International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

ENHANCE SECURITY FOR MEDICAL IMAGES THROUGH SECURE FORCE CRYPTOGRAPHY WITH STEGANOGRAPHY TECHNIQUES

S.Durgadevi[1], S.Jayasrilakshmi[2], S.Mohanraj[3], M.S.Anbarasi[4]

[1,2,3] Final year B. Tech, Dept. of Information Technology, Pondicherry Engineering College, Puducherry, India
[4]Assistant Professor, Dept. of Information Technology, Pondicherry Engineering College, Puducherry, India

---

Abstract - *A lot of techniques are used to protect and hide information from any unauthorized users such as Steganography and Cryptography. Steganography hides a message inside another message without any suspicion, and Cryptography scrambles a message to hide its contents. A united technique for information security has been incorporated using Cryptography and Steganography techniques for information security to prevent unauthorised access or unwanted interventions. It ensure a double layer of information security by both converting data in some other form and hiding its existence. In this project, we have a tendency to planned a hybrid security model for securing the diagnostic text information in medical images. Our system is developed through integrating steganography technique for image combining and extraction with hybrid encryption scheme. The planned hybrid encryption schema is constructed using a modified Secure Force (SF) for image encryption algorithms. The encrypted secret data has been hidden in a cover image using JSteg and LSB coding for steganography ensuring a highly secure communication.*

Key Words: **Steganography; Peak Signal-to- Noise Ratio (PSNR); Structured Similarity (SSIM); Cryptography; Advance encryption standard (AES); Secure force algorithm; Correlation. Jpeg image Steganography (JSTEG).**

1. INTRODUCTION

Information hiding may be a powerful technique utilized in information security. It takes two general approaches Cryptography and Steganography to hide internet communications.

1.1 Steganography

Steganography is the art and science of invisible communication in the sense that it does not specify anything whether any communication is taking place or not. Arithmetic secret writing was applied on secret message for lossless compression, that provided ~22% higher embedding capability. The compressed secret message is subjected to AES encryption; this provides higher security inside the cases of steganalysis attacks. Once compression and encryption were completed, LSB substitution and MPVD area unit are applied [12]. It is accomplished by hiding information in any other form of information, thus hiding the existence of the original information to be transmitted. Steganography means hat to hide messages' existence in another medium (audio, video, image, communication).Steganography is totally completely different from cryptography at intervals the sense that cryptography focuses entirely on keeping the contents of a message secret, whereas steganography focuses on keeping the existence of a message secret. Image steganography in which the information is hidden exclusively in images uses LSB algorithm. The two necessary conditions for the steganography security area unit obtained. Under the present technology state of affairs, analyze the identicalness of the cover and stego-cover, and think about that the steganography security ought to trust the key secrecy with algorithms open [11].The higher level security one has the higher level attacks one can resist.By specifying the role of key in steganography, the reqired conditions for a secure steganography algorithm rule in theory are formally conferred Image steganography terminologies are as follows:-

- **Cover-Image**: Original image that is expressly used as a carrier for hidden information to be transmitted.
- **Message**: Actual information that is utilized to cover into pictures. Message can be a comprehensible plain text or another image.
- **Stego-Image**: When embedding message into cover image what we tend to get is thought as stego-image.
- **Stego-Key**: A key that is used for embedding or extracting the messages from cover-images and stego-images.

1.2 Cryptography

Cryptography may be defined as a study of methods or techniques that involve security of data to be transmitted across a network. Cryptography involves encoding and decoding of data to prevent it from any alteration, modification or just listening of data by a third party. Cryptography is one amongst the most techniques that's being employed in computer security that converts information from its original form into associated indecipherable form.

1.3 Encryption

Encryption is the technique that converts any readable format into non-readable format. It takes any plain text and converts it into non-readable format with the use of any algorithm which may or may not use any key (or keys).

1.4 Decryption

Decryption is just the inverse process of encryption. It converts non-readable format into readable form by taking the encrypted text known as cipher text as input and applying the decryption algorithm to it, giving us the original plain text.

