IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 44-52
www.iosrjournals.org

CEET: A Compressed Encrypted & Embedded Technique for Digital Image Steganography

Palak Mahajan, Dr. Ajay Koul
School of Computer Science & Engineering, Shri Mata Vaishno Devi University, J&K, India

Abstract: *In this information era, digital information sharing and transfer plays a vital role and their use has increased exponentially with the development of technology. Thus providing security of data is a topic of concern. Data hiding is a powerful tool that provides mechanism for securing data over insecure channel by concealing information within information. Steganography inherits data hiding concept and passes information through host files in such a way that the existence of the embedded secret is unknown. This paper presents a joint application of compression, encryption and embedding techniques for implementing digital image steganography. Compression technique generates noise in the image. Inorder to retain the noise distortion to a minimum level, LSB insertion method is used for embedding purpose where the bits are inserted at the last 2 LSB's of the image. In this proposed technique the secret information is initially compressed and then the resultant bits are encrypted. Finally these encrypted bits are embedded into an image. The main objective is to develop an application that increases the steganographic capacity and enhances the stego image quality while keeping the security intact.*

Keywords: *Data Hiding, Steganography, Color Image, LSB Technique, JPEG-LS , Encryption*

I. Introduction

With the rapid development of digital technology and communication media, data such as text, images, audio, video, etc are growing importance in day to day life. A large amount of data is being transmitted over internet. There is always a threat of an intruder accessing the private information. So a mechanism needs to be implemented inorder to keep the integrity and confidentiality of the information. This has led to an explosive growth in the field of information hiding.

Cryptography is the most common word that is used in information hiding. Cryptography means converting the text from readable format to unreadable format. Cryptography applies encryption techniques to convert the message into non-readable form but it doesnot hides the message i.e., the encrypted message is visible [14]. Additionally it increases the curiosity level of the intruder to decrypt the code. It would be great to have something that can embed the secret message into some media in such a way that no one can guess whether anything is hidden or not. Steganography a branch of information hiding inherits this idea and hides information inside information [1]. Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended user knows about the existence of the message. This can be achieved by concealing the existence of information within a cover (text, image or audio file). Figure 1 shows a typical steganographic system. Steganography aims to make the secret communication undetectable, that is, to hide the presence of the secret message. It modifies the carrier in an imperceptible way so that it reveals nothing neither the embedding of a message nor the embedded message itself [19]. Steganography gives advantage to steganographer because visually attackers cannot notice anything suspicious about an image being modified [10].

Fig 1. A Steganographic system

Most of the steganography applications hide data inside images using variation of least significant bit (LSB) embedding technique. In LSB embedding data is hidden in the least significant bit of each byte in the image. With the advancement of steganography countermeasures to detect steganography has evolved. Attackers combat steganography using steganalysis [11]. The goal of steganalysis is to identify the suspected packages, determine whether or not they have any secret message encoded into them and, if possible, recover that message [6]. By using steganalysis techniques data hidden inside an image using normal LSB technique can be detected with probability ranging from 75% - 90%. Thus, there is a need of providing a strong and reliable steganography algorithm that can hide secret messages within images.

This paper documents the design and implementation of proposed data hiding application using steganography. The goal of proposed application is to maintain data integrity and confidentiality. Not only it hides the user's data (secret image) within an image, but it also compresses & encrypts the user's data. For compressing the image, JPEG lossless compression algorithm is used and then the image is encrypted by applying substitution cipher. To defend against steganalysis, proposed steganographic application selects cover image from library of images in such a way that the selected image is least likely to be vulnerable to steganalysis.

The paper is organised as follows: Section II presents the literature review. The background work of JPEG-LS compression, substitution cipher & LSB insertion is described in section III followed by proposed technique in section IV. In section V results are discussed. Finally section VI discuss about the conclusion.

II. Literature Review

Images are the most popular files that are used for data hiding. Steganography techniques can be classified into two broad categories: spatial domain and frequency domain techniques. All these techniques have their own characteristics. Spatial domain technique deals with modulating the least significant bits (LSB) plane of the cover-image [25]. In case of frequency domain, a cover-image is first transformed into the frequency coefficients such as discrete cosine transform (DCT) [18, 30], discrete fourier transform (DFT), and discrete wavelet transform (DWT) [7, 20]. After that the secret messages are embedded by modulating the magnitude of these coefficients.

