Security Improvisation in Image Steganography using DES

Manoj Kumar Ramaiya
Department of Computer Engineering
Suresh Gyanvihar University,
Jaipur, India
manojramaiya@gmail.com

Naveen Hemrajani
Department of Computer Engineering
Suresh Gyanvihar University,
Jaipur, India
naveennh@gyanvihar.org

Anil Kishore Saxena
Department of Comp.Sci. & Engg.
ShriRam College of Engg&Mgmt.,
Gwalior, India
anilkishoresaxena@gmail.com

Abstract— **The incredible evolution of Internet technologies & its applications require high level the security of data over the communication channel. Image steganography is a digital technique for concealing information into a cover image. Least Significant-Bit (LSB) based approach is most popular steganographic technique in spatial domain due to its simplicity and hiding capacity. All of existing methods of steganography focus on the embedding strategy with less consideration to the pre-processing, such as encryption of secrete image. The conventional algorithm does not provide the preprocessing required in image based steganography for better security, as they do not offer flexibility, robustness and high level of security.**

The proposed work presents a unique technique for Image steganography based on the Data Encryption Standard (DES) using the strength of S- Box mapping & Secrete key. The preprocessing of secrete image is carried by embedding function of the steganography algorithm using two unique S-boxes. The preprocessing provide high level of security as extraction is not possible without the knowledge of mapping rules and secrete key of the function. Additionally the proposed scheme is capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption.

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

I. INTRODUCTION

The growing prospects of modem communications 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 data integrity are required to protect against unauthorized access. It leads to an explosive growth in info hiding including copyright protection for digital media. Cryptography, Steganography, Digital Watermarking and fingerprinting all these applications of information hiding are quite diverse.

Cryptographic technique changes the message so that it cannot be understood but this can 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 or not. 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*"[13]. Thus the stegoimage should not diverge much from original cover image. Cryptography and steganography are widely used in the field of data hiding and has 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.

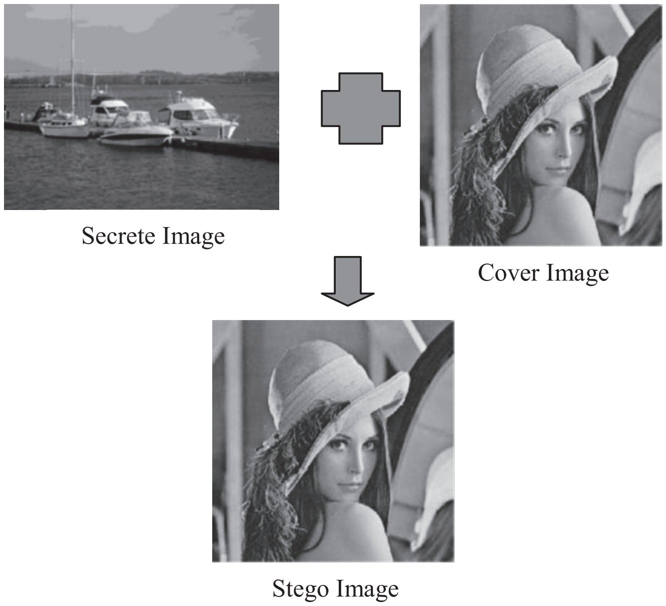


Fig. 1. The Block Diagram of Steganographic system

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

978-1-4673-4529-3/12/$31.00 ©2012 IEEE

embedding technique share the substantial goal of maximizing the capacity of the stego channel [11]. 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, hence known as LSB technique [2,4,8,9]. They are based on two techniques i.e. LSB replacement and LSB matching viz.

A. Peak Signal to Noise Ratio (PSNR) :

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:

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

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

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 representative of the quality of image i.e. the higher the PSNR, lower in the variation between cover image and stego image and vice – versa.

B. Steganographic Triangle :

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 Fig. 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.

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.

