ISSN No:-2456-2165

A Review of Steganography

Namrata Singh, Vinod Todwal
College:- RCEW

Abstract:-Steganography is a method for inserting digital data within a different digital medium like text, pictures, sound signals, or film signals, while not exposing its occurrence in the medium. Information safekeeping is an essential necessary domain in correspondence medium over the web system. In this paper, we focus on the information safekeeping technology with encoding or decoding. Steganographic techniques are utilized for concealed correspondence by concealing the data within the multimedia information documents. Moreover, film steganography is an operation to hide whichever kind of information into a transporting film document.

I. INTRODUCTION

These days, the necessity to guard digital data has evolved to be a significant theme. The term steganography blends the old greek terms steganos, meaning concealed, and graphos, meaning writing. It is the technique of concealing surreptitious data inside a different conveyor, for example picture, films, texts and graphics, to get the stego entity such that it is not changed after integration. In this manner, just the recipient is conscious of the existence of the surreptitious communication and may extract it. Steganography is categorized into two fields, namely spatial and frequency [1]. In the spatial field, the alterations are applied on the pixels of the initial picture. The surreptitious picture is embedded straight into these pixels. In the frequency field, the conveyor picture is changed from the first field to this one through the methods of field changing. The surreptitious communication is embedded into the changed coefficients of the concealer to become the stego picture [1, 2]. The frequency field has numerous benefits: it is more solid compared to the spatial method, it is lenient to cutting, condensing, picture handling, and so on [1, 2, 3]. There are numerous changes utilized to superpose a signal into the frequency field [3]. The most recognized techniques applied in the literature are Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), and Discrete Cosine Transform (DCT) [1, 3].

There are several metrics utilized to assess a steganography scheme, like the Mean Square Error (MSE), Structural Similarity (SSIM) Index, Peak Signal To Noise Ratio (PSNR), the volume, and the strength and safety [1, 2]. Strength is the capability of the stego picture versus various sorts of assaults, whereas the safety is the failure of the opponent to sense concealed pictures available just for the enabled user [5]. Steganalysis is utilized to sense the concealed data [5]. Of the multimedia data, digital pictures are the most generally and recurrently sent through the Web. Thus the necessity to guard them. Several kinds of pictures may be utilized as concealer media like Joint Photographic Experts Group (JPEG), Bitmap File Format (BMP), and Graphics Interchange Format (GIF) pictures [6]. This investigation is mainly focused on BMP pictures. It examined the steganographic techniques that insert communication in the LSB or Least Significant Bit of DCT coefficients. The insertion may be carried out in two manners, namely sequential and arbitrarily. The issue with the sequential insertion is the insecurity, the surreptitious communication may be sensed with ease. Among the suggested ameliorations of this method in past works is LSB-DCT with limit, it conceals information in arbitrary areas as per a limit [7]. The issue here is the restricted capacity in relation to the used limit, additionally it may be torn with ease in case this limit is found. Thus the goal of this work is to offer a new picture DWT technique with high insertion capacity and increased safety by utilizing a messy generator, the PWLCM or Piece Wise Linear Chaotic Map.

For concealing surreptitious data in pictures, there is a significant range of steganography methods; some are more intricate than others, while all of them possess robust and fragile factors. Dissimilar applications can necessitate complete transparency of the surreptitious data, while others necessitate a big surreptitious communication to be concealed. What steganography basically does is take advantage of people's vision, people's senses are not skilled to search documents that have data concealed within them, even though there are accessible software to perform what is termed steganalysis (sensing the utilization of steganography). The most widespread usage of steganography is to conceal a document within another document. Once data or a document is concealed within a conveyor document, the information is generally coded with a key.

