Reversible Data Hiding in Encrypted JPEG Bitstream using LSB based on chaos and the genetic algorithm.

Vaibhav Barve
Department Of Computer Engineering
Dattakala Group of Institute, Faculty of Engineering,
Swami Chincholi,Daund,Pune.
barvevaibhav31@gmail.com

Prof. S. S. Bere
Assistant Professor
Department Of Computer Engineering
Dattakala Group of Institute, Faculty of Engineering,
Swami Chincholi,Daund,Pune.
sachinbere@gmail.com

Abstract— Reversible data hiding has attracted plenty of interest recently. Being reversible, we can restore original digital information completely. It is a scheme where secret information is stored in digital media like image, video, audio to avoid unauthorized access and security purpose. Generally JPEG bit stream is used to store this key information, first JPEG bit stream is encrypted into well organized structure, after this secret data or key information is embed into this encrypted region by slightly changing the JPEG bit stream, useful pixels suitable for data embedding are calculated and according to this key details are embedded. In our proposed system we are using RC4 algorithm for encrypting JPEG bit stream, encryption key is accepted by system user which will also being in use at the time of decryption.

We are implementing improved least significant bit replacing steganography by using genetic algorithm. Initially, the number of bits that has to be embedded in a assured coefficient is adaptive. By using appropriate parameters, we can obtain very high capacity while protecting very high security. We are using logistic map for shuffling of bits and use GA (Genetic Algorithm) to locate correct parameters for the logistic map. Data embedding key is used at the time of data embedding.

By using exact image encryption and data embedding key, the recipient can easily extract the integrated secure information and absolutely recover the original picture as well as original secret data. When the embedding key is absent, the original image can be recovered approximately with adequate quality without getting the embedded key details.

Keywords – reversible data hiding, encryption, decryption, steganography, data embedding.

I. INTRODUCTION

Information hiding techniques can guard up more information in various digital media. Most data hiding techniques change the unique media in order to embed the key data. Although the distortions are often small and imperceptible, the reversibility is essential to some sensitive application. In application, such as in police officers, medical images, it is required to be able to reverse the noticeable picture back to the unique original picture for lawful concern. In military imaging and remote sensing, high accuracy is required. In some medical research, experimental information and details are costly and difficult to be obtained. Under these circumstances, the reversibility of the unique media is preferred. Reversible data concealing [1, 2] is a novel type of information hiding schemes, where at the moment, there are increasing interest in it.

It is impractical for human to differentiate between original image and stego image visually. Since, reversible data hiding can be thought as key interaction design. Without using meta-data, reversible information embedding gives true self verification plan by embedding its message confirmation rule [6]. Reversible Data Hiding (RDH) provides particular renovation of image and also extraction of details. Reversible data embedding is weak against harmful attack [3] [4] [5]. Initially reversible details embedding were invented by Honsinger1 in 1999. It was useful for lossless verification which was suffering from visible information reduction.

Fridrich et al. [7] initiate a new reversible data hiding technique to raise the embedding ability which works by adjusting the least significant bits (LSBs). The least significant bit plane of the cover image are compressed by their algorithm and then insert these compressed information and the embedded information into the cover image. Celik et al. [8] projected a generalized-LSBs algorithm to progress the performance of Fridrich et al.'s method in terms of storage, where the quantization residue of the cover picture can be accomplished after a quantization procedure and then the CALIC reversible compression technique is used to get the compressed

residues. The residue of the compression area is used to embed the secret information. Also [9] planned a high capacity picture steganography method based on inconsistent size LSB insertion.

Generally, RDH is used to embed information into picture which is open for Information hider. There might b condition in which image owner do not wish to share picture content to data hider. So it is essential to insert supplementary messages such as verification details etc. to cover picture. Buyer-Seller methodology can be applied by means of Treating Data hiding strategy [10], [11]. Here, a dealer encrypts information and entrench a secured signature given by customer. Seller will unable to get signature of customer and until customer doesn't make payment he will incapable to access the original version of information. Other method in which, secured images are divided into prevent and by tossing three LSBs of half the p in the prevent, one bit in each prevent is included [12]. At receiver's side, by examining the deviation of the pixel principles in every decrypted prevent, the key pixels get retrieved as well as the original picture is retrieved. An enhancement in this system is completed by Hong by developing link of the boundary between nearby prevents, and utilizing a side-match plan to accomplish a low mistake rate [13]. It also extended as separable Reversible Data Hiding plan. It is completed by contracting the secured information by applying a source programming strategy with part information it makes details extraction of information separate of security [14].