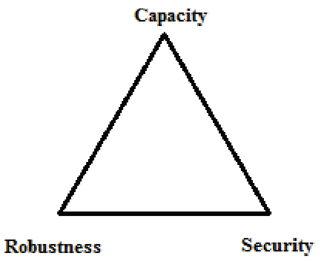


Fig. 2 The steganography Triangle

III. PROPOSED IMAGE STEGANOGRAPHY MODEL

Proposed steganography model is based on SDES function comprising of diffusion, S–Box mapping and secrete key.

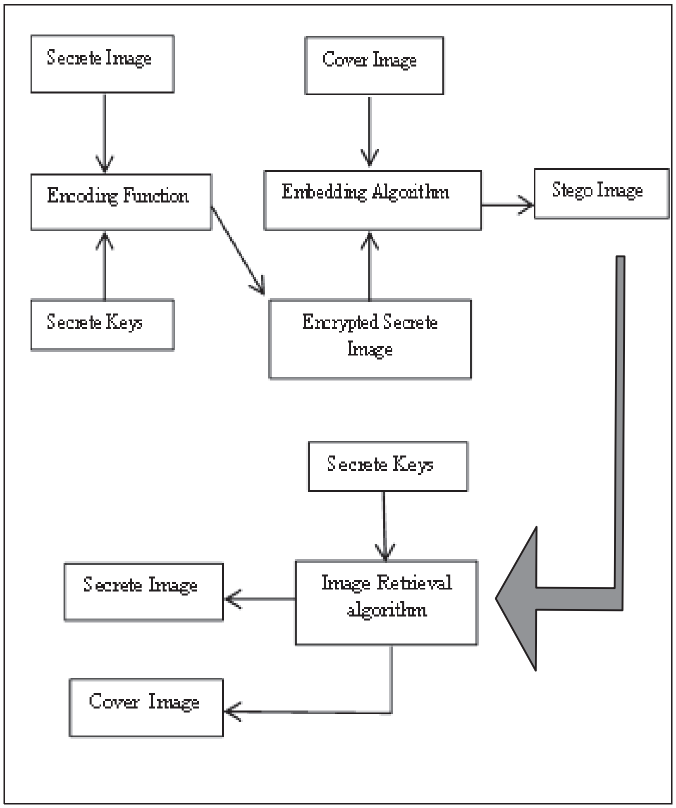


Fig. 3. Proposed Model for Steganography

A. Encoding Function

First the secrete image is selected (e.g. of 64×64). Now the intensity value of first pixel is converted from decimal to binary.

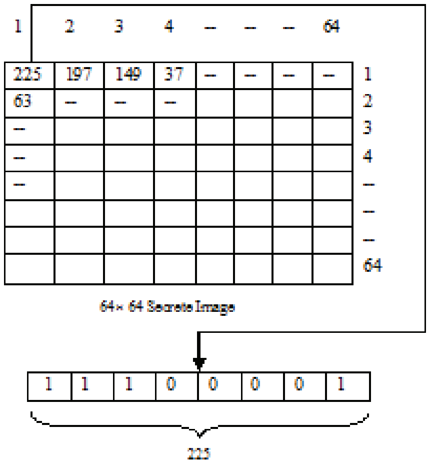


Fig. 4. Proposed Model for Steganography

For example the first pixel value of the Secrete image = 225
Then binary of $(225)_{10} = (1\,1\,1\,0\,0\,0\,0\,1)_2$

Now, input these 8- bit of secrete image to DES encoding function [14] described below.

