Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Genetic Algorithm Based Image Steganography for Enhancement of Concealing Capacity and Security

Abhishek Tripathy, Dinesh Kumar

Dept of Computer Science & Engineering

Shekhawati Institute Of Engineering & Technology

Sikar, Rajasthan (India)

Abstract— This paper proposes a Genetic Algorithm based steganography for enhancement of embedding capacity and security. Steganography is a method to provide secret communication between sender and receiver by concealing message in cover image. LSB bit encoding method is that the simplest encoding method to cover secret message in color pictures and grayscale pictures. Steganalysis is a method of detecting secret message hidden in a cover image. RS steganalysis is one of the most reliable steganalysis which performs statistical analysis of the pixels to successfully detection of hidden message in an image. This paper presents a secured steganography method using genetic algorithm to protect against the RS attack in color images. The proposed steganography scheme embeds message in integer wavelet transform coefficients by using a mapping function. This mapping function based on GA in an 8x8 block on the input cover color image. After embedding the message optimal pixel adjustment process is applied. By applying the OPAP the error difference between the cover image and stego image is minimized. Frequency domain technique is used to increase the robustness of proposed method. Use of IWT prevents the floating point precision problems of the wavelet filter. GA is used to increase the hiding capacity of image and maintains the quality of image. Experimental results are shows that the proposed steganography method is more secured against RS attack as compared to existing methods. Result showed that Peak signal to noise ratio and image utilization, 49.65 db and 100% respectively.

Keywords— Steganography, Integer Wavelet Transform (IWT), Genetic Algorithm (GA), RS Analysis, Selection, Mutation, Crossover, Mean Square Error (MSE), Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Utilization, Embedding Capacity.

I. INTRODUCTION

The standard and thought of "What You See Is What You Get (WYSIWYG)" which we have a tendency to encounter typically while printing images or other materials, is not any longer precise and wouldn't fool a steganographer as it does not always hold true. Images are over what we see with our Human Visual System (HVS); therefore, they can convey over 1000 words [1]. Steganography, the art of hiding messages inside other messages, is now gaining more popularity and is used on various media such as text, images, sound, and signals. However, none of the existing schemes can yet defend against all type of detection attacks. Using Genetic Algorithms which based on the mechanism of natural genetics and the theory of evolution, we can design a general method to guide the steganography process to the best position for data hiding [2].

In recent years, many productive steganography strategies have been proposed. Among all the strategies, LSB (least significant bit) replacement technique is wide used due to its simplicity and huge capacity. The bulk of LSB steganography algorithms embed messages in spatial domain, such as BPCS, PVD. Some others, such as Jsteg, F5, Outguess, embed messages in DCT frequency domain (i.e. JPEG images). In the LSB steganography, secret message is regenerate into binary string. Then the least significant bit-plane is replaced with the binary string. The LSB embedding achieves smart balance between the payload capability and visual quality. However, the LSB substitution method flips one half of the least-significant bits. So the artifacts in the statistics of the image area unit are easy to be detected [2].

