IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

VIDEO STEGANOGRAPHY TECHNIQUES FOR DATA HIDING – A perspective

Pooja H A
Department of Electronics and Communication Engineering
RNS Institute of Technology
Bangalore, India

Dr. Uma S V
Department of Electronics and Communication Engineering
RNS Institute of Technology
Bangalore, India

ABSTRACT: ***Since hackers can use fragile connections over corresponding networks to steal data, security issues should be considered when transmitting secret data. Steganography is a method of encrypting data sent between two parties. Text, image, video, and audio steganography are the four forms of steganography. Video steganography is an extension of image steganography in which any file with any extension is concealed inside a digital video. Since the video content is complex, detecting secret data is more difficult than for other steganography techniques. The key reason for using video steganography is that videos can store a lot of information. This paper gives a review on video steganography techniques for data hiding with enhanced security.***

Keyword: Video Steganography, MSE, PSNR, Stego-file, Cover-file.

I. INTRODUCTION

In today's digital world, the internet has emerged as the most popular means of communication. Every internet user demands secrecy, privacy, confidentiality, and authentication, among several other aspects. Information security is the analysis of sending and receiving data in a safe and secure manner. The two main information security techniques are cryptography and steganography. Both cryptography and steganography are information-security techniques, but their implementation differs.
Steganography is a technique for concealing hidden data in an ordinary carrier invisibly. A digital image, audio file, or video file may be used as the cover file or carrier. Trithemius invented the term "steganography" in the late 1400s, and its name comes from the Greek word for "covered or hidden writing." Steganography's primary objective is to discourage unintended users from stealing or losing sensitive information.

Steganography faces three major challenges: imperceptibility, robustness, and capacity, all of which are interdependent. Imperceptibility means that no one can detect the presence of the hidden message inside the cover media after it has been embedded. Robustness means that if anyone can find out that a hidden message exists, he won't be able to get it. The maximum amount of hidden data should be incorporated in such a way that the cover media's perceptibility, i.e. capability, is not compromised. Hiding can be performed in different domains, including spatial and transform domains.

Steganography has been divided into five types based on the type of cover object used, as shown in Fig 1. 1 [1]. Text steganography is primarily concerned with hiding text in both text and binary files. Inside a video, text can be scrambled or hidden in various ways. Text steganography has very high capacity when it comes to hiding text data in a Cover Text File. Many methods are used, such as sequencing, in which each character of the secret message is hidden in a fixed location of text or the secret message's binary value is hidden in the binary value of text. The main aim of digital image steganography is to hide data inside a cover image. Digital photographs are commonly used cover media in steganography due to their prominence in the modern internet era. A set of pixels can be described as a digital image. Data is concealed by choosing pixels based on their intensities. Many different image file formats exist in the world of digital images, the majority of which are designed for specific applications. Different steganographic algorithms exist for these various image file formats. A simple image steganographic model consists of an original image, known as the cover (I) image, in which the secret component secret message/image (M) is concealed, as well as a stego key (K), which is used to both hide and extract the information. The use of a stego key is intended to provide protection. Finally, after the steganographic process, an image is obtained. The effect is a stego-image (S) in which the pixel value varies from the pixel value of the original image, but the variations are so small that human eyes cannot perceive them. Video is a mixture of audio and a series of still images that pass in a continuous time sequence. Videos are becoming more common as a steganography cover object due to their higher embedding payload than digital images and their temporal features, which provide perpetual redundancy not available in digital images. Secret data can be easily disguised within a video due to the large number of frames available. The binary sequence

of video file is slightly differ from original file which cannot be easily be detected by human eyes. Protocol steganography is a technique for hiding hidden information in certain network protocols. There are covert channels in the layers of the OSI network model where steganography can be used. In the application layer of the TCP/IP protocol, steganography is used. Since there is a field in the IP header in the TCP/IP suite or the internet for data hiding, this form of technique is used at the network level to conceal the hidden message. Protocol Steganography makes use of flags and identification areas. Due to its high security, high embedding power, and high embedding performance, DNA steganography is becoming incredibly popular.

