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
www.iosrjournals.org

Video Steganography: A Survey

Bharti Chandel[1], Dr.Shaily Jain[2]
[1](Computer Science, Chitkara University, India)
[2](Computer Science, Chitkara University, India)

Abstract: *Recent advances in information technology have made quick delivery and sharing of multimedia information possible. But these advances in technology are leading breaches to information security and personal information. Digital Steganography provides capability to protect private communication that has become necessity in today's Internet era. Steganography is a technique to protect and conceal multimedia information in disguised manner or we can say it is the study of invisible communication. Steganography is a mixture of compression, encryption, watermarking and cryptography. Generally sharing of information takes place in the form of text, image, audio and video. Steganography uses image, text, video and audio to disguise secret information. In this paper we have analyzed only video steganography. In video steganography secret information is enveloped inside a video to make it safe from intruders. In this paper we have critically analyzed fundamental concepts, performance metrics and security aspects of video steganography. Different methods used for protecting secret information by using a video as cover media are explored. Comparisons between different video steganography techniques are also provided. Steganalysis is also discussed in brief.*

Keywords: *Frequency Domain, Steganography, Steganalysis, Spatial Domain*

I. Introduction

Steganography is a method of sharing secret information by making it inconspicuous to non authenticated users. [1] Steganography has been originated from Greek word Steganos and graphics. Steganos means covered or hidden and graphics means writing. Greek People used steganography to convey secret message through different methods [2]. Other method to maintain security of information is Cryptography and Watermarking. Of which former is mainly used for authentication and later is used for hiding message using encryption. A comparison of cryptography, watermarking and steganography has been provided through Table 1. Steganography is mainly used in security applications like covert communication, legal fields and copyright Control.

Security systems are mainly focusing on protection of secret information by using encryption or cryptography. Cryptography [3] provides security of information by altering meaning of information through scrambling or encoding by using encryption key. No matter how shatter proofed is our encrypted message, it will always be vulnerable to attack as intruder already knows the existence of secret information. Steganography is better than cryptography as it hides the existence of secret message from intruder. Adding information to a media file by altering its contents in an imperceptible way is known as Watermarking [4]. Watermarking is used for protection of copyright material as it must be robust against any type of attack. Watermarking makes our data protected through hiding data in the form of copyright protection but steganography hides data inside a cover object. In summary we can say that steganography provides us the mixture of cryptography and watermarking by adding imperceptibility.

On the basis of type of cover object steganographic has been classified in five forms as shown in Fig 1[13].Text Steganography mainly deals with concealing Text in Text Files and in Binary Files.[14] Text can be scrambled or concealed in any way inside a video. Text steganographic has very high capacity to hide text data in Cover Text File. Digital image steganography mainly deals with concealing data inside a cover image [15]. Being very popular in current internet era Digital images are considered to be highly used cover media in steganography [16]. Digital Image can be defined as a collection of pixels. Pixels based on their intensities are selected to hide data. Video can be considered as combination of audio and collection of still images which moves in constant time sequence. Videos are getting popular as a cover object in steganography due to high embedding payload than a digital image [5] [13] and temporal features of video also provide perpetual redundancy which is not available in digital images .Due to availability of large number of frames secret data can be easily disguised inside a video. Disguising secret information in some network protocols is known as protocol steganography. Noreka et. al. [17] described steganography in application layer TCP/IP protocol. Bartosz et.al [18] had described protocol steganography using relation between two or more protocols.DNA

Criteria	Cryptography	Steganography	Watermarking
Carrier Object	Text files or image	Any media file	Digital image/Audio
Secret information	Text	Any type of file	watermark
Secret key	Necessary	Optional	optional
Visibility	YES	Never	May or may not be
Objective	Protection	Secret communication	Copyright protection
Security	High	Very High	High
Capacity	High	High	Low

Table 1.1 Comparisons between Cryptography, Steganography and Watermarking

steganography is getting popular due to high security, high embedding capacity and high embedding efficiency. Andre et.al [19] had described steganography using DNA binary strands.

