NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 6, ISSUE 4, Apr.-2019

SECURING THE DATA USING VIDEO STEGANOGRAPHY

GADGOLI AMRUTA KRISHNA
Department of Electronics & Tele-communication VVPIET, Solapur, MS India
amrutakgadgoli@gmail.com

ABSTRACT

Steganography is a process of hiding important message or data inside other data to protect the important message from unauthorized users. Messages and converted data may be any type of data such as text, audio, image, and video. The main aim of steganography is to mask the hidden message and to prevent the hidden messages from being detected from unauthorized access.

In this project we proposed a frequency domain steganography technique for hiding large amount of data with high security a good invisibility and no loss of secret message. The basic idea to hide information in the frequency domain is to alter the magnitude of the entire DCT coefficient of cover image. The 2-D DCT converts the image block from spatial domain to frequency domain. The 2D-DCT of the video is taken and the secret message is embedded. The PSNR value is calculated to evaluate the quality of the video after the data hiding. The simulation results shows that the proposed algorithm is the best suited for steganography.

INTRODUCTION

The convenience of digital videos & its security plays an important role in today's communication. However each & every video communication application should give assurance about transferred video are readable only by authorized party. To avoid unauthorized attacks most applications apply steganography. It is the art and science of encodes a secret messages into an existing communication channel. The steganography protects by hiding the message into unimportant data.

There are another two technologies which are related to video steganography are related to video steganography are watermarking and fingerprinting. Watermarking is a technique in which it protects the owners property rights for media like image, music, software's by hidden watermark. Therefore the goal of steganography is secret messages while the goal of watermarking is the cover object itself. End to end authentication can be also used to keep image transfer integrity intact but end to end authentication is not possible in case of many image transfers because many server based internet services does not let a user to save contents in secure format and does not allow end to end authentication based protocol steganography is more useful for applications like copy rights, control of material, using in modern printers etc.

A steganography technique must fulfill three perspectives payload, security and constancy. Payload alludes to measure of data that can be covered up in the spread picture. Expanding payload rate is in strife with loyalty and security. The real objective of steganography procedure is to improve correspondence security by expanding implanting rate.

Pure steganography is the process of embedding the data into object without without using any private keys. Above diagram shows generalized block diagram of steganography. This type of steganography entirely depends on secrecy. It uses a cover object in which data is to be embedded, personal information to be transmitted and encryption, decryption algorithm to embed the message into image.

In video steganography Video is utilized as a spread media for implanting mystery message, where recordings can be said as an accumulation of edges and sound, either in compacted area or in uncompressed space. Video steganography is the innovation of concealing the very nearness of mystery messages by inserting these messages into innocent looking advanced video which is either crude or compacted design. Contrasted and the still pictures, the video has a considerably more limit, yet additionally has a measure of the spatial and fleeting redundancies that can likewise be utilized for implanting message. Most of the present steganography frameworks utilizes different sight and sound articles, for example, picture, sound, video and so on as spread media since individuals regularly transmit advanced pictures over email and other Internet correspondence. The objective of Steganography is to shroud the nearness of a message and to make an incognito channel. The message is covered up in another article thus the transmitted item will be indistinguishable looking to each individual's eye. Video records are commonly a gathering of pictures and sounds, so a large portion of the displayed methods on pictures and sound can be connected to video

documents as well. The extraordinary preferences of video are the extensive measure of information that can be covered up inside and the way that it is a moving stream of pictures and sounds.

ALREADY EXISTING METHODOLOGY

Video steganography schemes can be classified into two broad categories-
1) Spatial domain base 2) Transform domain based.
In spatial area based methodologies the mystery messages are installed straightforwardly. On spatial area the most widely recognized and straightforward Steganography strategy is LSB inclusion technique. In the LSB strategy the least huge bits of pixels is supplanted by the message which bits are permuted before implanting? Anyway the LSB inclusion technique is anything but difficult to be assaulted. Another steganography strategy named changed side match plot was proposed. It saves the video quality increments installing limit however isn't vigorous against assault since it is spatial area approach and no exchange is utilized. In view of the equivalent inserting limit our proposed technique improves both picture quality and security. Concealing the mystery message, picture in the spatial area can be effectively extricated by unapproved client.

PROPOSED METHODOLOGY

DCT has been used mostly for steganography purposes. These methods hide data bits in significant areas of the cover-image; a technique which makes them more robust to attacks. Generally, DCT is applied to image blocks of 8×8 pixels, and selected coefficients are used to hide data bitsIn this project we proposed a frequency domain steganography technique for hiding large amount of data with high security a good invisibility and no loss of secret message. The basic idea to hide information in the frequency domain is to alter the magnitude of the entire DCT coefficient of cover image. The 2-D DCT converts the image block from spatial domain to frequency domain.

