ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 7, Issue 7, July 2018

Medical Data Security using combination of Cryptography and Steganography with AES-LSB algorithm

Nayana Banjan, Prajkta Dalvi

***Abstract*— Transfer of medical data is a daily routine. But with that, information security has become a major concern in today's world. For this purpose, we have introduced the concept of cryptography and steganography in this paper. Cryptography is used to encrypt the original data by using symmetric key cryptography while steganography is used to hide that data in a cover medium such as audio, video, files or image. In this paper, patient's data is first encrypted using Advanced Encryption Standard Algorithm and then the encrypted data is hided in a medical image using image steganography by Least Significant Bit Algorithm. This hided data in the cover image is sent to the intended receiver. Inverse method in the receiver side is used to obtain the original data. This concept provides more security to the data as combination of cryptography and steganography is used which are illustrated using different evaluation parameters. This concept is implemented on MATLAB R2016a software. Besides using this method in medical field, it can also be used in satellite and military fields.**

***Index Terms*— Advanced Encryption Standard (AES), Least Significant Bit (LSB), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Stego**

I. INTRODUCTION

Cryptography is used to ensure that the contents of a message are very confidentiality transmitted and would not be altered. Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Cryptography serves following purposes:

Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of a message.

Authentication: Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.

Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.

Non- repudiation: Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.

Access Control: Access Control specifies and controls who can access what.

Availability: The principle of availability states that resources should be available to authorized parties all the times. [9]

Cryptography consists of two types:

1. Symmetric Key cryptography: When the same key is used for both encryption and decryption, then that mechanism is known as symmetric key cryptography. E.g. Data Encryption Standard (DES), AES, Triple DES, Blowfish algorithm.
2. Asymmetric Key cryptography: When two different keys are used, that is one key for encryption and another key for decryption, then that mechanism is known as asymmetric key cryptography. E.g. RSA algorithm. [10]

Steganography is the art and science of writing hidden messages in such a way that no one, except the sender and intended recipient, suspects the existence of the message, a form of security through hiding the message.ie., Steganography is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it. Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling. Like cryptography different types steganography techniques are available based on the hiding techniques, cover medium used etc.

Steganography techniques include image steganography, video steganography, text steganography etc.

In this paper, we have implemented image steganography which includes the following algorithms such as LSB algorithm, Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) algorithm.

II. LITERATURE SURVEY

Et.al. V.Mahalakshmi, S.Satheeshkumar and Dr.S.Sivakumar explained that the rapid development of data transfer through internet has made it easier to send the data accurate and faster to the destination. Unauthorized users modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are many approaches like Cryptography, Steganography, etc. In the information era, information sharing and transfer has increased exponentially. The information vulnerable to unauthorized access and interception, while in storage or transmission. Steganography is the major technique for secret communication. In this paper, image steganography and its different security methods to secure a medical image, particularly Magnetic Resonance Imaging (MRI). In steganography, the contents of the secret message is embedded into the cover medium. Three different steganographic algorithms is used, Least Significant Bit (LSB) algorithm, Division into block and Mean change modified method. The measurements are SSD (Sum of Squares of Differences), SAD (Sum of Absolute Differences), MAD (Maximum Absolute Differences) and Peak Signal to Noise Ratio (PSNR) are used to comparing them in terms of speed and accuracy. This paper was published in International
Journal of Computational and Applied Mathematics, Volume 12, Number 1 (2017). [6]

Et.al. Pratiksha Sethi and V. Kapoor proposed a technique which is adoptable for hiding information in image securely additionally that consumes less space complexity. In the proposed system, the file which user want to make secure is firstly compressed to shrink in size and then the compressed data is altered into cipher text by using AES cryptographic algorithm and then the encrypted data is concealed in the image. In order to hide the information over the image in complex manner the genetic algorithm based technique is implemented which is used to evaluate the valuable pixels where the data can be hide in a secure manner. In addition of that, for hiding the information in images, the LSB (least significant bits) based steganographic method is used after the selection of eligible pixels. The implementation of the anticipated technique is performed using JAVA technology and for performance evaluation the time and space complexity is computed. In addition of that a comparative study of the proposed technique using the image steganographic technique is also performed in terms of PSNR and MSE. This paper was published by International Journal of Computer Applications, Volume 144, Number 9, June 2016. [5]

