Secured Cryptography cum Steganography Model with Large Message Embedding behind Colored Image by using Genetic Algorithm and OPA Process

Abhishek Tripathy
Dept of Computer Science & Engineering
Shekhawati Institute Of Engineering & Technology
Sikar, Rajasthan (India)

Dinesh Kumar
Dept of Computer Science & Engineering
Shekhawati Institute Of Engineering & Technology
Sikar, Rajasthan (India)

ABSTRACT
This paper introduced a combined cryptography and steganography model to increase the security and the embedding capability of the standard colored images. Cryptography is used in this technique to provide more security. For this purpose we used a secret key (same for sender and receiver) for encryption and decryption process. Only sender and receiver can encrypt and decrypt the whole message by this secret key. For steganography we use genetic algorithm, optimal pixel adjustment process, integer to integer wavelet transform in frequency domain, inverse integer to integer wavelet transform. Genetic algorithm is applied here to achieve a mapping function of 8*8 matrix with minimum error difference between the input and the final image. In GA we use the block based mapping method because by using it we can preserve the input image properties. After it we employed the optimal pixel adjustment process for increasing the hiding capacity of the proposed algorithm in comparison to other existing algorithms. OPA process adjusts all the pixels of image optimally. MATLAB simulation results present that the hiding capacity and imperceptibility of image increase simultaneously. By using the optimization technique such as GA we can choose the best block size to reduce the computation cost and also increase the peak signal to noise ratio.

Keywords
Cryptography, Steganography, Genetic algorithm, Mapping function, Optimal Pixel Adjustment process, Peak signal to noise ratio, MATLAB

1. INTRODUCTION
One of the explanations that intruders will be sure-fire is that the majority of the data they acquire from a system is in an exceedingly type that they will browse and comprehend. Intruders might reveal the data to others, modify it to misrepresent a personal or organization, or use it to launch an attack. One resolution to the current downside is, through the utilization of steganography. Steganography may be a technique of activity info in digital media. In distinction to cryptography, it's to not keep others from knowing the hidden info however it's to stay others from thinking that the data even exists.

The word steganography comes from the Greek Steganos, which implies coated or secret and –graphy means writing or drawing. Therefore, steganography suggests that, accurately, coated writing. Steganography is that the art and science of activity info specified its presence can't be detected [1]. Secret info is encoded in a very approach specified the very existence of the data is hid in an exceedingly human perceptible.

The main goal of steganography is to speak firmly in an exceedingly utterly undetectable manner [2] and to avoid drawing suspicion to the transmission of hidden information [3]. Therefore, in existing communication strategies, steganography will be accustomed do hidden exchanges. The thought of steganography is to stay others from thinking that the info even exists and to not keep others from knowing the hidden information. If a steganography methodology causes anybody to suspect there's a secret info in an exceedingly carrier medium, then the tactic has unsuccessful [4].

2. BACKGROUND
This chapter will discuss the previous existing method of steganography. The design of magnetism systems victimization methods of optimization has been allotted with settled methods. However, these methods don't seem to be efficient, as a result of the article functions obtained from magnetism optimization issues area unit usually highly non-linear, stiff, multi extreme and non-differential. The dearth of one method on the market to subsume three-d issues, together with those with several goals to optimize, has generated the requirement to use numerical processes for optimization. This paper presents a way of worldwide optimization based on genetic algorithms. The Genetic Algorithms area unit a versatile tool, which might be applied as a world optimization method to issues of magnetism engineering, as a result of their simple to implement to non-differentiable functions and separate search areas. It's additionally shown how, in some cases, genetic algorithms have been applied successfully in magnetism issues, like antenna style, far-field prediction, absorbent material coatings style, etc.

For three decades, several mathematical programming methods have been developed to solve optimization issues. However, until now, there has not been one whole efficient and sturdy method to hide all optimization issues that arise within the totally different engineering fields. Most engineering application style issues involve the choice of style variable values that higher describe the behavior of a system. At an equivalent time, those results ought to cover the wants and specifications obligatory by the norms for that system. This last condition ends up in predicting what the doorway parameter values ought to be whose style results comply with the norms and additionally gift good performance that describes the inverse problem.

