A Data Embedding Technique for Gray scale Image Using Genetic Algorithm (*DEGGA*)

J. K. Mandal
Dept. of Computer Science and Engineering,
University of Kalyani
Kalyani, Nadia-741235, West Bengal, India
e-mail:- jkm.cse@gmail.com.

A. Khamrui
Dept. of Computer Science and Engineering
Future Institute of Engineering & Management, Kolkata
Sonarpur Station Road, Sonarpur, Kolkata-150, West Bengal
e-mail: amritakhamrui@rediffmail.com

***Abstract*—In this paper an authentication/data hiding technique through steganographic approach termed as DEGGA has been proposed using Genetic Algorithm. Large volume of message/ image is embedded in spatial domain using 3 x 3 masks from the source image in row major order. Four bits of the authenticating image is embedded per byte of the source image onto the rightmost 4 bit of each pixel. Mutation is applied on the embedded image. A method of bit handling is applied to keep the fidelity high. In the process of embedding dimension of the authenticating image followed by the content of the message/authenticating image. Reverse process is followed during decoding. Genetic algorithm is used to enhance a security level. Various statistical parameters computed are compared with the existing genetic algorithm based steganographic algorithm Ran- Zan et al. [1] which shows that proposed DEGGA obtained better results in terms of PSNR.**

Keywords- Data Embedding Technique for Grayscale Image using Genetic Algorithm (DEGGA), Genetic Algorithm (GA), peak signal to noise ratio (PSNR).

I. INTRODUCTION

Steganography is the art and science of hiding information into picture or other media in such a way that no-one apart from the sender and intended recipient even realizes there is a hidden information[1,2,3,4,10]. Steganography includes the concealment of digital information within computer files. Generally, a steganographic message will appear to be something else, may be picture, video, sound file, even the radio communication. This apparent message is the covertext. For instance, a message may be hidden by using invisible ink between the visible lines of innocuous documents. The hidden information is called stego message which may be open message, but may be encrypted one as well. Security is a big concern in modern day image trafficking across the network. Security can be achieved by hiding data within the image. Data hiding [9]) in the image has become an important technique for image authentication. Ownership verification and authentication is the major task for military people, research institute and scientist. Information security and image authentication has become very important to protect digital image document from unauthorized access [11]. Data hiding refers to the nearly invisible [6] embedding of information within a host data set as message, image, and video. In steganographic [7], [8] applications, the hidden data may be secrete message or secrete hologram or secrete video whose mere presence within the host data set should be undetectable; a classic example is that of a prisoner communicating with the outside world under the supervision of a prison warden. The data hiding represents a useful alternative to the construction of a hypermedia document or image, which is very less convenient to manipulate. The goal of steganography is to hide the message/image in the source image by some key techniques and cryptography is a process to hide the message content. To hide a message inside an image without changing its visible properties [5] the source image may be altered. The most common methods to make these alteration involves the usage of the least-significant bit (LSB) developed by [7] masking, filtering and transformations on the source image. [8] construct an algorithm for detecting LSB Steganography. This paper presents an algorithm that would facilitate secure message transmission using block based data hiding procedure. Most of the works [2],[3],[4],[12] use minimum bits of the authenticating image for embedding, but the proposed algorithm embed large amount of authenticating image/ message with a bare minimum distortion of visual property.

II. THE TECHNIQUE

In DEGGA insertion is made by choosing image mask in row major order. The dimension of the authenticating image is extracted first. A 3x3 mask is chosen from the host image. The dimension of the authenticating image along with the authenticating image is embedded into the host image. Genetic Algorithm is applied onto the embedded image to enhance a layer of security. Mutation procedure is applied on the embedded image onto the rightmost k bits by consecutive bitwise XOR operation on k steps and taking the MSB of the intermediate stream generated in each step. Schematic diagram of the technique is shown fig1.

