An Efficient Technique for Image Steganography

Varsha Atul Meshram¹ Amutha Jaykumar²
¹,²Department of Electrical Engineering
Veermata Jijabai Technological Institute, Mumbai, India

Abstract— Steganography is the art of hiding information that prevents detection without affecting the image. It is a technique to hide secret information in image or audio visuals without any evidence of alteration. Least Significant Bit (LSB) technique can hide only 10 to 15% of the data amounts of the cover image. LSB techniques used only true color image (24 bits color image). This is because the principle of those techniques was either to replace a special part of the frequency components of the vessel image, or to replace all the least significant bits of a multi-valued image with the secret information. In this work an improved version image steganography is used which will enhance the hiding capacity and also provides security for hidden text. Before hiding the message, it is encrypted using sequential coding & Advanced Encryption Standard (AES) algorithm using 128 bits as an input. In sequential coding technique, code is implemented sequentially starting with the top left pixel and then encodes information from top to bottom and left to right. Then the encrypted message is hidden in the stego-image with the help of random coding and is implemented randomly which encodes pixel across the entire image in an attempt to be less noticeable to analysis. The proposed technique provides more security & more data hiding capacity.

Key words: Steganography, Stego-image, LSB method, AES

I. INTRODUCTION

Steganography is defined as the art and science of writing hidden messages in such a way that no one else, apart from the intended recipient knows the existence of the message. The word “steganography” is basically of Greek origin which means “hidden writing”. The word is classified into two parts: steganos which means “secret” and “graphic” which means “writing”. However, in hiding information, the meaning of steganography is hiding text or secret messages into another media file such as image, text, sound or video. History of steganography dates back to 440 B.C. this technique was initiated by ancient Greeks, they shave the heads of their slaves and write the messages on their heads, after the hair had grown back, the slaves were sent to their allies without the enemy’s knowledge. Steganography was also used by Germans during the World War I and II. Also during the American Revolution, invisible ink was used by the revolutionaries for communication purposes. The motto behind developing steganographic methods is its application in secret communication between the members of an organization involved in mission critical situations like wars; also it can be used for communication between intelligence agencies etc.

The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this objective that has been planned to achieve the security of the secret message because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message. The basic terminologies used in the steganography systems are: the cover message, secret message, the secret key and embedding algorithm. The cover message is the carrier of the message such as image, video, audio, text or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually used to embed the secret information in the cover message.

The word “steganography” is often considered similar to “cryptography” and “watermarking”. The terms cryptography and watermarking are as discussed in Section IA and IB respectively.

A. Watermarking

Communication in watermarking is the host signal, with the embedded data providing copyright protection. The existence of a watermark is often declared openly.

B. Cryptography

It does not conceal the communication. Also it scrambles the data to prevent eavesdroppers understanding the content. Cryptography involves various methods and implementations.

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography can be broadly classified into four categories:
1) Text Steganography
2) Image Steganography
3) Audio Steganography
4) Video Steganography

The organization of the paper is as follows. Section II explains image steganography in detail along with its evaluation parameters. Sequential Coding Technique is discussed in Section III. Section IV discusses Random Encoding Technique. The AES algorithm is discussed in Section V. Finally the proposed algorithm is discussed in Section VI.

II. IMAGE STEGANOGRAPHY

In image steganography the information is hidden exclusively in images. The data which is to be hidden is known as secret message and the image which is used to hide the message is the cover image. The image obtained after embedding the message image in the cover image is known as stego image.

The embedding process depends upon the image steganography techniques selected. The stego image obtained should be identical to the cover image so that no one can identify the presence of message maintaining the Integrity of the Specifications.
The flow diagram of the encoding & decoding procedure involved in steganography is as shown in Fig. 1.

The secret message to be hidden & the cover image is given to an embedding function. This embedding function decodes the security & data hiding capacity. Once the secret message is embedded inside the image using secret key, the image is known as the stego-image. This completes the encoding process.

In the decoding process, the stego-image is given to an extraction algorithm. Using the secret key, the secret message can be retrieved back from the stego-image. Images are basically classified into 8 bit color image and 24 bit color image.

