An Effective Way of using LSB Steganography in images along with Cryptography

Unik Lokhande
Research Scholar
Government College of
Engineering, Aurangabad

ABSTRACT
Hiding data is a very important thing nowadays as the data travels over various unsecure networks. To avoid this problem cryptography is used which hides the data or scrambles your message, but cryptography alone cannot provide total security as the message is still available to perform cryptanalysis. Steganography hides the existence of the message. Most of the peoples use either cryptography or steganography to improve security. But a combination of both the techniques provides better security. This paper will describe an effective way of using cryptography along with a modification in LSB steganography in images.

General Terms
Image steganography

Keywords
LSB steganography, cryptography, AES

1. INTRODUCTION
Nowadays most of the data is stored digitally. Spreading of information has extensively increased since the development of the internet and millions of megabytes of data travel over the networks every day. This is increasing day by day. Internet is one of the main sources of commerce. Some of this data is personal and very sensitive like passwords, atm pins etc. which attracts a lot of attention. Attackers/hackers tend to use this data for wrong purposes. Therefore preserving, confidentiality and data integrity against unauthorized access is very important. Due to these security issues there are various ways that have been developed for securing information. First is Cryptography which changes the message into an unreadable format. This process is known as encryption; only intended user can convert it into a normal message. But this might generate the curiosity of the intruder as the encrypted message is available. A message in plain sight which is easily available will definitely attract the curiosity of a potential intruder as it will set him up with the challenge of cracking the code and generating sense out of the garbage message plus it might also plant the idea that the message must be something confidential as someone has taken the effort to write it in a code that can only be cracked by someone holding the key, as opposed to a hidden message which might go undetected and hence reducing the risk of attempts being made to decipher it. Hence it is sensible to hide the existence of the message so that no one can guess that there is a hidden or a secret message present. Now this is where the second method comes into play which is steganography. Steganography hides the existence of the message by hiding it into media like images or audio files. In order to provide a better security a combination of both the techniques is used. The most simple and common method is LSB Steganography. This stores the message by replacing the Least Significant Bit (LSB) values in the image pixels. As it is the simplest method the message can be stripped from the images easily. The main motive of this paper is to explain LSB Steganography in images and how to improve LSB steganography.

1.1 Cryptography
Cryptography is synonymous to encryption. Encryption is a process of converting plaintext (data or message) into ciphertext (encrypted text). Since ancient times it has been a practice to try and send a message to your allies without it being picked up an adversary. It is used to provide the strategic leverage needed in order to prevent any unwanted person from gaining any intelligence that might jeopardize the entire mission, for example Julius Caesar used to send messages to his generals in a coded format and the generals would decipher it using a key that only they had access to hence giving birth to “Caesar cipher”. This has been an essential element in the art of war and a way of communicating war strategies even during World War I. These “keys” or ciphers usually follow a logical pattern or an algorithm but with the advent of the age of information technology, these methods started becoming obsolete as major algorithms that were earlier known to only an elite group became common knowledge and software’s enhanced the process of guessing and cracking the algorithm patterns both previously known or newly created.

Cryptography acts as a shield for the data by keeping it safe form changes and pilferage and as a result has become a prerequisite when data needs to be transmitted via any public medium especially the internet or any other network. Cryptography can also be used as a tool for user verification, but can also be used for user authentication. Encryption is a process of converting plaintext into ciphertext. Decryption is a process where encrypted text or ciphertext is converted back into original message.

The following three cryptographic schemes are very popular typically used with some Cryptographic algorithm [1].

a) Secret key (or symmetric) cryptography
b) public-key (or asymmetric) cryptography and
c) Hash functions.

Secret key cryptography is also known as symmetric key cryptography or private key cryptography. In this scheme both sender and receiver uses the same key to encrypt and decrypt data. The use of a secured channel in order to exchange the key in the process of symmetric encryption lowers its utility usefulness. So the main problem arrives when the keys are to be exchanged. If user wants to communicate with different people with separate confidentiality level he has to use different number of keys for each individual. If there is a

group containing 'N' number of people. Who are using secret-key cryptography scheme, then it is mandatory to administer a number of keys equal to N * (N-1) / 2.

