Distortion Free Steganographic System Based on Genetic Algorithm

Heshem A. El Zouka
Department of Computer Engineering, College of Engineering and Technology
Arab Academy for Science & Technology and Maritime Transport,
Alexandria, Egypt

helzouka@aast.edu

Abstract — **Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. The research work in this paper shows that most of the steganographic systems proposed during the past decades usually substitute the insignificant parts of the image with the secret message. However, these systems don't pay attention to these parts, and the original image is distorted by some small amount of noise due the data embedding itself. This noise could reveal the existence of secret message and hence change the statistical profile of the cover image significantly. A simple attack such as Laplace filtering can exploit this fact and make the system detectable by the eavesdropper. In attempt to minimize the error introduced due to hiding foreign message into the cover image, a genetic algorithm approach will be employed efficiently in this paper in a way that examine the embedded bits. This has the advantage that the image remains nearly unchanged.**

Keywords - Security; Watermarking; Steganography; Information Hiding; Genetic Algorithm.

I. INTRODUCTION

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. By embedding a secret message into a digital image, a stego-image is obtained. It is important that the stego-image does not contain any easily detectable artifacts due to message embedding that could be detected by eavesdropper. There are many different steganographic methods that have been overviewed and analyzed by many researchers over the last few years. However, one common drawback of all current data embedding methods, is the fact that the original image is distorted by some small amount of noise due the data embedding itself. This noise could reveal the existence of secret message and hence, weakness the security value of the applied steganography method.

In this paper, we investigated most of the steganography methods which are based on substitution systems and have been proposed in the last few years. After analyzing the drawbacks in the analyzed steganography systems, we propose a steganographic system, which is based on genetic algorithm technology. The proposed system maintains such noise in a way that makes the transmitted signal undetectable. In addition, we built the software programs that provide the simulation results including the histograms of both the cover images and the stego images, and the variance between them. Also, the simulation results for all equivalent substitution techniques, which covered in this paper, are used here for comparisons purpose.

II. RELATED WORK

There are many different steganographic methods that have been proposed during the past decades. Most of the simple techniques can be broken by careful analysis of statistical properties of the channel's noise [1]. In substitution steganography technique [2], one can notice that: this method substitute insignificant parts of the image, e.g., the noise component of the cover with the secret message. These parts have specific statistical properties and the embedding process usually does not pay attention to them, and consequently change the statistical profile of the cover significantly. A simple attack such as "Laplace filtering" [3] can exploit this fact and detect the use of the steganographic system. In addition, these systems are extremely sensitive to cover modification and the attacker, who is not able to extract or prove the existence of a secure message can add a random noise to the transmitted cover in attempt to destroy the secret message.

Meanwhile, most of these stenography systems have a vital drawback, which is that the system doesn't discard image blocks where the desired relation of DCT coefficients for example [4] cannot be enforced without severely damaging the image data contained in this specific block. TCP/IP packet headers [5], [6] can also be reviewed easily. For example, firewall filters are set to test the validity of the source and destination IP addresses. Those filters can also be configured to catch packets that have information in supposed unused or reserved space. Based on the analysis of spread spectrum techniques [7], it can be observed that phase coding provide robustness against resembling of the carrier

 ISBN: 978-1-61208-100-7

signal, but at the same time it has a low data transmission rate. These techniques have a problem with the absolute phase of all following segment that followed the first modified one, since all of them will have a change that could be noticeable to the attacker. Moreover, at the receiver end; the embedding process is reversed and image restoration technique such as adaptive Wiener filter [8] is needed to estimate the original image.

III. SECURITY IMPLICATIONS AND SOLUTIONS

The proposed technique in this paper distorts the image insignificantly by making small modifications over a large number of pixels. We spread the secret message over a large area of cover image to produce a small modification on the carrier media. The new approach combines both Genetic approach and steganography to exchange secret messages in a way that it's impossible to discover without the knowledge of the cover image and the genetic algorithm that have been used.