Monica Adriana et.al [13] presented a spatial domain technique that applies LSB insertion to embed payload inside the color image. The algorithm is processed serially as well as in parallel by making use of threads to speed up the process of data hiding. The stego image generated has good imperceptibility but the algorithm lacks in security aspect as anyone can steganalyse it by retrieving the LSBs. Hung-Min et.al [4] proposed Highlight of exploiting modification direction (HoEMD) and adaptive EMD (AdEMD) methods that applies the module operation and considers the sensitive nature of a human visual system. HoEMD approach exploits pixel directions, greater the pixel directions more is the embedding capacity. AdEMD method uses pixel differencing to check how much data can be embedded in the edge and smooth area. To extract the message same differencing value is maintained before and after data is concealed. Masud Karim et.al [15] proposed a new method where the payload is stored into different position of LSB of image depending on the secret key. This method provides high security as attackers cannot extract information using general steganalysis tool, one needs the secret key to retrieve data. Praveen Kumar et.al [22] has used a combined approach for data hiding. Initially wavelet transformation is applied on secret information and then it is encoded using CNOT gate. Finally the encoded bits are inserted at LSBs using random generators. Chin Chen et.al [5] proposed an adaptive technique applied to the LSB substitution method. They presented an approach that exploits the correlation between neighbouring pixels to estimate the degree of smoothness. Smoothness degree determines the number of LSBs to be used for embedding. In [31], Ming Fu and Oscar Au used watermarking to implement visual cryptography [24]. The secret image is embedded as a watermark into a cover image and the cover image is divided that generates two high quality halftone images as share images. Individual share doesn't depict any information the shares need to be overlaid to reveal that secret image.

Manoj Kumar Ramaiya et.al [17] implemented steganography by using Data Encryption Standard (DES) on images. Encryption is performed by making use of s-boxes and in the final stage information is embedded by using last two LSBs insertion. Rajbir kaur et.al [12] used YCbCr color model instead of RGB model as cover file. Simply the payload is embedded inside the LSBs. Li and Wang [23] presented a steganographic method that modifies the quantization table (QT) and inserts the hidden bits in the middle frequency coefficients. QT generates 36 coefficients in each 8x8 block that embeds secret data into that yields a reasonable stego. Fangjun Huang et.al [2] presented channel selection rule for JPEG steganography. Perturbation error (PE), the quantization step (QS) [32], and the magnitude of quantized DCT coefficient (MQ) are used as factors for channel selection. Through proposed channel high security is obtained in JPEG steganography. Furuta et.al [16] proposed a new spatial domain technique called Bit Plane Complexity Segmentation (BPCS) which is based on Most Significant Bit technique. BPCS provides the ability to hide data

in higher bit planes of the cover image but it has low embedding capacity as changing most significant bits can cause significant changes in perception.

The main transform domain algorithm is JSteg. JSteg was amongst the first algorithms that implemented steganography on JPEG images [1]. From visual perspective it stood strongly against steganalysis, but failed against statistical steganalysis methods. S-Tools are the most popular steganographic tool available which are based on the LSB technique. S-Tools [1] reduce the number of colors in the image to only 32 colors and hides data in the LSB of each color pixel in the image. S-tools work with BMP file format and provide high image quality but have low embedding capacity.

III. Background Work

A reliable steganographic technique aims at three aspects: capacity (maximum amount of data that can be stored inside cover image), imperceptibility (the visual quality of stego-image and cover image should be same) and robustness. The capacity can be increased by using transformation (compression) technique while imperceptibility can be maintained by making changes at a minimum level during embedding. To provide robustness, the steganography technique needs to be backed up by an encryption scheme. This section discusses the techniques used for implementing compression, encryption and embedding algorithms.

A.JPEG-LS Compression

JPEG-LS is a lossless image compression algorithm that is used for JPEG images. It is a simple and efficient baseline algorithm that provides a low-complexity lossless and near-lossless image compression standard and offers good compression efficiency while maintain the quality of the image. The core of JPEG-LS is LOCO algorithm which based on prediction, residual modelling and context-based coding of the residuals [26]. Amongst other JPEG standards like JPEG 2000, the compression rate of JPEG-LS is faster and has high resolution.

