Reversible Watermarking On Medical Data

Deeksha Sharma, Abdul Khalid, Shradha Parashar

Abstract

Reversible watermark has drawn lots of interest recently. Different from other types of digital watermarks, a reversible watermark has a special feature that the original content can be completely restored. These files as any digital asset should be protected from unwanted modification of their contents, especially as they contain vital medical information. Thus their protection and authentication seems of great importance and this need will rise along with the future standardization of exchange of data between hospitals or between patients and doctors. In specific, the focus is on Electroencephalogram (EEG) Signal and how to embed numerical metadata within the data. This project describes a high capacity and high quality reversible watermarking method based on difference expansion and pixel selection. The privacy of the embedded data is assured because the private metadata will not directly embed on the data, but instead embed a surrogate random sequence, that is generated by a cryptographically safe pseudorandom number generator (PRNG) using the metadata as the input and a secret key as the seed. Hence, avoid leaking or revealing any information about the patient's sensitive information to the public. Even though the privacy of sensitive data attributes can be addressed through encryption, such an approach is inherently a blocking factor in data dissemination. This technique is then adapted here for interleaving patient information and message authentication code with medical data in a reversible manner, that is using lossless compression. The resulting scheme enables on a side the exact recovery of the original data that can be unambiguously authenticated, and on the other side, the patient information to be saved or transmitted in a confidential way. The redundancy in the digital content is used to achieve reversibility.

Keywords— **Difference Expansion, PRNG, LFSR, Watermarking**

1. I. Introduction

In digital watermarking, an invisible watermark is embedded into a digital content for the purpose of copyright The primary applications of watermarking are to protect copyrights and integrity verification [2]. The main reason for protecting copyrights is to prevent image piracy when the communication and protection, content authentication, counterfeit deterrence, forensic tracking, connected content or broadcast monitoring, etc [1].

Deeksha Sharma*, Computer Science Department, Noida institute of engineering and technology Gr.Noida, India.*

Abdul Khalid*, Computer Science Department, Noida institute of engineering and technology Gr.Noida, India.*

Shradha Parashar*, Computer Science Department, Institute of Technology & Management, Aligarh, India.*

transmitter sends it on the internet [3]. For integrity verification, it is important to ensure that the medical image originated from a specific source and that it has not been changed, manipulated or falsified. Medical data are stored for the following three purposes: [4].

- Diagnosis
- Database
- Long-term storage

Since an obtained medical data must be kept perfectly without any loss of information before the data is diagnosed by a doctor, the data should be compressed by lossless algorithm or should be stored without using compression. Note that a data compressed by lossless algorithm can be restored completely at the cost of low compression rate, while lossy algorithm loses information of the data in some degree in order to achieve high compression rate. When the data is diagnosed by a doctor at distant site, it cannot be exposed to public by using secured channel to transmit it [5, 6]. However, since any person with privilege can access to data which are contained in database and can modify them maliciously, the integrity of the data must be protected by using watermarking, which is called integrity watermark. Meanwhile, web-based database system contains valuable medical data resources for not only research purpose but also commercial purpose [8]. Therefore the copyright and intellectual property of the database should be also protected by a watermark, which is called copyright watermark [9]. Moreover, for long-term storage, the protection of the integrity and copyright of data is also critical issue [10]. First, when a person ("archiver") stored a data in the long-term storage system long ago and a different person ("viewer") refers to the data, the viewer can confirm the integrity of the data only through a watermark embedded in the data. Second, when a patient does not want his/her medical images open to the public; the copyright of the data is thought to belong to the patient. Therefore the patient can protect the copyright of the data by using watermarking.

II. Proposed Methodology

In order to embed metadata within the medical image/signal, utilize notions from data watermarking and channel coding. The sensitive metadata (social security number (SSN), birth date, and so on) will be embedded as a hidden watermark within the medical measurements of the patient. In order to provide additional protection and data resilience the watermark is first encrypted than embedded. The embedding will introduce virtually no distortion. An overview of this architecture is provided in Fig 1.

