ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 2, January 2018

Steganography Techniques for Secured Data Transmission

D. K. Aarthy[1], Humpy Vemulapalli[2], Janani.S[3], Sasikala.E[4]
Assistant Professor[1] ,UG Scholar[2,3,4], Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai
aarthy.d.k@ritchennai.edu.in[1], rkaries264@gmail.com[2], sivajanai16@gmail.com[3], sasielumalai8764@gmail.com[4]

Abstract: Steganography is an art of hiding information in methods that prevent detection of secret message. Steganography is used to transport records from one vicinity to different area thru public channel in hid manner. which will conceal secret information inside the shape of photos, there exists a massive variety of Steganography strategies a few are more complex than others and all of them have respective sturdy and susceptible points. distinct packages might have numerous necessities of the Steganography strategies used. In this paper extraordinary techniques of Steganography has been overviewed. it is also very beneficial within the manner of spotting the requirements of a more Steganographic set of rules and additionally it in brief reflects on which Steganographic methods are extra appropriate for which packages.

Keywords: DES, RSA, Triple DES, Secret Image, Steganography, Image processing, Brute force attacks, Hiding and Un-hiding.

I. Introduction

Image processing is one of the most popular approach that is used to convert an image into virtual form, so one can get an greater image or to extract a few useful facts from it. it is one form of signal dispensation where the input is photograph, video frame or image and output may be photo or characteristics related to that photo.

Image processing is one among the most unexpectedly developing technologies nowadays, with its packages in various factors of a business. It additionally performs the primary position in core studies area in engineering and laptop technological know-how disciplines too. The information hiding techniques are typically labeled into four most important categories which include, Covert channels, Steganography, Anonymity and Copyright marking.

A covert channel is a form of computer security that gives a channel for transfer of data in a manner that the statistics is secured. Robustness and imperceptibility are the maximum important distinctiveness of a hid channel. Copyright marking is a method this is used to shield the intellectual homes. on this kind of method a completely unique brand or a particular mark is embedded along with the piece of records to show the originality of the paintings. The copyright can be robust or sensitive depending upon the requirement. Anonymity is one of the mystery technique of communique in which each the transmitter and the receiver continue to be nameless in order that a 3rd birthday celebration, who's interested on the facts however isn't always a rightful user of the information, looses pathway of it.

There are several classifications wherein steganography may be categorised into sub lessons such as textual content, audio, video or photo steganography, depending upon whether textual content, audio, video or photograph is used as the duvet medium.

Linguistic Steganography (textual content Steganography or Cryptography) makes use of text as the cover media to hide the secret message whereas the technical covert channels paintings via exploiting the loopholes inside the OS, community model, protocols and so forth. In a pc-primarily based audio steganography machine, mystery messages are embedded in digital sound. the name of the game message is embedded by barely changing the binary series of a legitimate document. existing audio steganography software can embed messages in WAV, AU, or even MP3 sound files. [10] proposed a system which uses intermediate features of maximum overlap wavelet transform (IMOWT) as a pre-processing step. The coefficients derived from IMOWT are subjected to 2D histogram Grouping. This method is simple, fast and unsupervised. 2D histograms are used to obtain Grouping of color image. This Grouping output gives three segmentation maps which are fused together to get the final segmented output. This method produces good segmentation results when compared to the direct application of 2D Histogram Grouping. IMOWT is the efficient transform in which a set of wavelet features of the same size of various levels of resolutions and different local window sizes for different levels are used. IMOWT is efficient because of its time effectiveness, flexibility and translation invariance which are useful for good segmentation results.

Out of a majority of these accessible kinds of Steganography, virtual image steganographic strategies are moreover famous most of the researchers as photos are extra commonplace kinds of mediums that are used international for information transmission and additionally due to their data hiding ability.