B. Substitution Cipher

In encryption, substitution cipher is a method of encoding by which units of plaintext are replaced with ciphertext according to transformation rule; the "units" may be single letters, pairs of letters, triplet of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution. For encrypting the image, image transformation function is used [27]. MATLAB provides various image transformation functions that can be used for specifying the rule according to which the image can be encrypted. In this paper im2double function is used for image transformation. The im2double function converts the intensity of the image to double precision along with rescaling the data. The encryption function can then be formulated as

encryptImage= K - im2double(originalImage) **(1)**

where K is the key defining the intensity value to be subtracted. The key K is generated using random numbers (key generators). The function rand is provided by MATLAB to generate random numbers.

C. Least Significant Bit Insertion

Least significant bit insertion is one of the most common and technical embedding technique for hiding data inside the cover file. The amount of data to be hidden inside the image depends upon the size of the image and the number of least significant bits to be used. LSB insertion works simply just by replacing least significant bit of every pixel in cover image with the data to be hidden [25]. For example letter A (10000011) can be hidden using LSB insertion.

Pixel values before LSB insertion:

11000000	01001110	11110011
00000011	10101011	11000101
10000110	11111100	11000000

Pixel values after LSB insertion of 'A' will be:

1100000**1**	0100111**0**	1111001**0**
0000001**0**	1010101**0**	1100010**0**
1000011**0**	1111110**1**	1100000**1**

Altering the least significant bits will result in a color slightly different from the original one which is unable to be detected by human eye. The reason being human eye is not sensitive enough to recognize the difference in color between pixels which differs by just 1 unit [25].

IV. Proposed Work

The essence of steganography lies in the fact that the image bearing data should be statistically and visually identical to the original image so that an intruder cannot detect the presence of the hidden message. This goal is kept in mind while designing the proposed data hiding application. The block diagram of proposed steganographic system is given in figure 2.

A. Data Hiding Algorithm

A unique feature of proposed method is that it allows user to pick a suitable image as cover image which is less vulnerable to steganalysis attacks. A database of images is created from which appropriate cover images are extracted.

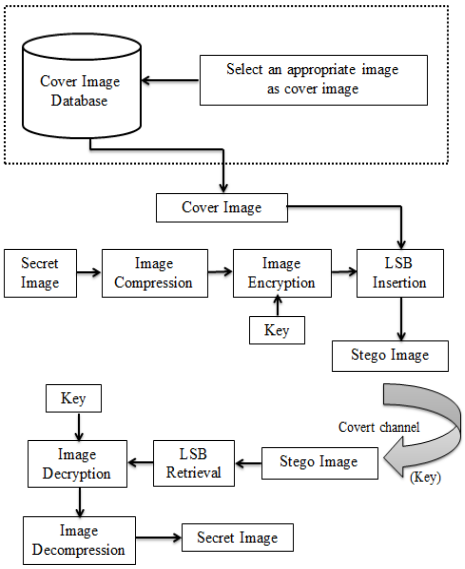


Fig 2. Block diagram of Proposed Steganographic system

Initially an appropriate image is selected from the cover image database which acts as the cover file. In the first layer, the secret data (image) is compressed by applying JPEG lossless compression algorithm maintaining the image quality at 75%. By applying JPEG-LS algorithm 54% of bytes of the image gets compressed. The compressed image so obtained is then encrypted by applying the substitution encryption algorithm in the second layer. A key is generated by random generator which is used in encryption. The encrypted image so obtained is converted into array of 0's and 1's. Finally these bits are then embedded into the cover image in the inner-most by inserting them into the last 2 LSBs of each pixel of the cover file. The image so obtained is the stego-image. The stego-image as well as the key is sent to the receiver over the covert channel. The key is sent using a secure key exchange technique.

Hiding Algorithm:

Input: Cover image Database D, Secret Image S
Output: Stego image SS
Step 1: Select a suitable Cover image C of size MxN from the database D.
Step 2: Now compress the secret image S of size MxN by applying JPEG compression technique.
Step 3: Generate key K from random number generator.
Step 4: Apply encryption function E on the image generated in step 2.
Step 5: Take the cover image C and embed the image generated in step 4 by inserting bits into the last 2 LSBs of C.
Step 6: Image generated in the previous step is the final Stego image SS.
Step 7: Transfer the Stego image SS & key K to the receiver
Step 8: End.