Et.al. Manish Trehan and Sumit Mittu suggested about how the data is embedded in the medical scanned images through the combined approach using both cryptography and steganography. The information and diagnosis by doctor both serve as the confidential information and hence is treated as secret data. The proposed LSB algorithm attempt to keep this secret data secure and at the same time, make the patients treatment accurate and fast. The approach is divided into two modules: embedding data and extraction of data from the patient scanned x-ray. The first module contains two main techniques: cryptography and steganography. In this the patient instead of any paper report is provided with the x-ray scanned containing the patient history and diagnosis. The second module contains the stego extraction, decryption algorithm and one added technique by which the doctors diagnose and patient history both is stored in the database for future reference. This paper was published by International Journal of Engineering Research and Technology (IJERT),
Vol. 4 Issue 06, June 2015. [1]

Et.al.by Md. Khalid Imam Rahmani, Kamiya Arora, and Naina Pal suggested a paper which describes the survey of both cryptography and steganography methods. The two important aspects of security that deal with transmitting information or data over some medium like Internet are steganography and cryptography. Steganography deals with hiding the presence of a message and cryptography deals with hiding the contents of a message. Both of them are used to ensure security. But none of them can simply fulfill the basic requirements of security i.e. the features such as robustness, undetectability and capacity etc. So a new method based on the combination of both cryptography and steganography known as Crypto-Steganography which overcome each other weaknesses and make difficult for the intruders to attack or steal sensitive information is being proposed. This paper also describes the basics concepts of steganography and cryptography on the basis of previous literatures available on the topic. This paper was published by International Journal of Advanced Computer Science and Applications, Volume 5, Number 7, 2014. [4]

III. PROPOSED METHOD

The basic block diagram of the method is given as follows:

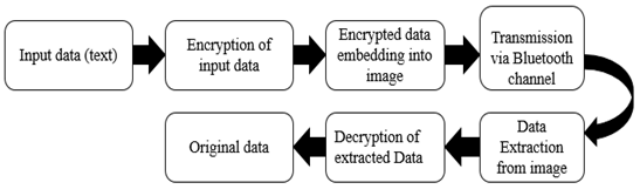

Fig.1 Basic Block Diagram

The block diagram of the proposed method is as follows:

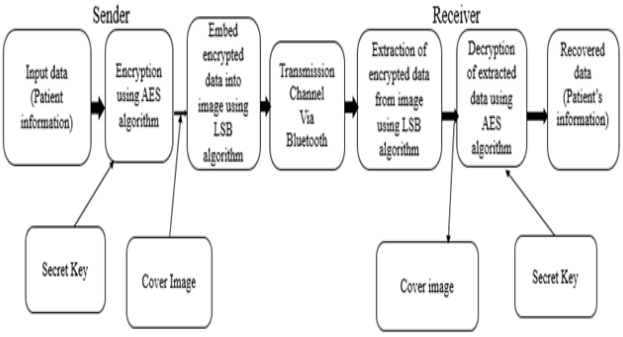

Fig. 2 Proposed System Model

Principle of working:
The input to the system is the patient's personal information such as the patient's name, age, gender, the disease diagnosed with etc. This input data is first encrypted using AES algorithm by using a 192 bit secret key. The encrypted data is then hided in a cover image of 8 bit using LSB algorithm. This image is then send to the intended receiver using Bluetooth module. The receiver will first extract the data from the stego image using LSB algorithm and then it is decrypted using AES algorithm by applying the same secret key of 192 bit. The original data is then obtained.

