Secure Transmission of Tele Medical Information using Dwt Watermarking & AES Encryption Algorithm

Bharathi C.[1] Amudha A.[2]
[1]Research Scholar [2]Associate Professor
[1,2]Department of electronics & Communication Engineering
[1,2]Ponnaiya Ramajayam College of Engineering & Technology, Thanjavur Tamilnadu, India

Abstract— The rapid advancement of internet has made it easier to send the data/image accurate and faster to the destination. But this advantage is also accompanied with the disadvantage of modifying and misusing the valuable information through intercepting or hacking .So in order to transfer the data/image to the intended user at destination without any alterations or modifications, there are many approaches like Cryptography, Watermarking and Steganography which are used particularly in the fields of medicine .Watermarking is a prevention technique used for preventing media files like images, audio & video files etc. This paper shows the detailed information about providing authentication or security for media data which are shared over internet. This research provides the information about the file encryption using AES algorithm and watermarking using DWT Algorithm. This study shows the idea of using combination of cryptographic algorithm and watermarking algorithm in securing media information’s. The message is encrypted and then the enciphered or encrypted message embedded into cover file and finally covered image is watermarked. The result of the process is watermarked image.

Key words: Watermarking, Digital Watermarking, AES Algorithms & Its Operations, DWT Watermarking Algorithm, Cryptography

I. Introduction

Telemedicine is the use of telecommunication and information technology to provide clinical health care from a distance. It has been used to overcome distance barriers and to improve access to medical services that would often not be consistently available in distant rural communities. It is also used to save lives in critical care and emergency situations.

Although there were distant precursors to telemedicine, it is essentially a product of 20th century telecommunication and information technologies. These technologies permit communications between patient and medical staff with both convenience and fidelity, as well as the transmission of medical, imaging and health informatics data from one site to another.

Early forms of telemedicine achieved with telephone and radio have been supplemented with video telephony, advanced diagnostic methods supported by distributed client/server applications, and additionally with tele medical devices to support in-home care.

Medical images contain valuable information which is related to health of the patient. Before analysing the medical images downloaded from the unsecured network, it is necessary to check whether the images are not meddled. For this reason, authentication of medical images such as Ultrasound scans, MRI scans, x-ray and Computer Tomography (CT) scans has to be watermarked. The host medical image can be watermarked with patient information which is already encrypted using AES algorithm before transmitting on the internet. At the physician’s end it has to dewater marked before proceeding for diagnostics. Medical cover images are watermarked with patient image as watermark which forms an invisible detection code.

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, and video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal.

Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications.

The term “watermark” was probably originated from the German term “wassermarke”. Since watermark is of no importance in the creation of the mark, the name is probably given because the marks resemble the effects of water on paper. Papers are invented in China over a thousand years ago. However, the first paper watermark did not appear until 1282, in Italy. By the 18th century, watermarks on paper in Europe and America had been used as trademarks, to record the manufactured date, or to indicate the size of original sheets. Watermarks are commonly used on bills nowadays to avoid counterfeiting.

In watermarking, changes in the stego object must have no effect on the watermark. Imagine if you had an illegal copy of an image that you would like to manipulate in various ways. These manipulations can be simple processes such as resizing, trimming or rotating the image. The watermark inside the image must survive these manipulations, otherwise the attackers can very easily remove the watermark and the point of steganography will be broken. Finally, we always assume that the attacker knows that there is hidden information inside the stego object.

Cryptography prevents intruder from getting information without a proper decryption key. Cryptography provides a means for secure delivery of content to the consumer. Legitimate consumers are explicitly or implicitly provided with a key to decrypt the content in order to view or listen to it.

II. Literature review

Watermarking digital multimedia [1]-[4] technique has rapidly grown in the recent past with the advancement in internet technology. This watermarking functionality helps to hide information, protect copyrights and for content identification of multimedia datas exchanged over the internet.

Medical image watermarking [5]-[8] functions desirely in supporting a patient by conveying his infirmity using medical images through unsecured networks such as the internet to expert doctors around the world. This practice helps to expand the possibility of distantly stationed patients where no expert medical doctor is accessible to increase their probability of endurance.

