iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VI **Month of publication:** June 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Different Aspects and Reviews on Steganography for Data Hiding

Sapna
Department of Electronics and Communication, JMIT Radaur,kuk university.

Abstract : Security of confidential information has always been a major issue from the past times to the present time. It has always been the interested topic for researchers to develop secure techniques to send data without revealing it to anyone other than the receiver. Therefore from time to time researchers have developed many techniques.to fulfill secure transfer of data and steganography is one of them. Steganography is the art and science of communicating in a way which hides the existence of the communication. Important information is firstly hidden in a host data, such as digital image, text, video or audio, etc, and then transmitted secretly to the receiver The main aim in steganography is to hide the very existence of the message in the cover medium. Steganography and cryptography are counter parts in digital security. The obvious advantage of steganography over cryptography is that messages do not attract attention to themselves, to messengers, or to recipients. Also, the last decade has seen an exponential growth in the use of multimedia data over the Internet.These include Digital Images, Audio and Video files. This rise of digital content on the internet has further accelerated the research effort devoted to steganography.In the current work we are going to present the different aspects and reviews on stegnography , that has been completed and studied by different authors.

Keywords: steganography,LSB.,DCT, DWT

I. INTRODUCTION

Now a day, a lot of applications are Internet-based and in some cases it is desired that the communication be made secret. There are two techniques are available to achieve this goal. One is cryptography, where the sender uses an encryption key to encrypt the message, this encrypted message is transmitted through the insecure public channel, and decryption algorithm is used to decrypt the message. The reconstruction of the original message is possible only if the receiver has the decryption key. The second method is steganography, where the secret message is inserted in another medium. Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attention.

A. General Steganography Systems

A general Steganography system is shown in Fig.1. It is assumed that the sender wishes to send via Steganographic transmission, a message to a receiver. The sender starts with a cover message, which is an input to the stegosystem, in which the embedded message will be hidden. The hidden message iscalled the embedded message. A Steganographic algorithm combines the cover massage with the embedded message, which is something to be hidden in the cover .The algorithm may, or may not, use a Steganographic key (stego key), which is additional secret data that may be needed in the hidden process. The same key (or related one) is usually needed to extract the embedded message again. The output of the Steganographic algorithm is the stego message.The cover massage and stego message must be of the same data type, but the embedded message may be of another data type. The receiver reverses the embedding process to extract the embedded message

\

Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

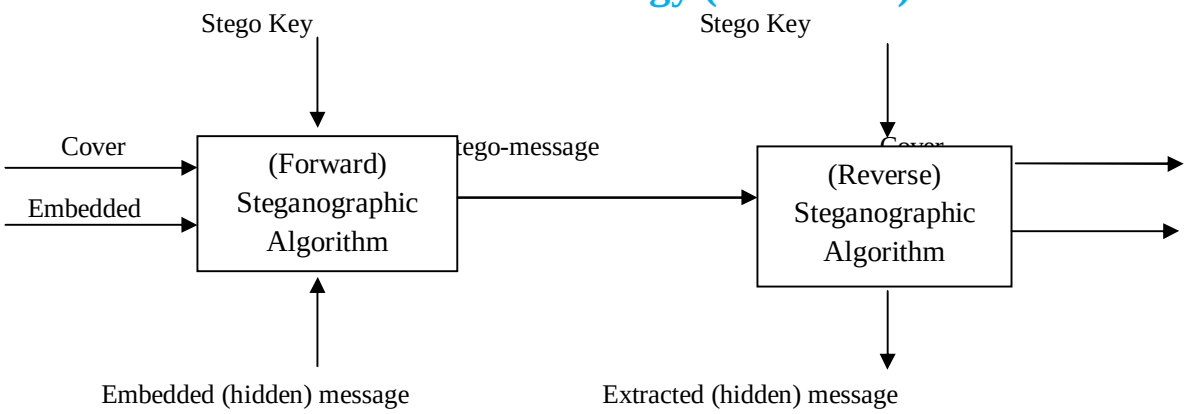


Fig. 1 General steganography system

B. Types Of Steganography

The majority of today's steganographic systems uses multimedia objects like video, image, audio etc. as cover object because people often send out digital pictures over email and other Internet communication In present approach, depending on the type of cover object, steganography can be separated into four types:

Text Steganography
Image Steganography
Audio Steganography
Video Steganography

II. RELATED WORK

C.H.Yang and C.Y. Weng(2008) have proposed a new adaptive least-significant- bit (LSB) steganographic method using pixel-value differencing (PVD) that provides a larger embedding capacity and imperceptible stego images. The method exploits the difference value of two consecutive pixels to estimate how many secret bits will be embedded into the two pixels. Pixels located in the edge areas are embedded by a k-bit LSB substitution method with a larger value of k than that of the pixels located in smooth areas. The range of difference values is adaptively divided into lower level, middle level, and higher level. For any pair of consecutive pixels, both pixels are embedded by the k-bit LSB substitution method. However, the value k is adaptive and is decided by the level which the difference value belongs to. In order to remain at the same level where the difference value of two consecutive pixels belongs, before and after embedding, a delicate readjusting phase is used. As compared to the past study of PVD and LSB the proposed approach provides both larger embedding capacity and higher image quality.

Abbas cheddad,joan condell(2008) have presented a Steganographic system which exploits the YCbCr colour space. YCbCr is intended to take advantage of human colour-response characteristics. The proposed algorithm outperforms both F5 and S-Tools. Moreover, the system demonstrates improved performance in retrieving the hidden data after applying image processing attacks in the form of additive artificial noise. As a performance measurement for image distortion Peak-Signal-to-Noise Ratio (PSNR), which is classified under the difference distortion metrics, can be applied to the Stego images. This study also shows that by adopting an object oriented Steganography mechanism, in the sense that we track skin tone objects in video frames, we get a higher PSNR value.

Ahmad T. Al-Taani. and Abdullah M.(2009) have proposed a novel Steganographic method for hiding information within the spatial domain of the gray scale image. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel. The proposed approach is tested on a database consists of 100 different images.the proposed approach hide more large information and gave a good visual quality stego-image that can be seen by human eyes,

V. Pankajakshan, G. Doerr, and P. K. Bora (2009) Motion coherency has recently been identified as a desirable property for watermarks embedded within video streams in order to withstand temporal frame averaging along the motion axis. Nevertheless, no tool has been proposed to easily evaluate the motion coherency of a given watermarking system. Today, this assessment relies on a computationally expensive procedure, namely, (1) embed a watermark, (2) perform temporal frame averaging, and (3) check for the

presence of the watermark. In this paper,author have designed a noval oracle to detect whether a video stream contains any motion-incoherent component or not. Since such incoherence can be introduced by nonmotion-coherent watermarking algorithms, this tool has proven to be most valuable to distinguish watermarked from nonwatermarked content. The oracle relies on some features extracted from error frames after motion compensation. Experimental results demonstrate the efficiency of the proposed method with uncompressed and compressed video streams.

Ozdemir Cetin, A. Turan Ozcerit (2009) Steganography, embedding secret data into unsuspected objects, has emerged as a significant sub-discipline of data-embedding methods. While mostly applied to still images in the past, it has become very popular for video streams recently. When steganographic methods are applied to digital video streams, the selection of target pixels, which are used to store the secret data, is especially crucial for an effective and successful-embedding process; if pixels are not selected carefully, undesired spatial and temporal perception problems occur in the stego-video. In this paper, two new steganographic algorithms are proposed utilizing similar histograms and dissimilar histograms. Both algorithms are based on selecting appropriate pixel approaches by focusing on perceptibility and capacity parameters of the cover video. When compared to traditional steganographic techniques, they not only result in improved temporal and spatial perception levels in the stego-video but also offer a relatively high data-embedding capacity.

