Medical Image Protection using Genetic Algorithm

S.Thangamani
Research Scholar
Department of Computer Science
School of Computer Science, Engineering and Applications Bharathidasan University, Trichirappalli

Abstract— The Goal of Covered Writing is to hide message sent secretly to destination during transmission. The Covered Writing is a limit for unauthorized access and provide better security. Data hide is art of science for secret information. A large number of commercial Covered Writing program use the least significant bit embedding as the method of choice for hiding data as it as low computation complexity and high embedding capacity but certain RS analysis is considered as one of the most famous Covered analysis algorithm which has the potential to detect the hidden message by statistic analysis of the pixels value. It has majority of the work no much optimal consideration robust security towards the encrypted data. This work introduced the concept of secure data hiding and transmission over the networks using LSB based Covered Writing with genetic algorithm. The genetic algorithm has been used for enhancing security. Genetic Algorithm is used to modify the pixel location of Covered image based on LSB Substitution which is another protection lock for the secret massage and detection of this is complex.

Key words: Genetic Algorithm, Statistical Analysis, Cover Image

I. INTRODUCTION

A. *Steganography*

The hiding of data is frequently called steganography. Steganography is a technology that hides a message within an object. Steganography plays an important role in information security [1, 2]. The origin of steganography is traced back to ancient civilizations. The ancient Egyptians communicated covertly using the hieroglyphic language, a series of symbols representing a message. The message looks as if it is a drawing of a picture although it may contain a hidden message. After the Egyptians, the Greeks used steganography, "hidden writing" where the name was derived [3]. The goal of steganography is to hide the fact that any form of communication is occurring by embedding messages into an innocuous looking cover medium such as digital image, video, audio and so on, while steganalysis focus on revealing the presence of the secret messages and extract them. In general, steganography approaches hide a message in a cover e.g. text، image, audio file, etc.

B. *Principles of Steganography*

There are three categories of steganography:

Pure steganography, secret key steganography, and public key steganography pure steganography requires no prior exchange of information between the two parties communicating and relies on secret through obscurity. This means that the algorithms not publicly known.

Secret key steganography usual uses a publicly known algorithm, and relies on a secret key chosen by the two parties communicating. This key is needed to both embed and extract the hidden information. Another possibility is public key steganography. It entails the sender using the recipient's public key to embed the information, which can only be detected using the recipient's private key.

C. *Image Steganography Methods*

There are a variety of methods used in which information can be hidden in images. In the following section, we present the most common methods. There are three common methods of steganography.

- Replacing Moderate Significant Bit
- Transformation Domain Techniques
- Replacing Least Significant Bit

D. *Types of Attacks*

1) *Visual Attack*

A visual attack is the simplest way of trying to detect an embedding. It is particularly effective against LSB embeddings, but it is useless against more advanced algorithms that do not embed into the pixels of the image directly like Jsteg. A visual attack begins by looking at the image as a whole. If an embedding is detected through color abnormalities the steganographic algorithm has been successfully attacked

2) *Statistical Attack*

Statistical attacks on LSB embeddings are much more effective than a visual attack. Statistical attacks make use of the relationship between bit-planes in an image or the relationship between pixels within a bit-plane to determine if a message is embedded into an image. Statistical attacks are typically tuned to work against a particular embedding algorithm, since different embedding strategies affect the perturbing of pixel values in a unique manner.

II. RELATED WORK

A. *Efficient Compression of Encrypted Grayscale Images*

Lossless compression of encrypted sources can be achieved through Slepian-Wolf coding. For encrypted real-world sources such as images, the key to improve the compression efficiency is how the source dependency is exploited. Approaches in the literature that make use of Markov properties in the Slepian-Wolf decoder do not work well for grayscale images. In this paper, we propose a resolution progressive compression scheme which compresses an encrypted image progressively in resolution, such that the decoder can observe a low-resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. Good performance is observed both theoretically and experimentally. Which has been shown to have much better coding efficiency and less computational complexity than existing approaches.