2. LITERATURE SURVEY

2.1 Survey on the Combination of Crypto-Watermarking techniques

A hybrid technique exploitation Watermarking and Cryptography was given in, for a transmission of protected text message. This scheme was supported on XOR cipher, Fibonacci series, PN sequence, RSA, Hill cipher, one bit, two bit Least Significant Bit (LSB) and three bit LSB. It evaluated the standard of watermarked images on the premise of Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), and Mean Square Error (MSE). It was absolutely determined that the one-bit LSB watermarking was higher as associated with to the two-bit LSB watermarking and three-bit LSB watermarking as a result of MSE and RMSE were small and PSNR was large [2] As an example, Patients and healthcare workers in one location cipher vital medical images via the planned quantum encryption scheme, sending the cipher images to the cloud [8]. The health care workers in another location accesses the images from the cloud, decrypting the content via the decryption techniques.

2.2 Survey on the Medical data transmission model for IoT-based Healthcare systems

Hybrid encryption schema is constructed employing a combination of Advanced Encryption Standard (AES), and Rivest, Shamir, and Adleman (RSA) algorithms [10]. The proposed model starts by encrypting the secret data; then it hides the result in a cover image using 2D-DWT-1L or 2D-DWT-2L. Each color and grayscale images are used as cover images to hide completely different text sizes.

2.3 Survey on the Image Steganography technique

Image Steganography using LSB Substitution Technique which consists of overview of steganography and techniques used in steganography and further have proposed a new approach in steganography based on Direct Wavelet remodel exploitation NSGA (Non Dominated Sorting Algorithm) for higher quality of stego image. Image steganography system is comprised two algorithms, one for embedding and one for extraction [2]. The embedding methodology hides a secret message among a canopy media (cover image), and also the result of embedding process is stego image. The main issue is that the key message won't be unperceived if a 3rd party tries to intercept the quilt media (cover image).The extraction methodology is alone as a result of it's the inverse of the embedding methodology, wherever the secret message is disclosed at the end. Image steganographic techniques like as Transform Domain based, Spatial Domain based, Palette based steganographic techiques[9].

2.4 Difference between Cryptography and Steganography

Cryptography prevents unauthorized party from discovering the content of communication [3] .However Steganography prevents discovery of the existence of communication (i.e., Cryptography makes knowledge meaningless and notable the message passing whereas Steganography tends to cover presence of hidden information and unknown the message passing).Cryptography alters the structure of secret message whereas Steganography doesn't alter the structure of secret message. Information hiding [7] aims to embed secret data into the multimedia system like image, audio, video, and text .In this study, two new quantum information activity approaches area unit advises. A quantum steganography approach is planned to a quantum secret image into a quantum cover image. A quantum image watermarking approach

is conferred to cover a quantum watermark gray image into a quantum carrier image.

2.5 Survey on the Hybrid Cryptographic techniques

Cryptography means data encryption and decryption. Encryption is the process of encrypting messages in a way that unauthorized persons cannot read it. The main algorithms used for data encryption are the Advanced Encryption Standard (AES) and the Secure Force algorithm [SF algorithm] [3]. AES is a symmetric encryption where the same key is used on both side. It has a fixed message block and keys of length. Longer keys make the cipher more difficult to break. The hybrid cryptographic encryption methods improve levels of security with authentication.

2.6 Survey on Content Based Image retrieval (CBIR) in cloud computing

Privacy in image retrieval becomes the most issue in CBIR outsourcing [4]. As an example, patients might not need to disclose their medical pictures to any others except to a particular doctor in medical CBIR applications. To formulate the matter, this paper considers 2 sorts of privacy threats. Firstly, a curious cloud server might investigate the owner's info for extra info. Secondly, once receiving the retrieved pictures, the question user might illicitly distribute these pictures to somebody unauthorized for edges. a completely unique quantum steganography framework for secure messages in fog cloud IoT is planned [5] . The approach relies on quantum entangled states, exclusive OR operation (XOR), gray code, and hash perform.