Sherly A P and Amritha P P (2010), in this paper author have proposed a new compressed video Steganographic scheme. In this scheme the data is hided in compressed domain. The data are embedded in the macro blocks of I, P frames and in B frames. The novel embedding technique Triway Pixel Value Differencing (TPVD) is used to increase the capacity of the hidden secret information and for to providing an imperceptible stego-image for human vision. This algorithm can be applied on compressed videos without degradation in visual quality

P.Yang,Li-xian,Xiao-yuan (2011) have proposed a big-capacity video steganography algorithm based on motion vector phase and convolutional code to increase the capacity of secret information in video steganography. By studying the moving information of P frame and B frame in every Group of Pictures (GOP), the interlace switch was used to trade with the secret information at first, and then the different size of motion vector phase was used to represent different information to denote the basic generator matrix and the convolutional code was used to insert secret information. The experimental results show that the proposed algorithm not only has a big capacity of insert information, but also has a good imperceptibility and great robustness for secret information. It can achieve high capacity in video steganogrphy and maintain good video quality as well.

H.A.Aly (2011))In This paper author deals with data hiding in compressed video. Unlike data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain which are vulnerable to steganalysis, we target the motion vectors used to encode and reconstruct both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video. The choice of candidate subset of these motion vectors are based on their associated macroblock prediction error, which is different from the approaches based on the motion vector attributes such as the magnitude and phase angle, etc. A greedy adaptive threshold is searched for every frame to achieve robustness while maintaining a low prediction error level. The secret message bitstream is embedded in the least significant bit of both components of the candidate motion vectors. The method is implemented and tested for hiding data in natural sequences of multiple groups of pictures and the results are evaluated. The evaluation is based on two criteria: minimum distortion to the reconstructed video and minimum overhead on the compressed video size

L.narayanan ,K.Prabakaran(2012) The proposed system utilizes Integer wavelet transformation in cover image so as to get the stego-image. The capacity of the proposed algorithm is increased as the only approximation band of secret image is considered. The extraction model is actually the reverse process of the embedding model. Experimental results show that proposed method gets stego-image with high capacity and security with certain robustness. Integer wavelet transforms are used to exploit the spatial and temporal correlation in and between the video frames or minimizing the embedding distortion. Another achievement of a wavelet basis is that it supports multi resolution .

Wien Hong Tung-Shou Chen (2012) have proposed a new data-hiding method based on pixel pair matching (PPM). The basic idea of PPM is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit. Exploiting modification direction (EMD) and diamond encoding (DE) are two data-hiding methods proposed recently based on PPM. The maximum capacity of EMD is 1.161 bpp and DE extends the payload of EMD by embedding digits in a larger notational system. The proposed method offers lower distortion than DE by providing more compact neighborhood sets and allowing embedded digits in any notational system. Compared with the optimal pixel adjustment process (OPAP) method, the proposed method always has lower distortion for various payloads. Experimental results reveal that the proposed method not only provides better performance

than those of OPAP and DE, but also is secure under the detection of some well-known steganalysis techniques,

Hai-Dong Yuan(2013) have proposed multi-cover adaptive steganography problem. Two secret sharing methods for natural images based on multi-cover adaptive steganography have been proposed. The secret information is adaptively shared into textured regions of covers by a spatial ±1 operation. In comparison to previous secret sharing methods, each of the proposed methods uses a simple share-constructing operation and each has lossless secret reconstruction and high quality shares.The proposed methods are more secure in terms of resistance against state-of-the-art steganalysis techniques. In comparison to previous steganographic methods, the proposed methods hide secret bits among textured regions with different covers and are thus difficult to detect. Moreover, the proposed methods can be used to adaptively embed location-sensitive secrets (e.g., secret images) and require no stego key for extracting the encrypted message.

Sagar Gujjunoori, B.B. Amberker(2013) The author have proposed two reversible data embedding schemes which embed the data during the process ofMPEG-4compression of video. The first schem eachieves good visual quality in terms of HVS based metrics which can be useful for high fidelity watermarking applications and the second scheme achieves higher embedding capacity by maintaining better visual quality which can be useful for the steganographic applications.the proposed method achieve more embeeding capacity by maintaining the visual quality. The widely used visual quality measure PSNR is not sufficient to assess the quality of the distorted image/video content.However, the HVS based visual quality metrics very much suitable when the data is embedded in the frequency domain using DCT.the proposed scheme has higher embedding capacity and visual quality.

