International Journal of Computer Architecture and Mobility

(ISSN 2319-9229) Volume 3 -Issue 3, May 2015

A Survey on Various Steganography Techniques and Their Modifications

Ritesh Upadhyay[#1], Prof. Y. S. Thakur[#2], Dr. D. K. Sakravdia[#3]

[1]*Department of Electronics & Communication Engineering, Ujjain Engineering College, Ujjain, M.P. (India)*

[1] riteshup4u0501@gmail.com, [2] ystgecu@yahoo.co.in, [3] sakravdia@rediffmail.com

Abstract- Information security is becoming very important part of our daily life. Information hiding is the very basic and fundamental step of security in information technology. Steganography is one of the technique by which information hiding can be achieved. The main purpose of steganography which means 'Hidden writing' is to hide the message in a cover media so that others will not be able to notice it. Steganography is a technology where modern data compression, spread spectrum, information theory and cryptographic technologies are brought together to satisfy the need for privacy on the internet. The aim of this paper is to analyze the various steganography techniques used for information hiding and to identify the areas in which this technique can be implemented, so that the human race can be benefited at large.

Keywords- steganography, cryptography, stego-object, AES, spatial domain, stego-key.

I. Introduction

Steganography is the art and science of hiding the fact that communication is established and will take place. Using the various steganography methods, we can integrate a confidential message inside a packet of normal looking information and transfer it without knowing to anyone of the existence of the confidential text or message. Security in information technology is a very essential method for data transfer confidentially. Steganography is one of the ways used for secure transmission of confidential information. Hiding information in media (like audio or video) is less suspicious than communicating encrypted files. The basic but important purpose of applying steganography techniques is to convey the information secretly by concealing the very existence of information in some other medium such as audio, video or image. These objects are called cover object or medium object of the various steganographic methods. The confidential information or message can also be of types like text, picture, image or video. These objects are known as message object. After application of steganographic method the generated output file is known as stego-object.

II. Principles of Steganography

The secret message is embedded inside the cover object in encrypted format by using a hiding algorithm and it is sent to a receiver over a network. The receivers then decrypt the message by applying the reverse process on the cover data and reveal the secret data [1].

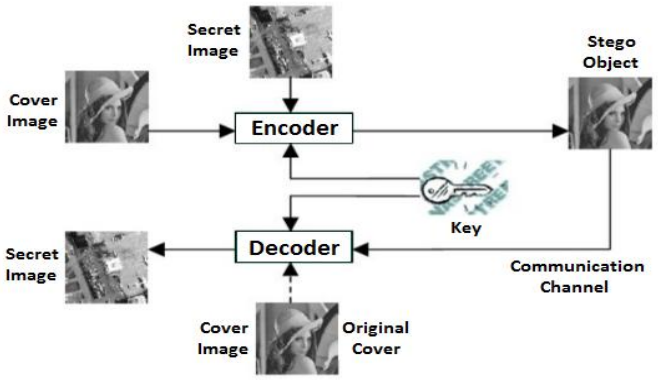

Fig. 1: The principle of Steganography

Fig. 1 shows the principle of Steganography. Steganography algorithm, tries to preserve the perceptive properties of the original image. A suitable image, called as cover/ carrier, is chosen. The secret message is then embedded into the cover using the Steganography algorithm, in a way that does not change the original image in a human noticeable way. The result is new image, the stego-image, which looks similar to the original image.

III. STEGANOGRAPHY TECHNIQUES

A. Categories of Steganographic techniques

Steganography is classified into 3 categories:

1) Pure steganography where there is no stego key. It is based on the assumption that no other party is aware of the communication.

2) Secret key steganography where the stego key is exchanged prior to communication. This is most susceptible to interception.

3) Public key steganography where a public key and a private key is used for secure communication.

B. Classification of Steganographic Methods

Steganography methods can be classified mainly into six categories (Fig. 2), although in some cases exact classification is not possible [2].