II. Techniques of Steganography

There are four one of a kind styles of steganography. they're:

- Substitution technique
- Transformation domain technique
- Statistical technique
- Distortion approach

A.Substitution Technique

In this paper [1] a secured sturdy approach of statistics protection is proposed. It presents two factor based totally LSB (Least good sized Bit)techniques for embedding secret data in the LSB's of blue components and partial inexperienced additives of random pixel places in the edges of photos. An adaptive Least vast Bit(LSB) based totally steganography is proposed for embedding statistics based totally on facts to be had in MSB's of red, green, and blue components of randomly selected pixels across easy areas. It is greater sturdy as it is incorporated with a sophisticated Encryption popular(AES).

In this paper [2] a new excessive potential Steganographic scheme the use of 3-D geometric fashions is proposed. The set of rules re-triangulates a component of a triangular mesh and embeds the secret facts into newly brought position of triangular meshes. This algorithm also resists towards uniform affine alterations such as cropping, rotation and scaling. The stego key's generated from the message to be embedded. The vertices of the triangle are used for embedding.

In this paper[3] method facts is embedded into the crimson plane of the image and the pixel is chosen using a random range generator. it is almost not possible to be aware the modifications in the photograph. A stego secret's used to seed the PRNG(Pseudo Random number Generator) to select pixel places. This paper focuses on increasing the security of the message and decreasing distortion rate.

In this paper [4] the writer proposed a unique method primarily based on LSB. statistics embedding is carried out the usage of a couple of pixels as a unit, in which LSB of the first pixel contains one bit of facts and a characteristic to 2 pixel values consists of some other bit of data. The proposed approach shows higher overall performance in terms of distortion and resistance towards current steganalysis. Embedding is carried out within the sharper side areas using a threshold. PSNR value is in comparison for adaptive and non-adaptive techniques of records hiding in gray scale & colour pix.

In this paper [5] the authors have suggested an algorithm which matches on color images (JPEG). the rims are chosen for information hiding to enhance robustness. The areas located at the sharper edges are extra complicated statistical capabilities and are rather dependent on the photograph contents. it's also extra tough to look at adjustments on the sharper edges than in smooth regions. within the embedding method, the RGB additives are separated, and primarily based on a shared key, one/extra additives are selected. the cover photo is divided into non-overlapping blocks. each block is rotated via a random degree decided by a mystery key. The resulting picture is rearranged as a row vector V by means of raster scanning. The mystery message is encrypted and by using the use of LSBMR, 2 mystery bits can be embedded into each embedding unit. The message is embedded after calculating the capability estimation the use of a threshold.

In this paper [6], a brand new photo steganography scheme is proposed in the spatial area. within the method, one byte of blue factor of pixels of an photo had been replaced with mystery bits of text information, which results in better picture pleasant. A stego key's used for protection functions.

In this paper [7] the authors advise noise filtering inside the starting before embedding. After extraction at receiving give up, ARQ (automated Repeat Request) is used for mistakes detection & correction. For relaxed transmission of facts, encryption & information hiding are mixed in a single step. Host photograph and mystery facts are transformed into bit move. before encryption of mystery information median filtering is used. The input values are transformed to ASCII and then to binary, the host photo RGB values are converted to binary. Substitution is finished person via individual the usage of encryption key. The LSB of each pixel octet is replaced by means of secret bit circulation. blunders detection and correction ensures accurate transmission of facts.

In this paper [8], the authors gift a observe of a new method for insertion of message in an picture. The last bits of pixel fee are used for insertion and retrieval of message. If the final bits of pixel price are 00 or 10, we can insert 0, else with the aid of including/subtracting 1 at that pixel cost we are able to insert 0. similarly 1 is inserted if closing bits are 01 or11. For elevated safety, message is embedded at pseudo random places. The message is retrieved further based at the pixel values of the last bits.

In this paper [9], the author proposes a novel technique for hiding statistics within the spatial area of the grey scale photograph. The Pixel value Differencing (PVD) approach segments the quilt image into non-overlapping blocks containing connecting pixels and modifies the pixel difference in each block (pair) for facts embedding. while embedding secret statistics, every pixel is cut up into two same parts. The variety of one's inside the most tremendous part is counted and the secret message is embedded in the least component according to the number of corresponding bits. The proposed approach is based totally on four-pixel differencing and LSB substitution.

