IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 8, Aug 2014, 67-76

AN EXPANDABLE BIT METHOD OF REVERSIBLE WATERMARKING TECHNIQUE ON MEDICAL SIGNALS BASED ON PSEUDORANDOM SEQUENCE

ANSHUL SHARMA[1], SHRADHA PARASHAR[2], NISHANT SAXENA[3] & ALOK GOSWAMI[4]

[1]Research Scholar, Department of Electronics & Communication, IEC Grater Noida Uttar Pradesh, India

[2]Research Scholar, Computer Engineering, Zakir Hussain College of Engineering and Technology, AMU Aligarh, Uttar Pradesh, India

[3]Research Scholar, Department of Electronics & Communication, Uttar Pradesh, India

[4]Assistant Professor, Department of Electronics & Communication, IEC Greater Noida, Uttar Pradesh, India

ABSTRACT

Now a days the information is transferred by using internet as it become easy and time saving. In this digital age the content can be easily change, copied & manipulate. In medical it become very crucial to established integrity of signal before utilization as it may cause wrong diagnosis of the patient. By using digital watermarking technique we can ensure the integrity of the signal. Reversible digital watermarking has provided a valuable solution to this problem. Digital watermarking is an act of hiding some information into signals. By using digital watermarking technique we can ensure the integrity of the signal. Once the information is embedded into the signal it will ensure the integrity but also change the signal to some extent. This embedded data will be removed after performing the integrity test. With this in mind, this work proposes techniques for hiding sensitive patient metadata within the actual medical signal, which are stored into a patient's medical record. In specific, the focus is on Electroencephalogram (EEG) Signal and how to embed numerical metadata within the data. EEG signals, common tasks are the detection of seizure or other brain related illnesses. The watermarking technique based on random sequence is one of the well-known robust digital watermarks. In this paper, we propose a new idea to restore the original signal from a watermarked signal which was embedded a random sequence. The technique is based on wavelet transform. We look into the binary representation of each wavelet coefficient and embed an extra bit to expandable wavelet coefficient.

KEYWORDS: Reversible Watermarking, LWT, PRNG, LFSR

INTRODUCTION

The surge of digital radiological modalities in modern hospitals and research institutes around the world, has led to the creation of a vast amount of medical digital assets, like signals and images. Modern health care infrastructure is based on digital information management. It is usual that a medical image is diagnosed before storing the signal in the long-term storage [1]. These files as any digital asset should be protected from unwanted modification of their contents, especially as they contain vital medical information. Although the recent advancement in information and communication technologies provide new means to access, handle and move medical images, they also allow easy manipulation and replication [2]. Embedding of watermark in region of interest (ROI) causes compromise with the diagnosis value of medical signal [3]. To achieve medical watermarking technique, proper selection of Non region of interest selection is a crucial task.

Some researchers already apply watermarking technique for medical data. Zhou et al [4] present a watermarking method for verifying authenticity and integrity of digital mammography image. They used digital envelope as watermark and the least significant bits (LSB) of one random pixel of the mammogram is replaced by one bit of the digital envelope bit stream. Instead of the whole data, only partial data, i.e. the most significant bits (MSB) of each pixel is used for verifying integrity. Other researchers adapt digital watermarking for interleaving patient information with medical images to reduce storage and transmission overheads [5]. Again, the LSB of image pixels are replaced for embedding. Chao et al. propose a discrete cosine transform (DCT) based data-hiding technique that is capable of hiding those EPR related data into a marked image [6]. The information is embedded in the quantized DCT coefficients. The drawback of the above watermarking approaches is that the original medical image is distorted in a non-invertible manner. Therefore it is impossible for watermark decoder to recover the original image. A reversible watermarking scheme involves inserting a watermark into the original image in an invertible manner in that when the watermark is extracted, the original image can be recovered completely [7][8][9][10]. Research has also been done in the area of reversible watermarking in medical images. Trichili et al [11] proposes an image virtual border as the watermarking area. Patient data is then embedded in the LSBs of the border. Guo and Zhuang present a scheme where the digital signature of the whole image and patient information is embedded [3]. Cao et al extend their work on digital envelope and embed their DE by making a random walk sequence and replace LSB of each selected pixel [12].