2.7 Survey on the Text steganography for hidden transmission of data

A novel text steganography technique referred to as AITSteg that provides finish-to-end security throughout the transmission of text messages via SMS or social media between end users [6]. The AITSteg technique is evaluated by considering a trustworthy state of affairs. AITSteg is in a position to stop varied attacks, together with man-in-the-middle attacks, message revelation, and manipulation by readers. A picture steganography approach supported Inverted LSB (ILSB) technique for securing the transmitted face pictures from the information processing camera because the IoT device to the house server within the local area network.

2.8 Survey on the Secure Force Cryptographic Algorithm

In Wireless detector Networks (WSN) the implementation of the SF algorithmic program [1] offers terribly low quality design. The encoding and decipherment method is sort of similar during this algorithmic program. The 5 encoding rounds will increase the effectiveness of the encoding procedure. This is often a four step algorithmic program supported straightforward mathematical operations (six numbers of operations) that operates on a four bit knowledge. However this causes an enormous quantity of confusion and spreading of information is formed to combat dissimilar styles of attacks. This algorithmic program consists of 4 steps. They are 1. Key elaborate 2. Key execute protocol 3. Encipher process 4. Decipher process.

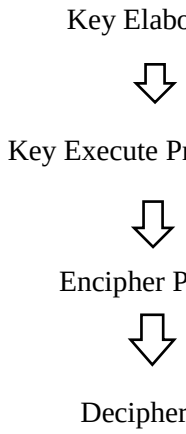

Fig -1: Secure Force Algorithm

3. OVERVIEW OF THE SYSTEM

3.1 Problem Definition

Image steganography needs to satisfy perceptual transparency, capacity of hidden data and robustness. The focus of the proposed system is to exploit the use of steganography in secure communication and information since the available image steganography techniques are:

1. Visual attacks
2. Structural attacks
3. Statistical attacks

3.2 System Model

In the proposed method, the data security mechanism for the storage system, in which the

cover image being enhanced and find its intensity. To compress the image, Huffman encoding is used to lossless compression. The error rate of the compressed image is very less when it is compared to other coding techniques. Our system provides cover image, that should be enhanced by histogram equalization and the original image is encrypted by using the Secure Force algorithm (SF algorithm) and Advanced Encryption Standard (AES) in a cryptography techniques. The enhanced cover image and encrypted original image needs to embedded by using JSTEG and LSB the steganography .Then the Huffman coding is a lossless compression, used to compressed the embedded image. The proposed system focuses on improving the current work in terms of reducing the time complexity and it reduce the complexity of encryption process.

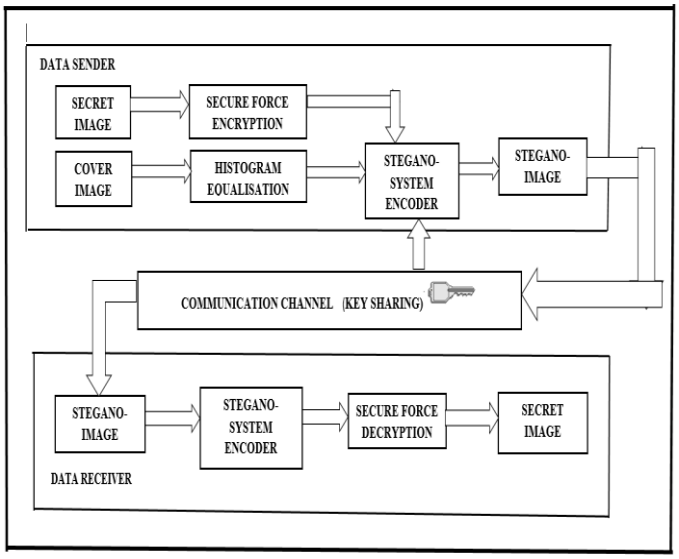

Fig -2: Architecture Diagram for Enhance security for medical images using secure force cryptography with Jsteg stegnographic techniques.

3.3 Cover Image Enhancement and Intensity finding

In this module, get any format of image / frame from the selected directory or current working directory. After getting the input image from directory, read the input image, if not read the image didn't go to another steps. After reading the input image, it will be converted into gray scale form. Then calculate the intensity values for input image in gray scale form. Enhance the input image. By finding the probability mass function & cumulative density functions. Then finally get the enhanced image.