Firstly, the image is divided into blocks and the parity bits from each block b1, b2,..,bi are computed and encoded with the corresponding bits in the text file which contains the secret message. The process is repeated for the whole selected blocks. If the computed parity bit pi and the secret bit mi are equal, then the encoded bit is zero and if the 2 input bits are different, then the output is one. Finally, the encoded bits are lined up to reconstruct the encoded file. Now, the file is ready to be encrypted and sent in any insecure channel to the receiver who had both, the secret key and a copy of the cover image which has been used. Therefore, the receiver of the encoded message will decipher the message using his secret key and the shared cover image.

3.1 ENHANCED EMBEDDING SOLUTION

After the encoding process had taken place, the output file was encrypted and sent directly to the other party as a cipher file. However, instead of sending an encrypted stream of bits, an alternative scheme can be adopted by injecting the stream of bits back to the cover image with a probability of 50% of changing the LSB of embedded pixels in target blocks using a fitness function. Our goal here is to embed one bit of the secret message m_i into one block of the cover image C, where C is composed of all the blocks {b1, b2,….,bi}, and since length of the message L(m) is less than the number of the target blocks N(b) the rest of the image can left unchanged. Moreover it's possible to select only some blocks bi in a rather random manner according to a secret key and leave the other unchanged. Therefore, the idea depends on spreading the secret message over the cover image using both a pseudo random number generator (PRNG) and a fitness function [9] that specifies one bit from each block of pixels randomly as follows:

$$P(I) = \sum_{j \in i} LSB(b_j) \bmod 2 \quad (1)$$

If the parity bit of one cover block bi doesn't match with the secret bit mi, the proposed genetic model will flip the LSB of one pixel in the block in attempt to make p(Ii) equals to mi and according to the employed fitness function which minimize the noise introduced to stego image as a result of embedding foreign bits of the secret message. Studying the properties of pixels surrounding the target pixel in a certain block by invoking a statistical fitness function that examine the number of 1's or 0's inside the chosen block will conceal the very existence of hidden information inside the stego image

3.2 EMPLOYED GENETIC ALGORITHM

Before communication starts, both sender and receiver have to agree on the location of the target blocks bi using a shared key value as the seed to a known PRNG algorithm. Each seed number can generate a set of random numbers, each of which allocates different locations of the blocks within the cover image. These blocks will be used as subjected pixels, from which the parity bits P(bi) are computed. The stego image file is then sent directly to the other parity with the encoded parity bits as mentioned before. The embedding process is preceded by extracting the parity bit through a reverse process to reconstruct the transmitted-hidden secret message.

However, the genetic algorithm is used to minimize the error due to hiding the foreign message carrier into cover images. The method is based on statistical analysis of images and their values are varying according to the applied key (seed) number. This is done by studying the neighboring pixels surrounding the chosen bit and changing its value to match the adjacent one in a way that prevent any statistical tracing. The Lina cover image in Figure 1 provides special features and will be used in this research work as a test image.

Figure 1. Lina Cover Image

The Genetic algorithm proceeds by dividing the image into blocks of 8*8 pixels and chooses the blocks in sequence according to a given seed number. The intensity of each

 ISBN: 978-1-61208-100-7

pixel x[i][j] within the chosen blocks is predicted according to the value of pixels in a specific neighborhood. Hence, the difference between the intensity of each pixel and its adjacent pixels is calculated as follows:

$$out[i][j] = in[i][j] - \frac{1}{64}\sum_{i:1-8}\ \sum_{j=1-8} x[i][j] \qquad (2)$$

where x[i][j] represents the pixel coordinates in the selected block region bi. For each tested pixel in the block, the average weighted sum of the surrounding pixels is computed and compared with the target pixel.