Generally, in style issues the variables area unit discreet from the mathematical purpose of view. However, most mathematical optimization applications area unit centered and developed for continuous variables. Presently, there are a unit several research articles regarding optimization methods; the standard ones area unit based on calculus, numerical methods, and random methods. calculus based mostly methods have

been intensely studied and area unit subdivided in two main classes: 1) the direct search methods find native maximum moving on a operate over the relative native gradient directions and 2) the indirect methods typically find the local ends finding a collection of non-linear equations, resultant of equaling the gradient from the article operate to zero, i.e., by suggests that of three-d generalization of the notion of the operates extreme points from elementary calculus provides a swish function without restrictions to find a potential maximum that is to be restricted to those points whose slope is zero all told directions. Each method have been improved and extended, however they lack strength for 2 main reasons: 1) they need an area focus, since they look for the most within the analyzed purpose neighborhoods; 2) they rely upon the existence of their spinoff, that several areas of practical parameters respect very little the notion of having derivatives and smoothness. The $64000 world has several discontinuities and yelling areas, that area unit why it's not stunning that the methods depending upon the restrictive necessities of continuity and existence of a spinoff area unit unsuitable for all, however a really restricted problem domain. Variety of schemes has been applied in several forms and sizes. The concept is sort of direct within a finite search area or a separate infinite search area; wherever the algorithms will find the article operate values in every area purpose one at a time. The simplicity of this kind of algorithm is extremely enticing once the numbers of prospects area unit very tiny. All the same, these outlines area unit usually inefficient, since they are doing not complete the wants of strength in big or highly dimensional areas, making it quite a laborious task to find the optimal values. Given the shortcomings of calculus based mostly techniques and also the numerical ones the random methods have exaggerated their popularity.

The methods of random search area unit known as evolutionary algorithms. The evolutionary techniques area unit parallel and globally sturdy optimization methods. They're based on the principles of selection of Darwin [5] and also the genetic theory of the selection of R.A. Fisher [6]. The applying of evolutionary techniques as abstractions of the natural evolution has been broadly evidenced [7]. In general, all algorithmic approaches based on population, that use choice and random variation to get new solutions, may be seen as evolutionary techniques. Indeed, the study of nonlinear issues victimization mathematical programming methods that can handle international optimization issues effectively is of extensive interest. Genetic Algorithms is one such method that has been a subject of dialogue by [8], [9], [10] and [11].

The genetic algorithm is an example of a search procedure that uses random choice for optimization of a operate by suggests that of the parameters area cryptography. The genetic algorithms were developed by holland [12] and also the most popular references area unit maybe Reuben Lucius Goldberg [13] and a more recent one by Back [14]. The genetic algorithms have been evidenced thriving for sturdy searches in advanced areas. Some papers and dissertations, like [7], state the validity of the technique in applications of optimization and sturdy search, crediting the genetic algorithms as efficient and effective within the approach for the search. For these reasons Genetic Algorithms area unit broadly utilized in daily activities, as much in scientific applications as in business and engineering circles. It's necessary to emphasize that genetic algorithms don't seem to be restricted to the search area (relative aspects to the continuity and derivatives existence among alternative properties). Besides, genetic algorithms area unit easy and very capable in their task of sorting out the target improvement.

Given time, it has been potential to break every steganographic system that has ever been revealed. As a result of this, new techniques area unit developed to boost upon the flaws of the forerunner. It's abundantly an equivalent case in steganalysis wherever the algorithms area unit usually tweaked or combined in order to attack the newest steganography algorithm.

The two fields therefore operate during a 'cat and mouse' vogue strategy with steganography about to be prior to the sphere specified covert communications may exist. There's then a entail steganalysis to catch up specified covert communications area unit minimized as much as potential.

One of the foremost basic steganographic techniques is achieved by manipulating the component values of the cover image in sequence specified they then be converted into code that can be accustomed reconstruct the message once extracting. The foremost fashionable method for developing this concept left a pattern within the starting of the photographs that steganalysts bought to light-weight. This light-emitting diode to the development of a series of techniques that would detect the existence of steganography inside any stegogramme that followed this embedding strategy, and so steganographers set regarding developing a new system that may render the attacks useless. This light-emitting diode to the development of randomized embedding in component values, and once more steganlalysts found a way for sleuthing steganography for all pictures created victimization this strategy. The chase has continuing for hundreds of legendary steganographic methods, and we area unit now at the purpose wherever a steganography algorithm has been developed that's resistant to all the legendary blind steganalysis methods, it's known as YASS (Yet another Steganographic Scheme). YASS embeds data into apparently random locations of a canopy image in such the way that no current method is able to identify any artifacts that change the way in to cracking the algorithm [14].