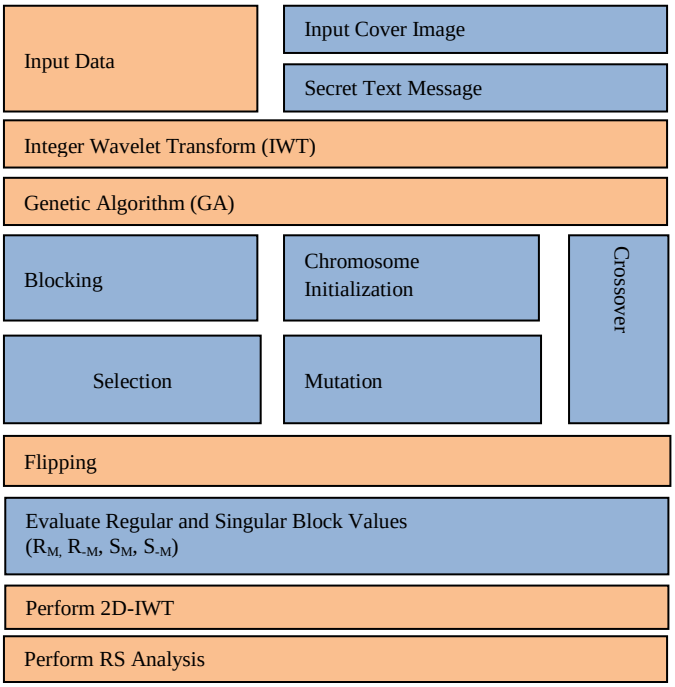
II. RELATED WORK

A. Elham Ghasemi, Jamshid Shanbehzadeh and Bahram ZahirAzami, A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm, 978-1-4244-9799-7/111$26.00 ©20 11 IEEE [3].

B. R.O., El.Sofy, H.H.Zayed, An adaptive Steganographic technique based on the integer wavelet transforms 978-1-4244-3778-8/09/$25.00 ©2009 IEEE [4].

© 2014, IJARCSSE All Rights Reserved

III. PROPOSED SYSTEM ARCHITECTURE



The above mentioned figure represents the general system functionalities of the developed algorithmic rule. The general system operate can be summarized by observant the figure mentioned above. The figure represents the real operative steps of the developed style. In the processing the program helps so as give a program to handle the developed model and to access the developed module. At the origination, the cover image is selected for embedding the information. Then the text data or the message is to be hand-picked so, so as to accomplish the motive of steganography the stego key appointed so at the opposite terminal the information can be retrieved by the key. Once the Key has been provided, the real application development for the RS analysis will be started with the assistance of strong GA improvement. In this technique at first the message is to be embedded in cover image. Genetic algorithmic rule is enjoying an important role for embedding more and more data in the image. In the architecture of the developed system the integer to integer wavelet transform has been done. Once the information has been embedded into the image file, then when embedding the image is again recovered so it's now able to be transmitted over the channel. On the opposite hand at the receiver terminal or the extraction terminal with the accurate assignment of the stego key the information is retrieved accurately.

IV. PROPOSED ALGORITHM

A. *Data embedding algorithm*

The proposed method for data hiding comprises of the following steps:

1. Take the input standard cover image.
2. Take the secret text message.
3. Apply the secret key (in digits only).
4. Perform the Integer Wavelet Transform of the input cover image using lifting scheme.
5. Add primal ELS to the lifting scheme.
6. Perform integer lifting wavelet transform on image.
7. Divide the input cover image in 8*8 blocks.
8. Select any of the wavelet coefficients (redundant coefficients) from the obtained high frequency coefficients.
9. Generate 64 genes containing the pixels numbers of each 8x8 blocks as the mapping function.
10. Initialize empty matrix to store the wavelet values.
11. Obtain 8 x 8 blocks for R G B.
12. Concatenate all coefficients together.
13. Store the coefficient in new image.
14. Embed in K-LSBs IWT coefficients each pixel according to mapping function.
15. Select any one of the pixels from RGB.
16. Now the selected coefficients are processed to make it fit for modification or insertion.
17. Fitness evaluation is performed to select the best mapping function.
18. The secret message plus the message length is embedded into this processed coefficients.
19. This modified coefficient is now merged with the unmodified coefficients.
20. Calculate embedded capacity.
21. Apply Optimal Pixel Adjustment Process on the image.
22. Convert image to binary.

© 2014, IJARCSSE All Rights Reserved

23. Finally, the inverse 2D-IWT on each 8x8 block is applied to obtain the Stego image.
24. Stego image will be obtained.

B. *Data extraction algorithm*

The proposed method for data extraction comprises of the following steps:

1. Take the desired stego image.
2. Apply the secret key same as given in embedding process.
3. Divide the stego image into 8x8 blocks.
4. Extract the transform domain coefficient by 2D IWT of each 8x8 block
5. Find the pixel sequences.
6. Select the desired pixels to process it.
7. Extract K-LSBs in each pixel.
8. Process the selected pixels coefficient to make it fit for extraction.
9. Now extract the message length and the secret message from these processed coefficients.
10. Secret message will be obtained.

