International Journal of Electrical, Electronics and Computer Engineering **5**(1): 61-66(2016)

ISSN No. (Online): 2277-2626

An Effective Algorithm on Image Steganography by using LSB

Harshal Badgujar*, Shiva Bhatnagar** and Ankit Chouhan**

**Research Scholar, Patel College of Science & Technology, Indore, (Madhya Pradesh), India*

***Assistant professor, Patel College of Science & Technology, Indore, (Madhya Pradesh), India*

(Corresponding author: Harshal Badgujar)

(Received 04 April, 2016 Accepted 02 June, 2016)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Steganography is the art and science of communicating in a way which hides the existence of the secret message communication. Many steganographic techniques are well developed but these are having some drawbacks. Existing systems are straight forward but has low ability to bear some signal processing or noises. So there is a need to propose a method which will provide better security for information along with better stego image quality for this purpose now I am proposing a method to transfer secret message towards destination this is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is comes from the Greek words "*stegos*" means "cover" and "*grafia*" means writing" [1] defining it as "covered writing". In image steganography the information is hidden exclusively in images. In this paper by using LSB technique we merge the data in digital image.

Keywords : steganography, LSB cryptography security hiding digital image

I. INTRODUCTION

Steganography is the technique of masking the actual data in digital image that communication is taking place, by shielding the information in other information. 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 steganographic techniques some are more complex than others and all of them haverespective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Information to be hidden/mask+ cover object/image = stegoobject/image

II. ASPECT OF STEGANOGRAPHY

The idea and practice of hiding information has a long history. In *Histories* the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message [2]. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with oneof the periods on the paper containing hidden information [3]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [4]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised.

Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [4]. The strength of steganography can thus be amplified by combining it with cryptograph.

Two other technologies that are closely related to steganography are watermarking and fingerprinting [5]. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden/masked in objects when using watermarking is usually a signature to signify origin or ownership for the purposeof copyright protection [6]. With fingerprinting on the other hand, different, unique marks are embedded indistinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties [5]. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial [4]. A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it [5].

Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether [7], forcing people to study other methods of secure information transfer. Businesses have also started to realize the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit [8]. Hiding information in a photograph of the company picnic is less suspicious than communicating an encryptedfile.Bhattacharyya et al.,[10] proposed a specific image based steganography technique for communicating information more securely between two locations by incorporating the idea of secret key for authentication at both ends in order to achieve high level of security. Before the embedding operation the cover image is segmented in different objects through normalized cut. As a further improvement of security level, the information has been permuted, encoded through integer wavelet transformation by lifting scheme and segmented in different parts and then each part has been embedded through modified LSB embedding method on different cuts of the cover image to form different stego objects. Finally stego image is formed by combining different stego objects and transmit to the receiver side. Sarreshtedari and Ghaemmaghami [11] proposed a high capacity method for transform domain image steganography is and algorithm works on the wavelet transform coefficients of the original image to embed the secret data by retaining integrity of the wavelet coefficients at high capacity embedding.

III. BASIC REQUIREMENTS OF STEGANOGRAPHIC SYSTEM

Invisibility – The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised.

Payload capacity – Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore requires sufficient embedding capacity.

Robustness against statistical attacks – Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a 'signature' when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.

Robustness against image manipulation – In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.

Independent of file format – With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.

IV. IMAGE STEGANOGRAPHY SYSTEM

A classical steganographic system's security relies on the encoding system's secrecy. Although such a system might work for a time, once it is known, it is simple enough to expose the entire received media (e.g., images of all formats) passing by to check for hidden messages ultimately, such a steganographic system fails. The proposed image stenography system is showed as in Fig. 1.

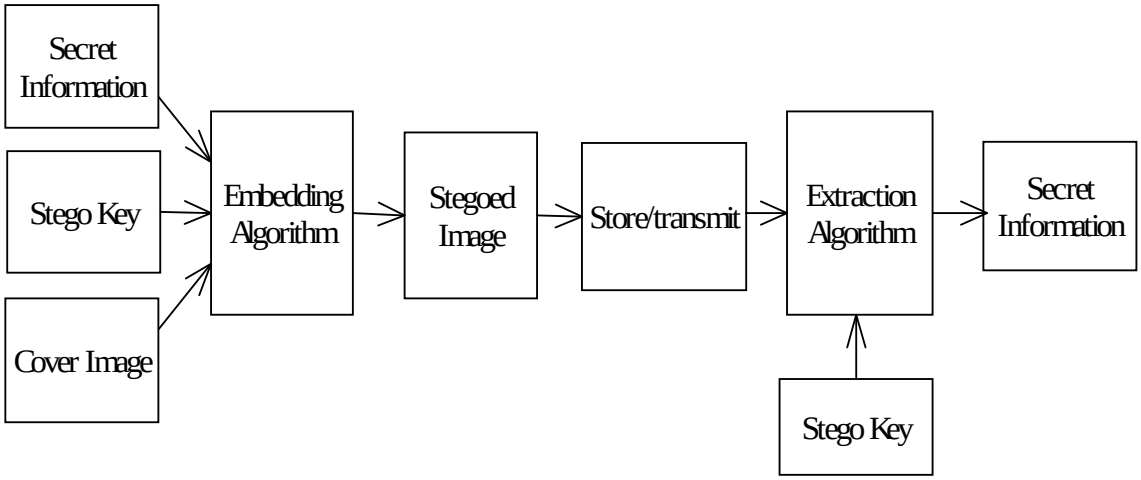

Fig. 1. Proposed Module Image Stenography.