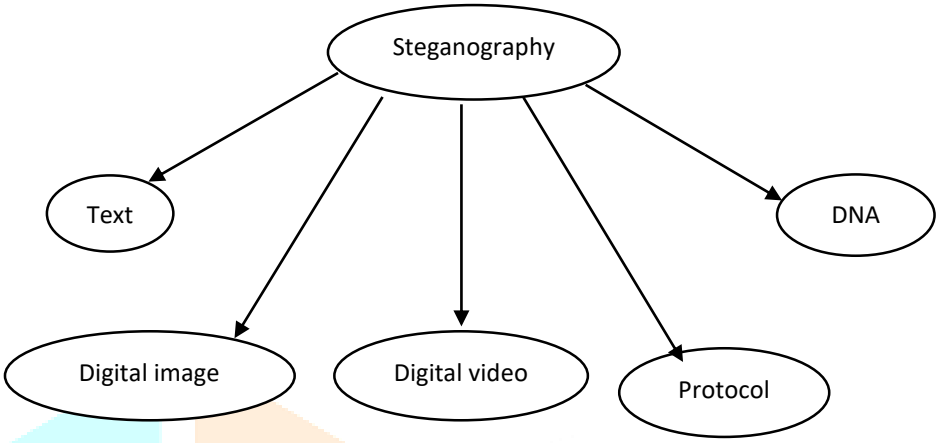

Fig 1.1 Types of Steganography

II. VIDEO STEGANOGRAPHY

Video steganography is a technique for hiding data in a video file while it is being created. Because of its size and memory requirements, video steganography is more suitable than multimedia files. A digital video containing a series of frames cooperating back at determined frame rates based on the video standards is known as video steganography. The details in certain individual frames is hidden using video steganography. It's difficult to see which frame the information or data are hidden in after they've been covered.

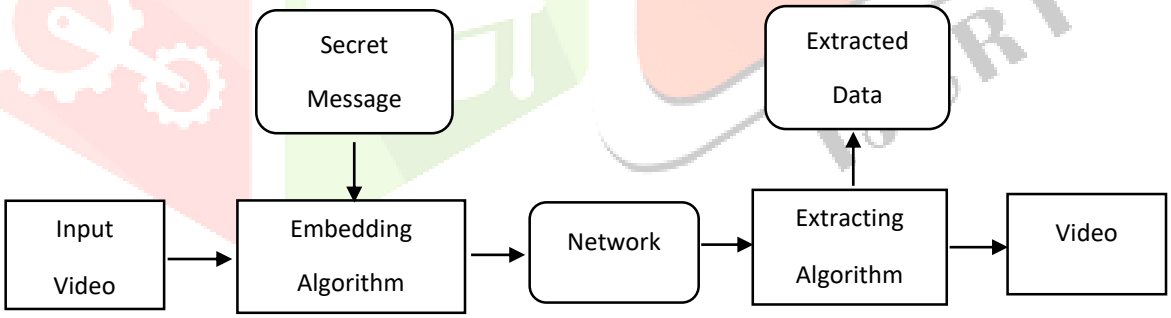

Figure 2.1 Block diagram of Video steganography

The block diagram of video steganography is shown in the Fig 2.1 [2]. Video is taken as input at the sender's end, and decomposed into a number of frames. With the support of certain embedding algorithms, the hidden message is inserted into the frames and sent over the network as stego-video. The stego-video is processed with some extracting algorithms at the receiver's end, and the secret data is extracted from the video sequences. The data is carried by the video sent by the sender to the recipient, but the presence of the data cannot be identified by an outsider.

Image steganography can be considered a subset of video steganography. The video stream consists of a series of identically timed still images accompanied by audio. Video steganography uses the same methods as image steganography. A smaller cover file can be used to conceal the hidden message as the hiding ability increases. As a consequence, a smaller stego-file can be used, which can be conveniently distributed over the internet. However, increasing the hiding capacity creates stego-file distortions. If an intruder notices the distortion, they may use it to their advantage. The benefit of using video as a cover medium for storing data is that it provides a vast amount of storage space. Since a video file is much more complicated than an image file, it offers more protection against an intruder. Another benefit is that the hidden data is undetectable to the naked eye because the difference in pixel color is so small. We can also conceal hidden data in audio files using video steganography because audio files contain unused bits. Video steganography is a better method than any other stenographic method when we need to store a large number of data.

III. VIDEO STEGANOGRAPHY MEASURES

For any successful video steganography system following measures should be considered:

A. Imperceptibility

The visibility of change within the cover media is referred to as imperceptibility. Increased invisibility of small changes in the cover item is referred to as high imperceptibility. Modern steganalysis methods are extremely intelligent when it comes to detecting minor changes. High imperceptibility has prompted researchers to develop steganography methods that are immune to steganography study [3] [4].

B. Payload

The amount of secret message that can be hidden within cover media is referred to as payload or power [5]. Due to their high embedding ability and embedding quality, video is becoming a common cover media object.