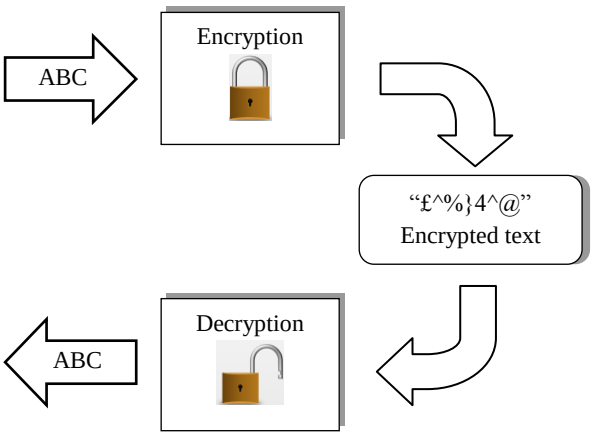


Fig. 1: Encryption and Decryption

Some of the symmetric key algorithms are:

a. Data Encryption Standard (DES)
b. Triple Data Encryption Standard
c. (Rivest Cipher) RC2
d. Advanced Encryption Standard (AES)

Public key cryptography is also known as asymmetric cryptography. In this scheme both sender and receiver share different set of keys used for encryption and decryption. When sender wants to send a secure message to receiver, sender uses receiver public key to encrypt the message. Receiver then uses his private key to decrypt it. The system uses a special method involving the use of two keys for encryption and decryption, namely a public key and a private key. In public key cryptography public key might be known to everyone but private key must be secret irrespective of the owner. The encryption is achieved using the public key and the cipher can only be decrypted with the use of the private key, which is revealed only to the intended recipient. To make the system more secure the keys are designed in such a way that even if the public key is breached and a hacker has gained access to it, he won't be able to use it to decipher the private key.

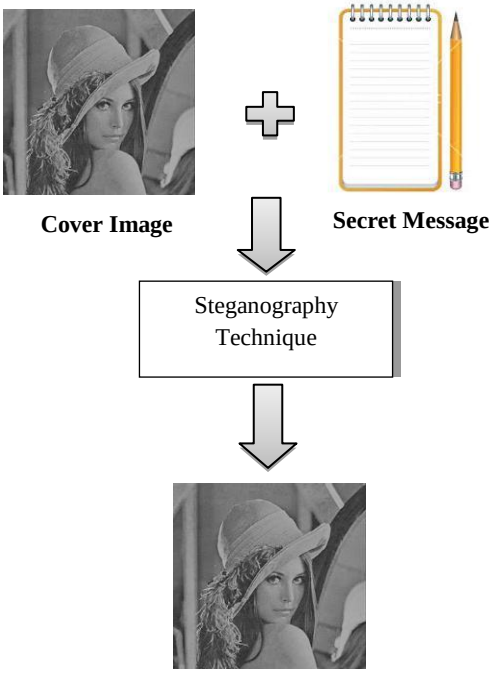
Some of the most commonly used asymmetric cryptography algorithms are:

a) RSA
b) DSA
c) Diffie-Hellman
d) Elliptic Curve Cryptography (ECC)

On the other hand, hash function encrypts information irreversibly by the means of mathematical transformation. Majority of operating systems make use of hash function to encrypt a password. The hash function computes the fixed length hash value entirely upon the number of plain text thereby making the recovery of the length or the content of the plain text unattainable. Hash functions are often used to warrant that the file has not been tampered with by an intruder or a virus. Hash algorithms are also used to obtain a digital signature of the file's content and thus can be used to check the file's integrity.

1.2 Steganography

The term Steganography is a combination of Greek words stegnos which means "covered or protected" and grafia means "writing"; so steganography itself means "concealed writing". Steganography is the science of hiding a message in a manner such that the existence of message is unknown. The existence of message is known only to the recipient of the message. In steganography the messages that have to be concealed can be injected or appended into another digital file that usually called as cover file or cover medium. In other words purpose of steganography can be explained as "the aim of steganography is to go incognito i.e. if no attention is drawn to the hidden message then stegnography has achieved its goal"[2].



.

Fig. 2: Basic process of steganography

The steganography techniques can be classified as 'fragile' or 'robust' depending upon the strength of the stego object against invader inspection. If the stego object manages to hold its hidden message as well as the cover object even after being subjected to multiple image processing techniques such as rotating, warping, cropping and blurring are categorized as robust and the others in which the hidden message is lost under jpeg compression or gets destroyed because of the use of image processing techniques are called as fragile [2].