3. PROPOSED SYSTEM

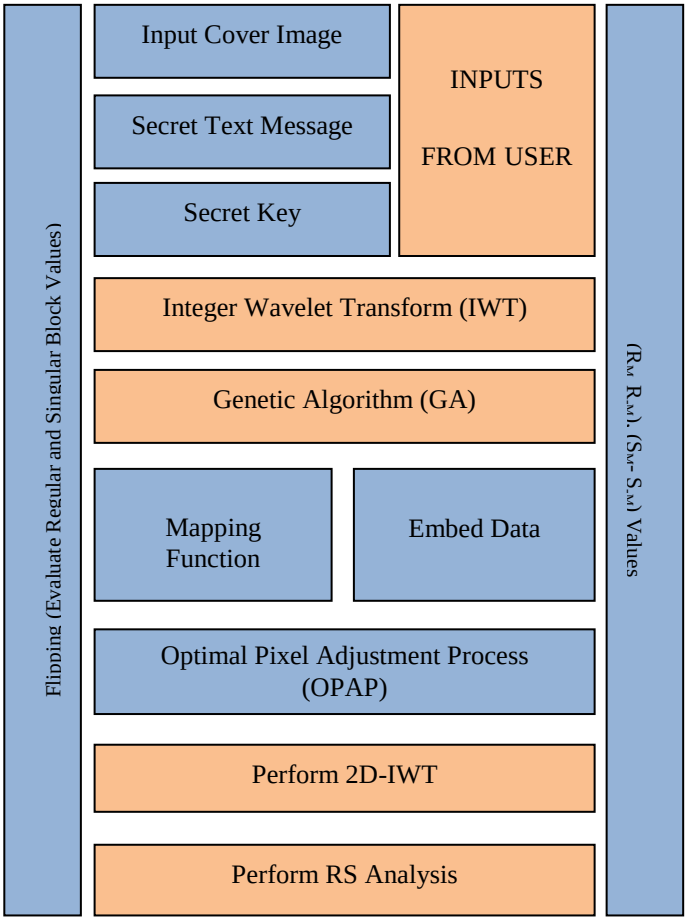


Fig. 3.1: Proposed System Architecture

Cover image to stego image with message embedding process as shown below in the figure:

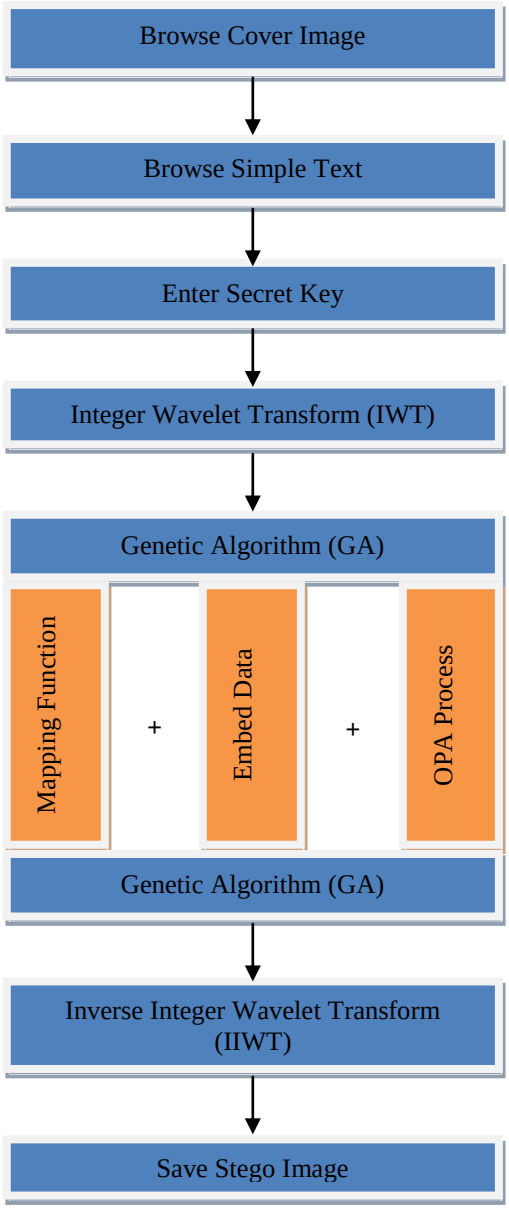


Fig. 3.2: Stego image generation process

3.1 Overall process to generate actual embedded message

Stego image to message extraction process is shown as below in figure:

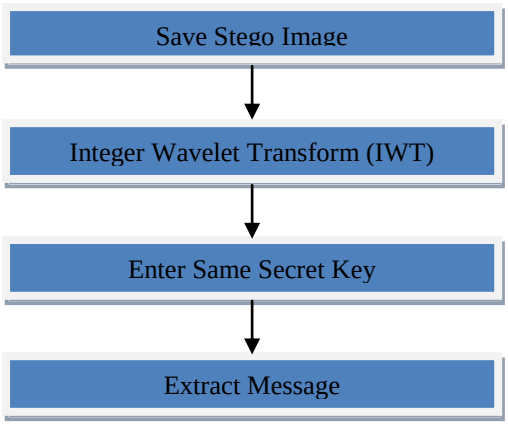


Fig. 3.3: Original message extraction process from stego image

4. EXPERIMENTAL RESULTS

4.1 The Embedding Module

Now, let us discuss the embedding process of the proposed algorithm. Of course, we need first to convert the secret message into a 1D bit stream. Of course the details of this step will depend on the particular message type. For example, in the case that the message is in text form, we can form the bit stream by simply converting the ASCII code of each character into an 8-bit binary representation, and then concatenating them as a sequence.

The next step that follows the cover adjustment is concerned with applying Integer Wavelet Transform (IWT) the on the cover image. However, the cover image is in true-color format (i.e. the image consists of three color planes: red, green and blue), so the wavelet transform is performed on each color plane separately. The embedding process stores (*N)* message bits in the least significant bits (LSB) of the IWT coefficients of the cover image. Furthermore, we have used the four sub-bands of the image transform for embedding. Of course, after the embedding process ends the stego image is produced by applying the *Inverse of the Integer Wavelet Transform* (*IIWT*) on the modified coefficients.

One thing is left to be considered. That is, we need to decide on the order by which the coefficients will be selected for embedding. We have employed the pseudorandom permutation as a secure selection scheme. The idea behind the permutation is that the permutation generator uses the stego key and produces as output different sequences of the set {1, 2, 3, …., length(Cover)}. Nobody can guess the generated random sequence without knowing the secret key. This ensures that only recipients who know the corresponding secret key will be able to extract the message from a stego-object.