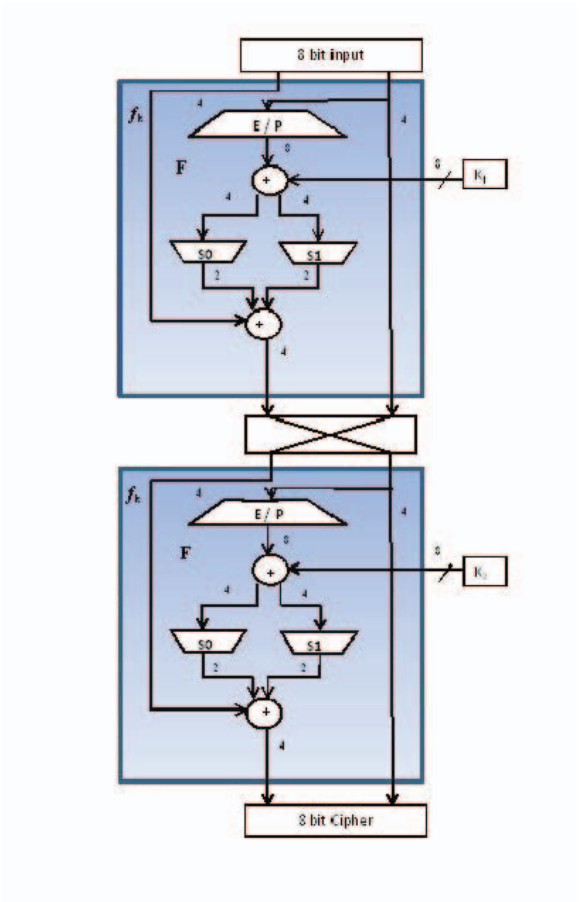


Fig. 5. Encoding Function Detail

1) *The function f_k:* The most complex component of DES is function f_k which consists of a combination of permutation and substitution functions. The function can be (typical)

$$f_k\,(L\,,R) = (\,L \oplus F(R\,,S_K),\,R\ \,)$$

Where L and R are the leftmost 4- bit and rightmost 4- bit of the 8 - bit first pixel value of the first pixel of the secrete image, S_K is the sub keys. The mapping of F is described as follows.The input is a four bit number (n1 n2 n3 n4). The first operation is an expansion / permutation operation defined as:

E / P							
4	1	2	3	2	3	4	1

$$n_4 \quad n_1 \quad n_2 \quad n_3 \quad n_2 \quad n_3 \quad n_4 \quad n_1$$

The 8 – bit sub key $K_1 = (\,K_{11}, K_{12}, K_{13}, K_{14}, K_{15}, K_{16}, K_{17}, K_{18}\,)$ is XOR ing with E/P output

$$n_4 + K_{11} \quad n_1 + K_{11} \quad n_2 + K_{11} \quad n_3 + K_{11}$$

$$n_2 + K_{11} \quad n_3 + K_{11} \quad n_4 + K_{11} \quad n_1 + K_{11}$$

Rename these 8 bits as:

$$\boldsymbol{b}_{0,0} \qquad \boldsymbol{b}_{0,1} \qquad \boldsymbol{b}_{0,2} \qquad \boldsymbol{b}_{0,3}$$

$$\boldsymbol{b}_{1,0} \qquad \boldsymbol{b}_{1,1} \qquad \boldsymbol{b}_{1,2} \qquad \boldsymbol{b}_{1,3}$$

The first 4 bits (first row) are fed into the S-box S0 to produce a 2 bit output and the remaining 4 bits (second row) are fed into S1 to produce another 2 bit output. These boxes are defined as follows:

$$S0 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 0 & 2 \end{array} \qquad S1 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$$

Fig. 6. S-Box Detail

2) *S- box operation :* The first and fourth input bits are treated as a 2- bit number that specify a row of the S-box, and the second and third input bit specify column of S- box.

For example if $(b_{0,0}\ b_{0,3}\,) = (00)$ and $(b_{0,1}\ b_{0,2}) = (10)$, then the output is from 0th Row , 2nd Column of S0, which is 3 , or (11) in binary. Similarly $(b_{1,0}\ b_{1,3}\,) = (00)$ and $(b_{1,1}\ b_{1,2})$ are used to index into S1 to produce additional 2 –bit. The 4 bits produced by S0 and S1 are XORed with leftmost 4 bits of input giving 4- bits output.