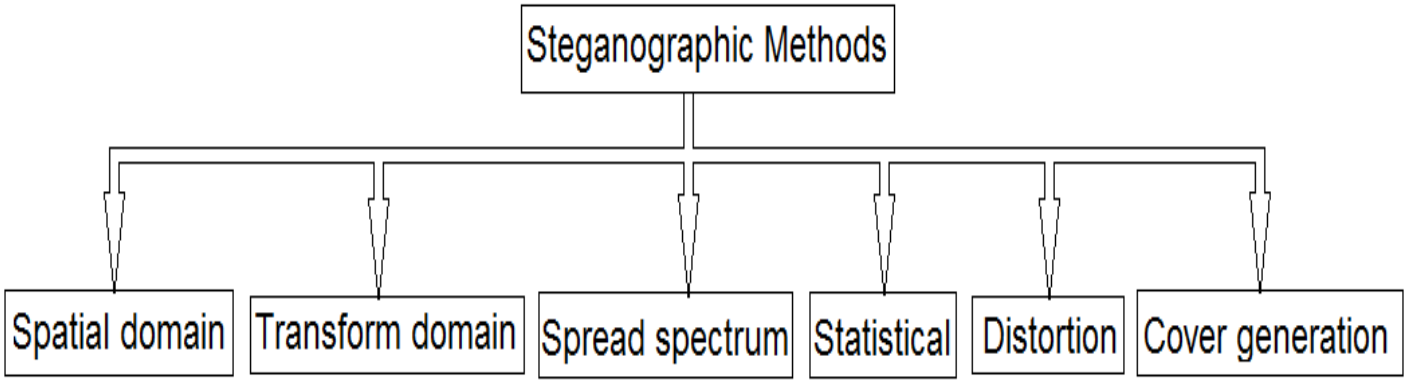

Fig. 2: Classification of Steganographic Methods

1) Spatial domain methods substitute redundant parts of a cover with a secret message (Substitution method).

2) Transform domain techniques embed secret information in a transform space of the signal (frequency domain)

3) Spread spectrum techniques adopt ideas from spread spectrum communication.

4) Statistical methods encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.

5) Distortion techniques store information by signal distortion and measure the deviation from the original cover in the decoding step.

6) Cover generation methods encode information in the way a cover for secret communication is created.

IV. Types of Steganography

In modern approach, depending on the nature of cover object, steganography can be divided into five types:

A. Text Steganography

Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters). It includes line-shift coding, word-shift coding and feature coding.

B. Image Steganography

Images are the most popular cover objects used for steganography. In the domain of digital images many different file formats exist and for these file formats different algorithms exist. These different algorithms used are least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter, Algorithms and transformations

C. Audio Steganography

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods like LSB coding, Phase coding, spread spectrum, Echo hiding which are used for audio steganography.

D. Video Steganography

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds.

E. Protocol Steganography

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. There are covert channels in the layers of the OSI network model where steganography can be used.

