ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

Optimal Reserving Room Based Reversible Data Hiding In Encrypted Images

Sreekutty T P[1], Shammy Arun Mathew[2]

M-Tech student (AE&I), Dept. of ECE, Lourdes Matha College of Science and Technology, Trivandrum, India[1]

Assistant professor, Dept of ECE, Lourdes Matha College of Science and Technology, Trivandrum, India[2]

ABSTRACT: An undesirable side effect of many water marking and data hiding schemes is that the host signal into which auxiliary data is embedded is distorted. In some applications which hide data into important images, permanent distortion of the image is unacceptable. Eg: X ray images. In these applications, a reversible data hiding method is required. Recently, more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. The proposed method consists of first, reserving the room for embedding the data, so that it is easy for the data hider to reversibly embed data in the encrypted image; then encryption of the image and finally embedding of data. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Existing method has low attack resistance due to inefficient selection of reserving room and low PSNR for embedded image. So for increasing attack resistance here proposes a Genetic algorithm based optimal reserving room selection for data hiding.

KEYWORDS: Reversible data hiding, Reserving room, Image encryption, Genetic algorithm, Histogram shift

I. INTRODUCTION

The recent interest of data hiding is fuelled by the increased amount of communication through the internet to transmit a large amount of information. Some of them may be secret information which is candidate to unauthorized access. In order to keep the unauthorized users away, variety of techniques has been proposed for providing a secure transmission of information. Data encryption and data hiding techniques have become popular and complement each other. Whereas data encryption transforms data into seemingly meaningless bits called cipher text through cipher algorithms, this enable only the user that has a key to decrypt the secret data from the cipher texts to the plain texts. For any unauthorized user who does not have a key, the cipher text will look like nothing but streams of meaningless codes. Although data encryption is a good way to prevent unauthorized user from accessing secret data, it still has some weaknesses. The appearance of cipher texts would give un-authorized user an impulse to recover them. Data hiding techniques embeds the important data inside multimedia data such as images, videos or audio. Digital images are considered good cover carriers because of their insensitivity to human visual systems.

Watermarking and steganography are two major kinds of information hiding technology. Watermarking is used to embed a distinguishable symbol, e.g., a signature or a trademark, into host signals to authorize the ownership of the signals, The Steganography is used to hide information inside information, thus hiding the existence of the communicated information.

The word steganography is of Greek origin which means "covered or hidden writing". The general purpose of steganography differs from cryptography, which is intended to make a message unreadable by a third party but does not

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

hide the existence of the secret communication. Some of authors categorize steganography as a form of cryptography although steganography is separate and distinct from cryptography where hidden communications are a form of secret writing.

Reversible data hiding is a relative young and fast growing technique which has tremendous interest from industry, military, medical field and law forensics. It is a highly multidisciplinary field combining image and signal processing with cryptography, communication theory, coding theory, signal compression etc. Data hiding is a technique by which some data is hidden into a cover media. The data may be any text related to the image such as authentication data or author information and cover media can be a text, or an image, an audio or video etc. At the receiver side it must be able to extract the hidden data. In some high-precision applications such as medical, military and remote sensing, it is highly desired that the original image should be perfectly recovered after data extraction. A data hiding technique satisfying this requirement is known as *reversible data hiding*. They are also called *invertible*, *lossless* or *distortion free data hiding*. Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted.

A technique in which secret messages are transferred from one person to another over the communication line called cryptography. The technique(s) used to convert the original data into secret code or data is called data encryption technique for all kinds of data such as textual data, Image data or multimedia data for secured communication over a network. Images encryption is different from the simple data encryption. So in general the data hiding in image involves four steps.

a. Selection of the secret media where the data will be hidden.
b. The undisclosed message or information that is needed to be masked in the cover image.
c. A function that will be used to hide the data in the cover media and its inverse to retrieve the hidden data.
d. An optional key or the password to authenticate or to hide and unhide the data.

The paper presents a new method for reversible data hiding in encrypted images by genetic algorithm based reserving room before encryption.

From the review of related work and published literature, it is observed that many researchers have proposed different techniques for reversible data hiding.Encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission and decrypt at the receiver end.