Kousik Dasguptaa, Jyotsna Kumar Mondalb(2013) have proposed a novel video steganography scheme for efficient and effective information hiding. In this era of Internet communication video is considered to be an effective and important tool for communication. Video steganography uses video as cover media for embedding secret data. A 3-3-2 LSB based scheme has been used as a base technique for video steganography. Imperceptibility and video quality are supposed to be two key parameters for deciding goodness of any steganographic scheme.Thus the base technique is enhanced using Genetic Algorithm (GA) which thrives to get an optimal imperceptibility of hidden data. An anti-steganalysis test is used to check for the innocence of the frame with respect to original frame. Experimental results show a substantial improvement in the Peak Signal Noise Ratio (*PSNR*) and Image Fidelity (*IF*) values after optimization over the base technique.

III.CONCLUSIONS AND FUTURE WORK

The security of data is of extreme importance in today's information-based society, including the fields of military, diplomacy, corporation, medicine, and even the individual, the information have to be safeguarded to avoid the unauthorized or illegal accesses and prevent the misuses and abuses. Any system, method or technique that deal with, processing information (data), and put this data in shapes or forms of media under the condition that it must be not visible in its new form for human observer. All such systems are called hiding systems for information. All these aspects we have covered in different reviews given by different authors, which also leads to new research on this field. In future we are going to use more advance scheme like video steganography with RC4 cryptographic algorithm for enhancing data security.

REFERENCES

[1] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, and Hung-Min Sun, “Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems”, IEEE Trans. Information Forensics and Security, vol. 3, no. 3, pp. 488-497, September 2008.

[2] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt’ Skin tone based steganography in vido files exploiting the YCBCR’ IEEE 2008.

[3] Ahmad R. Naghsh-Nilchi, , Latifeh Pourmohammadbagher’A New Approach to Steganography usingSinc-Convolution Method’International Journal of Vol:2 No: 8, 2008.

[4] Ahmad T. Al-Taani. , Abdullah M. AL-Issa. A novel steganographic method for gray-level images. International Journal of Computer, Information, and Systems Science, and Engineering, 3, 2009.

[5] V. Pankajakshan, G. Doerr, , P. K. Bora. Detection of motion-incoherent components in video streams. IEEE Transactions on Information Forensics and Security, 4:49{58, 2009.

[6] Ozdemir Cetin, A. Turan Ozcerit”A new steganography algorithm based on color histograms for data embedding into raw video streams” comp u t e r s & s e c u r i t y 2 8 (2 0 0 9) 6 7 0 – 6 8 2.