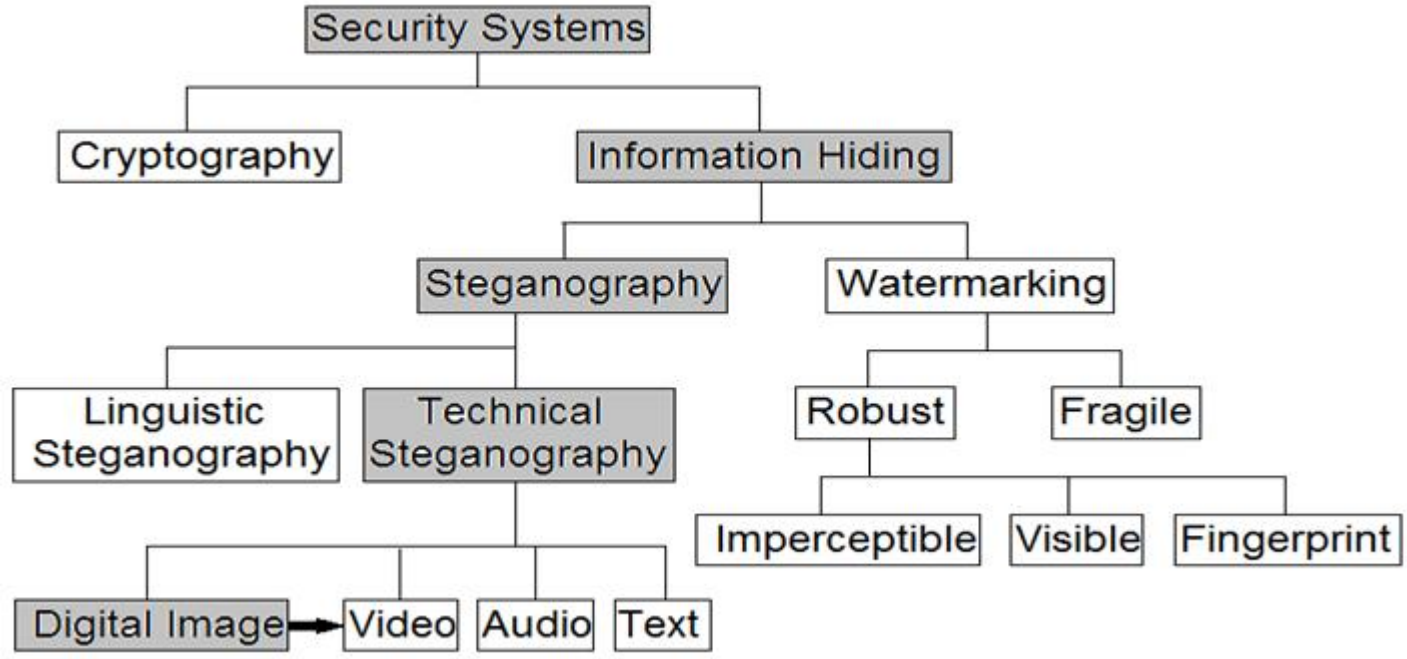

Fig. 3: The different embodiment disciplines of Information Hiding. The arrow indicates an extension and the colored block indicates the focus of our study.

V. Requirements of Steganographic Methods

A. Invisibility

The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised.

B. Payload capacity

Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore requires sufficient embedding capacity.

C. Robustness against statistical attacks

Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a 'signature' when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.

D. Robustness against image manipulation

In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.

E. Independent of file format

With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.

F. Unsuspicious files

This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

VI. Literature Review

A. Spatial Domain Methods (Substitution Method)

In Mamta Juneja et. al's [3] research paper a secured robust approach of information security is proposed. It presents two component based LSB (Least Significant Bit) methods for embedding secret data in the LSB's of blue components and partial green components of random pixel locations in the edges of images. An adaptive LSB based steganography is proposed for embedding data based on data available in MSB's of red, green, and blue components of randomly selected pixels across smooth areas. It is more robust as it is integrated with an Advanced Encryption standard (AES).

In Shamim Ahmed Laskar et.al's[4] method data is embedded into the red plane of the image and the pixel is selected using a random number generator. It is almost impossible to notice the changes in the image. A stego key is used to seed the PRNG (Pseudo Random Number Generator) to select pixel locations. This paper focuses on increasing the security of the message and reducing distortion rate.

In S.Shanmuga Priya et. al's [5] article the authors propose a novel method based on LSB. Data embedding is performed using a pair of pixels as a unit, where LSB of the first pixel carries one bit of information and a function to two pixel values carries another bit of information. The proposed method shows better performance in terms of distortion and resistance against existing steganalysis. Embedding is done in the sharper edge regions using a threshold. PSNR value is compared for adaptive and non-adaptive techniques of data hiding in gray scale & color images.

In B.Sharmila et. al.'s [6] article, the authors propose an algorithm which works on colour images (JPEG). The edges are chosen for data hiding to improve robustness. The regions located at the sharper edges present more complicated statistical features and are highly dependent on the image contents. It is also more difficult to observe changes at the sharper edges than in smooth regions. In the embedding procedure, the RGB components are separated, and based on a shared key, one or more components are selected. The cover image is divided into non-overlapping blocks. Each block is rotated by a random degree determined by a secret key. The resulting image is rearranged as a row vector V by raster scanning. The secret message is encrypted and by using LSBMR, 2 secret bits can be embedded into each embedding unit. The message is embedded after calculating the capacity estimation using a threshold.