We are implementing improved least significant bit replacing steganography by using genetic algorithm. Initially, the number of bits that has to be embedded in a assured coefficient is adaptive. By using appropriate parameters, we can obtain very high capacity while protecting very high security. We are using logistic map for shuffling of bits and use GA (Genetic Algorithm) to locate correct parameters for the logistic map. Data embedding key is used at the time of data embedding.

II. RELATED WORK

Reversible data hiding is a technique to insert extra information into some cover media like image, video, audio etc. with a reversible approach so that the unique cover image can be completely re-establish after extraction of the hidden information. Different skills have been bringing in into the typical reversible information hiding strategies to increase the performance. Encryption is an admired and efficient means of privacy security. In order to firmly share a secret image, before transmission other individual a content owner may encrypt the image and at the receiver side decrypt the image. This paper aims to provide thorough evolution and understanding of various existing data hiding algorithm for encrypted picture. It integrates and covers recent research work.

There are some techniques of Reversible Data Hiding in secured pictures have been suggested. In [16], Zhang separates the secured picture into block, and embeds one bit into each prevent by tossing three LSBs of 50 percent the p in the block. On the recipient part, the key pixels are produced and the original image retrieved by examining the variation of the pixel values in every decrypted block. Hong et al. enhanced Zhang's technique by exploiting connection of the boundary between nearby blocks, and using a side-match plan to accomplish a low mistake amount [17]. Zhang further proposed a separable RDH plan for secured pictures by compressing the secured details using a resource programming plan with side information, creating details removal separate of security [18]. Recently, Ma et al. suggested an RDH means for secured pictures by reserving some space before security [19]. To do so, LSBs of some pixels are first included into other p using a conventional RDH method, and the picture is then secured. Consequently, roles of these LSBs in the secured picture can be used for embedding information with the data-hider.

A novel reversible information hiding criteria, which can restore the preliminary image without the distortions from the mentioned picture following the invisible information have already been created, is proven in this document. This criterion [15] uses the zero or the lowest details of the histogram of an image and a little bit adjusts the pixel black and white prices to present information into the picture. It can present more information than lots of the current undoable information protecting methods. It is proven analytically and found experimentally that the optimum signal-to-noise amount (PSNR) of the mentioned picture created by this method in comparison to the preliminary picture is fully assured to be above 48 dB. 0

A picture can be separated as set of quantized DCT coefficients in non-overlapped blocks. After that is written into bitstream with entropy development, as per JPEG standard [12]. DC and AC coefficients are managed individually, during entropy development. After using one dimensional forecaster, coefficients are secured by using Huffman requirements. In case of AC coefficients, the coefficients are efficiently secured with the run length programming (RLC) as there are number of zero's. In the JPEG data file headlines, platforms of Huffman/VLC programming and quantization are defined and stored. For entropy development and understanding, these platforms are essential. By using Huffman requirements and the corresponding appended pieces, the entropy secured pieces are organized. Bitstream parsing investigates compacted pieces with respect to the JPEG structure and the Huffman platforms recovered from the JPEG data file headlines.

III. IMPLIMENTATION DETAILS

a. System Architecture

We identify useful pixels suitable for concealing of information so that the secured bitstream which holds key data can be decoded properly. The key concept pixels are secured by using RC4 algorithm. The data embedding and data security are managed by data embedding key and security key respectively. By using exact image encryption and data embedding key, the recipient can easily extract the integrated secure information and absolutely recover the original picture as well as original secret data. When the embedding key is absent, the original image can be recovered approximately with adequate quality without getting the embedded key details.

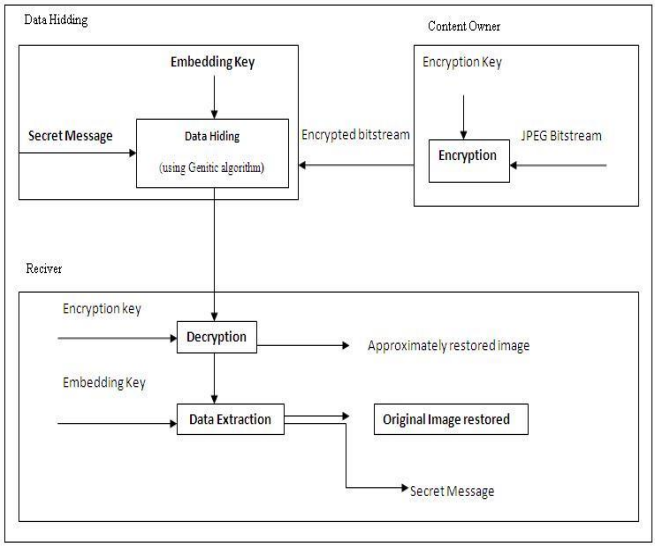

Fig 1: System Architecture

b. System Overview

The general framework of the suggested plan Consider the three events in the entire work-flow of encryption-embedding-extraction-restoration: material proprietor, information hider, and recipient, whose roles are described as follows.

