International Journal of Recent Research and Review, Vol. VII, Issue 2, June 2014

ISSN 2277 – 8322

Image Steganography By Using Integer Wavelet Transform And Genetic Algorithm To Perform Text Based Hiding Behind Gray Scaled or Colored Image

Abhishek Tripathy, Dinesh Kumar

Deptt. of Computer Science & Engineering, Shekhawati Institute of Engineering & Technology, Sikar (Rajasthan)

***Abstract* - Data security is one of the most prominent and vital requirement for the data communication over the communication channel. The data hiding with the security features is considered as the vital measure for the secured data communication. The process of sending messages between two parties through a public channel in such a way that it deceives the adversary from realizing the existence of the communication is known as steganography. A more secured steganographic model has been implemented in this proposed work for data hiding in the digital image data. In recent research works few algorithms have been proposed which consists of the marginal statistics that are preserved for achieving more security. Data hiding techniques can generally be divided into two categories: spatial and frequency domain. The first category deals with the embedding the messages in the Least Significant Bit (LSB) of the image pixel. This specific technique is sensitive against attacks like low pass filtering and compression however, on different facts this method's implementation is sort of straightforward and its concealing capability is high. What is more, this concealing technique improved the sensitivity and physical property drawback found within the spatial domain. This proposed work presents a novel technique to increase the hiding capacity and the imperceptibility of the image after embedding. The main feature of the presented work is the higher hiding capacity and imperceptibility, and these features enhance the robustness as well as quality of steganography. Wavelet transform has the capability to offer some information on frequency-time domain simultaneously. Haar rippling operates on information by scheming the sums and variations of adjacent components. This proposed work embeds the message inside the cover with the least distortion therefore we have to use a mapping function to LSBs of the cover image according to the content of the message. Genetic Algorithm is used to find a mapping function for the image blocks. Block based strategy will maintain native image property and scale back the algorithmic rule complexness compared to single component substitution. GA is employed to obtain an optimal mapping function to reduce the error difference between the cover and the stego image and use the block mapping method to preserve local image properties and to reduce the complexity of algorithm. After it the Optimal Pixel Adjustment Process applied to increase the hiding capacity of the algorithm in comparison to other existing systems. Here in this presented work the robust generic algorithm has been used for the RS analysis, and thus the development for RS has been done which makes this work superior than the existing works. The overall system architecture has been developed for the RS based GA. The overall work has been done on the MATLAB 7.10 (2010a version) and best satisfactory results have been obtained which presents the higher hiding capacity, the better imperceptibility and high security against attacks.**

***Keywords* - Steganography, genetic algorithm, wavelet transform, reversible statistical.**

I. INTRODUCTION

Now days the data communication with the security and authenticity has became one of the prominent factors in deciding the quality of data being sent and the quality of data communication. The secured data transmission is dominating in the network security, data transmission and communication based research and development. There are a number of researches going on in order to achieve the optimized secured data over the transmission channel. On the other hand the data transmission without any visual recognition is on the top in the security concerns. Therefore the data hiding and then transmission technique is leading in the communication world. One of these techniques comes under the roof of Steganography. The process of sending messages between two parties through a public channel in such a way that it deceives the adversary from realizing the existence of the communication is known as steganography. The ongoing development of computer and network technologies provides an excellent new channel for steganography. Redundancy contained by most digital documents. It means that there are some documents parts that can be modified without any impact on their entire quality. The document redundant parts can be realized in many ways. For this consider an image. Basically, image margins do not provide any important information and they used to hide an important message. Further, few pixels of the image can be changed to carry a little number of important bits as small changes (e.g., LSB of pixels) will not be noticeable to an unauthorized user or person. The redundant parts of a digital document can be identified in a different no of ways, so many steganographic methods can be developed for it. Technically steganography considers only methods and good techniques that can create covert channels of communication for unobtrusive transmission for military purposes [1].

