Secret Data Transmission using Vital Image Steganography over Transposition Cipher

Mamta Jain
Department of Information Technology
Mody University of Science and Technology
Laxmangarh, Rajasthan, India.
Email- mamta11.jain@gmail.com

Saroj Kumar Lenka
Department of Information Technology
Mody University of Science and Technology
Laxmangarh, Rajasthan, India.
Email- lenka.sarojkumar@gmail.com

Abstract— **The idea behind this paper describes a modality about secret interface over the globalization of the communication over the world. To accomplish this phenomenon, two varieties of security mechanism, cryptography and steganography is being applied. At the former stage, encryption is being provided to secret plain text using Vernam cipher (One–Time Pad) transposition technique, since Vernam cipher show good performance metrics in terms of less CPU running time, file size same after encryption and strong avalanche effect compare with all transposition cipher. And at the later stage, it transform cipher text into bytes and divides each byte into pairs of bits and assigns the decimal values to each pairs, which is known as master variable. master variable value range will be vary between 0 to 3. Depending upon the master patchy value, add that cipher text in the career image at Least Significant Bit (LSB) 6th and 7 th bit location or 7th and 8th bit location or 7th and 6 th or 8th and 7th bit location. Which shows the embedding location dynamicity of the algorithm depends upon dynamically changed master variable value. After completion of embedding and sending the stego image to the receiver side, retrieving process of the cipher text from the said locations will be done. And then decryption process to get the secret plain text back will be performed using the Vernam cipher transposition algorithms. In this we provide robust image steganography. Performance analysis observed using MSE and PSNR value.**

Keywords— *LSB; steganography; cryptography; Vernam cipher; encryption; decryption; embedding*

I. INTRODUCTION

Security of information has become the very tremendous term for information and communication technology now days. Variety of security metrics with better performance is required for the upcoming era of internet world and big data. To accomplish security phenomenon, two techniques are used for betterment of information secrecy, steganography over cryptography. Former is steganography, a method of secret communication in which secret information is embedded into other temporal or non temporal media. The word steganography has a Greek base. It means concealed writing. Numerous evidents have been retrieved from literatures as wax tablets, messenger's body, and writing message on a paper with lemon juice, as cover files. When secret data are obscure in the cover media files, it can be called as stego data. Various kinds of temporal or non temporal multimedia files can be used to obscure the secret data.Later case is cryptography, the secret information is enciphered by a key and an encryption algorithm and sent via the channel. Secret data cannot be stolen by a person or a process or an attack by seeing this without any information about the key. They can only notice that something is under transmission over the channel. But in former steganography case, the person or process or attacks will not even suspect that some secret information is on transmission.

The combination of cryptography and steganography are used for providing the security and increasing the strength to the transmitted secret data over internet communication. The profit of steganography over cryptography is it keeps the existence of the obscure data secret. The proposed method has two varieties of security. Former, the data is encrypted and later, the encrypted data is obscured into the LSB position of cover image. Hiding the data into LSB plane of cover image does not much affect its quality.

II. LITERATURE REVIEW

A huge variety of techniques have been used till now to hide the information within temporal and non temporal media files. Ross J. Anderson and Fabien A.P. Petitcolas suggested that each and every steganographic approach should have some limitations.They proposed an information theoretic approach for perfect secrecy using Shannon’s theory [1]. In the LSB method, cover file’s 8th bit of every byte is replaced by one bit of the secret information [2]. Gandharba Swain and S.K.lenka has been already discussed a double substitution cipher algorithm for encrypting at sender while decrypting at receiver and the embedding process was at LSB minus one as well as LSB positions alternatively [3]. In the other method, a text based image steganography using two square reverse ciphers is proposed. Data bit implanting is done at the 7th bit position of the cover image pixels in some choosed bytes. Tables are divided in such a manner that some alphabet as well as digits and special characters are missing [4]. Author suggested twelve square substitution cipher method, which includes alphabet and digit but some alphabet and some special character are again not included [5]. Amitava Nag et. al proposed an innovative scheme for image steganography by using an affine cipher encryption and LSB substitution technique to provide security measures and imperceptible visual quality [6]. Further Chandreyee Maiti et. al gave some steganography techniques as LSB steganography, steganography using the LSB and second last LSB position bit substitution and image steganography using diagonal pixels by using symmetric as well as public key cryptography to cipher the message [7]. Gandharba Swain and S.K. Lenka has been