DISCRETE COSINE TRANSFORM

Let I(x,y) denote an 8-bit grayscale cover-frame with x = 1,2,……,M_1 and y = 1,2,……,N_1. This $M_1 \times N_1$ cover-image is divided into 8 × 8 blocks and two-dimensional (2-D) DCT is performed on each of L = $M_1 \times N_1$ / 64 blocks.
Algorithm of proposed system-
Following are the algorithm steps for embedding phase-

1) Read the input video.
2) Select the video frame which will be carrier video frame.
3) Separate R frame, G frame and B frame from carrier video frame.
4) Divide the carrier video frame (R,G,B) into 8*8 non overlapping blocks.
5) Apply block DCT onto each 8*8 blocks separately.
6) Read the three different secret images to be embedded.
7) Make the secret images into binary form.
8) Embed the secret image into carrier video frame.
9) Take the IDCT of embedded video frame.
10) Now stego video frame is available, reconstruct video once again.

In above embedding phase first we read input video. The select video frame as a carrier video frame. After selecting as a carrier frame it divides into the R,G and B frame from the carrier video frame and separated from each other. After this step divided R,G,B into the 8*8 blocks separately. By dividing these R,G,B frame we have applied DCT on each 8*8 block. Next step is we have read three different secret images to be embed. Afterword converted into the binary form. After that embedded the the secret images into carrier video frame. After that we have taking IDCT of the embedded video frame. After this process got stego video frame to reconstruct video once again.
Following are the algorithm steps extracting phase

1) Take the stego video frame.
2) Separate the R frame, G frame, B frame from stego video frame.
3) Divide each stego frame (R,G,B) into 8*8 non overlapping blocks.

4) Apply block DCT on each frame separately.
5) Extract the secrete images.
6) Calculate PSNR

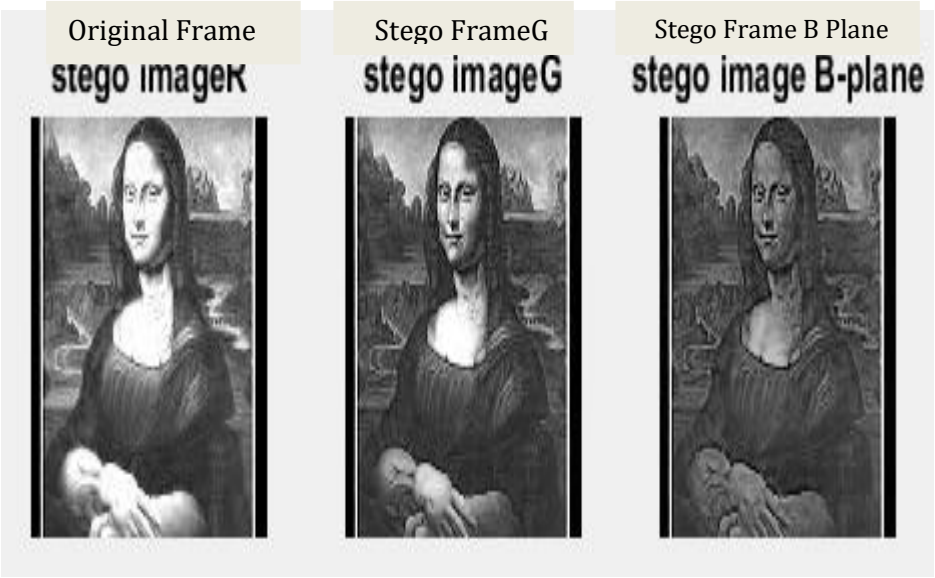
$$PSNR=10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$=20.\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$
$$=20.\log_{10}(MAX_I)-10.\log_{10}(MSE)$$

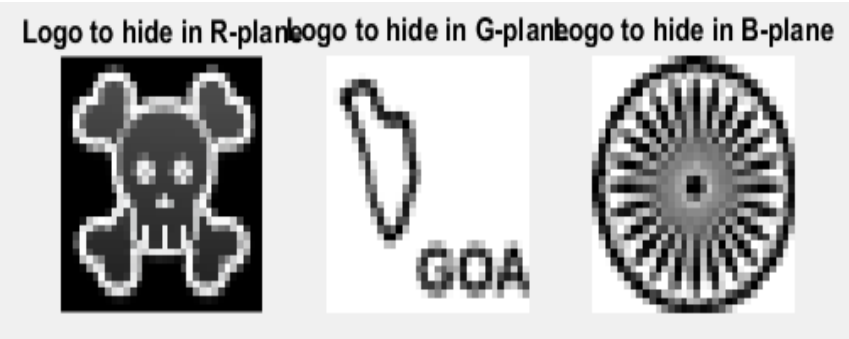
7) Calculate normalized co-relation.