C. Statistical Attacks

Statistical attacks [6] are attacks or methods used on stego objects to retrieve hidden or secret information. The algorithm for steganography must be immune to statistical attacks. It defines the function of robustness.

D. Security

Security is the most important aspect of any steganographic algorithm. The embedding mechanism should be highly secure with a low attack vulnerability. Several approaches to steganography message protection have been suggested [7].

E. Computational Cost

The two parameters used to quantify the computational cost of any steganography method are data hiding and data retrieval [8]. The time it takes to insert data within a cover video frame is called data hiding time, and the time it takes to retrieve the hidden message from the stego frame is called data retrieval time.

F. Perceptual Quality

Increasing in embedding capability could result in a decrease in video quality or a loss of the video's original content. The video steganography method must be able to monitor video quality degradation [9].

IV. VIDEO STEGANOGRAPHY TECHNIQUES

Video streams have a high spatial and temporal redundancy, making them a strong candidate for security applications such as military and intelligence communications [10]. Video steganography methods are divided into many categories. The embedding process, i.e. spatial or substitution based techniques [11, 12, 13, 14] and transform based techniques [14, 15], is one way to categorize video steganography techniques. As seen in Fig 3.1, videos can also be categorized based on compression, i.e. compressed [16] and uncompressed video techniques [17, 18]. Another method for categorizing video steganography techniques is to use classification, such as Format based and Video Codec Methods [19].

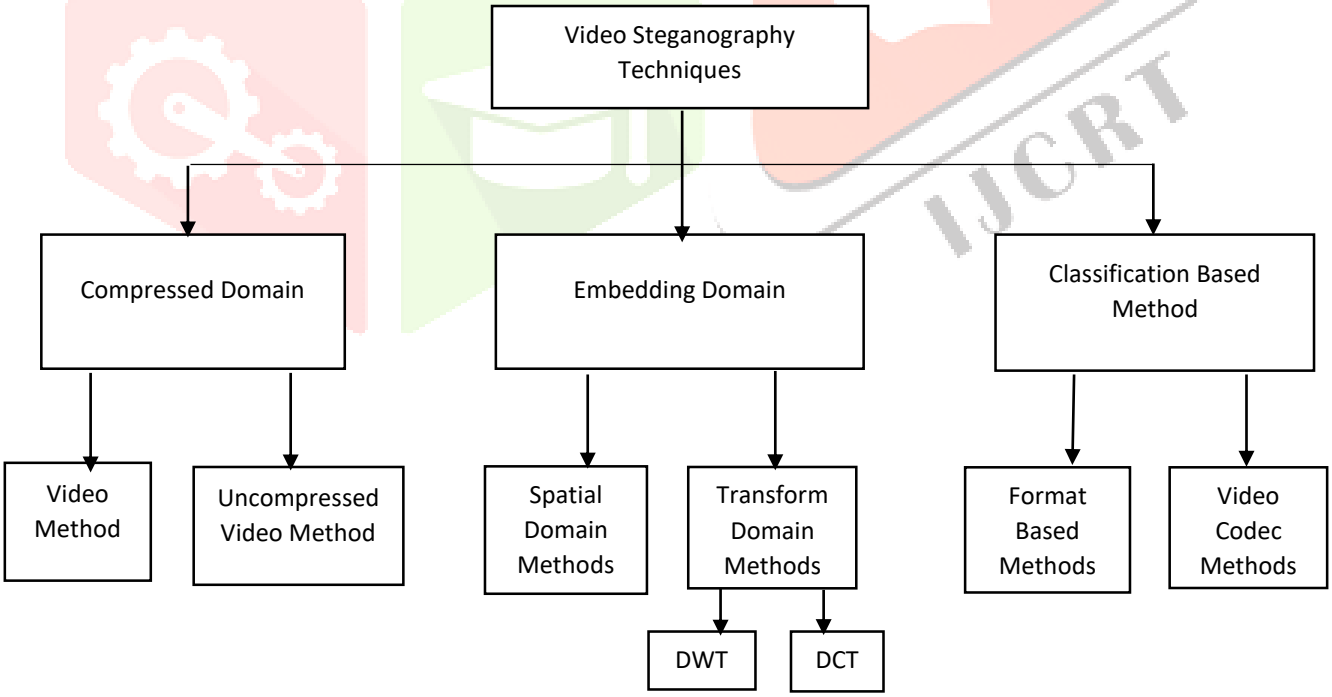

Fig 4.1 Video Steganography Techniques Classification

A. Spatial Domain Based Method

Data hiding in the spatial domain is based solely on pixel values. Least Significant Bit [21], [22], Bit-Plane Complexity Segmentation [23], and Pixel Mapping [24] are some of the spatial domain techniques.