B. Data Recovery

The process of recovering data is easy to implement. The needed input is the stego image and the key. The stego image is converted into binary array of 0's and 1's and then the color values of each pixel are studied and the corresponding LSBs are extracted. Finally these values are then concatenated using 8-bit binary format

and convert it into image matrix. Decryption is performed using the key. The resultant image is then decompressed while maintaining the quality of the image which reveals the secret image which was hidden.

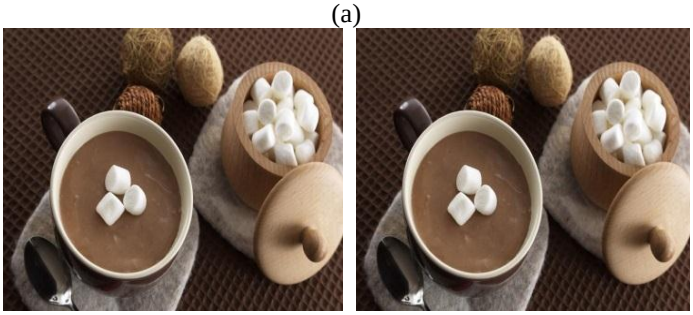
Extraction Algorithm:

Input: Stego image SS, Key K
Output: Secret image S
Step 1: Extract the last 2 LSBs of the stego image SS.
Step 2: Concatenate the array of extracted 0's & 1's into 8-bit binary format.
Step 3: Formulate the image matrix.
Step 4: Perform decryption on the image matrix by using the key.
Step 5: Decompress the resultant image.
Step 6: Image generated in the previous step is the secret image.
Step 7: End.

V. Results

This section discusses the results of using proposed application to hide data in an image. The algorithm is tested in MATLAB Version 8.1.0.604 (R2013a). Various images are used as cover image to implement the algorithm. Steganography exploits human perception as human senses are not trained to look inside an image that has information hidden inside them. Figure 3 shows the original cover and the stego images respectively.

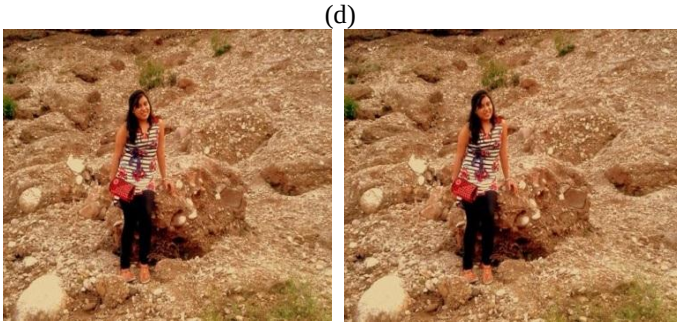
(a)



(b)

(c)

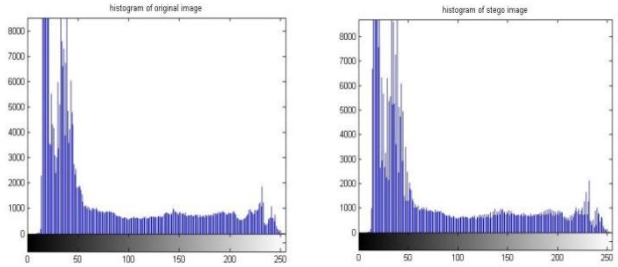
(d)



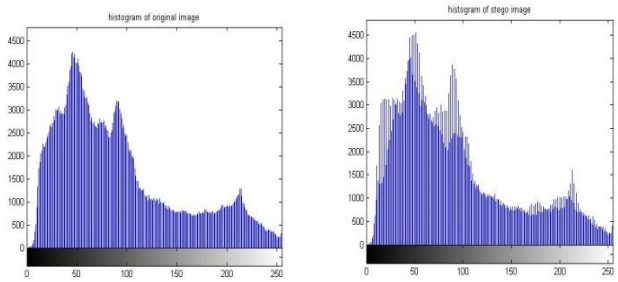
(e)

Fig 3. Cover images (left) & Stego images (right) (a) Bike, (b) Coffee, (c) Scene, (d) Violin, and (e) Girl

