Watermarking Techniques - A Study

Shyam Sundar[#1]

[#1]P.G. Scholar, Department of Electrical and Electronics Engineering, GBPIET, Pauri, India, shyam.sundar0401[at]gmail.com

Abstract: ***From the decades the development in the internet technologies is increasing more widely in daily life media data as images, audios, videos etc. Due to its facile use the media data can be transmitted and copied also. Because of some legal issues media data should be protected against uncertified users and operations. To protect the exploit of the media data watermarking technique is used. This is the modern technology to secure the data by encrypting information inside some digital media and is used for copyright protection. This paper dealt with the theories existed from past to present that helps to understand the watermarking technique for protection of medical images. It is important to maintain the authenticity of patient information security system is to be required.***

Keywords: water marking technique, media data, security system

1. Introduction

The continuous increase in computer technology in medical information, transferring has lead to a sudden increase in public awareness of the need for privacy and secrecy. It enables information to be shared between distant health professionals and manipulated and managed more easily due to which more attention should be required in information protection. Security in the information age has become a matter of jumbled data in such a way that prevents uncertified recipients from understanding it, yet allows certified receivers to make use of it. Security can be defined in terms of confidentiality, availability, integrity and authenticity.

Recently watermarking is preferred as a appreciative mechanism for protection of medical data. To transport data watermarking provides a new approach in medical information technology. The lead of watermarking technology is to give a sovereign and steady protection of contents. To develop a security method in medical content sharing it is necessary to guarantee their confidentiality, integrity and traceability in an independent way. In such a set-up, to improve medical image security watermarking has been shown as a complimentary mechanism. Watermarking allows installing a message in a host document by modifying the host content in an undetectable way.

The main objective of the present paper is to review the studies from to past to present done on the watermarking technique used to protect the medical data's confidentiality, integrity, authenticity and availability. For dealing with images applications, the objective of watermarking is to immerse invisibly message inside the image. The length of the transmitted message can be relatively important, in fact, longer that just for identification. According to the length of the message insertion of data can be made in distinct ways or desired agility. Some of the researches are as follows:

Anderson and Manifavas (1997) showed two contradictory things to a stream cipher to nourish it and to furnish it included property that small change in key cause small change in keystream.

U. Acharya et al. (2001) presented a technique with medical images for effective storage of interleaving patient particulars such as text acquaintance and physiological signals. Prior to interleaving encrypted text files using logarithmic technique and encrypted heart rate signals by DPCM and ADM techniques. For different images technique is tested and NRMSE observed less than 0.71% for 8 bit encoded pixel intensity. According to distinct plan security particulars further enhanced by selecting the location of interleaved bit to the allowed users.

U. Acharya et al. (2004) adapted watermarking for interleaving patient details during (joint photographic experts group) JPEG compression of medical images to minimize storage and transmission overheads. To ensure more security in the frequency domain the text data is encrypted before interleaving with images. The results of the work are tabulated and with interleaving spatial domain.

Table 1 Results of interleaving data with image in the frequency domain (source: Rajendra Acharya U. et al.)

Image	Text (NRMSE%)	DPCM (NRMSE%)	ADM (NRMSE%)
Angiogram	3.06	3.06	3.02
MRI	4.82	4.83	4.80
X Ray	4.67	4.67	4.60

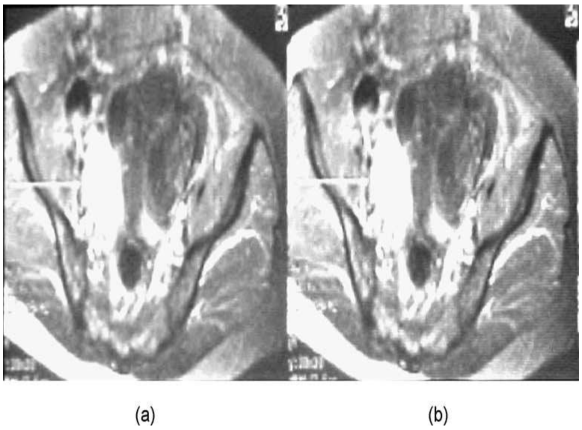

Figure 1: Result of interleaving text in the Angiogram image: (a) original image; (b) interleaved image.
PC: Rajendra Acharya U. et al.

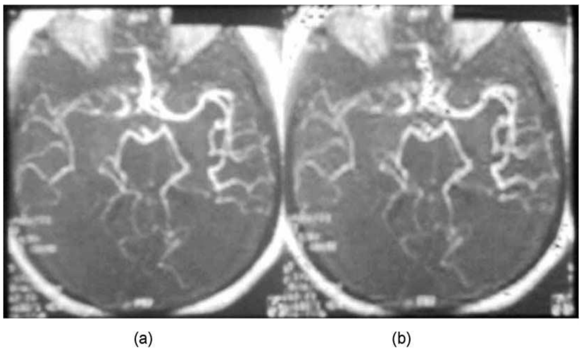

Figure 2: Result of interleaving text in the MRI image: (a) original image; (b) interleaved image.
PC: Rajendra Acharya U. et al.