1. Least Significant Bit (LSB)

One of the most popular data-hiding techniques is LSB. It's also a more straightforward method for transmitting data in the spatial domain in a secure manner. In safe transmission, LSB plays an important role. The least significant bit of the image is exchanged with the data bit in this technique [20].

2. Bit-Plane Complexity Segmentation (BPCS)
The sensitive data is hidden using the BPCS technique. 3-D set partitioning in hierarchical trees algorithm, Frame Selected Approach, and Modified BPCS [23] are some of the BPCS techniques used to hide data.

3. Pixel Mapping
In the spatial domain, the pixel mapping technique is used. The embedding pixels are chosen using certain mathematical functions. Until embedding, the selected pixel is checked to see if it is within the image's boundaries or not. Pixel mapping techniques for hiding data include the Integer Wavelet Transform and Embedding Plane Selection [24].

Table 1. Comparative analysis of spatial domain techniques

Technique	Description	Advantages	Disadvantages	Parameter
Non-Uniform Rectangular Partition [21]	It conceals an uncompressed hidden video stream without causing distortions in the host video stream. The partition codes are used to reconstruct the original image as closely as possible.	The video quality remains unchanged.	The error rate is higher	PSNR ranges upto 29db
Genetic Algorithm [22]	2 LSB method. The optimizer uses cost functions with two factors.	The PSNR value is high.	Generic algorithm works only in uncompressed domain	PSNR lies between 20 to 40 db
Modified BPCS [23]	Hybrid cryptography is used to encrypt the confidential information, which is then compressed. The details about the precise mapping of secret data is contained in the secret key.	Two levels of security is provided and also high embedding capacity is achieved.	The video quality is less.	PSNR is 35.4 db
Embedding Plane Selection [24]	Using some mathematical functions, the embedding bit planes are chosen, and then pixel mapping is applied.	Less time is spent on the activities and also provides good video quality.	Embedding capacity is less, Since cover image bit planes are all unsuitable for embedding.	PSNR lies between 36 to 38 db

B. Transform Domain Based Technique

Due to their high security, Transform Domain Based Techniques are thought to be less vulnerable to attacks. A digital image is a series of pixels that make up the image's high and low frequency elements. Edge pixels have a high frequency, whereas non-edge pixels have a low frequency. In video steganography, the discrete cosine transform (DCT) and discrete wavelet transform (DWT) are the two most common transform-based techniques.

1. DCT Based Techniques
The image is segmented into low, middle, and high frequency bands in DCT technique. High compression ratio and a low error rate are the advantages of this method. Bose-Chaudhuri-Hocquenghem (BCH) error-correcting codes [25], Intra-frame error propagation-free data hiding algorithm, and DCT-based perturbation programme, and secret message formulation and trailing coefficients are some of the DCT-based techniques.

2. DWT Based Techniques
Wavelet is a small wave with a time domain oscillation. DWT is a relatively new and effective method for concealing data. The DWT technique has the advantage of being able to perform both local and multi-resolution analysis. The inverse wavelet transform is used to restore the object's original format. Inverse two-dimensional DWT [26], Kanade Lucas Tomasi Tracking algorithm, Integer wavelet Transform, Arnold Transform, and Channel hiding are some of the DWT-based techniques used to hide data.

Table 2. Comparative analysis of transform domain based techniques

Technique	Description	Advantages	Disadvantages	Parameter
The BCH Error Correcting Codes [25]	BCH codes are used for encryption and encoding. The hidden message is encoded in the frame's DCT coefficient.	Provides high robustness and good hiding capacity.	Small amount of data is hidden.	PSNR ranges between 38.95 to 42.73 db
Inverse two-dimensional DWT [26]	The BCH codes are used to encrypt hidden messages. Confidential information is inserted into a DWT coefficient with a high frequency and security keys are used.	It is secure and robust.	Poor video quality.	PSNR ranges between 35.58 to 45.68 db

C. Format Based Method

For each video format, different techniques have been developed. H.264/AVC is the most recent video compression standard, with high compression efficiency and good network transmission adaptability [27]. Flash Video (.FLV) format video files are very common on the internet due to their simple structure and small size and MPEG is another video format. Some of the format-based techniques for hiding data include the Readable data hiding algorithm [28], Inter prediction scheme [29], Scene shift detection algorithm, Multivariate regression-flexible macro block ordering, Video steganography scheme, and Context adaptive variable length coding.