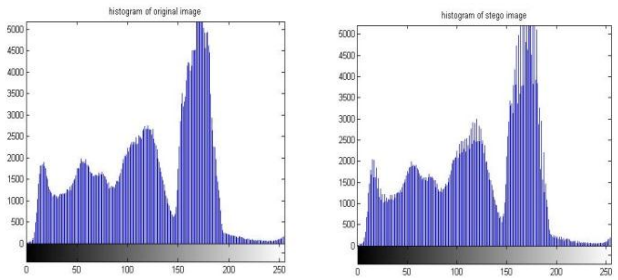
Visually all these images look identical, one cannot distinguish between cover image and stego image. This indicates that the stego images obtained from CEET have high imperceptibility. Histogram is a measure of the number of occurrence of pixels with respect to particular pixel value. Steganography changes the pixel value during embedding process, therefore the number of pixel having a particular pixel value changes. Hence lesser difference between the histograms of cover and stego-image is desirable. Figure 4 shows the histograms obtained by implementing the proposed technique. As depicted by the figure 4, there is a very minute change between the histograms of cover images and stego images. The overall structure of the original image still remains the same even after embedding secret image inside it.



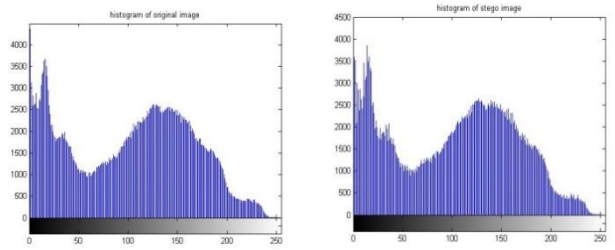
(a)



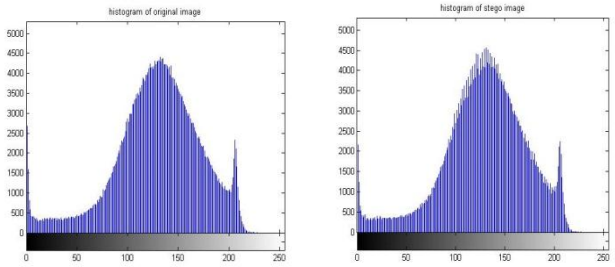
(b)



(c)



(d)



(e)

Fig 4. Histogram of Cover images (left) & Stego images (right) (a) Bike, (b) Coffee, (c) Scene, (d) Violin, and (e) Girl

The most important factor in steganography system is Peak Signal to Noise Ratio (PSNR). PSNR represents quality of image i.e. the higher the PSNR lower is the difference between cover image and stego image [6]. The measurement of the quality between the cover image f and stego-image g of sizes N x N is defined by PSNR as:

$$PSNR=10 \times \log (255^2 / MSE) \quad \textbf{(2)}$$

where

$$MSE=1/mn\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[(f(x,y)-g(x,y)]^2 \quad \textbf{(3)}$$

Here f(x, y) and g(x, y) represent the pixel value at the position (x, y) in the cover-image and the stego-image respectively. The goal of the stego system is to achieve high PSNR value inorder to make steganography successful.

Table 1 shows the PSNR value obtained from the proposed method CEET and S-Tools. Figure 5 represents the comparison between CEET and S-Tools.

Table 1. PSNR (in db).

Image	**CEET**	**S-Tools**
Bike	51.50	49.62
Coffee	51.06	48.98
Scene	51.16	48.18
Violin	51.11	50.04
Girl	51.26	49.44

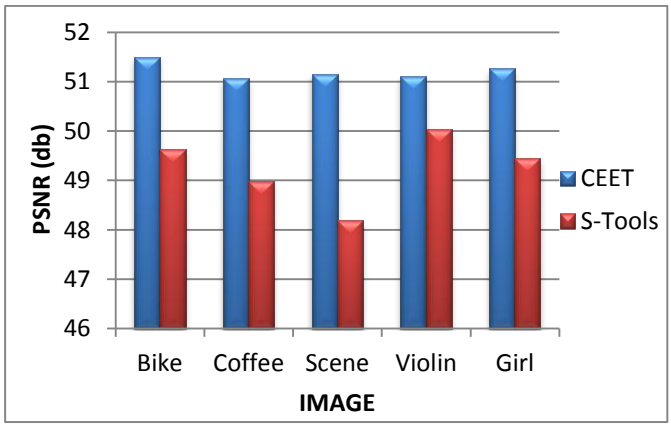


Fig 5. Comparison of PSNR (in dB) between CEET & S-Tools

High PSNR indicates good perceptual quality of stego-image. Here the resultant PSNR value of CEET is better than that of S-Tools. Table 2 represents the correlation coefficient for cover image and stego image. Correlation coefficient is very high which indicates the cover image and stego image are highly related.