B. *Quality Assessment of Color Image Compression using HAAR Wavelet Transform*

Images require substantial storage and transmission resources, thus image compression is advantageous to

reduce these requirements. This paper covers some background of wavelet analysis, data compression and how wavelets have been and can be used for image compression. The paper examines a set of wavelet functions (wavelets) for implementation in a still image compression system and discusses important features of wavelet transform in compression of still images, including the extent to which the quality of image is degraded by the process of wavelet compression and decompression. The effects of different wavelet functions, image contents and compression ratios are assessed.

C. Stream Ciphers Analysis Method

The purpose of this paper is to present and to discuss analysis methods applied in symmetric cryptography, especially on stream ciphers. The tests were made on some algorithms and also on the personal symmetric cryptographic algorithm, HENKOS, based on a pseudorandom number generator. The test confirms that the algorithm appears to be secure and fast. The paper describes first the main parts of the cryptosystem, its implementation and different analysis methods.

D. A Robust Embedded Data from Wavelet Coefficients

An approach to embedding gray scale images using a discrete wavelet transform is proposed. The proposed scheme enables using signature images that could be as much as 25% of the host image data and hence could be used both in digital watermarking as well as image/data hiding. In digital watermarking the primary concern is the recovery or checking for signature even when the embedded image has been changed by image processing operations. Thus the embedding scheme should be robust to typical operations such as low-pass filtering and lossy compression.

III. PROPOSED METHOD

A. Bit-planes [for Image Hide]

Each color channel R, G, and B in the RGB color space is represented by a number, and this number is represented by a number of bits. In my work with grayscale images the number of bits is eight. A bit-plane refers to all the bits at a single bit position across an image. Consider the number ten, whose 8-bit binary representation is "00001010". Starting from the right, we have a "0" in the zeroth bit-plane, a "1" in the first, a "0" in the second, and so on for all eight bits. In an image, a bit-plane refers to the 0 or 1 value at a given position for all pixels, laid out in the same format. In LSB Steganography, the least significant bit-planes are manipulated.

$$A_{n=}1/2[1-(1-1)^n] \quad \text{Or } a_{n=}n(\text{mode}2)$$

B. LSB Algorithm [Extract the Image]

Least Significant Bit Substitution is the process of adjusting least significant bit pixels of the carrier image. Least Significant Bit (LSB) embedding is a simple strategy to implement steganography. Like all steganographic methods, it embeds the data into the cover so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the least significant bit(s). This minimizes the variation in colors that the embedding creates. For example, embedding into the least significant bit changes the color value by one. Embedding into the second bit-plane can change the color value by 2. If embedding is performed on the least significant two pixels, the result is that a color in the cover can be any of four colors after embedding.

Steganography avoids introducing as much variation as possible, to minimize the likelihood of detection. In a LSB embedding, we always lose some information from the cover image. This is an effect of embedding directly into a pixel. To do this we must discard some of the cover's information and replace it with information from the data to hide. LSB algorithms have a choice about how they embed that data to hide. They can embed losslessly, preserving all information about the data, or the data may be generalized so that it takes up less space.

Position i = locate(cipher i , key blk) ,where

Position = { position i | 1 £ i £ length (M") | position, i Î{0,1,2,…, 2 blk -1}

The least significant bit is the right-most bit in a string. It is called that because it has the least effect on the value of the binary number, in the same way as the unit digit in a decimal number has the least effect on the number's value. The lsb also determines whether the given number is odd or even. The number 11100111 is an odd number, since it's lsb (1) is an odd number. If we use the term least significant bits (plural), we are commonly referring to the several bits closest to, and including, the lsb. Another property of the least significant bits is that they often change drastically if the number changes. For example, if we add 1 to our example number, 11100111, we will get 11101000. The result of this minimal addition is that the four least significant bits have changed their value.

C. Steganalysis

Steganalysis is the art and science of detecting a secret communication. Hiding a message will most likely leave detectable trace in the cover medium. The hiding information process changes the statistical properties of the cover, which is a steganalyst attempt to detect. The process of attempting to detect statistical trace is called statistical steganalyst.

One method for calculating this is compare each pixel (X,Y) to three adjacent pixels (X-1,Y), (X,Y-1) and (X-1,Y-1).