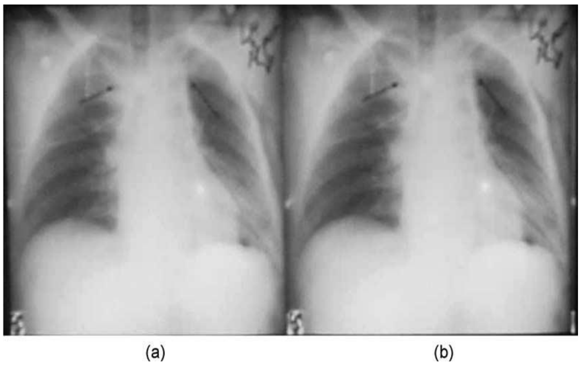

Figure 3: Result of interleaving DPCM error signal in the X-ray image: (a) original image; (b) interleaved image.
PC: Rajendra Acharya U. et al.

Using logarithmic techniques text files are encrypted and in frequency domain interleaved. The NRMSE was found to 5% less for different images.

Shiguo L et al. (2007) implemented commutative video encryption and watermarking during advanced video coding procedure based on H.264/AVC codec. The encryption and watermarking procedures are independent. Hence from encrypted videos watermarking can be extracted and can be re-watermarked. This keeps scheme safe against instant attacks, effective in modification, keeps subtle and vigorous against recompression is some extent. For secure video dispatch and distribution these properties makes the scheme secure.

Shiguo L et al. (2007) proposed a safe video distribution process which immerse a finger print code in video content at decryption process. The video content is managed by motion vector (MV) encryption at server side and at customer side is decrypted and fingerprinted simultaneously by the key and the fingerprint both combined into homogenous operations. Before embedding collusion attacks can be encoded with collusion resistant codes. Furthermore the quality of colluded copy's quality reduced to improve the watermark strength which makes collusion attacks out of work.

Celik et al. (2007) worked on cipher based look up table (LUT) to fix watermark which are noise rugged and detected without actual content. Watermark detection speed up by six orders of magnitude for a system.

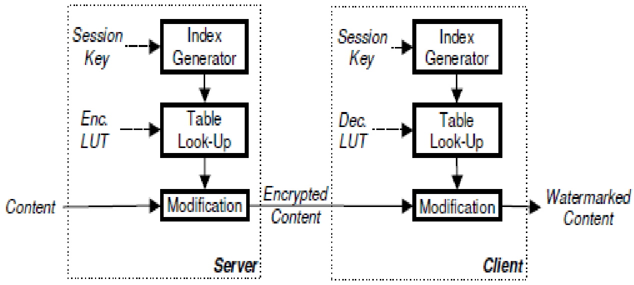

Figure 4: Encryption and corresponding joint decryption and watermarking procedures
PC: Celik et al. 2007

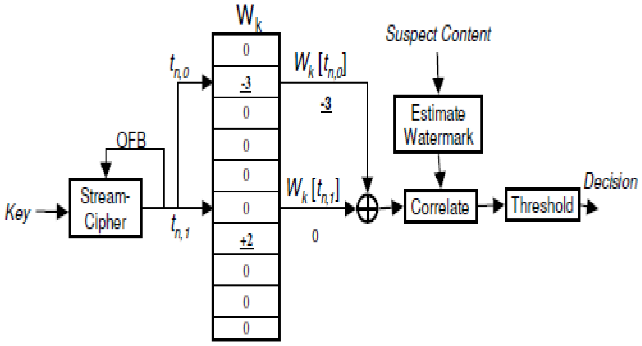

Figure 5: Detection procedure (S = 2) in which watermark sequence is reconstructed and correlated with the watermark estimate derived from the received signal

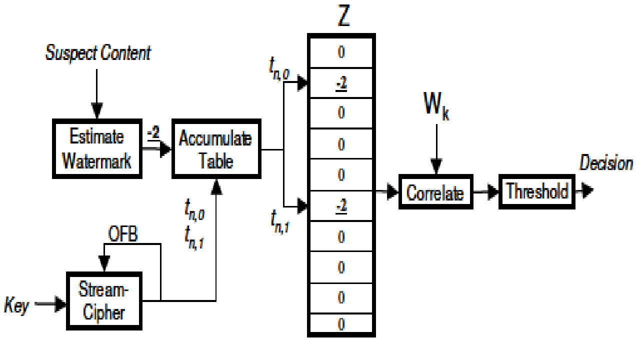

Figure 6: Alternate detection procedure. Watermark estimates are accumulated in an empty LUT at positions indicated by t_{ij}. This LUT is then correlated with the watermark LUT for detection

Braci S et al. (2009) evaluated a watermarking security based on quantization. To measure the security level theoretical and practical simulations are used for watermarking technique. The quantization index modulation (QIM) works as a secure system when used as a continuous key and prevents attacks. A secure version of classical trellis coded quantization watermarking is proposed. It permits the watermarking security level increased and for unauthorized users the encrypted message is hard to understand.

