ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 5, May 2015

Hybrid Encryption/Watermarking System for the Secured Transmission of Medical Images

Usha.S, Karthik.M

***Abstract*—The rapid evolution of multimedia and communication technologies offers new means of sharing and remote access to patient data. In particular, Medical imaging plays important roles in applications like Telesurgery, Telediagnosis, and so on. Hence transmission of medical images in a secure way is an emerging trend today. In this paper a hybrid methodology consists of encryption and watermarking is proposed for secure transfer of medical images.To verify the integrity of the medical image at the receiving side spatial and encrypted messages are obtained from the same medical image (original image), which are used as watermarks. The proposed method is simulated using MATLAB R2010b and results convey that the proposed method is robust against various geometric and frequency attacks.**

***Index Terms*—Encryption, Hamming Distance, Medical Image, Peak Signal to Noise Ratio, Watermarking**

I. INTRODUCTION

In this digitized era, digital information transfer has a great impact on human life. Hefty information content can be stored and transmitted with security. Governments, military, corporations, institutions, hospitals, and private businesses collect a confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. The confidentiality in information is being maintained by various techniques such as cryptography, stenography and watermarking.

Today, transfer of medical image in a secure way is vital for applications like telesurgery and telediagnosis, in this paper a joint encryption/watermarking system is proposed. This system is based on an approach which combines a substitutive watermarking algorithm, with an encryption algorithm. The purpose of the proposed system is to verify the reliability of an image within the spatial domain as well as the encrypted domain.

Digital watermarking is the process of computer-aided information hiding in a carrier signal; the hidden information no need to contain any relation to the carrier signals. The information to be embedded in a signal is called a digital watermark. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal. The watermarked digital signal is transmitted or stored, usually transmitted to another person in the unsecured transmission medium. If the unauthorized person hacks or modifies the signal, this is called an attack. The modification may not be malicious; the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted.

Encryption is a process which is used to secure the data and the encryption algorithms play a crucial role in efficient information security systems. Selective encryption technique is one of the most promising solution to increase the speed of encryption as compared to the full encryption. Selective encryption is a technique to save computational power, overhead speed and time. This technique also provides quick security by only encrypting a selected portion of a bit stream. Selective encryption is helpful for the multimedia content like images, video content and audio content.

In the proposed method Least Significant Bit-Discrete Wavelet Transform (LSB-DWT) along with selective encryption algorithm is used for protecting the medical images.

II. LITERATURE REVIEW

Dalel Bouslimi et al proposed a joint encryption/watermarking system [4] for verifying the reliability of medical images in 2012. This system is based on an approach which combines a substitutive watermarking algorithm, the quantization index modulation, with an encryption algorithm: a stream cipher algorithm or a block cipher algorithm. The image distortion is very low and that the achieved capacity is enough to embed reliability proof as well as some other data. Obviously, their joint watermarking/encryption system is slower than simply encrypting the image but it provides reliability control functionalities.

Puneet Kr Sharma and Rajni presented a technique of image watermarking using LSB Algorithm [8]. In this method, image watermarking using LSB algorithm has been used for embedding the message/logo into the image. If the watermark is embedded in the first LSB bit, the authors obtained the watermarked images without noticeable distortion. However the watermarks are embedded in the consequent bits i.e.

Manuscript received Aug 15, 2012.
***Usha. S**, Department of EEE, Kongu Engineering College, Perundurai - 638052, Erode, TamilNadu, India.*
***Karthik. M**, Department of EEE, Kongu Engineering College, Perundurai - 638052, Erode, TamilNadu, India.*

second towards last MSB bit, the image start distorted.

Rajendra Acharya et al proposed a paper "Compact Storage of Medical Images with Patient Information" [9]. Digital watermarking is a technique of hiding specific identification data for copyright authentication. This technique is adapted here for interleaving patient information with medical images to reduce storage and transmission overheads.

III. Proposed Method

In the proposed method the combination of LSB and DWT is proposed.

A. Embedding Process

Step 1: The DWT is applied to the cover image. The DWT Transform divides the image into 4 sub-bands LL, LH, HL and HH.

Step 2: The spatial message is embedded in the LH band using LSB algorithm. Here the cover image is LH band. The LSB of the cover image is replaced by the MSB of spatial message image based on thresholding factor.