IV. ALGORITHM

MATLAB 2016a is used for the implementation.

A. Introduction to AES algorithm

Advanced Encryption Standard (AES) is a standard for the encryption of electronic data. The U.S. government held in 1997 and now use in worldwide. AES is a symmetric-key algorithm which means that the same key is used both of sender and receiver. AES algorithm is of three types i.e. AES-128, AES-192 and AES-256.

(1)AES algorithm for encryption of data
Step 1: Enter the patient's data that is to be encrypted.
Step 2: Enter the secret key.
Step 3: The 128 bit data is divided into 16 Bytes. These bytes are mapped to a 4*4 array called as the state.
Step 4: AES operations such as Sub Bytes, Shift Rows, Mix Columns and Add Round Key are performed.
Step 5: Obtain the encrypted data.

(2) AES algorithm for decryption of data
Step 1: Read the encrypted message.
Step 2: Enter the same secret Key used by the sender.
Step 3: Apply inverse steps of Advanced Encryption Technique.
Step 4: Obtain the original data.

B. Introduction to LSB Algorithm

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file.

(1) LSB algorithm for data hiding
Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4; Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image.
Step 6: Calculate MSE and PSNR of the stego image.

(2) LSB Algorithm for Data Extraction
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.
Step 4: Obtain the hidden data and the cover image.

V. EVALUATION PARAMETERS

We have implemented this project using AES with LSB and AES with DWT algorithms. In order to compare our results, we have used evaluation parameters such as MSE and PSNR. The evaluation parameters are given below: [13]

1. Mean Square Error (MSE)

It is a figure of merit which indicates the degree of similarity or differences between two images. Lesser the MSE value of an image better is the quality and less distortion from the original.

$$\text{MSE}=\frac{1}{M}\times\frac{1}{N}\sum_{i=0}^{M}\sum_{j=0}^{N}(x(i,j)-y(i,j))^2 \quad \text{.....(1)}$$

Where,
M-Total number of rows
N-Total number of columns
(i,j)- (rows, columns)
x- Original Image
y- Reconstructed Image

2. Peak Signal to Noise Ratio (PSNR)

It is the ratio between maximum possible power and corrupting noise that corrupts the representation of the image.
Higher is the value, better is the quality of the image.