3) The Switch function: The function f_k only alters the leftmost 4 bits of the input. The switch function (SW) interchange the leftmost and rightmost 4-bits so that the second instance of f_k operate on different 4 bits. In the second instance the E/P , S0 , S1 functions are the same but the Sub key used is K_2.

Example: 8 Bit input to the Encoding Function:

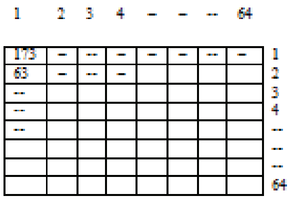
$(225)_{10} = (11100001)_2$, lets K_1= 10100100 & K_2= 01000011.

I / P	=	1 1 1 0 0 0 0 1
L	=	1 1 1 0
R	=	0 0 0 1
E/P	=	1 0 0 0 0 0 1 0
$\oplus$ K_1	=	0 0 1 0 0 1 1 0
S-Box Output	=	0 0 1 0
$\oplus$ L	=	1 1 1 0
SW Input	=	1 1 0 1 0 0 0 1
SW Output	=	0 0 0 1 1 1 0 1

This output of SW input to the second occurrence of function f_k using same S-Box but different key i.e. K_2.

Final O/P	=	1 0 1 0 1 1 0 1
	=	$(173)_{10}$

Hence $(225)_{10}$ of secrete image is converted into $(173)_{10}$ encrypted secrete image.



1	2	3	4	–	–	--	64	
173	–	--	–	–	–	--	–	1
63	–	--	–					2
--								3
--								4
--								--
								--
								--
								64

Fig. 7. Encrypted Secrete Image (64 × 64)

4) Bit Division: Taking the cipher encrypted image, the values are concerted from decimal to binary

The binary value of $(173)_{10} = (10101101)_2$

Next divide this 8 bit value into 4 part taking 2 bits in each

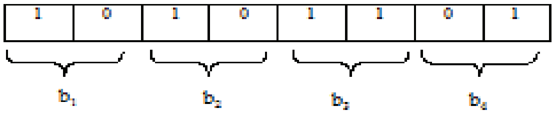
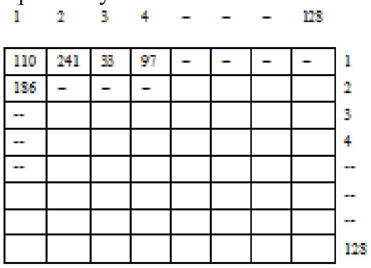


Fig. 8. Bit Division

After bit division we get value of b1 = 10, b2 = 10, b3 = 11, b4 = 01.

5) Insertion of Bit into the cover image : After receiving values of b_1, b_2, b_3, b_4 , these values are inserted into the cover image. These values are placed into the 2 bit LSB of the four consecutive pixels in cover image. Taking the pixels one by one from the cover image, the 2 LSB bits are replaced by 10,10,11,01 respectively.



1	2	3	4	–	–	–	128	
110	241	33	97	–	–	–	–	1
186	–	–	–					2
--								3
--								4
--								--
								--
								--
								128

Fig. 9. Cover Image (128 × 128)

Taking pixels value sequentially.

$(110)_{10}$ = $(0 1 1 0 1 1 1 0)_2$
$(241)_{10}$ = $(1 1 1 1 0 0 0 1)_2$
$(33)_{10}$ = $(0 0 1 0 0 0 0 1)_2$
$(97)_{10}$ = $(0 1 1 0 0 0 0 1)_2$