We can hide the secret information data into any image file format in this case we are embedding secret information in an PNG image, hence we will need one png file, also the data to be hidden can be any text file or image file hence we will need one more image file or text file. we are embedding in an PNG image as it provides lossless compression so that our data will not loss. We are using true color images so that minor changes will not be detected by human eye and existence of data is undetected.

V. PROPOSED ALGORITHM

The Rijndael, whose name is based on the names of its two Belgian inventors, Joan Daemen and Vincent Rijmen, is a Block cipher, which means that it works on fixed-length group of bits, which are called *blocks*. It takes an input block of a certain size, usually 128, and produces a corresponding output block of the same size. The transformation requires a second input, which is the secret key. It is important to know that the secret key can be of any size (depending on the cipher used) and that AES uses three different key sizes: 128, 192 and 256 bits. To encrypt messages longer than the block size, a mode of operation is chosen, which I will explain at the very end of this tutorial, after the implementation of AES. While AES supports only block sizes of 128 bits and key sizes of 128, 192 and 256 bits, the original Rijndael supports key and block sizes in any multiple of 32, with a minimum of 128 and a maximum of 256 bits.

Description of the Advanced Encryption Standard algorithm**:** AES is an iterated block cipher with a fixed block size of 128 and a variable key length. The different transformations operate on the intermediate results, called *state*. The state is a rectangular array of bytes and since the block size is 128 bits, which is 16 bytes, the rectangular array is of dimensions 4x4.The cipher key is similarly pictured as a rectangular array with four rows. The number of columns of the cipher key, denoted Nk, is equal to the key length divided by 32.

A state:
a0, 0	a0, 1	a0, 2	a0, 3
a1, 0	a1, 1	a1, 2		a0, 3
a2, 0	a2, 1	a2, 2		a2, 3
a3, 0	a3, 1	a3, 2		a3, 3
A key:
k0, 0	k0, 1	k0, 2		k0, 3
k1, 0	k1, 1	k1, 2		k0, 3
k2, 0	k2, 1	k2, 2		k2, 3
k3, 0	k3, 1	k3, 2		k3, 3

It is very important to know that the cipher input bytes are mapped onto the state bytes in the order a0,0, a1,0, a2,0, a3,0, a0,1, a1,1, a2,1, a3,1 ... and the bytes of the cipher key are mapped onto the array in the order k0,0, k1,0, k2,0, k3,0, k0,1, k1,1, k2,1, k3,1 ... At the end of the cipher operation, the cipher output is extracted from the state by taking the state bytes in the same order.

AES uses a variable number of rounds, which are fixed: A key of size 128 has 10 rounds. A key of size 192 has 12 rounds. A key of size 256 has 14 rounds. During each round, the following operations are applied on the state:

1. Sub Bytes: every byte in the state is replaced by another one, using the Rijndael S-Box

2. ShiftRow: every row in the 4x4 array is shifted a certain amount to the left

3. MixColumn: a linear transformation on the columns of the state

4. AddRoundKey: each byte of the state is combined with a round key, which is a different key for each round and derived from the Rijndael key schedule

VI. OBSERVATIONS

-The cipher key is expanded into a larger key, which is later used for the actual operations

-The roundKey is added to the state before starting the with loop

-The FinalRound() is the same as Round(), apart from missing the MixColumns() operation.

-During each round, another part of the ExpandedKey is used for the operations

-The ExpandedKey shall ALWAYS be derived from the Cipher Key and never be specified directly.

VII. AES OPERATIONS

Sub Byte , Shift Row ,Mix Column and Add Round Key

The Add Round Key operation. In this operation, a Round Key is applied to the state by a simple bitwise XOR. The Round Key is derived from the Cipher Key by the means of the key schedule. The Round Key length is equal to the block key length (=16 bytes).

Where: b(i,j) = a(i,j) XOR k(i,j)

A graphical representation of this operation can be seen as in Fig. 2.

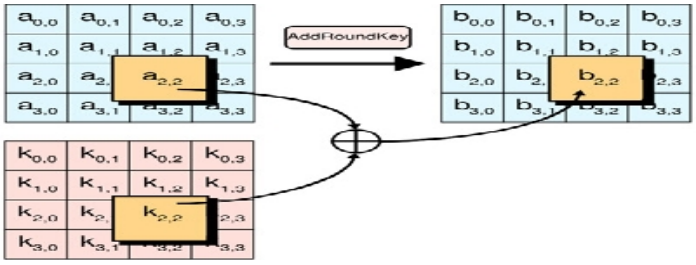

Fig. 2. AES Algoritham.