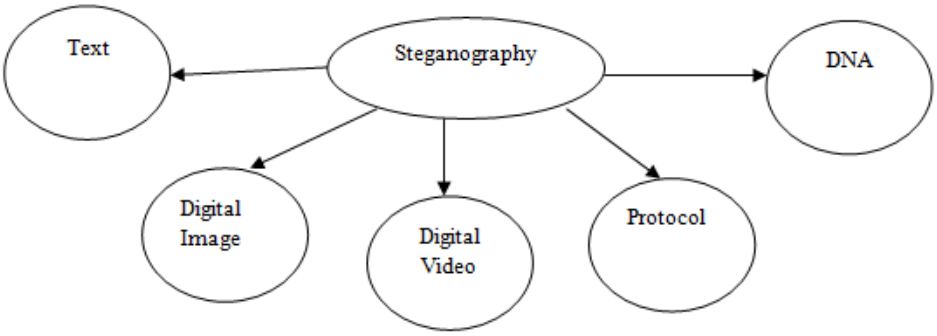

Fig 1.1 Types of Steganography

In this article Section II and Section III describes the General model of video steganography and describes the Video Steganography technique evaluation parameters, In Section III we have provided brief introduction of various video steganography techniques and Section IV provides the Literature review and Critical analysis of various techniques followed by conclusion in Section V.

II. General Model Of Video Steganography

The Video Steganography refers to using video as a cover object (carrier file) to hide some secret message inside the video file by using some embedding procedure. Video Steganography procedure can be mathematically represented as follows (Fig 1 is showing the graphical representation of video steganography procedure).

Let S_M denote the secret message to conceal inside cover video. Before applying anything on video (V) it must be divided into video frames. C_f denotes video the individual video frame. S_M will be embedded in C_f after applying Encryption algorithm (E_C).S_M can be anything like text file, video, audio or any other type of message. Three main procedures are included in this approach, namely Video file to frame conversion ($VT_{F)}$, Embedding Procedure (Em) and Extraction Procedure (Ex) [12].

VT_F: V -> C_F

E_M: C_F +E_M (E_C(S_M, E_K)) -> S_F

E_X: E_X (D_C, D_K, S_F) -> S_M

Where E_C(S_M, E_K) is S_M encryption procedure which combines with video frame to produce Stego Frame (S_F) .Further S_M is extracted from SF using Extraction Procedure as shown in Fig 1.2

III. Video Steganography Measures

A. Imperceptibility

Imperceptibility refers to the visibility of modification inside the cover media. High Imperceptibility means increasing the invisibility of slight modifications in cover object. Modern day steganalysis approaches are highly intelligent to detect slight modifications. High Imperceptibility has motivated researches to design steganalysis resistant video steganography methods [6] [7].

B. Payload

Payload or capacity refers to the amount of secret message that can be concealed inside cover media [8]. Video are gaining popularity as highly used cover media object due to their high embedding capacity and embedding efficiency.

C. Statistical Attacks

The attacks or methods applied on stego object to extract hidden or secret information are known as statistical attack [9].Steganography algorithm must be robust against statistical attacks.

D. Security

The most important feature of any steganographic algorithm is security. The embedding process should have high security with minimum vulnerability to attacks. Several approaches have been proposed to secure message in steganography [10].

E. Computational Cost

Data hiding and Data retrieval are the two parameters used to calculate computational cost of any steganography approach [11] .Data hiding time refers to the time required to embed data inside a cover video frame and data retrieval refers to extraction time of secret message from the stego frame.

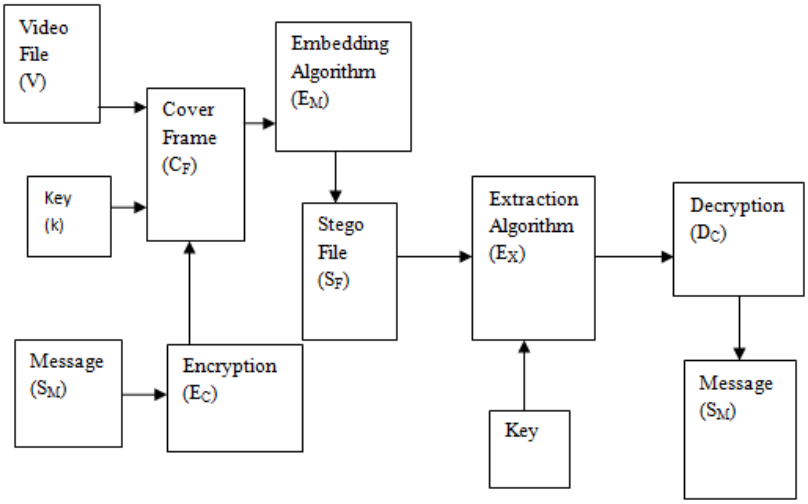

Fig 1.2 Video Steganography Diagram

F. Perceptual Quality

Increment in embedding capacity may also lead to degradation of video quality or degradation of original contents of video. Video steganography approach must handle control degradation of video quality.