978-1-4673-7910-6/15/$31.00 ©2015 IEEE

discussed extended hill cipher (a new block cipher) method, which uses a 128 bit key to encrypt the secret message and then the cipher text of the secret message is embedded into the carrier image in 6th, 7th and 8th bit locations of some of them selected pixels (bytes). The pixel selection depends upon the bit pattern of the cipher text [9]. R.S. Gutte et. al proposed an approach in such way that, data can be encrypted using Extended Substitution Algorithm and then this cipher text is concealed at two or three LSB positions of the carrier image [10]. Rashedul Islam et.al proposed a new steganography technique which was developed to hide huge amount of data in Bitmap image using filtering based algorithm, which uses most significant bit (MSB) for filtering purpose. This method uses the concept of status checking for insertion and retrieval of message [11].

Our proposed approach can be understood by referring the following sections. In section-III the working of Vernam cipher (One –Time Pad) transposition technique is discussed, in section-IV the embedding process, in section-V the proposed algorithm, in section-VI the experimented results and performance analysis, in section-VII the comparisons with existing techniques and in section-VIII the conclusion.

III. VERNAM CIPHER (ONE–TIME PAD) TRANSPOSITION TECHNIQUE

A dynamic collection of non-reoccurring characters as the input cipher text are used in Vernam cipher algorithm. If an input cipher text for transposition is used once, will never used again for any other secret data (so the name is one-time pad). Here Vernam cipher show good performance metrics in terms of less CPU running time, length of the cipher text equals the length of the original plain text and strong avalanche effect compare with all transposition ciphers [10]. The steps for the algorithm have been described here.

A. *Vernam Cipher Algorithm:*

- Treat each and every plain-text alphabet as a number in an rising sequence, i.e. A=0, B=1….Z=25.
- Do the same for each character of the input cipher text also.
- Add each number which corresponds to the plain- text alphabet to the corresponding input one –time pad alphabet number.
- If the sum thus produced is bigger than 26 then, subtract 26 from it.
- Translate each number of the sum back to the corresponding alphabet. It will give the output cipher text.

Let us apply the Vernam cipher algorithm to a plain text message is *HOW ARE YOU* using a one-time pad *NCBTZQARX* to produce a cipher-text message UQXTRUYFR as shown in Figure 1.

Fig. 1. Vernam Cipher Example

		H	O	W	A	R	E	Y	O	U
1.	Plain text	7	14	22	0	17	4	24	14	20
		+								
2.	One-time pad	13	2	1	19	25	16	0	17	23
		N	C	B	T	Z	Q	A	R	X
3.	Initial Total	20	16	23	19	42	20	24	31	43
4.	Subtract 26, If>25	20	16	23	19	16	20	24	5	17
5.	Cipher text	U	Q	X	T	Q	U	Y	F	R

IV. THE EMBEDDING PROCESS

First of all convert the carrier image into number of bytes for embedding. After that, conversion of the confidential cipher information into binary values will be done. The embedding of secret cipher data is to be done in each and every byte. But the position selection, where we have to embed the data in each byte, will be performed based on some pre defined bit pattern criteria. In each bytes either the 6th & 7th or 7th & 8th or 7th & 6th or 8th & 7th bit position are used for embedding. Here we are explaining an example for better understand the procedure.