1. Content owner: Parse the unique JPEG bitstream and secure the bitstream to cover up the major material of the unique picture. An security key is selected by the material proprietor. The secured bitstream must have the same framework as the unique so that it can be decoded properly to give an undistorted picture.

2. Data hiding: It embeds the key information into the secured JPEG bitstream. Suitable positions for information concealing are selected using Improve adaptive LSB with the help of genetic algorithm, and the possible embedding potential measured. We are using RC4 algorithm for encrypting the original image. User can choose his/her own encryption key. Same key is used for decryption of image at receiver's side.

3. Receiver: It draws out the key data and returns the JPEG bitstream. Receiver will require both encryption key and embedding key to draw out original image and secret information that is embedded into image at sender's side. Even if sender is not aware of embedding key original image can be retrieved.

c. Mathematical Model

We can describe Logistic map by $x_{n+1} = \mu x_n(1 - x_n)$
Where, $0 \leq \mu \leq 4 x_n \in (0,1)$
Bits to be Embedded in Each Coefficient,
$C = (c_0, c_1, \dots, c_{63})$
Where C denotes, the sequence of quantized DCT coefficients in a certain 8×8 JPEG block Shuffle message bit based on genetic algorithm $M = \{m_0, m_1, \dots m_{L-1}\}$. It denotes the length of the message.
Given pair of Input: (x_0, μ)

We are using the consecutive L different elements to form a vector. $Y = \{y_0, y_1, \dots y_{L-1}\} = .\{x_k, x_{k+1}, \dots x_{k+L-1}\}$

$I = \{i_0, i_1, \dots i_{L-1}\}$. It shows the suffix of sorted elements by arranging ŷ elements in descending order.

Message bits are shuffled according to I. ie. The bit having suffixed i_r in M is placed at position r.

d. Genitic algorithm

From the process of shuffling mentioned, we can say that the couple of parameters (x_0, μ) fix on the organization of shuffled message bits. To progress the performance of the shuffling technique, genetic algorithm is used to choose a correct pair of (x_0, μ). Here, we wish to improve quality of the stego image by comparing with of pick signal to noise ratio (PSNR) and choose PSNR as GA's fitness function:

$$\text{fitness} = PSNR = 10.log_{10}\{\frac{1}{255^2 MN}\sum_{m=1}^{M}\sum_{n=1}^{M}[d(m,n)]^2$$

Let, n and m are number of columns and rows of the cover image, correspondingly; d(m,n) is the variation between coefficients in spatial domain at position (m, n) in original picture and in the stego image. The method of relating

Genetic algorithm to maximize pick signal to noise ratio is declared as follows.

(1)Initialize population. Randomly generate L_p pairs of (x_0,μ), $x_0\varepsilon(0,1)$, $\mu \in (3.57)$. L_p is the size of population and each (x_0, μ) is an individual.

(2)For each (x_0, μ), bits of message are shuffled and put in the this message bits into the original picture by using our improved adaptive Least significant bit steganography, after that calculate Pick signal to noise ratio along with the stego cover image and the cover image, which can be the part of Genetic algorithm. In the subsequent operations, the entity with bigger fitness function will be measured best.

3) Operators of Genetic Algorithm—selection, crossover, and mutation—are operated to generate the next generation.

(4)Repeat (2) and (3) till the number of generation's equal's maximum generation maxGen(e.g., 100).

(5)Put out the best pair of *(x_0, μ)* selected by

Genitic algorithm

IV. EXPERIMENTAL RESULTS

The system is built using Java framework (version jdk 6) on Windows platform. The Netbeans (version 6.9) is used as a development tool. The system doesn't require any specific hardware to run; any standard machine is capable of running the application.