Steganography is the art of hiding information imperceptibly in a cover medium. The word "Steganography" is of Greek origin and it means that "covered writing". The main objective in steganography is to hide the existence of the key message among the quilt medium. Steganography and cryptography square measure counter elements in digital security and the main advantage of steganography that it has over cryptography is that messages do not provide attention to themselves or to messengers or to recipients. Further, the last decade has seen high growth within the transmission information use over the internet. These multimedia data include digital images, audio and video files. This growth of digital content on the internet has further increase the research effort regarding to steganography. The different applications of steganography embody secure military communications, multimedia system watermarking and procedure applications for authentication purposed to curb the matter of digital piracy. Although these aren't good applications of steganography, several steganographic algorithms will be used for these functions still [1].

The system being proposed here has some specification that makes it aloof from the other crowed made in the data communication techniques. In the work being developed the algorithm has been developed based on RS. Since now days the attacker modules are being prepare for the specific type of application. Meanwhile the RS attackers are prepared to attack over it, but the contribution of this developing work is that the RS has been designed for GA and thus the data security with the highly optimized and highly dense data can be embedded. On the other hand few visual perception factors are also there that makes the transmission data vulnerable for the attackers. Therefore in order to overcome that problem, here in this proposed work the RS module has been considered and the optimization has been done with the robust Genetic algorithm. It facilitates the system architecture to be highly dense or higher capacity and imperceptibility. Thus the developed system architecture has better features as compare to the other existing techniques.

A. *Definition*

1. Steganography: Steganography is that the art and science of writing hidden messages in such how that nobody, except the sender and meant recipient, suspects the existence of the message, a variety of security through obscurity. Steganography includes the concealment of information within laptop computer files. In digital steganography, electronic communications could embody steganographic committal to writing within a transport layer, for example document file, image file, and program. Media files square measure ideal for steganographic transmission due to their giant size.
2. Discrete wavelet transform: In numerical analysis and useful analysis, a separate rippling rework (DWT) is any rippling rework that the wavelets square measure discretely sampled. As with different rippling transforms, a key advantage it's over Fourier transforms is temporal resolution: it

captures each frequency and placement data (location in time).

3. Genetic algorithm: A genetic algorithm (GA) is a search heuristic that mimics the process of natural evolution. This heuristic is habitually wont to generate helpful solutions to improvement and search issues. Genetic algorithms belong to the larger category of Evolutionary algorithms (EA), that generate solutions to optimization issues victimization techniques impressed by natural evolution, like inheritance, mutation, selection, and crossover.
4. Least significant bit: In computing, the least significant bit (LSB) is the bit position in an exceedingly binary integer giving the units worth, which is, finding whether the quantity is odd or maybe. The LSB is few times settled to as the right-most bit, attributable to the convention in positional notation of writing smaller digit more to the correct aspect. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

B. *Problem definition*

In general, the steganalysis techniques can be categorized into six levels depending on how much information about the hidden messages require. These levels (ordered according to the increased amount of information acquired) are as follows:

1. Differentiation between cover and stego documents—this is the first step in steganalysis and the purpose of this technique is to determine if a given document carries a hidden message.
2. Identification of steganographic method—this technique identifies the type of steganographic method used and it is the so-called multi-class steganalysis.
3. Estimation of the length of a hidden message—this technique reveals the amount of embedded message as the acquired information.
4. Identification of stego-bearing pixels—this technique uncovers the exact locations where the pixels are used to carry the message bits.
5. Retrieval of stego-key— once the transmitted data which has been already staged reaches to the receiver terminal, and to access the received data a security key is required. This facilitates the authenticity of the data communication. The key is required to access the data. This technique provides access to the stego-bearing pixels as well as the embedding sequence.
6. Message extraction— once the data has been embedded then it becomes available for further transmission or communication. When the transmitted data approaches to the receiver terminal then it is required to be extracted so that the text data being transmitted can be retrieved. The process of extracting the text knowledge from the embedded or staged image knowledge is named as message extraction. This technique basically involves extracting and deciphering the hidden message to obtain a meaningful message.