The three of the most commonly used steganography techniques are explained in a nutshell below:

a) Least Significant Bit Algorithm: This is a simple logic in which the message is broken into 1 bit pieces and the least significant bit of each pixel of the cover object is used to carry the secret message pieces the method can be easily countered as the change in cover object is visible to the naked eye post 4th LSB. This technique is unsuccessful and visible to naked eyes, when the bits of the hidden message have more space to be placed than the cover image [3].

b) Patchwork Algorithm: these algorithms start off with the random selection of two pixels of the image and proceed simply to make the brighter pixel brighter and the darker one more dark. This method ranks a place higher in terms of complication when compared to the LSB technique but the good part is that the image continues to remain incognito despite filtering attacks [4].

c) Transform Domain Algorithms: This technique hides the message in significant areas of the cover image using complex algorithms such as DCT (Discrete Cosine Transformation) or Wavelet Transformation making the stego object more invincible against image processing attacks than LSB [2].

Steganographic system depends upon the following critical factors. They are robustness, capacity, and security [5, 6]. The conjugation between these characteristics can be depicted by the steganography triangle shown in Fig. 3. It represents the balance of the desired characteristics in relation with the steganographic method. They are co-dependent on each other and in order to enhance the quality of an element, one or both of the other elements need to be degraded. Robustness refers to an embedded message's ability to survive either a deliberate attack by a suspecting third-person or the random corruption by noise in some transmission phase. The maximum number of bits that can be implanted inside an image without damaging it and keeping it visually unscathed is determined by capacity. Security depends upon the embedded carrier's prowess at being indistinguishable or undetectable [8].

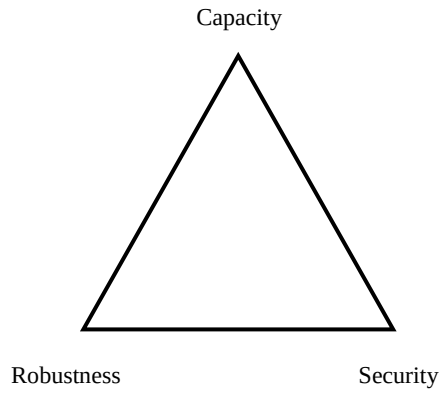


Fig. 3: Steganography triangle

2. PROPOSED METHOD

Neither cryptography nor steganography can provide efficient security; both the techniques have their own advantages. On the other hand a combination of both the techniques can used to achieve better security as compared to the individual technique. Here AES algorithm is used for encryption and hiding an encrypted message inside an image. After message is encrypted it is then embedded into image using LSB steganography. The proposed method has been divided into two phases; first one deal with the AES encryption and second one deal with the LSB Steganography.

2.1 Description of AES

AES is a symmetric block cipher which is based on substitution permutation network. AES has a fixed block size of 128 bits or 196bits or 256 bits. Depending on the block size there are three versions of AES namely AES-128, AES-196,

