International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Advanced Technique for Comprehensive Data Security

Pramendra Kumar[1], Vijay Kumar Sharma[2]

[1]M.Tech Scholar, Department of Computer Science, RIET, Bhankrota, Jaipur, Rajasthan, India
[2]Asst. Prof., Department of Computer Science, RIET, Bhankrota, Jaipur, Rajasthan, India

Abstract: ***In any communication, security is the most important task. With the advancement of technology and the wide use of World Wide Web for communication increase the challenges of security. Most of the classical security method are based on cryptography and stegnography techniques, but every time these technologies may not be reliable for communication of secrete information over a long distance. Where cipher text may easily arouse attackers'suspicion, the biggest concern in the field of steganography is the rapid advancement of research in steganalysis, the counter-technology of steganography. This merely means that steganography needs to add security services to its current repertoire, while not increasing the number of problems. However, in recent years, a lot of research has taken place in direction to trim down the security issues by contributing various approaches but different terrains pose separate challenges. These inadequacies of modern as well as traditional security methods, motivates to design a novel security system that improve the level of security. In this context, this paper has proposed a novel two layer security mechanism by combining the concepts of both, cryptography and stegnography techniques.***

Keywords: Cryptography, Stegnography, Security, Data hiding, Encryption

1. Introduction

From the past few decades, because of no boundary barriers of distance, easy accessing and the fast delivery of information the online web based system is more popular as a new communication media in between the end users. However, these online systems are vulnerable to a variety of well-known cyber-attacks. Cyber world needs high level of safeguard for expensive data during transmission over the open communication channel. The typical idea of security clearly assumes disjointing of users and attackers to provide safeguard against unauthorized access of secrete information. This need of security produce explosive growth of the field of information hiding which covers applications such as copyright protection for digital media, Cryptography, Steganography, Digital Watermarking and finger printing. All these applications of information hiding are quite diverse. However, the secrete information might be secure with the modern security techniques but most of the security methods are based on the cryptographic techniques. The aim of cryptography is to provide secure solutions to a set of parties who wish to carry out a distributed task and either do not trust each other or fear an external adversarial threat. The security method of cryptography encrypt plain text to generate cipher text, where the cyber attacker easily arouse these text and intercepts the communication between two separate users to modify, inject, or drop any communication packet [1, 2, 3]. The cryptography has several problems like;

- The information that has been encrypted might be accidently utilized on something that was not meant to be encrypted, and the person who was meant to obtain the message may not be able to read the message sent to them at all.
- Sometimes encryption may not be strong enough, and therefore, others may be able to easily intercept and interpret information.
- The encryption might be used in order for criminals to be able to easily and effortlessly perform crimes.
- Another drawback of cryptography is the limitations that have been enforced by certain governments,
- Many governments have created laws to either limit the strength of cryptographic systems or to prohibit it altogether and sometimes even the possession of a cryptographic algorithm - is illegal in certain countries.

To improve these limitations and to reduce the issues of cryptographic methods an alternative mechanism, the steganography has use widely. This is a powerful security tool that provides a high level of security, particularly when it is combined with encryption [4].Generally the concepts of this techniques differ from the cryptography, where the cryptography method converted the information in a encrypted form that an eavesdropper and cannot be understand, the Steganography technique embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion in some cases, sending encrypted information may draw attention, while invisible information will not.

Traditional steganography techniques rely on the encoding system's secrecy to secure the information. The system able to provide security but have a problem that if attacker known than it is simple enough to expose the entire received media passing by to check for hidden messages ultimately, such a steganographic system fails. Beside this problem in steganography the image and video codec are block-based and possible bit-errors usually destroy the data only in a single block or even all the blocks in the rest of the row of macro blocks (slice). These block errors decrease the visual quality drastically. Hence, the concealment of such block losses is a realistic situation in many cases, except for the damage of some header information. On the other hand, the majority of steganographic systems uses images as cover media because people often transmit digital pictures over email and other Internet communication but this techniques in same case may produce the same results as previous one that shows the single security technique either cryptography or steganography is not a turnkey solution to secure the secrete information over the open system. For a strong system it is always better to use both cryptography and steganography together. In this context, this paper has proposed a novel two layer security mechanism by combining the concepts of both, cryptography and stegnography technique.