In recent research works few algorithms have been proposed which consists of the marginal statistics that are preserved for achieving more security. Previous methods have less data hiding capacity. As we increase the data length distortion increases in the final stego image. The previous methods not strong against the RS attack. All the previous methods provide the basic path to hide the data behind the image. There was no provision about the increasing capacity of data as no effect on image and how to restrict the RS attack. So this is a big issue in steganography model that how we increase the hiding capacity without any distortion in the image quality and how we provide the security against the RS attack.

C. *Scope of the work*

The major scopes of this work are listed below.

1. Blind steganalysis**:** The proposed system has developed a framework in order to distinguish a stego image from a cover image. Mainly, it's been broken many steganographic ways from the literature. This technique usually uses an image processing technique that extracts sensitive statistical data, which employs a better technique to determine the existence of a secret message. In addition, this technique is often refined and accustomed sight a special variety of steganographic method. This property is very important once managing associate degree unknown and new steganographic technique.

2. Use of IWT and GA: The proposed system is extended to determine the best fitness function along with RS analysis to produce the stego image. This is vital info that permits associate degree someone to mount a lot of specific attack. From the literature review, it is a foresaid that the planned system is healthier resilient to applied statistical attack.
3. Message length estimation: It has been designed a simple yet effective technique based on first-order statistic to estimate the length of an embedded message. This estimation is crucial and commonly is needed if it's been will extract a hidden message. It has been have identified that the notches and protrusions can be utilized to approximate the degree of image distortion caused by embedding operation. In specific, this {method} attacks the steganographic method developed in past.
4. Steganographic payload locations identification: It has been bestowed a way to spot the locations wherever hidden message bits area unit embedded. This technique is one in every of the only a few researches within the literature that's able to extract extra secret info. Eventually, this information is very important for an adversary who wishes to remove a hidden message or deceive communication.
5. Enhancement of existing steganalysis techniques: It has been planned improvement to existing image steganalysis. Specifically, it's been hand-picked and combined many forms of options from many existing steganalysis techniques by employing a feature choice technique to make a additional powerful blind steganalysis. It has been shown that the technique has improved the detection accuracy and to boot reduced the machine resources. It has been additionally shown that by minimizing the influence of image content, the detection accuracy may be improved.

The remainder of the paper is organized as follows. In section II, a review of the necessary literature required to effectively implement our algorithm is presented. The proposed algorithm is described in Section III. After that, application of the proposed algorithm is discussed in section IV, and we draw our conclusion in the last section.

II. LITERATURE REVIEW

Steganography is the practice of encoding secret information in a manner such that the very existence of the information is concealed. Throughout history, several steganographic techniques are documented, as well as the employment of cleverly-chosen words, invisible ink written between lines, modulation of line or word spacing, and microdots [1, 2, 3]. Usually the secret information is concealed by the use of an innocuous cover as to not arouse suspicion if hostile agents discover the cover.

Taras Holotyak *et. al* [4] propose a new method for estimation of the number of embedding changes for non-adaptive ±k embedding in images. The similar author [5] has also advocate a new approach to blind steganalysis based on classifying higher-order statistical features derived from an estimation of the stego signal in the wavelet domain.

Agaian and Perez [6] propose a new steganographic approach for palette-based images. This newly approach has the advantage of secure data embedding, within the index and the palette or both, using special scheme of sorting. The presented technique also incorporates the use color model and cover image measures in order to select the best of the candidates for the insertion of the stego information.

Chen and Lin [7] propose a new steganography technique which embeds the secret messages in frequency domain to show that the PSNR is still a satisfactory value even the highest capacity case is applied. By seen the results of simulation, the PSNR is still a relaxed value even the highest capacity is applied. This is due to the different characteristics of DWT coefficients in different sub-bands. Since the most essential portion (the low frequency part) is kept unchanged while the secret messages are embedded in the high frequency sub-bands (corresponding to the edges portion of the image), good PSNR is not a imagine result. In addition, corresponding security is maintained as well since no message can be extracted without the “Key matrix” and decoding rules.

Kathryn Hempstalk [8] investigates using the cover’s original information to avoid making marks on the stego-object, by hiding basic files of electronic reside digital color images. This paper has introduced two image steganography techniques, Filter First and Battle Steg. These two techniques attempt to improve on the effectiveness of the hiding by using edge detection filters to produce better steganography.