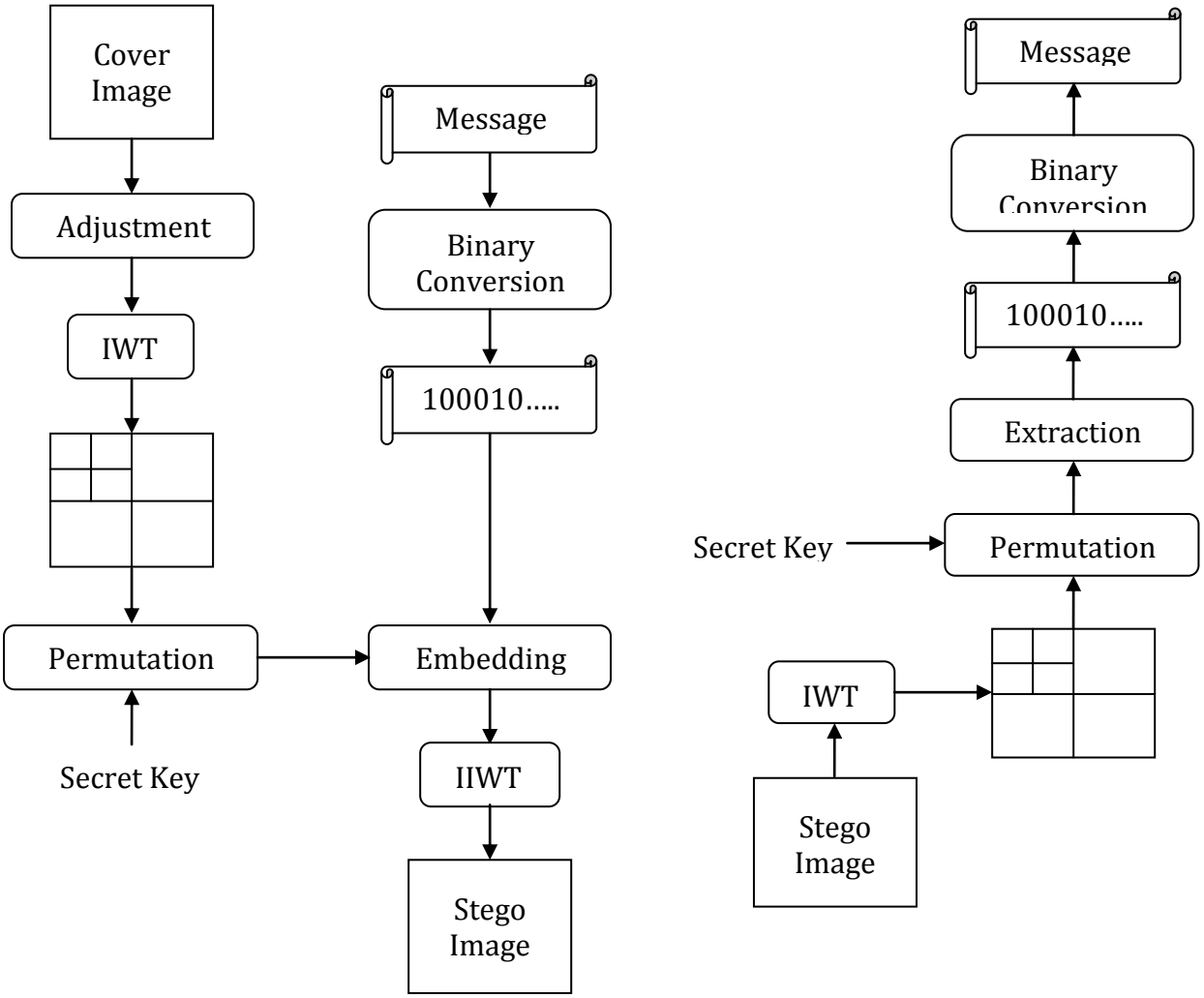
4.2 The Extraction Module

As shown in figure 4(b), the extraction process reverses the embedding operation starting from applying the IWT on each color plane of the stego image, then selecting the embedded coefficients, until extracting the embedded message bits from the *N* LSB's of the integer coefficients. Furthermore, the extracted bits are converted into its original digital form.

Obviously, the proposed scheme is blind since with the stego key only, the original cover-image is not needed to recover the embedded message from the received stego-image. In addition, the proposed scheme is considered secure. That is, without knowing the stego-key a passive warden can't extract the hidden message or even prove its very existence.

In high bit-rate data hiding we have two primary objectives: the technique should provide the maximum possible payload and the embedded data must be imperceptible to the observer. We stress on the fact that steganography is not meant to be robust. Any modifications to the file, such as conversions between file types and/or standard image processing, is expected to remove the hidden bits from the file.

Fundamentally, data payload of a steganographic scheme can be defined as the amount of information it can hide within the cover media. As with any method of storing data, this can be expressed as a number of bits, which indicates the max message size that might be inserted into an image.



(a) The embedding module (b) The extraction module

Fig. 4: Block diagram for hiding binary data in integer wavelet coefficients of an image