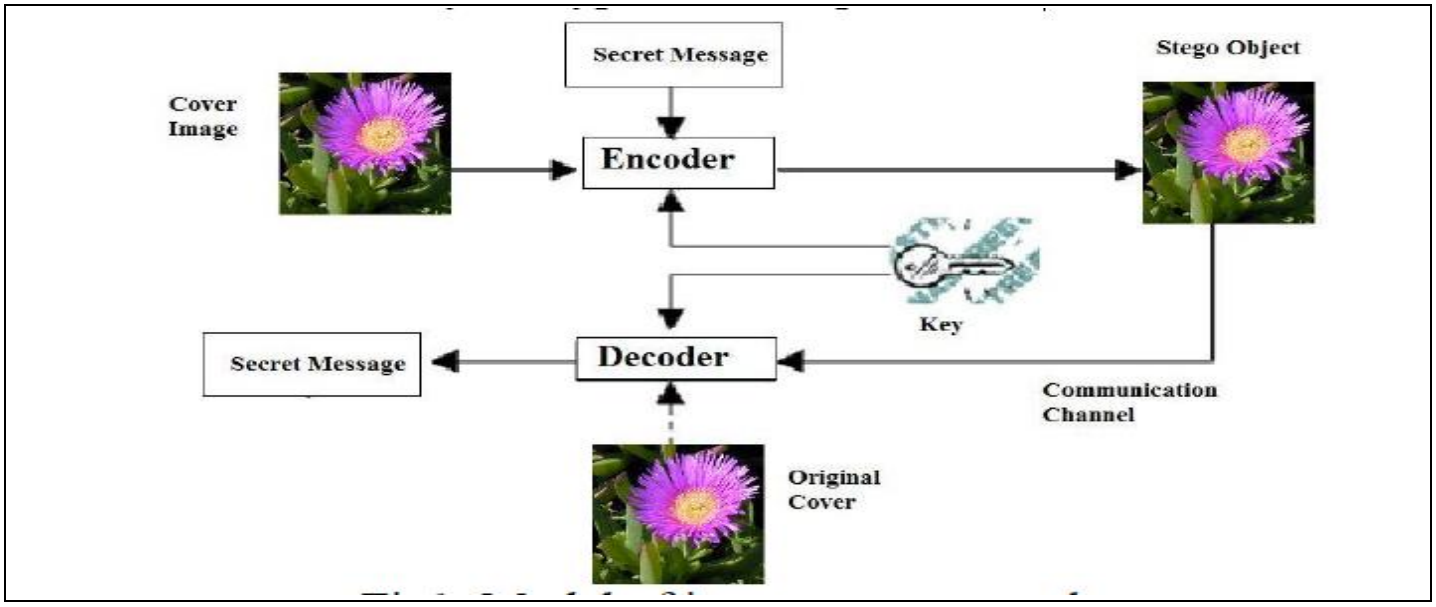

Fig. 1: Model of Image Steganography

II. LITERATURE REVIEW

Jain et al. (2012) wrote an article about steganography which is similarly a framework that may be used with the ultimate aim of hiding the whole information that may be used for ongoing communication, when you mask data within some different data. Steganography is the method of hiding the manner that communication is happening, by hiding data within a different data. An extensive variety of carrier text settings may be used, though digital images are the most dominant with regards to their repetition on the web. To hide secret information in images, there is a wide range of steganographic techniques and some are more complex than others, though all have certain advantages and disadvantages. Steganalysis, the recognition of this hidden information, is a typically difficult challenge and necessitates a thorough scrutiny, therefore the authors used "Edge Discovery Filter" [18].

Rafiuddin et al. (2013) introduced an article about steganography which is the technique and art of hiding information within different information in a way that is difficult or even challenging to say that it is present. Different carrier text installations may be used, though sophisticated images are the most recognized because of their repetition on the internet. The carrier may then be transmitted to a receiver without any third party noticing that it has a hidden communication. Protection of any steganography method depends on the characteristic of the image after hiding the information within the image. Features of stego image (final image) depend on the approximation of PSNR, SNR, and quantity of LSB modified. Direct LSB steganography process is the most used technique to hide secret information at every significant bit of the pixels in the stego-image. However, a suggested LSB technique separates the secret communication into a quantity of portions that have identical length (quantity of characters), and find the best Least Significant Bits of pixels in the stego-image that are arranged to each portion. The principal aim behind this method is to reduce to a minimum the number of LSBs that are changed. This shall trigger an increase in the approximation of PSNR and improve the characteristics of the stego image and consequently increase the resilience of the stego image against ocular attack. The study shows that the suggested technique provides significant change in outcome in comparison to the classic LSB framework [19].