METHODOLOGY

In the proposed paper a multilevel of security is provided. The technique is based on a message being converted into binary stream and hidden in the data in wavelet domain in such a way as to make the existence of the message unknown to an observer as shown in figure 1. For this purpose a stream of pseudorandom number (PRNG) is generated. These numbers are used for indexing i.e the position where bit are going to be embed. Every bit of watermark is embedded exactly on the position which generate by the mathematical model, here we used a modified version of linear feedback shift register (LFSR). A key is used to generate a series of number equal to the number of the pixel*8 (pixel is converted into 8 bit binary number) in watermark. 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 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 [13]. Most of the attacks are done onto high frequency band as the attackers do not want to harm the high information areas. For this purpose lifting based integer wavelet transform is used. The watermark is pseudo randomly distributed over the transformed signal. The extraction is done same as in reverse manner. The receiver picks the watermark sample bits and decodes them. If the extracted message is same as the embedded the integrity is verified. After the extraction reconstruction processes is done. In this process the original signal is retrieved.

PROPOSED TECHNIQUE

In order to embed metadata within the medical data, 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. The technique is based on a message being hidden in a data in wavelet domain in such a way as to make the existence of the message unknown to an observer. Only those individuals with a key

will be able to know the identity of the patient [10]. To increase the security the data is embedded into transformed domain. After transformation the signal 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 data and high frequency band contains relatively less information of data [11]. Most of the attacks are done onto high frequency band as the attackers do not want to harm the high information area. For this purpose lifting based integer wavelet transform is used. The watermark is converted in to form of zero and one. The watermark is pseudo randomly distributed over the transformed data.

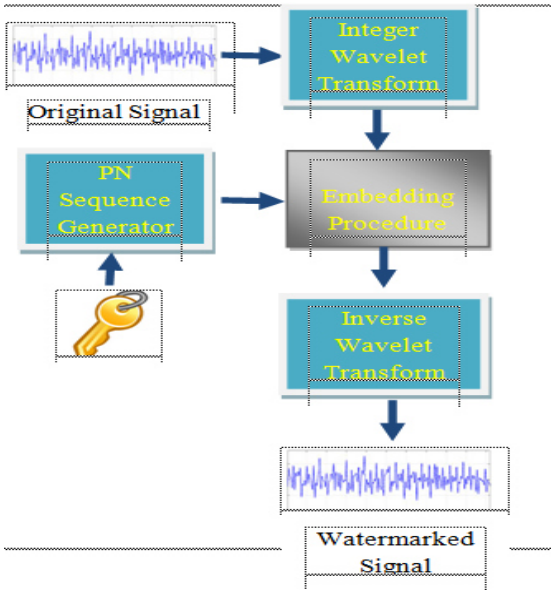

Figure 1: Watermark Embedding Procedure

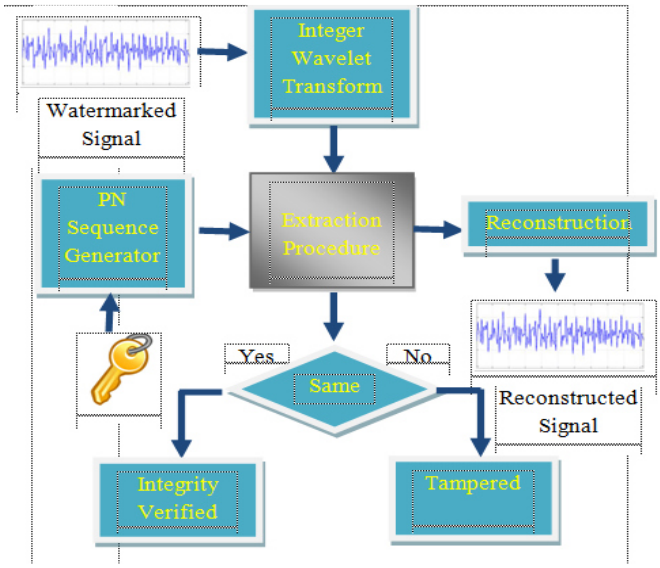

Figure 2: Watermark Extraction Procedure

The extraction is done same as in reverse manner, shown in figure 2. The extracted message is decoded and arrange in the same manner which is embedded. If the extracted message is same which is embedded the integrity is verified otherwise the sample is discarded and we request the sender to resend the data. The whole procedure is divided into five parts. Watermark construction

- Lifting Based Integer Wavelet Transform
- Pseudorandom Bits sequence Generator
- Watermarking Technique
- Watermark extraction and Reconstruction Process

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 or alphabets. This Number is converted into image. The gray scale value of each pixel in the image is converted into 8 bit binary number and then stored into a one dimensional array. The basic procedure is shown in the figure 3.

