



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Special Issue 6, July 2017

Compression of Steganographic Images by Dictionary Adaptive Approach

Manjula K¹, Nethravathi J², Shilpa L³

Assistant Professor, Dept. of Information Science Engineering, Sri Krishna Institute of Technology, Karnataka, India¹

B.E student, Dept. of Information Science Engineering, Sri Krishna Institute of Technology, Karnataka, India²

B.E student, Dept. of Information Science Engineering, Sri Krishna Institute of Technology, Karnataka, India³

ABSTRACT: Due to the explosive growth of Internet technologies and its applications, Steganography and Image Compression techniques have become an prominent area of research. Least Significant Bit (LSB) substitution, a spatial domain steganographic technique involves replacement of the least significant bit of randomly selected pixels in the cover image with the secret image bit. Image information transmission is always a challenge for public network because of its larger in size. To provide efficient and high security transmission, Dictionary adaptive compression approach is suggested on steganographic images. The increase in the efficiency and optimization in the payload capacity is achieved by the implementation of logistic maps for randomized pixel selection which is further optimized with Genetic Algorithm for pixel location modification. Visual cryptography is applied to secure shuffled stego image. Analyzed results shows the robustness of proposed techniques and algorithm in terms of improved payload capacity, less degradation in picture quality, secured transmission of images and high randomness in pixel selection.

KEYWORDS: Image Steganography, Compression, Dictionary Adaptive Approach, Logistic maps, Genetic Algorithm.

I. INTRODUCTION

Steganography literally means covered/hidden writing i.e., it is a art and science of hiding information in a cover media such as digital images, audio, video, text files in a way that conceals the existence of hidden data. The word steganography combines the Greek words steganos meaning “covered, concealed, or protected”, and graphien meaning “writing”. The main objective of steganography is unauthorized users should not be able to distinguish between cover media (media not containing any secret message) and stego-media (modified cover media containing secret message). Applications of steganography include enhancing robustness of image search engines, smart identity cards etc.

Today information is not only present in the form of text but also in the form of images. With the development of multimedia technology, more and more information comes from images. With the widespread of communication network, people’s requirement of digital images and multimedia information have grown increasingly. One emerging problem is that a growing size of digital data, particularly images. Another challenge is to maintain the image quality during the communication.

Several works have been reported for compression of the steganographic images. According to the distortion of image data, there are two categories in compression techniques, Lossless Compression and Lossy Compression. In our proposed paper lossless compression technique has been adopted, since the data during the compression process won’t be lost and can restore to its pre-compression status. One of the lossless technique, that is dictionary adaptive approach is used to perform image compression. This approach gains high compression ratio and it is the best technique for reducing the size of files containing more repetitive data. Size of the files can be reduced by analyzing the frequency of repetitive data.

To reduce the payload capacity of the pixels logistics equations are applied, which provide complex chaotic behavior. The random values generated using the logistics equations are to be converted into possible pixel positions. For the further optimization of pixels which are randomly selected, Genetic Algorithm is applied, where this belongs to the



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Special Issue 6, July 2017

larger class of evolutionary algorithm which generate solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation and selection.

The scope of the proposed paper is to reduce the size of the stegano images, minimal degradation in the picture quality by dictionary adaptive approach and high security transmission, high randomness in pixel selection by ensemble of logistics map with genetic algorithm. To secure the shuffled stego images, Visual Cryptography is applied.

II. RELATED WORK

[1] A Genetic Algorithm based Steganography using Discrete Cosine Transformation (GASDCT).

Proposing a novel embedding or authentication approach based on discrete cosine transformation for grey scale images. A 2×2 sub mask of source images is taken in row major order and discrete cosine transformation is applied on it to generate four components. Two bits of authenticated images are embedded into each transform co-efficient except the first one. In each co-efficient second and third position from LSB are chosen for embedding in the transform domain. Stego sub intermediate image is generated through reverse transform. Sub mask from this intermediate image is taken as initial population and new generation applied on initial population for security.

[2] Optimized Video Steganography using Genetic Algorithm.

In this paper a novel video steganography scheme for efficient and effective hiding. A 3-3-2 LSB based scheme has been used as a base technique for video steganography. Imperceptibility and video quality are supposed to be two key parameters for deciding goodness of any steganographic scheme. Thus the base technique is enhanced using GA which thrives to get an optimal imperceptibility of hidden data. An anti-steganalysis test is used to check the frame with respect to original frame. A performance and evaluation has been done of the proposed technique with the base technique on the basis of perceptibility and fidelity.

[3] Steganographic algorithm based on a chaotic map.

They proposed a stenography algorithm based on a single chaotic map to determine the pixel position of the host color image. The channel and the bitpass of the targeted value in which sensitive information bit can be hidden can also defeat may existing steganalytic attacks.

[4] Review of Image Compression Encryption Techniques.

A growing need for data and information transmission in a safe and quick manner researches in image protection and security through a combination of cryptography and compression technology being to take from the combination of these two methods. This may include into three categories based on their process sequences.