Step 3: The encrypted message is embedded in the HL band using LSB algorithm. Here the cover image is HL band. The LSB of the cover image is replaced by the MSB of spatial message image for the embedding process.

Step 4: By taking the IDWT the watermarked image is obtained by combining all the sub-bands.

Step 5: The watermarked image is encrypted using Selective Encryption Algorithm (SEA) with the symmetric key.

B. Extraction Process

Step 1: The encrypted watermarked image is decrypted using selective decryption algorithm (SEA). The watermarked image is recovered.

Step 2: The DWT is applied to the decrypted watermarked image. The DWT Transform divides the image into 4 sub-bands LL, LH, HL and HH.

Step 3: From LH and HL band, the spatial and encrypted message is recovered using LSB.

Step 4: Then by taking IDWT, the cover image is obtained.

C. Generation of Watermarks

The purpose of the proposed system is to verify the reliability of an image within the spatial domain as well as the encrypted domain. It relies on two main procedures: protection and verification. The protection stage consists of watermarking and encryption of an image. In this technique two messages, namely, Msg_s and Msg_e, which will be available in the spatial and encrypted domains, respectively are inserted into the image. The insertion and the extraction of each message depend on a watermarking key: K_{ew} is the key for the encrypted domain and K_{sw} is the key for the spatial domain. These two messages contain security attributes that will assess the image reliability in each domain. Indeed, each message also contains an Authenticity Code (AC), which identifies the image origin and an integrity proof.

Spatial Message

In the spatial domain, integrity is ensured by making use of a secure hash function (e.g., SHA1) computed on the image bit subset that is not modified by the watermarking process .The message available in the spatial domain, Msg_s is defined in the equation 1

$$\mathbf{MSG_s =< AC, SHA (nmb)> \quad (1)}$$

Encrypted Message

In the encrypted domain, integrity is controlled by verifying the presence of a secret pseudorandom sequence of bits generated using a secret watermarking key. The integrity of the watermarked-encrypted image is considered as valid if they retrieve these bits at specific locations within the SHA signature of each watermarked-encrypted block bytes. The verification of the image authenticity and integrity in the encrypted domain relies on extracting Msg_e given in the equation .2

$$\mathbf{MSG_e =< AC, PRNG (K_{ew}) > \quad (2)}$$

IV. Results and Discussion

The Magnetic Resonance image (MRI) of the brain of size 512x512 has been taken as a cover image and the watermarks (spatial and encrypted message) are generated from cover image using secure hash function and pseudorandom number generator. Figure 1 represents the original cover image and the watermarks (spatial and encrypted message) to be embedded.

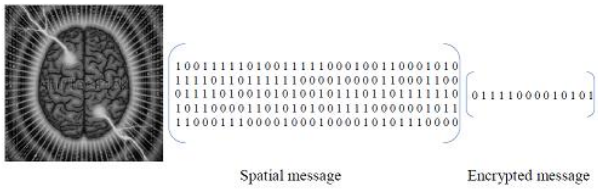

Fig 1: Original Cover Image and Watermarks

A. One Level DWT of Cover Image

The original cover image of size 512x512 has been taken and applied one level DWT, for the first level the image is divided into four sub-bands. Each band having the size of 256x256. The two sub bands are used as a cover image to embeds the spatial and encrypted message. The LH band is used as a cover image to embed the spatial message and HL band is used as a cover image to embed the encrypted message. Figure 2 shows the original cover image and the one level decomposition of the cover image.

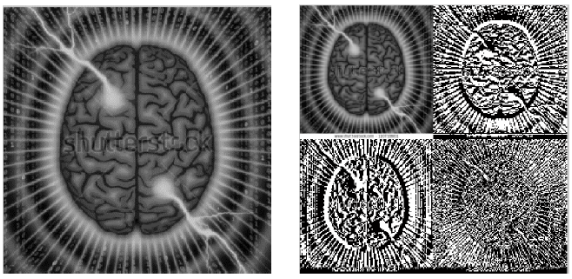

Fig 2: Cover image and one level decomposition of cover image

B. Watermarked Image

Watermark bits are embedded using LSB algorithm in the mid frequency sub bands (LH &HL) and IDWT is taken for each blocks. The embedded blocks concatenated and the watermarked image is shown in Figure 3.