In recent years medical image watermarking is primarily used to hide patient information such as patient's name, age, gender which can uniquely identify a patient by [9]. This patient related watermark information is extracted to determine the authenticity of the medical images. As the extracted watermark from the medical image matches the patient data in the doctor's office, it is proved that these medical images belong to a particular patient in [10].

Irany et al [11] proposes a high capacity reversible multiple watermarking scheme for medical images based on integer-to-integer wavelet transform and histogram shifting. It uses a scalable location map and incorporates efficient stopping conditions on both wavelet levels and different frequency sub bands. Lavanya et al [12] proposed non region of interest (NROI) based medical image watermarking schemes, where the patient details are embedded in non-ROI region of an image. The encrypted image is divided into non overlapping tiles to identify region of interest and non-region of interest. In examination site examiner embeds patient details in non-ROI.

This research proposes to use wavelet transform and BAT algorithm proposed by Xin-She Yang [13] for medical image watermarking. The medical image is transformed into wavelet domain. The type of mother wavelet and level of scaling are two parameters that are of interest to look for while applying the algorithm. Watermark in this case is a patient image. This patient image is embedded into the medical cover image in transform domain. The extraction process is an inverse algorithm to embedding process. From the watermark embedding and extraction process two performance parameters are computed in the form of peak signal-to-noise ratio (PSNR) and normalized cross correlation (NCC). This procedure of watermarking gives unpredictable outcomes for medical images as cover images with out of bounds PSNR and NCC values. These unpredictable results of watermarking algorithm can be controlled using optimization algorithms such genetic algorithm (GA), particle swarm optimization (PSO) and ant colony optimization (ANO). This research uses BAT algorithm for optimizing the PSNR and NCC values during watermark embedding and extraction process. The results of simulation show a better performance of BAT algorithm over GA and non-optimization watermarking process for medical images with patient image as watermark.

Eswaraiah et al [14] proposed a Region of Interest (ROI) and Least Significant Bit (LSB) based fragile watermarking technique for tamper detection and recovery of medical images. At first, medical image is divided into ROI and NROI. Later, authentication information is inserted into ROI and recovery information into NROI. To increase embedding capacity in ROI, authentication information is compressed using Run Length Encoding (RLE) technique before inserting into ROI.

Crypto-watermarking strategy in multispectral images provides security where watermarking is used to preserve the monochromatic image and crypto protocol provides ownership protection of multispectral images during transmission through insecure medium .This method combines watermarking based on Arnold transform which create meaningless image of monochrome image embedded into three level DWT of multispectral image and utilizes modulus-shifting algorithm crypto protocol on multispectral image by [15].

III. SCHEMATIC BLOCK DIAGRAM

At first, the patient information which must be transmitted securely through internet is given to AES algorithm for encryption. By using 128 bit key it encrypts the information and gives the output as enciphered information for watermarking.

The algorithm takes 10 rounds for such encryption process. The output of AES that is enciphered information is then embedded into cover image. Again the embedded image is watermarked using DWT watermarking algorithm with its blocks. Finally the process produces the watermarked image as a result at sender side.

Now the watermarked image received by doctor at receiver side is first dewater marked and then decrypted to get original information.

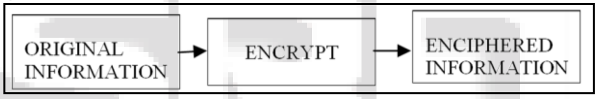


Fig. 1: Process of Encryption using AES Algorithm

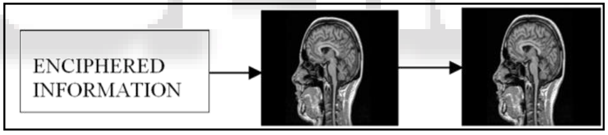
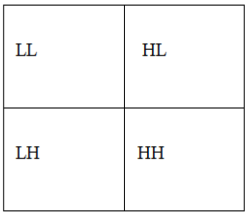


Fig. 2: Process of Watermarking using DWT Algorithm

IV. DWT WATERMARKING ALGORITHM

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The basic idea of discrete wavelet transform(DWT) in image process is to multi-differentiated decompose original signal into wavelet transform coefficients which contains the position information which comprises one low-frequency district(LL) and three high-frequency districts(LH,HL,HH).The original signal can be completely reconstructed by performing Inverse Wavelet Transformation on these coefficients.



