International Journal of Recent Research and Review, Vol. VII, Issue 1, March 2014

ISSN 2277 – 8322

An Integer Wavelet Transform Based Steganography Technique for Concealing Data in Colored Images

Preeti Chaturvedi[1], R. K. Bairwa[2]

[1]*M.Tech Scholar, Deptt. of CSE, Kautilya Institute of Technology & Engineering, Jaipur (Raj.),India*

[2]*Assistant Professor, Deptt. of CSE, Kautilya Institute of Technology & Engineering, Jaipur (Raj.),India*

Email: preetichobey@gmail.com

***Abstract*- Steganography is the art and science of writing hidden messages in such the way that no one, except the sender and supposed recipient, suspects the existence of the message, a variety of security through obscurity. In digital Steganography, electronic communications may embrace Steganography committal to writing inside of a transport layer, such as a document file, image file, program or protocol. The proposed work presents a replacement Steganography technique is to produce security to pictures that contain crucial knowledge. The proposed approach depends on LSB technique.**

***Keywords*- Steganography, LSB, Wavelet Transform, GA, TCP/IP, OPA**

I. INTRODUCTION

The word steganography is of Greek origin and suggests that "concealed writing" from the Greek words steganos which means "covered or protected", and graphic which means "writing". The first recorded use of the term was in 1499. The advantage of steganography, over cryptography alone, is that message does not attract attention to them. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and will in themselves be criminatory in countries wherever secret writing is prohibited. Therefore, whereas cryptography protects the contents of a message, steganography may be said to shield each messages and human activity parties. It includes the concealment of information inside pc files. Media files are ideal for Steganography transmission as a result of their large size. The smallest amount significant Bit (LSB) substitution is associate degree example of spatial domain techniques. The fundamental plan in LSB is the direct replacement of LSBs of clattery or unused bits of the cover image with the secret message bits. Till now LSB is the most popular technique used for information concealing because it's simple to implement offers high concealing capability, and provides better control to stego-image quality [1]. Algorithms victimization LSB in greyscale images may be found in [2, 3, 4]. The other type of hiding method is the transform domain techniques which seemed to overcome the robustness and physical property issues found in the LSB substitution techniques. There are many transforms which will be used in information hiding, the foremost wide used transforms are; the separate cosine transform (DCT) which is employed in the common compression format JPEG and MPEG, the separate moving ridge transform (DWT) and the separate Fourier transform (DFT). most recent researches area unit directed to the employment of DWT since it is used in the new compression format JPEG2000 and MPEG4, samples of victimization DWT can be found in [5, 6]. In [7] the secret message is embedded into the high frequency coefficients of the moving ridge transform whereas deed the low frequency coefficients sub band unaltered. Whereas in [8].The advantages of transform domain techniques over spatial domain techniques area unit their high ability to tolerate noises and some signal process operations but on the opposite hand they are computationally complex and hence slower [5]. A number of these techniques calculate the hiding capability of the quilt per its native characteristics as in

[2, 7, 8, 9]. However, the steganographic transform-based techniques have the subsequent disadvantages; low hiding capability and complicated computations [5, 6]. Thus, to get over these disadvantages, the present paper, the employment of optimum element adjustment algorithmic rule to hide information into the whole number moving ridge coefficients of the quilt image in order to maximize the hiding capability the maximum amount as doable. we tend to conjointly used a pseudorandom generator perform to pick out the embedding locations of the whole number moving ridge coefficients to extend the system security.

Steganography may be a methodology of activity a secret message in any cover media. Cover media may be a text, or a picture, associate audio or video etc. it's associate associatecient art of activity info in ways a message is hidden in associate innocent trying cover media in order that won't arouse an eavesdropper's suspicion [10]. A covert channel might be defined as a communications channel that transfers some kind of info employing a methodology originally not intended to transfer this kind of information. Observer's area unit unaware that a covert message is being communicated. Only the sender and recipient of the message notice it. In digital steganography, electronic communications might include steganographic coding inside of a transport layer, like a document file, image file, program or protocol. Media files area unit ideal for steganographic transmission as a result of their massive size.

Wavelet Transform: Rippling domain techniques have become very fashionable as a result of the developments within the rippling stream within the recent years. Rippling transform is employed to convert a spatial domain into frequency domain. The use of rippling in image handwriting model lies within the incontrovertible fact that the rippling transform clearly separates the high frequency and low frequency info on an element by element basis.