In this paper, the authors proposed an edge adaptive scheme that selects the embedding areas in step with the scale of the secret pixels inside the cowl image. in this information message and the distinction among consecutive embedding stage, the primary scheme initializes a few parameters, which might be used for estimating the ability of the chosen regions. in the end stego image is received after pre-processing. A area adaptive scheme is implemented to the spatial Least tremendous Bit(LSB) domain and the difference between adjoining pixels is used as a criterion for vicinity choice and LSBMR (LSB Matching Revisited) as the facts hiding algorithm.

In this paper [11], a predictive approach to enhance the histogram-based reversible statistics hiding technique is proposed. interleaving predictive degrees are used. maximum pixels are predicted with the aid of their two neighbourhood pixels and four neighbouring pixels within the column-primarily based and chess-board primarily based approach. The distinction cost of every pixel between the unique photo and the stego-picture stays inside ± 1.Pixels in abnormal columns could be expected by pixels in even columns or vice versa. within the embedding manner predictive error values of strange columns are used to generate a histogram to embed mystery information. The predictive mistakes values are transformed to get the stego-photograph.

In this paper [12], the authors have proposed a randomization technique that makes use of RGB values of coloration photos to enhance imperceptibility. In the three channels crimson, BLUE, inexperienced the LSB of any individual of the three channels is used as a pointer to decide embedding capability within the different two channels. within the randomization technique, the LSB of anyone of the channels (RGB) are used to indicate how facts must be hidden in the remaining 2 channels. If the last two bits of the channel are 00 there is no hidden facts, if it is 01 records is embedded most effective in channel 2, if it's miles 10 statistics is embedded in channel 1 and if it is 11 facts is embedded in both the channels. 3 methodologies are used. they're:

1. purple is used as default pointer.

2. consumer selects any channel as pointer.

3.tips are selected based on a cyclic collection and facts is embedded.

In this pictures have been taken and equal size information is embedded the use of all methodologies. based totally at the histogram look at and the values of MSE and PSNR (imply square error and height signal to Noise Ratio) the third technique i.e. the randomized technique has higher secrecy and overall performance with more desirable embedding capacities.

In this paper [13] the authors propose the usage of a film clip as carrier file to increase the capacity of secret information. The methodology works on the concept of replacement of whole non-touchy pixel and the substitution of some part of the sensitive pixel with secret records. A movie clip is a temporal series of dimensional samples of field of vision with every pattern being a frame of the movie. The parts of a movie clip can be divided into moving and static components. The static and the dynamic parts can be received via Pixel level evaluation, probability evaluation or shade Histogram method and stored in a static and dynamic buffer. In static element embedding system one pixel is used to save three characters using the method xij = i+(j–1)*d in which i is the initial vicinity, j is man or woman of the name of the game facts and d is the distance between two embedding pixels. In dynamic element embedding MSB method is used. A unique stego- secret's used for the dynamic portion. primary advantage of this method is greater hiding ability.

In this paper [14], the authors have analysed the distinctive steganographic strategies based on virtual logic and proposes a brand new more desirable steganographic technique based on it. The provider image is chosen depending at the facts to hold. This method makes use of virtual operations primarily based on good judgment gates and shift operators to embed/derive the hidden records from picture information. depending on the size of the facts to embed the carrier picture is split into rows and records is embedded using virtual operations.

B.Transformation Domain Method

In this [15] paper, the authors advocate a way that makes use of two gray scale photos of size 128 x 128 which might be used as secret pix and embedding is finished in RGB and YCbCr domains. The pleasant of stego photographs are properly in RGB area by means of evaluating the PSNR values. the new approach referred to as Integer Wavelet rework (IWT) has been used to cover mystery photographs in the coloration cover image. The authors have as compared the PSNR values and image quality whilst embedding is finished inside the RGB and YCbCr domains.