Kaur et al. (2012) published an article about information safety which has become a main concern for all who utilize public tunnels to send their confidential data in this computer generation as well. Many techniques have been generated over a perfect prospect to communicate the secret message without the risk of losing confidentiality. Steganography is among the widely recognized processes utilized to mask the confidential information within images without being perceived by people's eyes. The authors showed the use of steganography with 2k correction method and border recognition method in this work. This process evolves to be better to any previous works with regards to its capability of transmitting more messages with superior discretion. This may be achieved by setting up more data in border positions when compared to the smooth varieties of the image as people's eyes may not discern the distortion at borders successfully. The suggested algorithm gives superior PSNR values compared to various methods used as part of steganography [20].

Kaur et al. (2001) showed an article about borders of an RGB image which has been discerned by half and half border locator which is the mixture of 3x3 lattice sorting and sobel border identifier, and subsequently the composition shall be inserted into the main portion of borders of the shading image. Experiments show that the authors have achieved elevated setting up limit and enhanced the characteristics of the stego image [21].

Rekha et al. (2012) introduces an article about steganographic and cryptographic methods which are a great concern in digital generation. Everyone requires security in this internet world. As the quantity of users grows, the secrecy in communication has become more and more essential. Rearrangement of data size and text quality via communication tunnel is an important trial for steganographic method. Least Significant Bit is among the essential and actual steganography methods in spatial area, addition of data in any occasion significant bits has elevated ocular quality though not resilient against distortion and hence not really safe. In the suggested method, the secret data is encrypted by using composite encoding method, that is Advance Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) method to protect the secret communication. Here, Lempel Ziv Welch method contains the necessary quantity of data to talk to information quantity. At that moment, border finding method identifies the sharp element of image to hide the secret data. The principal element of the suggested method is to provide superior protection by using the concepts of cryptography and picture steganography. Even if the attackers know about the secret information, they are unable to retrieve the correct information. Difference can be observed by inspecting the results of literature works and the suggested method. Superior encoding methods are taken to provide superior protection with steganography [22].

Dhaka et al. (2013) published an article about a new steganographic method for pictures which is a kind of spatial field data concealing method. To conceal the confidential data in initial picture or host picture, the useful tunnel choosing method is employed. In the past picture steganographic method, the authors concealed the confidential information in the just 2, 3, or 4 bits or a maximum of 5 bits of one pixel in a picture which generates the low value of PSNR and elevated value of RMSE or Root Mean Square Error, both being the picture quality boundaries. The suggested method may insert a significant quantity of information compared to past methods and demonstrates superior outcomes of picture quality boundary [23].

Kulshreshta et al. (2013) introduced an article about the fundamental structure of steganography which consists of three elements, namely the host picture, the communication, and the key. The transporter may be a computerized picture; it is the item which shall transport the concealed communication. A key is utilized to decrypt/interpret/find the concealed communication. This may be a password, a black-code, a pattern, and so on. In this work, the authors suggest a novel type of steganography, which addresses the demerits of basic LSB replacement and a symmetric encoding calculation termed Blowfish algorithm [24].

