International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 01 | Jan - 2021 ISSN: 2582-3930

Secure Text/Image Data Communication by Image Steganography into Video Sample using Wavelet Technique

Mr. Kamlesh Deshmukh[1] , Mr. Neelabh Sao[2]

1 Mr. Kamlesh Deshmukh MTechScolar, Computer Science, Rungta College of Engineering And Technology, Bhilai, CG, India

2 Mr. Neelabh Sao, Assistant Professor, Department of Computer Science Rungta College of Engineering And Technology, Bhilai, CG, India

ABSTRACT - Steganography is a method of concealing private or delicate information inside something that emits an impression of being nothing out of regular. Diverse carrier file formats can beused, for example text documents, audio tracks, digital images,and videos. But, due to immense advancement of information over the web, video steganography has turned into a very popular decision for data hiding. In video steganography, secret information is concealed inside a video to keep it safe from gatecrashers. There exists variety of techniques for hiding secret information in a video, each having their own qualities and shortcomings. This paper is an attempt to present a comprehensive study of various state-of-the-art video steganography methods in spatial domain developed in the past decade which are very beneficial for video steganography analysts to acquire better outcomes, high proficiency and security. The paper also suggests with recommendations to improve on existing video steganography techniques.

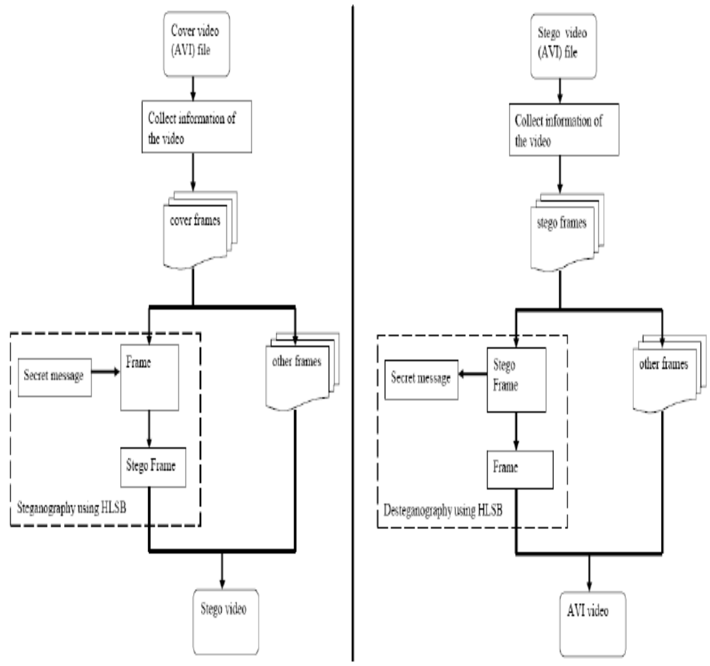
Keywords—Video Steganography; Spatial domain; Embedding;Payload; DCT; DWT; PSNR

1. INTRODUCTION

Notwithstanding the way that the Internet is used as well-known venues for users to access desired data, it has in like manner opened another passage for assailants to get valuable and intellectual information of other users with little effort.Steganography offer an assurance system that prevents meddlers from any progressing communication between an approved transmitter and its beneficiary. Steganography is the way towards hiding some profitable data inside other common information [16]. Steganography has been originated fromGreek word Steganos and graphics. Steganos implies secured or covered up and graphics implies writing. Carrier data is also referred as "cover object". Cover object can be perceived in various forms, for example, audio, text, image, and video. The data which is embedded in the cover object using an embedding algorithm is referred as "secret message". A “stego-object” is acquired by consolidating the embedded data with the cover object. Figure represents the general model of a typical steganographic method.Embedding efficiency, Payload, and Robustness arethe three noteworthy prerequisites incorporated in any fruitful steganographic technique [20,21]. Embedding efficiency relies on how exact are the stego object's qualities after the embedding, and undetectable of secret message from the stego object. In other words, the steganographic method is efficient if it incorporates encryption, indistinctness and imperceptibility qualities.