The ShiftRow operation**:**

In this operation, each row of the state is cyclically shifted to the left, depending on the row index

The 1st row is shifted 0 positions to the left.

The 2nd row is shifted 1 positions to the left.

The 3rd row is shifted 2 positions to the left.

The 4th row is shifted 3 positions to the left.

A graphical representation of this operation can be found in Fig. 3.

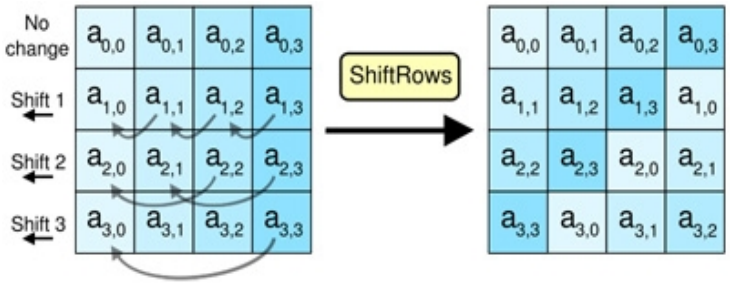

Fig. 3. AES Algoritham.

Note that the inverse of ShiftRow is the same cyclically shift but this time to the right. It will be needed later for decoding.

VIII. STATE DIAGRAM

In proposed method secret data is embedded within image, State diagram describe the behavior of a system, subsystem, or an individual object. A system is assumed to remain in its current state until some new event occurs. State diagram show changes in system state or object attributes in response to external events or triggers. The state diagram as shown in Fig. 4 and 5.

To Hide:

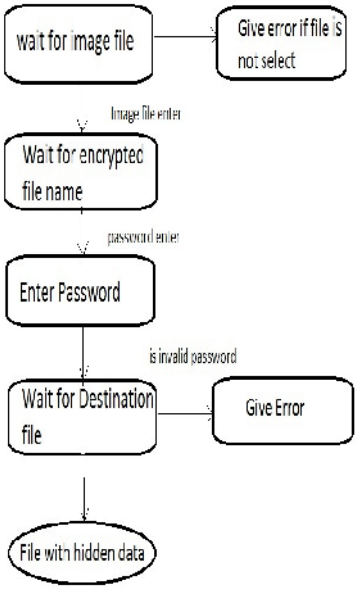

Fig. 4. State Diagrams to Hide

To Extract

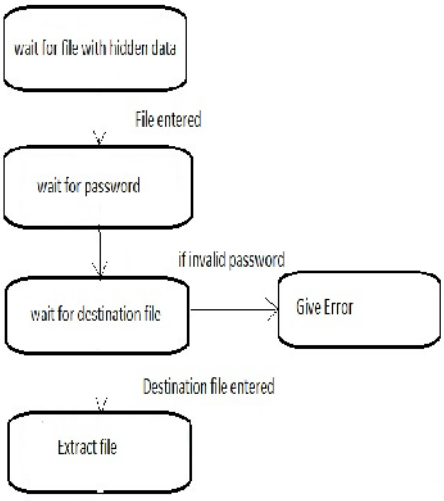

Fig. 5. State Diagrams to extract

IX. EXPERIMENTS AND RESULTS

Fig. 6. PNG image before embedding and after embedding respectively.

X. CONCLUSION AND FUTURE SCOPE

The hiding /masking is really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Through this paper I am doing overcome the problems of steganography like supporting file format and security in this paper we use all type of file format for steganography as well as double security check the future scope for this paper is time consumption for processing and updation on security.

REFERENCES

[1]. Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[2]. Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996.

[3]. Wayner, P., (2002). Disappearing cryptography. 2nd ed. Morgan Kaufmann Publishers.

[4]. Chris Shoemaker, "Hidden Bits: A Survey of Techniques for Digital Watermarking" Independent Study EER-290 Prof Rudko Spring 2002.

[5]. Fridrich, J., Goljan, M. and Du, R.., (2001). "Reliable Detection of LSB Steganography in Grayscale and Color Images." Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, October 5, 2001, pp. 27- 30.

[6]. Po-Yueh Chen and Hung-Ju Lin (2006). "A DWT Based Approach for Image Steganography", *International Journal of Applied Science and Engineering*, 2006. **4**, 3: 275-290

[7]. Misiti M., Misiti Y., Oppenheim G., and Poggi J., (2000). Wavelet Toolbox for Use with MATLAB, User Guide Math Works Inc., 2000.

[8]. Sudhir Goswami & Jyoti Goswami (2014). "An efficient algorithm of steganography using JPEG Colored Image'' Interanational conference onrecent advance in engineering (ICRAIE-2014)May-2014.

[9]. Provos, N. and Honeyman, P: (2003). "Hide and Seek: An introduction to steganography". *IEEE security and privacy*, **01** (3): 32-44,May-June 2003.

[10]. Bhattacharyya S Kshitij and A P Sanyal G, (2010). "A Novel Approach to Develop a Secure Image Based Steganographic Model using Integer Wavelet Transform," *International Conference on recent Trends in Information, Telecommunication and Computing*, pp.173-178, 2010.