Keerthi et al. (2014) wrote an article concerning a new technique of black and white picture steganography which is founded on border sensing and adjustable several bits replacement. The pixels found in the border areas typically show more haphazard properties compared to the plane areas. In the suggested technique, the Sobel operator is utilized to calculate the gradient value of the pixels of the host picture. Consequently, every border of the host picture, both horizontal and upright, is completely sensed. The sharper borders are adjustably kept and the weaker borders are removed, depending on the length of the private information. So, the sharper borders shall be utilized prior to the weaker borders and the plane areas for information incorporation. Thereafter, the information insertion pathway is deduced by utilizing a PseudoRandom Number Generator (PRNG) and several bits of private information are adjustably inserted into k-LSBs of the pixels found in the pathway. The magnitude of k relies on the gradient value of every pixel. The greater the gradient value, the greater the k value [25].

Kaur et al. (2014) showed an article concerning computerized steganography which is utilized to secure computerized material or information like document, pictures, sound, and video clips that have been corrupted wrongly. In this research, the authors keep the quality of sound and picture and to guarantee the proprietorship, they suggest a novel LSB utilizing border sensing in computerized steganography. They administer a two stage steganography on pictures and sound which can be document or picture in safer format. Employing LSB methods can impact less on the picture pixel quality and soundtrack quality. Here, they may haphazardly chose borders and insert the document or picture by taking into account the picture quality, soundtrack quality, and non-perception of soundtrack. This work gives the suggested calculation more security because of the two stage steganography which provides the resilience and good quality of pictures or soundtrack [26].

Tamanna et al. (2015) introduces an article concerning steganography which is a method to hide data to a degree that no one other than the sender and the targeted recipient expect the occurrence of concealed information. Steganography is the art of hiding vital data in a manner that limit identification. The steganography used to carry essential data from merely one place to another place by utilizing universal shared network as part of a subtle manner. Steganography conceals completely the occurrence of data to guarantee that if vital, it normally attracts no doubt in any case. Steganography implies that hiding a secret data (the embedded communication) within a larger one (origin host) in such a manner that a third party may not recognize the obvious occurrence of composition of the concealed communication [1]. Many dissimilar service provider file templates may be utilized, though computerized pictures are the most dominant due to the recurrence on the web. To conceal secret vital information within pictures, there are a large selection of steganographic methods, some significantly more complex than others, and all have corresponding benefits and drawbacks. Various software have in fact dissimilar particularities for the steganography method utilized. This specific paper guarantees to give a presentation to picture steganography it uses and methods. It further projects to find the conditions of a satisfactory steganography calculation policy and rapidly show which

steganographic methods are apt to be more suitable for which uses [27].

Goswami et al. (2016) wrote an article about steganography which is a technique of concealing private data within a multimedia transporter as picture file, soundtrack file, and video clip. This is different from cryptography which is used to render a communication undecipherable by an onlooker though does not conceal the presence of the confidential message. Investigation challenges in picture steganography are to augment the proficiency with regards to the payload volume of the private data, resilience against ocular assaults and statistical assaults. Picture steganography in Wavelet conversion field have superior strength against statistical assaults than picture steganography in the spatial field and DCT field whereas DCT picture steganography have superior invisibility in contrast to Discrete Wavelet Transform (DWT) picture steganography. The joint method of DWT and DCT gives the benefits of the two methods. The suggested calculation shows composite DCT-DWT computerized picture steganography calculation. The suggested method insertion, the picture incorporated is a transparent portion of a picture than alternative techniques displayed in results. Steganography is executed by inserting the picture in middle frequency coefficient set of the three stage DWT conversion of the cover picture, then the block DCT conversion and insertion in chosen HH DWT coefficient sets [28].

Kaur et al. (2011) introduced a paper about the multimedia material that are transmitted through the web, therefore it is a pressing necessity now to secure the information from wrongful assaults. This results in investigation in the field of computerized watermarking which aims to secure the patent data of the owners. In this work, a DCT founded watermarking method is suggested which gives better resilience to picture treating assaults like JPEG condensation, buzzing, turning, translation, and so on. In this method, the watermark is inserted in the center frequency band of the DCT blocks transporting inferior frequency elements and the elevated frequency secondary band elements stay unutilized. The watermark is integrated by adapting the DCT coefficients of the picture and by utilizing the secret key. The watermark may thereafter be retrieved by utilizing this secret key without passing through the initial picture. Performance evaluation demonstrates that the watermark is resilient [29].