2. Related Work

A novel image adaptive stegnographic technique have proposed in [5], in which the integer wavelet transform domain called as the Robust Image Adaptive Steganography using Integer Wavelet Transform. According to information theoretic prescriptions for parallel Gaussian models of images, data should be hidden in low and mid frequencies ranges of the host image, which have large energies.[6] worked out the specific design principles and elements of steganographic schemes for the JPEG format and their security. The detect ability is evaluated experimentally using a state of art blind steganalyser.

A novel approach has been proposed a combination of three different LSB insertion algorithms [7] on GIF image through stegcure system. The unique feature about the stegcure is being able to integrate three algorithms in one Steganography system. By implementing public key infrastructure, unauthorized user is forbidden from intercepting the transmission of the covert data during a communication because the stego key is only known by the sender and the receiver. [8] Proposed a work which deals with public- key Steganography in presence of passive warden. The main aim is to hide the secret information within cover documents without giving the warden any clue and without any preliminary secret key sharing. This work explores the use of trellis coded quantization technique to design more efficient public key scheme.

LSB based steganography algorithm presented [9] with high data hiding capacity as four LSB's are used to hide data, high confidentiality as distortions which can cause suspicions for the intruders, are removed through filtering techniques and two level high security is applied. A security model is proposed which imposes the concept of secrecy over privacy for text messages [10]. The proposed model combines cryptography; steganography and along with an extra layer of security has been imposed in between them. A noval approach has been proposed a scheme embeds a larger-sized secret image while maintaining acceptable image quality of the stego-image [11] and also improved image hiding scheme for gray scale images based on wet paper coding.

Author describe in [12], a steganographic model which utilizes cover video files to conceal the presence of other sensitive data regardless of its format. The model presented is based on pixel-wise manipulation of colored raw video files to embed the secret data. The paper also presents a quantitative evaluation of the model using four types of secret data. The model is evaluated in terms of both the average reduction in Peak Signal to Noise Ratio (PSNR) compared to the original cover video; as well as the Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames.

The paper [13] proposes a new method for the real-time hiding of information used in compressed video Bit streams. The method is based on the real-time hiding of information in audio steganography. This method of steganography is very similar to the two discussions of image steganography and video steganography. A new compressed video secure steganography (CVSS) algorithm is proposed. In this algorithm, embedding and detection operations are both executed entirely in the compressed domain, with no need for the decompression process. In order to make faithful and secure communication, a dual layer hiding technique [14] proposed.

The paper [15] presents hiding the data behind the image then encrypts the image byusing hyper-chaos encryption algorithm. In this algorithm, shuffling matrix and diffusing matrix are generated based on Chen's hyper-chaotic system. Firstly, the Chen's hyper-chaotic system is used to shuffle the position of the image pixels, and then use Chen's hyper-chaotic system to confuse the relationship between the original image and the cipher image.

A novel steganography technique mainly based on joint photographic expert group (JPEG) is proposed in [16]. This technique is based on 2-D Block-DCT, where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain. The proposed method provides acceptable image quality and a large message capacity. Overall, the proposed method matches the requirement of steganography with a larger message capacity and good image quality. The method has larger message capacity than Jpeg-Jsteg method. To ensure the security against the steganalysis attack, a new steganographic algorithm for 8bit(grayscale) or 24 bit (color image) is presented in paper [17], based on Logical operation. Algorithm embedded MSB of secret image in to LSB of cover image. In this n LSB of cover image, from a byte is replaced by n MSB of secret image. The image quality of the stego-image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is derived. A steganography technique which embeds the secret messages in frequency domain proposed in [18].Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. In proposed method cryptography algorithm is used to convert the secret messages to an unreadable form before embedding. Algorithms keep the messages from stealing, destroying from unintended users on the internet and hence provide satisfactory security. Blowfish algorithm is used for encryption and decryption of text message using a secret-key block cipher. Designed to increase security and to improve performance algorithm uses a variable key size up to 448 bits.

A practical steganographic implementation ST-FMM [19] proposed to hide text inside grey scale images. Using the Five Modulus Method secret message is hidden inside the cover image. FMM consists of transforming all the pixels within the 5×5 window size into its corresponding multiples of 5. After that, the secret message is hidden inside the 5×5 window as a non-multiples of 5. Since the modulus of non-multiples of 5 are 1,2,3 and 4, therefore; if the reminder is one of these, then this pixel represents a secret character. The secret key that has to be sent is the window size. The main advantage of this novel algorithm is to keep the size of the cover image constant while the secret message increased in size. Peak signal-to-noise ratio is captured for each of the images tested. Based on the PSNR value of each images, the stego image has high PSNR value. Hence this new steganography algorithm is very efficient to hide the data inside the image.

