IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECRET COMMUNICATION USING MULTI-IMAGE STEGANOGRAPHY FOR MILITARY PURPOSES.

Pratik Wani[a], Anuja Nanaware[b], Sneha Shirode[c], Aishwarya Suram[d], Prof. Archana Jadhav[a*],

[a] *Department of Information Technology, JSPM'S Rajarshi Shahu College Of Engineering, Tathawade, Pune-411033*

[b] *Department of Information Technology, JSPM'S Rajarshi Shahu College Of Engineering, Tathawade, Pune-411033*

[c] *Department of Information Technology, JSPM'S Rajarshi Shahu College Of Engineering, Tathawade, Pune-411033*

[d] *Department of Information Technology, JSPM'S Rajarshi Shahu College Of Engineering, Tathawade, Pune-411033*

[a*] *Associate Professor, Department of Information Technology, JSPM'S Rajarshi Shahu College Of Engineering, Tathawade, Pune-411033*

***Abstract*— Information security plays an important role in processing data transfer. Transferring sensitive data or communicating online is already a challenge due to security concerns. Generally, we use cryptography to encrypt information and to send sensitive messages in the form of text. Today, there are several methods used to hide information in any form. One such method is steganography. Creating a confidential communication system that includes Multi-image steganography will lead to secure communication between sender and receiver without interruption by cyber criminals. Image steganography is a key feature of the hidden information in which ciphertext is embedded in an image called an image cover that is almost impossible for attackers to see with their physical eyes. Hidden information can be any type of text, images, sound, and even videos within the cover photo. The concept of Multi-image Steganography is that the secret code is divided into many parts and recorded in many cover images. We have therefore suggested two ideas for steganography images to make it more challenging for cyber criminals to hide data. This paper proposes the Least important bit (LSB) method of Steganography and Advanced Encryption Encryption (AES) methods for Cryptography to create a secure and secure system. Here the sender and recipient use the same key to encrypt and decrypt encrypted data known as the symmetric key.**

***Keywords*— Multi-Image Steganography, Cryptography, Least Significant Bit LSB Steganography, Advanced Encryption Standard AES Cryptography, Information Hiding.**

I. INTRODUCTION

Today communication systems are digitally digitized to prevent data transfer over networks. Information security is really important for a variety of purposes, especially in confidential data transfer systems, digital content access control systems digital content distribution, data storage, and data protection for hackers. Data transfer through any communication channel requires strong encryption techniques for data security purposes. Recent advances and extensive research into information technology really highlight the need for secure, secure and secure data transfer.

Generally, we use cryptography to encrypt information and to send sensitive messages in the form of text. There are many algorithms professionally developed for privacy. AES (Advanced Encryption Standard) [10] is one of them listed. AES was an industry standard and emerged as a highly efficient writing system due to the built-in advantage of better security with less complex application. AES is a different kind of Rijndael algorithm [7] Today, there are a number of methods used to hide information in any way that the human senses can detect. One such technique is steganography. Encryption is a popular and important

algorithm that is widely accepted with regard to information security.

A. *Cryptography*

Cryptography can be defined as the process of protecting information and communication by using and integrating and interpreting encrypted messages, which can be demonstrated in situations where communication is established between two parties in an unsafe way that is not easily heard by third parties or outside. community. [11] Cryptography contains a collection of encryption techniques that include encryption and encryption frameworks, integrity, digital signing, data privacy protection, and privacy or communication services.

B. *AES (Advanced Encryption Standard)*

It was necessary to replace DES as its main size is very small. With the growth of computer power, it is considered a threat to the full attack of search keys. DES triples were designed to overcome this problem but were found to be slow. This is where AES starts light, which is found to be 6x times faster than TripleDES. The most popular and widely accepted symmetric encryption algorithm that can be achieved today is the Advanced Encryption Standard (AES). Unlike DES, in AES the number of cycles varies and depends on the length of the key. AES operates using '128-bit keys, 192-bit keys, and 256-bit keys' with cycles of '10,12 and 14' respectively. In modern cryptography, AES is widely accepted and supported on both hardware and software. To date, no effective crypto-analytic attacks against AES have been detected. In addition, the AES has a relatively flexible key length, which allows for a level of 'future assurance' against the development of the ability to perform critical searches. It has been 20 years since the launch of the AES but still nothing has been taken. current attacks, which is why it can safely be called the unbreakable standard of encryption. For these reasons, we will use AES in our proposed system approach.

C. *Steganography*

In our project, we will be using the concept of steganography used to hide data. The word steganography is derived from two Greek words: 'steganos' means cover and 'graphos' means to write and usually refers to encryption or encryption. In this project, we use it to provide security and privacy. The content used to encrypt the data is called the cover material, while the cover and the hidden data are called the stego object. The whole process of steganography can be illustrated as shown below in Fig-1.

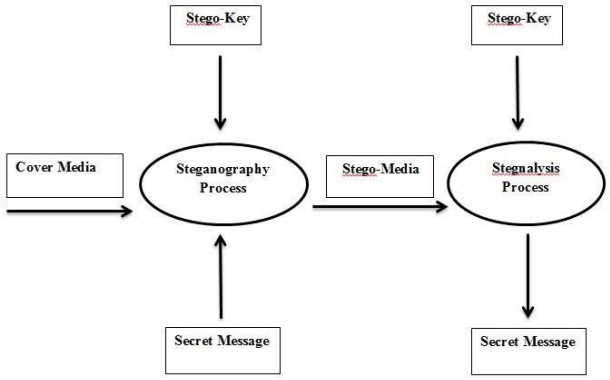

Fig-1

D. *Types of Steganography*

The techniques of steganography are divided into five: image steganography, video steganography, network steganography, text steganography, and audio steganography.

Types of Steganography:

- Image To Image
- Text To Image
- Image To Text
- Video To Voice
- Voice To Video

Our system uses text to image steganography. The simplest way to do this process is by inserting the confidential data bits in LSB positions of digital image.[12]

E. *Text to image/ Image Steganography*

Digital photography is a very safe way to manage sensitive information online using steganography. The picture is taken with the camera, the camera light will hear something to be taken, and it will be displayed on the camera screen. An image is a combination of pixels; image specification depends on the pixel. Pixel is a light minute object on the display screen. The human eye cannot detect pixels in an image. Pixel is made up of three parts. Three Red Pixels, Blue Pixel (R, G and B). Each pixel has a depth of 24 by 3 bits [8]. Each part is equal to one byte. Any color is made up of a combination of these three components. The number of bytes varies from 0 to 255. The color will be displayed based on the number of bits, 0 is very dark and 255 is very bright. The image size is given in pixels, for example, the image size is 600 * 450, and the image is a combination of 2,70,000 pixels. The pixel is made up of three parts on each part of an 8-bit size, for example, 11111111 pixel bits 0000000000000000 and the pixel will be red in color. Depending on the RGB values the pixel color will change. The encrypted message that will be embedded within the image is converted into bits depending on its ASCII value. Then these pieces of data will be stored in the image depending on the steganographic process used [9]. Steganography is associated with various advanced

technologies where data is hidden in an image file. This can be done by changing the less important pieces in the original data.

F. Crypto-Steganography

[14] With the help of LSB Steganography and the AES Algorithm Technique, we can apply high-level information security without covering image damage. Least Significant Bit (LSB) is a system in which the last part of each pixel is adjusted and replaced by data for a private message. The AES has a flexible built-in within the main length, which allows for a level of "future assurance" against the progress of the ability to perform important key searches. For example, it is 128 bits long, that is, AES works on 128 bits of blank text to produce 128 bits of ciphertext.

II. RELATED WORKS

To safely transfer data over the Internet. image steganography and cryptography, there have been a number of advanced methods. Below we have presented some of the key findings of our literature review of the corresponding system proposed in this paper.

The proposed model [1] uses the AES cryptography algorithm and contains steganography methods: a genetic algorithm and a reconnection method. By using a genetic algorithm it is possible to improve search in the perfect S to improve the quality of the resulting image. The reconnection process is integrated with a genetic algorithm to generate new solutions by testing trajectories that connect high quality color steganography solutions.

In [2] the author provided major changes to the Advanced Encryption Standard (AES) to improve security and ease of use with a focus on Symmetric Key Cryptosystem and AES algorithm. The paper suggested a new key usage process, a proper switch key to achieve faster working time and less memory usage. Calculations are made based on the AES-128 bit version.

Reference Paper [3] has developed a data encryption system using the Modulus function and colour images. This process focuses on hiding the image inside another large cover image.
It also outlines a proposed way to improve performance depending on both the secret message volume and stego file quality.

[4] examines the various in-depth learning methods found in the image of steganography. In steganography, the cover image is used in such a way that the hidden data is not seen and thus makes it less suspicious than in secret writing. In contrast, Steganalysis is used to detect the presence of any secret message covered in an image and to extract hidden data. The in-depth learning strategies used for image steganography are divided into three categories mainly traditional methods, methods based on the Convolutional Neural Network and General Adversarial Network-based. Traditional methods are frameworks that use non-machine learning methods or in-depth learning algorithms. CNN-based methods are based on the depth of convolutional neural networks to embed and extract secret messages and GANbased methods use other GAN methods.

In this paper [5] the author proposes a system that uses both cryptography and steganography to ensure two levels of data security. The purpose of this paper is to develop a new way to use XOR functionality for encrypting data and embedding embedded images - randomly using a user-selected key. To embed data within a cover image The Steganography Bit (LSB) method has been used. The encrypted message that will be embedded within the image is converted into bits depending on its ASCII value.

Furthermore in[6] the author introduced the best Least Least Significant Bit (LSB) method based on steganography imageenhancing existing LSB conversion techniques to improve the security level of encrypted information. It is a new way to change the LSB with a real RGB color image. The paper also used the Peak Signal-to-Noise Ratio (PSNR) to measure the quality of stego photos. The PSNR value gives a better result because the proposed method changes the minimum number of image bits. The results obtained show that the proposed method leads to LSB based on steganography imagery using a secret key that provides better security issues and PSNR value than standard LSB based steganography methods.

III. PROPOSED SYSTEM

In our system, we use a method to hide data inside an image (two images of us) called photo steganography. People can't make a difference or see when data is embedded in images. In our system we use three-layer security namely. with login authentication, cryptography and steganography provide unparalleled high data security over the network.

A. Methodology

In this program, User provides private data as input. After accessing the private data system it will encrypt the private data and split the ciphertext into two parts. After that two ciphertexts are embedded with cover images i.e. taken from the user / use default images and create stego ciphertext images respectively. Then send those pictures to the recipient. At the end of the recipient, the user will extract the images of stego (by steganalysis process) and after extracting the images; remove encryption ciphertexts and reassemble them to restore blank text. We receive private data and disclose confidential data.

- [15] In LSB Steganography, confidential information is stored somewhere in the LSB image.
- Take two representations of hidden information and write over the LSB of each byte inside the cover image
- Formula: cover photo + secret key + hidden message = stego photo

- Advanced LSB method for hiding private information written in text files in colored images.
- Each secret image is converted to its corresponding ASCII value and each code is converted to 8-bit binary, and each bit is inserted into the last LSB of each pixel cover image.

The system proposes an Advanced Encryption Standard (AES) algorithm for encrypting text and images and LSB which means the least important steganography method of encrypting data in an image after data encryption.

In the first step, the Sender types a secret message to be sent and that secret message is encrypted using the AES encryption algorithm. When the sender sends an audio message that message will be converted from speech to text using the Google API and the encryption key will be generated. In addition, an embedded text message is embedded to cover the image using the LSB steganography method. Then both stego images are merged using the AES algorithm and the secret key.

Now the direct reversal of all the steps is done on the side of the receiver. First, on the receiver side, the removal of hidden images from stego images is performed. Then two stego images are removed from encryption using the AES algorithm using the same key used to encrypt the two cover images on the sender's side. Finally, we remove ciphertext from stego images. And when the sender sends the audio information we will again turn that cypher text into an audio message using the google API. Then the data embedded in the cover image is extracted. Finally, the data is decrypted using the same key which was used to encrypt the data in the initial module at the sender's side.

B. System Architecture

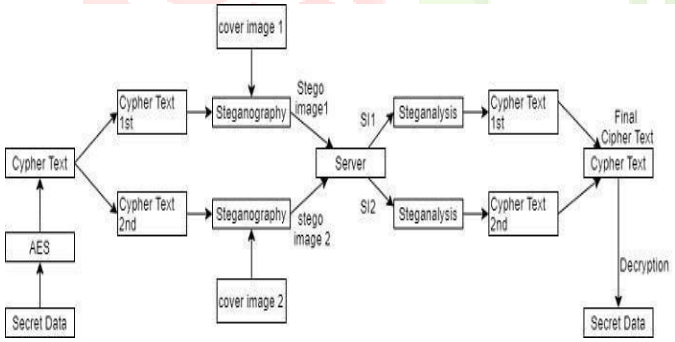

Fig-2

The Flow of the System is:

1. Take secret data/messages.
2. Encrypt the secret data and divide the ciphertext.
3. Embedded ciphertext with cover images and create stego images.
4. Send stego-images.
5. Unsteg the stego-images.(steganalysis) 6. Decrypt the ciphertext and merge the plain text.
7. Get secret data.
8. Display secret data/message.

IV. RESULTS AND DISCUSSIONS

We have created a web application to give access to authorized users of the application to transmit and communicate sensitive data between them using images.

Figure 3. It shows the login module of our system where the first security layer i.e. login authentication is established. The sender must log in using his or her credentials and the public key (encode / decode password) to forward or make secret encryption or remove encryption and continue texting to encrypt.

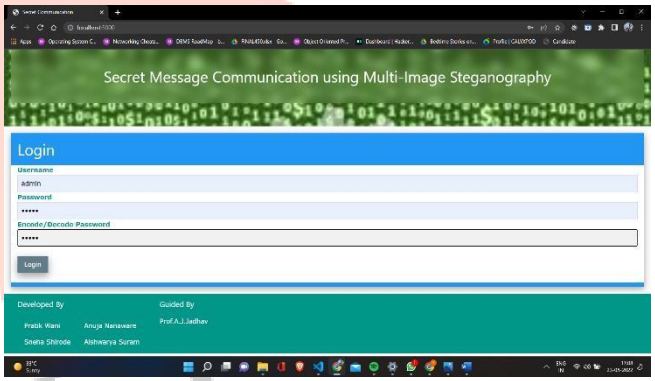

Fig-3

A. Encryption Interface

Fig.4. has the steganography module which has the encryption interface where the user will select and upload two cover images as shown below to hide the secret text taken as input via the voice module into it post the encryption process. "*This is a secret message*" is the secret message we communicating here.

Fig-4

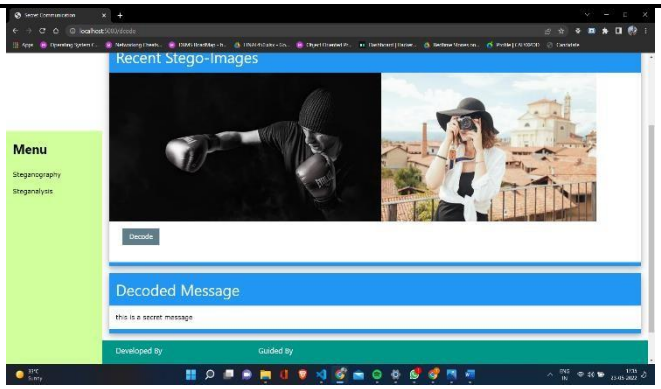

Fig-6

Lastly, with help of the AES algorithm, we convert this plain text into ciphertext. Further, we divide this ciphertext into two parts and embed them into the images we uploaded using image steganography; as illustrated in fig.5.

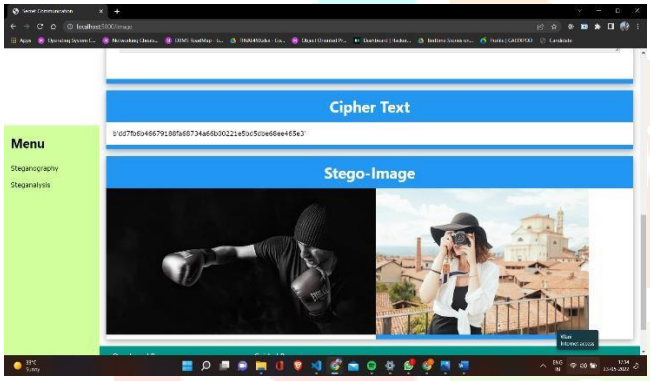

Fig-5

Now, these images; rather called stego-images are communicated to the sender, where the decryption takes place.