Guptam et al. (2015) published an article concerning steganography which is a craft and a discipline of messaging in a manner that conceals the presence of the message. It is additionally termed "covered writing" as it utilizes a "cover" of a communication for transmitting any vital private communication. In the steganographic situation, the private information is initially hidden inside a different item which is referred to as the "cover item" to form the "stego-item" and subsequently this novel item may be sent or stockpiled. Utilizing various methods, they may transmit confidential information as a picture, an audio file, or even a video clip by incorporating it into the transporter, creating a stego-signal. At the recipient's side, the confidential information may be retrieved from the stego-signal by utilizing various calculations. The principal aim of steganography is to message safely in a totally untraceable way and to prevent attracting doubts to the sending of a concealed information. It not just stops others from learning the concealed data, but it further stops others from contemplating the very existence of the data. In case a steganography technique makes a person doubtful that there is hidden data within a transporter medium, then the technique is unsuccessful [30].

Kaur et al. (2013) introduced an article about steganography which is a way to conceal information within pictures for secret communication. Lately, steganography and steganalysis are two fundamental fields of investigation that implicate a quantity of uses. These two fields of investigation are essential particularly when dependable and safe data exchange is needed. Steganography is a craft of inserting data inside a host picture without creating statistically consequent changes to the host picture. Steganalysis is a technology which tries to crush steganography by sensing the concealed data and retrieving. In this work, the scientists suggest a picture steganography that may confirm the dependability of the data being sent to the recipient. This work is founded on the contrast of the DCT and DWT technique. This work shows a new method for picture steganography founded on DWT, where DWT is utilized to convert the initial picture (host picture) from spatial field to frequency field. The empirical yields demonstrate that the calculation has an elevated volume and a satisfactory imperceptibility in contrast to DCT. Furthermore, PSNR of host picture with stego-picture demonstrates the superior outcomes compared to the current steganography methods. Additionally, DWT technique is best when the payload volume is augmented [31].

Goel et al. (2013) wrote an article about steganography which is an essential field of investigation lately implicating a quantity of uses. It is the discipline of inserting data into the host picture, that is document, video clip, and picture (payload) without creating statistically consequent changes to the host picture. The contemporary safe picture steganography introduces a difficult job of relocating the inserted data to the target without being sensed. In this article, a DCT founded strong technique has been devised. The host picture is partitioned into 8x8 blocks and DCT is administered on the picture. The document to be concealed is inserted in the diagonal components of the blocks by replacing a haphazard variable in place of the bits of the document to be inserted. It is found that the suggested calculation is stronger with superior CER and Normalized coefficient [32].

Mamata et al. (2012) introduced an article about steganography which is the technique of concealing the presence of information in a different carrier medium to realize covert messaging. It is the discipline of inserting data into the host picture, that is document, video clip, and picture (payload) without creating statistically consequent changes to the host picture. This article addresses concealing credit card numbers in a picture file (empty logo) by utilizing DCT founded steganography and DWT founded

steganography. It is a new lossless safe information insertion calculation where the essential data may be inserted into the host picture whilst maintaining the quality of host picture and keeping the safety of the information. The safety of the information inserted and host picture quality are two major challenges that have to be taken into account while incorporating the information. Scramble Data Embedding in Mid-frequency range of DCT (SDEM-DCT) and Scramble Data Embedding in Mid-frequency range of DWT (SDEM-DWT) calculation comprises of three main protection phases that may be utilized to conceal credit card numbers of clients within the bank's logo. The implementation and contrast of methods is assessed according to the boundaries PSNR, Correlation, MSE, Capacity, Embedding capacity, and Processing time [33].