IV. IMPLEMENTATION AND DESIGN

In this section we will show how the Genetic algorithm is employed to search for suitable pixels within the blocks which by changing their least significant bits (LSBs) will introduce a lesser embedded noise to the stega image. If the system fails with one pixel within the target block another offspring is generated. The matching process will start over again till the program is succeeded in finding the flipped LSB which introduce lesser cost compared with the suggested noise threshold value. The genetic algorithm (GA) will finish the task either when it successfully finds the appropriate matched threshold value, or the closer one using different seed numbers. Finally, the program will print out the largest match between the generated offspring and the threshold value in a way that fulfil the objective of steganography which is concealment of existence. The whole proposed Genetic algorithm is illustrat6ed in the following statements:

4.1 MODEL DESCRIPTION

Chosen the target pixels in the selected blocks is a classic case of a combinatorial optimization problem. The intensity of each pixel is associated with a cost Cij. The cost of pixels is varying according to difference between the target pixels and the weighted sum of the surrounding pixels within one block. The objective is to obtain a solution with a minimum cost in terms of intensity difference and for each computed offspring; the elapsed time is computed in the provided searching algorithm. If n is the number of pixels in each tested block, then, the GA which has a behavior of cyclic approach will search for the fittest and optimal solution obtained by n!. It will be a huge number as the size of the block is increased, so the complexity of searching for the appropriate pixel within the block will not be suitable at all. However, the full optimality is not an a objective behind this paper. The employed genetic algorithm can be classified into 2 main parts based on the algorithm proposed recently by Ray et al. [10], which is called the modified order crossover (MOC) which in turn based on the order crossover (OCX) for solving Travelling Sales Person (TSP) problem [11]. The authors of these two algorithms used a new operation called the Nearest Fragment (NF) Heuristic and thy referred to their GA as (FRAG_GA). In addition the authors compared their results with other GA's that use different crossover methods, such as SWAP_GATSP [12] and OX_SIM [13]. We decided to choose an adaptive Ray et al. method on selecting the most suitable pixels in the target blocks which are subjecting to change in attempt to change the computed parity bit of each block separately. The adaptive algorithm is based on two main parts; swapped inverted crossover mechanism and the Fitness function as illustrated in the following sections.

4.1.1 SWAPPED INVERTED CROSSOVER

The main idea behind swapped inverted crossover (SIC) genetic algorithm is to find a better pixel on which its LSB is subject to change and introduce a minimum distortion to the image. The most suitable pixel will be chosen according to the crossover criteria which are based on the computed cost: difference between the intensity of the tested pixel and the weight sum of its neighborhood. Hence, the most suitable pixels from the target blocks are chosen with minimum introduced artifacts. The process is repeated with different seed numbers to all blocks populations in the tested image in attempt to calculate minimum value of all costs (Cij). The process of applying one, two, or both cutting points on the formulated population is illustrated in the following steps:

1. One point SIC - This is can be done by selecting on crossover point randomly to cut on. Suppose the two parents and a cut point from parent 1 is 4:
   a. Parent1 (1 2 3 4 5 6 7 8 9)
   b. Parent2 (5 1 4 6 8 9 2 7 3)

   where these numbers represent the cost of each pixel found in the target block for a given seed number.

2. The head of Paent1 will be flipped to be 4 3 2 1. By removing these point from Parent 2; the remaining pixels on parent 2 will be 5 6 8 9 7 to produce O1 and O2 offspring:

   O1 (4 3 2 1 5 6 8 9 7)
   O2 (5 6 8 9 7 4 3 2 1)

3. Doing the same procedure with parent 2, as cutting on point 6 and flip the head to be 6 4 1 5. Then removing these points from parent one. Similarly, by alternating output of parent 2 the offspring O3 and O4 will be generated:

   O3 (6 4 1 5 8 9 2 7 3)
   O4 (8 9 2 7 3 6 4 1 5)

4. The processes will continue until examine all generated outputs O5,O6, O7, and O8.

5. Two points SIC – where each parent will be cut to three pieces (head, middle, and tail) using two cut points (P1 and P2). For example 4 and 6 on parent1 & 6 and 9 on parent 2:
   Parent1 (1 2 3 4 5 6 7 8 9)
   Parent2 (5 1 4 6 8 9 2 7 3)

6. By flipping the parent 1 head to be 3 2 1 and flipping parent 1 tail also to be 9 8 7 to produce :
   O9 (3 2 1 4 5 6 7 8 9)
   O10 (7 8 9 4 5 6 3 2 1)