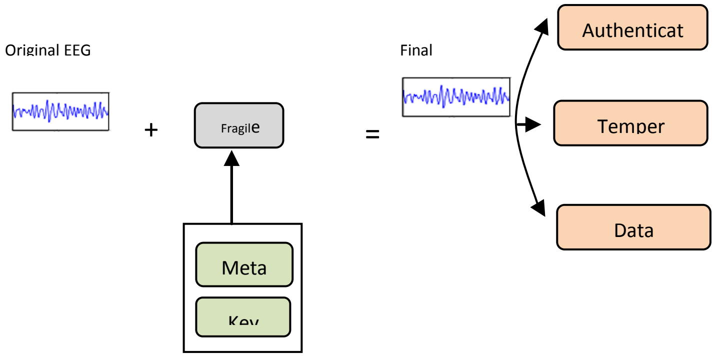


Fig 1: Overview of approach for signals

Once the metadata are effectively fused within the medical signal, there are three supported modes of operation:
1) Tamper Detection by examining the presence of the fragile watermark.
2) Data Authentication through correlation with the originally embedded metadata. For example, if the SSN of a patient is embedded in an EEG signal, then using the SSN and a secret, one can verify that the data indeed belong to the patient with a specific Social Security Number.
3) Data Retrieval. The rightful owner of the data can provide the secret key to someone else, who is now at a position to retrieve the embedded metadata from the medical signal.

III. Approach Used

In the proposed paper a multilevel of security is provided. The technique is based on a message being encoded and hidden in a data in wavelet domain in such a way as to make the existence of the message unknown to an observer shown in fig 2. The encryption of watermark, while being able to maintain a high level of security for the patient identity. Only those individuals with a key will be able to know the identity of the patient. To increase the security the data is embedded into transformed domain. After transformation the signal/image is divided into two bands, first is low frequency band and second is high frequency band. The low frequency band contains important information of the signal and high frequency band contains relatively less information of signal. Most of the attacks are done onto high frequency band as the attackers do not want to harm the high information areas as shown in fig 1. For this purpose lifting based integer wavelet transform is used. The algorithm organizes wavelet coefficients to generate wavelet blocks, and applies a novel method to classify these wavelet blocks based on human visual system (HVS). The watermark is first encrypted and then converted in to form of zero and one. The watermark is pseudo randomly distributed over the transformed signal. The extraction is done same as encryption in reverse manner. The receiver picks the watermark sample bits and decrypts them shown in fig 3.

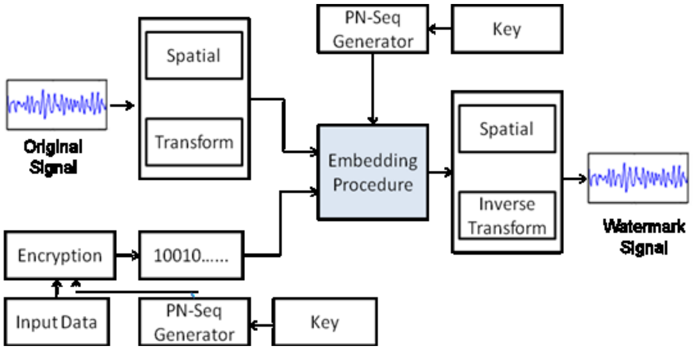


Fig 2: Watermark Embedding Procedure for Signals

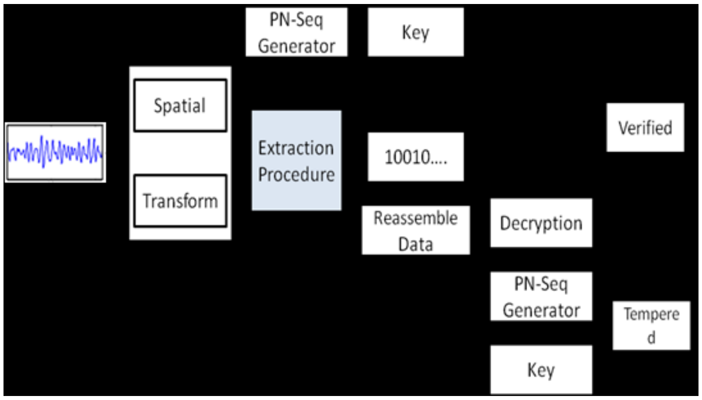


Fig 3: Watermark Extraction Procedure

A) *Watermark Construction*

Let us describe now how the private metadata are embedded into the hidden watermark. The social security number (SSN) of the patient is used as watermark. The SSN of patient is available in decimal number. This number is encrypted using 8 bit PN sequence. The number is modulo 2 added with the generated PN sequence. The encrypted watermark sequence is converted from decimal to binary. The basic procedure is shown in the fig 4