III. CONCLUSION

This paper presents a comprehensive review of video steganographic techniques. Difference between steganography, cryptography, and watermarking were discussed. An overview of steganography using different cover types was presented and special attention was paid to video steganography and its applications. Various categorizations of the existing techniques were illustrated. Techniques belonging to each domain were discussed and comparisons between those techniques were presented highlighting their advantages and disadvantages. Furthermore, popular image and video quality metrics available in the literature were discussed. Finally, steganalysis was surveyed from the point of view that improves the design of good steganographic systems. Based on this review, the following recommendations may help interested researchers in video steganography.

REFERENCES

[1]. S. Bhattacharyya,. "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier." Journal of global research in computer science 2, no. 4 (2011).

[2]. S. Saejung, A. Boondee, J. Preechasuk, and C. Chantrapornchai, "On the comparison of digital image steganography algorithm based on DCT and wavelet," in Computer Science and Engineering Conference (ICSEC),2013 International, 2013, pp. 328–333.

[3]. M. Tayel, H. Shawky and A. E. S. Hafez, "A New Chaos SteganographyAlgorithm for Hiding Multimedia Data," 14th International Conference on Advanced Communication Technology, pp. 208 – 212, 2012.

[4]. N. Sathisha, G. N. Madhusudan, S. Bharathesh, K. B. Suresh, K. B. Raja and K. R. Venugopal, "Chaos based Spatial Domain Steganography using MSB", International Conference on Industrial and InformationSystems(ICIIS), pp. 177-182, 2010.

[5]. N. Raftari and A.-M. E. Moghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT," in 2012Fourth International Conference on Computational Intelligence,Communication Systems and Networks (CICSyN), 2012, pp. 295–300.

[6]. N. Sathisha, K. Suresh Babu, K. B. Raja, K. R. Venugopal and L. Patnaik,"Embedding Information In DCT Coefficients Based On AverageCovariance" International Journal of Engineering Science andTechnology (IJEST), 3 (4), 3184-3194. 2011.

[7]. A. Danti, and P. Acharya. "Randomized embedding scheme based on DCT coefficients for image steganography." IJCA Special Issue on recent trends in Image Processing and Pattern Recognition (2010).

[8]. D. Neeta, S. Kamalapur and D. Jacobs, "Implementation of LSB steganography and Its Evaluation for various Bits" in Digital InformationManagement, 2006 1st International Conference on. 06/01/2007; DOI:10.1109/ICDIM.2007.369349

[9]. N. Kafri and H. Y. Suleiman, "Bit-4 of frequency domain-DCTsteganography technique," in First International Conference on Networked Digital Technologies, 2009. NDT ,09, 2009, pp. 286–291.

[10]. J. M. Rodrigues, J. R. Rios, and W. Puech. "SSB-4 System ofSteganography using bit 4." In 5th International Workshop on ImageAnalysis for Multimedia Interactive Services. 2004.

[11]. B. Bakhache, J. M. Ghazal, and S. E. Assad, "Improvement of the Security of ZigBee by a New Chaotic Algorithm," IEEE Syst. J., vol. Early AccessOnline, 2013.

[12]. S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang, "On the security of a chaotic encryption scheme: problems with computerized chaos infinite computing precision," Comput. Phys. Commun., vol. 153, no. 1, pp. 52–58, Jun. 2003.

[13]. S. Tao, W. Ruli, and Y. Yixun, "Perturbance based algorithm to expand cycle length of chaotic key stream," IEEE Electron. Lett., vol. 34, no.9,pp. 873–874, Apr. 1998.

[14]. E. Walia, P. Jain, Navdeep, "An Analysis of LSB & DCT basedSteganography", Global Journal of Computer Science and Technology,April, 2010, Vol. 10, pp. 4-8.

[15]. S. K. Mutt and S. Kumar, "Secure image steganography based on Slantlettransform," in Proceeding of International Conference on Methods and models in Computer Science, 2009. ICM2CS 2009, 2009, pp. 1–7.

[16]. Y. Wang and P. Moulin, "Optimized Feature Extraction for Learning-Based Image Steganalysis, "IEEE Trans. Inf. Forensics Secur., vol. 2, no.1, pp. 31–45, Mar. 2007.