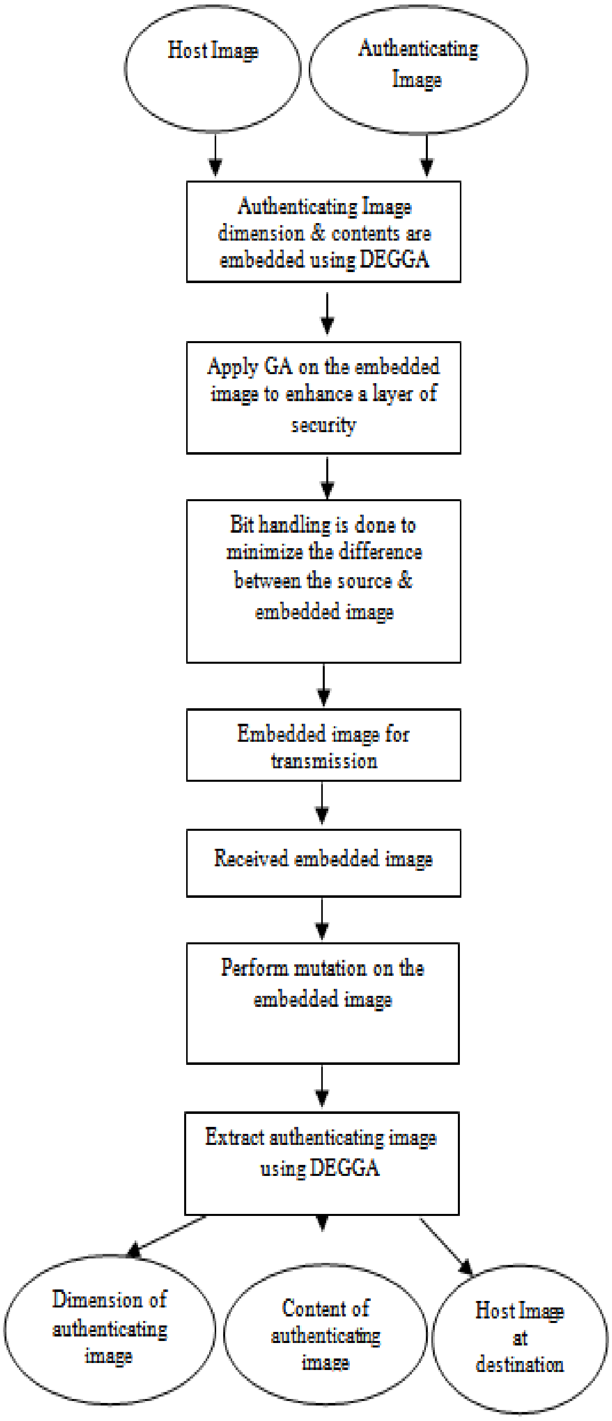

Host Image
Authenticating Image
Authenticating Image dimension & contents are embedded using DEGGA
Apply GA on the embedded image to enhance a layer of security
Bit handling is done to minimize the difference between the source & embedded image
Embedded image for transmission
Received embedded image
Perform mutation on the embedded image
Extract authenticating image using DEGGA
Dimension of authenticating image
Content of authenticating image
Host Image at destination

Fig 1: Schematic diagram of DEGGA

Algorithm of insertion and extraction is given in section A and B respectively. A complete example is given in section C.

A. *Algorithm for insertion*

This scheme use gray scale image for secure message transmission. An authenticating image of size m x n is chosen. The size of the host image is p x q.

Input: Host image of size pxq, authenticating image of size pxq.
Output : Embedded image of size pxq.
Method: Insertion of authenticating image bitwise into the source image.
Algorithm:

Step1: Obtain the size of the authenticating image m x n.

Step2: For each authenticating message/image, Read source image block of size 3x3 in row major order. Extract authenticating message/image bit one by one. Replace the authenticating message/image bit in the rightmost 4 bits within the block, four bits in each byte.

Step3: Read one character/ pixel of the authenticating message/ image at a time.

Step4: Repeat step 2 and 3 for the whole authenticating message/ image size, content.

Step 5: Perform mutation operation for the whole embedded image. For mutation rightmost 3 bits from each bytes is taken. A consecutive bitwise XOR is performed on it for the 3 steps. It will form a triangular form and first bit from each step is taken.

Step 6: A bit handling method is performed on the embedded image. If the difference between the host and embedded image is ± 16 then 16 will be added to the embedded image to keep intact the visibility of the embedded image.

Step 7: Stop

B. *Algorithm for extraction*

The authenticating image is received in spatial domain. The embedded image is taken as the input and the authenticating message/ image size, content are extracted from it.