In Shweta Singhal et.al's [7] paper a new image steganography scheme is proposed in the spatial domain. In the technique, one byte of blue factor of pixels of an image has been replaced with secret bits of text data, which results in better image quality. A stego key is used for security purposes.

In Rajkumar Yadav et. al.'s paper [8], the authors present a study of a new method for insertion of message in an image. The last two bits of pixel value are used for insertion and retrieval of message. If the last two bits of pixel value are 00 or 10, we can insert 0, else by adding/subtracting 1 at that pixel value we can insert 0. Similarly 1 is inserted if last two bits are 01 or 11. For increased security, message is embedded at pseudo random locations. The message is retrieved similarly based on the pixel values of the last two bits.

In M.B.Ould MEDENI et.al.'s article [9], the authors propose a novel method for hiding information within the spatial domain of the gray scale image. The Pixel Value Differencing (PVD) method segments the cover image into non-overlapping blocks containing two connecting pixels and modifies the pixel

difference in each block (pair) for data embedding. While embedding secret data, each pixel is split into two equal parts. The number of 1's in the most significant part is counted and the secret message is embedded in the least part according to the number of corresponding bits. The proposed method is based on four-pixel differencing and LSB substitution.

In Weiqi Luo et. al.'s paper [10], the authors propose an edge adaptive scheme which can select the embedding regions according to the size of the secret message and the difference between two consecutive pixels in the cover image. In the data embedding stage, the scheme first initializes some parameters, which are used for estimating the capacity of the selected regions. Finally stego image is obtained after pre-processing. A region adaptive scheme is applied to the spatial LSB domain and the difference between two adjacent pixels is used as a criterion for region selection and LSBMR (LSB Matching Revisited) as the data hiding algorithm.

In C.H.Yang et. al.'s article [11], a predictive method to enhance the histogram-based reversible data hiding approach is proposed. Two interleaving predictive stages are used. Most pixels are predicted by their two neighborhood pixels and four neighboring pixels in the column-based and chess-board based approach. The difference value of each pixel between the original image and the stego-image remains within ± 1. In interleaving predictions, pixels in odd columns will be predicted by pixels in even columns or vice versa. In the embedding process predictive error values of odd columns are used to generate a histogram to embed secret data. The predictive error values are converted to get the stego-image.

In G.Sahoo et. al.'s [12] article the authors recommend the use of a movie clip as carrier file to increase the capacity of secret data. The methodology works on the concept of replacement of entire non-sensitive pixel and the substitution of some part of the sensitive pixel with secret data.

A movie clip is a temporal sequence of two dimensional samples of visual field with each sample being a frame of the movie. The parts of a movie clip can be divided into moving and static parts.

The static and the dynamic parts can be obtained through Pixel Level Analysis, Likelihood Analysis or Colour Histogram Technique and stored in a static and dynamic buffer. In static portion embedding process one pixel is used to store three characters using the formula xij = i+(j– 1)*d where i is the initial location, j is character of the secret data and d is the distance between two embedding pixels. In dynamic portion embedding MSB method is used. A different stego-key is used for the dynamic portion. Main advantage of this method is more hiding capacity.

In Bawankar Chetan.D et. al.'s article [13] a prioritized sub blocks by pattern matching scheme is used to embed the code and a micro controller used for sake of security where it transmits a pre-programmed key at the beginning of each process. The steganalysis algorithm is continued only if the received key is correct at the destination; otherwise retrieving secure information from cover image is not accomplished. Perceptual multimedia sources enable data embedding as well as lossy compression either imperceptibly or with a controllable amount of perceptual degradation, whereas non-perceptual sources like text and executable codes require loss-less processing, transmission and storage. The image is divided into blocks. A block is selected for embedding based on a pattern. Several blocks are rejected due to various reasons like high visibility, non reversible at receiver side etc. In each sub block only the middle pixel is selected for hiding information. The secret message is encrypted to enhance security. In this paper the authors propose a steganographic model in which the hidden message can be composed and inserted in the cover in real-time. This is realized by designing and implementing a secret key steganographic micro architecture employing Field Programmable Gate Arrays FPGA. Four steganographic algorithms were found to be suitable for hardware implementation.