7. The same thing happens with the second parent producing O11 and O12.

4.1.2 THE FITNESS FUNCTION

After generating the above 12 offspring (O1 to O12) , the fitness function runs sequentially on all populations of the chosen blocks and the suitable pixels which are subjected to change with minimum cost can be chosen based on the following algorithm:

```
---------------------------------------------------------------------
i = 1
S0 = S
max = 0
while i <  n-1
      if Ci,j+1 > max
            Begin
                  max = Ci,j+1
                  x = i
            End
S1 ← swap pixelx with pixel1
S2 ← swap pixelx with pixel Lx; where L is the left pixel
.....
S8 ← swap pixelx with pixeln
S  ← max ( S0, S1,.....,S8)
Return S
End
---------------------------------------------------------------------
```

Clearly, the matching process will run, comparing the extracted parity bits with the embedded secret message bits. Therefore, this operation will be applied to the selected parents that will be copied several times. Each copy is then mutated using a different seed number with suitable neighbor pixels. The process proceeds till we find the minimum of these switching criteria and exchange it to match the original embedded bit. This operation is undertaken on one of the selected seed after the mutation operation is performed to produce the most suitable pixel which is subject to change and hence no statistical artifacts are introduced to the image. Using the same cover image, the recipient will treat each block separately by running the same algorithm reversely until the secret message is extracted.

A further improvement is possible if the sander and recipient generate a number of cover images to be verified with the embedded messages. By doing this we can minimize the searching time of the fitness function by about half, and increases the probability of finding the closest matches with the suggested threshold noise value. Therefore, the two communicating parties can agree on which group of images they are going to use. This method guaranteeing that a minimum changes will be detected within the image that hold the information. Although the idea is attractive in that it allows a smaller message to be hidden in the cover image without changing the image significantly, the difficulty is that the complexity of time and space will be increased exponentially if the number of the pixels in the subjected block is doubled. However, our aim is not to increase the block size, but to increase only the length of the embedded message, which will be achieved by increasing the number of blocks within the image and hence reducing the blocks sizes. On the other hand, a compression technique could be employed and allow us to compress the transmitted message even further more.

V. SIMULATION RESULTS

The simulation results showed that the text message could be embedded with a non noticeable degradation of the image. Studying the histogram of Laplace filter in Figure 2 for the provided lena image, we notice that on average, the amount by which the image is modified is smaller than some known substitution embedding systems that we investigated in this research work.

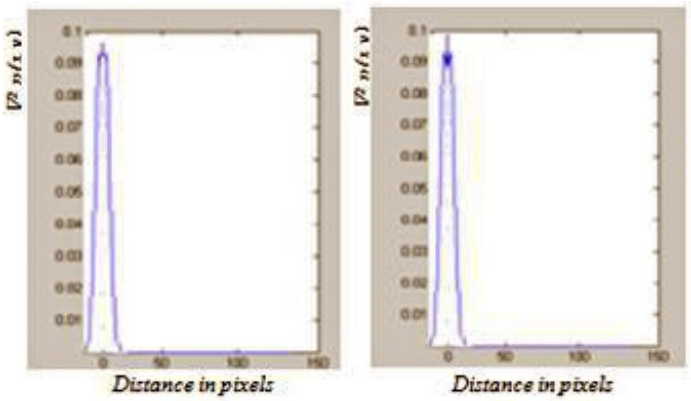

Figure 2. Laplace Filter : (a) the Cover Image (b) The Stego image

For example, comparing the distortion introduced by PGMStealth [1991] and the new technique, we can clearly see that the new technique provides visibly fewer and less peaks than PGMStealth filtered histogram which has a wider band and many peaks clustered around zero as shown in Figure 3. Also comparing our results with the experimental results obtained by other Genetic watermarking algorithms such as Shieh et al. [14], we see that our proposed method

greatly minimizes the effect of the noise caused by the embedding process itself, since it has the ability to keep and refine the results within the selected regions; identifies the one of the most suitable pixels corresponding to the marks placed on the image and allow choice of the correct settings to the threshold healthy pixels**,** and thus making the watermarked image perceptually similar to the original one.