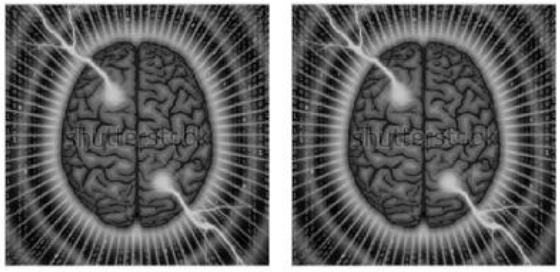

Fig 3: Original Image and Watermarked Image

Table 1 lists the comparative performance of image quality metrics like Peak to signal to Noise Ratio (PSNR), Similarity (SIM) and Universal Quality Index (UQI) of the proposed method with the conventional techniques.

Table 1: Image Quality Metrics

S.NO	WATERMARKING SCHEME	PSNR	SIM	UQI
1	LSB	75.61	0.999	0.999
2	DWT	52.03	0.996	0.993
3	LSB-DWT	52.04	0.997	0.996

From the table 1, it is realised that LSB algorithm works in a better way when compared to the other two techniques. But the performance has to be analysed by recovering the watermarks after incorporating various attacks over the transmitted image.

C. *Encryption Using Selective Encryption Algorithm*

Using SEA and the key the watermarked image is converted in to stego image which is shown in Figure.4.

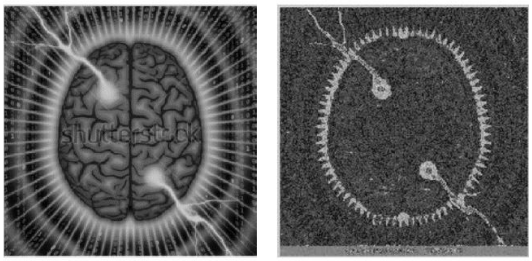

Fig 4: Watermarked and Stego Image

D. *Watermark Recovery*

The stego image is transmitted via the unsecure channel to the receiver. At the receiving side, the watermarked image is extracted from the stego image using the symmetric key and one level DWT is applied to the watermarked image. Watermark bits are extracted in the mid frequency sub bands (HL & LH) based on the pixel position obtained from key and message block using LSB algorithm. The recovered watermarks are obtained and IDWT is taken to obtain the recovered cover image. The recovered watermarks and the recovered cover image are shown in Figure 5.

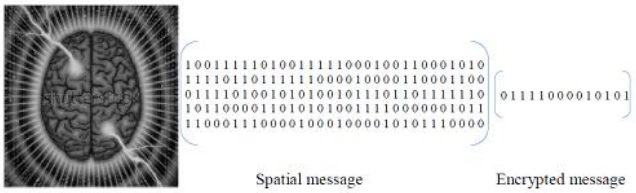

Fig 5: Recovered cover image and watermarks

E. *Comparative Analysis*

The similarity value of recovered spatial message is highlighted in the figure 6.

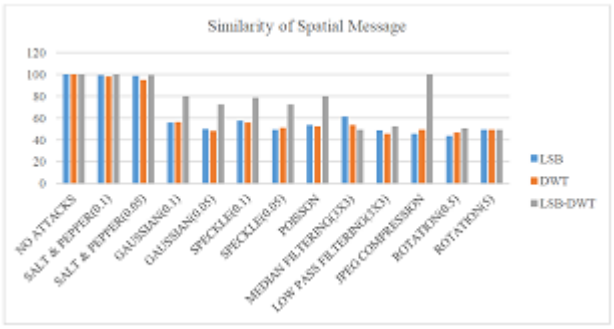

Fig 6. Similarity of recovered spatial message

The similarity value of recovered encrypted message is projected in the figure 7.

Fig 7. Similarity of recovered encrypted message

From the figure 6 & 7, it is observed that except for median filtering and rotation attacks, the proposed method performs in a better way when compared to the existing techniques.

The hamming distance metrics of recovered spatial and encrypted message is projected in the Figure 8 & 9.