LL	HL
LH	HH

Fig. 3: Single Level DWT Decomposition of an Image

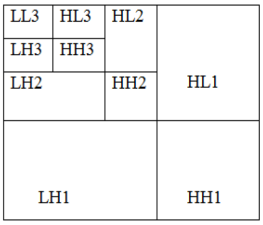


Figure 4. Three Level 2-Dimensional DWT Model

The four non overlapping coefficient sets of an image is shown in figure 1 and their corresponding coefficient sets are given below:

$$W_{LL}^{J} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} g(x)g(y)W_{LL}^{J-1}(2u-x)(2v-y)$$

$$W_{LH}^{J} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} g(x)h(y)W_{LL}^{J-1}(2u-x)(2v-y)$$

$$W_{HL}^{J} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} h(x)g(y)W_{LL}^{J-1}(2u-x)(2v-y)$$

$$W_{HH}^{J} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} h(x)h(y)W_{LL}^{J-1}(2u-x)(2v-y)$$

where J is the level of the 2-D DWT, g(n) and h(n)are the impulse responses of the low-pass and high-pass filters respectively and W0LL=W(u, v) is the original image.

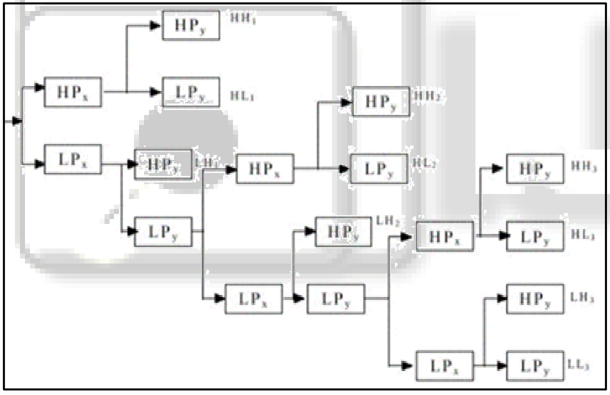


Fig. 5: Shows Schematic Diagram of Wavelet Transform

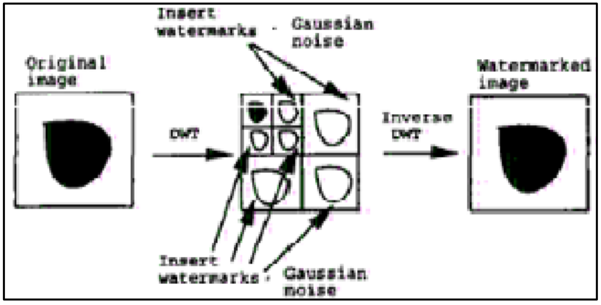


Fig. 6: Shows Decomposition & Reconstruction of an Image

A. *Watermark Embedding*

The algorithm to embed a watermark in the original image is summarized as follows:

1) Decompose the original image into four levels (thirteen subbands).
2) Any binary image with approximately equal number of 0s and 1s is utilized as a watermark image.
3) Generate a pseudo-random binary sequence containing either 1 or +1.
4) The subband pairs (LH3, LH2), (HL3, HL2), and (HH3, HH2) at level 3 and level 2 are selected to calculate the changes made in these middle frequency subbands.
5) The pseudo-random binary sequence generated from the binary image is rearranged in three different ways to be embedded in the LH3, HL3, HH3, LH2, HL2, and HH2 using the pixel-wise computation.
6) Apply the IDWT (Inverse Discrete Wavelet Transform) using the newly updated sub-band values at the level 3 and level 2 to obtain the watermarked image.

B. *Watermark Extraction*

Watermark detection is accomplished without referring to the original image.

1) Decompose the watermarked image into four bands.
2) Compare the watermark added in the HH1 band and the difference of the DWT coefficients in HH1 bands of the watermarked and the original images by calculating their cross correlations. If there is a peak, watermark is detected.
3) If 2 is not satisfied, do that in HL1 and LH1 bands, respectively.
4) If watermark is still not detected, compose the signals in the LL1 band into four additional subbands LL2, LH2, HL2, and HH2 and repeat 2-3.