In Tanmay Bhattacharya et. al.'s article [14] the authors use a session based encryption and cross fold transposition for embedding. The secret text is converted to its binary form and cross fold transposition is performed. This binary form is perturbed by genetically generated session-key and embedded within the host image. For extraction both the stego image and the original image along with the session-key is sent.

In Chin-Chen Chang et.al.'s paper [15] an adaptive method is proposed. Data is hidden based on codeword grouping. A set of code words generated using palette generation algorithm is employed in index-based images. A code word grouping based steganographic scheme for index encoding images is presented. The relationship of code words is explored to group different member sub-clusters. The size of the sub-cluster determines the hiding capacity. To enhance hiding capacity sub-clusters with larger members are grouped together & sub-clusters with smaller members are grouped together. In the embedding procedure the sub-cluster to which the closest searched codeword belongs is identified, and the original encoded codeword is modified to hide secret message. The number of sub-cluster members indicates how many bits of secret message can be embedded. A set of thresholds is used to determine members of sub-cluster.

Therefore choosing an adequate threshold is important. To improve security the sequence of embedding pixels is re-organized using a pseudo random generator.

B. Transform Domain Methods

In Hemalatha.S et.al's [16] paper, the authors propose a method that uses two gray scale images of size 128 x 128 that are used as secret images and embedding is done in RGB and YCbCr domains. The quality of stego images is good in RGB domain by comparing the PSNR values.

The authors have used Integer Wavelet Transform (IWT) to hide secret images in the color cover image. The authors have compared the PSNR values and image quality when embedding is done in the RGB and YCbCr domains.

In another article by Hemalatha .S et. al. [17] Integer Wavelet Transform (IWT) have been suggested to hide multiple secret images and keys in a color cover image which is more efficient.

The cover image is represented in the YCbCr color space. Two keys are obtained, encrypted and hidden in the cover image using IWT. In Keith.L. Haynes 's article [18] the author studies the use of image steganography to breach an organization's physical and cyber defenses. The proposed method utilizes computer vision and machine learning techniques to produce messages that are undetectable and if intercepted cannot be decrypted without key compromise. To avoid detection DWT (Discrete Wavelet Transform) is used. The goal of a computer vision system is to allow machines to analyze an image and make a decision as to the content of that image. The computer vision can be categorized as Model-Based & Appearance Based which uses example images and machine learning techniques to identify significant areas or aspects of images that are important for discrimination of objects contained within the image. Machine learning is different from human knowledge/ learning. A computer has to make decision of the presence of a face based on the numbers contained in a 2D matrix.

The feature is identified by using Haar feature selection. The goal is to identify the set of features that best distinguishes between images in the different classes. In the proposed method the cover image does not contain a secret message, rather the classification of the image yields the hidden message. Since the proposed algorithm utilizes ordinary unmodified images, there are no inherent indicators of covert communication taking place.

In S.Arivazhagan et. al.'s work [19] the authors propose a method that works in the transform domain and attempts to extract the secret almost as same as the embedded one, maintaining minimal changes to cover image by using techniques like median maintenance, offset & quantization. A modified approach for embedding colour images within colour images is proposed and it overcomes the limitations in embedding. Arnold Transform is applied on the secret image to increase robustness. This transformed image is then split into the three colour planes R, G, B and are subjected to DWT individually, converted to bit stream and then concatenated to be embedded in the cover image which is also subjected to DWT.

In Anindya Sarkar et. al.'s paper [20] the authors propose a Matrix Embedding with Repeat Accumulate (ME-RA) based steganography in which the host coefficients are minimally perturbed such that the transmitted bits fall in a cosset of a linear code, with the syndrome conveying the hidden bits. The hiding blocks are pseudo-randomly chosen. A powerful repeat accumulate code is used for error correction. The authors have compared QIM (Quantization Index Modulation) and ME-RA methods. The comparisons with a slight modification of the

MERA (puncture and non-shrinkage) methods with different decoding methods are also tabulated.

