Review on Encrypted Image with Hidden Data Using AES Algorithm

Tarun Goyal[1], Ms. Shazia Haque[2]

[1]B.Tech Final Year Student, Information Technology Department, Poornima College of Engineering, Jaipur, India
Email Id: 2014pceittarun@poornima.org
[2]Associate Professor, Information Technology Department, Poornima College of Engineering, Jaipur, India
Email Id: shazia@poornima.org

Abstract— Steganography is the art of hiding the fact where communication is taking place, by hiding information in other information. Steganography becomes more important as more people join the cyberspace revolution. . In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. Steganography include an array of secret communication methods that hide the message from being seen or discovered. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. In addition to this our project also adds security to both the data hidden and the image that carries the information. Security is provided by Encrypting the data that is sent in the image and again encrypting the image that carries the information using AES algorithm. This encryption of the data and image thus provides double security layer.

Keywords—Steganography, Encryption, Decryption, AES algorithm.

I. INTRODUCTION

Now a day sharing of information on internet increases due to that the chances of misuse or duplication also increases. So for making the data safe we do the encryption. Encryption means encoding a message in such a way so that only authorized party can access it. So, by making the data encrypt we provide a security to our data from vulnerable attacks. The security of data mainly depend on four major aspects Data Confidentiality, Data Integration, Data Authentication, Data Freshness. Data confidentiality is the context of computer system allow authorized user to access sensitive and protected data. Data Integration is the maintenance and the assurance of accuracy and consistency of data. Data Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Data Freshness implies that data is recent and it ensures that no adversary replayed old messages. Steganography is the art of hiding the fact where communication is taking place, by hiding information in other information. In case of steganography attacker don't be aware that the information is hiding in another type of information like hiding the data in an image. The attacker only able to see the image like the other images on internet so, due to that the chances increases that the data safely able to reach the receiver end. In contrast, to the cryptography where we convert data into a cipher text instead of plain text. So, due to that attacker able to know the important information being transferred and try to convert that information in plain text or try to change it. By using the advanced encryption standard (AES) for encryption of data make the data safe because advanced encryption standard is a safest algorithm. It is a symmetric-key encryption standard adopted by the U.S government. Advanced encryption standard is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information [1]. It is the best algorithm for keeping the data safe as well as the steganography added the security because in case of steganography the attacker don't be aware that the information is hiding in another type of information. Steganography exist from a very long time. In ancient time people perform steganography as tattooing a secret message on the shaved head of a messenger, and letting his hair grow back before sending him through enemy territory. The other approach is marking the document with invisible secret ink or mark selected characters within a document by pinholes and to generate a

pattern or signature. But as the technology become updated the different techniques with more security are there to achieve that functionality. We study about the new techniques for approaching steganography and the proposed model further in this paper.

II. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard(AES) is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption as well as for decryption. It is a non-feistal algorithm. Advanced encryption standard works on both software and hardware. The AES is based on "substitution-permutation network". It is a block cipher with a block length of 128 bits. It consists of 10 rounds of processing for 128 bit keys, 12 rounds for 192 bit keys and 14 rounds for 256 bit keys. The Advanced Encryption Standard (AES) algorithm is one of the block cipher encryption algorithm that was published by National Institute of Standards and technology (NIST) in 2000[2].

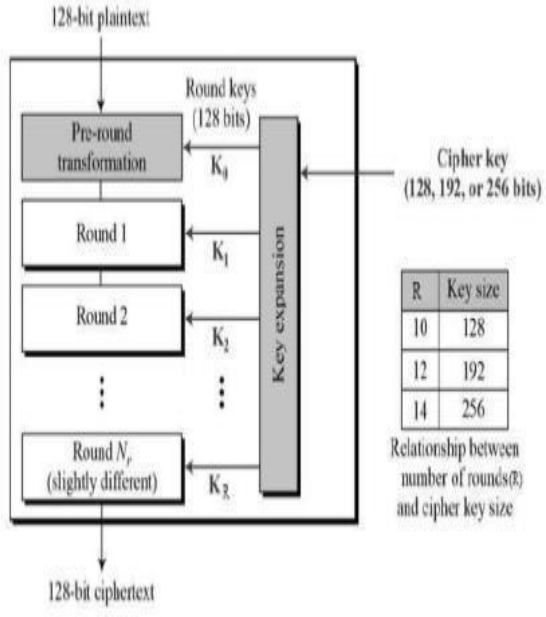

Fig.1: Basic AES Model

The main aims of this algorithm was to replace DES algorithm after appearing some vulnerable aspects of it. AES is an iterated symmetric block cipher, which means that AES works by repeating the same defined steps multiple times. AES is a kind of secret key encryption algorithm and AES operates on a fixed number of bytes. AES as well as most of the encryption algorithms is reversible. Which means that almost the same steps are performed to complete both encryption and decryption in reverse order. The AES algorithm operates on bytes, which makes it simpler to implement and explain.