[17]. D. Caragata, S. El Assad, B. Bakhache, and I. Tutanescu, "Secure IP over Satellite DVB Using Chaotic Sequences". Engineering Letters journal.Volume 18, number 2, 2010, pp. 135-146.

[18]. Nitin Jain, Sachin Meshram, Shikha Dubey ," Image Steganography Using LSB and Edge – Detection Technique ", International Journal of Soft Computing

and Engineering (IJSCE) , Volume-2, Issue-3, July 2012.
[19]. Kazi Azizuddin Rafiuddin1, Chetan Kumar," Improvement in LSB Image Steganography using Message Partitioning ", International Journal of Recent Research and Review, Vol. VI, Issue 3, December 2013.
[20]. Amanpreet Kaur, Sumeet Kaur," Image Steganography Based on Hybrid Edge Detection and 2k Correction Method ", International Journal of Engineering and Innovative Technology (IJEIT)Volume 1, Issue 2, February 2012.
[21]. Sarabjeet Kaur and Sonika Jindal ," Image Steganography using Hybrid Edge Detection and First Component Alteration Technique ", International Journal of Hybrid Information Technology Vol.6, No.5 (2013).
[22]. S. N. Rekha, Y. Manjula, M.Z. Kurian ," A Secured Lsb Image Steganography System Using Edge Detection, Low Compression And Hybrid Encryption Methods ",International Journal Of Advanced Technology In Engineering And Science.
[23]. Vijaypal Dhaka ,Ramesh C. Poonia, Yash Veer Singh ," A Novel Algorithm for Image Steganography Based on Effective Channel Selection Technique ",International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 3, Issue 8, August 2013.
[24]. Aishwary Kulshreshta , Ankur Goyal," Image Steganography Using Dynamic LSB with Blowfish Algorithm ", International Journal of Computer & Organization Trends –Volume 3 Issue 7 – August 2013.
[25]. Keerthi K M ," A Novel Steganographic Method based on Edge Detection and Adaptive Multiple Bits Substitution ", International Journal of Computer Applications (0975 – 8887) Advanced Computing and Communication Techniques for High Performance Applications (ICACCTHPA-2014).
[26]. Navneet Kaur1 and Sunny Behal ," Audio Steganography Using LSB Edge Detection Algorithm ", International Conference on Communication, Computing & Systems (ICCCS) 2014.
[27]. Tamanna , Ashwani Sethi," Steganography: A Juxtaposition between LSB DCT, DWT ", International Journal of Computer Applications (0975 – 8887) Volume 126 – No.11, September 2015 .
[28]. Anuradha Goswami1, Sarika Khandelwal," Hybrid DCT-DWT Digital Image Steganography ", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 6, June 2016.
[29]. Blossom Kaur1, Amandeep Kaur2, Jasdeep Singh ," Steganographic Approach For Hiding Image In DCT Domain ", International Journal Of Advances In Engineering & Technology, July 2011.
[30]. Sumeet Gupta1, Dr. Namrata Dhanda," Audio Steganography Using Discrete Wavelet Transformation (DWT) & Discrete Cosine Transformation (DCT) ", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 17, Issue 2, Mar – Apr. 2015.
[31]. Gurmeet Kaur* and Aarti Kochhar ," Transform Domain Analysis of Image Steganography ", International Journal for Science and Emerging Technologies with Latest Trends" 2013.
[32]. Stuti Goel, Arun Rana,Manpreet Kaur ,"ADCT-based Robust Methodology for Image Steganography ", Image, Graphics and Signal Processing, 2013.
[33]. Mamata J, Poornima G," Comparative Analysis of Embedding Data in Image using DCT and DWT Techniques ",International Journal of Science and Research (IJSR),2012.
[34]. Yugeshwari Kakde, 2Priyanka Gonnade, 3Prashant Dahiwale," Audio-Video steganography", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems, 2015.