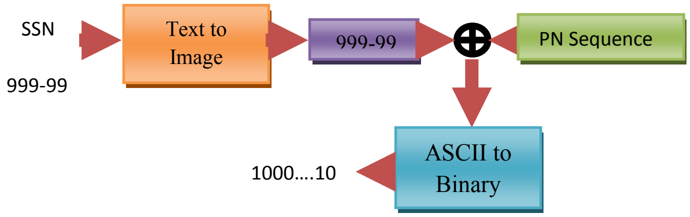
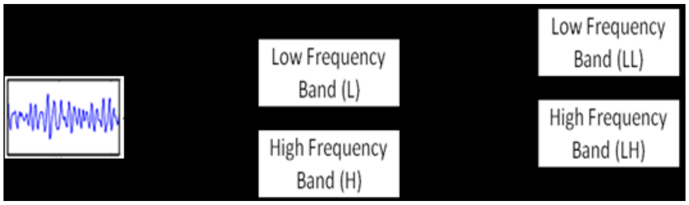


Fig 4 : Encrypted watermark in binary format

B) *Lifting Based Integer Wavelet Transform*

The wavelet transform is a valuable tool for Multi resolution analysis that has been widely used in image processing applications [11]. The wavelet transform has a number of advantages over other transforms as it provides a multi resolution description, it allows superior modeling of the HVS, the high-resolution sub bands allow easy detection of features such as edges or textured areas in transform domain. In the transform coding of signal, the signal is projected onto a set of basis functions, and the resultant transform coefficients are encoded. Efficient coding requires that the transform compact the energy into a small number of coefficients. The LWT transform the signal into two band, low frequency and high frequency band shown in fig 5. In this work one level decomposition of signal is done. Second level decomposition can also be used but the embedding capacity will be decrease.



1st level decomposition 2nd level decomposition

Fig 5: 2 level Wavelet Decomposition

C) Pseudorandom Bits sequence Generator

True random bit generator requires a naturally occurring source of randomness. Designing a hardware device or software program to exploit this randomness and produce a bit sequence that is free of biases and correlations is a difficult task. Additionally, for most cryptographic applications, the generator must not be subject to observation or manipulation by an adversary. So pseudorandom bit generator is used to create a sequence of bits that appears to be random, here LFSR is used to generate PN sequence. LFSR based stream cipher circuit give good data security for low cost secure communication[13].

A ***linear feedback shift register*** is a register of bits that performs discrete ***step*** operations that

- Shift all the bits one position to the left and
- Replace the vacated bit by the ***modulo two addition*** of the bit shifted off and the bit at a given ***tap*** position in the register shown in the fig 6.

Linear feedback shift registers (LFSRs) are used in many of the key stream or bit sequence generators that have been proposed in the literature. There are several reasons for this [14]:

1. LFSRs are well-suited to hardware implementation;
2. They can produce sequences of large period;
3. They can produce sequences with good statistical properties; and
4. Because of their structure, they can be readily analyzed using algebraic techniques.

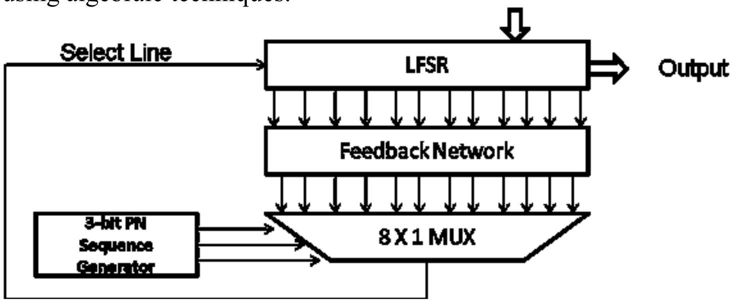


Fig 6: Working of LFSR

In an LFSR, the bits contained in selected positions in the shift register are combined in some sort of function and the result is fed back into the register's input bit. By definition, the selected bit values are collected before the register is clocked and the result of the feedback function is inserted into the shift register during the shift, filling the position that is emptied as a result of the shift.