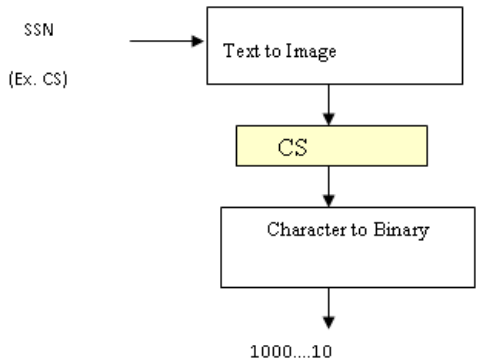

Figure 3: Watermark in 8 Binary Format

Lifting Based Integer Wavelet Transform

The wavelet transform is a valuable tool for Multi resolution analysis that has been widely used in signal processing applications [13]. 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 images, the image is projected onto a set of basis functions, and the resultant transform coefficients are encoded [14]. 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 figure 4. In this work one level decomposition of signal is done. Second level decomposition can also be used but the embedding capacity will be decrease.'

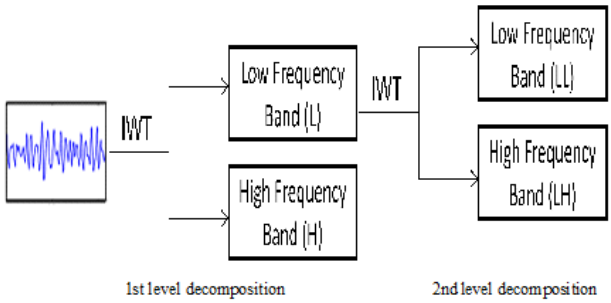

Figure 4: 2 Level Wavelet Decomposition

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.

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 figure 5.

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 [10]:

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

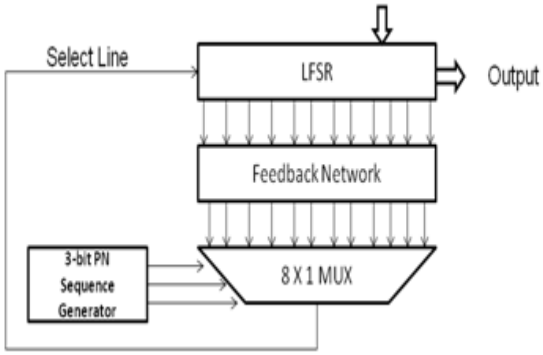

Figure 5: Working of LFSR

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 as shown in figure 5. 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 [15].

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 [16]. An extension is done by adding a 3 bit multiplexor. The selected number is converted into 3 bit binary and feed back as selector. The selector select particular tap and this process is repeated until desired number of numbers are generated. This multiplexor is used to select the tap randomly. This will increase the randomness 7 times.

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

Table 1: Tapping Sequences

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]

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 figure 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.

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, b=0 and n= total number bit to embed

Step 1: for i=1 to n

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

Step 3: Compute difference of x and y i.e diff=|x-y|.

Step 4: Convert decimal diff into 3 bit binary and store in a variable code.

Step 5: Put bit b into next to LSB position into c and store in a variable code.

Step 6: Compute new sample value x' and y' as x'= avg + $\left\lfloor \frac{code\ +1}{2} \right\rfloor$ and y'= x'-code.

This process can also be depict as follows

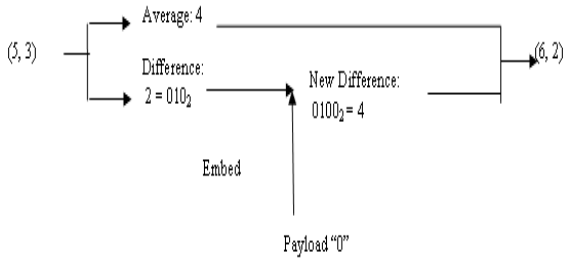

Figure 6: Example to Show Watermark Embedding Procedure

Watermark Extraction and Reconstruction Process

Step 1: For i=1 to n

Step 2: Compute difference of x' and y' i.e diff'=|x'-y'|. Compute average of x and y i.e avg= $\left\lfloor \frac{x+y}{2} \right\rfloor$

Step 3: Convert decimal diff' into 4 bit binary and store in a variable code'. Conver the decimal difference of x and y i.e diff=|x-y|.