Input: Embedded image of size pxq,
Output: Host image of size pxq, authenticating image of size pxq.
Method: Extract bits of authenticating image from embedded image

Step 1: Perform reverse mutation procedure by consecutive bitwise XOR operation on the rightmost 3 bits of each byte in three steps. The first bit of each step is taken as the output.

Step 2: Read the image block of size 3x3 in row major order.

Step 3: For each block, extract the authenticating image from the rightmost 4 bits of each byte replace authenticating message/ image bit position in the block by '1'. For each 8 (eight) bits extraction construct one character/ one image pixel.

Step 4: Repeat step 2 and 3 to complete decoding as per size of the authenticating image.

Step 5: Stop

C. *Example*

Consider the image jet (figure 2a) to be inserted into each mask of the image Lena (figure 2b). Four bits of the Airplane image is inserted into each byte of the Lena image. Insertion is done in the rightmost four bits of the byte of Lena. Resultant image after embedding is shown in figure 2c. Bold bits are message bits in the resultant image. Applying mutation on 3 rightmost bits figure is shown in 2d.

11111111 11101011 11001100 10110011 10001110
10011111 11111111 10110011 11001100

Figure 2a: Bytes of Airplane image

00111110 11001100 10011100 11011011 01100111 10101010
11111111 11101011 11001100 10110011 10001110 10011111
01010101 10101111 11111111 11000011 10001000 00110011

Source image block 1 Source image block 2 Figure

Figure 2b: Source image Lena

0011**1111** 1100**1111** 1001**1110** 1101**1110** 0110**1001** 1010**1111**
1111**1011** 1110**1100** 1100**1100** 1011**1111** 1000**1111** 1001**1011**
0101**1011** 1010**0011** 1111**1000** 1100**0011** 1000**1100** 0011**1100**

Stego image block 1 Stego image block 2

Figure 2c: Stego lena

0011**1100** 1100**1100** 1001**1101** 1101**1101** 0110**1001** 1010**1100**
1111**1011** 1110**1111** 1100**1111** 1011**1100** 1000**1100** 1001**1011**
0101**1011** 1010**0011** 1111**1000** 1100**0011** 1000**1111** 0011**1111**

Stego image block 1 Stego image block 2

Figure 2d: Mutated Stego Lena

III. Results, comparison and analysis

A study has been made on various images using DEGGA technique. This section represents the results and discussion and a comparative study between DEGGA and existing approach Ran- Zan et al.[1] in terms of visual interpretation and peak signal to noise ratio. Figure 3a shows the host image lena and baboon. Figure 3b shows the embedding images jet, scene, tiff. Figure 3c shows the result of embedding. Table I show the PSNR value for each embedding image against the source image. From the table it is seen that the maximum value of the PSNR is 34.832 and that of minimum value of the PSNR is 34.806. In comparison with Ran-Zan et al [1] method it is seen that the maximum value of the PSNR as obtained is 32.9 but the DEGGA approach the PSNR is 34.826 which is much more than existing one. It is also seen for the table II that in each case the DEGGA obtain better results than RAN- ZAN et al [1].

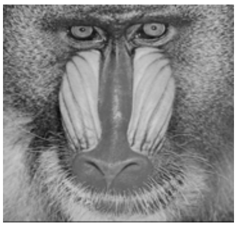
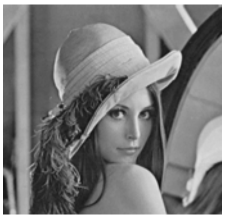
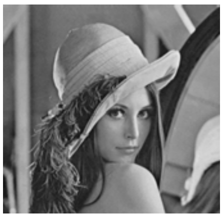
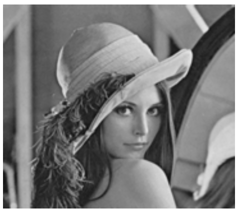
	
3.a.i. Host lena (512x512)	3.a.ii Host baboon (512x512)
3.b.i. Authenticating jet (512x256)	3.b.ii. Authenticating scene (512x256)
	