The feedback function in an LFSR has several names: XOR, odd parity, sum modulo 2. Whatever the name, the function is simple: 1) Add the selected bit values, 2) If the sum is odd, the output of the function is one; otherwise the output is zero.

The bit positions selected for use in the feedback function are called "taps". The list of the taps is known as the "tap sequence". By convention, the output bit of an LFSR that is n bits long, the feedback tapping are kept changing which make the generated code quite complex.

The following tables contain m-sequence feedback sets for LFSR,

Selection	LFSR Tapping
1	[12, 11, 10, 4]
2	[12, 11, 10, 2]
3	[12, 11, 8, 6]
4	[12, 11, 7, 4]
5	[12, 10, 9, 3]
6	[12, 10, 5, 4]
7	[12, 9, 8, 5]

Table 1: Tapping Sequences

Some tests are performing on the 10000 sample of random numbers. For this purpose a NIST test suit is used. Some of the test which are successful are shown as follows.

a) Test for the Longest Run of Ones in a Block

Description: The focus of the test is the longest run of ones within M-bit blocks. The purpose of this test is to determine whether the length of the longest run of ones within the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence]. Note that an irregularity in the expected length of the longest run of ones implies that there is also an irregularity in the expected length of the longest run of zeroes. Long runs of zeroes were not evaluated separately due to a concern about statistical independence among the tests.

b) Non Overlapping Template Matching Test

Description: The focus of this test is the number of occurrences of pre-defined target substrings. The purpose of this test is to reject sequences that exhibit too many occurrences of a given non-periodic (aperiodic) pattern. For this test and for the Overlapping Template Matching test, an m-bit window is used to search for a specific m-bit pattern. If the pattern is not found, the window slides one bit position. For this test, when the pattern is found, the window is reset to the bit after the found pattern, and the search resumes.

c) Lempel Ziv Complexity Test

Description: The focus of this test is the number of cumulatively distinct patterns (words) in the sequence [43]. The purpose of the test is to determine how far the tested sequence can be compressed. The sequence is considered to be nonrandom if it can be significantly compressed. A random sequence will have a characteristic number of distinct patterns.

d) Test for frequency within a Block

Description: The focus of the test is the proportion of zeroes and ones within M bit blocks. The purpose of this test is to determine whether the frequency of ones is an M-bit block is approximately M/2.

e) Random Excursion variant test

Description: The focus of this test is the number of times that a particular state occurs in a cumulative sum random walk. The purpose of this test is to detect deviations from the expected number of occurrences of various states in the random walk.

D) Watermarking Techniques

Compared with other watermarking technique this work is based on transforming the signal domain from spatial domain to transform domain via integer wavelet transform. The integer wavelet transform is used because it is lossless and also removes the irregular redundancy between the signals. As illustrated in fig 1, the watermark is embedded in to signal M and obtained a watermarked signal M'. Before sending it to content authenticator, the signal M' has to be altered or tampered by some intentional attacker or might not. If the authenticator finds that there is no alteration perform on signal M', the authenticator will remove the watermark to retrieve the original content of the signal, which result a new signal M''. by the definition of reversible watermark, the retrieved signal M'' will be exactly same as original signal M.

In this method, the payload will embed in the difference of the signal value. For a pair of signal values (x,y) in a EEG signal, define their interger average l and difference h as $l = \frac{x+y}{2}$, h = x-y (1)

Where lower bound of the average is selected.

$x' = l + \left\lfloor\frac{h+1}{2}\right\rfloor, y' = l - \left\lfloor\frac{h}{2}\right\rfloor$ (2)

The least significant bit (LSB) of the difference number h will be selected embedding area. As h= [h/2].2+LSB(h) (3)

With LSB(h)=0 or 1, to prevent any overflow and underflow problems, we embed only in changeable difference numbers. In the binary representation the integer, an expandable h could add one extra bit b after its LSB, with b=0 or 1. More precisely, h could be replaced by a new difference number h'=2h+b, without causing an overflow and underflow. Thus for each expandable difference number, one could gain one extra bit. The reversible expandable operation from h to h' is called difference expansion.

For a digital signal, pair consists of two neighboring values or two with a same difference number. The pairing could be done horizontally, or by a key based pattern. The paring could be through all values of the signal or just a portion of it. In this paper payload is embedded with one pair, then on the embedded signal, and then embed another payload with another pairing and so on. An integer wavelet transform is applied on each pair.