Wang and Moulin [9] provided that the independently and identically distributed unit exponential distribution model is not a sufficiently accurate description of the statistics of the normalized periodogram of the full-frame 2-D image DFT coefficients.

Park *et.al* [10] proposed a new image steganography method to verify whether the secret information had been removed, forged or altered by attackers. This proposed method covers secret data into spatial domain of digital image. In this paper, the integrity is verified from extracted secret information using the AC coefficients of the discrete cosine transform (DCT) domain.

Ramani, Prasad, and Varadarajan [11] propose an image steganography system, in which the data hiding (embedding) is realized in bit planes of subband wavelets coefficients obtained by using the Integer Wavelet Transform (IWT) and Bit-Plane Complexity Segmentation Steganography (BPCS).

Farhan and Abdul [12] have presented their work in message concealment techniques using image based steganography. Anindya *et.al* [13] present further extensions of yet another steganographic scheme (YASS), is a method based on embedding data in randomized locations so as to resist blind steganalysis. YASS is a technique of JPEG steganographic that hides data in the discrete cosine transform (DCT) coefficients of randomly chosen image blocks.

Adnan Gutub *et.al* [14] merge between the ideas from the random pixel manipulation methods and the stego-key ones to propose our work, which takes the least two significant bits of one of the channels to indicate existence of data in the other two channels. This work showed good results especially in the capacity of the data-bits to be hidden with relation to the RGB image pixels.

Mohammed and Aman [15] uses the Least Significant Bits (LSB) insertion to hide data within encrypted image data. Aasma Ghani Memon et.. al. [16] provides a new horizon for safe communication through XML steganography on Internet.

Zaidan *et.al* [17] has presented a model for protection of executable files by securing cover-file without limitation of hidden data size using computation between cryptography and steganography.

Vinay Kumar and Muttoo [18] has discussed that graph theoretic approach to steganography in an image as cover object helps in retaining all bits that participate in the color palette of image.

Wang *et.al* [19] presents a new steganography based on genetic algorithm and LSB. Souvik Bhattacharyya and Gautam Sanyal [20] propose a novel steganographic method for hiding information in the transform domain of the gray scale image. The proposed approach works by converting the gray level image in transform domain using discrete integer wavelet technique through lifting scheme.

Nadia M. Mohammed [21] has presented four new methods in steganography systems to embed secret data in compressed images. In spatial domain two methods are working, known as moving window and odd/even LSB, others methods are working in transform domain, known as odd/even DCT and DCT+DWT.

Zaidan *et.al* [22] has proposed a multi-cover steganography using remote sensing image.

Shaamala *et.al* [23] has studied the effect DCT and DWT domains on the imperceptibility and robustness of Genetic watermarking. Results of watermark image quality and attacks based on peak signal-to-noise ratio (PSNR) numerical correlation (NC) is analyzed, and the DWT results showed more robustness high imperceptibility than DCT in watermarking based on GA.

Shiva Kumar *et.al* [24] propose Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques (PCRSMT). The cover image is divided into 64 blocks of 4*4 each and DWT is applied to every block. The resulting 1 to 64 blocks of vertical band of 2x2 each are isolated and IWT is applied to get 1x1 blocks. The DWT and IWT are applied to payload and IWT coefficients of payload are embedded with that of cover image. IDWT and IIWT are applied to derive stego image. In addition error detection and correction technique is also applied to ensure more secured communication. It is seen that the robustness and capacity of hiding are improved with very little tradeoffs in PSNR.

III. Proposed Work

The proposed work ensures the security against the RS analysis and to take this, the application should be designed with a plan to overcome all the limitation considered in the previous research work. The current aim to design the architecture of the proposed work depends completely on a robust process of safeguarding the input to the application. This strategy incorporate implementing least important bit for embedding the key message of the quilt image. The next issue which might be encountered is the loss of quality of the image and the planning done for safeguarding the quality of the image which is achieved by implementing Genetic Algorithm. It is a technique of search used in computing to find exact or approximate solutions to optimization and search problems.