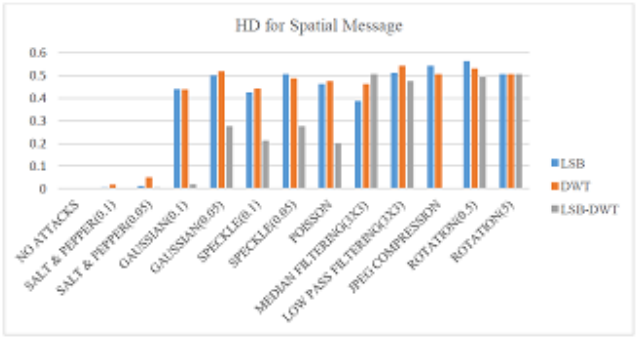

Fig 8: Hamming Distance for recovered spatial messages

Fig 9: Hamming Distance for recovered encrypted Messages

From the figure 8 & 9, it is noted that except for median filtering and rotation attacks the proposed method outperforms when compared to the existing spatial and frequency domain techniques.

V. CONCLUSION

In the proposed method the watermarks are generated from the cover image and the watermarks are called as spatial message and encrypted message. The watermark bits are embedded in the mid frequency bands using the spatial domain and frequency domain. Embedding the watermarks in mid bands, which increases the robustness of the watermarks. And the watermarked image is transmitted securely as a stego image using selective encryption algorithm over the unsecured transmission media. At the receiving end, the embedded watermarks are extracted from the decrypted stego image using reverse process. The robustness of the proposed method is analyzed by incorporating various attacks over the transmitted cipher text. The performance of the proposed method is analyzed by calculating various image quality metrics like Similarity and Hamming Distance. The simulation results shows that the proposed LSB-DWT algorithm is robust against various attacks except Median Filtering and Rotation attack than existing methods.

REFERENCES

[1] B. Chen, and G. W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1423-1443, May 2001.

[2] Chih-chin Lai and Cheng-chih Tsai, " Digital Image Watermarking using Discrete Wavelet Transform and Singular Value Decomposition," IEEE Trans Inst & Meas., , vol. 59, no.11, pp.3060-3063, Nov. 2010.

[3] G. Coatrieux, C. Le Guillou, J.M. Cauvin, and C. Roux, "Réversible Watermarking for knowledge digest embedding and reliability control in Medical Images," IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 2, pp. 158- 165, Mar. 2009.

[4] D.Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images," ," IEEE Trans. Inf. Technol. Biomed.,vol. 16, no. 5, Sep. 2012.

[5] C.Deepshikha , G. Preeti , B.C. Gaur Sanjay, and Anil Gupta, "LSB Based Digital Image Watermarking for Gray Scale Image," IOSR J.Comp.Engg, vol. 6, pp. 36-41, Sep. 2012.

[6] L. Perez-Freire, F. Perez-Gonzalez, , T. Furon, and P. Comesaña, "Security of Lattice-based Data Hiding against the Known Message Attack," IEEE Trans Inf. Fore and Sec .vol. 1, no. 4, pp. 421-439, Dec. 2006.

[7] N. Merhav, "On Joint Coding for Watermarking and Encryption," IEEE Transactions on Inf. Theory, vol. 52, no. 1, Jan. 2006

[8] P. K. Sharma and Rajni, " Analysis of Image Watermarking using Least Significant Bit Algorithm," Int.J. Info. Sci. and Tech., vol.2, no.4, pp. 95-101, July 2012.

[9] 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.

S.Usha, presently working as an Assistant Professor(Senior Grade) in EEE Department, Kongu Engineering College, Perundurai, Erode, TamilNadu. She received her B.E.,in Electronics and Communication Engineering in1992 at Bharathiar University, Coimbatore. M.E. in Power Electronics and Drives in 2008 at Anna University, Chennai. She is presently working for her Ph.D in the area of Network Security. She had published several papers in International and National Conferences . Her area of interest includes Network Security, Mobile ad hoc Networks and Digital Image Processing.

M. Karthik graduated in Electrical and Electronics Engineering from Manonmaniam Sundaranar University, Tirunelveli, India and received the Master degree in Applied Electronics from Anna University, Chennai, India in 2004. He is currently with Kongu Engineering College affiliated with Anna University, Chennai. He has published and presented several papers in International journals and conferences respectively. He has also conducted several workshops and seminars in his research area. His research interest includes Fuel Cell Hybrid Electric Vehicles, Energy conversion/storage systems, Renewable Energy systems Modeling and Integration with Electric Grid.