IV. Video Steganography Techniques

High spatial and temporal redundancy of video streams makes them good candidate for security applications like military and intelligence communications applications [20]. Video Steganography Techniques can be classified into various techniques. One way to categorize video steganography techniques is on the basis of embedding method i.e. Spatial or Substitution based techniques[21,22,23,24] and transform based techniques[24,25]. Videos can also be classified on the basis of Compression i.e. Compressed [26] and Uncompressed Video techniques [27, 28] as shown in Fig 3.1. Another approach to classify video steganography techniques is based on classification i.e. Format based and Video Codec Methods [13].

A. Spatial Domain Based Method

Spatial Domain Methods basically deals with hiding information in pixels of video frames. The most popular method of steganography is Least Significant Bit method (LSB) [12] due to its high embedding capacity, less embedding complexity and ease in implementation .Least Significant method performs embedding of secret message in least significant or most significant bit by randomly selecting pixel from a digital image or a digital video frame .Let P[i] is representing pixel of an image. Binary form of this pixel can be
P[i] = {a_7, a6, a5, a4, a3, a2, a1, a0}

Where a_7 is most significant bit (MSB) and a_0 is least significant bit (LSB). Pixel Value Differencing (PVD) [29] is another approach of achieving spatial domain based steganography. Secret message bits are concealed in pixels by dividing them on the basis of their difference which provides better results in terms of imperceptibility and high embedding capacity.

Spatial Domain based methods are popular due to high embedding capacity but these are highly vulnerable to statistical attacks like image filters, rotation, cropping and scaling. To achieve high robustness and high security against steganalysis attacks Transform domain methods are preferred as described below.

