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 conceal its contents. A merged technique for data security has been proposed using Cryptography and Steganography techniques for information security to prevent unauthorized 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 proposed a hybrid security model for securing the diagnostic text data in medical images. Our system is developed through integrating steganography technique for image combining and extraction with hybrid encryption scheme. The proposed hybrid encryption schema is built 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.

Index Terms— Steganography: Peak Signal-to-Noise Ratio (PSNR); Structured Similarity (SSIM); Cryptography; Advance encryption standard (AES); Secure force algorithm; Correlation. Jpeg image Steganography (JSTE).

I. INTRODUCTION

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

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 coding was applied on secret message for lossless compression, which provided ~22% higher embedding capacity. The compressed secret message is subjected to AES encryption; this provides higher security in the cases of steganalysis attacks. After compression and encryption, LSB substitution and MPVD 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 to conceal messages’ existence in another medium (audio, video, image, communication). Steganography is different from cryptography in the sense that cryptography focuses only 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 are obtained. Under the current technology situation, analyze the indistinguishability of the cover and stego-cover, and consider that the steganography security should rely on 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 necessary conditions for a secure steganography algorithm in theory are formally presented. Image steganography terminologies are as follows:-

- **Cover-Image**: Original image which is explicitly used as a carrier for hidden information to be transmitted.
- **Message**: Actual information which is used to hide into images. Message could be a plain text or some other image.
- **Stego-Image**: After embedding message into cover image what we get is known as stego-image.
- **Stego-Key**: A key that is used for embedding or extracting the messages from cover-images and stego-images.

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 of the main techniques that is being used in computer security that converts information from its normal form into an unreadable form.

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).

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.

II. LITERATURE SURVEY

2.1 Survey on the combination of Crypto- Watermarking techniques

A hybrid technique using Watermarking and Cryptography was presented in, for a transmission of protected text message. This scheme was based 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 quality of watermarked images on the basis of Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), and Mean Square Error (MSE). It was observed that the one-bit LSB watermarking was better as related to the two-bit LSB watermarking and three-bit LSB watermarking because MSE and RMSE were small and PSNR was large [2]. For example, Patients and healthcare staff in one location encrypt important medical images via the proposed quantum encryption scheme, sending the cipher images to the cloud [8]. The health care staff in another location accesses the images from the cloud, decrypting the content via the decryption method.

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

Hybrid encryption schema is built using 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. Both color and grayscale images are used as cover images to conceal 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 [2] and further have proposed a new approach in steganography based on Direct Wavelet Transform using NSGA (Non Dominated Sorting Algorithm) for better quality of stego image.

Image steganography system is comprised two algorithms, one for embedding and one for extraction [3]. The embedding process hides a secret message within a cover media (cover image), and the result of embedding process is stego image. The main issue is that the secret message will not be unnoticed if a third party tries to intercept the cover media (cover image). The extraction process is simply because it is the inverse of the embedding process, where the secret message is revealed at the end. Image steganographic techniques [9] such as Transform Domain based, Spatial Domain based, Palette based steganographic techniques.

2.4 Difference between Cryptography and Steganography

Cryptography[3] prevents unauthorized party from discovering the content of communication but Steganography prevents discovery of the existence of communication (i.e., Cryptography makes data gibberish and known the message passing while Steganography tends to conceal presence of hidden data and unknown the message passing). Cryptography alters the structure of secret message while Steganography does not alter the structure of secret message.

Information hiding [7] aims to embed secret data into the multimedia such as image, audio, video, and text. In this study, two new quantum information hiding approaches are put forward. A quantum steganography approach is proposed to hide a quantum secret image into a quantum cover image. A quantum image watermarking approach is presented to hide a quantum watermark gray image into a quantum carrier image.

2.5 Survey on the Hybrid Cryptographic techniques

Cryptography is a term for data encryption. Encryption cryptography is the process of encoding messages in a way that hackers cannot read it, but that can be authorized personnel. The two main algorithms used for data encryption in this work are the Advanced Encryption Standard (AES) and the Secure Force algorithm [SF algorithm] [3]. AES is a symmetric cipher where the same key is used on both side. It has a fixed message block size of 128 bits of text (plain or cipher), and keys of length 128,192 or 256 bits. When longer messages are sent, they are divided into 128-bit blocks. Apparently, longer keys make the cipher more difficult to break, but also enforce a longer encrypt and decrypt process.

The study of hybrid cryptographic encryption methods and also use of other encryption techniques to improve their level of security and also to study their amalgamation of hybrid techniques which was included the combination of cryptographic and digital watermarking methods. In terms of security

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

Image privacy becomes the main concern with CBIR outsourcing [4]. For example, patients may not want to disclose their medical images to any others except to a specific doctor in medical CBIR applications. To formulate the problem, this paper considers two types of privacy threats. Firstly, a curious cloud server may look into the owner’s database for additional information. Secondy, after receiving the retrieved images, the query user may illegally distribute these images to someone unauthorized for benefits.