$$\text{Normalized co-relation } r = ryx = \frac{C(yx)}{\sqrt{v(y)v(x)}} = \frac{\frac{1}{n}\sum_{i=1}^{n}(yi-y)(xi-x)}{\sqrt{\frac{1}{n}\sum_{i=1}^{n}(yi-y)^2 \times \frac{1}{n}\sum_{i=1}^{n}((xi-x)^2)}}$$

In above extracting phase we have taken stego video frames and separated R, G & B frame from stego video frame. Divide each stego frame R,G,B into 8*8 non overlapping blocks. And applied block DCT on each frame separately. In next step we have extracted secrete images. From this we can calculate PSNR from above formula. We also calculate the normal co-relation by the above given formula.

RESULTS

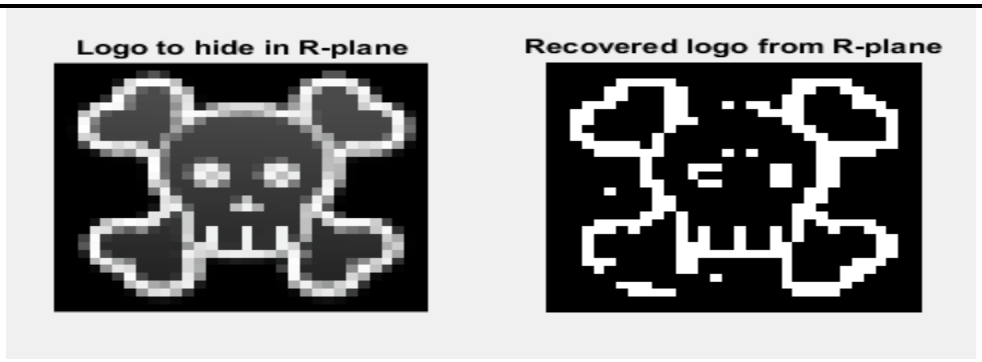


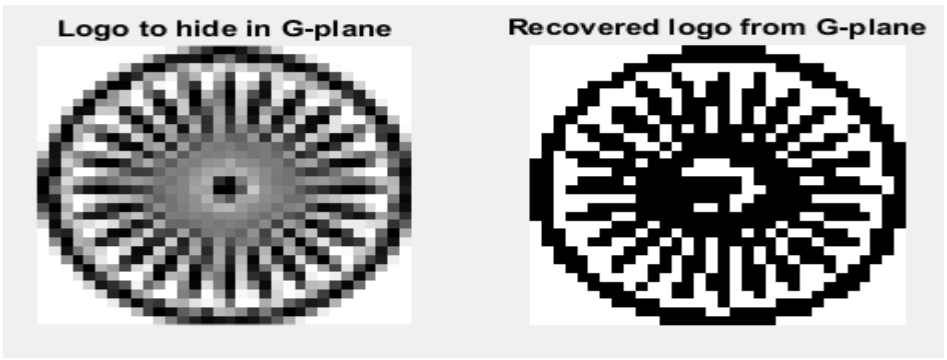


If We consider Quality Factor q = 100 then compression ratio and graph which we will obtain is shown below.