3.4 Secret Image Cryptographic Techniques

In this module, get any format of image / frame from the selected directory or current working directory. After getting the secret image from directory, read the secret image. If not read the image didn't go to another steps. After reading the input image, it may converted into gray scale form. Apply SF with AES algorithm to it. Finally get the encrypted image.

3.5 Embedding and extraction of secret image over cover image

From cryptographic and enhancement module, outputs are combined by embedding method, to get the embedded image. After the data embedding, embedded image is kept for encoding. This encoding is used for data transmission. Then applies to de-embedding scheme to get the recovered image and message image separately. After that, decrypt the message image, to get the exact message image.

3.6 Input & Output

Input – The scanned Medical images of the patients as shown in Fig-3 are given as input.

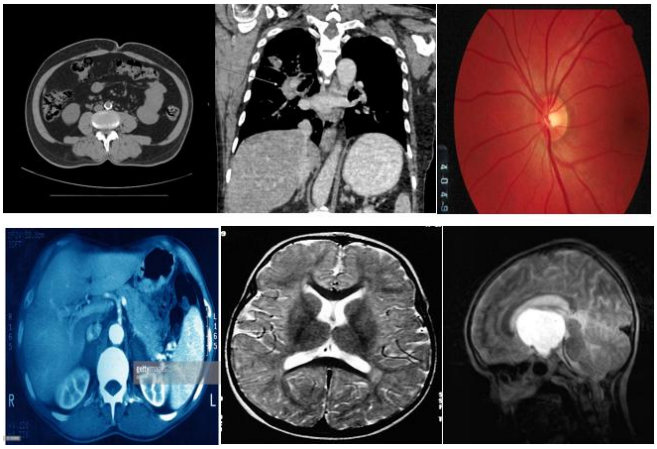

Fig -3: Secret medical images

The sender will choose the cover image as shown in Fig -4 are given as input.

Fig -4: Cover images

Output – The stegno-image is obtained by combining encrypted secret image over cover image as shown in Fig-5 respectively.

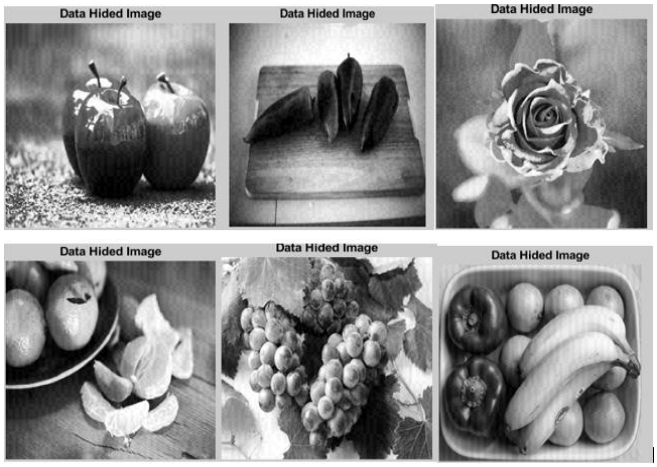

Fig -5: Secret image embedded with grayscale cover image

4. EXPERIMENTAL RESULTS AND EVALUATION

4.1 Simulation Environment

The implementation of our projected system was meted out victimisation the MATLAB R2018a and MATLAB R2014a package running on a private pc with a two.07 gigacycle Intel (R) Core (TM) I3 central processing unit, four GB RAM and Windows ten because the software system. The metric calculation determines the standard of the projected security model. These metrics calculate the quantitative relation between the first image and therefore the stego image. The obtained results were evaluated supported 3 parameters; the height Signal to Noise quantitative relation (PSNR), Structural Similarity (SSIM) and Correlation. PSNR calculates the physical property of the stego-image. The upper the worth of PSNR of stego image reveals a better quality of stego image or a better physical property of hidden message. SSIM measures the structural similarity between 2 pictures. Its price ranges between -1 and one. Once 2 pictures are nearly identical, their SSIM is near to one. Correlation determines what quantity 2 signals or vectors are similar or totally different in part and magnitude once 2 sets of knowledge are powerfully connected along. It reaches its most once the 2 signals are similar. It's calculated by victimisation the subsequent equation: Correlation = Where n is that the variety of pairs of knowledge, X is that the input image, and Y is that the stegno image.