Ex. Suppose we have two sample values (x,y), Where x,y ϵ Z and we would like to embed one bit b, where b ϵ (0,1) into (x,y) into a reversible way. More specifically, let's assume X=3, y=5 and b=0

Step1: Compute average l of x and y i.e l= $\left\lfloor\frac{x+y}{2}\right\rfloor$

Step 2: Compute difference h of x and y i.e h=|x-y|.

Step 3: Convert decimal h into binary and store in a variable code.

Step 4: put bit b into next to LSB position into c and store in a variable code'.

Step 5: Compute new sample value x' and y' as x'=l + $\left\lfloor\frac{h+1}{2}\right\rfloor$ and y'= l-. $\left\lfloor\frac{h}{2}\right\rfloor$

This process can also be depict as follows

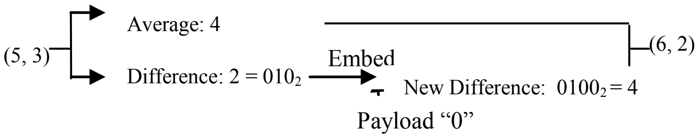


Fig 7: Reversible Watermark Process

IV. Experimental Result and Discussion

The experiments were carried out in 60 sec data of EEG Signal. The robustness of the data to various medical signal processing operations was evaluated using BER. The BER is evaluated by varying the strength of each degradation process. In the proposed method the BER was observed to be zero. The embedded signal is perceptually identical to the original under normal observation. In order to determine the degradation in the embedded image with respect to the host signal, metrics namely, PSNR, MSE are used to measure the distortion produced after embedding process. The signature is used as image. The experimental results are shown fig 7.

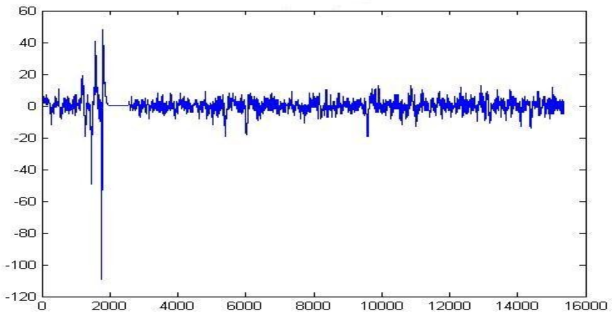


Fig 7: Original EEG signal of 60 sec

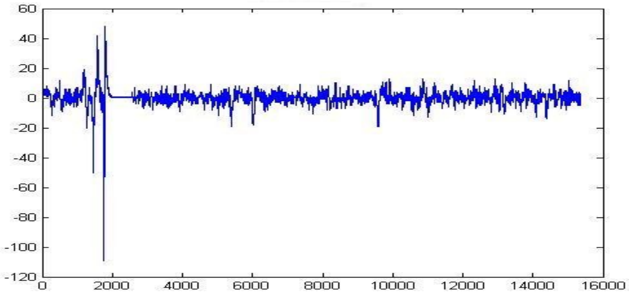


Fig 8: Watermark Signal

Fig 9: Signature to be embedded

A) Time Analysis

The quality assessment of the watermarking technique is done to measure the amount of the time required to embed and to extract the data. Lower the time required means better technique as shown in figure 10. The time required by the LSB method to embed and extract the watermark signature is very less.

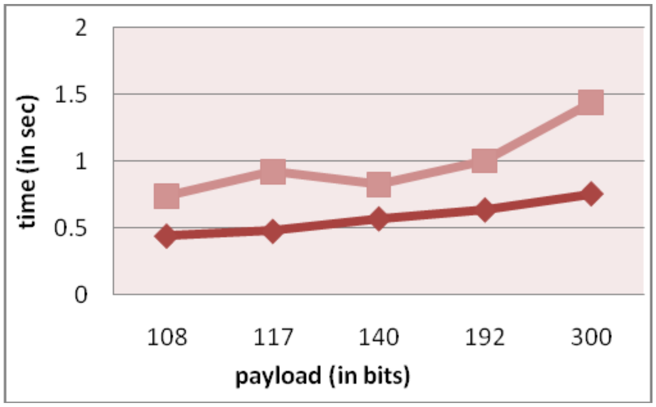


Fig 10: Time require embedding watermark

Indicators:

LSB Method

Reversible Method

	Input data size	LSB	Reversible Method
1	60	0.5365	0.5609
2	70	0.5460	0.5464
3	80	0.5500	0.4103
4	90	0.5477	0.5628
5	100	0.5550	0.5665

Table 2: Time require embedding watermark

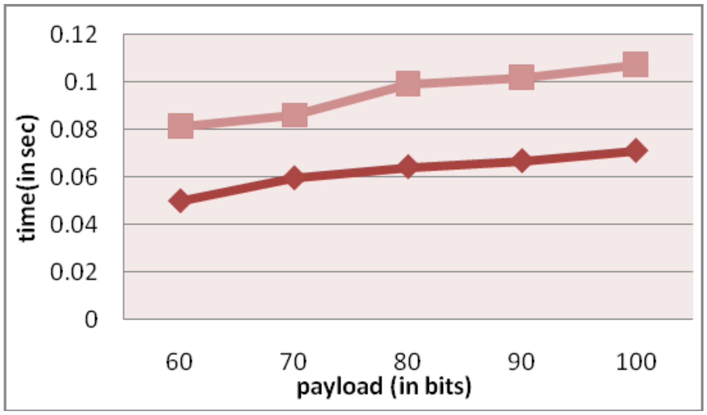


Fig 11: Time require extracting watermark

S no.	Input data size	LSB	Reversible Method
1	60	0.0499	0.0814
2	70	0.0595	0.0860
3	80	0.0642	0.0540
4	90	0.0667	0.1017
5	100	0.0710	0.1073

Table 3: Watermark Extraction Time Analysis,

B) Peak Signal to Noise Ratio (PSNR)

The quality assessment of a signal after embedding is done to measure the amount of distortion due to data hiding. PSNR penalizes the visibility of noise in a signal. It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Values over 40 dB in PSNR are acceptable in terms of degradation, which means no significant degradation is observed by human eye. The proposed method has a higher PSNR of 46 dB shown in figure 12. Higher is the PSNR, the manner is the difference between the original and embedded signal.

PSNR = 10. log10 (MAXi2/MSE)

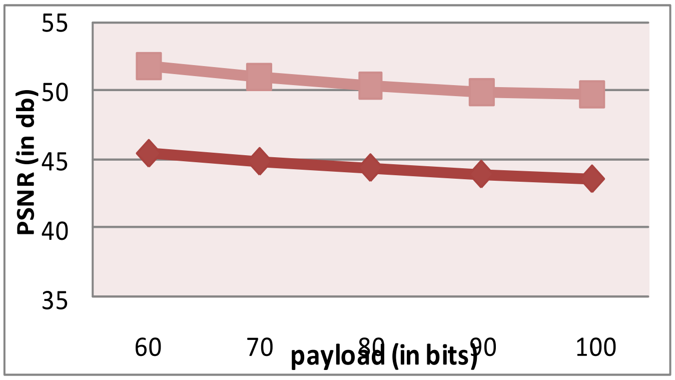


Fig 12: PSNR analysis

S no.	Input data size	LSB	Reversible Method
1	60	45.3903	51.9669
2	70	44.8185	51.0327
3	80	44.3709	50.4781
4	90	43.9098	49.8777
5	100	43.5754	49.4465

Table 4: Peak Signal to Noise Ratio Analysis

C) Mean Square Error

In statistics, the mean squared error (MSE) of an estimator is one of many ways to quantify the difference between values implied by the data hiding and the true values of the signal. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. MSE measures the average of the squares of the "errors". The difference occurs because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate. The experimental results shown in figure 13.