Pan W et al. (2010) used reversible watermarking to implement medical image access and usage control policy. For integrity and traceability of data different security systems required. Reversible watermarking is useful for monitoring image integrity, authenticity and right of access. The model OrBAC was used to access control policy requirements. For implementing security policy OrBAC API is responsible. They merge both techniques to give protection to the data. When the violation is detected automatic alert raised.

Pan et al. (2011) proposed a new reversible watermarking technique which identifies parts of the image that can be watermarked with two distinct HS modulations: pixel histogram shifting (PHS) and dynamic error histogram shifting (DEHS). They considered specific signal content in terms of low distortion and capacity for both natural and medical images. This method is brittle and any enhance the watermark.

Bouslimi et al. (2012) merged a QIM and a cipher algorithm or a block cipher algorithm. They proposed a new joint watermarking/encryption system to protect a medical image. This system gives message in spatial domain and encrypted domain. Even though the image is encrypted it gives message to verify the reliability of the image. Experimental results showed that image distortion is low and achieved capacity is sufficient to embed reliability proof. The system is slower but gives reliable control functions, for image decryption execution time is not affected. The security system is not interfered with combining encryption and watermarking. Security system depends on the knowledge of encryption and watermarking keys.

2. Conclusion

From the literature reviewed concluded that the necessity of smart and safe diagnosis is paramount in the medical world. Watermarking is the best answer to make medical images safe and secure. It can give reliability to medical image by asserting its integrity and its authenticity. Watermarking allows authorized receivers to understand the data and it cannot be misused and manipulated by the unauthorized users. More and more researches are still required in watermarking security technique so that it cannot occupy more space and can be used as reliable as possible to authorized users. Future work consists of integrating administration elements into the model and vigorous against collusion or resynchronization.

Acknowledgement

I would like to thank my supervisor Y Singh, professor of electronics department for helping me in improving the draft, providing liberal guidance at every stage of this work and sparing time for discussions as and when desired by me.

References

[1] U. Rajendra Acharya, D. Acharya, P. Subbanna Bhat, and U. C. Niranjan, "Compact storage of medical images with patient information," IEEE Trans. Inf. Technol. Biomed., vol. 5, no. 4, pp. 320 323, Dec. 2001.

[2] W. Pan, G. Coatrieux, N. Cuppens-Boulahia, F. Cuppens, and C. Roux, "Watermarking to enforce medical image access and usage control policy," in Proc. 6th Int. Conf. Signal-Image Technol. Internet-Based Syst., Kuala Lampur, Malaysia, Dec. 2010, pp. 251–260.

[3] L. Shiguo, L. Zhongxuan, R. Zhen, and W. Haila, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[4] S. Braci, R. Boyer, and C. Delpha, "Security evaluation of informed watermarking schemes," in Proc. 16th IEEE Int. Conf. Image Process., Nov. 2009, pp. 117–120.

[5] L. Shiguo, L. Zhongxuan, R. Zhen, and W. Haila, "Joint fingerprint embedding and decryption for video distribution," in Proc. IEEE Int. Conf. Multimedia Expo., Jul. 2007, pp. 1523–1526.

[6] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/ watermarking system for verifying the reliability of medical images," in IEEE Trans. on infor. tech. in biomedicine., vol. 16, no. 5, pp. 891-899, Sep. 2012.

[7] R. Anderson and C. Manifavas, "Chameleon: A new kind of stream cipher," in Proc. 4th Int. Workshop Fast Software Encryption, Haifa, Israel, Jan. 1997, vol. 1267, pp. 107–113.

[8] U. Rajendra Acharya, U. C. Niranjan, S. S. Iyengar, N. Kannathal, and L. C. Min, "Simultaneous storage of patient information with medical images in the frequency domain," Comput. Methods Programs Biomed, vol. 76, pp. 13–19, 2004.

[9] W. Pan, G. Coatrieux, N. Cuppens-Boulahia, F. Cuppens, and C. Roux, "Reversible watermarking based on invariant image classification and dynamical error histogram shifting," in Proc. Annu. Conf. IEEE Eng. Med. Biol. Soc., Boston, MA, 2011, pp. 4477–4480.

[10] M. Celik, A. N. Lemma, S. Katzenbeisser, and M. van der Veen, "Secure embedding of spread spectrum watermarks using look-up-tables," in Proc. Int. Conf. Acoust., Speech Signal Process., Apr. 2007, vol. 2, pp. 153–156