Table 2. Correlation Coefficient

Image	**Correlation Coefficient**
Bike	.99997
Coffee	.99997
Scene	.99996
Violin	.99997
Girl	.99993

The parameters are evaluated for both CEET and S-Tools which is shown in table 3. The proposed application CEET provides high security since encryption is applied as well as embedding capacity has also been increased by using compression algorithm keeping in mind the visual perspective of steganography.

Table 3. Parameters analysis of CEET & S-Tools

Features	**CEET**	**S-Tools**
Payload Capacity	High	Low
Imperceptibility	High	High
Robustness	Medium	Low
PSNR	High	Medium
Security	High	Medium
MSE	Low	Low

VI. Conclusion

This paper introduces the concept of steganography - a powerful data hiding technique. In this paper the proposed method CEET uses compression, encryption and LSB embedding in order to hide and recover data. Applying compression in the first layer helped in reducing the size of secret data thereby providing high payload capacity in the cover image since 54% bytes of secret image gets compressed. Also encryption at inner layer results out to be an asset that increased the security of data against steganalysis. Finally using last 2 LSB's of cover image for embedding purpose enabled more space in the cover image as well as maintains the imperceptibility of cover image. Interlacing all these techniques together helped in achieving the goal of steganography which is embedding highest possible rate while remaining undetectable to steganalyse. As privacy is the upmost priority in the digital communication domain, steganography undoubtedly plays a growing role in information security. So, one should be aware of steganography and its implications.

References

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to Steganography", *IEEE Conference on Security and Privacy*, pp. 32-44, 2003.

[2] Fangjun Huang, Jiwu Huang, and Yun-Qing Shi, "New Channel Selection Rule for JPEG Steganography", *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 4, pp. 1181-1191 August 2012.

[3] Avinash Srinivasan, Srinath Thirthahalli Nagaraj, and Angelos Stavrou, "HIDEINSIDE – A Novel Randomized & Encrypted Antiforensic Information Hiding", *International Conference on Computing, Networking and Communications, Communications and Information Security*, 2013.

[4] Hung-Min Sun, Chi-Yao Weng, Chin-Feng Lee, and Cheng-Hsing Yang, " Anti-Forensics with Steganographic Data Embedding in Digital Images ", *IEEE Journal on selected areas in Communications*, Vol. 29, No. 7, pp. 1392-1403, 2011.

[5] C.C. Chang, P. Tsai, and M.H. Lin, "An Adaptive Steganography for Index- based images using Codeword Grouping", *Advances in Multimedia Information Processing-PCM, Springer*, Vol. 3333, pp. 731–738, 2004.

[6] "Peak Signal to Noise Ratio (PSNR)" from Wikipedia http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

[7] Moh Zan and Nyein Aye," A Modified High Capacity Image Steganography using Discrete Wavelet Transform", *International Journal of Engineering Research & Technology* (IJERT), Vol. 2,No. 8, pp. 2712-2715, August - 2013.

[8] Piyush Marwaha and Paresh Marwaha," Visual Cryptographic Steganography in Images", *Second International conference on Computing, Communication and Networking Technologies*,2010.

[9] Cryptography" from Wikipedia, http://en.wikipedia.org/wiki/Encryption

[10] Jan Kodovsky, Jessica Fridrich and Vojtech Holub, "Ensemble Classifiers for Steganalysis of Digital Media", 432 *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 2, pp. 432-444, April 2012.

[11] J. Fridrich and M. Long, "Steganalysis of LSB encoding in color images" ,*Multimedia and Expo*, vol. 3, pp. 1279-1282, July 2000.

[12] Rajbir kaur, Surbhi Gupta, and Parvinder S. Sandhu, "Randomized Steganography using Ycbcr Color Model Characteristics", *International Conference on Computer and Communication Technologies* (ICCCT' 2012) May 2012, Phuket.