Table 3. Comparative analysis of format based techniques

Technique	Description	Advantages	Disadvantages	Parameter
Readable data hiding algorithm [28]	A novel readable data-hiding algorithm that embeds data into the quantized discrete cosine transform (DCT) coefficients of I frames without introducing intra-frame distortion drift into the H.264/advanced video coding (AVC) video host.	High embedding capacity. Very low visual distortions	Poor Robustness.	PSNR ranges between 38.58 to 42.9 db
Inter prediction scheme [29]	The scene change information is hidden using an encoded sequence.	Simplest method. Does not affectthe video quality.	Used only in uncompressed domain	-

Performance Metrics:

Mean Square Error (MSE) [30]: MSE is a formula that determines the sum of the squares of the errors. Mean Squared Error is the average squared difference between an initial image and the resultant (stego) image.

$$\text{MSE} = \frac{1}{H*W} \sum_{i=0}^{h} (P(i,j) - S(i.j))^2$$

Where, H and W =Height and Width

P (i, j) =Original Frame

S (i, j) =Corresponding Stego frame.

Peak Signal to Noise Ratio [30]: The PSNR is the ratio of a signal's maximum potential power to the power of corrupting noise. The logarithmic decibel scale is commonly used to express PSNR. PSNR is the most widely used metric for determining the efficiency of lossy compression reconstruction. PSNR is a measurement of reconstruction efficiency that approximates human experience. While a higher PSNR usually implies a higher-quality reconstruction, the opposite may be true in some situations. The spectrum of validity of this metric must be treated with extreme caution. It is only conclusively true when findings from the same material are compared.

PSNR is most easily defined via the mean squared error (MSE). It is expressed by,

$$\text{PSNR} = 10 \log \frac{L\text{^}2}{MSE}$$

Where, L - Maximum intensity it is taken as 255

Typical values for the PSNR is 30 to 50 dB, where higher is better.

CONCLUSION

Data Confidentiality as well as integrity has been affected by eavesdropping and unauthorized accessing of information transmitted through the internet. That arise the need for information security. So the security is getting the major attention due to the increased use of internet. To deal with this problem one of the effective solution is the Steganography. In this paper we have presented a review of some different video steganography techniques and also its strengths. The methodology, benefits, and drawbacks of various video steganography techniques are surveyed and compared.