In the proposed method, the message is embedded on Integer Wavelet Transform coefficients based on Genetic Algorithm. Thereafter, OPAP algorithm is applied on the obtained embedded image. We use Genetic Algorithm to find a mapping function for all the image blocks. In our GA method, a chromosome is encoded as an array of 64 genes containing permutations 1 to 64 that point to pixel numbers in each block. The main idea of applying OPAP is to minimize the error between the cover and the stego image. In this work, we adopted genetic algorithm to search for a best adjustment matrix. Genetic algorithm is a basic algorithm for optimization. It transforms an optimization or search problem as the process of chromosome evolution. When the best each is selected after many generations, the optimum or sub-optimum solution is found. Genetic algorithm important operations are reproduction, crossover and mutation.

This work presents a novel steganography technique that will ultimately increase the capacity of data embedding and the imperceptibility of the image after embedding. The proposed system architecture is highlighted as below:

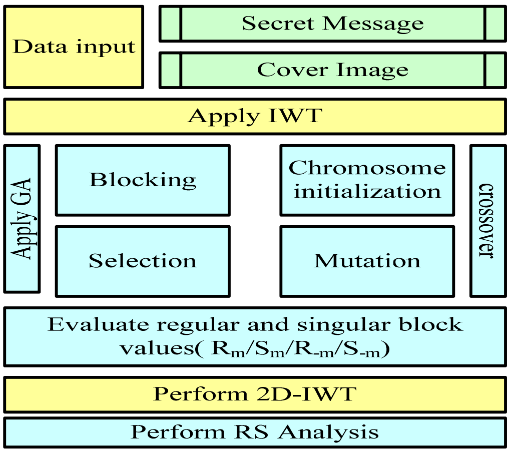

Fig. 1 System architecture of the proposed work

The overall system design can be expressed as follows:

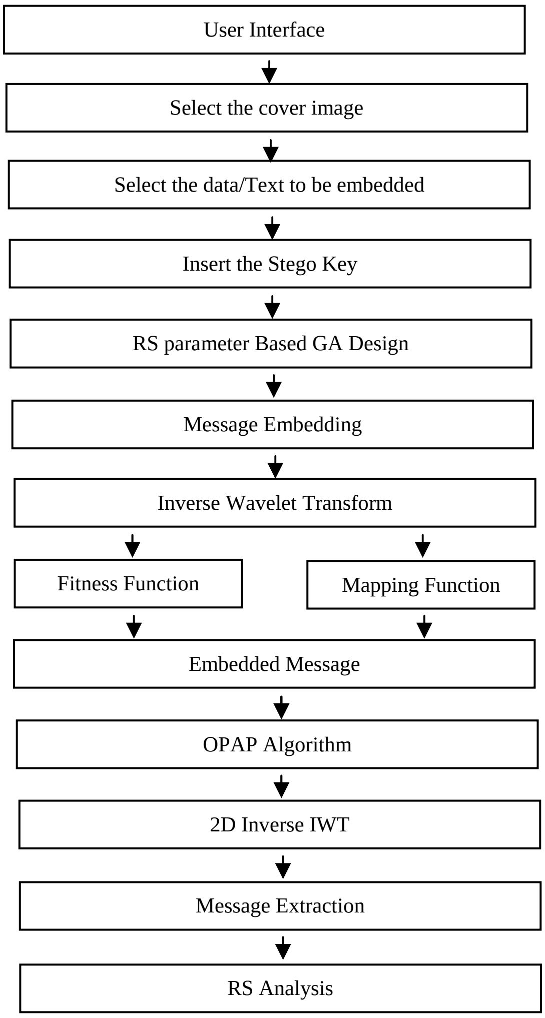

Fig. 2 The overall functional flow diagram

The above mentioned figure represents the overall system functionalities of the developed algorithm. The overall system function can be summarized by observing the figure mentioned above. The figure represents the real operative steps of the developed design. In the processing the user interface helps so as to provide a user interface to handle the developed model and to access the developed module. At the inception, the cover image is selected for embedding the data. Then the text data or the message is to be selected and then in order to accomplish the motive of steganography the stego key is assigned so that at the other terminal the data can be retrieved by putting the key. Once the Key has been provided, the real application development for the RS analysis will be started with the help of robust GA optimization. In this technique initially the message is to be embedded in cover image. Genetic Algorithm is playing a vital 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 data has been embedded into the image file, then after embedding the image is again recovered and then it is now ready to be transmitted over the communication channel. On the other hand at the receiver terminal or the extraction terminal with the accurate assignment of the stego key the data is retrieved accurately.