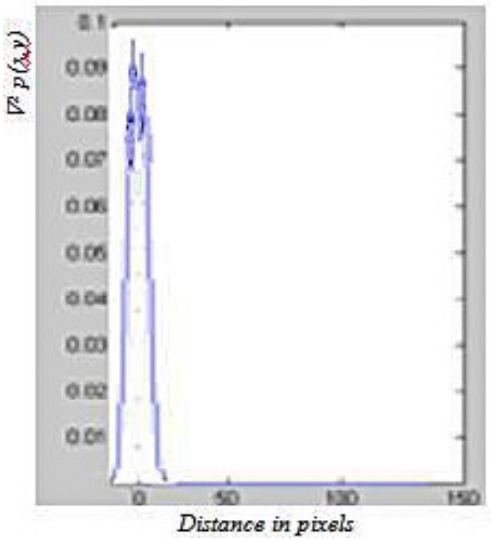

Figure 3. Laplace Filter of PGMStealth Stego Image

5.1 CONSIDERATION OF VALIDITY

Consider a message that is intended to be transmitted using an embedding process based on genetic algorithm. Without losing generality we may consider this to be a sting of n bits. We also require an appropriate fitness function that embed one bit in one block of the cover image such that the number of blocks exceed the length of the message itself (L). Using a seed of length l bits and a random number generator to identifies the target blocks in the cover image where l << number of blocks. This idea is attractive in that it allows short messages to be embedded within a cover image without introducing any noticeable noise in the stego image. The communicating stego image will also be meaningless to the attacker unless he knows both the entire random number generator, fitness function, and the original cover image. In this approach we use the seed number to generate a sequence of numbers representing the target blocks in the cover image where the parity bits are computed. The parity bits are compared to the stream bit sequences of the secret message. The difficulty with this approach is that the results obtained from the experiments we ran that the longest match between the message and the obtained parity bits was nearly within the ratio of one half. Therefore by changing one least significant bit in the pixels contained the target block will flip the value of the computed parity bit and hence match the subjected message bit. Using a genetic algorithm equipped with a fitness function allowed us to select the appropriate pixel within the block which introduces a minimum cost compared to suggested threshold noise value. Thus enhancing the security value of the whole system by improving the and the statistical properties of the stego image significantly. Moreover if we use a block size of 8x8 pixels, there is a one in 64 chance of finding one LSB that complementing its value will match the fitness function. However, to improve this ratio with larger block size, the chance embedding large messages will be reduced accordingly. In addition the searching time could be increased by nearly 100 times compared to the smaller block size as the experimental results showed.

5.2 ATTACKS ON THE GENETIC BASED ALGORITHM

The effort the attacker needs to break the proposed system will not rely only on discovering which fitness function has been used or which number generator method has been applied to select the target blocks where the embedding process had take place, but also on which cover image the two communicating parties are sharing. In addition, the sender will send the seed number to the recipient either encrypted or hidden into another unimportant cover image, which if discovered and applied to the transmitted stego image, the extracted information will be useless. Only the recipient who has the security knowledge of both the stenographic system and the true cover image, which is shared in advance, will be able to extract the true message information using a reverse embedding process.

VI. CONCLUSION AND FUTURE WORK

In this paper we proposed a new steganography algorithm that uses a Genetic algorithm and a random number generator to produce minimum distortion free images from the original ones. The results of the proposed approach showed that the encoding process distorted the image insignificantly by making small modifications over large numbers of pixels. The algorithm divides the image into small blocks that are analyzed for parity check values equivalent to the embedded bit. The technique was designed with the intent of maximizing the quality of the stego image by the aid of fitness function that introduced extremely small modification to the cover images. Initial investigations showed that this modification was difficult to detect visually, and there is no tell-tale artifact could be picked up during the investigation process. In order to compare the provided approach with other established methods, many stego-analysis techniques were investigated and applied to the stego image. Testing our proposed steganographic algorithm's using the adaptive fitness function, we found that the stego image does not show any artifacts and thus, it gives no indication that the image contains any hidden