The complete process of encryption and decryption in AES is:

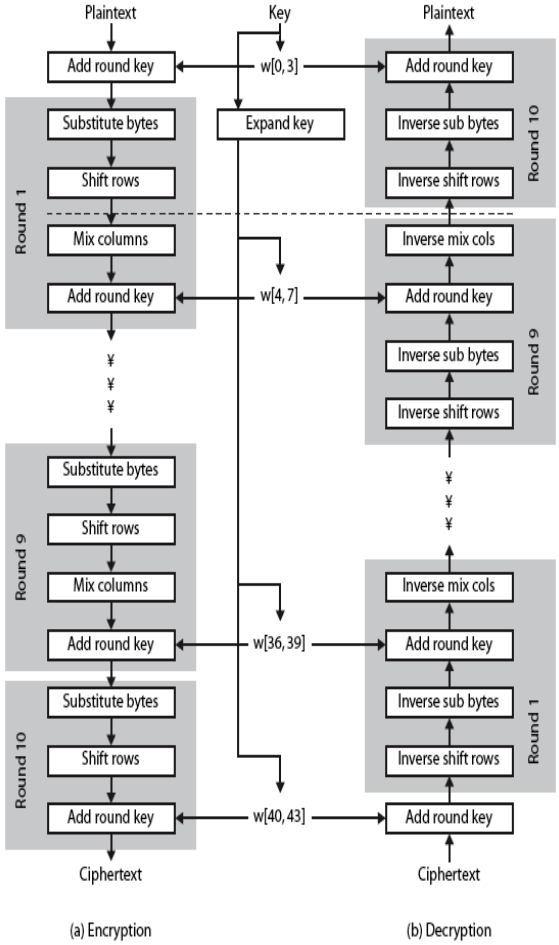

Fig.2: Encryption and Decryption in AES

III. EXISTING TECHNIQUES

1. LEAST SIGNIFICANT BIT (LSB) TECHNIQUE

Least significant bit (LSB) insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is

presented, in which the number of LSBs used for message embedding / extracting depends on the local characteristics of the pixel. The advantage of LSB-based method is easy to implement and high message pay-load.

DISADVANTAGES

- LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image.
- An attack on the stego-image is very likely to destroy the message.
- An attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image.

2. EMBEDING SECRET MESSAGE IN RGB 24 BIT COLOR IMAGE

This technique is introduced by Nosrati et al. This technique is irreversible data hiding technique that means once the covert image embedded on the original image the original image is lost i.e. from stego-image original image cannot be recovered in extraction process. This is achieved by applying the concept of the linked list data structures to link the secret messages in the images. First, the secret message that is to be transmitted is embedded in the LSBs of 24 bit RGB color space. The secret message bytes are embedded in the color image erratically and randomly and every message contains a link or a pointer to the address of the next message in the list. Also, a few bytes of the address of the first secret message are used as the stego-key.

DISADVANTAGES

- It requires extra space for pointers within image obstructing the possibility of extra message.
- During extraction if first pointer get corrupted or not traceable on receiver location then whole message becomes unrecoverable.

3. HISTOGRAM SHIFTING OF ORIGINAL MESSAGE

This technique is proposed by Ni et al. This is a reversible data hiding technique that means original image also get recovered by extracting the information. This algorithm first finds the peak point and zero point in the histogram, records the coordinate of these points and keep the information as overhead information. After this the peak points of the histogram shifted to right by 1 and embed the secret message into the resulting space.

DISADVANTAGES

- This method will not able to perform when more than one peak and low point exits in the histogram as the overhead message increases.
- If the receiving end doesn't have the knowledge of these points in a histogram then the extraction process fails.