In this paper [16] the Integer Wavelet rework (IWT) approach had been recommended to cover more than one mystery photos and through using mystery keys in a coloration cowl picture which is extra efficient. the duvet image is represented in the YCbCr colour area. two keys are obtained, encrypted and hidden within the cover image using IWT.

In this paper [17] the author research the usage of photo steganography to breach an corporation's physical and cyber defenses. The proposed approach utilizes laptop imaginative and prescient and machine learning strategies to supply messages which can be undetectable and if intercepted can not be decrypted with out key compromise. To keep away from detection DWT (Discrete Wavelet remodel) is used. The aim of a pc vision gadget is to allow machines to investigate an picture and make a decision as to the content material of that photograph. The laptop vision can be classified as version-based& look based which uses instance snap shots and gadget mastering techniques to identify extensive areas or aspects of pixel that are important for discrimination of items contained in the photograph. system mastering is different from human knowledge/ gaining knowledge of. A laptop has to make selection of the presence of a face primarily based on the numbers contained in a 2nd matrix. The characteristic is diagnosed through the usage of Haar characteristic selection. The goal is to discover the set of features that quality distinguishes among snap shots within the one of a kind lessons. within the proposed method the duvet image does no longer contain a mystery message, as a substitute the category of the image yields the hidden message. since the proposed algorithm makes use of ordinary unmodified pixel, there are not any inherent indicators of covert communiqué taking vicinity.

In this paper [18] the authors advise a Matrix Embedding with Repeat gather (ME-RA) based totally steganography in which the host coefficients are minimally perturbed such that the transmitted bits fall in a coset of a linear code, with the syndrome conveying the hidden bits. The hiding blocks are pseudo-randomly chosen. A effective repeat collect code is used for errors correction. The authors have as compared QIM (Quantization Index Modulation) and ME-RA strategies. The comparisons with a slight change of the ME- RA (puncture and non-shrinkage) methods with exclusive decoding methods also are tabulated. The authors highlight that the usage of ME in preference to QIM within the YASS (but another Steganographic Scheme) that offers progressed steganalysis performance but software complexity is greater.

In this paper [19], the authors have introduced an more suitable approach with the assist of JPEG steganography together with a suitable encryption method the use of a symmetric key cryptographic algorithm. The JPEG cover picture is broken into eight x

eight blocks of pixel. DCT is implemented to every block and quantization is achieved and information is encrypted using a brand new encryption method which makes use of CRC checking.

In this paper [20], the authors compare the benefit of embedding in JPEG 2000 pix with the previous technique of embedding in JPEG photographs. most of the steganographic methods are primarily based on JPEG because as a block DCT codec JPEG lends itself a good candidate for statistics hiding because of its fixed block shape. JPEG 2000 that is an upcoming nevertheless photo coding popular can be used to hide excessive quantity facts. If records is embedded in the output of tier-2 coding, i.e. the JPEG 2 hundred packets, it may be guaranteed that every one the embedded facts will be obtained with out mistakes and in accurate order. however, difficulty lies inside the amendment of packets for embedding, because the bit-streams are compactly compressed with the aid of the arithmetic coder. Careless change could bring about failure of expanding compressed picture. in the embedding process the image is decomposed the use of wavelet rework. (quantity of wavelet decomposing tiers & image length ought to be related to the host picture), Lazy Mode Coding (magnitude Refinement pass is suitable for steganographic purposes) is used for embedding.

In this paper [21] the authors suggest a methodthat is based totally on a seamless integration of JPEG2000 lossy compression scheme and bit-plane complexity segmentation(BPCS) steganography. In bit-aircraft decomposition an n bit photo is decomposed into a set of n binary snap shots with the aid of bit slicing operations, blended with changing binary information in LSB bit planes with mystery records. The BPCS steganography uses bit-plane decomposition and traits of human vision. In JPEG 2000, wavelet coefficients of an photograph are quantized into a piece-plane structure. each bit aircraft of the cover image is segmented into small length 8x8 blocks and are categorised into informative / noise like blocks, the use of a threshold of the complexity αzero (e.g. fee of αzero zero.three αmax) αmax is the feasible complexity fee. the name of the game document is segmented into a sequence of blocks containing 8 bytes of information which might be seemed as 8x8 binary pixel. If secret block is much less complicated than the threshold α0, conjugate (XOR) extra complex. (α=αmax – α). The picture will now be a conjugated image. Then it's far changed every with noise block inside the bit planes with the assist of block of secret information. If block is conjugated keep it within the conjugation map. Blocks may be randomly selected by using the use of a random-number generator. additionally embed the conjugation map with mystery statistics (generally the primary noise like block). mystery records is embedded after tier-2encoding.