A. 8 Bit Color Image

8 bit color system [2] is very limited but true direct color system, there are three bits (2^3 = 8 possible levels) for each of the R and G components, and the two remaining bits in one byte pixel to the B component (four levels), enabling 256 (8x8x4) different colors. Since normal human eye is less sensitive to the blue component than to the red or green, so it is assigned one bit less than the both. There are two forms of 8-bit color graphics. The most common graphics uses a separate palette of 256 colors, where each of the 256 entries in the palette maps to given red, green, and blue values. In most color maps, each color is usually chosen from a palette of 16,777,216 colors (24 bits: 8 red, 8 green, 8 blue). The other form is one in which the 8 bits directly describe red, green, and blue values, typically with 3 bits for red, 3 bits for green and 2 bits for blue as shown in table 1. This second form of color graphics is often called 8-bit truecolor, as it does not use a palette at all, and is more similar to the 15-bit, 16-bit and 24-bit true color modes.

B. 24 Bit Color Image

24 bit color image [2] is best defined by RGB color model in which each color appears in its primary spectral component of red, green and blue. In which RGB primary values are at three corner, the secondary color cyan, magenta and yellow are at three other corner, black is at the origin and white is at the corner farthest from the origin. Line joining the two corners has equal values for red, green and blue. This produces various shades of grey. The locus of all these points is called the grey line. In RGB model, each pixel is composed of RGB values and each of these colors requires 8-bit for its representation. Hence each pixel is represented by 24 bits. So total number of color possible with 24-bit RGB image is (256^3) = 16,777,216.

8 bit color image will have 2^8 = 256 shades in the image. On the other hand, the 24 bit color image will have 2^24 = 16,777,216 color variations. Hence the proposed algorithm uses 24 bit color image.

C. Evaluation parameters for Image Steganography

Generally image steganography is categorized in following aspects:
1) High Capacity: Maximum size of information can be embedded into image.
2) Perceptual Transparency: After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to cover image.
3) Robustness: After embedding data should stay in fact if stego-image goes into some transformation such as cropping, scaling, filtering & addition of noise.
4) Temper Resistance: It should be difficult to alter the message once it has been embedded into stego-image.
5) Mean Square Error: The mean square error is given by Eq. 1.
   \[ MSE = \frac{1}{MN} \sum_{m,n} (I_{m,n} - I'_{m,n})^2 \]  
   (1)
6) Peak Signal Noise Ratio: The peak signal to noise ratio is given by Eq. 2.
   \[ PSNR = 10 \log_{10} \frac{255^2}{MSE} \]  
   (2)

III. SEQUENTIAL CODING

The possibilities of today’s communications need the special means of data security especially on computer network. Network security is very important, as the amount of data being exchanged on the Internet increases. So, there is a great need of confidentiality and data integrity, which is required to protect the data against unauthorized access and use. Because of this new method is developed for hiding information, is called ‘Sequential coding’.

Sequential coding having two parts,
1) Sequential Encoding
2) Sequential Decoding

A. Sequential Encoding

In the proposed method, the input secret message of 128 bits is encrypted using key k1. Initially text message is converted into ASCII value including space value. The header is applied to the beginning of the message which is to be encoded. Image size is determined for encoding. Using XOR key, message is encrypted. The ASCII value is then converted into binary. The data points are hidden using a RGBBGRGR Order behind RGB colored image. The encoding Code is implemented sequentially starting with the top left pixel and then encodes information from top to bottom and left to right.

B. Sequential Decoding

For decryption & extraction of text message from image, the same XOR key will be used. The header is removed by taking modulus of message embedded image with 2, so as to get digital bits. The binary data is converted into integer value. Integer values are then converted into characters. The characters will be written into the text file thereby separating message & image.
IV. RANDOM CODING

In this technique, a random key is used to choose the pixels randomly and embed the message. This will make the message bits more difficult to find and reduce the realization of patterns in the image.