A novel quantum steganography framework for secure messages in fog cloud IoT is proposed [5]. The approach is based on quantum entangled states, exclusive OR operation (XOR), gray code, and hash function.
2.7 Survey on the Text steganography for hidden transmission of data

A novel text steganography technique called AITSteg, which provides end-to-end security during the transmission of text messages via SMS or social media between end users [6]. The AITSteg technique is evaluated by considering a trusted scenario. AITSteg is able to prevent various attacks, including man-in-the-middle attacks, message disclosure, and manipulation by readers. An image steganography approach based on Inverted LSB (ILSB) technique for securing the transmitted face images from the IP camera as the IoT device to the home server in the LAN network.

2.8 Survey on the Secure Force Cryptographic Algorithm

In Wireless Sensor Networks (WSN) the implementation of the SF algorithm [1] offers very low complexity architecture. The encryption and decryption process is almost similar in this algorithm. The five encryption rounds increases the effectiveness of the encryption procedure. This is a four step algorithm based on simple mathematical operations (six numbers of operations) that operates on a four bit data. But this causes a huge amount of misunderstanding and dispersal of data is created to combat dissimilar types of attacks. This algorithm consists of four steps. Fig 2.8.1 shows the whole process of Secure Force algorithm step by step.

Key Expansion

Key Management Protocol

Encryption Process

Decryption Process

Fig 2.8.1 Secure Force Algorithm

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 be 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-3.2.2 Architecture Diagram for Enhance security for medical images using secure force cryptography with Jsteg steganographic 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 may 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.3.6.1 are given as input.

The sender will choose the cover image as shown in 3.6.2 are given as input.

**Output** – The stegno-image is obtained by combining encrypted secret image over cover image as shown in Fig 3.6.3 respectively.

IV. EXPERIMENTAL RESULTS AND EVALUATION

4.1 Simulation Environment

The implementation of our proposed system was carried out using the MATLAB R2018a and MATLAB R2014a software running on a personal computer with a 2.07 GHz Intel (R) Core (TM) i3 CPU, 4 GB RAM and Windows 10 as the operating system. The metric calculation determines the quality of the proposed security model. These metrics calculate the ratio between the original image and the stego image. The obtained results were evaluated based on three parameters; the Peak Signal to Noise Ratio (PSNR), Structural Similarity (SSIM) and Correlation. PSNR calculates the imperceptibility of the stego-image. The higher the value of PSNR of stego image reveals a higher quality of stego image or a higher imperceptibility of hidden message. The PSNR is calculated according to the following equation:

\[
\text{PSNR} = 10 \log_{10} \left( \frac{I^2}{MSE} \right)
\]

Where \(I\) = Max value of pixels in Original image.

SSIM measures the structural similarity between two images. Its value ranges between -1 and 1. When two images are nearly identical, their SSIM is close to 1. Correlation determines how much two signals or vectors are similar or different in phase and magnitude when two sets of data are strongly linked together. It reaches its maximum when the two signals are similar. It is calculated by using the following equation: Correlation =

\[
\frac{n \sum xy - (\sum x)(\sum y)}{\sqrt{n(\sum x^2)-(\sum x)^2} \sqrt{n(\sum y^2)-(\sum y)^2}}
\]

Where n is the number of pairs of data, X is the input image, and Y is the stego image.

4.2 Security Analysis

In this model, the comparisons were conducted between the cover image and the stego-image. That is to guarantee less distortion occurs within to the original cover image after concealing the secret message image. The image is encrypted by using the secure force encryption method. Then it is being embedded using JSteg stenography.
techniques. It was found that JSteg gives better PSNR and SSIM results compared with other steganographic techniques in case of both color and gray scale images as shown in Fig 4.2.2 respectively. It was found that PSNR and SSIM values for both embedding and extracting remain same which gives lossless compression. The correlation were almost equal to one with all of the color and gray images as shown in Fig 4.2.2 respectively. For evaluation Fig 4.2.1 was taken respectively.

**Fig 4.2.1 Cover and Secret message image for analysis**

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 Fig 4.2.4 respectively.

**Fig 4.2.3 Metric calculation for Extracted image**

**Fig 4.2.4 Intensity finding for Cover and Stegno image**

**V. CONCLUSION AND FUTURE ENHANCEMENT**

In this paper, a new secure communication model has been presented that combines cryptography and steganography techniques to provide two layer of security, so the steganalyst can’t reach to plaintext without knowing the secret key to decrypt the ciphertext. Firstly the secret images has been encrypted by using the Secure Force-AES algorithm then the encrypted images has been hidden in cover image by using JSTEG and LSB methods. Due to this combination, the secret image can transmit over open channel because the cipher image does not look meaningless but its presence is concealed by using steganography for hiding cipher image in the cover images. The two parameters such PSNR and MSE are calculated.

In the future work, we are looking forward to try applying the proposed method on audio and video. Also, we are looking forward to enhance the proposed method to make the capacity higher than it while keeping the same PSNR or higher.

**REFERENCES**