4.2 Security Analysis

In this model, the comparisons were conducted between the duvet image and therefore the stego-image. That is to ensure less distortion happens inside to the first cowl image when concealing the key message image. The image is encrypted by mistreatment the secure force coding methodology. Then it's being embedded mistreatment JSteg stenography techniques. it absolutely was found that JSteg provides higher PSNR and SSIM results compared with different steganographic techniques just in case of each color and grey scale pictures as shown in Fig.7 severally. it absolutely was found that PSNR and SSIM values for each embedding and extracting stay same which supplies lossless compression. The correlation were nearly adequate to one with all of the colour and grey pictures as shown in Fig-8 severally.For evaluation one of the image in Fig -4 was taken and shown in Fig-6 respectively.

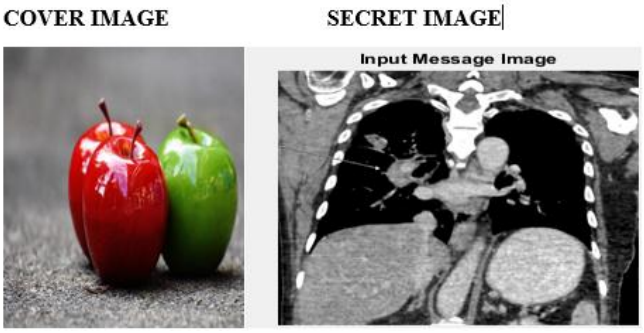

Fig -6: Cover and Secret message image for analysis

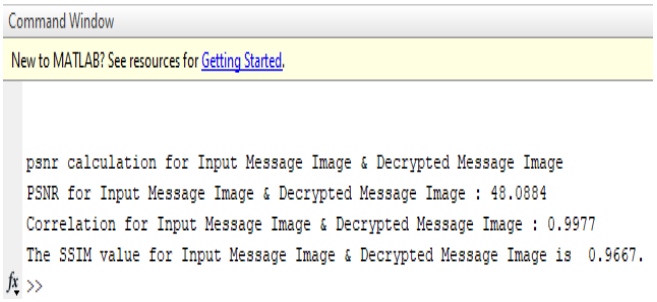

Fig -7: Metric calculation for embedded image

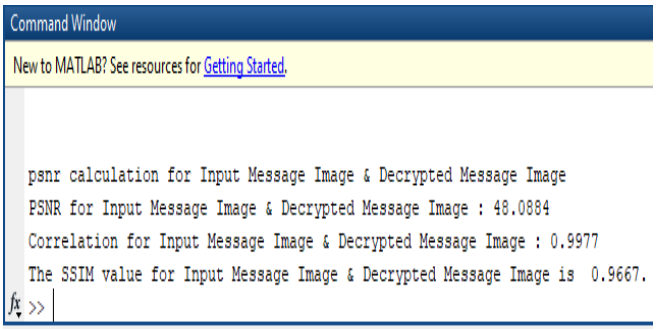

Fig -8: Metric calculation for extracted image

The intensity values for enhanced cover and stegno image was plotted with number of pixels in X-axis and Pixel values in Y-axis as shown in Chart -1 respectively.