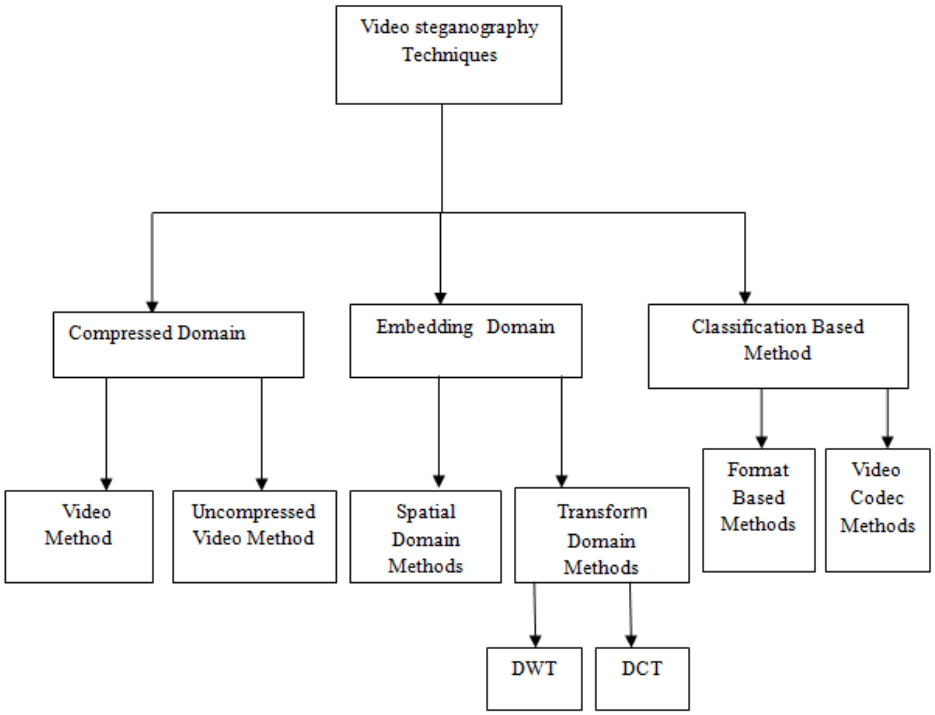

Fig 3.1 Video Steganography Techniques Classification

B. Transform Domain Based Technique

Table Transform Domain Based Techniques are considered to be less prone to attacks due to high security. Digital image is collection of pixels which are present in high and low frequency components of image. The edge pixels are high frequency pixels and non edge pixels are low frequency pixels. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are the two most popular transform based techniques in video steganography. DCT coefficients are considered as main destination of hiding in DCT transform method. Yanquing et al. [30] had achieved high security and high visual quality by using DCT coefficients based on Genetic algorithm. Difference of non-zero DCT coefficients had been chosen to achieve PSNR of 38.26 at high embedding rate with high security [31].

DWT method decompose the digital image or frame into four sub band with lower sub band having relevant information and high sub band having finer details [12].Ghasemi et al.[32] had proposed embedding in 4 X 4 block of DWT coefficients using Genetic algorithm based functions and then OPAP is applied to achieve PSNR of 35.17 db.

C. Format Based Method

Various techniques have been designed for a particular video format. H.264/AVC is latest video compression standard with high efficiency in compression and well adaptation for network transmission [12]. Due to simple structure and small size Flash Video (.FLV) format video files are considered to be very popular on internet. Mozo et al [33] has described a technique based on its simple structure to embed secret message in video tags to achieve good visual quality without any distortion.

V. Literature Survey

In 2007 Daniel Socek et.al [20] has proposed an extended version of encryption algorithm of video which is applicable on both lossy and lossless low motion video codec and extension to this encryption algorithm as a new steganography algorithm to disguise a video inside a video with high security and low computational cost. There are two main types of video encoding standards i.e. compressed and uncompressed. Bin Liu et.al [26] has proposed compressed video secure steganography algorithm to achieve high security with robustness against statistical attacks without decompression process. Run level pairs which are formed by quantization of 8X8 discrete cosine transformed (DCT) are selected as positions to embed secret bits. Video steganography is famous due to high spatial and temporal redundancy. This feature can be easily applied to

design a steganography algorithm with high security and high embedding efficiency. For example M.Jafar et.al [34] has proposed a compressed video steganography using temporal and spatial features of video signal. The proposed algorithm has constant bit rate, high imperceptibility and embedded data has been extracted without full decomposition. There are many video steganography schemes proposed on motion vectors as they are used to remove temporal redundancies in video frames. Feng Pan et. al [35] has proposed an enhanced version of motion vector based video steganography algorithm by concealing data in motion vectors of cover media. This algorithm has maintained embedding capacity of 4 bits of secret message per 6 motion vectors i.e. approximately 2/3 of total number of motion vectors and PSNR value of more than 30dB. Due to low computational complexity and high bit rate of watermark channel Least Significant bit (LSB) is high used to embed secret data in steganography algorithm. R.Mritha [23] has proposed a modified least significant algorithm for video steganography with high security.

Significant growth of video data over internet had made it a popular choice for steganography. Embedding capacity and embedding efficiency are contrary to each other. Maintaining security along with high embedding capacity in steganography is a difficult task. Ramadhan et.al [25] had proposed high payload and high secure video steganography algorithm with hiding ration of 28.12% and PSNR ranged between 35.58-45.68dBs.To achieve high security BCH(15,11) encoding and segmentation has been applied on secret message before embedding using 2D-DWT domain , two security keys have been used to provide additional security. Ramadhan et.al [43] had also proposed another technique using Wavelet Domain based on the KLT Tracking Algorithm and High security using BCH codes.KLT algorithm has been applied for the detection of facial region of interest in video frames and message has been embedded in RGB pixel values of these pixels using 2D-DWT domain method by generating four sub bands. This proposed algorithm needs some further modification for robustness against some video processing attacks and artificial attacks.