$$\mathrm{MSE} = \frac{1}{m} + \sum_{i=0}^{m-1} [I(i) - K(i)]2$$

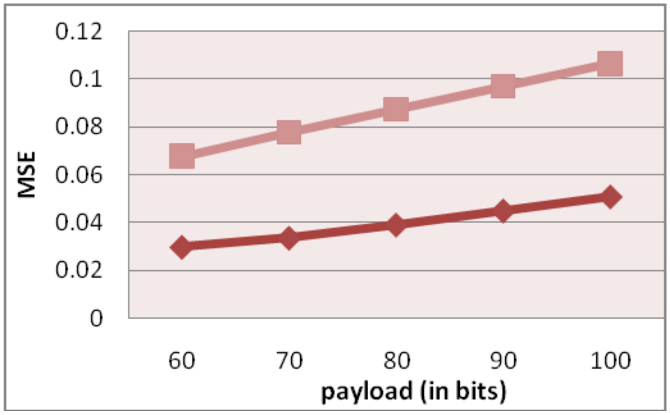


Fig 13: Mean Square Error Analysis on Signal

S no.	Input data size	LSB	Reversible Method
1	60	0.0146	0.0330
2	70	0.0182	0.0385
3	80	0.0206	0.0432
4	90	0.0237	0.0491
5	100	0.0262	0.0538

Table 5 : Mean Square Error Analysis

D) Noise attack

Noise Attack as a result of transmission of the data embedded image through the channel, channel noise could get added to the embedded signal which could affect the accuracy of recovery of data at the receiver end. To study the effect of channel noise, AWGN noise was generated with certain SNR, added to the embedded image to get the signal distorted due to the noise. The spread based technique performs quite well in the case of noise contaminated signal as compare to other digital watermarking technique. When payload is taken in the form of image the BER is relatively less (robust), the data can be retrieve in this case but when payload is taken in text, it is very fragile against minor changes shown in figure 14.

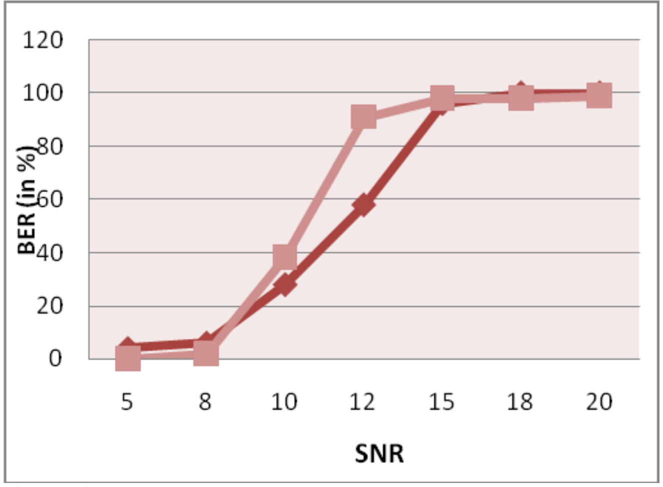


Fig 14: Bit Error Rate

E) Filter Attack

An intruder can harm the signal. The signal can low pass or high pass the signal using any filter. In this case the if the signal is low pass the watermark will exactly recovered if embedding is perform on transformed signal. But the spatial domain watermarking will not result properly in filter attack.

Signal
Low Pass Filter
Low Frequency

Fig 15: Filter Attach Basics

F) Payload Capacity

It is measure of describing the capacity of watermarking algorithm as how much data can be embedded into a signal and extracted without a data loss. The payload capacity of reversible technique is high as shown in figure 16.

Capacity Increases
LSB
Reversible Method

Fig 16: Payload capacity

V. Conclusion

In this project a high capacity, high quality, reversible watermarking method is introduced. An signal is partitioned into pairs of pixels value, the expandable difference number for difference expansion is done. By exploring the redundancy in the signal reversibility is achieved. As difference expansion brings extra storage space, compression is not necessary. Of course employing compression can either increase the hiding capacity or reduce visual quality degradation of data.

In this work the metadata embedding within medical time-series data is done. Here shown that this embedding does not distort the visual appearance of the medical signale and it also does not induce any changes in the diagnosis. On a technical level the following contributions are offer:

- Effectively combine watermarking and channel coding schemes for providing the sufficient resilience on the metadata retrieval
- Robust technique with localized fragile watermarks that can pinpoint the type and location of a potential tampering
- Finally, evaluate the robustness of the proposed schemes under various transformations and attacks using publicly available EEG datasets.