IV. CONCLUSION

In the proposed work, a unique Genetic algorithmic rule primarily based secured steganography technique is introduced that is meant to defeat almost all familiar existing steganalysis strategies. The proposed system design facilitates the better standard technical for steganography. This method optimizes localization in which the message or the user specified data is to be embedded in the cover image. This overall system has been designed for steganography that facilitates the text based data hiding in the image file. The proposed method embeds the text message in Discrete Wavelet Transform coefficients based on Genetic algorithm and then OPAP algorithm applied to obtain embedded image file. Wavelet transform has the capability to offer some information on frequency-time domain simultaneously. Haar wave operates on knowledge by hard the sums and variations of adjacent components. This wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. One good feature of the Haar wavelet transform is that the transform is equal to its inverse. Each transform computes the data energy in relocated to the top left hand corner. Haar is used with lifting scheme here. In this work, we introduced a steganography technique to increase the capacity of image to hide maximum data and the imperceptibility of the image. Genetic algorithm 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 or cover image properties. We applied the OPAP to increase the hiding capacity of the algorithm in comparison to other existing systems. However by this method, the computational complexity is high, our results show that capacity and imperceptibility of image have increase simultaneity. We can select the best block size to minimize the computation cost and to increase the PSNR using optimization algorithms such as genetic algorithm. The results of experiment show that this method works properly, Image utilization up to 100% and is considered to give almost the optimum solution that not achieved yet.

This proposed work presented a new technique to increase the data hiding capacity on standard images 512*512 using Inverse Wavelet Transform as well as genetic algorithm based on RS analysis and least distortion in the stego image. There is minimal error difference between the cover and the stego image. Genetic algorithm is used to find a mapping function for all the image blocks. Block based strategy can maintain local image property and reduce the algorithm complexity compared to single pixel substitution. In the proposed GA method a chromosome is encoded as an array of 64 genes containing permutations 1 to 64 that point to pixel numbers in each block. GA operation mating and mutation are applied on every chromosome. The process of mutation causes the inversion of some bits and produces some new chromosomes, after it, we choose elitism which means the best chromosome will survive and be passed to the next generation. Selecting the fitness function is one of the most important steps in designing a GA based method. Whereas our GA objective is to improve the quality of image, Pick Signal to Noise Ratio (PSNR) can be appropriate evaluation test. The main idea of applying OPAP is to minimize the error difference between the cover and the stego image. Conducting RS-analysis and minimizing R blocks using genetic algorithm has shown an optimal result for our proposed work. However, there are certain limitations to the proposed work also. The proposed work is a semantic oriented security design which is experimented on single computer system. The data hiding technique is restricted to image, but video, speech and other biometrics is out of scope yet. Heavy Steganographic is not performed in the proposed work. However, our future work will be on addressing the above mentioned issues.

V. References

[1] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in HS Venter, JHP Eloff, L Labuschagne and MM Eloff (eds), Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically).

[2] R Sridevi, Dr. A Damodaram, Dr. SVL.NARASIMHAM, efficient method of audio steganography by modified lsb algorithm and strong encryption key with enhanced security, Journal of Theoretical and Applied Information Technology, 2009.

[3] Chander Kant, Rajender Nath, Sheetal Chaudhary, Biometrics Security using Steganography, International Journal of Security, Volume (2) : Issue (1), 2008.

[4] Taras Holotyak, Jessica Fridrich, and David Soukal, Stochastic Approach to Secret Message Length Estimation in ±k Embedding Steganography, Communications and Multimedia Security 2005.

