UACEE International Journal of Advances in Computer Science and its Applications – IJCSIA
Volume 3 : Issue 2 [ISSN 2250 – 3765]
Publication Date : 05 June 2013

Image Steganography : Self Extraction Mechanism

Manoj Kumar Ramaiya[1] , Naveen Hemrajani[2] , Anil Kishore Saxena[3] , Monika Sharma[4]
[1,2]Department of Computer Engineering, Suresh Gyanvihar University, Jaipur, India
[3,4]Department of Comp.Sci. & Engg., ShriRam College of Engg. & Mgmt., Gwalior, India
[1]manojramaiya@gmail.com, [2]naveennh@gyanvihar.org, [3]anilkishoresaxena@gmail.com, [4]monika.mini22@gmail.com

***Abstract*— The incredible evolution of Internet technologies & its applications requires high level of security for data over the unsecured communication channel. Digital image steganography is technique for hiding information into a cover image. Least Significant-Bit (LSB) based approach is popular steganographic technique in spatial domain due to its simplicity and robustness. All the existing methods of steganography focus on embedding mechanism with less consideration to the pre-processing, such as encryption of secrete image. The conventional steganographic model does not provide the preprocessing, needed in image based steganography for better security.**

The proposed work presents a unique technique for Image steganography based on the S- Box mapping. The preprocessing of secrete image is carried by shuffling of secrete image blocks using three 4×4 unique S-boxes. The preprocessing provide high level of security as extraction is not possible without the knowledge of mapping rules of Substitution box. The proposed scheme is also capable of holding self extraction mechanism to recover the secrete image.

Keywords: Steganography, S-Box mapping , LSB Technique, Cryptography, Preprocessing of Secrete Image.

I. INTRODUCTION

The growing prospects of modern communication need the exceptional means of security especially in computer network communication. The network security is gaining importance as the data being exchanged on the Internet increases. Therefore, the confidentiality and integrity of data required to be protected against unauthorized access. It leads to an explosive growth in info hiding including copyright protection for digital media. Cryptography, Steganography, Digital Watermarking and fingerprinting are unique and highly diverse techniques for information hiding.

Cryptographic technique changes the message so that it cannot be understood but this generates inquisitiveness level of an intruder. It would be rather more sensible if the secret message is cleverly embedded in another media so that no one can guess if anything is hidden. The idea results in steganography, a branch of information hiding by masking secret information within other information. The word steganography comes from the Greek *Steganos* which means "covered" or "secret" and *Grafia* means "writing" or "drawing" i.e., Steganography means literally "*covered writing*"[11]. Thus the stegoimage should not diverge much from original cover image. Cryptography and steganography are widely used in the field of data hiding and have received significant attention from both industry and academia in the recent past. Former conceals the original data but latter conceals the very fact that data is hidden. Steganography provides high level of secrecy and security by combining with cryptography. Throughout history, Steganography has been widely used to secretly communicate information between people.

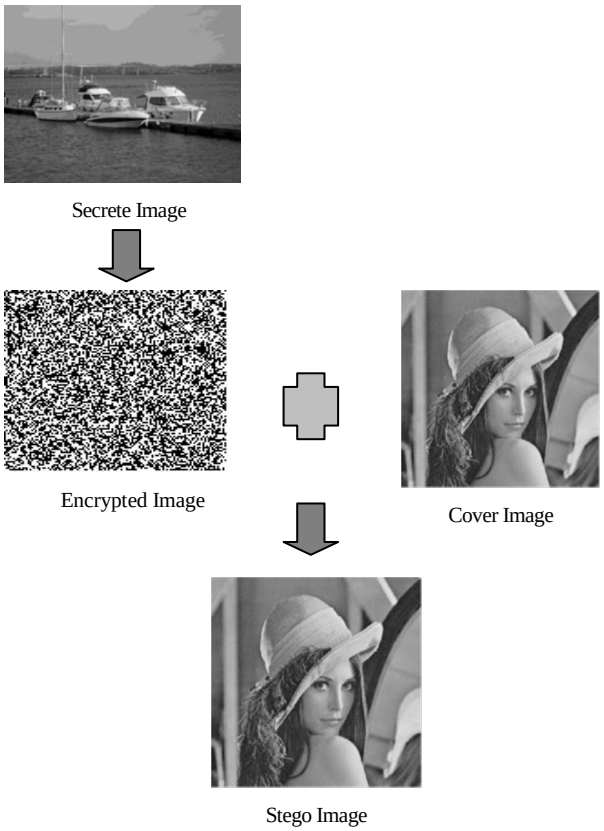


Figure 1. The Block Diagram of Steganographic System

II. RELATED WORKS.

There are large numbers of steganography embedding techniques proposed in the literature. These techniques modify the cover image with different approaches. But the entire embedding technique share the substantial goal of maximizing the capacity of the stego channel [9]. In other words, the aim is to embed at highest possible rate while remaining undetectable to steganalysis attack. Special domain embedding technique operates on the principal of tuning the parameter of the cover

image (payload or disturbance) so that the cover image and the stego image are nearly identical with very little and imperceptible difference to observer.