Example -Assume that the data to be sent is: **11001011 01111010.** Suppose the different bytes of the image are A, B, C, D etc. The first 2 bit 11 will be embedded in 8th & 7th bit position of A, because their decimal value is 3. Then the next 2bit 00 will be embedded in 6th & 7th bit position of B. Then next 2bit 10 is embedded in 7th & 6th bit position of C and so on. That means if the present pair of bits which is to be embedded has decimal value 0,1,2,3 respectively then the embedding will be done in the 6th & 7th, 7th & 8th, 7th & 6th and 8th & 7th bit positions respectively of the current byte. The embedding process is shown in table I.

TABLE I. SELECTION OF BIT LOCATION IN A BYTE USING MASTER VARIABLE

Carrier File Byte	Operation	Location	Master variable Value (n)
Byte A	Embed(11)	8th & 7th	3
Byte B	Embed(00)	6th & 7th	0
Byte C	Embed(10)	7th & 6th	2
Byte D	Embed(11)	8th & 7th	3
Byte E	Embed(01)	7th & 8th	1
Byte F	Embed(11)	8th & 7th	3
Byte G	Embed(10)	7th & 6th	2
Byte H	Embed(10)	7th & 6th	2
So on			

V. THE PROPOSED ALGORITHM

Step1 – In this phase convert the carrier media file into number of bytes.

Step2- In another phase, apply Vernam Cipher transposition technique on secret data to get the cipher text.

Step3- Cipher text is to be converted into binary values.

Step4- Check that length of carrier image must be large enough to obscure the cipher text.

Step5- In this phase embedding will be performed with the discussed embedding process.

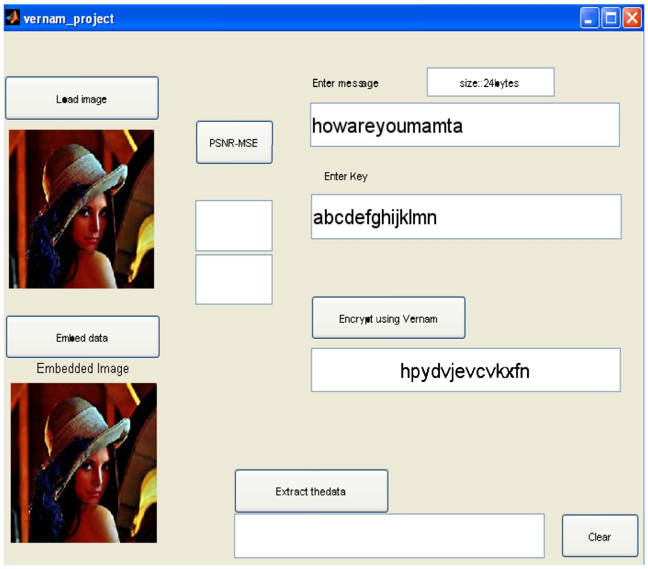
Step6- Transmits the output stego image to the network for recipient.

Step7- Receiver gets the hidden information by applying reverse process as sender performs on secret data.

Now it is clear that in each pixel we are hiding two bits of secret cipher data bits. So one byte of cipher can be accommodated in 4 bytes of image. Hence for n byte cipher text there is a need of carrier image of 4n bytes length. Any good steganographic approach must have the following characteristics: (i) able to obscure a sufficient amount of payload, (ii) able to survive with search attacks, (iii) the quality reduction of the stego image should not be noticeable and at last (iv) able to provide at least two variety of security. Thus the above proposed algorithm show has all these characteristics in well manner.

VI. THE EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

The experimentation of proposed method has been done in MATLAB with the help of Graphical user interface and it provides convenience to the user. These results have been displayed in Figure 2.



Enter message

size::24bytes

howareyoumamta

Enter Key

abcdefghijklmn

hpydvjevcvkxfn

Fig. 2. (a) Screenshots of the screen at sender after ciphering (Vernam cipher) and embedding.

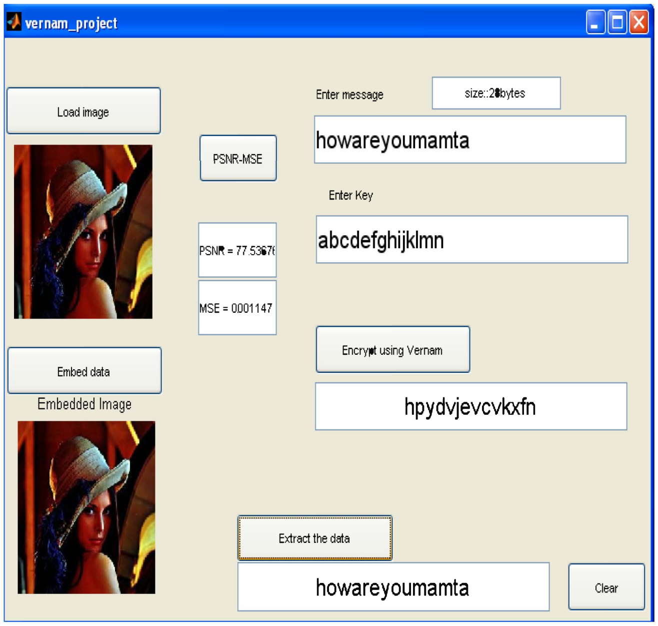
The peak signal-to-noise ratio (PSNR) terminology is a technical phenomenon, which shows the relation between the maximum possible power of a transmitted signal and the power of disturbing noise, which affects the representation of the transmitted signal. PSNR value shows the quality of regeneration of steganography images. The signal is the original image, and the noise or disturbance is the error introduced by some steganography algorithm. The PSNR at various amount of cipher for same image is shown in table 2, which is measured in decibels (dB). PSNR values declining below 30 dB indicate a quite low quality i.e. deformation caused by embedding as well as 40 dB and above shows the high quality stego image [8].

PSNR outcome is defined by the mean square error (MSE) for two P×Q monochrome images, x as well as y show image coordinates, SGxy (stego image) and CVxy (cover image), one of the images is approved a noisy surmise of the other is defined:

$$\text{M.S.E} = \frac{1}{PQ} \sum_{x=1}^{P} \sum_{y=1}^{Q} \left(SG_{xy} - CV_{xy} \right) \qquad (1)$$

$$\text{PSNR} = 10 \log 10 \left\{ \frac{CVmax^{2}}{\text{M.S.E}} \right\} \qquad (2)$$

Where CVmax = the maximum 255 pixel value, for 8-bit cover images [8].



Enter message

size::28bytes

howareyoumamta

Enter Key

abcdefghijklmn

PSNR = 77.5367

MSE = 0.001147

hpydvjevcvkxfn

howareyoumamta

Fig. 2. (b) Screenshots of the screen at receiver after retrieving secret data and PSNR & MSE Value

TABLE II. OBSERVED MSE & PSNR VALUE FOR DIFFERENT SIZE PAYLOADS

Image	Cover Image size(in kilo bytes)	Amount of Secret cipher embedded(in bytes)	MSE (Mean Square Error)	PSNR (in decibles)
Leena	10.8	128	0.0052	70.97
Leena	10.8	64	0.0029	73.49
Leena	10.8	32	0.0014	76.76
Leena	10.8	16	0.0006	80.10
Leena	10.8	8	0.0004	81.59

VII. COMPARATIVE STUDY

In this article dynamic method for embedding of the secret cipher information is performed in 6th and 7th or 7th and 8 th or 7th and 6th or 8th and 7th bit locations, which is fully based on the dynamic changed value of the master patchy variable. This algorithm shows multi-transpose ability, so it is less susceptible to frequency analysis and known plain text attacks. We have implemented this algorithm for alphabets, but one can include any kind of symbols with their corresponding integer number, so that it can provides more payloads. If this algorithm is compared to LSB and injection methods, it is better in terms of intrusion prevention. In this new method the embedding locations dynamicity is proposed, which shows robust mechanism for variable bit positions depending on secret message.

TABLE III. COMPARISON WITH OTHER SCHEMES PROPOSED BY OTHER RESEARCHERS

Scheme	Observed PSNR in (dB)	MSE	Imperceptibility /Quality
Gandharba Swain, Saroj Kumar Lenka [5]	74.41	0.0025	Good
Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh [7]	30.48	0.0012	Not Good
Gandharba Swain, Saroj Kumar Lenka [9]	74.91	0.0024	Good
R.S. Gutte,Y.D. Chincholkar and P.U. Lahane [10]	73.40	0.0030	Good
Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain [11]	74.39	0.0024	Good
Our Proposed Method	81.59	0.0004	Better

The comparison of existing techniques results proposed by other researchers and our proposed results on the basis of PSNR and MSE values is shown in table III.

VIII. CONCLUSION

This proposed work uses a very efficient Vernam cipher transposition technique, which uses a one-time pad, and discarded after a single use, and this technique of encryption shows good performance metrics in terms of less CPU running time, file size same after encryption and strong avalanche effect compare with all transposition cipher therefore, is more suitable for short secret messages communication. It can be applicable for keeping password secure in online banking system. This article shows bi level security in terms of steganography over cryptography. The degradation in image quality cannot be noticeable easily. The PSNR value is better & MSE value is very less as compared to many of the existing algorithms. From Comparison Analysis in table 3, it is concluded that the proposed approach is better than already existing techniques. It provides better imperceptibility/quality. This algorithm is also a stronger and robust as well as secures one compared to other algorithms. No visual defects can be observed from the corresponding stego images. It can also be referred to devise new algorithms how to send different language secret text or image in audio as well as video files with more dynamicity.

REFERENCES

[1] R. J. Anderson and F. A.P. Petitcolas, "On The Limits of steganography", IEEE Journal of selected Areas in communication, 16(4), pp. 474-481,Special Issue on Copyright & Privacy protection. ISSN 0733-8716, May 1998.

[2] M. A. B. Younes and A. Jantan, "A New Steganography Approach for Image Encryption Exchange by using the LSB insertion", IJCSNS International Journal of Computer Science & Network Security, Vol 8, No 6 , pp. 247-254, June 2008.

[3] G. Swain and S..K..Lenka, "Steganography-Using a Double Substitution Cipher", International Journal of Wireless Communications and Networking, Volume 2, Number 1, pp.35-39. ISSN: 0975-7163, June 2010.

[4] G. Swain and S. K. Lenka, " A Technique for Secure Communication using Message Dependent Steganography",Special issue of IJCCT, Vol. 2,No. 12,2010.

[5] G. Swain and S. K. Lenka, "Steganography using the Twelve Square Substitution Cipher and Index Variable" ,IEEE transactions on Image Processing, pp. 84-88, 2011.

[6] A. Nag, J. P. Singh, S. Khan and S. Ghosh," A Weighted Location Based LSB Image Steganography Technique", Springer ACC 2011, Part II, CCIS 191, pp. 620–627, 2011.

[7] C. Maiti, D. Baksi, I. Zamider, P. Gorai and D. R. Kisku," Data Hiding in Images Using Some Efficient Steganography Techniques",Springer SIP 2011, CCIS 260, pp. 195–203, 2011.

[8] B. Li,.,et al. "A survey on image steganography and steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, pp. 142-172, 2011.

[9]G. Swain and S..K..Lenka, "A Dynamic Approach to Image Steganography Using the Three Least Significant Bits and Extended Hill Cipher" Advanced Materials Research, vol.403-408, pp.842-849,2012.

[10] S. Padmapriya, S. Saravanapriya and D. Jayachitra," Performance Analysis of Various Encryption Algorithms for Data Communication", International Journal of Computer Science And Technology,vol. 3,No 3,pp.1202-1204,2012.

[11]R.S. Gutte, Y..D. Chincholkar and P..U. Lahane." Steganography for two and three lsbs using extended substitution algorithm", ICTACT Journal on communication technology, vol. 4, pp. 685-690, issue 01, 2013.

[12]Md. R. Islam, A. Siddiqa, Md. P. Uddin, A. K. Mandal and Md. D. Hossain," An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", IEEE Conference on Informatics, Electronics & Vision, 2014.