4. MODIFIED HISTOGRAM SHIFTING OF ORIGINAL MESSAGE

This method is presented by Kuo et al. This technique is a reversible technique that is based on the block division to conceal the data in the image. In this approach the cover image is divided into several equal blocks and then the histogram is generated for each of these blocks. Maximum and minimum points are computed for these histograms and shift the histogram right and left by 1 near the maximum points so that the embedding space can be generated to hide the data at the same time increasing the embedding capacity of the image. A one bit change is used to record the change of the minimum points in location map. In this approach the receiver will extract the location map from the stego- image, gets the information about the maximum and minimum points in a histogram and extract the secret message. This method increases the data hiding capacity inside the cover image.

DISADVANTAGES

- High Computation time.
- Algorithm Complexity and distortion is high.
- Security is less because single key is used for the whole process.
- Generation of histogram is a difficult and time consuming process [5].

IV. PROPOSED MODEL

In proposed model we use the AES algorithm for encrypt the data and then embed that data in an image that's the work of a sender and the key get generated that delivered to

a receiver so he/she able to encrypt. Before sending that image which having the data to a receiver it will send to a image provider who will do some changes in it and generate a new key then the data get send to a receiver side and for decrypting that the receiver have to use the both the keys of image provider as well as of the sender. This help to increase the security and if somehow attacker able to know that secret data get sent and able to retrieve the encrypt data but due to AES he/she not able to know the original data because the AES encrypt information not been able to decrypt by anyone without key. It is the safest algorithm.

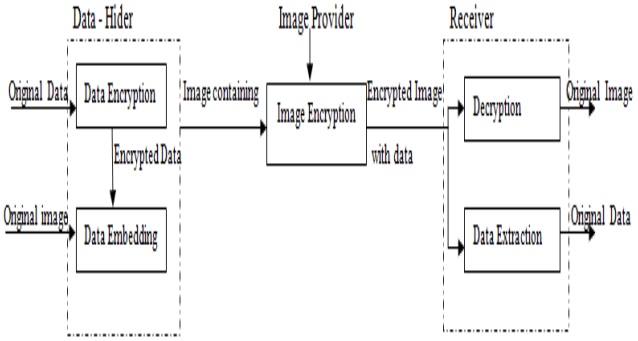

Fig.3: Architecture Diagram of Proposed System

1. DATA ENCRYPTION AND DATA EMBEDDING:-Sender change the original message in a cipher text using AES algorithm in this and then embed that message in an image of his/her choice.
2. IMAGE ENCRYPTION:-In this module the image protector try to encrypt the image by applying some password on it The encrypted image is saved in .png (Portable Network Graphics) file format. When the image is tried to be opened it appears as a blank black image.
3. DECRYPTION AND DATA EXTRACTION:- For decryption the receiver needs the key of an image protector so that he/she able to separate both the original image and encrypted data and than for decryption of that data he/she needs the key of a sender that provide double security and attacker don't able to get the information[5].

ADVANTAGES

- The proposed model uses two keys that help in increase security.
- It uses less time in implement.
- If somehow attacker able to get encrypt data then also he/she not able to decrypt it due to AES algorithm.

V. CONCLUSION

This proposed model is safer than other existing methods. This algorithm help us to overcome the problems that existing systems having as well as the proposed model using the two keys that help us to increase the security as well as in this model we are using the AES algorithm that is the fastest as well as safest algorithm that increases the security of our data.

VI. ACKNOWLEDGEMENT

I am thankful and like to express my sincere gratitude to the Head of Department Mr. Amol Saxena and my guide Ms. Shazia Haque for support, guidance and for continuous encouragement. Due to your guidance and support I am able to complete that paper. I sincerely thanks to all my lecturers and friend for helping me in many ways and gave valuable advises.

REFERENCES

[1] Radhika D.Bajaj, Dr. U.M. Gokhale "Design and Simulation of AES Algorithm for Cryptography", International Journal of Engineering Science and Computing, Volume 6, Issue 6, June 2016.
[2] Radhika D.Bajaj, Dr. U.M. Gokhale "AES ALGORITHM FOR ENCRYPTION" International Journal of Latest Research in Engineering and Technology, Volume 2, Issue 5, May 2016.
[3] Himanshu Gupta "Twin Key Implementation in AES", IOSR Journal of Computer Engineering, Volume 16, Issue 5, Sept 2014.
[4] Dr. R. Prema "AES Algorithm Based Secure Data Transmission for Wireless Sensor Networks", International Journal of Applied Engineering Research, Volume 11, 2016.
[5] Muthulakshmi P, Shathvi K, Aarthi M, Seethalakshmi V "Encrypted image with hidden data using AES algorithm",International Journal of Science, Engineering and Technology, Volume 5, Issue 4, April 2016.