In this work, novel blind data hiding technique in medical signal using integer wavelet transform is done i.e. there is no need of original signal to find out the watermark from the watermarked signal. The method allows the simultaneous extraction of data to keep the patient's information secret on the other hand at same time ensure the integrity of the medical signal. The level of security is increased by encrypting the watermark data before adding to the host signal. The experimental results have shown that the proposed watermark in a transformed domain is invisible to human eyes and very robust to various attacks. In spatial domain, the implemented watermarking is very fragile against attacks but imperceptible. Simulation results show that the selection of bands to embed the watermark is very important (in this case best band is Low band). As the low band contains the high information so the attacker doesn't want to harm that high information area. The obtained result shows higher value of PSNR, and very less BER in noisy signal. Thus the visual quality is superior compared to the existing data hiding methods.

References

[1] M kallel., I Fourati and M.S. Bouhlel. "Medical Image Watermarking Scheme for preserving the image history". 2nd IEEE International Conference on Information and Communication Technologies from Theory to Applications (ICTTA'06), 24-28 April 2006, Damascus Syria

[2] C.Rey and J.L.Dugelay, "an overview of watermarking algorithms for image authentification", Technical Report, Institut EURECOM, Sophia Antipolis, France, 2002.

[3] Chu H, Qiao L, Nahrstedt K. "Secure multicast protocol with copyright protection". ACM SIGCOMM Comput Commun Rev 2002;32(2):42–60.

[4] Jacob Str¨om and Pamela C. Cosman, "Medical Image Compression with Lossless Regions of Interest", Signal Processing, 59, 1997

[5] KT Dockray, "Software for Online Telemedicine Reporting", Proc. 11th IEEE Symposium on Computer-Based Medical Systems, 1998

[6] Myron Frommer, "Telemedicine: The Next Generation is Here", Proc. Working Conference on Research Challenges, 2000

[7] Laura Pierucci and Enrico Del Re, "An Interactive Multimedia Satellite Telemedicine Service", IEEE Multimedia, Vol.7, No.2, pp.76–79, 2000

[8] Jana Dittman and Frank Nack, "Copyright - Copywrong", IEEE Multimedia, Vol.7, No.4, pp.14–17, 2000

[9] Weidong Cai, Dagan Feng and Roger Fulton, "Webbased Digital Medical Images", IEEE Computer Graphics and Applications, Vol.21, No.1, pp.44–47, 2001

[10] Bruce Davie, Valerie Florence, Andrew Friede, Jerry Sheehan and James Sisk, "Bringing Health-Care Applications to the Internet", IEEE Internet Computing, Vol.5, No.3, pp.42–46, 2001

[11] J. B. Feng, I. - C. Lin, C. S. Tsai, and Y. P. Chu, "Reversible watermarking: Current Status and Key Issues", International Journal of Network Security, vol. 2, pp. 161-171, May 2006.

[12] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding", in Proc. International Conference on Image Processing, New York, 2002, pp. 157-160.

[13] J. Tian, "Reversible data embedding using a difference expansion", IEEE Transactions on Circuit Systems and Video Technology, vol.13, pp. 890-896, Aug. 2003.

[14] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding", IEEE Transactions on Image Processing, vol. 14, pp. 253-266, Feb. 2005.

Deeksha Sharma was born in India in August 1990. She has completed graduation in Information Technology from Aligarh college of Engineering and Technology, Aligarh India in 2011 and pursuing post graduate degree in Software Engineering from Noida institute of engineering and technology Gr.Noida. Her interest areas are Advanced Digital Signal Processing, Security Application, and Digital Image Processing

Abdul Khalid was born in India in March 1975. He has completed graduation in Computer Engineering from Galgotia College of engineering and technology Gr.Noida, India in 2006 and post graduate degree in Computer Engineering from Galgotia College of engineering and technology Gr.Noida in 2008. He joined the Department of computer Science & Engineering at Noida institute of engineering and technology Gr.Noida, as assistant Professor and has more than 8 years of experience in teaching. He has published 2 papers in National and International Conferences and Journals.

His interest areas are Genetic Algorithm, Software Reliability, Software Engineering.

Shradha Parashar was born in India in June 1988. She has completed graduation in Computer Engineering from Aligarh college of Engineering and Technology, Aligarh India in 2009 and post graduate degree in Computer Engineering from Zakhir Hussain college of Engineering and Technology, AMU, Aligarh. She joined the Department of computer Science & Engineering at ITM , Aligarh, as a assistant Professor and has more than 3 years of experience in teaching. She has published 7 papers in National and International Conferences and Journals.

Her interest areas are Advanced Digital Signal Processing, Security Application, and Digital Image Processing.