[5] Taras Holotyak, Jessica Fridrich, Sviatoslav Voloshynovskiy, Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics, Communications and Multimedia Security 2005.

[6] Sos S. Agaian and Juan P. Perez, New Pixel Sorting Method For Palette Based Steganography And Color Model Selection, 2004.

[7] Po-Yueh Chen and Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering 2006. 4, 3: 275-290.

[8] Kathryn Hempstalk, Hiding Behind Corners: Using Edges in Images for Better Steganography, 2006.

[9] Ying Wang and Pierre Moulin, Statistical Modelling and Steganalysis of DFT-Based Image Steganography, Proc. of SPIE Electronic Imaging, 2006.

[10] Youngran Park, Hyunho Kang, Kazuhiko Yamaguchi, and Kingo Kobayashi, Integrity Verification of Secret Information in Image Steganography, The 29th Symposium on Information Theory and its Applications (SITA2006), Hakodate, Hokkaido, Japan, Nov. 28, Dec. 2006.

[11] K. Ramani Dr. E. V. Prasad Dr. S. Varadarajan, Steganography using bpcs to the integer wavelet transformed image, IJCSNS International Journal of Computer Science and Network Security, Vol .7, No.7, July 2007.

[12] Farhan Khan and Adnan Abdul-Aziz Gutub, Message Concealment Techniques using Image based Steganography, *The 4th IEEE GCC Conference and Exhibition*, Gulf International Convention Centre, Manamah, Bahrain, 11-14 November 2007.

[13] Anindya Sarkary, Kaushal Solankiyy and B. S. Manjunathy, Further Study on YASS: Steganography Based on Randomized Embedding to Resist Blind Steganalysis, Proc. SPIE - Security, Steganography, and Watermarking of Multimedia Contents (X), San Jose, California, Jan. 2008.

[14] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi, Pixel indicator high capacity technique for RGB image based steganography, WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008.

[15] Mohammad Ali Bani Younes and Aman Jantan, A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008.

[16] Aasma Ghani Memon, Sumbul Khawaja and Asadullah Shah, STEGANOGRAPHY: A new horizon for safe communication through XML, Journal of Theoretical and Applied Information Technology, 2008.

[17] A.A.Zaidan, Fazidah.Othman, B.B.Zaidan , R.Z.Raji, Ahmed.K.Hasan and A.W.Naji, Securing Cover-File

Without Limitation of Hidden Data Size Using Computation Between Cryptography and Steganography, Proceedings of the World Congress on Engineering 2009 Vol I WCE 2009, July 1 - 3, 2009, London, U.K.

[18] Vinay Kumar, S. K. Muttoo, Principle of Graph Theoretic Approach to Digital Steganography, Proceedings of the 3rd National Conference; INDIACom-2009.

[19] Shen Wang, Bian Yang and Xiamu Niu, A Secure Steganography Method based on Genetic Algorithm, Journal of Information Hiding and Multimedia Signal Processing, Volume 1, Number 1, January 2010.

[20] Souvik Bhattacharyya and Gautam Sanyal, Data Hiding in Images in Discrete Wavelet Domain Using PMM, World Academy of Science, Engineering and Technology 68 2010.

[21] Nadia M. Mohammed, Multistage Hiding Image Techniques, Raf. J. of Comp. & Math’s. , Vol. 7, No. 2, 2010.

[22] A. A. Zaidan, B. B. Zaidan, Y. Alaa Taqa, M. Kanar Sami, Gazi Mahabubul Alam and A. Hamid Jalab, Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem, International Journal of the Physical Sciences Vol. 5(11), pp. 1776-1786, 18 September, 2010.

[23] Abduljabbar Shaamala, Shahidan M. Abdullah and Azizah A. Manaf, Study of the effect DCT and DWT domains on the imperceptibility and robustness of Genetic watermarking, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011.

[24] K B Shiva Kumar, K B Raja, R K Chhotaray, Sabyasachi Pattnaik, Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques, Int. J. Comp. Tech. Appl., Vol 2 (4), 1035- 1047, IJCTA, July-August 2011.