C. *RS-analysis algorithm*

The proposed method for RS analysis comprises of the following steps:

1. Create function for non-positive flipping (F-)
2. Create function for non-negative flipping (F+)
3. Change LSB as per flipping
4. Initialize Relative number of regular block after positive flipping (R+) = 0;
5. Initialize Relative number of Singular block after positive flipping (S+) = 0;
6. Divide Stego Image into 8 x 8 blocks
7. For a modified block B, apply the non-positive flipping F_- and the non-negative flipping F_+ on the block. The flipping mask M_+ and M_- are generated randomly. The result is B'_+ and B'_-.
8. Estimate F (B'_+), F (B'_-) and F (B).
9. Iterate step 1 and 2 for 1000 times. Define four variables to categorize the blocks by comparison of F (B'_+), F (B'_-) and F (B).
10. Calculate cumulative correlation (C)
11. Calculate correlation for non-positive flipping (Cn)
12. Calculate correlation for non-negative flipping (Cp)
13. Estimate P_{+R}, the count of the occurrence when the block is regular under the non-negative flipping.
14. Estimate P_{+S}, the count of the occurrence when the block is singular under the nonnegative flipping.
15. Estimate P_{-R}, the count of the occurrence when the block is regular under the non-positive flipping.
16. Estimate P_{-S}, the count of the occurrence when the block is singular under the non-positive flipping.
17. If Cn>C
18. Increase P_{-R}
19. $P_{-R} = P_{-R} + 1$
20. Else
21. Increase P_{-S}
22. $P_{-S} = P_{-S} + 1$
23. If Cp>C
24. Increase P_{+R}
25. $P_{+R} = P_{+R} + 1$
26. Else
27. Increase P_{+S}
28. $P_{+S} = P_{+S} + 1$
29. Compare P_{+R} to P_{+S} and P_{-R} to P_{-S}, and therefore the labels of the block are determined
30. If $P_{+R} / P_{+S} > 1.8$
31. Label of the block 'R+'
32. If $P_{+S} / P_{+R} > 1.8$
33. Label of the block 'S+'
34. If $P_{-R}/P_{-S} > 1.8$
35. Label of the block 'R-'
36. If $P_{-S} / P_{-R} > 1.8$
37. Label of the block 'S-'
38. At last, the blocks are categorized into 4 groups R+R−, R+S−, S +R−, S +S−
39. Reject the block which doesn't fall in Step 38
40. Use genetic Algorithm for minimizing R- block

The blocks, which are not included in the 4 categories, are not processed in following steps. Compared with the cover image, the amounts of (R+ R−) and (S+ R−) blocks are increased in the stego-images. This phenomenon can be detected by the steganalysis method RS analysis. The final target of the proposed algorithm is to decrease the amount of R− blocks. Therefore genetic algorithm is deployed to adjust them to maintain the visual quality of image as in follow section.

© 2014, IJARCSSE All Rights Reserved

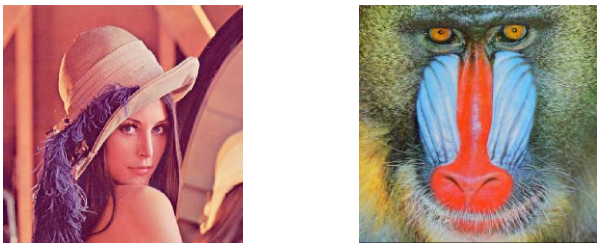
D. *Optimization technique or genetic algorithm*

The proposed method for genetic algorithm comprises of the following steps:

1. Perform Chromosome Initialization Steps.
2. Select every 3 adjacent pixels in the block
3. Initialize maximum Fitness as 0
4. Initialize Alpha as 0.88
5. Flip second lowest bit randomly for number of time
6. For kk = 1: length (Block)-2
7. Chrom = Block (kk:kk+2);
8. Cp = non_negative_flipping (Chrom);
9. Cn = non_positive_flipping (Chrom);
10. Initialize e1 and e2 as 0
11. Compute Correlation (C, Cn, and Cp)
12. If Cn<C
13. e1 = 1;
14. End
15. If Cp > C
16. e2 = 1;
17. End
18. Apply PSNR = SNR (Chrom-Cn); // See Line-7
19. Apply FITNESS = alpha*(e1+e2) +PSNR
20. If fitness>maxfitness
21. maxfitness = fitness;
22. Chrommax = Cp;
23. crossover = crossover+1;
24. End
25. Replace chromosome with new one
26. Compute P_{-S} and P_{-R}
27. If $P_{-S} > P_{-R}$
28. Block is successfully adjusted
29. End
30. Compute difference, diff1 = $P_{+R} - P_{-R}$
31. Compute difference, diff2 = $P_{+S} - P_{-S}$
32. If diff1>0.05*diff2
33. Adjust the next block

In the proposed technique, the blocks are labeled before the adjustment. Thus, the computational hardness is reduced. The use of the genetic method avoids the exhausting searching and the algorithm is easy to be implemented.

IV. EXPERIMENTAL RESULTS ANALYSIS AND DISCUSSION



a) Lena Image (JPG, 512x512) b) Baboon Image (JPG, 512x512)

Fig. 1 Input Cover Images

Figure 2 show the histogram of input cover images. Now the various algorithms such as data embedding, RS analysis and genetic applied on the cover images. The output stego image histogram after embedding the data is represented in Figure 3.

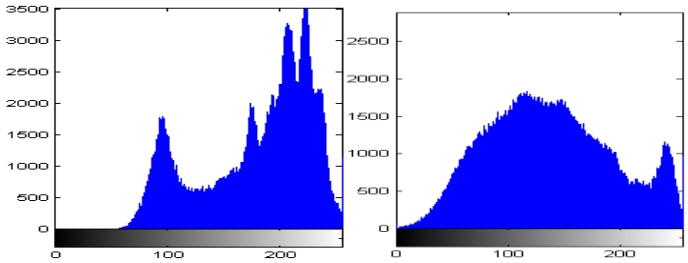
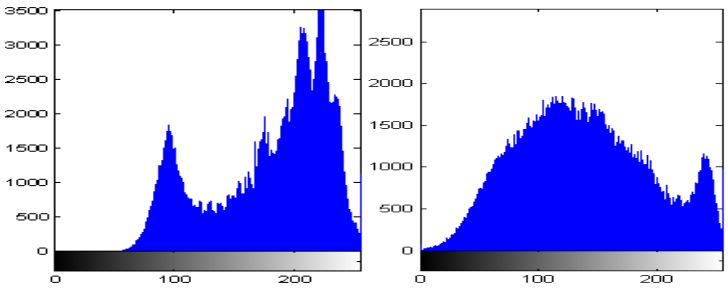
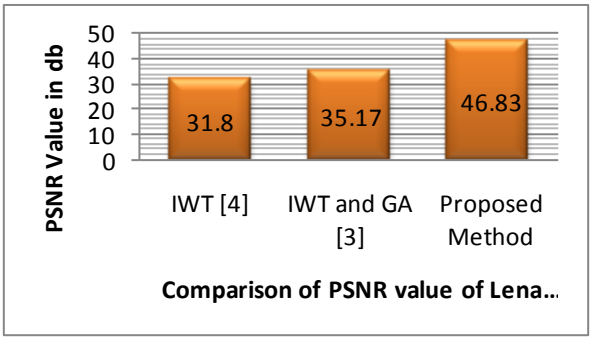