Step 4: Extract the next bit to LSB and store in an array.

Step 5: Compute new value as L=x' – $\left\lfloor \frac{diff'+1}{2} \right\rfloor$

Step 6: Compute original sample value x and y as x=L+ $\left\lfloor \frac{diff'}{2} \right\rfloor$ and y= x-diff'.

CONCLUSIONS

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 signal 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. Such a process can be introduced in signal management software and participate to improve maintainability of the system while preserving patient privacy. This technique insure 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. 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 reconstruction process completely reconstructs the watermarked signal to original signal. There will be no miss diagnosis during the examination.

FUTURE WORK

- Error correcting codes can be used for better results.
- Colored watermark can be applied on signal.
- For reversible watermarking, there is a limitation of maximum payload, depending on the capacity of original data being used, it can be improved.
- A hybrid approach can be applied by embedding audio watermark along with the video watermark
- It can have an interactive GUI, so that it can be used for commercial application.
- The LFSR is used for the pseudorandom number generation purpose, the hardware of this PN sequence generator can also be implement.
- A more effective PRNG can be used here. The signals are one dimensional so it is very necessary to use a PRNG which is more random and the repetition of any number is very less.

REFERENCES

1. Wakatani, A. 2002, "Digital Watermarking for ROI MedicalImages by Using Compressed Signature Image", 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02), pp. 2043-2048.
2. Coatrieux, G., Sankur, B. & Maitre, H. 2001, "Strict Integrity Control of Biomedical Images", SPIE Conference 4314: Security and Watermarking of Multimedia Contents III.
3. Guo, X. & Zhuang, T. 2003, "A lossless watermarking scheme for enhancing security of medical data in PACS", Medical Imaging 2003: PACS and Integrated Medical Information Systems: Design and Evaluation, Feb 18-20 2003, The International Society for Optical Engineering, SanDiego, CA, United States, pp. 350-359.
4. Zhou, X.Q., Huang, H.K. & Lou, S.L. 2001, "Authenticity and integrity of digital mammography images", IEEE Transactions on Medical Imaging, vol. 20, no. 8, pp. 784-791.
5. Acharya, R., Anand, D., Bhat, S. & Niranjan, U.C. 2001, "Compact storage of medical images with patient information", IEEE transactions on information technology in biomedicine : a publication of the IEEE Engineering in Medicine and Biology Society, vol. 5, no. 4, pp. 320-323.
6. Chao, H.M., Hsu, C.M. & Miaou, S.G. 2002, "A data-hiding technique with authentication, integration, and confidentiality for electronic patients records", IEEE Transactions Information Technology in Biomedicine, vol. 6, no. 1, pp. 46-53. IJCSNS International Journal of Computer Science and Network Security, vol.7 no.9, September 2007 28
7. Fridrich, J., Goljan, M. & Du, R. 2001, "Invertible authentication", Security and Watermarking of Multimedia Contents III, Jan 22-25 2001, Society of Photo-Optical Instrumentation Engineers, San Jose, CA, pp. 197-208.

8. Fridrich, J., Goljan, M. & Du, R. 2002, "Lossless data embedding-new paradigm in digital watermarking", Applied Signal Processing, no. 2, pp. 185-196.
9. Celik, M.U., Sharma, G., Tekalp, A.M. & Saber, E. 2002, "Reversible data hiding", International Conference on Image Processing , pp.157-160.
10. Tian, J. 2003, "High capacity reversible data embedding and content authentication", IEEE International Conference on Acoustics, Speech and Signal Processing 2003, pp. 517-520.
11. Trichili, H., Bouhlel, M., Derbel, N. & Kamoun, L. 2002, "A new medical image watermarking scheme for a better telediagnosis", 2002 IEEE International Conference on Systems, Man and Cybernetics, Oct 6-9 2002, Tunisia, pp. 557-560.
12. Cao, F., Huang, H.K. & Zhou, X.Q. 2003, "Medical image security in a HIPAA mandated PACS environment",Computerized Medical Imaging and Graphics, vol. 27, no. 2-3, pp. 185-196.
13. N. Zierler and J. Brillhart, On Primitive Trinomials, Information and Control v. 13, pp 541-554, 1968, and v. 14, pp. 566-569, 1969
14. R. Calderbank, 1. Daubechies, W. Sweldens, and B.-L. Yeo. Wavelet transforms that map integers to integers. Appl. Comput. Harmon. Anal., 5(3):332369, 1998.