3.b.iii. Authenticating tiff 512x256	3.c.i.Embedded using jet
	
3.c.ii. Embedded using Scene	3.c.iii. Embedded using tiff

TABLE I. PSNR, MSE, IF OF VARIOUS IMAGES IN FIG 3A VS 3C

Host Image	**Embedding Image**	**PSNR**	**MSE**	**IF**
Baboon	Jet	34.826	21.40	0.998
Baboon	Scene	34.804	21.511	0.998
Baboon	Tiff	34.830	21.38	0.998
Lena	Jet	34.826	21.399	0.999
Lena	Scene	34.803	21.513	0.998
Lena	Tiff	34.821	21.425	0.999

TABLE II. COMPARISON OF PSNR VALUES

Host Image	**Embedding Image**	**PSNR of Ran et al[1]**	**PSNR of DEGGA**
Lena	Jet	32.71	34.826
Lena	Scene	32.55	34.803
Lena	Tiff	32.9	34.821

IV. CONCLUSION

In this paper a novel embedding approach based on genetic algorithm has been proposed through which large amount of information can be embedded. This paper shows that the proposed technique obtained better PSNR ratio than the existing approach RAN- ZAN et al[1] as a result more data can be embedded with better quality.

ACKNOWLEDGMENT

The authors express deep sense of gratitude to the IIPC Project of AICTE, of the department of CSE, University of Kalyani, India where the computational works have been carried out.

REFERENCES

[1] Ran-Zan Wang, Chi- Fang Lib, and Ja- Chen Lin, “Image hiding by optimal LSB substitution and Genetic algorithm,” 2001 Pattern Recognition Society. Published by Elsevier Science Ltd.

[2] Ghoshal N., Mandal, J. K. “A Bit Level Image Authentication /Secrete Message Transmission Technique (BLIA/SMTT)”,Association for the Advancement of Modelling & SimulationTechnique in Enterprises (AMSE), AMSE journal of SignalProcessing and Pattern Recognition, Vol. 51, No. 4, pp. 1-13,France, 2008.

[3] Ghoshal N., Mandal, J. K. et al., “Masking based Data Hiding and Image Authentication Technique (MDHIAT)”, proceedings of 16th International Conference of IEEE on Advanced Computing and Communications ADCOM-2008, ISBN: 978-1-4244-2962-2, December 14-17th, Anna University.

[4] Ghoshal N., Mandal, J. K. et al., “Image Authentication by Hiding Large Volume of Data and Secure Message Transmission Technique using Mask (IAHLVDSMTTM)”, Proceedings of IEEE international Advanced Computing Conference IACC’09, ISBN:978-981-08-2465-5, March 6-7th, Thapar University, Patiala, India.

[5] Nameer N. EL-Emam, “Hiding a large Amount of data with High Security Using Steganography Algorithm,” Journal of Computer Science ISSN 1549-3636, vol. 3, no. 4, pp. 223-232, 2007.

[6] C.Y. Lin and S. F. Chang, “A robust image authentication method surviving JPEG lossy compression,” Proc. SPIE, vol. 3312, San Jose, pp. 296-307, Jan. 1998.

[7] R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques,” Proc. of ICIP, Thissaloniki, pp. 1019-1022, Greece, 2001.

[8] S. Dumitrescu, W. Xiaolin and Z. Wang, “Detection of LSB steganography via sample pair analysis,” IEEE Trans. on Signal processing, Vol. 51, no. 7, pp. 1995-2007, 2003

[9] P. Moulin and J. A. O’Sullivan, “Information-theoretic analysis of information Hiding,” IEEE Trans. On Info. Theory, vol. 49, no. 3, pp. 563-593, March 2003.

[10] S. Pavan, S. Gangadharpalli and V. Sridhar, “Multivariate entropy detector based hybrid image registration algorithm,” IEEE Int. Conf. on Acoustics, Speech and Signal Processing, Philadelphia, Pennsylvania, USA, pp. 18-23, March 2005.

[11] C. Rechberger, V. Rijman and N. Sklavos, “The NIST cryptographic Workshop on Hash Functions,” IEEE Security & Privacy, vol. 4, pp. 54-56, Austria, Jan-Feb 2006.

[12] Ghoshal N., Mandal, J. K. “A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT)”, Malaysian Journal of Computer Science, ISSN 0127-9094, Vol. 21, No. 1, pp. 24-32, 2008.