3. Proposed Work

To apply the security for important data at the time of communication over unsecured channels the proposed approach provide two layer of security by combining the functionality of cryptography & stegonagrphy. The figure 1 presents the overall methodology that is adopted to secure data.

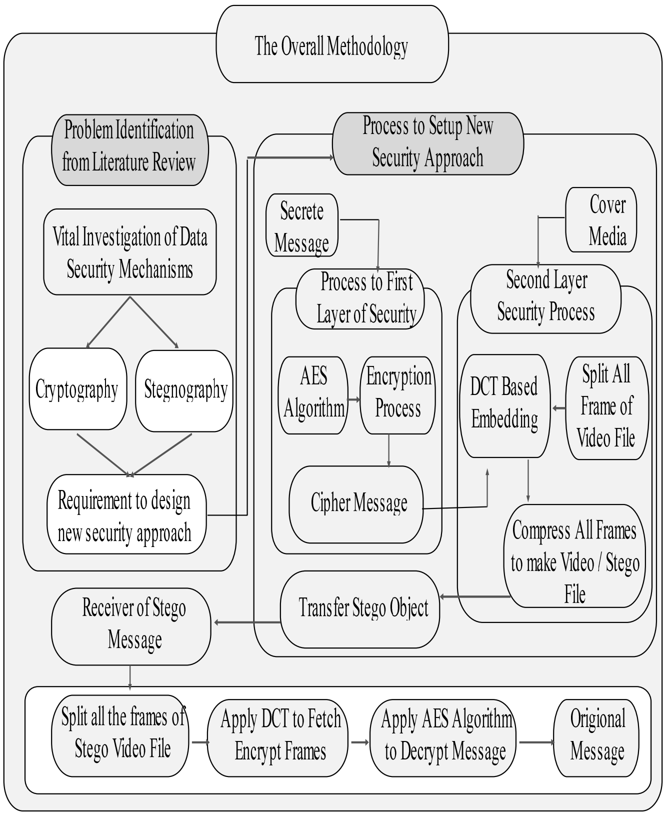

The Overall Methodology
Problem Identification from Literature Review
Vital Investigation of Data Security Mechanisms
Cryptography
Stegnography
Requirement to design new security approach
Process to Setup New Security Approach
Secrete Message
Cover Media
Process to First Layer of Security
Second Layer Security Process
AES Algorithm
Encryption Process
DCT Based Embedding
Split All Frame of Video File
Cipher Message
Compress All Frames to make Video / Stego File
Receiver of Stego Message
Transfer Stego Object
Split all the frames of Stego Video File
Apply DCT to Fetch Encrypt Frames
Apply AES Algorithm to Decrypt Message
Origional Message

Figure 1: Adopted Methodology to Secure Data

At first level of security secrete message is encrypted by using the Advance Encryption Standard (AES) algorithm that produce cipher file. The cipher file cannot be easily understand by any other user and secrete message can only be accessible after decode process with the right key which only contain by the actual receiver. After the encryption process the cipher file has split into 8 frames to increase the security level. For the second level of security a video file has taken into account, firstly split all the frames of video file and randomly select a extracted frame that supply as the input to Discrete Cosine Transform (DCT) based embedded algorithm with the cipher text file to hide the encrypt message. After complete this process all the extracted frames of video file has combine to generate the video as original one. The outcome file also known as stego file provide the second layer of security to information and no one can easily notice that running video has the hide information. Sender may send this stego file to receiver over the unsecured channel for the secure communication of secrete information. Whenever the receiver finds the stego file, apply the reverse methodology from the sender to get the correct secret message.