Steganography generally exploit human perception because human senses are not trained to look for file that has hidden information inside them. Therefore steganography disguises information from people trying to hack them. Payload is the amount of information that can be hidden in the cover object. The most widely known image steganography algorithm is based on modifying the least significant bit of pixel value by either LSB replacement or LSB matching.

The measurement of the quality between the cover image f and stego-image g of sizes N x N (for 8 bit gray level) is defined by PSNR as:

$$PSNR = 10 \times \log (255^2 / MSE)$$

$$\text{Where MSE} = \sum_{N=0}^{N-1} \sum_{N=0}^{N-1} (f(x,y)g(x,y))^2 / N^2$$

Where f(x,y) and g(x,y) represent the pixel value at the position (x, y) in the cover-image and the stego-image respectively. The PSNR is expressed in dB. PSNR is evocative of the quality of image i.e. the higher the PSNR, lower is the variation between cover image and stego image.

Several important issues need to be considered when studying steganographic systems. They are steganographic robustness, capacity, and security [2,3]. The relationship between them can be expressed by the steganography triangle shown in Figure 2. It represents balance of the desired characteristics associated with steganographic method. They are interdependent on each other and in order to improve one element, one or both of other elements needs to be sacrificed.

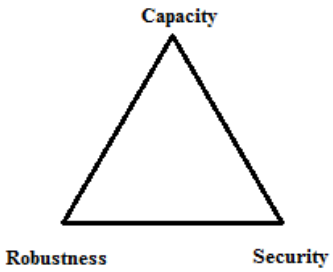


Figure 2 The steganography Triangle

Robustness refers to an embedded message's ability to survive either deliberate attack by a suspecting third party or the random corruption by noise during some phase of the transmission. Capacity refers to the maximum number of bits which could be embedded in the image, without the stego-image remains undetectable and visually intact. Security is the ability of an embedding carrier to remain undiscovered.

III. PROPOSED IMAGE STEGANOGRAPHY MODEL

Proposed steganography scheme is based on encoding function consisting of principal of diffusion and confusion using S–Box mapping.

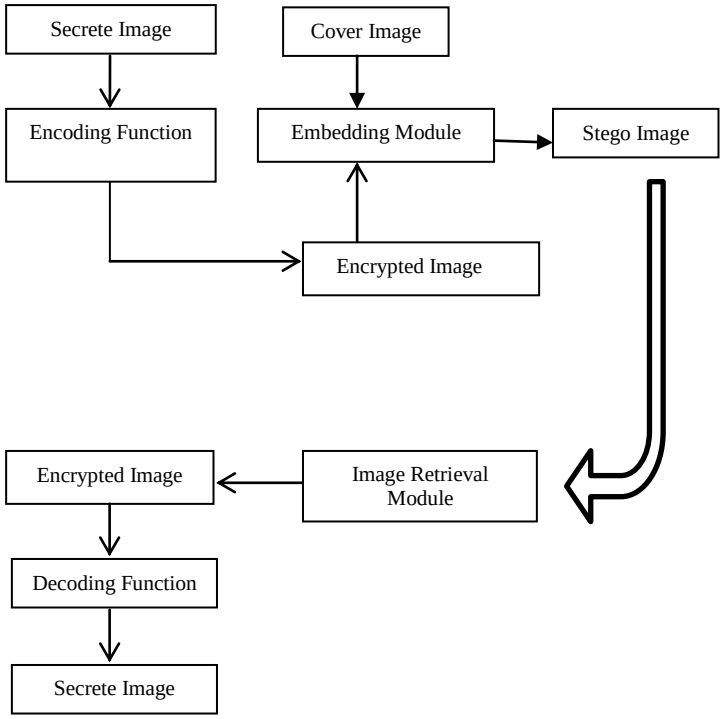


Figure 3. Proposed Model for Steganography

A. *Encoding Function :*

1) **Formation of blocks from Secrete image :** First the secrete image is selected (e.g. of 256×256) and is divided into blocks of 4×4 pixel.