RGB pixel's intensity values can be easily used to embed information in LSB of cover video file because modifications made to these pixels are almost invisible to HVS (Human Visual System) [25].LSB substitution being the most simple and less complex method can be easily utilized to embed secret information. A.Swathi et.al [37] has proposed a method of video steganography using selection of embedding location by applying polynomial equations. Speed of data extraction and data embedding depends on the steganography algorithm. M.Ramalingam et.al [45] has proposed an enhanced version of Hidden Markov model to increase the speed of data embedding and extraction process. Hidden Markov models (HMM) are based on markov chains which are considered to be most suitable for increasing the speed of retrieval and extraction process due to no use of memory for states and independence of conditional probabilities of all states on the time in sequence. The HMM performs embedding of secret data by locating colored objects and applying some mathematical tools to model these objects in spatial domain.

Any successful steganography technique must consider some factors like imperceptibility, antisteganalysis and payload capacity but some factors contradict to each other, for example increasing payload capacity leads to distortion of imperceptibility and distortion of imperceptibility leads to vulnerability to attacks. Hence any steganography scheme can be considered as optimization problem where steganography technique hides secret message inside the cover video frame. Koushik et.al [38] had proposed an optimized technique for basic video steganography technique using genetic algorithm. Optimizer has been used to optimize a 3-3-2 LSB technique to achieve PSNR between 20 to 40dB and improved image fidelity (IF) as compared to previous existing method.

VI. Conclusion

In this paper summarization of common approaches and tools used for digital video steganography techniques has been done. A comparison between common video steganographic methods in digital video is also provided with a highlight on strength and weakness of each method in conclusion. The research of video steganography techniques can be explored in effective selection of cover media, to identify methods for embedding secret message with high imperceptibility, high embedding capacity, high embedding efficiency with optimum data hiding locations, low computational cost of data retrieval and data embedding rate, high security, different video files extension, different types of secret message like video inside video, image inside video, audio inside video and so on. Research can be also be explored in the area of embedding secret text message in different language other than English language. Further video encryption techniques can also be improvised.