V. AES ALGORITHM

AES is the short form of Advanced Encryption Standard. It is FIPS approved cryptographic algorithm used to protect electronic data. It is symmetric block cipher which can encrypt and decrypt information. Encryption part converts data into cipher text form while decryption part converts cipher text into text form of data. AES algorithm used different keys 128/192/256 bits in order to encrypt and decrypt data in blocks of 128 bits.

AES type	Key Length	Block Size	Number of rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Table 1:

AES is implemented in both hardware and software to protect digital information in various forms data, voice, video etc. The different transformations operate on the intermediate results, called states. AES uses a variable number of rounds, which are fixed:

During each round, the following operations are applied on the state.

1) Sub Bytes

Every byte in the state is replaced with the corresponding Rijndael S-Box.

2) Shift Row

Each row in the 4×4 array is shifted a certain amount to the left. It arranges the state in a matrix and then performs a circular shift for each row. This is not a bit wise shift. The circular shift just moves each byte one space over. A byte that was in the second position may end up in the third position after the shift. The circular part of it specifies that the byte in the last position shifted one space will end up in the first position in the same row.

3) Mix Column

A linear transformation on the columns of the state which states that transformation of a column to a new column.

4) Add Round Key

Each byte of the state is combined with a round key, which is different for each round and derived from the Rijndael key schedule.

A. AES Operations

1) Substitute Bytes Operation

The Sub Bytes operation is a non-linear byte substitution, operating on each byte of the state independently. The substitution table(S-Box) is invertible and it is not just a random permutation of these values in matrix and there is a well defined method for creating the s-box tables.

It is simply a table lookup using a 16×16 matrix of byte values called an s-box. This matrix consists of all the possible combinations of an 8 bit sequence (28 = 16×16 = 256) which is constructed by the composition of two transformations:

- Taking the multiplicative inverse in Rijndael finite field.
- Then applying an affine transformation which is documented in the Rijndael documentation.

Since the S-Box is independent of any input, pre calculated forms are used, if enough memory (256 bytes for one S-Box) is available. Each byte of the state is then substituted by the value in the S-Box whose index corresponds to the value in the state a (i, j) = SBox [a (i,j)] .

2) ShiftRow Operation

In this operation, each row of the state in cyclically shifted to the left, depending on the row index.

- The first row of state is not altered, since it is shifted 0 positions to the left.
- The second row is shifted 1 position to the left in a circular manner.
- The third row is shifted 2 positions to the left in a circular manner
- The fourth row is shifted 3 positions to the left in a circular manner.

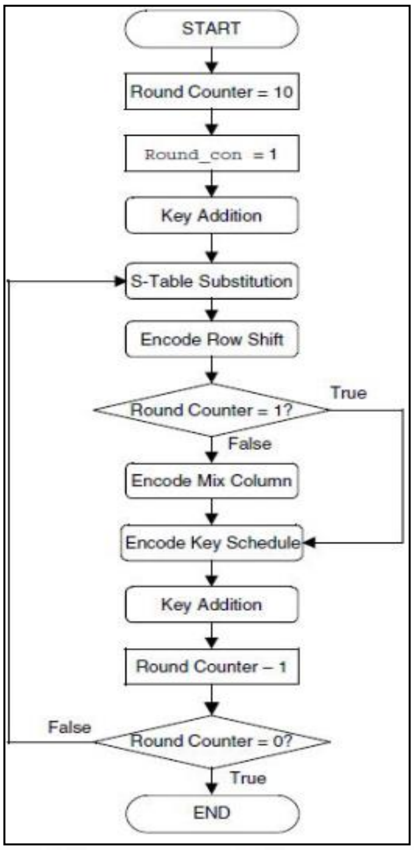


Fig. 5: Shows Flow Chart for AES Encryption Algorithm

3) MixColumns Operation

This stage (known as MixColumn) is basically a substitution and each column is operated on individually. It operates at the column level it transforms each column of the state to a new value that is a function of all four bytes in the column. The four bytes of each column of the state are combined using an invertible linear transformation.

4) The AddRoundKey Operation

In this stage, bits of state are bitwise XORed with the 128 bits of the round key. The operation is viewed as a columnwise operation between the 4 bytes of a state column and one word of the round key. This transformation is as simple as possible which helps in efficiency but it also effects every bit of state. The Round Key is derived from the Cipher key by the means of the key schedule. The Round Key length is equal to the block key length (=16 bytes).