C.Statistical Method

In this paper[22], the authors have proposed a practical methodology in order to minimize the additive distortion in steganography with general embedding operation which is more flexible and easy. Syndrome-Trellis Codes (STC) are used to improve the security of the system. STC divides the samples into different bins (binning) which is a common tool used for solving many information-theoretic and also data-hiding problems. The proposed method can be used in both spatial & transform domain. A proper distortion function is chosen which makes statistical detection difficult. If the distortion function has been specified once, then the proposed framework provides all tools for constructing practical embedding schemes. The distortion function or the embedding operations need not be shared with the recipient.

In this research paper [23] the authors have 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. The codebook is partitioned into several clusters before embedding in order to achieve imperceptibility. 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 ofGo,the embedding process is invoked. If X is equal to the ithcodeword 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.

In this article [24] a new approach to wet paper codes using random linear codes of small co-dimension is used which improves embedding efficiency is proposed. To prevent from attack, the selection channel should not be publicly available even in any partial form. A possible remedy is to select it according to some side information that is in principle unavailable to the attacker (e.g.) random or that cannot be well estimated from the stego image. Steganography with non shared selection channels requires codes for memories with defective cells also called wet paper codes. This paper provides a new tool for steganography a coding method that empowers the steganographer with the ability to use arbitrary selection channels while substantially decreasing the number of embedding changes. The algorithm helps in the combination of wet paper codes with matrix embedding arbitrary selection channels and thus improves embedding efficiency by using the random linear codes of small co-dimension.

In this paper [25] the authors have presented a lossless data hiding which is robust against JPEG / JPEG 2000 compression. The image is split into 8 x 8 blocks and each block is split into two subsets (A, B). For each block the difference value α is calculated where α is the arithmetic average of differences of pixel pairs within the block. This α is selected as a robust quantity for embedding the information bit. Each bit of the secret message is associated with a group of pixels eg. A block in an image. The bit embedding strategy used is as follows, If α is located within a threshold & to embed bit 1, shift α to right/left beyond a threshold by adding/subtracting a fixed number from each pixel value within one subset. To embed 0, the block is intact. If α is located outside the threshold, always embed 1 thus shifting the value α away beyond a threshold. Then error correction code is applied.

D.Distortion Method

In this paper [26], the authors have used an errors correcting codes with the help of steganographic protocols. An most suitable code is one which makes maximum of the maximum embeddable (MLE). The approach 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 changed into s to embed the message m, s is from time to time referred to as the stego- statistics, and adjustments on s are translated on the quilt-medium to acquire the stego-medium. Relation between steganographic algorithms and errors correcting codes are discussed.

In this paper [27], the authors have proposed an photograph healing method in steganography. The photo is blurred earlier than hiding the message photograph the usage of special point unfold function and randomly generated key. Sequential LSB embedding within the R aircraft is executed in this task. The number of rows and columns of the message picture is encrypted in the primary row of the cover photo. before placing, the authentic message photograph is blurred the use of the precise PSF (factor spread characteristic). The parameters used for blurring with PSF are used as keys throughout de- blurring. the secret key values are despatched via a comfy channel (Tunnelling).The secret photo is recovered the use of the two keys and a 3rd key, that is randomly generated and depends at the content of the hiding message.

In this paper distinctive steganographic methods were studied and have been labeled into exceptional techniques. As many new application regions are recognized like internet banking, mobile communication security, cloud security and so on., the perception into the steganographic ideas will certainly guide us to perceive new regions and to enhance its applications within the already current regions additionally.

