"STEGANOGRAPHIC SCHEME FOR OUTSOURCED BIOMEDICAL TIME SERIES DATA USING AN INTELLIGENT LEARNING"

[1]Harshala N. Pundkar, [2]Dr. Atul S. joshi ,
[1]Student, [2]Associate Professor
[1]Department of Electronics & Telecommunication ,
[1]Sipna College of Engineering and Technology, Amravati, India

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. In addition, the correlation between modified frequency coefficients and the watermark sequence in wavelet.

***Keywords*: ECG, Steganography, time series data, watermarking**.

I. 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.

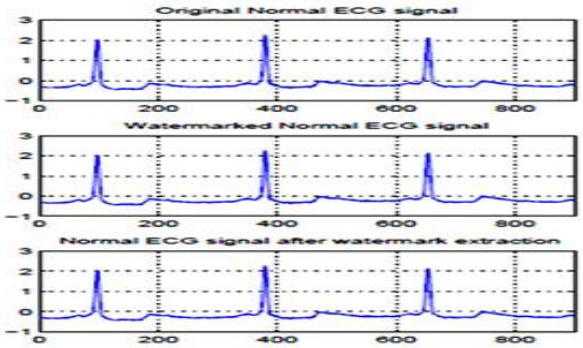

Fig. ECG signals before applying the steganographic operation and after

the steganographic operation as well as after extracting the hidden data

The digital Watermarking technology seems to have the potential of fulfilling such a need as it embeds imperceptible information into the content, which is never removed during normal usage or causes inconvenience to the users. Digital watermarking authenticity and integrity are achieved by embedding control information as watermarks in the image, whereas confidentiality is

not achieved. Encryption can be viewed as a pre protection mechanism because, once decrypted or its digital signature deleted or lost, the information is no longer protected and it becomes hard to verify its integrity and its origin. On the other hand, watermarking is considered as a posteriori control mechanism as the image content is still available for interpretation while the remaining is protected. Thus, it is regarded as a complementary technique since it doesn't achieve confidentiality. Therefore, the implementation of a system that combines encryption standards with watermarking techniques and provides security to the medical images whether encrypted or decrypted, is the main concern of this project. Different types of watermarking methods have been proposed to provide the security services required for telemedicine applications.

II. LITRETURE REVIEW

The watermark scheme needs to address a significant challenge related to biomedical data that is insertion of a watermark must not result in changing health and medical data of a patient to a level where a decision maker (or system) can misdiagnose the patient. If a patient is misdiagnosed, it might not only put his life on risk but also results in significantly enhancing the cost of health care. There has been little research to address the issues related to time series biomedical data such as EEG and ECG. Many authors have attempted the various techniques for security of biomedical data and the various techniques proposed by many authors are shown below:

Anand et al. [5] proposed an efficient watermarking technique in spatial domain of medical image for hiding the watermark by swapping its bits with the grey level pixels of watermark. The privacy of patient's information was protected because of the encryption of the watermarked information and the diagnostic value of the medical images after watermarking is not lessened in any way, with no change in the system configuration or software, the methodology could be employed to other types of patient data such as Electroencephalogram (EEG), Phonocardiogram (PCG) etc.

Balasamy et al. [6] generated a multiple watermarking technique which created watermarks by fusing more than one images by arithmetic blend extension method. This method is not vulnerable against different types of geometric attacks.

Coatrieux et al. [7] described the relevance of watermarking in medical images by presenting different scenarios, one devoted to the authentication and other to the integrity while doing trace of the images with control of the patient's records.

Coatrieux et al. [8] designed a watermarking technique in which different identifiers like Digital Imaging and Communications in Medicine(DICOM) standard, unique patient identifier or Anonymous European Patient Identifier are combined in order to improve medical image protection in terms of maintainability and authenticity.

Dong et al. [9] developed a feasible and novel watermarking algorithm in the encrypted domain by using Discrete Cosine Transform (DCT) and logistic chaotic map. Zero watermarking technique is used for ensuring the authenticity and integrity of medical image. Experimental results show the improved results in comparison withnon-encryptedimagewatermarkingintermsofrobustnessandvariousattacks.

Khor et al. [12] proposed a watermarking technique in multiframes for medical images and for saving processing time, multicores technology is used. The experimental results show that elapsed time is much less on parallel than in sequential watermarking processing along with imperceptibility and robustness.

Kishore et al. [13] proposed an efficient watermarking technique in medical images. The medical images for this algorithm are used in the similar manner as an envelope image in the watermarking procedure, which remains visible to everyone on the network with patient images in wavelet domain. BAT algorithm is used optimally to perform the embedding process which results high Peak Signal to Noise Ratio (PSNR)and normalized cross correlation coefficient (NCC) values.

Milanova et al. [16] proposed three watermarking techniques. The first technique embeds ROI with the digital signature of the image and the image can be reverted back to its original value. This technique is known as Strict Authentication Watermarking (SAW). The second technique which is known as Strict Authentication Watermarking with Joint Photographic Experts Group Compression (JPEG) also uses the same principal as the first technique however, it is able to survive some degree of JPEG compression. The third technique is known as Authentication Watermarking with Tamper Detection and Recovery (AW-TDR) which can localise tampering. At the same time it can reconstruct the original image.

Mohananthini and Yamuna [18] introduced an algorithm by using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) for watermarking process. Red Green Blue (RGB) components of original images are decomposed by using SVD on two level LL subband. Watermark used contains Patient's identification number, Patient name, Patient age, Patient sex, Patients diagnosis information, Patient treatment information and Doctor's signature. This algorithm produces better results with salt and pepper noise, robustness, Gaussian noise, Gaussian blur, median filtering, JPEG compression with quality of 50, rotation, smoothening, sharpening, intensity transformation and row column blanking.