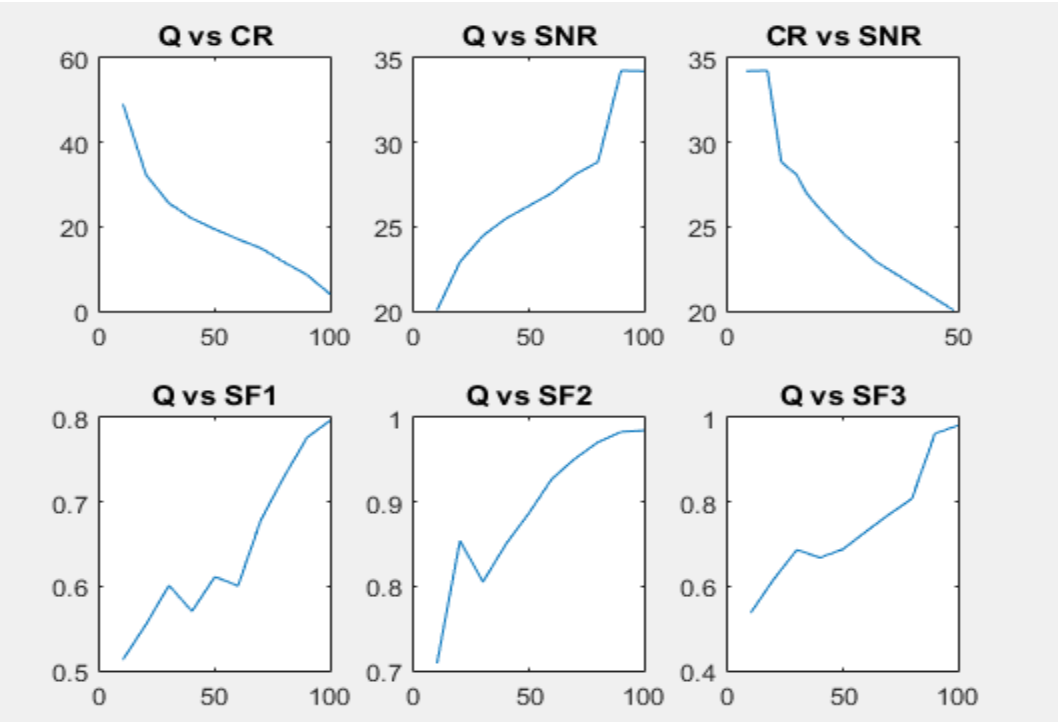
compression_Ratio = 3.9304

snr = 37.7249
sf1 =0.9530
sf2 =0.9796
sf3 = 0.9806


Logo to hide in R-plane
Recovered logo from R-plane


Logo to hide in G-plane
Recovered logo from G-plane


Logo to hide in B-plane
Recovered logo from B-plane
GOA
GOA


Q vs CR
Q vs SNR
CR vs SNR
Q vs SF1
Q vs SF2
Q vs SF3

CONCLUSION

The paper presents an overview of the proposed model. We propose a steganography process in frequency domain to improve security and image quality compared to existing. Algorithms which are normally done in spatial domain. The demand of robustness in image steanography field is not requested as strongly as it is in watermarking field. As a result, image steganography method usually neglects the basic demand of robustness. But in our project we thought a improve robustness of the proposed method, which will provide extra shield to stego video frame from stealing, destroying from unintended users etc.

REFRENCES

I. R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in DCT domain based on hamming and BCH codes," 2016 IEEE 37th Sarnoff Symposium, Newark, NJ, 2016, pp. 208-213. doi: 10.1109/SARNOF.2016.7846757

II. G. R. Rajesh and A. S. Nargunam, "Steganography algorithm based on discrete cosine transform for data embedding into raw video streams," IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2013), Chennai, 2013, pp. 554-558. doi: 10.1049/ic.2013.0370

III. R. J. Mstafa, K. M. Elleithy and E. Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," in IEEE Access, vol. 5, pp. 5354-5365, 2017. doi: 10.1109/ACCESS.2017.2691581

IV. Kaushik et al.," Analytical Study of L.S.B & D.C.T Algorithm in Audio-Video Steganography " International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 5, May – 2016, pp. 123-127

V. Mansi Dave, 2 Hinal Somani," A SURVEY ON DIGITAL VIDEO STEGANOGRAPHY TECHNIQUES USED FOR SECURE TRANSMISSION OF DATA", International Journal of Advance Research and Innovative Ideas in Education, Vol-2 Issue-6 2016

VI. M. Amiruzzaman, "Steganographic Covert Communication Channels And Their Detection," A Master thesis submitted to Kent State University, August 2011.

VII. A. Westfeld and A. Pfitzmann, Attacks on steganographic systems - breaking the steganographic utilities ezstego. In Jsteg, Steganos, and S-Tools - and Some Lessons Learned, Springer: Lecture Notes in Comput. Sci.,2000, pp. 61–75.

VIII. A. Westfeld, F5 — A steganographic algorithm, Springer: Lecture Notes in Comput. Sci., 2001, pp.289–302.

IX. J. Fridrich, M. Goljan, and D. Hogea, Steganalysis of JPEG images: Breaking the F5 algorithm, Springer: Lecture Notes in Comput. Sci., 2002, pp. 310–323.

X. M. Khodaei, K. Faez, "Image Hiding by using genetic algorithm and LSB substitution," Proc. Int. Conf. on Image and Signal Proc., Berlin, Vol. 1634, pp. 404–411, 2010.

XI. C. Chang, C. Chan, Y. Fan. "Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels," Pattern Recognition, vol. 39, pp. 1155–1167, 2006.