*, 18(4):697–706, 2015.

[12] Henrique S Malvar and Dinei AF Florêncio. Improved spread spectrum: a new modulation technique for robust watermarking. *Signal Processing, IEEE Transactions on*, 51(4):898–905, 2003.

[13] Umut Orhan, Mahmut Hekim, and Mahmut Ozer. Eeg signals classification using the k-means clustering and a multilayer perceptron neural network model. *Expert Systems with Applications*, 38(10):13475–13481, 2011.

[14] Hong Peng, Bing Li, Xiaohui Luo, Jun Wang, and Zulin Zhang. A learning-based audio watermarking scheme using kernel fisher discriminant analysis. *Digital Signal Processing*, 23(1):382–389, 2013.

[15] Donald B Percival and Andrew T Walden. *Wavelet methods for time series analysis*, volume 4. Cambridge university press, 2006.

[16] B Planitz and A Maeder. Medical image watermarking: a study on image degradation. In *Proc. Australian Pattern Recognition Society Workshop on Digital Image Computing, WDIC*, 2005.

[17] George Voyatzis and Ioannis Pitas. The use of watermarks in the protection of digital multimedia products. *Proceedings of the IEEE*, 87(7):1197–1207, 1999.

[18] Chong Wang, Xiaohong Ma, Xiangping Cong, and Fuliang Yin. An audio watermarking scheme with neural network. In *Advances in Neural Networks–ISNN 2005*, pages 795–800. Springer, 2005.

[19] Stephen B Wicker. *Error control systems for digital communication and storage*, volume 1. Prentice hall Englewood Cliffs, 1995.

[20] Dong Zheng, Yan Liu, Jiying Zhao, and Abdulmotaleb El Saddik. A survey of rst invariant image watermarking algorithms. *ACM Computing Surveys (CSUR)*, 39(2):5, 2007.