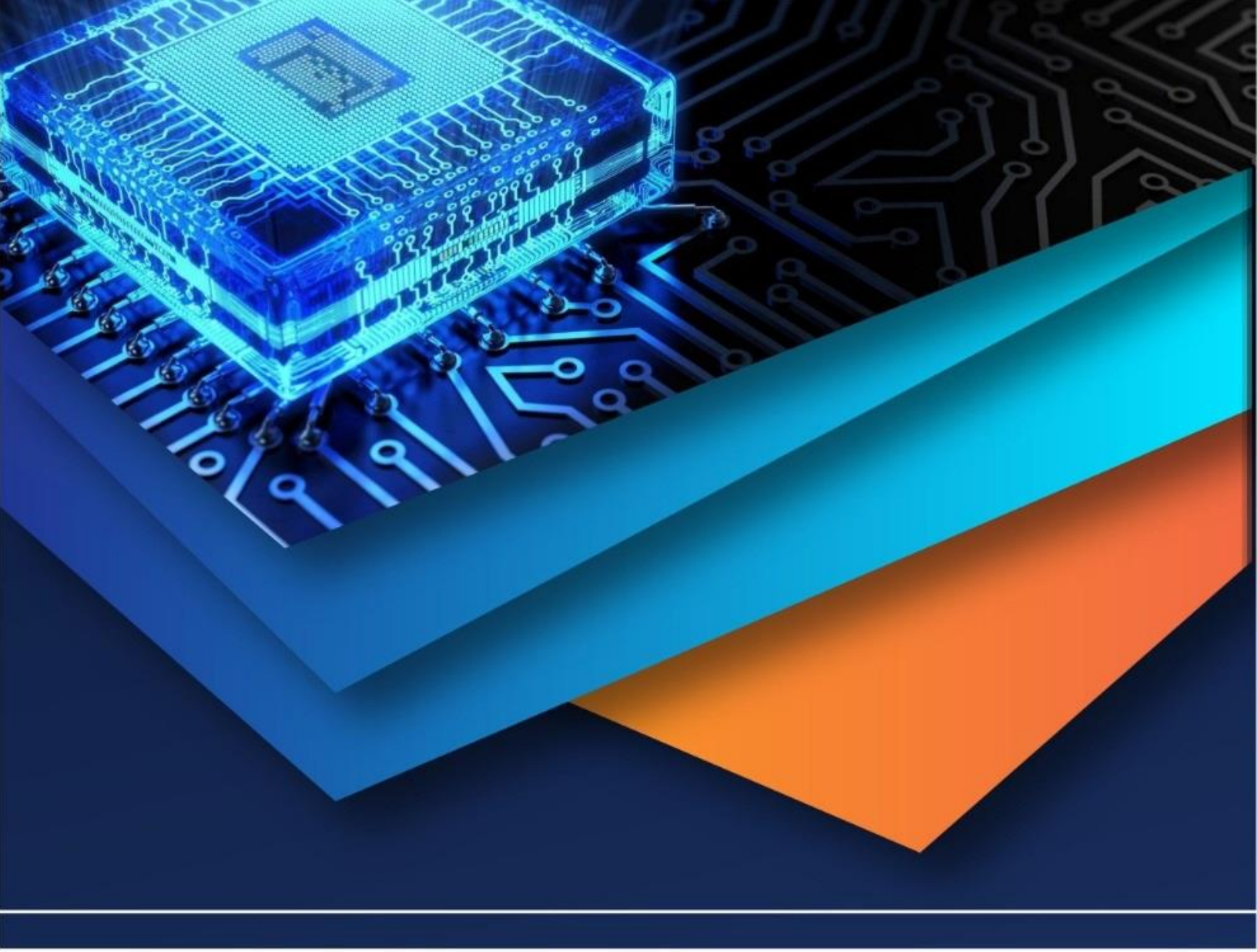
[7] Sherly A P and Amritha P P,”A Compressed Video Steganography using TPVD”, International Journal of Database Management Systems(IJDMS) Vol.2, No.3, August 2010 DOI: 10.5121/ijdms.2010.2307 67.

[8] Peng Yang,Li-xian wei,Xiao-yuan yang,”Big-capacity video steganography based on motion vector phase and convolutional code “8april 2011.

[9] H. A. Aly. Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error. Information Forensics and Security, IEEE Transactions on, 6(1):14{18, March 2011.

[10] Lakshmi narayanan ,K.Prabakaran ,G.Bhavani R, " A High Capacity Video Steganography Based on Integer Wavelet Transform", Journal of Computer Applications ISSN: 0974 – 1925, Volume-5, Issue EICA2012-4, February 10, 2012.

[11] Wien Hong , Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching." IEEE Transactions on Information Forensics And Security, Vol.7, No.1, Feb 2012, 176-184.
[12] Hai-Dong Yuan"Secret sharing with multi-cover adaptive steganography" Information Sciences 254 (2013) 197–212.
[13] Sagar Gujjunoori*, B.B. Amberker DCT based reversible data embedding for MPEG-4 video using HVS characteristics" Journal of information security and application 18 (2013),157-166.
[14] Kousik Dasguptaa,∗, Jyotsna Kumar Mondalb Paramartha Dutta," Optimized Video Steganography using Genetic Algorithm (GA)" Procedia Technology 10 (2013) 131 – 137.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY