LSB Steganography based on Variable Key Encryption

Menka Goswami
Dept. of CSE, NIT Hamirpur,
Hamirpur, HP,
INDIA

Vishal Gupta
Dept. of CSE, BTKIT,
Dawarhat, Uttarkhand,
INDIA

Anil Kumar
Dept. of CSE, UTU,
Dehradun, Uttarakhand,
INDIA

ABSTRACT
In this paper we have explored a new dimension in image steganography and propose a deft method for image – secret data – keyword (steg key) based sampling, encryption and embedding the former with a variable bit retrieval function. The keen association of the image, secret data and steg key, varied with a pixel dependent embedding results in a highly secure, reliable L.S.B. substitution. Meticulous statistical analysis has been provided to emphasize the strong immunity of the algorithm to the various steganalysis methods in the later sections of the paper.

Keywords
Encryption, L.S.B., Secret data.

1. INTRODUCTION
The sole role of steganography is to conceal the fact that any communication is taking place. Secret messages are embedded in cover objects to form stego objects. These stego objects are transmitted through the insecure channel. Cover objects may take the form of any irrelevant / redundant digital image, audio, video and other computer files.

In secure transmission of the stego objects without suspicious lies the success of steganography[7]. Staganalysis methods aim at estimating retrieval of potentially hidden information with little or no knowledge about the steganographic algorithm or its parameters.

An extensive study of the related papers [2],[3],[5],[6],[7],[8] has given shape to this concept. We have meticulously analyzed the possibilities in the sphere of maximizing randomization, minimizing deviations and structuring strong coherence among the working sets. This paper is aimed at further increasing the equalization and reliability of the substitution based steganography from its referrals.

2. PROPOSED ANALYTICAL MODEL FOR ENERGY DETECTOR
In our method we have mainly four components as sampling, encryption , embedding and decryption. Sampling plays a key role here in our procedure, it involves the homogeneous selection of pixels for encryption which strengthen the steganography procedure. Encryption is the procedure where implementing algorithms, we apply our tricks to match all steganographic characteristics. Then we embed the message in the sampled pixels with strong and efficient algorithm, subsequently use the decryption method to retrieve the image in the receiver end.

2.1 Sampling
Sampling is intricately associated with successful steganography and plays a central role in the process. In this paper, we have explored a highly secure and weight balanced algorithm to obtain variable samples spread equally throughout the cover image.

This papers explores a highly secure method of image steganography. The samples are selected based on the input cover object, secret massage and the steg key. Further, a striking feature of the sampling function is that the sample count decreases exponentially as we move inwards from the periphery to the Centre of the picture. This is based on the idea that the centre of the picture is usually more meticulously noticed and focused on by the human eye, and peripheral parts generally attract lesser meticulous keen notice. The sampling is strengthened keeping in mind the visible changes in the histogram, thereby repulsing steganalysis deftly. Further, the function ensures that approximately equal number of pixel samples have been selected from all four quadrants, to prevent clustering of samples from a single one.

2.2 Encryption
All tables and figures will be processed as images. You need to embed the images in the paper itself. Please don't send the images as separate files.

We encrypt the secret message using a 2 – level encryption function. The first level of encryption is based on the secret message and steg-key and the second level encryption parameters consist of the intermediate message and the secret message. We perform a steg- key based cyclic modification of the secret message followed by inter operable second level encryption.

In the first level :

Let P be the Steg key array and Pi be the ith position of the input steg key.

Cycle- pass (P) cyclically generates the P elements until n(P) = n(0)

N = number of elements / characters
Then, we do a corresponding character increment / decrement as :
If i factor of n(E),
then ;
$e_i = o_i$ - dec – 3 lsb (cycle – pass (p_i))
else;
$e_i = o_i$ + dec – 3 lsb (cycle – pass (p_i))

Now, we get an encrypted message e with the same number of elements as original message o.

This first level encrypted message and the secret message are the parameters of the second – level encryption function.

This first level encrypted message and the secret message are the parameters of the second – level encryption function.

$E_0 = e_0$

$E_i = e_i + e_i\text{-}1$

Consequently, we get a second – level encrypted message E, which is all set to be sent through the insecure channel.

2.3 Embedding

In LSB based steganography [1], [2], the embedding of the encrypted message E in the selected sample pixel set S is done in a color-component varied bit encryption method.

Step 1: Function RGB-image (RGB value) returns the maximum intensity color component, taking the pixel RGB value as parameter.

We extract from the selected pixel as follows :

R -> red component value in the range of 0 - 255

G -> green component value in the range of 0 - 255

B -> blue component value in the range of 0 – 255

Step 2: Convert the values to hexadecimal. Thus we get a MSB. and a LSB. value in the range of 0 – e.

Step 3: Convert the LSB hex value to decimal

Step 4: Convert the decimal value to ASCII

Step 5: The function max Intensify (R, G, B) is celled, which returns the color component of maximum intensity.

Step 6: The last 3 bits are encrypted from the maximum intensity color component and the last 2 bits are essential for the other 2 component. Thus we get 7 bits as either.

Step 7: The encrypted input Ei is converted into its ASCII as follows: And is mapped on to the selected pixel Si.

1	2	3	4	5	6	7
r1	r2	r3	b1	b2	g1	g2
r1	r2	b1	b2	b3	g1	g2
r1	r2	b1	b2	g1	g2	g3

Fig. 1. Embedding format for 7 bits.

e1	e2	e3	e4	e5	e6	e7

Fig. 2. . Encrypted ASCII bits.

Fig. 3. Cover Image

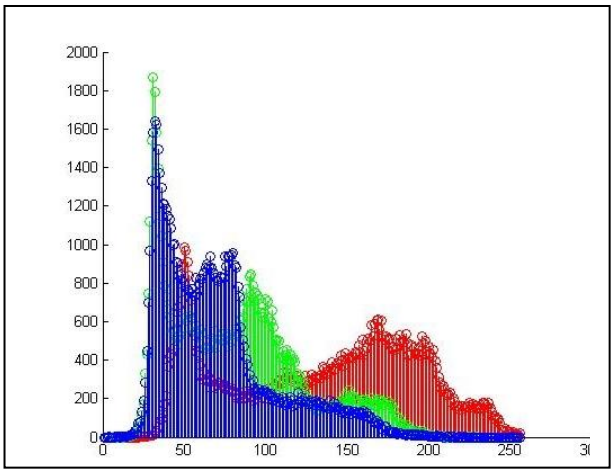

Fig. 4. Histogram of original image

Step 8: The modified R,G,B LSB values are connected back to its decimal values, which are in turn converted into the R, G, B LSB modified hexadecimal values.

Step 9: The combined R,G,B MSB and LSB values are merged together and converted to decimal values ranging from 0 – 255

Step 10: The R, G, B values are merged into 1 single RGB value and the value is set as that modified RGB value in the selected pixel Si.

Fig. 5. Stego image

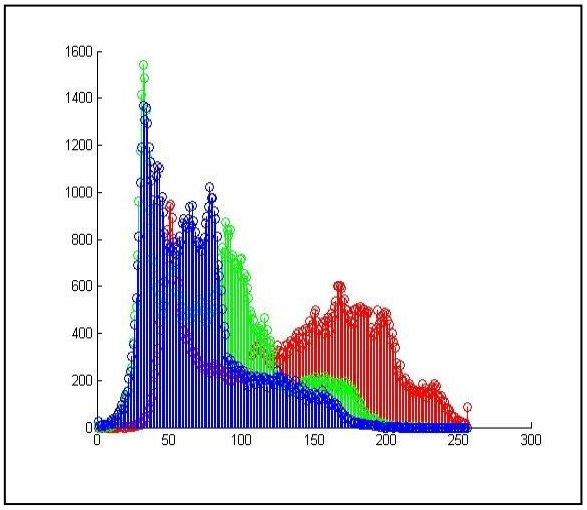

Fig. 6. Histogram of stego image

2.4 Decoding And Decreption

The initial phase consists of retrieving the necessary information required for decoding from the corner pixels. In the first step we need to retrieve two important parameters from the encrypted image as secret message size and order of the stego images(incase of Split and Send Algorithm(SSA)).
Then we intend decoding the original message from the stego image and concatenate them in order to obtain the secret message. We first, apply the sampling algorithms to obtain the samples used for encoding. Then we proceed as below:
Step 1: From the samples obtained, we get the values of the second level encrypted message E. We evaluate the message as:
$e_0 = E_0$
$e_i = E_i$ XNOR e_{i-1}, Where E is the second level encrypted message and e is the first level encrypted message.

Step 2: Then we decrypt the message e as ,Loop from O to the size of the message
e ⟶ O to n(e). if I is a factor of n(e) then,
$O_i = e_i$ + dec – 3 lsb (cycle – pass (p_i))
else
$O_i = e_i$ - dec – 3 lsb (cycle – pass (p_i))

Thus we get the original secret message O, with the same number of elements as the encrypted message e.

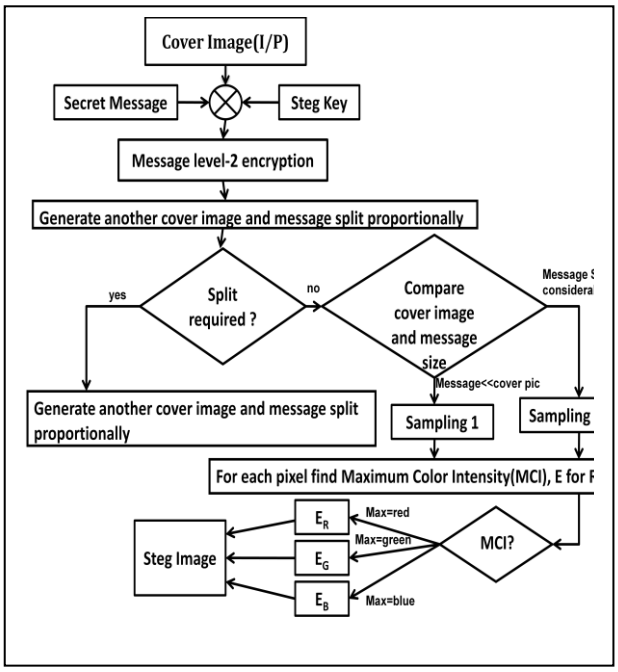

Fig. 7. Flowchart of Encryption, Sampling and Embedding

2.5 SPLIT AND SEND

To remove the constraint of a fixed size secret message, we intent to put forward an automatic adjustment algorithm. This segment is mainly concerned with ensuring that input secret message size to be embedded bears a fairly reasonable ratio to the cover image size for which the distortion is negligible. The dynamic ratio value is defined depending on the dynamics of the image and the concentration of the color component values across the cross sections of the image. Based on the above concept , our algorithm warn against suspicion and suggests the use of another cover image or the copy of the same cover image, which can be generated automatically. On agreement we split the secret data in the best-proportion and the re-sample it. This process of splitting and re-sampling is a recursive process and terminates once an optimally permitted ratio is reached. We store the necessary values required for decoding in the four corners of a picture.

3. RESULTS AND ANALYSIS

We deployed the statistical studies further clarify the proximity and negligible distortions produced in the stego image in the process of execution of the above proposed algorithms. From the table underneath it is noted that the statistical parameters like the MEAN, STANDARD DEVIATION and VARIANCE change only in their distant decimals thus proving its strong resistance to steganalysis.

Image / Statistical parameters	Original Image	Stego Image
MEAN	71.3067	71.3057
VARIANCE	4.3272e+003	4.3272e+003
STANDARD DEVIATION	65.7814	65.7818

Fig. 8. Mean, Variance, Standard deviation

CC / Image	Horizontal	Vertical	Left Diagonal	Right Diagonal
Original Image	0.0715	0.0456	0.0894	0.08864
Encrypted Image	0.0717	0.0452	0.0895	0.08862

Fig. 9. Co-relational Co-efficient

4. CONCLUSION

We conclude widening the window of image steganography through intensive improvisations done in almost all the processes of the evaluation.

This paper widens the spectrum of diffusion and randomization in substitution based steganography. We have aimed at strong coherence and security of data underlying strong randomization and encryption. We propose to step into a yet another new horizon by migrating to frequency domain for restructuring discrete randomization to continuous spectrum in our later endeavors.

Further, sharp transitions among adjacent pixels have been avoided. Analysis of Co-relational Co-efficient(CC) among the adjacent pixels show that there is a mass diffusion of statistical parameters in the stego image as compared to the original image. The diffusion is uniform throughout the encrypted image. The correlation decrease further with increase in the size of the secret message, although slightly and thus potent itself against various statistical attacks.

5. REFERENCES

[1] A. D. Ker, “Steganalysis of LSB matching in grayscale images”, IEEE Signal processing letters, vol. 12, no. 6, pp. 441-444, 2005.

[2] C.-K. Chan, L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognition Vol. 37,Issue 3, pp. 469-474, 2004.

[3] Stefan Hetzl1 and Petra Mutzel2, “A Graph–Theoretic Approach to Steganography” J. Dittmann, S. Katzenbeisser, and A. Uhl (Eds.): CMS 2005, LNCS 3677, pp. 119–128, 2005(IFIP International Federation for Information Processing 2005).

[4] Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, “ Steganography and Digital Watermarking," School of Computer Science, The University of Birmingham.

[5] C. Cachin, “An information-theoretic model for steganography,” Information and Computation vol. 192, pp. 41–56, July 2004. (Preliminary version appeared in Proc. 2ndWorkshop on Information Hiding, Lecture Notes in Computer Science, vol. 1525, Springer, 1998.).

[6] B. Pfitzmann, “Information hiding terminology,” in Information Hiding, First International Workshop (R. Anderson, ed.), vol. 1174 of Lecture Notes in Computer Science, pp. 347–350, Springer,1996.

[7] Rajarathnam Chandramouli, Mehdi Kharrazi, and Nasir Memon, “Image Steganography and Steganalysis: Concepts and Practice” T. Kalker et al. (Eds.): IWDW 2003, LNCS 2939, pp. 35–49, 2004.(Springer-Verlag Berlin Heidelberg 2004).

[8] R. Chandramouli and N. Memon, “Analysis of lsb image steganography techniques,”IEEE Intnl. Conf. on Image Processing, vol. 3, pp. 1019–1022, 2001.