The first category i.e. cryptographic technology followed by compression method focuses more on image security than the reduction of the size of data. The second combination compression technology followed by cryptographic method has an advantage where the compression technology can be lossy, lossless or combination of both. The third category compression and cryptography technology in a single process either partially or in the form of compression sensing providing a good data safety assurance with such a low computational complexity that it is eligible for enhancing the efficient and security of data information transmission here we can add up one of the compression technology on a steganographic images i.e. the application of this adaptive compression to obtain a high compression rate the adaptive compression work to reduce the size by analyzing frequencies separately and the relating them in a dictionary or tabular forms.

[5] JPEG Algorithm Analyzing and Application in Image Compression Encryption of a Digital Chaos.

The digital images also face the huge pressure of a man data storage and transmission. it may be attacked during transmission process thus it is necessary to focus our attention of image compression technology, this will explain about necessity and classification of image compression technology then we make a depth analyzing of JPEG image compression algorithm. we focus on JPEG encoding algorithm and make a detailed description of JPEG encodes decoder control process.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Special Issue 6, July 2017

[6] Novel Image Compression Encryption Hybrid Algorithm Based on Key Control Measurements Matrix in Compressive Sensing.

A new image compression encryption hybrid algorithm is proposed to realizing compression and encryption simultaneously when the key is easily distributed stored or unauthorized. the input images will be divided in to four blocks to compression and encrypt then the pixel of two adjacent enhanced randomly by random matrix. these are constructed by utilizing circulant matrices and controlling the original row vectors of circulant matrices with logistics maps.

[7] An Efficient Encryption then Compression Technique For Encrypted image using SVD.

This proposes a lossy compression technology for encrypted images using discrete wavelet transform singular value decomposition(SVD) and Huffman coding. this mainly based on both significant and less significant coefficient are encrypted using pseudo random number sequence and then it will be compressed respectively at receiver side a reliable decompression technology is used reconstructed the original image content with the help of compressed bit stream and secret keys.

III. SYSTEM ARCHITECTURE

In this section, we discuss the architecture of Optimal Pixel Selection in Lossless Compression Image Steganography of Ensemble of Logistic Maps with Genetic Algorithm. This is based on Lossless Symmetric compression which perform the compression technique on the steganography image.

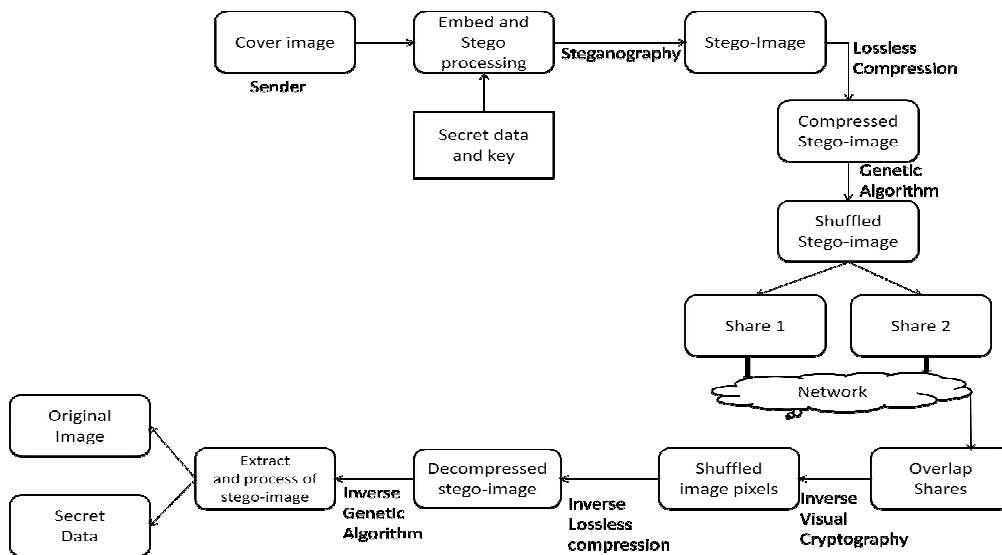


Figure 1: Architecture of Image compression.

Figure 1 shows the architecture of Lossless Compression image steganography of ensemble of logistic maps. in this the source image will be given as input to the spatial domain as Image steganography can be broadly classified into spatial domain transform domain, spread spectrum and model based steganography. In spatial domain, secret message/data is embedded in pixel value directly whereas transform domain methods achieve embedding by first transforming the image from spatial to frequency domain using any one of the transforms such as discrete cosine transform(DCT), discrete wavelet transform (DWT), Hadamard transform. Dual tree DWT, double density dual tree DWT (DD DTDWT), ridge let transform, curvelet transform etc. and then embedding is done in suitable transform coefficients.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

In Least Significant Bit (LSB) method, embedding can be achieved by simply replacing LSB of the randomly selected pixel in the cover image with the secret message bit and then that will undergo steganography process in turn will be getting a stego-image. an efficient lossless symmetric compression technique will be applied on the stego-image. which defined to reduce the size of communicating image data over the network by changing the bit representation of each pixel over the image. The image size reduction is required to provide the efficient communication over the network. As the image size gets compact, there are lesser chances of image distortion over the communication. The importance of image compression is to emphasize the large size image to smaller bit form so that the secure information transmission will be obtained. the process will be done without any loss in the quality of stego-image with that compressed stego-image by genetic algorithm the image will get distorted, this algorithm which is used to modify the pixel location of stego-image and the detection of this message is complex and it has been used for enhancing the security. It is achieved by breaking into two shares based on a threshold and will stored. at receiver side if she/he want to process the image through network they can take those shares and by inverting the visual cryptography the shuffled pixel image will be obtained and by inverting the compression method the decompressed stego-image and by inverting genetic algorithm the stego-image will be extracted and processed then the related image and the secret data will be obtained to the receiver respectively.