Parameters	Substitution	Transformation	Statistical	Distortion
Imperceptibility	High	High	Medium	Low
Robustness	Low	High	Low	Low
Payload Capacity	High	Low	Low	Low
Method used	Integer Wavelet Transform ,Matrix Embedding with repeat accumalate code	Enhanced JPEG steganography, BPCS steganography	Additive distortion function in steganography, Matrix Embedding with wet paper code	Use of error correcting codes in steganography, Image blurring with sequential LSB embedding

Table 1: Difference between Steganography Methods

Conclusion

In this paper different steganographic methods were studied and were categorized into different techniques. As many new application areas are identified like internet banking, mobile communication security, cloud security etc., the insight into the steganographic principles will definitely guide us to identify new areas and to improve its applications in the already existing areas also.

References

[1] 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.

[2] P.Thiyagarajan,V.Natarajan,G.Aghila, V.Pranna Venkatesan, R.Anitha,(2013)"Pattern Based 3D ImageSteganography",3DResearch center, Kwangwoon University and Springer 2013, 3DR Express., pp.1-8.

[3] Shamim Ahmed Laskarand 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.

[4] 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.

[5] 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.

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

[7] Fahim Irfan et. Al. 's (2011) "An Investigation into Encrypted Message Hiding through ImagesUsing LSB ", International Journal of EST,

[8] Rajkumar Yadav, (2011) "A Novel Approach For Image Steganography In Spatial Domain UsingLast 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] Christo Ananth, A.S.Senthilkani, S.Kamala Gomathy, J.Arockia Renilda, G.Blesslin Jebitha, Sankari @Saranya.S., "Color Image Segmentation using IMOWT with 2D Histogram Grouping", International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 3, Issue. 5, May 2014, pp-1 – 7

[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] Venkata Abhiram.M, Sasidhar Imadabathuni, U.Padmalochini, Maheedhar Imadabathuni and Ramya Ramnath (2009), "Pixel Intensity Based Steganography with Improved Randomness", International Journal of Computer Science and Information Technology, Vol 2, No 2, pp.169-173.

[13] 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, pp103-110.

[14] Jaswinder Kaur, Inderjeet & Manoj Duhan, (2009) "A Comparative Analysis of Steganographic Techniques", International Journal of Information Technology and Knowledge Management, Vol.2, No. 1, pp 191-194.

[15] 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.

[16] Hemalatha.S, U.Dinesh, Acharya andRenuka.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.

[17] 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

[18] 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.

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

[20] Po-Chyi & C.-C.Jay Kuo, Fellow, IEEE(2003) "Steganography in JPEG 2000 Compressed Images", IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, pp 824-832.

[21] Hideki Noda, Jeremiah Spaulding, Mahdad.NShirazi & Eiji Kawaguchi (2002) "Application of Bit- Plane Decomposition Steganography to JPEG 2000 Encoded Images", IEEE Article.

[22] Tomas Filler, Student Member, IEEE, Jan Judas and Jessica Fridrich, Member, IEEE, (2010) "Minimizing Additive Distortion in Steganography using Syndrome Trellis Codes", IEEE Article, pp.1-17.

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

[24] Chin-Chen Chang & Chih-Yang Lin (2006) "Reversible Steganography for VQ-Compressed Images Using Side Matching and Relocation ",IEEE Transactions on Information Forensics and Security, Vol. 1. No.4, pp 493-501.

[25] Zhicheng Ni, Yun Q.Shi, Nirwan Ansari, Wei Su, Qibin Sun & Xiao Lin (2004) "Robust Lossless Image Data Hiding, IEEE Article.

[26] Mamoun SOUIDI, (2010) "Steganography and Error Correcting Codes", International Journal of Computer Science and Information Security, Vol.8.No.8, pp147-149.

[27] D.P.Gaikwad and S.J.Wagh, (2010) "Colour Image Restoration For An Effective Steganography", I-manager's Journal on Software Engineering, Vol.4.No.3, pp.65-71.