Histograms give a rough sense of the density of the data, and often for estimating the density estimating probability density function of the underlying variable. The total area of a histogram used for probability density is always normalized to 1

RS Analysis of Original Image(Red Green Blue)
Positive Regular 34.1888 33.3984 34.7443
Positive Singular 19.577 19.5984 19.9097
Negative Regular 35.4187 34.509335.3455
Negative Singular 16.3574 15.8447 16.7419

D. Genetic Algorithm [Embedding]

Genetic algorithm based steganogrpahy method incorporates simple LSB embedding technique to hide the data in an image. Each pixel in a 24bit color image is represented by three bytes where each byte represents the intensity of the three primary colours namely red, green, and blue (RGB),

respectively. The data is hidden randomly in the LSB of each byte of the pixels. The image considered for hiding secret data is a cover image and stego image is obtained by hiding the secret message in a cover image. This research work elucidates the implementation of genetic algorithm to protect the secret data against RS attack in color images. RS steganalysis classifies block flipping into three types. They are positive flipping F1, negative flipping F-1, and zero flipping F0. RS steganalysis analyses three primary colours namely red, green and blue individually for color images initially, the image is divided into several blocks. Subsequently, flipping functions such as positive flipping and negative flipping are applied on each block of pixels. Let RM denotes relative number of regular group and SM denote relative numbers of singular groups. According to the statistical hypothesis of the RS steganalysis

The genetic algorithm optimizes the image quality and security of the data. Each pixel in a block is considered as a chromosome. Some chromosomes are considered for forming an initial population of the first generation in genetic algorithm. Several generations of chromosomes are created to select the best chromosomes by applying the fitness function to replace the original chromosomes. Reproduction randomly duplicates some chromosomes by flipping the second or third lowest bit in the chromosomes. Several second generation chromosomes are generated. Crossover is applied by randomly selecting two chromosomes and combining them to generate new chromosomes. This is done to eliminate more duplication in the generations. Mutation changes the bit values in which the data bit is not hidden and exchanges any two genes to generate new chromosome. Once the process of selection, reproduction and mutation is complete, the next block is evaluated. The fitness function enables to optimize the value through several iterations. Fitness is calculated by the probability of regular and singular groups when positive flipping and negative flipping is applied. Ultimately, the stego-image undergoes RS analysis and the values between original and stego-image are compared. In this study, a chromosomes chromosome G in GA consisting of 2k genes can be described by a key permutation as G= g 0 g1 …g 2*K*-1, (18) where g0 represents the first element of the key,g1 represents the second element of the key, and so on. For example suppose k=3, then the chromosome length are 2^3 =8 and they can be represented.

E. Proposed GA:

1) Step 1. Initialization

Starting from the first pixel, select two pixels adjacent to each other in a row.

These are known as the initial chromosomes in the genetic terminology.

2) Step 2. Reproduction and Mutation

Flip the second lowest bits in the chromosomes randomly to generate the four possible chromosomes of the next generation.

3) Step 3. Selection

Select the best possible chromosome which maximizes the value of the flipping function

F=_.Prop[f-(Ci)<f(Ci)]+_.PSNR

Where and are positive constants. Also the Probability Prob[f-(Ci)<f(Ci)] must be greater than some threshold.

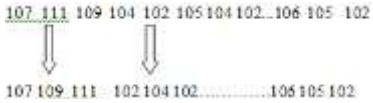
4) Step 4. Calculate the label of the adjusted image block using genetic algorithm. The block is successfully adjusted.

5) Step 5. Crossover. Shift the chromosomes one pixel, go to step 2. If crossover has been applied two times, stop the cycle.

6) Step 6. After a block is adjusted, calculate R ,R−, S and S− of the image. If the difference between R and R− is more than 5%, or the difference between S and S− is more than 5%, adjust the next block. Selection of two pixels adjacent to each other in a row for initial state.