Payload or hiding capacity is the second fundamental prerequisite refers to the quantity of secret message that we can hide inside the cover object. There is an exchange-off between the hiding capacity and the embedding efficiency. On increasing the hiding capacity, the quality of stego object maybe reduced which diminishes the algorithm's efficiency. Digital watermarking is another technology that is firmly confused with steganography.

This technique utilizes a protection mechanism to shield the copyright ownership information from unauthorized users. This process is proficient by hiding the watermark information into plain carrier data.Watermarking is of two sorts: visible watermarking and invisible watermarking. In visible watermarking the watermarkinserted is visible on the media as in case of broadcaster's logoon the TV screen. In invisible watermarking the watermarkis not visible, similar is with steganography them essage embedded is invisible. Fundamental difference amongst steganography and watermarking is that inwatermarking the information about details of owner isembedded while in steganography message which can beintercepted by only sender and receiver is embedded,watermarking can be visible and invisible while steganographyis only invisible. Intruders might not be able to even intercept that this carrier contains a secret message.
Figure demonstrates the general similarities and contrastsbetween steganography, cryptography, and watermarking methods.



(a) (b)

2. LITERATURE SURVEY

Cheddad et al. [1] proposed a skin tone information hiding method which relies on upon the YCbCr color space.Different methods such as object detection and compression techniques use YCbCr. In YCbCr, the correlation between RGBcolors is segregated by isolating the luminance (denoted as Y)from the chrominance red (denoted as Cr) and the chrominance blue (denoted as Cb). In this manner, the human skin areas are perceived, the Cr of these areas are used for concealing thesecret information. In general, the method has a constrained embedding capacity because embedding of the secret message is performed just in the Cr plane of the skin area.
The determination of appropriate pixels in whichsecret message will be embedded is particularly important forviable and effective embedding.

Ozdemir Cetin, A. TuranOzcerit [2] presented two new steganographic methods utilizing similar and dissimilar histograms. Histogram rates acquiredfrom every video frame is the most essential distinction between these two data-hiding algorithms. The review has been additionally enhanced by two extra methodologies namely block-based and frame-based techniques to watch few impacts for crucial parameters like the no. of modified bits, and HDC(hidden data capacity). It can be reasoned that the frame-based techniques have outperformed the block-based techniques in similar histogram approaches; the block-based techniques deliver better outcomes over the frame-based techniques in dissimilar histogram approaches.

KousikDasgupta et al [3] designed a hash based LSB (Leastsignificant bit) technique for video steganography. In this work,eight bits of the secret information are isolated into 3,3,2 and inserted into the least significant bit of RGB pixel values of the cover frames respectively. This dissemination pattern is taken on the grounds that the chromatic impact of blue to the human eye is greater than that of red and green pixel. Thus, the video quality is not relinquished but we could increment the payload.The proposed method is contrasted with existing LSB (Leastsignificant bit) based steganography techniques and the outcomes are observed to be inspiring.

Cetin et al [4] proposed a blind data hiding method forvideo steganography based on histogram techniques to keep thedetectable quality level of secret data in the cover video at thevery least. In this work, the frames of the cover video areisolated into sub-regions and the values of the histogram ofthese are figured separately to decide the region of interest.

Sunil. K. Moon et al [5] proposed a secure method forvideo steganography based on computer forensic method. The secret message is validated and encoded using a secret key and the nembedded in the 4 least significant bit (LSB) of every pixel of the video frames. To exchange the validation key to the receiver, it is hidden into one of the frame known by both the sender and receiver. The aim of using the computer forensic method is the legitimacy of the videos obtained.

SnehaKhupse and Nitin N. Patil [6] proposed an adaptive video steganography method in which ROI in a frame is utilized instead of the entire frame. This method uses human skin tone as carry object for hiding the secret message. For skinregion detection, morphological dilation techniques and filling operation are used.

3. METHODOLOGY

This work is based on image encryption. According toan existing technique [11], which is applied on enciphering application in which image is transmitted over unsecured channels. To encrypt the image for the transmission over unsecured channels, image is divided into blocks. The image when divided into blocks, these divided blocks are rearranged to encrypt the image. The blocks are shuffled into fixed pattern and this pattern is decided by the message which used for encryption. The message is derived based on relationship between pixels of the image. The proposed algorithm can be applied in the following steps:-

Pre-processing Phase: In the pre-processing phase, the two random video frames are chosen as input images which need to encrypt and second image is the image from which key need to generate.