Discrete rippling transform: In numerical analysis, a separate ripple make over (DWT) is any ripple makes over that the wavelets square measure discretely sampled like different ripple transforms, a key advantage over Fourier transforms is temporal resolution i.e. it captures each frequency and placement knowledge (location in time).

Genetic algorithm: A genetic algorithm (GA) may be a search heuristic that mimics the process of natural evolution. This heuristic is routinely used to generate helpful solutions to improvement and search issues. Genetic algorithms belong to the larger class of biological process algorithms (EA), that generate solutions to optimization issues victimization techniques affected by natural evolution, like inheritance, mutation, selection, and crossover. GA may be a technique which mimics the genetic evolution as its model to unravel issues. The given problem is taken into account as input and also the solutions area unit coded in keeping with a pattern. The fitness operate evaluates each candidate solution most of which area unit chosen every which way. Evolution begins from a completely random set of entities and is recurrent in succeeding generations.

Different styles of Steganography:

The four main classes of file formats that can be used for steganography are:

i. Text
ii. Images
iii. Audio
iv. Protocol

Text steganography: Activity info in text is historically the foremost vital methodology of steganography. A straightforward methodology was to hide a secret message in each ordinal letter of every word of a text message. Due to the beginning of the web and due to the various kind of digital file formats it's remittent in importance. Text steganography mistreatment digital files aren't used fairly often because the text files have a very small amount of redundant knowledge.

Image steganography: Images area unit the foremost popular cover objects for steganography. A message is embedded in a digital image (cover image) through an embedding algorithm, by mistreatment the key. The resulting stego image is transmitted to the receiver. On the other hand, it is processed by the extraction algorithm mistreatment identical key. Throughout the transmission of stego image, it may be monitored by some unauthenticated persons WHO will only notice

the transmission of a picture but can't guess the existence of the hidden message.

Audio Steganography: Audio Steganography is masking, which exploits the properties of the human ear to hide info observably. An audible, sound becomes voiceless within the presence of another louder sounding sound .This property allows to select the channel in which to hide info. Although it's almost like images in steganographic potential, the larger size of purposeful audio files makes them less popular to use than images [11].

Protocol Steganography: The term protocol steganography refers to embedding info at intervals network protocols like TCP/IP. Associate example of its activity info within the header of a TCP/IP packet in some fields that can be either optional or area unit never used.

II. LITERATURE SURVEY

A formula by that the knowledge capacity can reach 500th of the initial cover image. It provides high quality of stego image over the present LSB primarily based technique [12]. In this paper, we attempt to optimize these two main needs by proposing an advanced method for hiding data in colored images by combining the use of adaptational hiding capacity function that hides secret data within the number wavelet coefficients of the cover image with the optimum pixel adjustment (OPA) formula [13]. A high capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion within the cover image and high level of overall security [14].

Incorporate the idea of secret key for authentication at each the ends in order to realize high level of security. During this paper, a specific image primarily based steganography technique for communication data a lot of firmly between 2 locations is projected [15].

High capacity and security steganography using discrete wavelet transform (HCSSD). During this paper the two level wavelet transform is applied as cover and payload. The payload wavelet coefficients square measure encrypted and coalesced with wavelet coefficients of cover image to generate stego coefficients supported the embedding strength parameters alpha and beta [16].

A novel steganography scheme supported number wavelet transform and Genetic formula. Simulation results show that the novel scheme outperforms adaptational steganography technique supported number wavelet transform in term of peak signal to noise magnitude relation and capacity, 35.17 sound units and 500th respectively [17].

Embedding process stores up to 4 message bits in each number co-efficient for all the transform sub-bands. This paper presents a abstract view of the digital steganography & exploits the use of a host information to cover a piece of knowledge that is hidden directly in media content, in such the way that it is unperceivable to an individual's observer, however easily detected by a laptop [18].

A technique for image steganography supported DWT. This paper presents a unique technique for Image steganography supported DWT, where DWT is employed to remodel original image (cover image) from spatial domain to frequency domain. First, 2 dimensional discrete wavelet transform (2-D DWT) is performed on a grey level cover image of size M × N and Huffman coding is performed on the secret messages/image before embedding. Then each little bit of Huffman code of secret message/image is embedded within the high frequency coefficients resulted from discrete wavelet transform. Image quality is to be improved by conserving the wavelet coefficients within the low frequency sub-band [19]. As compared to the current transform domain information concealing strategies this scheme can provide an efficient capacity for information concealing without sacrificing the initial image quality [20].

A new formula to cover text in any colored image of any size using wavelet transform. It improves the image quality and imperceptibility. Their technique sustains the protection attacks. This new technique provides better physical property and security of communication. This technique provides double security by involving blowfish that satisfies the requirement of imperceptibility [21].

LSB primarily based edge adaptational image steganography. Edge adaptational stenography on

frequency domain improves security and image quality compared to the sting adaptational stenography on spatial domain [22].

A new technique of steganography technique supported DWT transform. The projected technique has ability to cover secret message in a very digital image. The secret message is embedded into the image by dynamical wavelet co-efficient. The standard of the stego image is of the projected technique is extremely close to that of the initial one [23].

The simplest insertion technique in steganography is LSB replacement steganography. Within the LSB replacement technique, the least vital little bit of the element values square measure replaced with the bit values of the message. The method of sleuthing the secret message hidden within the cover media through steganography is understood as steganalysis. Steganalysis strategies are devided in two categories, one that attacks color images or grayscale images and second one that attacks on each color and grayscale images. However, regardless of the said kind of image, some of the steganalysis strategies attack solely on LSB embedding, whereas others attack on completely different strategies that conjointly include LSB embedding. Few of the steganalysis strategies suspect the message hidden within the image whereas few alternative steganalysis strategies observe the length of the message hidden within the image [24].

A steganalysis technique uses autocorrelation coefficients in colour and grayscale images. They recommend that insertion of secret message weakens the correlation between the neighbor pixels and thereby enable one to observe the message [25].

Abdelwahab and Hassaan [26] projected a data concealing technique within the DWT domain that decomposed each secret and canopy images with 1-level DWT. The disadvantage of this technique is that the extracted information isn't completely as same as the embedded original version. This is improved by Neda Raftari and Ruler Masoud Eftekhari Moghadam [27]. World Health Organization propose a new image steganography technique supported IWT and Munkres' assignment formula that embeds secret image in frequency domain of cover image with high matching quality. The development is obtained with higher computation. Here each cover and secret images square measure grey scale images.

El Safy, R.O, Zayed. H. H, EI Dessouki. A [28], used an adaptational steganographic technique supported IWT, that improves the concealing capacity and PSNR compared to DWT technique projected by B. Lai and L. Chang [29]. The concealing capacity and PSNR square measure further improved by Elham Ghasemi, Jamshid Shanbehzadeh and Bahram ZahirAzami [30], World Health Organization use a steganographic technique supported IWT and Genetic formula. silvia Torres-Maya, Mariko Nakano-Miyatake and Hector Perez-Meana propose a picture steganography system supported Bit Plane complexness Segmentation (BPCS) and IWT [31], within which the data is hidden in bit planes of subband wavelet coefficients obtained by using the IWT. To increase information concealing capacity the expendable IWT constant live outlined by a complexness measure using BPCS.

Guorong Xuan et al [32], propose a watermarking technique using IWT within which the watermark is embedded within the middle bit planes of the IWT coefficients within the middle and high frequency subbands. All told these papers message bits square measure hidden in grey scale image. Within the following paragraph some of the papers in color image steganography field square measure reviewed. Masud, Karim S.M., Rahman, M.S., Hossain, M.I. [33], projected a new approach supported LSB using secret key.

The secret key encrypts the hidden data and then it is hold on into completely different position of LSB of image. This provides superb security. Xie, Qing., Xie, Jianquan., Xiao, Yunhua [34]., projected a technique within which the knowledge is hidden all told RGB planes supported HVS (Human Visual System). This degrades the standard of the stego image.

In the technique projected by Sachdeva S and Kumar A, [35], the Vector quantisation (VQ) table is employed to cover the secret message that will increase the capacity and conjointly stego size. the method projected by subgenus Chen, R. J., Peng, Y. C., Lin, J.J., Lai, J. L., Horng, S. J [36], presents the novel multi-bit bitwise adaptational embedding formula for

information concealing by evaluating the foremost similar value to switch the initial one. Roy, S., Parekh, R., [37] projected an improved steganography approach for concealing text messages at intervals lossless RGB images which is able to suffer from withstanding the signal processing operations. Minimum deviation of fidelity primarily based information embedding technique has been projected by Mandal, J.K., Sengupta, M., [38] where two bits per byte are replaced by choosing the position willy-nilly between LSB and up to fourth bit towards mutual savings bank.

A DWT primarily based frequency domain steganographic technique, termed as WTSIC is also projected by equivalent authors [39] where secret message/image bits stream square measure embedded in horizontal, vertical and diagonal components. Shejul, A. A., Kulkarni, U.L [40], projected an formula in that binary images square measure considered to be secret images which square measure embedded within the quilt image by taking the HSV (Hue, Saturation, Value) values of the quilt image into thought. The secret image is inserted into the quilt image by cropping the quilt image in keeping with the skin tone detection and then applying the DWT. during this technique the capacity is just too low.

Sarreshtedari, S., Ghaemmaghami, S [41], projected a technique to realize a better quality of the stego image using BPCS (Bit Plane complexness Segmentation) within the wavelet domain. The capacity of each DWT block is estimated using the BPCS. Rubab, S., Younus, M., [42], projected a posh technique using DWT and Blowfish cryptography technique to cover text message in color image.

III. PROPOSED SYSTEM

High Level Design:

Design is one in each of the foremost necessary phases of code development. The planning may additionally be a precise methodology throughout that a system organization is established that's able to satisfy the sensible and non-functional system wants. Huge Systems area unit forever area unit rotten into sub-systems that offer few connected set of services. The planning process output is an architecture description. With regular analysis and improvement modish of algorithm, steganography taken as a big desiring to cover information and to boot the present work appears that it had been plenty of efficient doggo a plenty of information. GA is applied to understand associate optimum mapping perform to chop back the error distinction between the input cover and also the stego image and use the block mapping methodology to preserve native image properties and to chop back the complexness of algorithm. Optimal component adjustment process applied to increase the hiding capability of this algorithm compared to different existing systems.

Design Problems

The proposed work presents a replacement steganographic technique so as to embed hatful of information in colored images whereas keeping the activity degradation to a minimum level victimization whole number riffle rework (IWT) and Genetic algorithm (GA). This technique permits concealment a data in uncompressed color image. Our motivation to hide knowledge in images is to produce security to pictures that contain crucial knowledge. Proposed approach depends on LSB technique which is able to interchange more than one bit from each component to hide secret message, but the protection of the key knowledge may be improved by combining the smallest amount important bit and riffle rework. The aim of the {planning|the look} is to plan the solution of a problem given by the document wants. This specific part is that the start in moving from disadvantage to the solution domain. The planning of the system is that the most vital issue affecting the standard of the computer code package and contains a significant impact on the coming phases, in the main testing and maintenance. The proposed work is basically experimental test-bed for analysis of RS-attack victimization LSB what is more as genetic algorithm.

Assumptions and Dependencies

1. The first assumption of the work is that the user is taking the input of original image and not any processed image or manipulated image. The secondary assumption is that the user is predicted to use the standard cryptography algorithm in an exceedingly most secure system and network.

2. The fundamental dependency of the work is to run the applying, user wants the MATLAB setting and to use application and appraise its basic conception, user wants associate noise free image and information in plain text format only.

Constraints

The application depends on the optimisation victimization genetic rule inside the present steganographic application. Here limitation is that it has been found that whenever an image input is subjected to such kinds of process then there's several loss of actual quality of image. Thus on resist RS analysis, the impact on the relation of pixels should be stipendiary which can't be achieved by adjusting wholly different bit planes. The implementation may be procedure infeasible in non theoretical application. Thus for overcome this limitation, GA is applied to calculate the upper adjusting mode that the image quality will not be degraded to higher extent.

Proposed System

In the proposed methodology, the message is embedded on whole number riffle rework coefficients supported Genetic algorithm. Thereafter, OPAP algorithm is applied on the obtained embedded image. Genetic algorithm to find a mapping performs for all the image blocks has been used. In GA methodology, a body is encoded as an array of 64 genes containing permutations 1 to 64 that point to range of component s in each block. The most plan of applying OPAP is to minimize the error between the quilt and so the stego image. In this work, we tend to adopted genetic algorithm to search for a best adjustment matrix. Genetic algorithm could be a basic algorithm for optimization. It transforms an optimization or search downside because the process of body evolution. Once the best each is chosen when several generations, the optimum or sub-optimum resolution is found. Genetic algorithm necessary operations square measure reproduction, crossover and mutation.

The figure 1 represents the real operative steps of the developed vogue. Within the process the program helps thus as give a program to handle the developed model and to access the developed module. At the origination, the quilt image is chosen for embedding the data. Then the text knowledge or the message is to be hand-picked thus, thus on accomplish the motive of steganography the stego key appointed thus at the alternative terminal the data may be retrieved by the key. Once the Key has been provided, the real application development for the RS analysis is started with the help of robust GA improvement. In this technique initially the message is to be embedded in cover image. Genetic rule is enjoying a very important role for embedding a lot of and a lot of knowledge within the image. Within the architecture of the developed system the whole number to whole number riffle rework has been done. Once the data has been embedded into the image file, then once embedding the image is again recovered thus it's now able to be transmitted over the channel. On the alternative hand at the receiver terminal or the extraction terminal with the accurate assignment of the stego key the data is retrieved accurately.

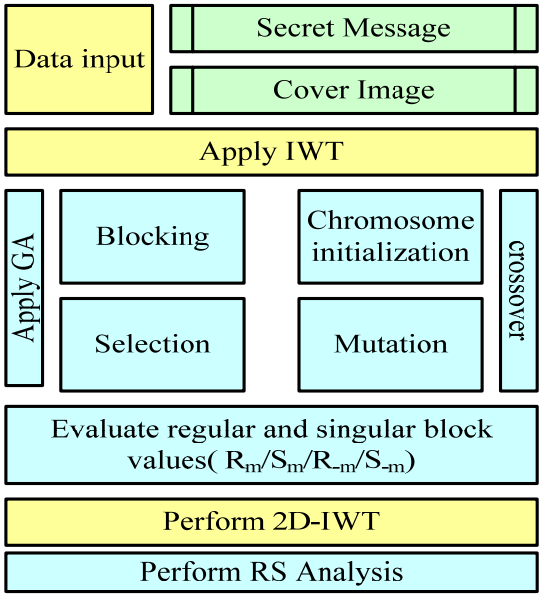

Fig. 1 System Architecture of the proposed work

IV. PROPOSED WORK

The detailed study, analysis and development measure distributed in the system design a section of the presentation. In the meantime, we have a procedure to measure planning to be discussing the detail of the proposed system and hence developed. During this section, details and flow chart of every module has been described. The structure chart shows work flow, the

helpful descriptions of measurement conferred in the flow chart diagrams.

Embedding Algorithmic Program

The projected model is ready by using two fundamental modules as explained below:

Step1: Scan the duvet image file into a two dimensional decimal array to handle the file information additional easily.

Step2: Histogram modification is to stop overflow or underflow that happens when the modified values in whole wave coefficients produce stego-image constituent values to exceed 255 or to be smaller than 0. This problem was found to be caused by the values close to 255 or zero.

Step3: Divide the duvet image into 8x8 non overlapping blocks. By this division every 8x8 block are often classified as a sleek or advanced block.

Step4: Transform every block to the transform domain using Haar wavelet transform that prodeuce result in four sub bands LLI, LHI, HLI and HHI.

Step5: Calculate concealing capability of every coefficient. From experiments, we have a tendency to found that as we have a tendency to lower the bits wont to hide the secret message in the LL sub band the resulted distortion in the stego-image becomes lower; in order that we have a tendency to modified this concealing capability operate by using completely different ranges for k for the ICSH, metric capacity unit and HH sub bands where its values square measure form 1 to four. For the LL sub band the value of k is equal to zero and in some cases the bits used is fixed to solely bits to reinforce the stego-image quality.

Step6: Insert L bits of message into the corresponding indiscriminately chosen coefficients. Random selection of coefficients provides additional security where the sequence of the message is just famous to each sender and receiver by using an antecedently given secret key.

Step7: Apply best constituent adjustment algorithmic program, while taking into thought that every modified coefficient stays in its concealing capability range where each price of L is calculated according to the absolute price of the wave coefficients any vital modification during this price can produce completely different price of L to be calculated at the receiver. The most idea of using the optimum constituent adjustment (OPA) algorithmic program is to reduce the error difference.

V. CONCLUSION AND FUTURE ENHANCEMENTS

In this work, we have proposed a data hiding scheme that hides data into the integer wavelet coefficients of an image. The system combines a data hiding technique and the optimum pixel adjustment algorithm to increase the hiding capacity of the system compared to other systems. The proposed system hide secret data in a random order using a secret key only known to both sender and receiver. In this method, embeds different number of bits in each wavelet co-efficicient according to a hiding capacity function in order to increasing the hiding capacity without losses of the visual quality of resulting stego image. The proposed system also minimizes the error difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm.

The current proposed method is only applicable on colored image as well as on gray scaled image but not applicable on audio, video and other biometrics yet. Very large amount of message cannot feed in image. So the future work should focus on large message embedding, improve the data or message embedding capacity, security against attacks, hiding techniques apply to audio & video.

VI. REFERENCES

[1] N. Wu and M. Hwang,"Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan.2007..

[2] C. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469-474, Mar. 2004.

[3] Changa, C. Changa, P. S. Huangb, and T. Tua, "A Novel bnage Steganographic Method Using Tri-way Pixel-Value Differencing," Journal of Multimedia, Vol. 3, No.2, June 2008.

[4] H. H. Zayed, "A High-Hiding Capacity Technique for Hiding Data in images Based on K-Bit LSB Substitution," The 30th International Conference on Artificial Intelligence Applications (ICAIA - 2005) Cairo, Feb. 2005.

[5] S. Lee, C.D. Yoo and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Transactions on Information Forensics and Security, Vol. 2, No.3, Sep. 2007, pp. 321-330.

[6] M. Ramani, Dr. E. V. Prasad and Dr. S. Varadarajan,"Steganography Using BPCS the Integer Wavelet Transformed bnage", UCSNS International Journal of Computer Science and Network Security, VOL. 7 No.7, July 2007.

[7] P. Chen, and H. Lin, "A DWT Approach for bnage Steganography,"International Journal of Applied Science and Engineering 2006. 4, 3:275:290.

[8] Lai and L. Chang, "Adaptive Data Hiding for bnages Based on Harr Discrete Wavelet transform," Lecture Notes in Computer Science,Volume *4319/2006.*

[9] A. Westfeld, "F5a steganographic algorithm: High capacity despite better steganalysis," 4th International Workshop on Information Hiding, pp.289-302, April 25-27, 2001.

[10] D. Kahn., The Codebreakers, the comprehensive history of secret communication from ancient times to the Internet, Scribner, 1996.

[11] T. Morkel, J.H.P. Eloff, M.S. Olivier, An Overview of Image Steganography, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[12] T. R. Gopalakrishnan Nair, Suma, Manas, Genetic Algorithm to Make Persistent Security and Quality of Image in Steganography from RS Analysis, Swarm Evolutionary and Memetric Computing Conference (SEMCCO), Vishakhapatnam, 2012.

[13] 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.

[14] 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.

[15] R.J. Anderson and F.A.P. Petitcolas, On the Limits of Steganography, J. Selected Areas in Comm., vol. 16, no. 4, 1998, pp. 474–481.

[16] Souvik Bhattacharyya and Gautam Sanyal, Data Hiding in Images in Discrete Wavelet Domain Using PMM, International Journal of Electrical and Computer Engineering, 5:6 2010.

[17] D. Kahn., The Codebreakers, the comprehensive history of secret communication from ancient times to the Internet, Scribner, 1996.

[18] Gustavus J. Simmons, The prisoners problem and the subliminal channel, Proceedings of CRYPTO, 83:51–67, 1984.

[19] Ross J. Anderson. and Fabien A.P.Petitcolas, On the limits of steganography, IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright and Privacy Protection, 16:474–481, 1998.

[20] S.P.Mohanty, Digital Watermarking: A Tutorial. 1999.

[21] G. Davida, M. Chapman and M. Rennhard, A practical and effective approach to large-scale automated linguistic steganography, Proceedings of the Information Security Conference, pages 156–165, October 2001.

[22] Jr. L. M. Marvel, C. G. Boncelet and C. T. Retter, Spread spectrum image steganography, IEEE Trans., on Image Processing, 8:1075–1083, 1999.

[23] Nasir Memon, R. Chandramouli, Analysis of LSB based image steganography techniques, Proceedings of IEEE ICIP, 2001.

[24] Kran Bailey and Kevin Curran, An evaluation of image based steganography methods, International Journal of Digital Evidence Fall 2003, 2003

[25] Ahmed A. Abdelwahab and Lobna A. Hassaan, "A Discrete Wavelet Transform Based Technique For Image Data Hiding", 25th National Radio Science Conference, 2008.

[26] Neda Raftari and Amir Masoud Eftekhari Moghadam, "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", Sixth Asia Modelling Symposium, 2012, pp 87-92.

[27] El Safy, R.O, Zayed. H. H, El Dessouki. A, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", IEEE conference, 2009, pp 111-117.

[28] Lai and L. Chang, "Adaptive Data Hiding for images Based on Harr Discrete Wavelet transform," Lecture Notes in Computer Science, Volume 4319, 2006.

[29] Silvia Torres-Maya, Mariko Nakano-Miyatake and Hector Perez-Meana, "An Image Steganography Systems Based on BPCS and IWT", 16th IEEE International Conference on Electronics, Communications and Computers, 2006.

[30] Guorong Xuan, Jiang Zhu, Jidong Chen, Yun Q. Shi, Zhicheng Ni and Wei Su, "Distortionless data hiding based on integer wavelet transform", IEEE Electronic letters, December 2002 Vol. 38 No. 25, pp. 1646-1648.

[31] Masud, Karim S.M., Rahman, M.S., Hossain, M.I., "A New Approach for LSB Based Image Steganography using Secret Key", 14th International Conference on Computer and Information Technology (ICCIT 2011), (Dhaka, Bangladesh 22-24 December, 2011), IEEE Conference Publications, 286-291.

[32] Xie, Qing., Xie, Jianquan., Xiao, Yunhua, "A High Capacity Information Hiding Algorithm in Color Image", 2nd International Conference on E-Business and Information System Security (EBIISS2010), (Wuhan, China, 22-23 May, 2010), IEEE Conference Publications, 1-4.

[33] Sachdeva, S and Kumar, A., "Colour Image Steganography Based on Modified Quantization Table", Second International Conference on Advanced Computing and Communication Technologies (ACCT), (Rohtak, Haryana, India, 7-8 January 2012), IEEE Conference Publications, 309-313.

[34] Chen, R. J., Peng, Y. C., Lin, J. J., Lai, J. L., Horng, S. J., "Novel Multi-bit Bitwise adaptive Embedding Algorithms with Minimum Error for Data Hiding" Fourth International Conference on Network and System Security (NSS 2010), (Melbourne, Australia, 1-3 September 2010), IEEE Conference Publications, 306-311.

[35] Roy, S., Parekh, R., "A Secure Keyless Image Steganography Approach for Lossless RGB Images", International Conference on Communication, Computing and Security (ICCCS '11), ACM Publications, 573-576.

[36] Mandal, J.K., Sengupta, M., "Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF)", Second International Conference on Emerging Applications of Information Technology (EAIT 2011), (February 19-20 2011), IEEE Conference Publications, 298-301.

[37] Mandal, J.K., Sengupta, M. "Authentication/Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC)", International Symposium on Electronic System Design (ISED), (Bhubaneswar, India, 20-22 December, 2010) IEEE Conference Publications, 225-229.

[38] Shejul, A. A., Kulkarni, U.L, "A DWT based Approach for Steganography Using Biometrics", International Conference on Data Storage and Data Engineering, (Bangalore, India, 9-10 February 2010), IEEE Conference Publications, 39-43.

[39] Sarreshtedari, S., Ghaemmaghami, S. High Capacity Image Steganography in Wavelet Domain. In Proceedings of 2010 7th IEEE Consumer Communications and Networking Conference (CCNC) (Las Vegas, Nevada, USA, 9-12 January 2010), IEEE Conference Publications, 1-5.

[40] Rubab, S., Younus, M.,"Improved Image Steganography Technique for Colored Images using Wavelet Transform", International Journal of Computer Applications, Volume 39- No.14, February 2012, 29-32.

[41] Ghoshal, N., Mandal, J.K., "A Steganographic Scheme for Colour Image Authentication (SSCIA)", International Conference on Recent Trends in Information Technology (ICRTIT 2011), (Madras Institute of Technology, Chennai, India June 03-05, 2011), IEEE Conference Publications, 826-831.

[42] Ghoshal, N., Mandal, J.K., "Controlled Data Hiding Technique for Color Image Authentication in Frequency Domain (CDHTCIAFD)", Second International Conference on Emerging Applications of Information Technology,IEEE Conference Publications, 284-287.