The authors highlight that the use of ME instead of QIM within the YASS (Yet another Steganographic Scheme) that provides improved steganalysis performance but software complexity is more.

In Prosanta Gope et. al.'s article [21], the authors introduce an enhanced JPEG steganography along with a suitable encryption methodology using a symmetric key cryptographic algorithm.

The JPEG cover image is broken into 8 x 8 blocks of pixel. DCT is applied to each block and quantization is done and data is encrypted using a new encryption method which uses CRC checking.

C. Statistical Methods

In Jessica Fridrich et.al.'s research paper [22] the authors propose a reversible embedding scheme for VQ-compressed images that is based on side matching and relocation. The new method achieves reversibility without using the location map. Even a tiny distortion of the original content is not applicable in some sensitive applications such as military, medical / fine art data. Therefore the value of reversible methods of steganography is increasing. VQ (Vector Quantization) is a popular compression technique because of its simple encoding and decoding procedures. To achieve better imperceptibility the codebook is partitioned into several clusters before embedding. The input needed will be a VQ compressed image, a stream of secret bits, a super codebook SC, clusters of the super codebook SC and multiple hit maps. The output will be a VQ stego image. Block X in the cover image will fall into one of the three following cases. If X is equal to the ith codeword of Go, the embedding process is invoked. If X is equal to the ith codeword of G1, no secret bit can be embedded and a compensation procedure is needed to avoid conflicting with case 1. If X does not belong to G0 U G1, no secret bit can be embedded and X is skipped. Secret bits can be embedded only in case 1.

D. Distortion Methods

In M.B.Ould MEDENI et.al.'s article [23], the authors use error correcting codes in steganographic protocols. The method referred to as matrix encoding, requires the sender and recipient to agree in advance on a parity check matrix H. The cover medium is processed to extract a sequence of symbols v, which is modified into s to embed the message m, s is sometimes called the stego-data, and modifications on s are translated on the cover-medium to obtain the stego-medium. In this article, a relationship between steganographic algorithms and error correcting codes were discussed.

VII. Conclusion & Future Work

In this paper we studied and analyzed different steganographic techniques used for information hiding. The application of steganographic systems mainly range over a wide area from intelligence agencies, medical imaging, internet banking, online elections, military and so on. These varieties of application make steganography a hot topic for study. The type and the size of secret message should be kept in mind while deciding the cover medium (object) to be used for steganography. Currently, digital images are the most popular carrier files that can be used to transmit secret information. Our survey of various steganographic principles will definitely guide us to identify new areas of research and also to improve its applications in the already existing areas.

REFERENCES:

[1] Jagvinder Kaur and Sanjeev Kumar, " *Study and Analysis of various Image Steganography Techniques*" IJCST Vol. 2, Issue 3, September 2011

[2] Stefan Katzenbeiser & Fabien A.P.Petitcolas(1999), "*Information Hiding Techniques for Steganography and Digital Watermarking",* Artech House, Computer Security series, Boston, London.

[3] Mamta Juneja and Parvinder Singh Sandhu, (2013) "*A New Approach for Information security using an Improved Steganography Technique*", Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424.

[4] Shamim Ahmed Laskar and Kattamanchi Hemachandran, (2013) "*Steganography Based On Random Pixel Selection For Efficient Data Hiding*", International Journal of Computer Engineering and Technology, Vol.4, Issue 2, pp.31-44.

[5] S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy, (2012) "*Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain*", International Journal of Engineering Research and Applications,, Vol2, Issue 3, pp. 2632-2637.

[6] B. Sharmila and R.Shanthakumari, (2012) "*Efficient Adaptive Steganography For Colour Images Based on LSBMR Algorithm*", ICTACT Journal on Image and Video Processing, Vol. 2, Issue:03, pp.387-392.

[7] Shweta Singhal, Dr.Sachin Kumar and Manish Gupta, (2011) "*A New Steganography Technique Based on Amendment in Blue Factor*", International Journal of Electronics Communication and Computer Engineering, Vol.2, Issue 1, pp.52-56.