 ISBN: 978-1-61208-100-7

information. Comparing the Laplace filter histogram for the provided cover image with the one which contains the embedded message, we noticed that on average, the amount by which the image is modified is smaller than other known substitution steganographic systems that we investigated. Looking at the pixel repetition histogram of the stego image and comparing it with the histogram of the original image, it can be observed that there are only very small differences between them, and there are a few fine lines distributed over some parts of the histogram. For the future work we recommend that the cryptography methods should be taken more seriously into account in order to design a more successful steganographic system and in an attempt to provide a secure function to the steganography process. In addition to make the communication even more secure, we recommend that the secret message should be compressed or encoded before the encryption process takes place. This is important because in this way we will minimize the amount of information that is sent, and hence minimizing the chance of degrading the image.

VII. REFERENCES

1. E. Franz. Steganography preserving statistical properties, proceeding of the 5th internationally Workshop on information Hiding, Noordwijkerhout, The Netherlands, October 2002, LNCS 2578, pp. 278-294, Springer 2003.

2. Fabien A. Petitcolas, R. J. Anderson, and M. G. Kuhn, Information Hiding- A Survey, Proceedings of the IEEE, vol. 87, no.7, pp. 1062-1078. Jul. 1999.

3. A. Heurtas and G. Medioni, Detection of Intensity Changes with Subpixel Accuracy Using Laplacian- Gaussian Masks, IEEE Transactions on pattern analysis and machine intelligence, vol. pami-8, no. 5, pp. 651-664, September 1986.

4. R. Anderson, R. Needham, and A. Shamir, The Steganographic File System, in Proceedings of the Second International Workshop on Information Hiding, vol. 1525 of Lecture Notes in Computer Science, Springer, pp. 73-82 , 1998

5. D. Piscitello and A. Chapin, Open Systems Networking: TCP/IP and OSI, Addison-Wesley, Reading, Massachusetts, **pp**. 582-596, 1993.

6. Joseph J. K. Ó Ruanaidh and Gabriella Csurka, A Bayesian Approach to Spread Spectrum Watermark Detection and Secure copyright protection for Digital Libraries. IEEE Conference on Computer Vision and Pattern Recognition (CVPR'99), Vol. 1, pp. 207-212, Fort Collins, Colorado, USA, 23-25 June 1999.

7. A. Westfield and A. Pfitzmann, "Attacks on steganographic Systems". 3rd International Workshop on. Information Hiding, Dresden, Germany, pp. 61-75, September 1999.

8. M. Peyravian, A. Roginsky, and N. Zunic, Hash-Based Encryption System. Computers & Security Vol. 18, No.4, pp. 345-350 , 2003.

9. The USC–SIPI. Image database, Signal & image processing Institute, Electrical Engineering Department, University of Southern California. <URL: htpp://sipi.usc.edu/database/>, May 10, 2010.

10. M. Kwan, How gifshuffle works, Technical report, Helsinki University of Technology, Full-text, June 2004. < URL: http://www.darkside.com.au/gifshuffle/description.html>

11. P. Borovska., "Solving the Travelling Salesman Problem in Parallel by Genetic Algorithm and Multicomputer Cluster", International Conference on computer Systems and Technologies, pp. 421-430, 2006.

12. S. Ray, S. Bandyopadhyay and S. Pal, "New operators of genetic algorithms for traveling salesman problem" Cambridge : icpr, vol. 2, pp. 497-500, 2004, Vol. 2.

13. E. Lawie, "Combinatorial Optimization; Networks and Moatroids"., Holt, Rinehart, and Winston, New York, pp. Full-text, 1976.

14. Shieh, C., et al., Genetic watermarking based on transform domain techniques. Pattern Recognition, vol. 37, no. 3, pp. 555-565, 2004.

 ISBN: 978-1-61208-100-7