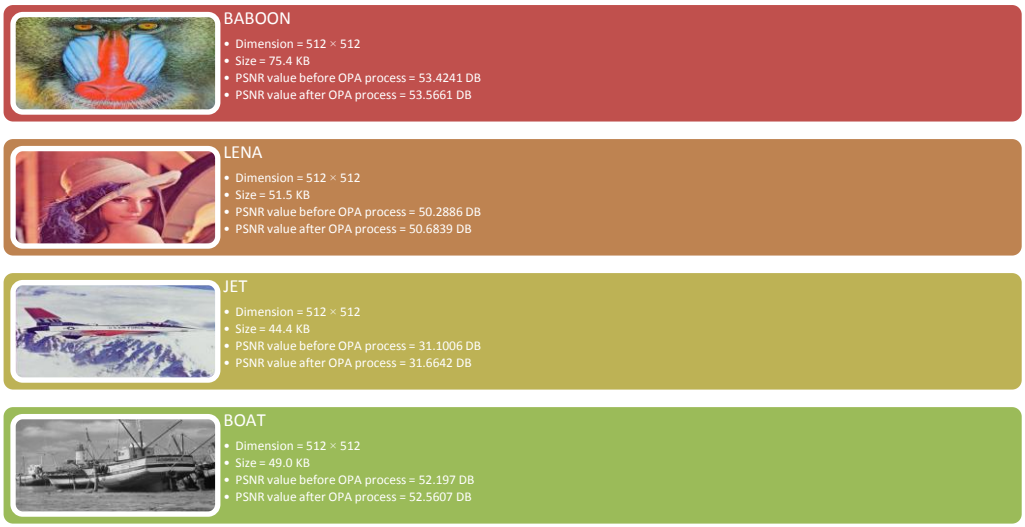
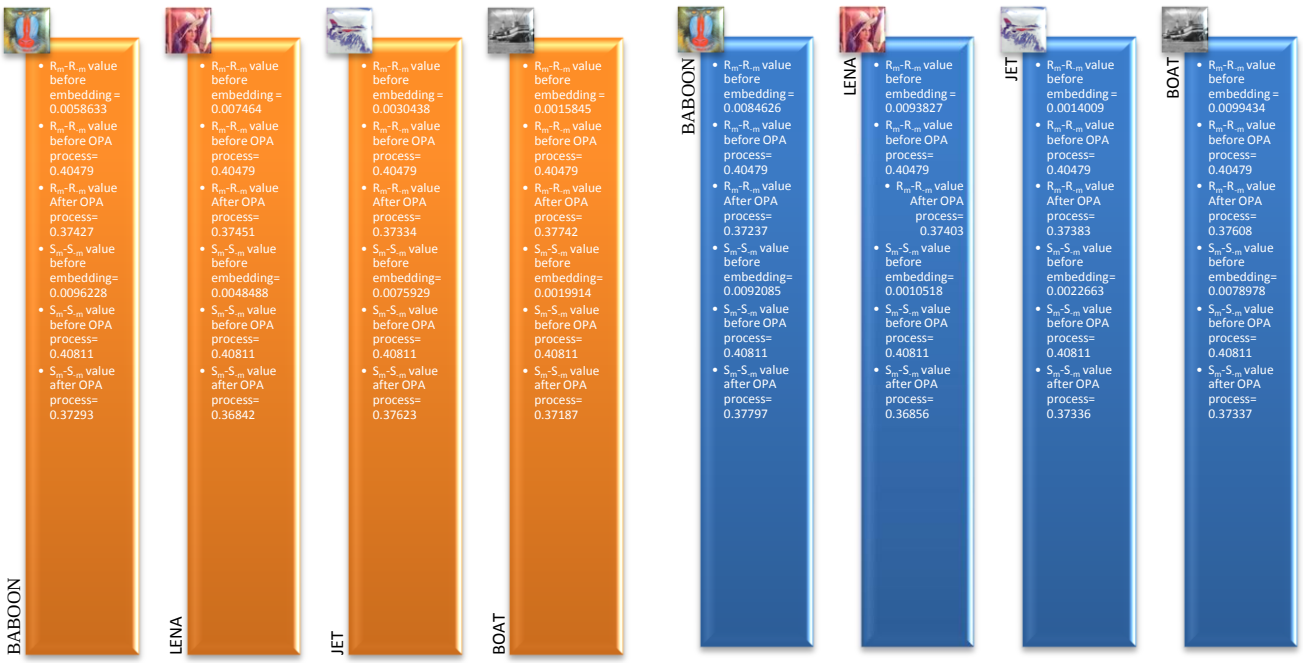


Fig. 5: Image comparison based on size and PSNR value when dimension 512 × 512 and k=4

Fig. 6: Image comparison based on size and PSNR value when dimension 300 × 300 and k=4



512 ×512 dimension and K=4 300 × 300 dimension and K=4

Fig. 7: RS Analysis value comparison

5. CONCLUSION

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We pointed out the enhancement of the image steganographic system using LSB approach to provide a means of secure communication. A *stego-key* has been applied to the system during embedment of the message into the cover-image. In our proposed approach, the message bits are embedded randomly into the cover-image pixels instead of sequentially. Finally, we have shown that steganography that uses a key has a better

security than non-key steganography. This is so because without the knowledge of the valid key, it is difficult for a third party or malicious people to recover the embedded message. However there are still some issues need to be tackled to implement LSB on a digital image as a *cover-object* using random pixels.