F. Initialization:

At first, many individual solutions are randomly generated to form an initial population. As said before, we need to find the optimal adjustment list J in order to perform LSB matching so that the distortion of the stego image can be minimized. In the Genetic algorithm, the population represents the solution. Thus, for initialization, an initial population, P of chromosome, p1, p2… pn, is generated randomly.



G. Fitness Evaluation

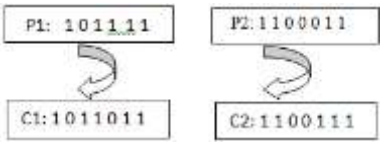
The fitness of each individual in that population is evaluated based on fitness function. The fitness value is length of displacement of pixels.

H. Parent Selection

After fitness evaluation, parents are chosen based on their fitness. During each iteration, a percentage of the existing population is selected (which is called parents) to create a new population. Parents are selected through a fitness-based process, where fitter solutions (as measured by a fitness function) are typically more likely to be selected and its used by the crossover and mutation operators to produce two offspring for the new population. In this work ,the roulette wheel is used for the selection procedure. In roulette wheel selection, individuals are given a probability of being selected that is directly proportionate to their fitness.

I. Crossover:

At first, a random number between 0 and 1 is generated and compared to a parameter called the probability of crossover, Pc. If the random number is larger than Pc, then two parents are chosen randomly from the population P, and the left and right parts of these two agents are exchanged. On the other hand, if the random number is not larger than Pc, then crossover will not happen. The crossover probability can be changed from 0.0 to 1.0. Our empirical studies have shown that better results are achieved by a crossover probability of 0.7, which implies that the probability of a selected chromosome surviving to the next iteration unchanged ranges from 0.3.



Mutation:

In the mutation procedure, a random number between 0 and 1 is generated and compared to a parameter called probability of mutation, Pm. If the random number is larger than Pm, then a gene is selected randomly from the current population, P, and the genes on this population are changed, e.g. 0 becomes 1 and vice versa. Then this mutated gene will be placed back into population of the current generation.

J. Generating a New Population

After the last three steps, new population is generated.

K. Stopping Criteria

The algorithm, previously described, carries out the steps one by one in sequence and when they have been performed it is said that one generation has passed. At the end of each generation Genetic algorithm checks stop criteria. Because of the nature of Genetic algorithms, most of the times it is not clear when the algorithm should stop, so the criterion is usually based on statistical information such as number of generation, fitness value of the best chromosome or average fitness value of chromosomes in the population, duration of evolution process and so on.

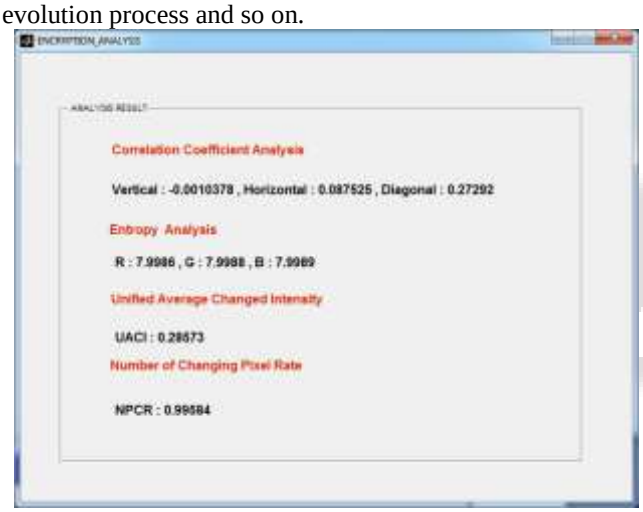


Fig. 1: Encryption Analysis

IV. Discussion and Analysis

A. Definition

The proposed method and the LSB hiding methods, hiding every bits of the secret message in one pixel of the image which usually chosen randomly therefore the secret message used in this paper has number of characters used to converted binary bits, to hide those bits have the certain number of pixels are needed. In this paper, the results of the proposed and LSB hiding methods are analyzed based on the ratio between the number of the identical and the non identical bits between the pixel color values and the secret message values. The resultant images and the analysis table which present the ratio success obtained by the proposed hiding method when applied on the a and b images respectively.