$$\text{PSNR}=10\log_{10}\frac{(2^n-1)^2}{MSE} \quad \text{.....(2)}$$

Where,
n- Number of bits in Cover Image

VI. RESULT AND ANALYSIS

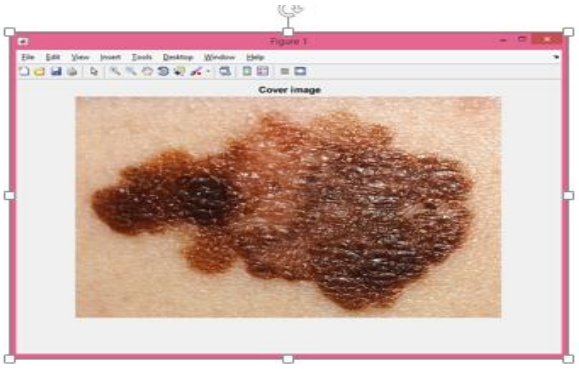

Fig 3: Cover image

Fig. 4: Stego image

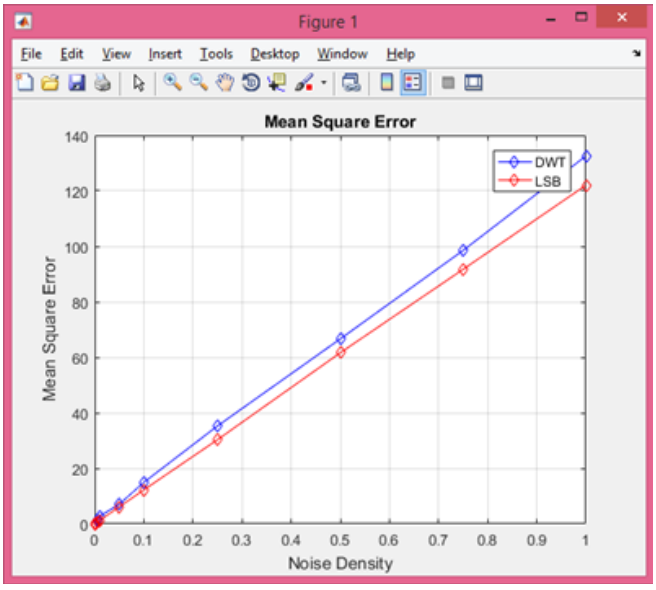

Fig.5: Comparison of MSR values

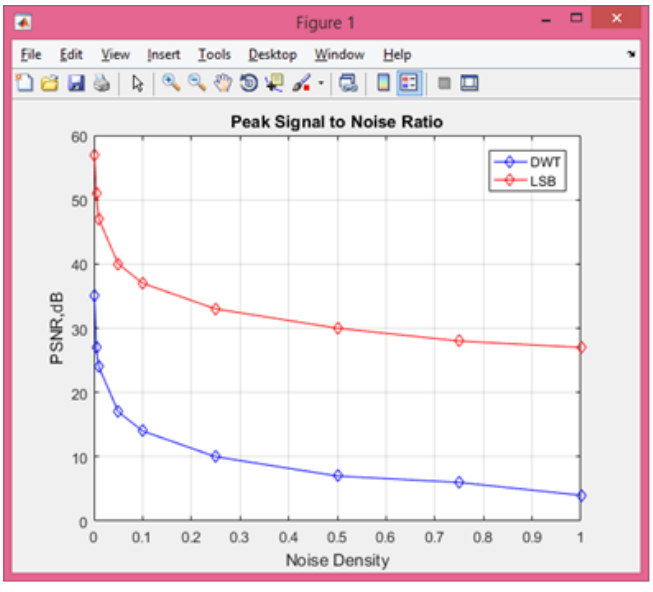

Fig. 6: Comparison of PSNR values

Table I: Comparison of various image formats

Image format	PSNR	MSE
.jpg	58.2430	0.0982
.png	57.0244	0.1363
.tif	58.0619	0.1248
.bmp	57.7467	0.1336

For better efficiency of the project, high PSNR and less MSE is required. Fig.5 presents a graph based on mean square error v/s noise density. The graph shows that the project implemented using Advanced Encryption Standard algorithm with Least Significant Bit steganography gives less Mean Square Error as compared to Advanced Encryption Standard algorithm with Discrete Wavelet Transform steganography.

Fig.6 presents a graph on Peak Signal to Noise Ratio v/s Noise Density. The graph shows that the project implemented using Advanced Encryption Standard algorithm with Least Significant Bit steganography gives high Peak Signal to Noise Ratio as compared to Advanced Encryption Standard algorithm with Discrete Wavelet Transform steganography.

Table 6 specifies the different image formats of Cover Image that can be used to hide the encrypted data. Among all the given formats, .jpg format provides high PSNR and less MSE.JPEG files use data loss compression and redundant graphical information is discarded by this method without a significant impact on the picture. Therefore, cover image must be in .jpg format to obtain better results.

VII. CONCLUSION

We have implemented the concept of cryptography and steganography for the security of medical data. Two methods were used i.e. AES cryptography with LSB steganography and AES cryptography with DWT steganography. AES encryption used here can process data of 128 bit and uses a key size of 192 bit. The results of both the methods are compared using evaluation parameters i.e. MSE and PSNR. Better Peak Signal to Noise Ratio and less Mean Square Error is obtained for AES cryptography with LSB steganography. Also we have compared various image formats used for the cover image in which the data is to be hided. Based on image formats like .jpg, .png, .tif and.bmp, .jpg gives better results.