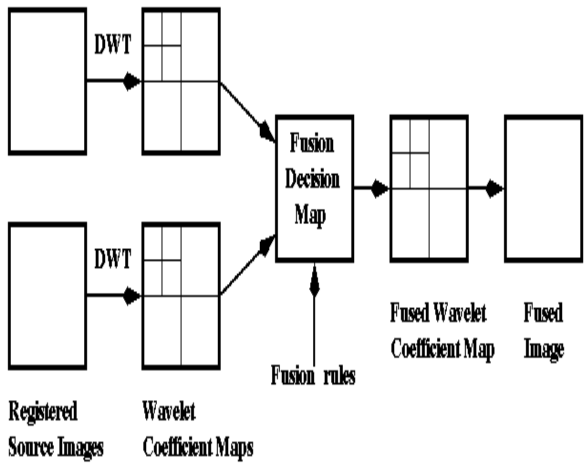
Feature extracted: In the second phase, the textual features of the first image is extracted using the wavelet transform algorithm. The wavelet transform algorithm will extract the features like energy, entropy etc. from the image.

Wavelet Transform Algorithm:

1. Count all the number of pixels in the matrix in which the data is saved.
2. Store the counted pixels in matrix P[i,j].
3. Check similarity between pixels in the matrix by applying histogram technique.
4. Calculate contrast factor from the method.
5. The elements of pixel need to be normalized by dividing the pixels.

6. Apply DCT with its level of decomposition.

7. Apply DWT1 and DWT3 with HAAR family and its level of decomposition.



4. RESULT

Initial Graphical User Interface is shown below:

Table contained different techniques, Noise, PSNR, MSE, BER and MAD:

S.No.	Applied Technique	Applied Noise	PSNR	MSE	BER	MAD
1	DCT	No	69.1385	0.954167	0.119271	0.195604
2	DCT	Gaussian	37.8466	21.808	2.72599	2.72599
3	DCT	Poisson	37.8333	21.837	2.72962	2.72962
4	DCT	Salt & Paper	37.8336	21.8364	2.72995	2.72995
5	DCT	Speckle	37.8333	21.837	2.72962	2.72962
6	DCT	High Stream	69.1385	0.954167	0.119271	0.195604
7	DCT	Low Stream	69.1385	0.954167	0.119271	0.195604
8	DCT	Frame Drop	69.1385	0.954167	0.119271	0.195604
9	DCT	Frame Trim	69.1385	0.954167	0.119271	0.195604
10	L1DWT	No	72.0153	0.715625	0.089453	0.146703
11	L1DWT	Gaussian	37.8407	21.8202	2.7276	2.7276
12	L1DWT	Poisson	37.8333	21.837	2.72962	2.72962
13	L1DWT	Salt & Paper	37.8335	21.8364	2.72955	2.72955
14	L1DWT	Speckle	37.8333	21.837	2.72962	2.72962
15	L1DWT	High Stream	72.0153	0.715625	0.089453	0.146703
16	L1DWT	Low Stream	72.0153	0.715625	0.089453	0.146703
17	L1DWT	Frame Drop	72.0153	0.715625	0.089453	0.146703
18	L1DWT	Frame Trim	72.0153	0.715625	0.089453	0.146703
19	L3DWT	No	76.07	0.477083	0.059635	0.097802
20	L3DWT	Gaussian	37.8368	21.8292	2.72865	2.72865
21	L3DWT	Poisson	37.8333	21.837	2.72962	2.72962
22	L3DWT	Salt & Paper	37.8335	21.8366	2.72957	2.72957
23	L3DWT	Speckle	37.8333	21.837	2.72962	2.72962
24	L3DWT	High Stream	76.07	0.477083	0.059635	0.097802
25	L3DWT	Low Stream	76.07	0.477083	0.059635	0.097802
26	L3DWT	Frame Drop	76.07	0.477083	0.059635	0.097802
27	L3DWT	Frame Trim	76.07	0.477083	0.059635	0.097802
28	DCT+L3DWT	No	83.0014	0.238542	0.029818	0.048901
29	DCT+L3DWT	Gaussian	37.8349	21.8335	2.72918	2.72918
30	DCT+L3DWT	Poisson	37.8333	21.837	2.72962	2.72962
31	DCT+L3DWT	Salt & Paper	37.8335	21.8366	2.72957	2.72957
32	DCT+L3DWT	Speckle	37.8333	21.837	2.72962	2.72962
33	DCT+L3DWT	High Stream	83.0014	0.238542	0.029818	0.048901
34	DCT+L3D	Low	83.00	0.2385	0.0298	0.0489

