IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 2, July 2022

Secret Communication using Multi-Image Steganography for Military Purposes

Pratik Wani[1], Anuja Nanaware[2], Sneha Shirode[3], Aishwarya Suram[4], Prof. Archana Jadhav[5]
Students,Department of Information Technology[1,2,3,4]
Associate Professor, Department of Information Technology[5]
JSPM'S Rajarshi Shahu College Of Engineering, Tathawade, Pune, Maharashtra, India
wanipratik30@gmail.com, anujananaware9155@gmail.com, snehashirode1305@gmail.com
aishwarya.suram1234@gmail.com, ajjadhav_it@jspmrscoe.edu.in

Abstract: *Information security plays an important role when considering data transmission. Transmission of sensitive data or communication through the internet turns out to be challenging due to security concerns. Generally, we use cryptography for information hiding and sending secret messages in the form of text. Nowadays, there are several techniques used for hiding information in any medium. One such technique is steganography. Building a secret communication system including Multi-image steganography will result in secure communication between the sender and the receiver without any interference from the hackers. Image steganography is the main aspect of information hiding where the ciphertext is embedded into an image called a cover image which is next to impossible for the intruders to see with their naked eyes. The hiding information can be any form of text, images, audio, and even videos inside a cover image. The conceptual definition of Multi-image Steganography is that the secret code is divided into multiple parts and is etched into multiple cover images. So we proposed two image steganography ideas to make it very challenging for the hackers to conceal the data. Thispaper proposes the Least significant bit(LSB) technique of Steganography and the Advanced Encryption Standard(AES) technique of Cryptography to build a safe and secure system. Here the sender and the receiver use the same key to encrypt and decrypt the data which is popularly termed a symmetric key.*

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

I. INTRODUCTION

Today communication systems have been digitally transferred to secure data transfer over networks. Information security is really important for a variety of purposes, especially in confidential data transfer, digital content access control systems for digital content distribution, data retention, and data protection from hackers. The transmission of data through any channel of communication needs strong encryption techniques for purpose of data security. The recent development and extensive research in information technology highlights the need for safe, secure and protected transmission of data.

Generally, we use cryptography for information hiding and sending secret messages in the form of text. There are many algorithms developed by experts for secrecy. AES (Advanced Encryption Standard) [5] is one of them on the list. AES has been the industry standard and emerged as a frontrunner efficient encryption method because of the inbuilt advantage of better security with less implementation complexity. AES is a variant of the Rijndael algorithm [6] Nowadays, there are several techniques used for hiding information in any medium wherein human senses cannot perceive rather sense it. One such technique is steganography.Encryption is a popular and important algorithm that is widely accepted regarding information security.

1.1 Cryptography

Cryptography can be defined as the process of protecting information and communication by using and compiling and deciphering coded messages, this can be proved in cases where communication is established between the two parties through an unsecured method that can easily be listened to by third parties or outside the public. Cryptography contains

DOI: 10.48175/IJARSCT-5880

a collection of encryption techniques that include encryption and frameworks for encryption, integrity, digital signing, data privacy protection, and confidential transactions or communications. In this paper we will talk about different data encryption techniques; especially methodology that uses public key cryptography, i.e. DES and AES.[2]

1.2 DES (Data Encryption Standard)

The DES algorithm was created by the National Institute of Standards and Technology (NIST) in the early 1970s. Since it is a symmetric key algorithm, it uses the same key for both encryption and decryption of data. This process takes blank text from 64-bit blocks and converts them to ciphertext using 48-bit keys. Although it was a popular encryption algorithm in the '90s, it was replaced by the AES in terms of modern computer computing power. Encryption strength is related to key size, and this is why DES found itself a victim of further technological advances in computing. After that it was easy to remove DES encryption as 56-bit was no longer good enough to handle new technological advances and that is why it faced new challenges of being at risk of secrecy attacks.

1.3 AES (Advanced Encryption Standard)

It was necessary to replace DES as its key 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 to shine, which is found to be 6x times faster than Triple-DES. The most popular and widely accepted algorithm for symmetric encryption that can be accomplished today is the Advanced Encryption Standard (AES). Unlike DES, in AES the number of cycles varies and depends on the key length. AES works on using 128-bit keys, 192-bit keys, and 256-bit keys having 10,12 and 14 rounds 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. Additionally, AES has an inherently flexible key length, allowing a level of 'future assurance' against the advancement of the ability to perform key searches. It has been 20 years since the launch of the AES but still has not adopted any known. attack right now, which is why it can safely be called the unbreakable global standard of encryption.

Table 1: Showing Experimental Analysis of DES and AES

Comparative criterion	DES Algorithm	AES Algorithm
Encryption Time (in sec)	215.9359	99.871
Decryption Time (in sec)	183.5455	84.8904
MSE	8185.4343	8149.8396
NPCR	99.6643	99.6399
PSNR(dB)	7.6057	7.5523
UACI	51.2496	50.8584

In [7] a new comparative study between DES and AES were presented. With the theoretical comparisons, experimental analysis and comparison is done for DES and AES algorithms. Based on the text files used and the experimental result it was concluded that AES algorithm consumes least encryption and decryption time as compared to DES algorithm. For these reasons, we will use AES in our proposed system approach.

1.4 Steganography

Steganography is the technique for hiding data and aims to hide data in such a way that any eavesdropper cannot observe any changes in the original media. Steganography is a data encryption method and aims to encrypt the data in such a way that any listener can see the changes in the original media. This is usually related to the way of hiding the existence of contact data. It hides information facts. It is a process of hiding data from one digital media to another digital media and retrieving the same information afterwards.

1.5 Steganography Process

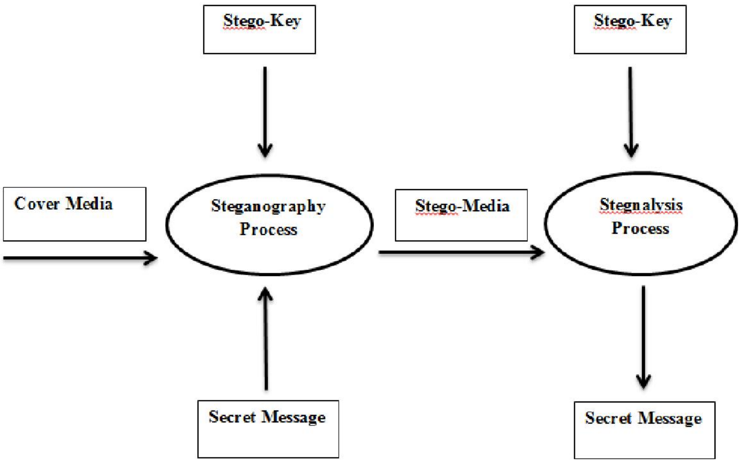


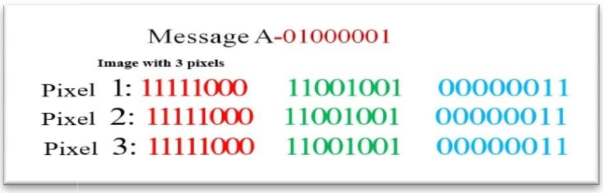
Figure 1: Steganography process

- **Secret Message:** The data that you need to insert inside the digital media.
- **Stego-key:** The key used in the Steganography process.
- **Cover Media:** The medium utilized in Steganography procedure, for example, picture, video and audio.
- **Sender Algorithm:** The technique utilized in this Steganography process.
- **Stego-Media:** The media coming about because of including the mystery message into a spread media utilizing Stego-key and encoding calculation.
- **Receiver Algorithm:** The technique used to extract the mystery message from Stego-media utilizing stego-key

1.6 Steganography using LSB

In our proposed approach we will be using LSB-based image steganography which is known as one of the most well-known techniques used for steganography. And in addition to today's most popular method, steganography is the use of LSB image pixel data. This investigation is used for a single piece of LSB. It includes each piece of dual content and one piece of all pixels in the original image. This strategy works if the record is longer than the text message and if the image is grey, when the LSB technique is applied to all 24-bit image bits, three bits can be encoded in each pixel. Example: We can use images to hide. Things if we replace the last part of all the coloured,bytes from the message.[1]

Image with 3 pixels



Message A-01000001

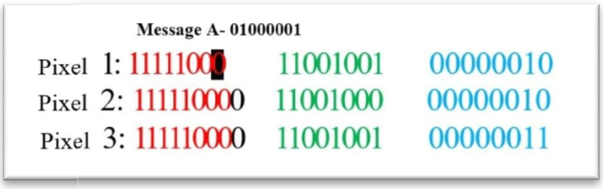
Image with 3 pixels

Pixel 1:	11111000	11001001	00000011
Pixel 2:	11111000	11001001	00000011
Pixel 3:	11111000	11001001	00000011

Fig. 2: Message A before encryption

Now we hide our message in the image.

Message A- 01000001



Message A- 01000001

Pixel 1:	11111000	11001001	00000010
Pixel 2:	111110000	11001000	00000010
Pixel 3:	111110000	11001001	00000011

Fig. 3: Message A after encryption

DOI: 10.48175/IJARSCT-5880

1.7 Types of Steganography

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

A. 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.[17]

a. Text to image/ Image Steganography

A digital image is the most secure way to carry sensitive information through the internet using steganography. The image is captured using the camera, the light of the camera will sense the object which should be captured, and it will be displayed on the screen of the camera. Image is the combination of the pixels; the resolution of the picture depends upon the pixel. Pixel is the minute area of illumination on a display screen. Human eyes cannot sense the pixels in the image. Pixel is made of three components. Three components of the pixel are Red, Green and Blue (R, G and B). Each pixel has a depth of 24 bits which is 3 bytes [3]. Each component is of size one byte. Any color is formed by the combination of these three components. The byte value varies from 0 to 255. The color will be displayed based on the value of the bits, 0 is the darkest and 255 is the brightest. The size of the picture is given in the pixels, for example, the size of the picture is 600*450, and then the image is the combination of 2,70,000 pixels. pixel is made of three components which of each component is the size of 8 bits, for example, 11111111 00000000 00000000 is the pixel bits then the pixel will red in color. Depending upon the RGB values the pixel color will be changed. The secret message which is to be embedded inside the image is converted into the bits depending on their ASCII value. Then these data bits will be stored in the image depending on the steganographic technique used [9]. Steganography is related to a variety of high technology where data is hidden into an image file. This can be done by replacing redundant bits of less important in the original data.

b. Crypto-Steganography

[4]With the help of LSB Steganography and the AES Algorithm Technique, we can use 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 a bit of private message data. The AES has built-in flexibility within the main length, which allows for a level of "future assurance" against the progress of the ability to perform critical 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

In order to transmit the data securely through the internet. image steganography and cryptography, there have been several methodologies developed. Below we have provided some important findings we came across while doing a literature survey for the corresponding system proposed in this paper.

The proposed model in [9] uses the AES cryptography algorithm and contains steganography methods: genetic algorithm and method re-linking. By using a genetic algorithm it is possible to improve the search to a perfect S in order 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 colour steganography solutions.

In [10] the author provided major changes to the Advanced Encryption Standard (AES) to improve security and ease of use with a focus on the Symmetric Key Cryptosystem and AES algorithm. The paper suggested a new key implementation process, the right shift key technique to achieve faster working time and less memory usage. Calculations are made based on the AES-128 bit version.

Reference Paper [11] 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.

[12] 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 [13] 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 of using XOR functionality for encrypting data and embedding embedded images - randomly using a user-selected key. To embed data within the cover image The least Steganography method Bit(LSB) has been used. The encrypted message to be embedded within the image is converted to bits depending on its ASCII value.

Furthermore in[14] 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. EXISTING SYSTEM

Every user wants to secure their data and personal information from hackers and any other harmful attacks. The transmission of data from the source environment to destination environment should take place in a secure manner. For secure transmission of data, there occurs a crucial need of a special technique called Cryptography. Cryptography is one of the popular ways of sending critical information in a secret way. It hides the existence of the message. Cryptography includes following important terms:

- **Plain Text-** It is the original message or text on sender’s side.
- **Cipher Text -** It is the encoded message or text of the main message or text.
- **Encryption or Encoding -** The process of converting clear text to encrypted text is known as Encryption.
- **Decryption or Decoding -** The method of changing secret message back into ordinary readable form of message is known as Decryption

The main disadvantage of cryptography is that the original text can be known and the cipher text is visible but we can’t read although which can be decoded by the attacker.So, the security is at risk. That is why to increase the security and improve the transmission of data we propose a system where along with cryptography, steganography is also used.

IV. PROPOSED SYSTEM

In this system, User give secret data as input. After receiving secret data system will encrypt secret data and divide cipher text into two parts. After that two-cipher text embedded with cover images i.e take from user /apply default images and create stego images for respective cipher text. Then send that image to receiver. At the receiver end, user will unsteg the stego images. after unstegoing images decrypt the cipher text and merge plain text. We get secret data then display the secret data.

- In LSB Steganography, hidden information is stored somewhere in the LSB image
- Take the binary representation of the hidden information and overwritethe LSB of each byte within the cover image
- Formula: cover image + secret key + hidden message = stego image

DOI: 10.48175/IJARSCT-5880

- Improved LSB method for hiding secret information written in text file into color image.
- Each character of the secret image is converted into its equivalent ASCII value and then each code is converted into 8 bits binary, and each bit is inserted into the last LSB of each pixel of the cover image.

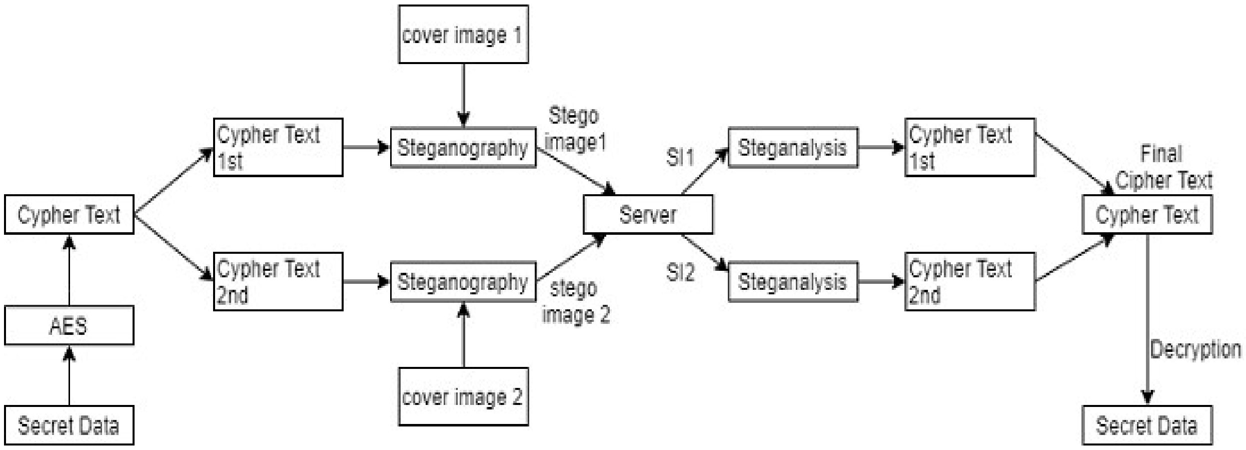


Fig 4: Proposed system flowchart

The system proposes an Advanced Encryption Standard (AES) algorithm for encryption of text as well as images and LSB i.e., least significant bit steganography approach for masking the data onto an image after encryption of the data.

In the first step, Sender types of the secret message to be sent and that secret message is encrypted using AES encryption algorithm. If sender sends audio message, then that message will convert from speech to text using google API and secrete key will be generated. Further, the enciphered text message is embedded on to cover image using the LSB steganography technique. And then both the stego images are enciphered using an AES algorithm and a secret key. Now the exact reverse of all the steps are performed at the receiver's side.

First at the receiver's side, extraction of the enciphered images from the stego images is performed. Then the two stego images are decrypted using the AES algorithm by using the same key that was used to encrypt those two cover images at sender's side. At receiving end, we extract cypher text from stego images. And if sender has sent the audio information, then again, we will convert that cypher text into the audio message using google API. Then the data embedded onto 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.

V. EXPERIMENTAL RESULTS

A system with a three-layer security will be developed to produce a very safe approach by merging image steganography with cryptography which will hide the text for secret communication. This system will be very difficult to hack, and nobody can detect secret communication between military personnel. This will provide an end-to-end encrypted communication system.

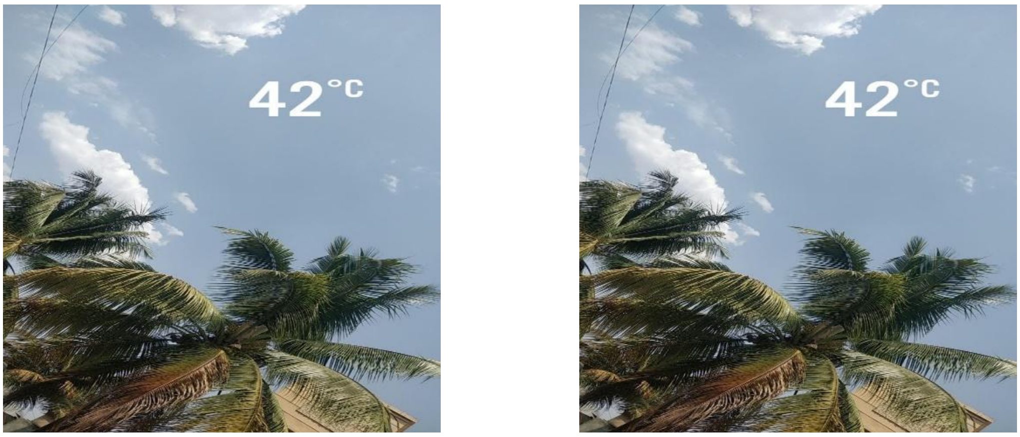


Fig 5: Original and stego-image of tree.

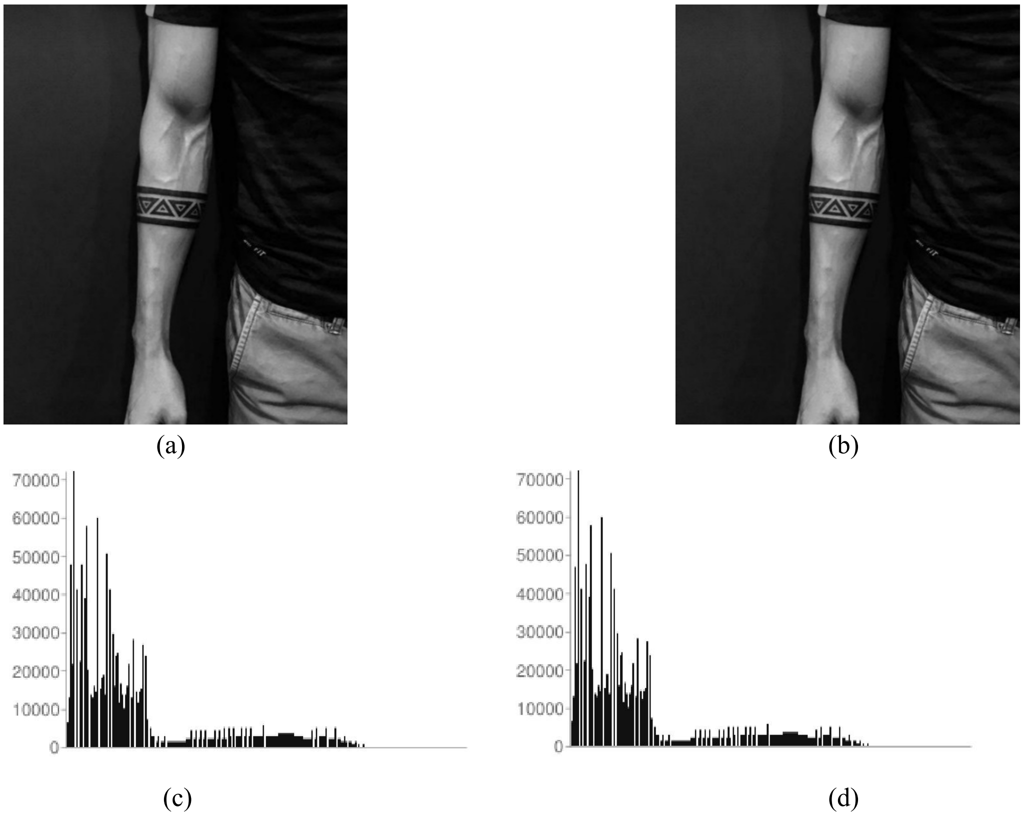
The proposed method is experimented wherein; the plaintext(secret message) is first encrypted using AES algorithm to generate a ciphertext. A key is used based on symmetric cryptosystem where same key is used for encryption and decryption process. The ciphertext is then divided and embedded in two image files using LSB-based steganography technique. Then these so generated stego-image(s) are sent to intended recipient, where the reverse process i.emethod of retrieving firstly the embedded messages in the stego-images and then the original message is decrypted from it using same key used during encryption. Below is one ofthe original and encrypted images from this above experiment.

In this work we evaluate and compare the original image with the stego-image so obtained after using our proposed technique and hence studied the percentage of change between the original image and stego-image.

Using the statistical illustration in terms of histogram we depict how our proposed approach is effective compared to existing approaches.

In figure 5:

a. original/cover image
b. stego-image
c. histogram of the original/cover image
d. histogram of stego-image



(a) (b)

(c) (d)

Figure 6: Results obtained for the proposed method

Table 2: Results obtained for proposed method

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

VI. DISCUSSION

Image histogram proves to be one of the most methodical feature for analysing the difference between cover image and stego-image. The proposed approach we use is a hybrid between LSB-based steganography and cryptography using AES algorithm. Table 3, makes it clear that in this technique the degradation of cover-image will be very low as pixels identified are at distant from one another, embedding capacity is good along-with the hiding capacity. This technique discards involvement of complexity, rather provided and protected with the AES(Advanced Encryption Standard) algorithm with key size 256 bits.

VII. CONCLUSION

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 concluded that by using crypto-steganography, one can achieve two levels of security. There will be no third party interruption by using this technique because no one can even know that data is embedded into the image as there will be no noise created in the cover image. It provides a high level of integrity and confidentiality of messages.

In summary, this paper has elaborated various techniques for information hiding used in recent times mainly Image steganography using the LSB algorithm and for the encryption of the text we described AES cryptography which will divide the ciphertext into two which further gets embedded into two image files that are two stego image. We also proposed the steganalysis concept which is the study of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography. The main approach to building this system is to provide strong security which will avoid detection of the data mainly when the hacker is desperate to decrypt the information.

REFERENCES

[1]. IJSTR VOL-8, ISSUE 12, DECEMBER 2019: Image Steganography Using LSB by Dr.Amarendra K, Venkata Naresh Mandhala, B.Chetangupta, G.GeethaSudheshna, V.Venkata Anusha.

[2]. 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

[3]. 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.

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

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

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

[7]. IJEIT VOL-2, Issue 6, Dec 2012: Analysis and Comparison between AES and DES Cryptographic Algorithm. By Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma.

[8]. IJSRISSN(online): 2319-7064: A Comparative Study of Steganography and Cryptography by Pranali R. Ekatpure, Rutuja N Benkar.

[9]. Aura Conci, Andre Luiz Brazil, Simone Bacellar Leal Ferreira, TruemanMacHenry, —AES Cryptography in Color Image Steganography by Genetic Algorithms

[10]. 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)

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

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

[13]. Secure Data Transfer Through Internet Using Cryptography and Image Steganography, —IEEE Southeast Conference 2020

[14]. 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

[15]. 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):1820–182

[16]. 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.

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