For future purpose, the results can be made better by using AES encryption with a key size of 256 bit. Instead of LSB or DWT steganography, Discrete Cosine Transform steganography can also be used.

ACKNOWLEDGMENT

All the authors are thankful to Usha Mittal Institute of Technology for providing the necessary facilities and support. We are thankful to our principal Dr. Sanjay Pawar for the necessary guidance. We are also thankful to all teaching and nonteaching staff for their support.

REFERENCES

[1] Sumit Mittu and Manish Tehran, "Steganography and Cryptography Approaches Combined using Medical Digital Images", *International Journal of Engineering Research and Technology (IJERT)*, Vol. 4, Issue 06, pp. 189-192, June 2015.
[2] Srinath N K, Usha B A, Narayan K and Tushara C K, "Analysis of Data Embedding Technique in Image Steganography A Survey", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 3, Issue 6, pp.7306-7311, June 2014.
[3] Vinay Pandey, Angad Singh and Manish Shrivastava, "Medical Image Protection by Using Cryptography Data-Hiding and Steganography",' *International Journal of Emerging Technology and Advanced Engineering*, Vol. 2, Issue 1, pp. 106-109, January 2012.
[4] Md. Khalid Imam Rahmani, Kamiya Arora and Naina Pal, "A Crypto-Steganography: A Survey", *International Journal of Advanced Computer Science and Applications*, Vol. 5, no. 7, pp. 149-155, 2014.
[5] Pratiksha Sethi and V Kapoor, "A Secured System for Information Hiding in Image Steganography using Genetic algorithm and Cryptography", *International Journal of Computer Applications*, Vol. 144, No. 9, pp. 5-11, June 2016.
[6] V Mahalakshmi, S Satheeshkumar and Dr. S Sivakumar, "Performance of Steganographic Methods in Medical Imaging", *International Journal of Computational and Applied Mathematics*, Vol. 12, no. 1, pp. 549-556, 2017.
[7] Ming YANG, Monica TRIFAS, Lei CHEN, Jaleesa ELSTON, Dorothy BUENOS-AIRES and Lei SONG, "'Secure Patient Information and Privacy in Medical Imaging", *Systematics, Cybernetics and Informatics*, Vol. 8, No. 3, pp. 63-66, 2010.
[8] A Joseph Amalraj and Dr. J John Raybin Jose, "A Survey paper on Cryptography Techniques", *International Journal of Computer Science and Mobile Computing*, Vol. 5, Issue 8, pp. 56-59,August 2016.
[9] Mitali, Vijay Kumar and Arvind Sharma, "A Survey on various Cryptography Techniques", *International Journal of Emerging Trends and Technology in Computer Science*, Vol. 3, Issue 4, pp. 307-312, July- August 2014.
[10] Vishnu S Babu and Prof. Helen K J,"A study on combined Cryptography and Steganography", *International Journal of Research Studies in Computer Science and Engineering*, Vol. 2, Issue 5, pp. 45-49, May 2015.
[11] Rahul Joshi, Lokesh Gagnani and Salony Pandey, "'Image Steganography with LSB", *'International Journal of Advanced Research in Computer Engineering and Technology*, Vol. 2, Issue 1, pp. 228-229, January 2013.
[12] Manish Shrivastava and Vinay Pandey, "Secure Medical Image Transmission using Combined Approach of Data-hiding, Encryption and Steganography", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, Issue 12, pp. 54-57, December 2012
[13] Farhan R. Patel, Dr. A N Cheeran, "Performance Evaluation of Steganography and AES encryption based on different formats of the image", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 4, Issue 5, pp.659-664, May 2015.

The author has pursued Bachelor of Technology in Electronics from Usha Mittal Institute of Technology, SNDT Women's University, Mumbai. The author has previously published a research paper on image processing.

The author has pursued Bachelor of Technology in Electronics from Usha Mittal Institute of Technology, SNDT Women's University, Mumbai. The author has previously published a research paper on image processing.