Steganography Module: This module is used to hide a secret data from the user into the input image using key based selection algorithm the data are stored in the input image using LSB technique.

Genetic Algorithm: This module is used to change the pixel positions of the stego-images which is used to provide security for the secret data and the cover image.

Visual Cryptography: The output of genetic algorithm is given as input to this module which uses the visual cryptography algorithm to divide them into two secret shares.

Compression Technique: The compression is here defined to reduce the size of communicating image data over the network by changing the bit representation of each pixel over the image. The image size reduction is required to provide the efficient communication over the network. As the image size gets compact, there are lesser chances of image distortion over the communication. Image Compression involved in this technique condenses the data and thus increases the message hiding capacity and furthermore adds additional security to it. These reasons of image compression requirement is given here:

- 1) To provide the large storage to multimedia information or data.
- 2) To provide the effective communication for slow communication medium.
- 3) The compression provides the effective communication without changing the hardware requirements.

Compression Algorithm: Image compression plays a key role in many important applications, including image database, image communications, remote sensing. One of the criticality of compression algorithm is the encoding mechanism. The encoding mechanism can be lossy or loss less. The lossy method provides the high compression ratio at cost of information loss whereas the lossless compression methods are comparatively slow and provides less compression ratio. In this work, a dictionary adaptive approach is defined to achieve effective compression ratio without degrading the image quality. The dictionary based approach basically maintains the bits information as well as its transformed bit sequence so that the symbol or the pixel transformation will be obtained effectively. The working of this dictionary method depends on many factors such as the number of bits to present a particular word as well as the frequency of word over the image.

In the general form, the high frequency words are represented by lesser bit length and the low frequency words are presented by large bit length so that the reduction in the bits over the image encoding will be obtained. As the encoding



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Special Issue 6, July 2017

process is performed sequentially, the image pixels are examined under the intensity sequence so that the dictionary is analyzed under algorithmically.

According to this repetitive information count, the dictionary or the table is maintained. Once the table is maintained, the bit sequence is applied to encode or compress the information. The decompression algorithm of these approaches is just reverse to the actual algorithm. The adaptive algorithms are adaptive so that the decoding will be done effective. The table can be regenerated during the decompression process at the receiver side. Another important factor while performing the image encoding is the sequence in which the image pixel will be read. The sequence can be left to right, right to left, top to bottom or the zigzag approach. The successive intensity pixels are analyzed and recognized as the sequence pixels or the image so that the maximum repetitive combinations will be obtained. Based on this sequence, the dictionary is maintained in the form of table and the new generated codes are obtained.

IV. CONCLUSION

In this paper, the concept of logistics maps and genetic algorithm is employed for the selection of the optimal pixel positions for least significant bit method. For the high security of images steganography is applied and the compression of stegno images for the storage efficiency and for the minimal degradation in the quality of pixel. Visual Cryptography is applied to secure the shuffled stego images. The analyzed results prove the robustness of the algorithm against security analysis and in retaining the picture quality.

REFERENCES

- [1] Amrita Khamrui, J J Mandal, "A Genetic Algorithm based Steganography using Discrete Cosine Transformation (GASDCT)", international conference on computational intelligence: Modelling Techniques and Applications (CIMTA), 2013, pp. 105-111.
- [2] Koushik Dasgupta, Jyotsna Kumar Mondal, Paramartha Dutta, "Optimized Video Steganography using Genetic Algorithm", International Conference on Computational Intelligence Modeling Techniques and Applications(CIMTA), 2013, pp. 131-137.
- [3] Ali Kanso, Hala S. Own, "Steganography algorithm based on a chaotic map", Commun Nonlinear Sci NumerSimulat, 2012, pp. 3287-3302.
- [4] EmySetyaningsih, RetantyoWardoyo, "Review of Image Compression and Encryption Techniques", International Journal of Advanced Computer Science and Applications, 2017.
- [5] Li Zhiqiang, Sun Xiaoxin, Du Changbin, Ding Qun, "JPEG algorithm analysis and application in image compression encryption of digital chaos", third International Conference on Instrumentation, Measurement, Computer, Communication and Control, 2013.
- [6] Nanrun Zhou, Aidi Zhang, Fen Zheng, Lihua Gong, "Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing", ELSEVIER journal, 2014.
- [7] Monaj Kumar, Ankita Vaish, "An efficient encryption-then-compression technique for encrypted images using SVD", ELSEVIER journal, 2016.