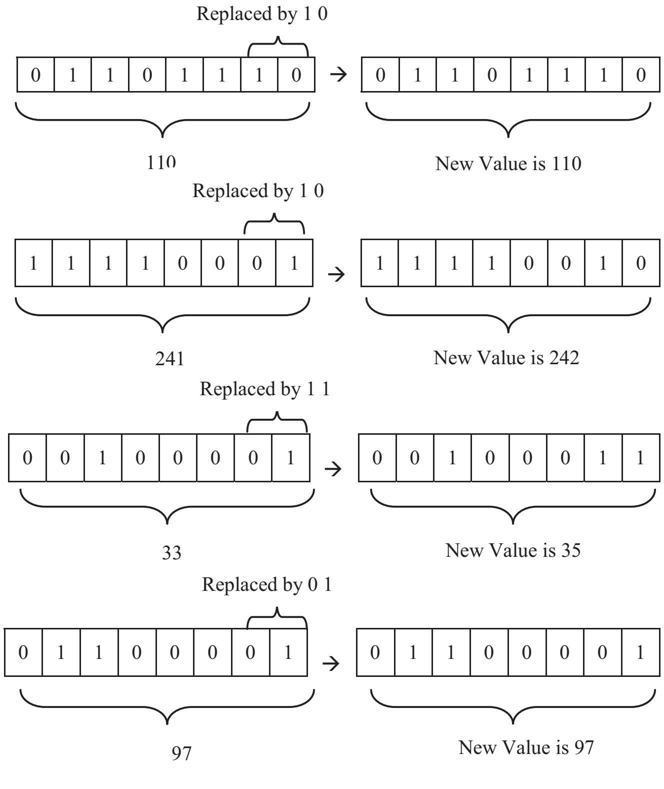


Fig. 10. Insertion of Bit into Cover Image

6) Formation of Stego Image: After receiving the new pixel value the stego image is formed by replaceing these values at their original position. Likewise the pixels value on by one from encrypted secrete image and insertion into the cover image and replaced them. Result becomes the stego image.

1	2	3	4	--	--	--	128	
110	242	35	97	--	--	--	--	1
--	--	--	--					2
--								3
--								4
--								--
								--
								--
								128

Fig. 11. Formation of Stego Image (128 × 128)

- Encoding Algorithm:

Input: A gray level Secrete Image (m × n), A gray Level Cover of size (2m × 2n);
Output: Stego Image of size (2m × 2n);

Steps:

1. Input each pixel value of the secrete image one by one to the image encoding Function (f_k), which produces the encrypted secrete image.
2. Divide the each pixel value of encrypted secrete image into 4 parts containing 2 bits each.
3. Insert these pixel values into the LSB position of first four pixels in the cover image one by one.
4. End.

B. Image Retrival: At the receiving end decoding of stego image perform the following process:

1) Generate the 2 LSB bits from the stego Image:

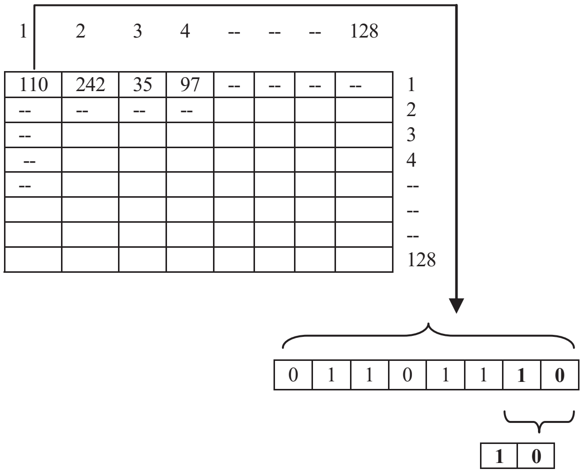


Fig. 12. LSB (2 Bits) Extraction of Stego Image

The pixels are processed one by one from the stego image. Convert it into binary values and take 2 LSB bits from four consecutive pixel values:

Similarly taking next three pixels. i.e. 242, 35, 97;