REFERENCES

1. Bharti Chandel1, Dr.Shaily Jain, "Video Steganography: A Survey" in IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 11-17.
2. Angitha John, Anjana Baby, "A Survey on Video Steganography" in International Journal of Science and Research (IJSR) ISSN: 2319-7064, Volume 8 Issue 4, April 2019.
3. Yi-Tu.Wu, F.Y. Shih, Genetic algorithm based methodology for breaking the steganalytic systems, Systems, Man and Cybernetics, Part B: Cybernetics, IEEE Transactions on, 36(1), Feb 2006, pp.24-31, doi: 10.1109/TSMCB.2005.852474.
4. M. Kharrazi, H.T. Cover Selection for Steganographic Embedding, Image Processing, IEEE International Conference, Oct 2006, Atlanta, GA, ,doi: 10.1109/ICIP.2006.312386
5. C.Abbas, C.Joan and C.kevin, Digital Image steganography: survey and analysis of current methods, Signal Processing, 90(3), March 2010, 727752, doi:10.1016/j.sigpro.2009.08.010
6. W.Andreas, P.Andreas, Attacks on Steganographic Systems, Information Hiding, 1768, Oct 2000, pp.61-76, doi: 10.1007/10719724_5.
7. V. Sathya, K. Balasubraminvam, N. Murali, M. RajaKumaran, Vigneswari, Data Hiding in audio signal, video signal text and JPEG images, IEEE INTERNATIONAL CONFERENCE ON ADVANCES IN ENGINEERING ,SCIENCE AND MANAGEMENT(ICAESM), March 2012, pp.30-31.
8. T. Shanableh, Data Hiding in MPEG video files using multivariate regression and flexible macro block ordering, IEEE Transaction. Inf. Forensics, Security, 7(2), 2012, pp.455-464, doi: 10.1109/TIFS.2011.2177087.
9. Mansi Dave, Hinal Somani, "A Survey on Digital Video Steganography Techniques Used For Secure Transmission of Data" in IJARIIE-ISSN(O)-2395-4396 Vol-2 Issue-6 2016. F.
10. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding – a survey, Proc IEEE, 87(7), 1062-1078.
11. C. Ozdemir, O. Turan, A new steganography algorithm based on color histograms for data embedding into raw video streams, Computer & Security,28(7),October 2009,670-682.
12. S.Manish,K.Sushmita, R.Richa, Video Steganography using Pixel Intensity Value LSB Technique, International Journal on Recent and Innovation Trends in Computing and Communication,3(2),2015,287-290.
13. R.Mritha, Stego Machine- Video Steganography using Modified LSB Algorithm, World Academy of Science, Engineering and Technology,5, Feb 2011.
14. K. Naveen,B. NagKishore, M. Vasujadevi, Image Hiding in a Video-based on DWT & LSB Algorithm, International Conference on Photonics, VLSI & Signal Processing ,2014.
15. M. Ramadhan, E. Khaled, A High Payload Video Steganography Algorithm in DWT Domain Based on BCH Codes (15, 11), Wireless Telecommunications Symposium (WTS), New York, April 2015, 1-8.
16. Bin Liu, Y.Chunfang, L. Fenlin, S.Yifeng, Secure Steganography in Compressed Video Bitstreams, Availability, Reliability and Security (ARES), Barcelona, March 2008.
17. H. Frank, G. Bernd, Watermarking of uncompressed and Compressed Video, Signal Processing, 66(3), May 1998, 283-301.
18. X.Changyong, P.Xijian, A Steganographic Algorithm in Uncompressed Video Sequence Based on Difference between Adjacent Frames, Image and Graphics(ICIG), Aug.2007, 297-302.
19. M.M. Sadek, A.S. Khalifa, G. M. Mostafa, Video Steganography: A Comprehensive Review, Multimedia Tools Applications, 74, March 2014, 7063-7094.
20. S. Singh and G. Agarwal, "Hiding image to video: A new approach of LSB replacement", *International Journal of Engineering Science and Technology*, vol. 2, no.12, pp. 6999-7003, 2010.
21. S. D. Hu and U. K. Tak, "A Novel Video Steganography based on Non-uniform Rectangular Partition", IEEE international conference on computational science and engineering, pp. 57-61, Aug. 2011.
22. K. Dasgupta, J. K. Mondal and P. Dutta, "Optimized Video Steganography using Genetic Algorithm (GA)", International Conference on Computational Intelligence: Modeling, Techniques and Applications- Elsevier, vol. 10, pp. 131-137, Dec. 2013.
23. S. P. Bansod, V. M. Mane and R. Ragha, "Modified BPCS Steganography using Hybrid Cryptography for Improving Data embedding Capacity", IEEE International Conference on Communication, Information & Computing Technology (ICCICT), pp. 1- 6, Oct. 2012.
24. S. Bhattacharyya, A. Khan, A. Nandi, A. Dasmalakar, S. Roy and G. Sanyal, "Pixel Mapping Method (PMM) Based Bit Plane Complexity Segmentation (BPCS) Steganography", IEEE World Congress on Information and Communication Technologies (WICT), pp. 36 – 41, 2011.
25. R. J. Mstafa and K. M. Elleithy, "A DCT-based Robust Video Steganographic Method Using BCH Error Correcting Codes", IEEE Conference on Long Island Systems, Applications and Technology, pp. 1 -6, April 2016.
26. R. J. Mstafa and K. M. Elleithy , "A High Payload Video Steganography Algorithm in DWT Domain Based on BCH codes (15, 11)", IEEE Wireless Telecommunications Symposium (WTS), pp 1-8, April 2015.
27. S. Mansi, M.Vijay, Current status and key issues in image steganography: A survey, Computer Science Review, 13-14, Nov 2014, 95-113.
28. X. Ma, Z. Li, H. Tu, and B. Zhang, "A Data Hiding Algorithm for H.264/AVC Video Streams without Intra- Frame Distortion Drift", IEEE Transactions On Circuits And Systems For Video Technology, vol. 20, no. 10, pp. 1320 – 1330, Oct. 2010.
29. S. K. Kapotas and A. N. Skodras, "A new data hiding scheme for scene change detection in h.264 encoded video Sequences", IEEE International Conference on Multimedia and Expo, pp. 277-280, June 2008.
30. S. Suma Christal Mary M.E (Ph.D) "IMPROVED PROTECTION IN VIDEO STEGANOGRAPHY USED COMPRESSED VIDEO BITSTREAMS", International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766.