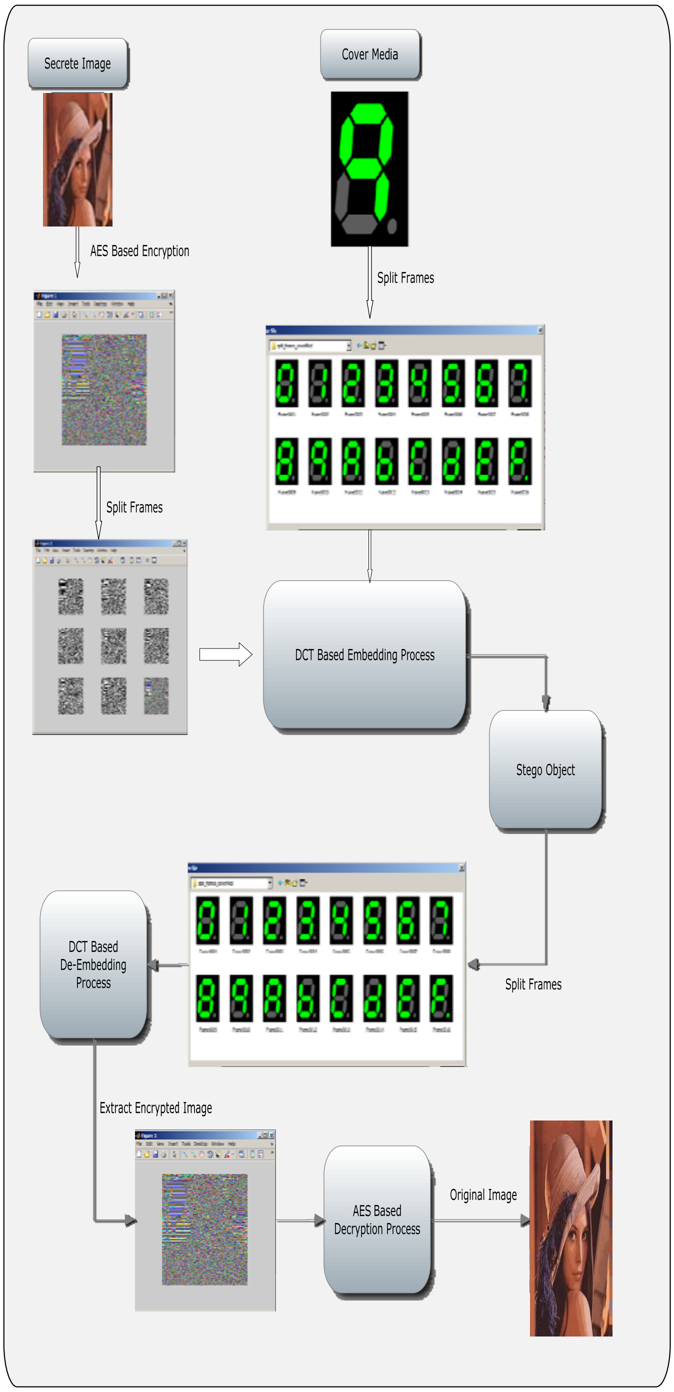


Figure 2: Proposed System Flow steps

The figure 4.5 & 4.6 clearly present the detailed steps of proposed system that adopt to provide the security to the information.

4. Experimental Results

Experiments are carried out using the MATLAB to evaluate the performance of the proposed approach. Numerous experiments are performed to ensure the quality measurement between the cover frame (original frame) and the stego frame (Frame that hide the secrete message). The frame quality parameters peak signal to noise ratio (PSNR) is used to examine the quality of the proposed approach.

4.1 Peak Signal to Noise Ratio (PSNR)

PSNR is one of metrics to determine the degradation in the embedded image with respect to the host image. It shows the quality of image after hiding the data. For the quality measurement between the cover image (original image) and the stego image the ratio of difference between image quality parameters (PSNR) are often used. For the better quality of the stego image the higher value of the PSNR between original image and the stego image shows better quality of the image and also indicate lower error. To compute the value of the image quality parameter PSNR, first of all the block calculates the value of MSE (Mean Square Error) by using the following the mathematical equation

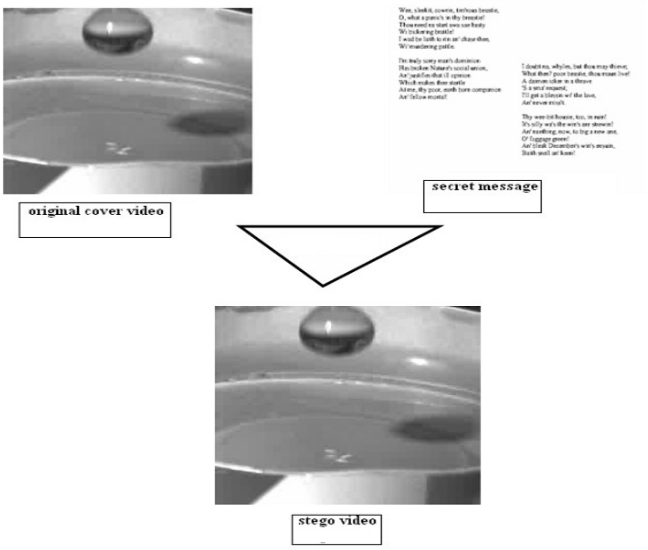
$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[L(i,j) - K(i,j)]^2$$

$$PSNR = 10\log_{10}\left(\frac{MAX_i^2}{MSE}\right)$$

Where

MAXI=Maximum value of pixel in Original image
m=No. of Row in Original image
n= No. of Column in Original image

In comparative analysis, proposed approach has executed with the same parameter as taken by [20]. Two video has taken in consideration (drop.avi, flame.avi) to evaluate results.