Ni et al. [2] introduces “Reversible data hiding,” a RDH technique which utilizes zero or minimum point of histogram. If the peak is lower than the zero or minimum point in the histogram, it increases pixel values by one from higher than the peak to lower than the zero or minimum point in the histogram. While embedding, the whole image is searched. Once a peak-pixel value is encountered, if the bit to be embedded is '1' the pixel is added by 1, else it is kept intact. Alternatively, if the peak is higher than the zero or minimum point in the histogram, the algorithm decreases pixel values by one from lower than the peak to higher than the zero or minimum point in the histogram, and to embed bit '1' the encountered peak-pixel value is subtracted by 1. The decoding process is quiet simple and opposite of the embedding process.. The advantages of this method are – (i) it is simple, (ii) it always offers a constant PSNR 48.0dB, (iii) distortions are quite invisible, and (iv) capacity is high. The disadvantages are – (i) capacity is limited by the frequency of peak-pixel value in the histogram, and (ii) it searches the image several times, so the algorithm is time consuming.

V. Sachnev, [3] presented “Reversible watermarking algorithm using sorting and prediction,. This paper presents a reversible or lossless watermarking algorithm which employs prediction errors to embed data into an image. A sorting technique is used to record the prediction errors based on magnitude of its local variance. The proposed reversible watermarking algorithm is a combination of efficient well-known existing techniques and new techniques which enables performance significantly. Using a new rhombus prediction scheme enables the efficient exploitation of sorting. A set of sorted prediction errors can be efficiently used for low distortion data hiding. The histogram shift

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

method exploited over the sorted prediction errors produces excellent ratio between capacity and distortion. Thus, capacity can be significantly increased.

L. Luo et al., [4] presented a paper entitled "Reversible image watermarking using interpolation technique,". This paper, presents a novel reversible watermarking scheme using an interpolation technique to generate residual values named interpolation-errors, which are demonstrated to be of greater decorrelation ability. By applying additive expansion to these interpolation-errors, achieve a highly efficient reversible watermarking scheme, which can guarantee high image quality without sacrificing embedding capacity, which can embed a large amount of covert data into images with imperceptible modification. Different from previous watermarking schemes, we utilize the interpolation-error, the difference between interpolation value and corresponding pixel value, to embed bit "1" or "0" by expanding it additively or leaving it unchanged. Due to the slight modification of pixels, high image quality is preserved. According to the experimental results, the proposed reversible scheme provides a higher capacity and achieves better image quality for watermarked images.

Xinpeng Zhang [5] introduces "Reversible data hiding in encrypted images," a novel reversible data hiding in encrypted images. The entire uncompressed image is first encrypted by a stream cipher. The additional data can be embedded into the image by modifying a small proportion of encrypted data. That is the encrypted image is first divided into several blocks .By flipping 3 LSBs of the half of pixels in each blocks, room can be vacated for the embedded bit. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered

II. TECHNICAL DETAILS

In this section, it describes a method for reversible data hiding in encrypted images by genetic algorithm based reserving room before encryption. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. This paper, describes novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. This method can achieve real reversibility, that is, data extraction and image recovery are free of any error.

Reversible data hiding is atechniue by which the original cover can be losslessly recovered after the embedded message is extracted. Losslessly vacating room from the encrypted image is reltively difficult and inefficient and it cannot achieve good image quality. So for achieving real reversibility, room for data hiding is reserved prior to image encryption.

Inefficient selection of reserving room may low attack resistance ie, poor security and also low PSNR for embedded image. PSNR (peak signal to noise ratio) represents the distortion level between marked image and cover image. So here a genetic algorithm based optimal selection is used for the selection of reserving room for data hiding.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