B. LSB Substitution

It is used for this techniques the position of the binary values are exchanged. So that method its very useful for image processing. The substitution method is very helpful for encrypted and hide the data or image to extract the correct position of that image. Here The genetic algorithm used for find the best pixels to the embedded. The best pixels calculated based fitness values. The fitness value is length of displacement of pixels. After crossover function preformed and sometimes process of the mutation is a modify the pixels.

Fig. 2: Encrypt Based on RGB Colour

Fig. 3: Embedded image in Cover Image

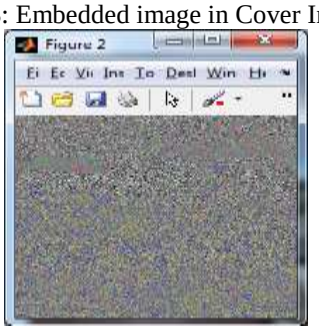


Fig. 4: Extra Image[LSB SUBSTITUTION]

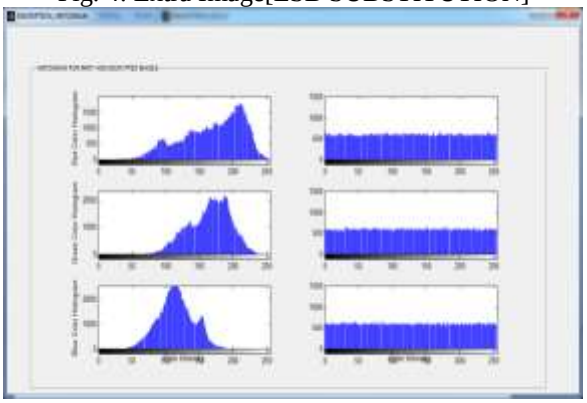


Fig. 5: Evaluation Based on Histogram

V. CONCLUSION AND FUTURE WORK

Steganography is the art of secret communication. It is the science of hiding a message in such a way that only sender and recipient are aware of existence of the message. The main advantage of steganography is that it will not attract the attackers. The RS analysis is one of the strongest steganalysis, which detects the secret message by the statistical analysis of pixel values. The objective of this paper is to establish a highly RS-resistant secure model with steganography method using Genetic algorithm. It enables to achieve security and enhance image quality. In this method, the pixel values of the stego image are modified by the genetic algorithm to retain their statistical characteristics. Thus, it is difficult to detect the existence of the secret message by the RS analysis. Further, implementation of this approach enhances the visual quality of the stego image. the length of the secret message increases, the probability of detection of secret message by RS analysis also increases. However, our future work focus upon the improvement in embedding capacity and further improvement in the efficiency of this method.

REFERENCES

[1] J. J. Chae and B. S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients," University of California, Santa Barbara, CA 93106.
[2] Yun Q. Shi, "Reversible Data Hiding," New Jersey Institute of Technology, Newark, NJ 07102, USA.
[3] Kamrul Hasan Talukder and Koichi Harada, "Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image,"
[4] Musbah J. Aqel , Ziad A. Alqadi , Ibraheim M. El Emary, "Analysis of Stream Cipher Security Algorithm," Journal of Information and Computing Science, ISSN 1746-7659, vol. 2, no. 4, 2007, pp. 288-298.
[5] S.Imaculate Rosaline, C. Rengarajaswamy, "A Steganographic Substitution technique using APPM for encrypted pixels,".
[6] Sapna Sasidharan and Deepu Sleeba Philip, "A Fast Partial image Encryption Scheme with Wavelet transform and RC4," International Journal of Advances in Engineering & Technology,.©IJAET ISSN: 2231-1963.
[7] Manikandan R, Uma M, "Reversible Data Hiding for Encrypted Image," Journal of Computer Applications ISSN: 0974 – 1925,vol. 5, Issue EICA2012-1, February 10, 2012
[8] C.Rengarajaswamy, K. Vel Murugan, "Separable Extraction of Concealed Data and Compressed Image,".
[9] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, pp. 1129–1143, 2009.
[10] L. Luo et al., "Reversible imagewatermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.
[11] 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.
[12] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996.
[13] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct.2010.