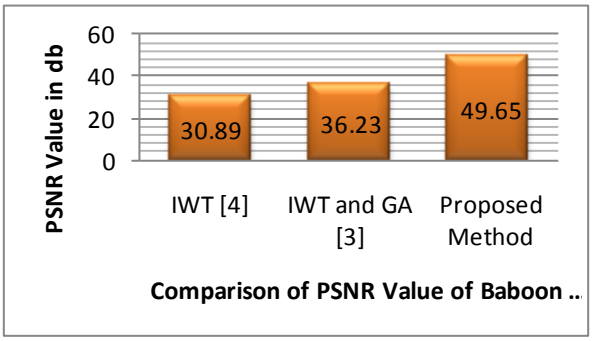
Fig. 2 Input Cover Image Histogram

© 2014, IJARCSSE All Rights Reserved





PSNR (dB) for Lena Image
Fig. 4 PSNR Comparison for Lena Image



PSNR(dB) for Baboon Image
Fig. 5 PSNR Comparison for Baboon Image

Figure 4 and 5 highlights the comparison of the obtained PSNR between our proposed method and methods in [3], [4]. Hence, it can be seen that the proposed system has better performance in compared to majority of the Steganographic techniques using integer wavelet transform and genetic algorithm with RS analysis.

V. CONCLUSIONS

Steganography is a method that provides secret communication between two parties. It is the science of hiding a data or message or information in such a secure way that only and only sender and recipient are aware about the presence of the message. The main advantage of this type of secures communication or we can say steganography is that it does not make any attention about the message to attackers or we can say does not attract the attackers. Strongest steganalysis method which known as RS analysis detects the secret hidden message by using the statistical analysis of pixel values.

The main aim of this proposed work is to develop a steganography model which highly RS-resistant using Genetic algorithm and Integer Wavelet Transform. This proposed work introduced a novel steganography technique to increase the capacity and the imperceptibility of the image after embedding. This model enables to achieve full utilization of input cover image along with maximum security and maintain image quality. GA employed to obtain an optimal mapping function to lessen the error difference between the cover and the stego image and use the block mapping method to preserve the local image properties. In this proposed method, the pixel values of the stego image are modified by the genetic algorithm to retain their statistical characteristics. So, it is very difficult for attacker to detect the existence of the secret message by using the RS analysis technique. We applied the OPAP to increase the hiding capacity of the algorithm in comparison to other systems. However, the computational complexity of the new algorithm is high. Further, implementation of this technique improves the visual quality of the stego image same as input cover image. But, as we increase the length of the secret message, the chance of detection of secret hidden message by RS analysis also increases. The simulation results showed that capacity and imperceptibility of image had increased simultaneity. Also, we can select the best block size to reduce the computation cost and to increase the PSNR using optimization algorithms such as GA. However, future works focus upon the improvement in embedding capacity and further improvement in the efficiency of this method.

© 2014, IJARCSSE All Rights Reserved

VI. FUTURE SCOPE

This proposed work is restricted to specific functionality only. The proposed work is experimented on single computer system, not on any network. Standard input cover image is only used in this steganography method. Proposed method is not applicable on audio, video and other biometrics yet. Large message steganography cannot be performed as the embedding capacity confines the data feed.

This work could be extended to following future enhancement:

1. Improve the data embedding capacity and more security against all types of attacks.
2. Security design experimented over multiple computers or network.
3. The data hiding technique apply to audio, video and other biometrics.
4. The steganography for bulk data be performed without the embedding capacity confines the data feed.
5. Protect the system against histogram attack.

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, Digital Image Steganography: Survey and Analysis of Current Methods, Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

[2] Samir Kumar Bandyopadhyay, Tuhin Utsab Paul and Avishek Raychoudhury, Genetic Algorithm Based Substitution Technique of Image Steganography, Journal of Global Research in Computer Science, Volume 1, No. 5, December 2010.

[3] Elham Ghasemi, Jamshid Shanbehzadeh and Bahram ZahirAzami, A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm, 978-1-4244-9799-7/111$26.00 ©20 11 IEEE.

[4] R.O., El.Sofy, H.H.Zayed, An adaptive Steganographic technique based on the integer wavelet transforms 978-1-4244-3778-8/09/$25.00 ©2009 IEEE.

© 2014, IJARCSSE All Rights Reserved