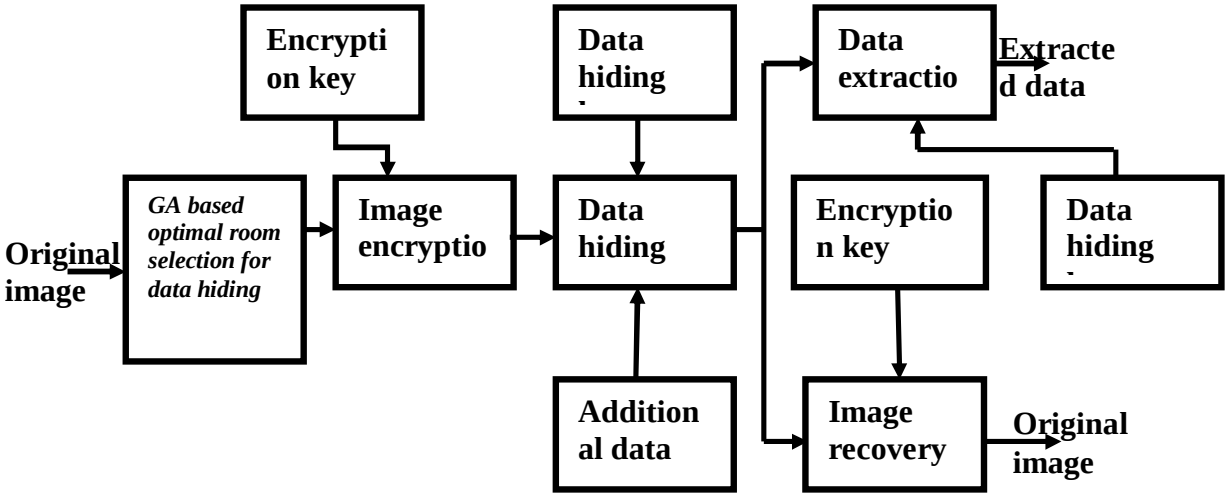


Fig 1:Block diagram

In this technique the content owner first reserve enough space on original image and then converts the image into its encrypted version with the encryption key using a standard cipher. Then in data embedding process data hider only needs to accommodate data into the spare space previous emptied out. At the receiver, content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

RRBE (reserving room before encryption) consists of four stages: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery.

a) Generation of encrypted images

It consists of two steps: image partition, self reversible embedding followed by image encryption. Image partition step divides the original image into two parts A and B using genetic algorithm, then LSBs of A are reversibly embedded into B with a standard RDH algorithm so that LSBs of A can be used for accommodating messages, at last encrypt the rearranged image to generate its final version.

Image partition: In this step the original image is divided into no: of overlapping blocks. Genetic algorithm is used for selecting the blocks which contain relatively more complex textures. The content owner selects the particular block with the highest features to be A, and puts it to the front of the image concatenated by the rest part B with fewer textured areas.

Self-reversible embedding: The goal of self-reversible embedding is to embed the LSB-planes of A into B by employing traditional RDH algorithms.

Image encryption: Rearranged image is encrypted using standard cipher. The encrypted bits can be calculated through exclusive or operation with a random number generated via a standard cipher determined by the encryption key

b) Data Hiding In Encrypted Image

In this module, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the space which was previously emptied out by LSB replacement technique.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

c) Data Extraction and Image Recovery

Data extraction is completely independent from image decryption

Case 1: Extracting Data from Encrypted Images to manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. When the database manager gets the data hiding key, he can decrypt and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

Case 2: In this module, after generating the marked decrypted image, the content owner can further extract the data and recover original image.

III. ROLE OF GENETIC ALGORITHM IN OPTIMUM SELECTION OF RESERVING ROOM

Reversible data hiding is a techniue by which the original cover can be losslessly recovered after the embedded message is extracted. Losslessly vacating room from the encrypted image is reltively difficult and inefficient and it cannot achieve good image quality.so for achieving real reversibility, room for data hiding is reserved prior to image encryption.

Inefficient selection of reserving room may low attack resistance ie, poor security and also low PSNR for embedded image. PSNR (peak signal to noise ratio) represents the distortion level between marked image and cover image. So here a genetic algorithm based optimal selection is used for the selection of reserving room for data hiding.

Genetic Algorithms (GA) are direct, parallel, stochastic method for global search and optimization, which imitates the evolution of the living beings, described by Charles Darwin. GA are part of the group of evolutionary Algorithms (EA). The evolutionary algorithms use the three main principles of the natural evolution: reproduction, natural selection and diversity of the species, maintained by the differences of each generation with the previous. The evolution usually starts from a population of randomly generated individuals and happens in generations. In each generation, the fitness of every individual in the population is evaluated, multiple individuals are selected from the current population (based on their fitness), and modified to form a new population Genetic Algorithms works with a set of individuals, representing possible solutions of the task. The selection principle is applied by using a criterion, giving an evaluation for the individual with respect to the desired solution. The best-suited individuals create the next generation. The large variety of problems in the engineering sphere, as well as in other fields, requires the usage of algorithms from different type, with different characteristics and settings.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

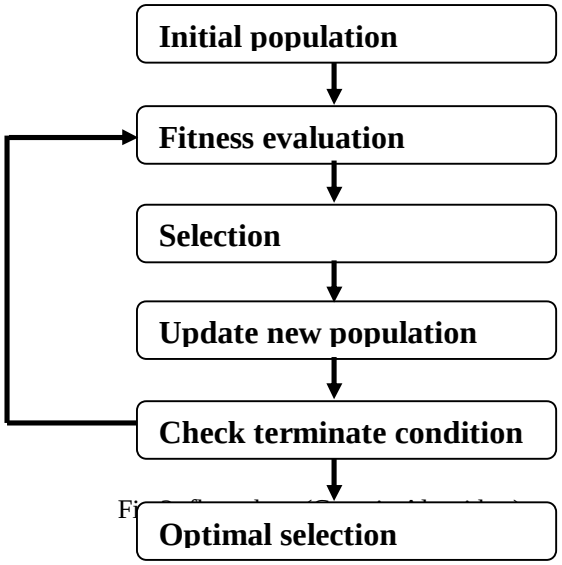
International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014