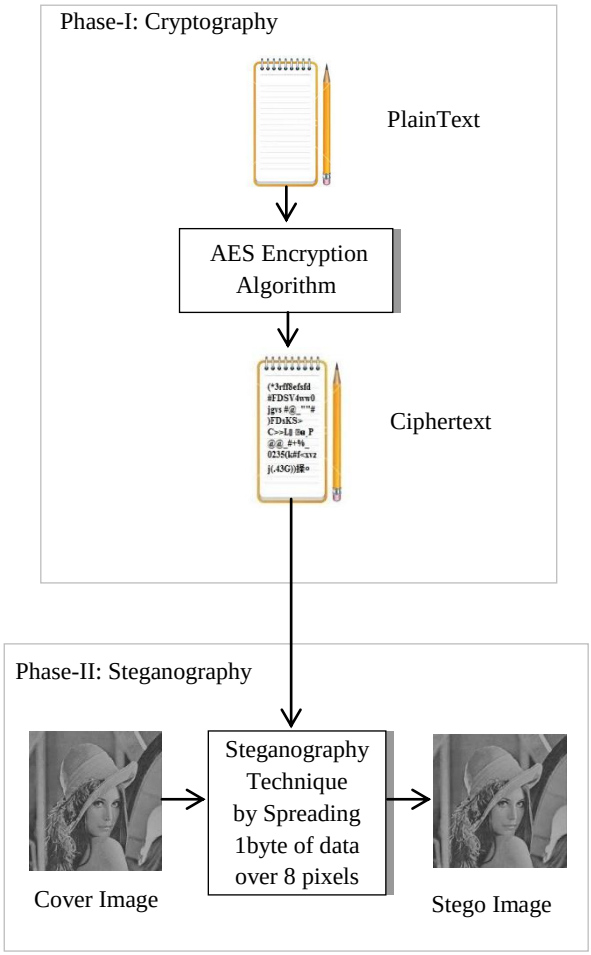


Fig. 4: Proposed Method

And AES-256 and these numbers represent repetitions of transformation rounds (10, 12, and 14 respectively). In this proposed system AES-128 is used. AES is simple, easy to implement and with slight a change in the 'steps of the process like bitwise left or right shift or xor changes the complexity of the process can be increased. The main loop of AES performs four main functions. These functions are: [9]

- Substitution of bytes: This scrambles each byte.
- Shifting Rows: Scrambles each row.
- Mixing columns : Scrambles each columns
- Adding Round Keys : Encrypt

2.1.1 Substitution of Bytes

This is called subByte because of substitution of bytes during forward process. This step involves a look up table. The look up table consist of entries which are arrived at by using multiplicative inverse and bit scrambling notions in order to sabotage the bit level correlations inside each byte. This look up table is used to arrive at a replacement byte that will substitute a given byte in the input state array. One can use a better substitution algorithm for a better output of this stage [9].

2.1.2 Shifting of Rows

This step causes shifting of rows of the state array during forward process. This transformation aims at scattering the byte order of all 128 bit blocks [9].

2.1.3 Mixing of Columns

This step involves combining 4 bytes in each column and mixing byte separately in each column during the forward process. The purpose of this step is additional scattering of the 128 bit input block. The shift-rows step along with mix-column step causes each bit of ciphertext to depend on every bit of plaintext after 10 rounds of processing [9].

2.1.4 Add the Round Key

In this step the round key is added to the output of the preceding step during the forward process. The actual encryption is performed on this step when each byte in the State is XORed with the subkey [9].

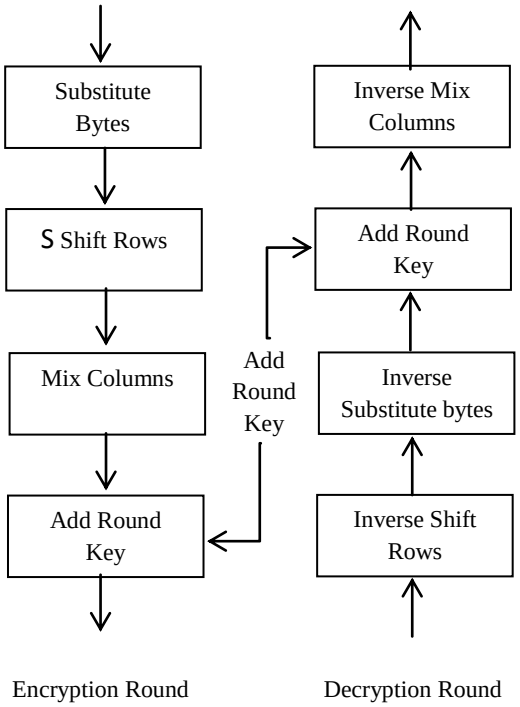


Fig. 5: Encryption and Decryption using AES

2.2 LSB Steganography

As it is important to choose a good Steganography technique it is equally important to choose a good cover image. The images can be broadly classified into two main categories; lossy and lossless. JPEG format comes under lossy compression and in order to achieve extremely high compression it losses data. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. Each pixel in image is made from the combination of RGB pixel which is represented by 3 bytes in 24-bit bitmap. Three bytes are used to represent the red, blue and green color values of each pixel. However this is not the case with an 8-bit bitmap which uses 1-byte. Here each pixel is denoted by an offset instead its color value in a palette. So it is best to use 24-bit bitmap because when an image is of high quality and resolution it is easier to hide information inside it. Using LSB steganography one can embed 3 bit data in each pixel of 24-bit BMP image and replace those LSB's with 3 message bit.

The method proposed in this paper makes use of LSB Steganography but instead of replacing all 3 LSBs of a pixel it is replacing only one bit of a single color component. This can be red, green or blue color component from the pixel.