B. Decryption Interface

The receiver has to log in using the credentials and enter the same encode/decode password as that of the user whom he trying to communicate with. The steganalysis, a module is where the total decryption takes place. We retrieve the embedded ciphertext from the stego-images, merge them and then finally decipher it to get the original secret text as illustrated below in fig.6.

Fig.7. shows the cover image(original image) before data is embedded

Fig-7

Fig.8. shows the stego image after the data is embedded. We can clearly see that there is no distortion or interference in the picture. It's nothing more than a cover image.

Fig-8

Fig-9

In Fig.9. Similarly we have here another illustration of cover image and stego image after embedding message.

The proposed method is tested there; plain text (encryption) is first encrypted using the AES algorithm to produce ciphertext. The key is used based on the symmetric cryptosystem where the same key is used for the encryption process and the writing process. The ciphertext was then separated and embedded in two image files using the LSB-based steganography method. Then these stego images produced so much are sent to the intended recipient, where the retrieval process i.e. how to retrieve embedded messages from stego images and then the actual message is encrypted using the same key used during encryption. In this exercise we examine and compare the first image with a stego image obtained after using our proposed method and thus learn the percentage of change between the original image and the stego image.

By using a mathematical model according to the histogram we show how our proposed method works compared to the existing methods.

In figure 5:

(a) : original/cover image

(b) : stego-image

(c) : histogram of the original/cover image

(d) : histogram of stego-image

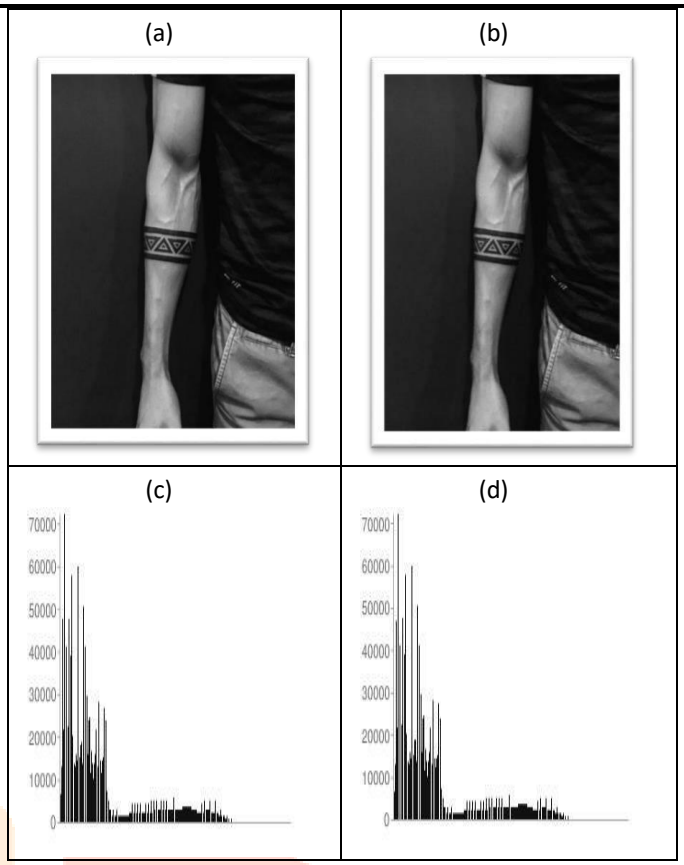

Fig-10

Designation	Value
size of image in pixels	262144
Size of image in bit	26911456
Size of message encrypted in bits	3264
Size of message encrypted and compressed in bits	4608
Percentage of compression	17%
Number of bits changed	3749
Percentage change	0.059%
Security size	Security of AES key is 256 bits

Table-1: Results obtained for proposed method

Image histogram proves to be one of the most effective aspect of analyzing the difference between a cover photo and a stego photo. The proposed method we use is a combination between LSB-based steganography and cryptography using the AES algorithm. Table 3, makes it clear that in this process the destruction of the cover image will be much lower as the pointed pixels are farther apart, the embedding capacity is better and the hiding power. This process eliminates the complexity involved, instead providing and secured with an AES (Advanced Encryption Standard) algorithm with a key size of 256 bits.