Chromosomes

For the genetic algorithms, the chromosomes represent set of genes, which code the independent variables. Every chromosome represents a solution of the given problem. Individual and vector of variables will be used as other words for chromosomes. From other hand, the genes could be Boolean, integers, floating point or string variables, as well as any combination of the above. A set of different chromosomes (individuals) forms a generation. By means of evolutionary operators, like selection, recombination and mutation an offspring population is created.

Selection

In the nature, the selection of individuals is performed by survival of the fittest. The more one individual is adapted to the environment - the bigger are its chances to survive and create an offspring and thus transfer its genes to the next population. In EA the selection of the best individuals is based on an evaluation of fitness function or fitness functions. Examples for such fitness function are the sum of the square error between the wanted system response and the real one; the distance of the poles of the closed-loop system to the desired poles, etc. If the optimization problem is a minimization one, than individuals with small value of the fitness function will have bigger chances for recombination and respectively for generating offspring.

Cross over

In genetic algorithm cross over is a genetic operator used to vary the programming of chromosomes from one generation to the next. Cross over is simply a matter of replacing some of the genes in one parent by the corresponding genes of the other.

Mutation

The mutation process causes the inversion of some bits and produces some new chromosomes. The purpose of mutation in GAs is preserving and introducing diversity.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

IV. EXPERIMENTS AND RESULTS

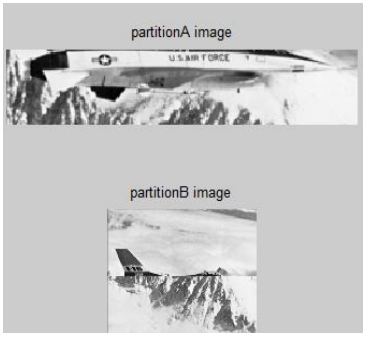
The proposed approach will be tested on public available standard images, which include “Lena”, “Airplane”, “Barbara”, “Baboon”, “Peppers” and “Boat” [19]. The size of all images is 512 ×512× 8. The objective criteria PSNR is employed to evaluate the quality of marked decrypted image quantitatively.

$$MSE = \frac{1}{mn}\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}[I(i,j) - K(i,j)]^2$$

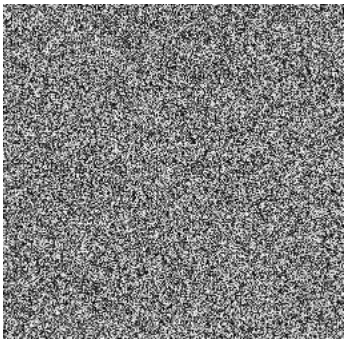
$$PSNR = 10\log_{10}\left[\frac{Max1}{MSE}\right]^2 \ in\ dB$$

Where I= cover image, K= Marked image, Max1=Max grey value ie,255.

(a)



(b)



(c)

(d)

(e)

Fig3: (a) Original image (b) Image partition (c) Encrypted image (d) Marked decrypted image (e) Reconstructed image

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

V. CONCLUSION

Reversible data hiding is a technique by which the original cover can be losslessly recovered after the embedded message is extracted. Losslessly vacating room from the encrypted image is reltively difficult and inefficient and it cannot achieve good image quality. So for achieving real reversibility, room for data hiding is reserved prior to image encryption. Here an idea about optimal reserving room based data hiding in encrypted image is presented. Inefficient selection of reserving room may low attack resistance ie, poor security and also low PSNR for embedded image. PSNR (peak signal to noise ratio) represents the distortion level between marked image and cover image. So here a genetic algorithm based optimal selection is used for the selection,which improves the PSNR than the previous methods

REFERENCE

[1] K. Ma, W Zhang, X Zhao, " Reversible data hiding in encrypted images by reserving room before encryption" *IEEETrans.inf foencics network*.vol.8 no.3 Mar 2013
[2] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," *IEEETrans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006.
[3] L. Luo *et al*., "Reversible image watermarking using interpolation technique, "*IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193,Mar. 2010.
[4] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.
[5] X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.
[6] P M Sivaraja, "Data hiding scheme for digital images based on genetic algorithms with LSBMR," International *Journal of Computer Applications (0975 – 8887)Vol 59– No.5, December 2012*