Wee, sleekit, cowrin, tim'rous beastie,
O, what a panic's in thy breastie!
Thou need na start awa sae hasty
Wi bickering brattle!
I wad be laith to rin an' chase thee,
Wi' murdering pattle.

I'm truly sorry man's dominion
Has broken Nature's social union,
An' justifies that ill opinion
Which makes thee startle
At me, thy poor, earth born companion
An' fellow mortal!

I doubt na, whyles, but thou may thieve;
What then? poor beastie, thou maun live!
A daimen icker in a thrave
'S a sma' request;
I'll get a blessin wi' the lave,
An' never miss't.

Thy wee-bit housie, too, in ruin!
It's silly wa's the win's are strewin!
An' naething, now, to big a new ane,
O' foggage green!
An' bleak December's win's ensuin,
Baith snell an' keen!

Figure 3: Drop.avi

Table 1 Present the comparative PSNR result of proposed approach against the techniques has been used in [20].

Table 1: PSNR Value of Frames

Name of the video file	Results obtained using Proposed Approach	Results obtained using HLSB [60]
Drop	46.2912	44.34
Flame	50.2615	42.66

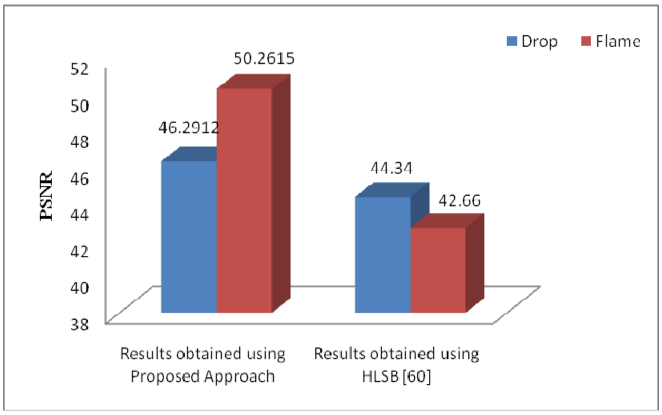


Figure 4: Comparative Result of Proposed Approach

The investigated approach has also not change its sizes as approach proposed in the [21], shown in following figures.

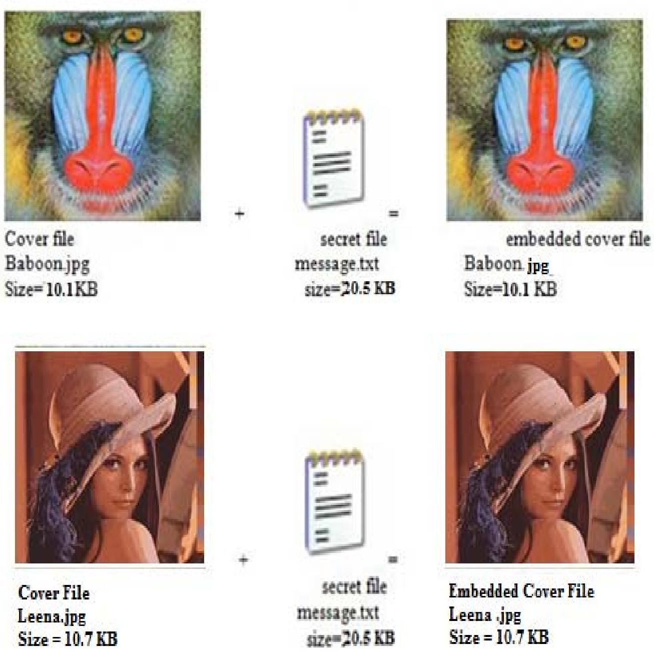


Figure 5: Size based comparative results

The results clearly indicated the superiority of the proposed approach over the other that has been indicated in the [20, 21].