Steganography is a technique which set a secret path of communication between two nodes. It is secret medium of science for hiding a data in a secure way so that hacker not knows the presence of the data. In this method for hiding purpose we use a genuine image that is noise free and standard image. Behind this image we embed a message that can be in may lines of sentence. After embed the message the image send to the receiver. In between the communication between the sender and receiver many people over the network i.e. hackers are interested to know that what is actually sent by the sender. So the main advantage of this type of secures technique is that it does not make any type of attention about the message to hackers. The proposed method also restrict the strongest steganalysis method that one known as the RS analysis.

The main idea behind this presented technique is to establish robust steganography architecture which defeats RS-attacks by using Genetic algorithm. Presented work presents a highly secured and robust steganography idea to increase the hiding capacity and PSNR value after embedding the data in cover image. Generally by the previous existing all techniques the image quality was degrades as we increase the capacity of hiding material but by the present technique we achieve 100% utilization of cover image as well as maintain the overall image quality. In this proposed work genetic algorithm is applied to maintain the local image properties. The pixel values of the stego image are modified by this algorithm to maintain their statistical characteristics. So by this attacker are in deep trouble for detect the existence of the secret message by using the RS analysis technique. We also applied the OPAP to reduce the distortion in the stego image as compared to the cover image. The OPA process also increases the hiding capacity of image by the pixel adjustment in suitable place.

Wavelet transforms that map integers to integers allow perfect reconstruction of the original image. The proposed algorithm deals with true-color images. The embedding process stores up to 3 to 6 message bits in each integer coefficient for all the transform sub-bands.

The algorithm pre-adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered. The information capacity provided by the proposed algorithm can reach 50% of the original cover image size. Furthermore, experimental results showed that this scheme retains high quality of the stego-image over the existing LSB-based methods.

6. FUTURE WORK

The knowledge of the technology is still limited to mainly the research individuals and academia; however there is a growing understanding that this technology could be used widely. UTM should carry out more research into the field of information hiding. In future, we would extend the system to be more robust and efficient. The research will include the enhancement of the algorithm that will utilize the entire image for embedding the message. We will also analyze the processing time to generate the random number and introduce method(s) to minimize the time.

As we increase the length of the secret data, the chance of detection of secret hidden message by attackers also increases. Future works focus upon the length problem as well as on histogram attack.

7. REFERENCES

[1] C. Cachin, “An Information-Theoretic Model for Steganography”, in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.

[2] R. Chandramouli, N. Memon, “Analysis of LSB Based Image Steganography Techniques”, IEEE pp. 1019-1022, 2001.

[3] N.F. Johnson, S. Jajodia, “Staganalysis: The Investigation of Hiding Information”, IEEE, pp. 113-116, 1998.

[4] D. Artz, “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing, pp. 75-80, May-Jun 2001.

[5] C. Darwin, The Origin of the Species, Cambridge, Ma., Harvard University Press, 1967.

[6] R.A. Fisher, The Genetical Theory of Natural Selection. Clarendon press, Oxford 1930.

[7] A.D. Channon, and R.I. Damper, "Towards the Evolutionary Emergence of Increasingly Complex Advantageous Behaviours". International Journal of Systems Science, 31(7), pp. 843-860, 2000.

[8] Carlos D. Toledo, "Genetic Algorithms for the numerical solutions of variational problems without analytic trial functions", arXiv:Physics/0506188, pp. 1-3, June 2005.

[9] J. Holland, “Genetic Algorithms” Sci. Am. pp.114-116, 1992.

[10] T. Bäck and H. P. Schwefel, "An Overview Of Evolutionary Algorithms" Evolutionary Comput. 1: pp. 1-23, 1993.

[11] Allen B. Tucker (Jr.), The Computer Science and Engineering Handbook, CRC Press, USA, pp. 557-571, 1997.

[12] J.H. Holland, Adaptive in Natural and Artificial Systems. Ann Arbor, MI: University of Michigan Press, 1975.

[13] D.E. Goldberg, Genetic Algorithms, in Search, Optimization & Machine Learning. Addison Wesley, 1997.

[14] T. Bäck, Evolutionary Algorithms in Theory and Practice: Evolution Strategies, Evolutionary Programming, Genetic Algorithms. Oxford University Press, N.Y.,1996.