Block size = 4×4 pixel = 16 Pixel
Total number of blocks = 256×256 / 4×4 = 4096 Blocks
Bits needed to represent address of 4096 blocks = 12
Assigning the
address of first block = 0000 0000 0000
address of last block = 1111 1111 1111

2) **Transposition of Blocks using S-Box Mapping :** The groups of 4 bits of the adresses block is inputted to the S1, S2, S3 S-boxes respactively. These S-box satisfied strictly avalanche criterion (SAC) properties.
Every block in the input image now transfers to the new address calculated by three S-Boxes. The operational detail & definition of S-Box as follows:

S1

	00	01	10	11
00	9	1	6	10
01	5	11	15	7
10	12	4	0	13
11	2	8	14	3

S2

	00	01	10	11
00	7	11	5	0
01	10	1	13	8
10	3	14	4	15
11	12	6	9	2

S3

	00	01	10	11
00	2	13	3	11
01	12	9	15	1
10	6	4	8	14
11	0	7	10	5

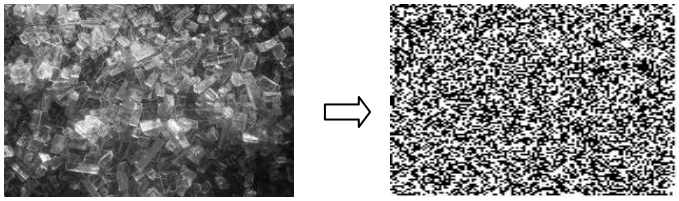
Figure 4. S-Box Definition

Suppose address of Block is = 1011 0101 0011

1 0 1 1 0 1 0 1 0 0 1 1
S1 S2 S3

The input 1011 is applied to S1, 0101 to S2 and 0011 applied to S3. First and fourth bits of input represent row and second and third bit represent column in S-Box. So the input 1011 treated as an 11(third row) and 01 (second column) giving output 8 in S1. This output is now converted into four bit binary sequence giving 1000. Likewise 0101 & 0011 inputting gives output 13 (1101) & 11(1011).

Hence final new block address is: 1000 1101 1011.
So the new location of 1011 0101 0011 (2899th Block) is 1000 1101 1011 (2267th Block).
In the same ways the new addresses of all the 4096 blocks are calculated and rearranged accordingly.



Secrete Image(256×256) Encrypted Image(256×256)

Figure 5. Transposition of Secrete Image

B. *Embedding Module*

The embedding module contains:

1) **Hiding Adress into Cover image :** Cover image having size of 512×512 is divide into four 256×256 regions the first region contain information about adress of block and rest three region contain information about encrypted image.

First Region (Contain Address of Blocks) (256×256)	**Second Region** (Contain 3 bits of each pixel of encrypted image) (256×256)
Third Region (Contain 3 bits of each pixel of encrypted image) (256×256)	**Forth Region** (Contain 2 bits of each pixel of encrypted image) (256×256)

Cover Image (512×512)

Figure 6. Stego Image Distribution

First region of cover image is divided into 4096 blocks of 4×4 pixels.12 bit modified address of every block is stored in first 12 pixel and four remaining unchanged. Now the LSB of all 12 pixel is modified and replaced by the bits of the block address.

2) **Hiding Encrypted Image into Cover image :** The pixel value (8bit) of encrypted image is hidden in the corresponding pixel in the cover image.The first 3 bits of first pixel of encrypted image is distributed in 2nd region , next 3 bits in 3rd region and 2 bits in 4th region. The bits from encrypted image replace the bits of cover image.

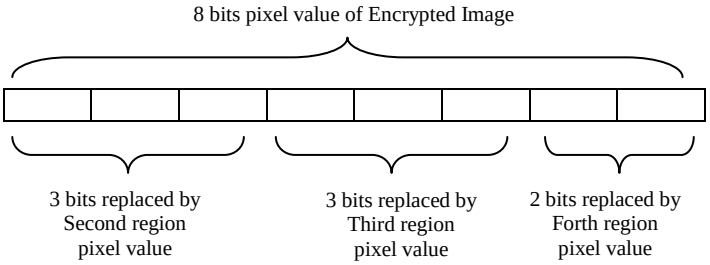


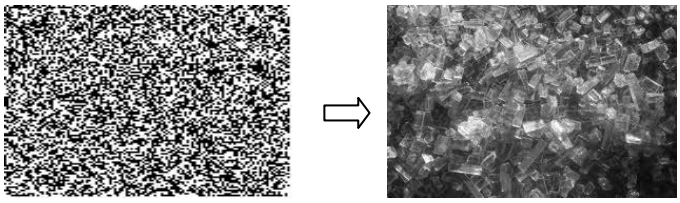
Figure 7. Bits distribution

C. *Image retrival module :* The Image retrival module conatin following steps.

1) **Recovery of encrypted Image :** Secrete image is recovered by taking one pixel simuteneously from second , third and forth region. Now by taking 3 LSB from second region pixel, 3 LSB fron third region pixel and 2 bits from forth region pixel forms 8 bits of first pixel of encrypted image. Likewise by taking every pixel one by one from above region forms whole encrypted image.