References

[1] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn: Information Hiding-A Survey, Proc. IEEE, 1999.
[2] N. Provos and P. Honeyman, Hide and Seek: An introduction to steganography, IEEE Security and Privacy, 1(3), 2003, 32-44.
[3] K.G.Paterson, Cryptography from Painings: A snapshot of Current Research, Information Security Technical Report, 7(3), September 2002, 41-54.
[4] M. Bachrach, F.Y. Shih, Image Steganography and steganalysis, Wiley Interdisciplinary Reviews: Computational Statistics, 3(3), 2011, 251-259.
[5] M. Jafar, K. Morteza, An adaptive scheme for compressed video steganography using temporal and spatial features of the video signal, International Journal of Imaging System and Technology,19, December 2009,306-315.
[6] 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 2006,24-31.
[7] M. Kharrazi, H.T. Cover Selection for Steganographic Embedding, Image Processing, IEEE International Conference, Oct 2006, Atlanta, GA.
[8] C.Abbas, C.Joan and C.kevin, Digital Image steganography: survey and analysis of current methods, Signal Processing, 90(3), March 2010, 727-752.
[9] W.Andreas, P.Andreas, Attacks on Steganographic Systems, Information Hiding, 1768, Oct 2000, 61-76.
[10] 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 2012,30-31.
[11] T. Shanableh, Data Hiding in MPEG video files using multivariate regression and flexible macro block ordering, IEEE Transaction. Inf. Forensics, Security, 7(2), 2012, 455-464.
[12] S. Mansi, M.Vijay, Current status and key issues in image steganography: A survey, Computer Science Review, 13-14, Nov 2014, 95-113.
[13] M.M. Sadek, A.S. Khalifa, G. M. Mostafa, Video Steganography: A Comprehensive Review, Multimedia Tools Applications, 74, March 2014, 7063-7094.
[14] E. Satir, H. Isik, A Compression-based text steganography method, Journal of System and Software, 85(10), Oct 2012, 2385-2394.
[15] A.Cheddad, J.Condell, K.Curran, P. Mckevitt, Digital image steganography: Survey and analysis of current methods, Signal Processing, 90(3), March 2010, 727-752.
[16] I.Anastasia, T.Spyros, T.Halkidis, S.George, A novel technique for image steganography based on high payload method and edge detection, Expert System with Application, 39(14), October 2012, 11517-11524.
[17] L.Norka, P.James, Y.Payman, C.Steve, Syntax and Semantics-Preserving Application Layer Protocol Steganography, Information hiding, 3200, 2005, 164-179.
[18] J.Bartosz, M.Wojciech, S.Krzysztof, PadSteg:introducing inter-protocol steganography, Telecommunication Systems,52(2),February 2013,1101-1111.
[19] L. Andre, R.Christoph, B. Wolfgang, R. Hlimar, Cryptography with DNA binary strands, Biosystems,57(1),June 2000,13-22.
[20] F. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding – a survey, Proc IEEE, 87(7), 1062-1078.
[21] 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.
[22] 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.
[23] R.Mritha, Stego Machine- Video Steganography using Modified LSB Algorithm, World Academy of Science, Engineering and Technology,5, Feb 2011.
[24] K. Naveen,B. NagKishore, M. Vasujadevi, Image Hiding in a Video-based on DWT & LSB Algorithm, International Conference on Photonics, VLSI & Signal Processing ,2014.
[25] 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.
[26] Bin Liu, Y.Chunfang, L. Fenlin, S.Yifeng, Secure Steganography in Compressed Video Bitstreams, Availability, Reliability and Security (ARES), Barcelona, March 2008.
[27] H. Frank, G. Bernd, Watermarking of uncompressed and Compressed Video, Signal Processing, 66(3), May 1998, 283-301.
[28] 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.
[29] H.-C. Wu, N.-I. Wu, C.-S. Tsai, M.-S. Hwang, Image Steganographic scheme based on pixel-value differencing and LSB replacement methods, IEE Proceedings- Vision, Image and Signal Processing,152(5),October 2005,611-615.
[30] G. Yanqing, K.Siangwi, Y. Xingang, Secure Steganography based on binary particle swarm optimization, Journal of Electronics (China), 26(2), February 2009, 285-288.
[31] L. Chiang, L. Shiang, High-Performance JPEG steganography using complementary embedding strategy, Pattern Recognition, 41(9), September 2008, 2945-2955.
[32] E. Ghasemi, J. Shanbehzadeh, B. ZahirAzami, A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm, Communication and Signal Processing ,February 2011,pp 42-45.
[33] A.J. Mozo, M.E Obien, C. J. Rigor, D. F. Ravel , Video Steganography using Flash Video(FLV) ,Instrumentation and Measurement Technology Conference, May 2009, 822-827.
[34] M.Jafar, K.Morteza, An adaptive scheme for compressed video steganography using temporal and spatial features of the video signal, International Journal of Imaging Systems and Technology,19(4), December 2009,306-315.
[35] F.Pan, L. Xiang, X.Y. Yang, Y. Guo, Video Steganography using motion vector and linear block codes, Software Engineering and Service Sciences, Beijing, July 2010, 592-595.
[36] S. Po- Chyi, L.Ming-Tse, W. Ching-Yu, A practical design of high volume steganography in digital video files, Multimedia Tools and Applications,66(2), September 2013,247-266.
[37] A.Swathi, S.A.Kjilani, Video Steganography by LSB substitution using Different Polynomial Equations, International Journal of Computational Engineering and Research ,2(5),September 2012,1621-1623.
[38] D. Kousik, K. Jyotsna, D. Paramartha, Optimized Video Steganography using Genetic Algorithm(GA) , International Conference on Computational Engineering and Research, 2(5),September 2012,1621-1623.
[39] M. Athira, R. Reshma, S. B.Sasidhar, N.V.kalyankar, Audio-Video using Forensic Technique for Data Security, International Journal of Computer Engineering & Technology,5(12),December 2014,154-157.
[40] K.Parvathi, K.Mahesh, Various Techniques in Video Steganography- A Review, International Journal of Computer & Organization Trends, 5, February 2014.

[41] R.J.Mastafa ,Elleithy, K.M, A Highly Secure Video Steganography using Hamming Code(7,4),System, Applications and Technology Conference(LISAT),IEEE Long Island ,Farmingdale New York,2014.
[42] Ramadhan J. Mstafa ,Khaled M. Elleithy, A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes.
[43] J. U. Duncombe, Infrared navigation—Part I: An assessment of feasibility (Periodical style), IEEE Trans. Electron Devices, 11, Jan. 1959, 34-39.