	WT	Stream	14	42	18	01
35	DCT+L3D WT	Frame Drop	83.00 14	0.2385 42	0.0298 18	0.0489 01
36	DCT+L3D WT	Frame Trim	83.00 14	0.2385 42	0.0298 18	0.0489 01

5. CONCLUSION

In this paper, we have presented a review and analysis of video steganography techniques in spatial domain. Distinction between steganography, cryptography, and watermarking were also examined. Then, video steganography techniques of spatialdomain were discussed and their performance assessments,video preprocessing, and secret messages preprocessing werespotlighted. The accompanying proposals are recommended tocome up of a proper technique for information hiding:

1. For real time security strategies, proposing a video steganography technique that keeps up an exchange off between video quality, payload, and robustness would be more suitable.
2. Proposing a steganographic method that consolidates steganography with other system protection methods such ascryptography and error correcting codes. In this way,encrypting and encoding the secret massage before embedding will give an extra security level to the secret message and robustness against attacks.
3. Proposing a video steganography method that utilizes a part of the video for embedding the secret message rather thanutilizing the whole video. Such a technique will prompt to improve the quality of stego video and enhance the resistance against attacks.

6. REFERENCES

[1] Cheddad A, Curran K, Condell J, McKevitt P, "Skin tone basedSteganography in video files exploiting the YCbCr color space", IEEEInternational Conference on Multimedia and Expo, 2008, pages 905–908

[2] A. TuranOzcerit, Ozdemir Cetin, "A new steganography algorithm basedon color histograms for data embedding into raw video streams",www.elsevier.com/locate/coseVol. 28, Issue 7, Oct. 2009

[3] J.K. Mandal, ParamarthaDutta, KousikDasgupta, "Hash Based LeastSignificant Bit Technique for Video Steganography(HLSB)",International Journal of Security, Privacy and Trust Management, Vol 1,No. 2, April'12

[4] Cetin O,Ozcerita A T, Akarb F, M Cakiroglua,Bayilmis C, "Ablindsteganography method based on histograms on video files", The ImagingScience Journal Vol. 60, issue 2, 2012

[5] Sunil. K. Moon, Rajeshree. D. Raut, "Analysis of Secured VideoMSteganography Using Computer Forensics Technique for Enhance DataSecurity", IEEE Second International Conference on Image InformationProcessing, pages 660-665, 2013

[6] S Khupse, N Patil, "An Adaptive Steganography Technique for VideosUsing Steganoflage", International Conference on Information andComputer Technologies pages 811-815, 2014

[7] PoojaShinde, TasneemBanoRehman, "A Novel Video SteganographyTechnique", International Journal of Advanced Research in ComputerScience and Software Engineering Vol. 5, issue 12, Dec. 2015

[8] Nor Ashidi Mat Isa, MrithaRamalingam, "Fast retrieval of hidden datausing enhanced hidden Markov model in video steganography",www.elsevier.com/locate/asocVol. 34, September 2015.

[9] Nishi Khan, Kanchan S. Gorde, "Video Steganography by UsingStatistical Key Frame Extraction Method and LSB Technique",International Journal of Innovative Reasearch in Science, Engineering andTechnology Volume 4, issue 10, Oct.,2015

[10] Khaled M. Elleithy,Ramadhan J. Mstafa, "A video steganographyalgorithm based on Kanade-Lucas-Tomasi tracking algorithm and errorcorrecting codes", Multimed Tools Appl, 2016

[11] KavitaKadam, Mrs. Kavitha, PriyaDunghav, AshwiniKoshti,“Steganography Using Least Significant Bit Algorithm”, InternationalJournal of Engineering Research and Applications Volume 2, Issue 3,May-Jun 2012.