2) **Recovery of Secrete Image from Encrypted image :** Encrypted image is divided into block of 4×4 pixel.The address of block is calculated by taking first region of stego image.first 12 pixel amongs 4×4 pixel (16 pixel) are taken and one LSB from these 12 pixel gives 12 bits of codes. These 12 bits are inputted to the reverse S-Box mapping giving actual address of that block. Every block from

the first region of stego image gives original address of that block into the secrte image.



Encrypted Image(256×256) Secrete Image(256×256)

Figure 8. Secrete Image Recovery

IV. RESULTS AND ANALYSIS:

Proposed model is stronger Steganography technique because without prior knowledge of S-box mapping function and bits distribution mechanism, the extraction of secrete image from the stego image is impossible. Moreover quality of cover image is also not degraded due to variation in maximum three LSB of 50% of pixel which reflects only 0 – 8 difference pixel value and two LSB of 25% of pixel which reflects only 0 – 3 difference pixel value and rest having only one bit difference which reflect only 0-1difference.

Additionally the proposed scheme is capable of not just scrambling data but also changes the intensity of the pixels which contributes to the safety of the encryption.

TABEL I CAPACITY & PSNR

Name of Image	Size (Pixel)	Capacity	PSNR In DB
Baboon	512× 512	25 %	41.63
Cameraman	512× 512	25 %	41.98
Lena	512× 512	25 %	41.88
Pirate	512× 512	25 %	42.81
Living room	512× 512	25 %	41.83

V. CONCLUSION:

In the proposed steganographic model, the strength of S-box mapping and confusion of pixel value and address of blocks for encrypting secrete image, improves security and robustness compare to existing algorithms.

Steganography, especially combined with the cryptography is a powerful tool which enables to communicate secretly. With the rapid development of digital technology and internet, steganography has advanced a lot over past years.

All of the existing methods of steganography focus on the embedding strategy and lesser consideration to the pre-processing stages, such as encryption of secrete image, as they depend heavily on the conventional encryption algorithms which obviously are not tailored to steganography applications where flexibility, robustness and security are required. Essentially, either increasing the steganographic capacity while retaining the imperceptibility (stego image quality) or increasing the imperceptibility while keeping the steganographic capacity represents a substantial support

ACKNOWLEDGMENT

The principle author's acknowledgment is due to Sh.R.S.Sharma, Chairman, ShriRam Group of Colleges (SRGOC) for the inspiration and dedication to carry the research.

REFERENCES

[1] Yambin Jina Chanu , Themrichon Tuithung , Kh Manglem singh," A Short Survey on Image Steganography and Steganalysis Technique " , IEEE Trans. ,2012 science and Management (ICAESM- 2012) 709 -713.

[2] 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.

[3] 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.

[4] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Parta Pratim Sarkar " An Image Steganography Technique using X-Box Mapping", IEEE Trans. International Conference Advances in Engineering,

[5] Guilliang Zhu, Weiping Wang, "Digital Image Encryption algorithm based on pixel", ICIS – 2010 IEEE International Conference 29-31 Oct 2010, pp – 769 – 772.

[6] Zhang Yun-peng , Liu Wei " Digital Image Encryption Algorithm Based on chaos and improved DES ", System, man and Cybernatics ,SMC 2009 , IEEE International Conference 11-14 Oct 2009, pp 474-479.

[7] Saeed R. Khosravirad, Taraneh Eghlidos and Sharokh Ghaemmaghami, "Higher Order Statistical of Random LSB Steganography", IEEE Trans. 2009, pp 629 - 632.

[8] N Provos and P. Honeyman, "Hide and seek: An Introduction to Steganography", IEEE Security and Privacy, 2003, pp32-44.

[9] Donovan Artz" Digital Steganography: Hiding Data within Data ", Los Alamos National Laboratory, IEEE Trans. 2001, pp 75-80.

[10] K Suresh Babu , K B Raja, Kiran Kumar k, Manjula Devi T H, Venugopal K R, L M Pathnaik" Authentication of Secrete Information in Image Steganography", IEEE Trans. 13.

[11] Schaefer " A Simplified Data Encryption Standard Algorithm ", Cryptologia, January 1996.

[12] M. Dawson, S. Tavares, "An Expanded Set of S-box Design Criteria Based on Information Theory and its Relation to Differential-like Attacks", Advances in Cryptology – EUROCRYPT 1991, LNCS 547, Springer-Verlag, 1991