Random coding having two parts,
1) Random Encoding
2) Random Decoding

A. Random Encoding

In this process of encoding method, a random key is used to randomize the cover image and then hide the bits of a secret message into the least significant bit of the pixels within a cover image. The transmitting and receiving end share the stego key and random-key. The random-key is usually used to seed a random number generator to select pixel locations in an image for embedding the secret message.

B. Random Decoding

In this process of extraction, the process first takes the key and then random-key. These keys take out the points of the LSB where the secret message is randomly distributed. Decoding process searches the hidden bits of a secret message into the least significant bit of the pixels within a cover image using the random key. In decoding algorithm the random-key must match i.e. the random-key which was used in encoding should match because the random key sets the hiding points of the message in case of encoding. Then receiver can extract the embedded messages exactly using only the stego-key.

V. ADVANCED ENCRYPTION STANDARD (AES)

AES is a symmetric encryption algorithm. This algorithm uses a 128 bit data block, & three different key sizes 128, 192 & 256 bits. The 128 bit data block is divided into 16 bytes & mapped into 4*4 array called as state. It is an iterative algorithm. The total no. of rounds Nr is depend on the key length Kr. The flowchart for AEC encryption & decryption is as shown in Fig.2 and 3.

VI. PROPOSED SYSTEM

Fig.4 shows the flowchart of the proposed scheme. The message of 128 bits is encrypted first using sequential encoding scheme discussed in Section III A. This encrypted text message is again encrypted using AES algorithm explained in Section V. Thus the secret message is encrypted thrice thereby strengthening the security aspect.

Now, the thrice encrypted message is embedded into image using Random Encoding scheme discussed in Section IV A. The advantage of this proposed approach is that an unauthorised receiver would need to guess 3 keys approximately to decode the secret message from image.
Finally the output of AES decoding algorithm is
given to sequential decoding algorithm discussed in section
V along with key k1. Thus the secret message is finally
obtained after the three stage decryption proposed
procedure. The complexity of the proposed algorithm is
increased by using 3 keys thereby making the procedure
difficult to decipher.

Fig. 5: Flow graph of proposed method decryption

VII. CONCLUSION
Steganography refers to the technology of hiding data into
digital media without any change. In this paper, along with
existing techniques of image steganography, some new
methods for hiding data in images are discussed. Data can
be encrypted using sequential coding & AES algorithm
using two keys. Third key is used to hide encrypted data
inside the stego-image with the help of random coding. The
proposed technique provides more security & more data
hiding capacity.

REFERENCES
Image Steganography using BPCS: Survey and
Analysis." IOSR Journal of Computer Engineering
(IOSR-JCE) 15.4 (2013).
steganography technique for hiding image in an image
using Lsb method for 24 bit color image." International
Sabir. "High capacity steganography method based
upon RGBA image." Int J Adv Res Comput Commun
Eng (ISSN: 2278-1021) 4.6 (2015).
Image Steganography Techniques. on" International
Journal of Advanced Research in Computer and
Communication Engineering 2.3 (2014).
LSB based image steganography techniques." Computer
Communication and Informatics (ICCCI), 2014
International Conference on. IEEE, 2014.
parameters of image steganography techniques."
Research Advances in Integrated Navigation Systems
(RAINS), International Conference on. IEEE, 2016.
Kumar Singh. "A hybrid approach of image
steganography." Computing, Communication and
Automation (ICCCA), 2016 International Conference
on. IEEE, 2016.
Saranya. "Security Enhancement in Image
Steganography a MATLAB Approach." Middle-East
Algorithm and BPCS Technique for a Securing Image
Data." (2016).
BPCS steganography using Hybrid
cryptography for improving data embedding capacity." Communication, information & computing technology
(ICICT), 2012 international conference on. IEEE,
2012.
steganography technique based on MSB using bit
differencing." Innovative Computing Technology
(INTECH), 2016 Sixth International Conference on.
IEEE, 2016.
image steganography in spatial domain." Emerging
trends in VLSI, embedded system, nano electronics and
telecommunication system (ICEVENT), 2013
and Performance Evaluation of Text Data Hiding
Technique using Sequential Encoding and Decoding
Technique."