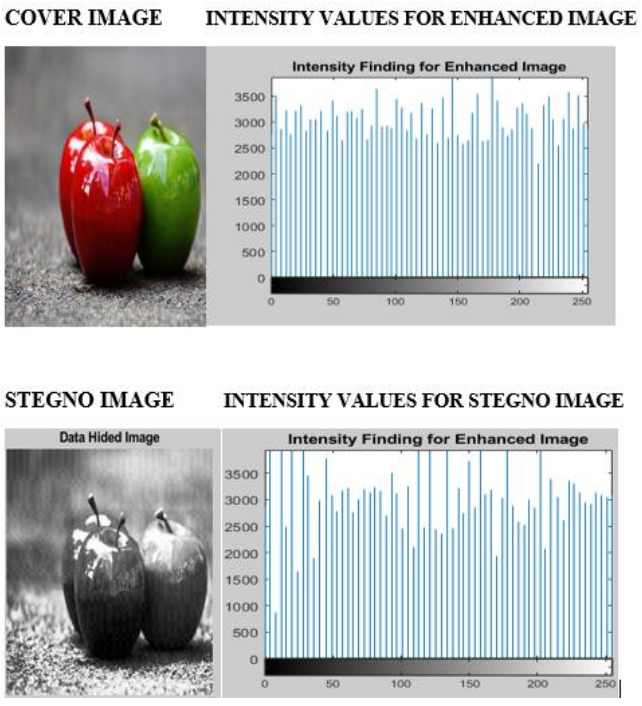

Chart -1: Intensity finding for Cover and Stegano image

5. CONCLUSIONS AND FUTURE ENHANCEMENT

In this paper, a replacement secure communication model has been given that mixes cryptography and steganography techniques to provide a pair of layer of security, that the steganalyst can't reach to plaintext whereas not knowing the key key to decipher the ciphertext. First of all the key photos has been encrypted by using the Secure Force-AES algorithmic program then the encrypted photos has been hidden in cowl image by using JSTEG and LSB ways. As a result of this combine, the key image can transmit over open channel as a results of the cipher image does not look meaningless but its presence is hid by using steganography for concealing cipher image at intervals the cowl photos. The two parameters such PSNR and MSE are calculated. At intervals the long run work, we have a tendency to tend to are attempting forward to try and do applying the projected methodology on audio and video. Also, we have a tendency to tend to ar attempting forward to strengthen the projected methodology to form the aptitude over it whereas keeping an analogous PSNR or higher.

REFERENCES

[1] Sonali Mishra, Ananya Dastidar "Hybrid Image Encryption and Decryption using Cryptography and Watermarking Technique for High Security Applications"IEEE International journals, 2018.

[2] B.G.Aagarsana1, Anjali, T.K.Kirthika, Mr. S. Sivakumar "Image Steganography using secured force algorithm for hiding audio signal into colour image", IRJET access Volume 5, Feb 2018.

[3] Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara " Data security using Cryptography and Steganography techniques", IJACSA access, Vol 7, 2016 November.

[4] Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun and Kui Ren " A privacy preserving and copy-deterrence content based image retrieval scheme in cloud computing" IEEE access, Vol 11, November 2016.

[5] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, M. Shamim Hossain, Senior Member Samir Elmougy and Ahmed Ghoniem, "Secure quantum steganography protocol for fog cloud Internet of Things", IEEE access, 2018.

[6] MiladTale by Ahvanooey, QianmuLi, Jun Hou1, Hassan Dana Mazraeh and Jing Zhang "AITSteg: An Innovative Text

Steganography Technique for Hidden Transmission of Text Message via Social Media",IEEE Access,Volume:XX,August,2018.

[7] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, M. Shamim Hossain, Senior Member Samir Elmougy and Ahmed Ghoniem, "Efficient quantum information hiding for remote medical image sharing", IEEE access, 2017.

[8] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty and Muhammad Talha, "Robust Encryption of Quantum Medical Images", IEEE Access, November 2017.

[9] Shamim Ahmed Laskar and Kattamanchi Hemachandran," A review on Image steganalyis techniques for attacking steganography", IJERT, Vol 3, January 2014.

[10] Mohamed Elhoseny, Gustavo Ramírez-González, Osama M. Abu-Elnasr, Shihab A. Shawkat, Arunkumar N, Ahmed farouk, " Secure medical data transmission model for IoT-based healthvare systems", IEEE access, March 2015.

[11] Yan Ke, Jia Liu, Min-Qing Zhang, Ting-Ting Su and Xiao-Yuan Yang, "Steganography Security: Principle and Practice", IEEE Access, November 2016.

[12] Awdhesh K. Shukla1,2, Akanksha Singh3, Amod Kumar1,2 "A Secure and High-capacity Data-hiding Method Using Compression, Encryption and Optimized Pixel Value Differencing", IEEE Access, Volume XX,2017.