If a letter 'a' is to be embedded in image which is represented as 01100001 in binary the first bit 0 is embedded in only one color component of the pixel. One can use any color component for this purpose but here only the blue color components are used to understand this process. The following example will help to understand the process better. Consider there are 8 adjacent pixels (24bytes) with RGB encoding. The pixels values are shown inside their respective color.

10001101	01110110	11101011
11010010	10000011	00110011
10111010	11101011	10000001
10001101	01110110	11101011
11010010	10000011	00110011
10111010	11101011	10000001
10001101	01110110	11101011
11010010	10000011	00110011

Fig. 6: Original grid of image

The letter 'a' which has binary representation 01100001 is embedded into the least significant bits of this part of the image. By overlaying these 8 bits over the LSB of the 24 bytes above get the following grid is obtained (where bits in bold have been changed).

10001101	01110110	1110101**0**
11010010	10000011	00110011
10111010	11101011	10000001
10001101	01110110	1110101**0**
11010010	10000011	0011001**0**
10111010	11101011	1000000**0**
10001101	01110110	1110101**0**
11010010	10000011	00110011

Fig. 7: Modified grid of image

Here letter 'a' is embedded into an image grid and in order to do so only 5 LSBs are needed to be changed. The LSB values of which every bit must be changed in the source image. There is a fifty percent chance that the required value is already in the LSB of color channel. So there is no need to change value here, Because of vector nature of colors. Even if every bit in our source image needs to be changed, the change will still be very minute.

More modifications can be done on this method like, one can store each bit in a new color component every time the message bit progresses. Or can use pseudo random number generators to store each bit into random color component's LSB. As the proposed method used only one of the color components of the pixel the damage done to the pixel is very less as compared to the sequential LSB technique. In sequential LSB technique all the LSB of color components of the pixels are changed. The one drawback of this method of steganography method is that its ability to hold less amount of data than sequential LSB technique.

2.2.1 Steganography Algorithm for proposed method

The main steps of algorithm are:
1. Get a pixel from bitmap image.
2. Take the first bit of the message byte
3. Extract just one color component from the pixel.
4. From this color component acquire its LSB.
5. If the color-bit of color component is different from the message-bit, set or reset the bit.
6. Repeat the same process for the other remaining message bits.3

3. CONCLUSION

The proposed method is very easy to implement and most of the pixel values are retained as the method only uses a single color component in pixel. A combination of both the techniques provides better security against attacker. The message cannot be easily stripped from the image which is opposite case in LSB steganography in which all the LSB are replaced. This method depends upon the conservation of every last bit of information in the image. The image losses its ingenious color information upon being converted to a lossy format such as JPEG file. One more disadvantage associated with LSB technique is that the attacker can change all the LSB of the image thus destroying message in the image.

4. ACKNOWLEDGMENTS

I sincerely thank my research guide Prof A. K. Gulve Department of Computer science and engineering, Government College of engineering Aurangabad, for his guidance, encouragement, valuable suggestions and moral support throughout the progress of this research.

5. REFERENCES

[1] Rajani Devi.T "Importance of Cryptography in Network Security" International Conference on Communication Systems and Network Technologies IEEE 2013(462 - 467).

[2] N. F. Johnson and S. Jajodia, "Steganalysis: The Investigation of Hidden Information", IEEE Information Technology Conference, September 1998.

[3] J. Cummins, P. Diskin, S. Lau and R. Parlett, "Steganography and Digital Watermarking", School of Computer Science, the University of Birmingham, 2004.

[4] J. Watkins, "Steganography – Messages Hidden in Bits", 2008.

[5] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forens. Security 5 (2) (2010)201-214.

[6] Ge Huayong, Huang Mingsheng, Wang Qian, "Steganography and Steganalysis Based on Digital Image", IEEE Trans. International Congress on Image and Signal Processing, (2011) 252-255.

[7] Nur Hadisukmana, Yosua Kristianto "Steganography Software with Combination of Encryption Algorithms for Multimedia Files" First International Conference on Informatics and Computational Intelligence IEEE Dec-2011(100 - 105).

[8] Manoj Kumar Ramaiya ,Naveen Hemrajani, Anil Kishore Saxena "Security Improvisation in Image Steganography using DES" 2012 IEEE(1094 - 1099).

[9] Parag Kadam, Mangesh Nawale, Akash andhare, Mukesh Patil "Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique" Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering February 21-22 2013 IEEE.