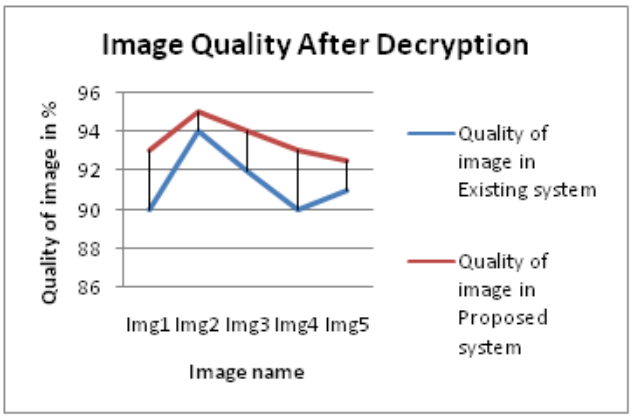

Fig 1: Quality of Image after decryption

Figure 1 describes the quality of the stego image ie. Image after decryption, this graph shows that the quality of stego image in the proposed system is better than that of existing.

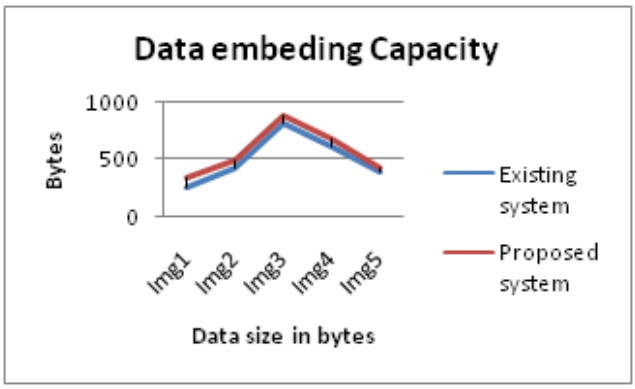

Fig 2: Data Embedding Capacity

Figure 2 shows that the data embedding capacity of the image is improved in our proposed system.

Table 1: Data embedding capacity of image in bytes

Image Name	Existing system	Proposed system
Img1	252	340
Img2	421	490
Img3	817	878
Img4	615	684
Img5	386	428

Data embedding capacity of the image is improved by using genetic algorithm.GA calculates the best pair of bits so that we can shuffle message bits with those bits.

V. CONCLUSION

We propose an RDH methodology for secured JPEG bitstream with LSB depending on Genetic Algorithm and chaos. The distinctive JPEG bitstream is appropriately secured to cover up the image content with the bitstream structure preserved. The main concept pixels are protected with RC4 and integrated into the secured bitstream by altering the appended pixels. By using the embedding and encryption keys, the receiver can dig out the included information and completely recover the picture used initially. Even if the embedding key is misplaced the unique image can be retrieved with satisfactory high quality without getting the included information. In our recommended system we are adding in two areas. First, we present improved flexible LSB Steganography that can comprise data adaptively and thus can fulfill various necessities (great security, high capacity, great picture high quality etc.). Our technique reduces deterioration of the

steganography image by finding the best applying between the key concept and the cover picture depending on chaos and the Genetic Algorithm (GA).

ACKNOWLEDGMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

References

[1] Y. Q. Shi, Z. Ni, D. Zou, C. Liang, and G. Xuan, 2004 "Lossless data hiding: Fundamentals, algorithms and applications," in Proc. IEEE Int. Symp. Circuits Syst., Vancouver, BC, Canada, (May 2004), vol. II, pp. 33–36.

[2] J. B. Feng, I. C. Lin, C. S. Tsai, and Y. P. Chu, 2006 "Reversible watermarking: current status and key issues," International Journal of Network Security, vol. 2, No. 3, pp. 161-171.

[3] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

[4] T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

[5] F. M.Willems and T. Kalker, "Coding theorems for reversible embedding," DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 66, pp. 61–78, 2004.

[6] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896 Aug. 2003.

[7] J. Fridrich, M. Goljan, R. Du, 2001, "Invertible authentication" Proceedings of SPIE Photonics West, vol. 3971, Security and Watermarking of Multimedia Contents III, San Jose, CA, pp. 197–208.

[8] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, 2005, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol.14, no.2, pp.253–266

[9] Lee, Y.K., and Chen, L.H., 2000, 'High capacity image steganographic model', IEE Proc., Vis. Image Signal Process., 2000, 147, (3), pp. 288–293.

[10] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.

[11] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[12] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[13] W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.

[14] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[15] Z. Ni, Y. Shi, and N. Ansari et al., "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[16] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[17] W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.

[18] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[19] K. Ma, W. Zhang, and X. Zhao et al., "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, 2013.