[8] Rajkumar Yadav, (2011) "*A Novel Approach For Image Steganography In Spatial Domain Using Last Two Bits of Pixel Values*", International Journal of Security, Vol.5 Iss. 2 pp. 51-61.

[9] M.B.Ould MEDENI and El Mamoun SOUIDI, (2010) "*A Generalization of the PVD Steganographic Method*", International Journal of Computer Science and Information Security, Vol.8.No.8, pp156- 159

[10] Weiqi Luo, Member, IEEE, Fangjun Huang, Member, IEEE, and Jiwu Huang, Senior Member, IEEE, (2010) "*Edge Adaptive Image Steganography Based on LSB Matching Revisited*", IEEE Transactions on Information Forensics and Security, Vol.5.No.2, pp.201-214.

[11] C.-H. Yang and M.-H. Tsai, (2010) "*Improving Histogram-based Reversible Data Hiding by Interleaving Predictions*", IET Image Processing, Vol.4. Iss. 4 pp. 223-234.

[12] G.Sahoo & Rajesh Kumar Tiwari (2009) "*Hiding Secret Information in Movie Clip: A Steganographic Approach*", International Journal of Computing and Applications, Vol. 4, No.1, pp 103-110.

[13] Bawankar Chetan.D, Hande.K.N, Jaiswal .A.A & Bute. A (2009) " *Pattern Matching With External Hardware For Steganography Algorithm*", International Journal of Information Technology and Knowledge Management, Vol. 2 No.2, pp 289-295.

[14] Tanmay Bhattacharya, Manas Paul & Arindam Dasgupta (2009) "*A Novel session Based Text Encryption & Hiding Technique Using Bit Level Cross Fold Transposition & Genetic Algorithm*", International Journal of Information Technology and Knowledge Management, Vol. 2, No.2, pp.419-423.

[15] Chin Chen Chang, Piyu Tsai & Min-Hui Lin (2004) "*An Adaptive Steganography for Index-Based Images using Codeword Grouping*", Springer-Verlag Berlin Heidelberg 2004, pp.731- 738.

[16] Hemalatha.S, U.Dinesh Acharya and Renuka.A, (2013) "*Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB and YCBCR domains*", International Journal of Advanced Information Technology, Vol.3, No.3, pp.1-9.

[17] Hemalatha.S, U.Dinesh Acharya and Renuka.A, Priya.R Kamnath, (2013) "*A Secure and High Capacity Image Steganography Technique*", Signal & Image Processing – An International Journal, Vol.4, No.1, pp.83-89.

[18] Keith L.Haynes, (2011) "*Using Image Steganography to Establish Covert Communication Channels*", International Journal of Computer Science and Information Security, Vol 9, No.9, pp. 1- 7.

[19] S.Arivazhagan, W.Sylvia Lilly Jebarani, and S.Bagavath (2011) "*Colour Image Steganography Using Median Maintenance*", ICTACT Journal on Image and Video Processing, Vol. 2, Iss:01, pp.246-253.

[20] Anindya Sarkar, Member, IEEE, Upamanyu Madhow, Fellow,IEEE, and B.S.Manjunath, Fellow, IEEE, (2010) "*Matrix Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Steganography*", IEEE Transactions on Information Forensics and Security, Vol.5.No.2, pp.225-239.

[21] Prosanta Gope, Anil Kumar and Gaurav Luthra , (2010) "*An Enhanced JPEG Steganography Scheme with Encryption Technique*", International Journal of Computer and Electrical Engineering , Vol.2.No.5, pp924-930.

[22] Jessica Fridrich, Miroslav Goljan, David Soukal (2006) "*Wet Paper Codes With Improved Embedding Efficiency* ", IEEE Transactions on Information Forensics and Security, Vol 1. No.1, pp 102-110.

[23] M.B.Ould MEDENI and El Mamoun SOUIDI, (2010) "*Steganography and Error Correcting Codes*", International Journal of Computer Science and Information Security, Vol.8.No.8, pp147-149.