VI. ADVANTAGES

The proposed system has the following advantages:

1) Transmission and storage overhead are reduced by using the proposed watermarking algorithm.
2) Since the proposed algorithm is eliminating the problem of transmission and storage overhead therefore no additional file is sent.
3) The diagnosis made by doctor and the prescribed data given by doctor is done so as to provide security and can n be sent to another doctor if required.
4) The data given by the doctor is inevitable so legal prosecution against the unintentional and intentional diagnosis made by the doctor can done easily if required.
5) The watermarking scheme does not influence the diagnosis made by reducing the visual clarity of the

image because the patient information is hidden and it is invisible and the imperceptibility of the image it does not change actually.

6) In any way the diagnosis value of the does not get lessened.
7) The proposed algorithm give a very effective utilization of memory and efficient transmission time and cost.
8) In various application such as copyright protection, owner identification and copy control the algorithm are very much applicable.
9) Encryption of information helps to protect certain watermarking attacks such as removal attacks, geometric attacks, etc.

VII. Conclusions

The paper contains information about the secured transmission of medical images along with the encrypted patient information .Related work focuses on watermarking using DWT algorithm and encryption using AES cryptographic algorithm .These processes helps in retaining the desired quality of the medical image .Thus the proposed paper provides better security, effective utilization of memory ,transmission cost and time .Finally eliminating the problem of transmission and storage overhead since no additional file is sent .

References

[1] Cox I J, Killian J, Leighton F T and Shamoon T, "Secure Spread Spectrum Watermarking for Multimedia". IEEE Transaction on Image Processing, vol.6, no, 12, pp.1673–1687(1997).

[2] M.D. Swanson, M. Kobayashi and A.H. Tewfik "Multimedia Data Embedding and Watermarking Technologies", Proceedings of the IEEE, vol. 86, no. 6, pp.1064 1087(1998).

[3] Podilchuk, Christine I., and Wenjun Zeng. "Image-adaptive watermarking using visual models." IEEE Journal on Selected Areas in Communications, vol.16, no. 4, pp.525539 (1998).

[4] Hartung, Frank, and Martin Kutter. "Multimedia watermarking techniques."Proceedings of the IEEE, vol. 87, no. 7 pp.1079-1107(1999).

[5] Hailey, D., P. Jacobs, J. Simpson, and S. Doze. "An assessment framework for telemedicine applications." Journal of Telemedicine and Telecare 5, no. 3, pp.162-170(1999).

[6] Güler, Nihal Fatma, and Elif Derya Übeyli. "Theory and applications of telemedicine", Journal of Medical Systems 26, no. 3 (2002): 199-220.

[7] Hailey, David, Risto Roine, and Arto Ohinmaa. "Systematic review of evidence for the benefits of telemedicine." Journal of Telemedicine and Telecare 8, no. suppl 1 (2002): 1-7.

[8] Smith, Anthony C., M. Bensink, N. Armfield, J. Stillman, and L. Cattery. "Telemedicine and rural health care applications." Journal of postgraduate medicine 51, no. 4 (2005).

[9] Zain, Jasni M., and Abdul RM Fauzi. "Medical image watermarking with tamper detection and recovery." In Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE, pp. 3270-3273. IEEE, 2006.

[10] Navas, K. A., and M. Sasikumar. "Survey of medical image watermarking algorithms." In Proc. Internation Conf. Sciences of Electronics, Technologies of Information and Telecommunications, pp. 25-29. 2007.

[11] Irany, Behrang Mehrbany, Xin Cindy Guo, and Dimitrios Hatzinakos. "A high capacity reversible multiple watermarking scheme for medical images." In Digital Signal Processing (DSP), 2011 17th International Conference on, pp. 1-6. IEEE, 2011.

[12] Lavanya, A., and V. Natarajan. "Watermarking patient data in encrypted medical images." Sadhana 37.Part 6 (2012).

[13] Xin-She Yang and Amir H. Gandomi, Bat Algorithm: A Novel Approach for Global Engineering Optimization, Engineering Computations, Vol. 29, Issue 5, pp. 464--483 (2012).

[14] Eswaraiah, R.; Reddy, E.S., "A Fragile ROI Based Medical Image Watermarking Technique with Tamper Detection and Recovery" Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on , vol., no., pp.896,899, 7-9 April 2014.