Priya and Sadasivam [19] proposed a lossless reversible watermarking scheme in which watermark is embedded using a reversible Least Significant Bit (LSB) embedding scheme. This scheme combines hashing, compression, and digital signature techniques to create a content dependent watermark making use of compressed ROI for recovery of ROI.

Sharma et al. [20] proposed a watermark embedding technique using wavelet transform . First level DWT is used for the transforming the cover and watermark images to frequency domain. LL subband is selected from watermark image and format it using modulus functions. The watermarked image is encrypted by using the stream cipher cryptographic techniques in order to achieved two level of security which may provide a potential solution to existing telemedicine security problem of patient's identity theft.

Watermarking in medical images is much curtailed because of its data tampering problem as the data shown in medical image is highly important for the patient. Watermarking techniques for medical have flaws like some techniques lack in watermark embedding capacity, resistance towards network attacks, watermark recovery, low Bit Error Rate(BER),application on colour images, protection of ROI, recovery of corrupted watermark and high degree of invisibility. So, there is a requirement of a technique which can provide high embedding capacity, high security, high robustness against attacks, fully reversible, without lowering the PSNR value. As discussed above, all watermarking techniques are efficient while considering one or other parameters like limited robustness, low visual quality, limited capacity and incomplete reversibility but lacks in improving all the parameters parallel.

III. CONCLUSION

An intelligent learning-based watermarking scheme for biomedical data can be develope. 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 biomedical 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.

IV. ACKNOWLEDGMENT

I would like to express my sense of gratitude to my guide Dr. A. S. Joshi for this valuable guidance which helped me in the project idea. The blessings, help and guidance given by him time to time will carry me for a long way in the journey on which I about to embark.

REFERENCES

1. Abou-Loukh SJ, Gatea SM (2011) Spoken word recognition using slantlet transform and dynamic time warping. Nahrain University. Coll Eng J (NUCEJ) 14(1):34–45
2. Abou-Loukh SJ, Zeyad T, Thabit R(2010) Ecg classification using slantlet transform and artificial neural network. J Eng 16(1):4510–4528
3. Alattar AM (2004) Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans Image Process 13(8):1147–1156
4. An L, Gao X, Li X, Tao D, Deng C, Li J (2012) Robust reversible watermarking via clustering and enhanced pixel-wise masking. IEEE Trans Image Process 21(8):3598–3611Multimed Tools Appl
5. Anand D, Niranjan UC (1998) Watermarking medical images with patient information. In: Proceedings of the 20th annual international conference of the ieee on engineering in medicine and biology society, vol 2. IEEE, pp 703–706
6. Balasamy K, Dharshini MD, Gayathri S, Geetha MM (2016) Image authentication system using fused watermarking technique. Int J Innov Res Comput Commun Eng 4(1):189–193
7. Coatrieux Gouenou, Maitre H, Sankur B, Rolland Y, Collorec R (2000) Relevance of watermarking in medical imaging. In: Proceedings IEEE EMBS international conference on information technology applications in biomedicine. IEEE, pp 250–255
8. Coatrieux G, Quantin C, Montagner J, Fassa M, Allaert F-A, Roux C (2008) Watermarking medical images with anonymous patient identification to verify authenticity. In: MIE, vol 136, pp 667–672
9. DongJ,LiJ,DuanY(2015)Arobustwatermarkingalgorithmforencryptedmedicalimagesbasedondct encrypted domain. In: International conference on electronic science and automation control. Citeseer, pp 140–143
10. Eswaraiah R, Sreenivasa Reddy E (2014) Medical image watermarking technique for accurate tamper detection in roi and exact recovery of roi. Int J Telemed Appl 2014:13
11. Kennedy J, Eberhart R (1995) Particle swarm optimization. In: Proceedings of the IEEE international conference on neural networks, 1995, vol 4, pp 1942–1948
12. Khor HL, LiewS-C,Zain JM(2016) Parallel digital watermarking process on ultrasound medical images in multicores environment. J Biomed Imag 2016:4
13. Kishore PVV, Kishore SRC, Kiran Kumar E, Kumar KVV, Aparna P (2015) Medical image watermarking with dwt-bat algorithm. In: 2015 international conference on signal processing and communication engineering systems (SPACES). IEEE, pp 270—275
14. Lafta MM, Alwan IM (2011) Watermarking in image using slantlet transform. Iraqi J Sci 52(2):225–230
15. Manasrah T , Al-Haj A(2008) Management of medical images using wavelets-based multi-watermarking algorithm. In: IIT 2008 international conference oninnovations in information technology 2008. IEEE, pp 697–701

16. Milanova MG, Ford C, Kountchev R, Kountcheva R (2003) Digital watermarking for medical images. In: METMBS, pp 509–520
17. Mohammed RT, Khoo BE (2012) Image watermarking using slantlet transform. In: 2012 IEEE symposium on industrial electronics and applications (ISIEA). IEEE, pp 281–286
18. Mohananthini N ,Yamuna G (2015) A study of dwt-svd based multiple watermarking scheme for medical images. IJ Netw Secur 17(5):558–568
19. Lakshmi Priya R, Sadasivam V (2015) Protection of health imagery by region based lossless reversible watermarking scheme. Sci World J 2015 24. Rivest R (1992) The md5 message-digest algorithm. https://www.ietf.org/rfc/rfc1321.txt
20. Sharma A, Dave M, Singh AK, Ghrera SP (2015) Encryption based medical image watermarking against signal processing attacks. In: Proceedings of international conference on future computational technologies (ICFCT 2015), pp 82–88