[13] Monica Adriana Dagadita, Emil Ioan Slusanschi, and Razvan Dobre, "Data Hiding using Steganography", *IEEE 12th International Symposium on Parallel and Distributed Computing*, 2013.

[14] Rajput A.S., Mishra N., and Sharma S., "Towards the growth of image Encryption and Authentication Schemes", *International Conference on Advances in Computing, Communications and Informatics* (ICACCI), 2013.

[15] S. M. Masud Karim, Md. Saifur Rahman, and Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", *Proceedings of 14th International Conference on Computer and Information Technology* (ICCIT 2011) , December 2011.

[16] Furuta T., Noda H., Niimi M., and Kawaguchi E, "Bit-plane decomposition steganography using wavelet compressed video", *Joint Conference of the Fourth International Conference*, pp. 970 - 974, 2003.

[17] Manoj Kumar Ramaiya, Naveen Hemrajani, and Anil Kishore Saxena, "Improvisation of Security aspect in Steganography applying DES", *International Conference on Communication Systems and Network Technologies*, 2013.

[18] Raja, K. B., C. R. Chowdary, K. R. Venugopal, and L. M. Patnaik, "A secure Image Steganography using LSB, DCT and Compression techniques on raw images", *Third International Conference on Intelligent Sensing and Information Processing*, (ICISIP 2005), pp. 170-176, 2005.

[19] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Biometric Inspired Digital Image Steganography", *15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems*, 2008

[20] Moh Moh Zan and Nyein Aye, "A Modified High Capacity Image Steganography using Discrete Wavelet Transform", *International Journal of Engineering Research & Technology* (IJERT), Vol. 2, August 2013.

[21] Mei-Ching Chen, Anuradha Roy, Benjamin M. Rodriguez, Sos S. Agaian, and C. L. Philip Chen, "An Application of Linear Mixed Effects Model to Steganography Detection", Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, October 2009.

[22] R Praveen Kumar and V Hemanth, Mshareef, "Securing Information Using Steganography", *International Conference on Circuits, Power and Computing Technologies*, 2013.

[23] X. Li and J. Wang, A Steganographic method based upon JPEG and Particle Swarm Optimization Algorithm, *International Journal on Information Sciences*, Vol. 177, pp. 3099-3109, August 2007.

[24] Debashish Jena, "A Novel Visual Cryptography Scheme", *IEEE International Conference on Advanced Computer Control*, 2009.

[25] D. Sandipan, A. Ajith, and S. Sugata," An LSB Data Hiding Technique using Prime Numbers", *Third International Symposium on Information Assurance and Security, Manchester, UK, IEEE CS press*, 2007.

[26] Ying Xie, Xiaojun Jing, Songlin Sun, and Linbi Hong, "A Fast and Low Complicated Image Compression Algorithm for Predictor of JPEG-LS", *IEEE International Conference on Network Infrastructure and Digital Content*, 2009.

[27] "Cryptography and Network Security principles and practices", William Stallings, Pearsons education, first Indian reprint 2003.

[28] Chuan Qin, Chin-Chen Chang, Ying-Hsuan Huang, and Li-Ting Liao, "An Inpainting-Assisted Reversible Steganographic Scheme using a Histogram Shifting Mechanism", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 23, No. 7, pp. 1109-1118, July 2013.

[29] Jessica Fridrich and Jan Kodovsky, "Rich Models for Steganalysis of Digital Images", IEEE *Transactions on Information Forensics and Security*, Vol. 7, No. 3, pp. 868-882, June 2012.

[30] Chen Heng, Braeckman Geert, Munteanu Adrian, and Schelkens Peter, "Reversible DCT-based lossy-to-lossless still Image Compression", *20th IEEE International Conference on Image Processing* (ICIP) , 2013.

[31] Ming Sun Fu and Oscar C. Au, "Joint Visual Cryptography and Watermarking", IEEE *International Conference on Multimedia and Expo* (ICME), 2004.

[32] Wei-Jen Wang, Cheng-Ta Huang, and Shiuh-Jeng Wang, "VQ Applications in Steganographic Data Hiding Upon Multimedia Images", *IEEE Systems Journal*, Vol. 5, No. 4, pp. 528-537, December 2011.