5. Conclusion and Future Work

In current scenario technology face various challenges. Security of secrete message in one of the most challenging face in current scenario. In this term to provide more security to the information at the time of communication over unsecured channel a novel advance technique for data security is proposed in this paper. The approach proposed two layer of security to the information by combining the cryptography and steganography technique. If a level of the proposed approach will fail to secure the information, message will be safe with the second level of security mechanism of proposed approach that is the key contribution of this work.

For the future work the work can be done in direction to improve the time efficiency that proposed approach has taken into account to secure and retrieve the original information from the cover media. Apart from the time proposed way can be implemented with the audio file instead to video file to improve the hiding quality of the secrete message.

References

[1] Jefferson, D. et al. “Analyzing internet voting security”, 2004. ACM, 47(10):59-64.

[2] Schneier, B. “Secrets & Lies: Digital Security in a Networked World”. Wiley Computer Publishing. .

[3] Xia, H. &Brustoloni, J.C. 2005. Hardening web browsers against main-in-the-middle and eavesdropping attacks. Proceedings of the International Conference on World Wide Web, 489-498.

[4] Neil F. Johnson and SushilJajodia, “Steganalysis: The Investigation of Hidden Information,” IEEE conference on Information Technology, pp. 113-116, 1998.

[5] Currie, D.L. & Irvine, C.E., “Surmounting the effects of lossy compression on Steganography”, 19thNational Information Systems Security Conference, 1996

[6] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn. “Information Hiding – A Survey”, Proceedings of the IEEE, special issue on protection of multimedia content, July 1999, pp. 1062 – 1078.

[7] Monika Agarwal “TEXT STEGANOGRAPHIC APPROACHES: ACOMPARISON” International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013

[8] Arvind Kumar, Km. Pooja, “Steganography-A Data Hiding Technique” InternationalJournal of Computer Applications ISSN 0975– 8887, Volume 9– No.7, November 2010.

[9] Wang, H. & Wang, S. 2004. Cyber warfare: Steganography vs. steganalysis. Communications of the ACM, 47(10):76-82.

[10] Lisa M.Marvel and Charles T. Retter, “A Methodology for Data Hiding using Images,” IEEE conference on Military communication, vol. 3, Issue. 18-21, pp. 1044-1047, 1998.

[11] Giuseppe Mastronardi, Marcello Castellano, Francescomaria Marino, “Steganography Effects in Various Formats of Images. A Preliminary Study,” International Workshop on Intelligent data Acquisition and Advanced Computing Systems: Technology and Applications, pp. 116-119, 2001.

[12] LIU Tong, QIU Zheng-ding “A DWT-based color Images Steganography Scheme” IEEE International Conference on Signal Processing, vol. 2, pp.1568-1571, 2002.

[13] Jessica Fridrich, MiroslavGoijan and David Soukal, “Higher-order statistical steganalysis of palette images” Proceeding of SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia ContentsV, vol. 5020, pp. 178-190, 2003.

[14] Jessica Fridrich and David Soukal, “Matrix Embedding for Large Payloads” SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents, vol. 6072, pp. 727-738. 2006.

[15] Yuan-Yu Tsai, Chung-Ming Wang “A novel data hiding scheme for color images using a BSP tree” Journal of systems and software, vol.80, pp. 429-437, 2007.

[16] Shilpa P. Hivrale, S. D. Sawarkar, Vijay Bhosale, and SeemaKoregaonkar “Statistical Method forHiding Detection in LSB of Digital Images: An Overview World Academy of Science, Engineeringand Technology, vol. 32, pp. 658-661, 2008.

[17] K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal,L. M. Patnaik, “Robust Image Adaptive Steganography using Integer Wavelets” International conference on Communication Systems Software, pp. 614-621, 2008.

[18] Jan Kodovsky, Jessica Fridrich “Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain” Proceedings of SPIE, the International Society for OpticalEngineering, vol. 6819, pp. 681902.1-681902.13, 2008.

[19] L. Y. Por, W. K. Lai, Z. Alireza, T. F. Ang, M. T. Su, B. Delina, “StegCure: A Comprehensive Steganographic Tool using Enhanced LSB Scheme,” Journal of WSEAS Transctions on Computers, vol. 8, pp. 1309-1318, 2008.

[20] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta "Hash Based Least Significant Bit Technique For Video Steganography(Hlsb)",International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012

[21] Harshitha K M, Dr. P. A. Vijaya "Secure Data Hiding Algorithm Using Encrypted Secret Message", International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012