V. CONCLUSION AND FUTURE WORK

In this age of civilization exchanging data for communication through the network is an integral part of every organization and every sector of society. Our proposed algorithm is to secure this communication with a secure communication system by creating a distributed connection. This algorithm imposed an encrypted text which has been encrypted by using the AES algorithm within a JPEG image and then the image file is sent over the network i.e. we combine the concept of Cryptography and Steganography to make an illusion to the hacker that the sender sends an unsuspicious media file to the receiver. As an image file appears in the network as an innocent media file so it does not attract the hacker as the content of security. In this paper, we conclude that two levels of security can be achieved using crypto-steganography. By using this technique, third parties will not be interrupted because no noise will be generated in the cover art, so no one can even know that the data is embedded in the image. It provides a high level of integrity and confidentiality of messages. A large number of algorithms are being developed to overcome the delays in existing algorithms and increase the security level of data transmitted over the internet. Although there are many message detection techniques developing simultaneously, detection does not guarantee to retrieve all the information. Crypto steganography is the technique in which we encrypt data using the key and use that key to pseudo-randomly embed the data into the pixels of the cover image. Even if we change the bits of the components of the pixels of the image, there will be no further distortion in the stego image, but there will be some distortion that the human eye cannot see. In addition, we hide and transmit the data in the noisy picture so that the data is more secure. In this way, the stego image will be the same as the cover image. Numerous application areas are developing like cloud security, online communication sites etc., the vision into the cryptosteganographic principles will make us find vivid areas of application.

REFERENCES

1] Aura Conci, Andre Luiz Brazil, Simone Bacellar Leal Ferreira, Trueman MacHenry, —AES Cryptography in Color Image Steganography by Genetic Algorithms

[2] Design and Implementation of a Modified AES Cryptography with Fast Key Generation Technique, —2020 IEEE International Women in Engineering Conference on Electrical and Computer Engineering(WIECON-ECE)

[3] An Improved Secret Message Capacity Using Modulus Function Based Color Image Data Hiding, —2018 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM)

[4] N.Subramanian, Somaya Al-Maadeed, Ahmed Bouridane, Image Steganography: A Review of the Recent Advances, — IEEE Conference Volume 9, 2021

[5] A New Approach for LSB Based Image Steganography using Secret Key, —Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011), Dhaka,Bangladesh

[6] SREELAKSHMI(2015, Nov 9), " Image Steganography using LSB," https://www.slideshare.net/SreelekshmiSree1/image- steganography-using-lsb/

[7] K. Curran and K. Bailey, "An Evaluation of Image Based Steganography Methods," Multimedia Tools and Applications, Vol. 30 Issue 1, pp. 55 – 88, July 2006.

[8] Osuolale and A. Festus, "Secure Data Transfer Over the Internet Using Image Crypto Steganography." in International Journal of Scientific & Engineering Research, 8(12), pp. 6-9, December 2017.

[9] T. Jamil, "The rijndael algorithm," IEEE potentials, vol. 23, no. 2, pp. 36–38, 2004.

[10] A.J. Raphael and V. Sundaram, "Cryptography and Steganography-A Survey", International Journal of Computer Technology and Applications, Vol. 2, No. 3, pp. 626-630, 2016.

[11] J. Fridrich and M. Goljan, —Digital image steganography using stochastic modulation‖, SPIE Symposium on Electronic Imaging, San Jose, CA, 2003

[12] T. Morkel, J. H. P. Elloff, M.S. Olivier, —An Overview of Image Steganography

[13] Image Steganography Using Steg with AES and LSB, -2021 IEEE 7th International Conference on Computing Engineering and Design (ICCED)

[14] Jain M and Lenka S K 2016 A review of digital image steganography using LSB and LSB array. Int. J. Appl. Eng. Res. 11(3):1820–1824

[15] The 5th International Conference on Electrical Engineering- Boumerdes(ICEE-B) Oct 29-31 2017,Algeria – An Improved Approach for LSB-Based Image Steganography using AES Algorithm. [16] J. Fridrich and M. Goljan, —Digital image steganography using stochastic modulation‖, SPIE Symposium on Electronic Imaging, San Jose, CA, 2003