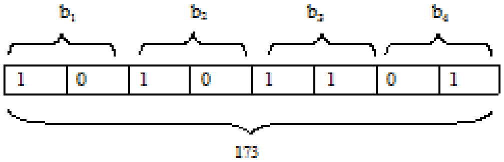
$(242)_{10} = (1\ 1\ 1\ 1\ 0\ 0\ \mathbf{1}\ \mathbf{0})_2$

$(35)_{10} = (0\ 0\ 1\ 0\ 0\ 0\ \mathbf{1}\ \mathbf{1})_2$

$(97)_{10} = (0\ 1\ 1\ 0\ 0\ 0\ \mathbf{0}\ \mathbf{1})_2$ receiving,

$b_1 = \mathbf{1\ 0}$; $b_2 = \mathbf{1\ 0}$; $b_3 = \mathbf{1\ 1}$; $b_4 = \mathbf{0\ 1}$;

2) Concatenation of results: Now concatenating theinput, the 8 bits of first pixel value of encrypted secrete image is obtained as



3) Formation of Encrypted Secrete Image: Now the generated value placed into first position. Likewise taking the next four pixel value from stego image the process is repeated and the whole encrypted secrete image is retrived.

1	2	3	4	--	--	--	64	
173	--	--	--	--	--	--	--	1
63	--	--	--					2
--								3
--								4
--								--
								--
								--
								64

Fig. 13. Encrypted Secrete Image (64× 64)

4) Generation of Secrete image: Now the pixel value from encrypted secrete image are again inputed to DES encoding function with same parameter and keys one by one (but used in reverse order) to obtained first pixel value of original secrete image.

After execution of the decoding function f_k the first pixel value $(\ 173\ )_{10}$ of encrypted image transforms into first pixel value $(\ 225\ )_{10}$ of secrete image and finally, the original image is generated..

- Decoding Algorithm:

Input: Stego Image of size (2m × 2n);
Output: A gray level Secrete Image (m × n) ;

Steps:

1. Input each pixel and take 2 bit LSB from 4 consecutive pixel value of the stego image.

2. Concatenated four 2bit LSB get 8 bits of encrypted secrete image.

3. These 8 bits are input to decoding Function (fk) using same parameter but keys value used in reverse order getting first pixel value of secrete image.

4. End.

IV. RESULTS AND ANALYSIS:

Proposed model is stronger Steganography technique because without knowing the secrete keys, S-box mapping function, the extraction of secrete image from the stego image is impossible. Moreover quality of cover image is also not degrading due to variation in two LSB of each pixel which reflects only 0 – 3 difference pixel value.

Additionally the proposed scheme is capable of not just scrambling data but it 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	64× 64	25 %	54.58
Cameraman	64× 64	25 %	55.01
Lena	64× 64	25 %	59.28
Pirate	64× 64	25 %	51.63
Living room	64× 64	25 %	50.19
Women-darkhair	64× 64	25 %	52.85

V. CONCLUSION

In the proposed DES based steganographic model the strength of S-box mapping and secrete key for encrypting secrete image, improves security and image quality 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 give no 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. The research and analysis motivates that the steganographic capacity and stego image imperceptibility are the most important aspects of image steganographic systems. Essentially, either increasing the steganographic capacity while maintaining the imperceptibility (stego image quality) or enhancing the imperceptibility while maintaining the steganographic capacity represents a significant contribution

ACKNOWLEDGMENT

The principal author acknowledgment is due to Sh.R.S.Sharma, Chairman, ShriRam Group of Colleges (SRGOC) for the encouragement and blessing 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] Jasmin Cosic , Miroslav Bacai, “ Steganography and Steganalysis Does Local web Site contain “Stego” Contain “ , 52 th IEEE Trans. International Symposium ELMAR-2010, Zadar, Croatia 2009 ,pp 85 – 88.

[7] 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.

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

[9] J. Mielikainen, LSB Matching Revisited, IEEE Signal Process. Lett. 13 (5) (2006) 285-287.

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

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

[12] 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.

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

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