RESEARCH ARTICLE OPEN ACCESS

DCT Based Secret Image Hiding In Video Sequence

M. Suresh Kumar, G. Madhavi Latha
Department of Electronics & Comm Engg. Sree Vidyaniketan Engineering College. Tirupati, Andhra Pradesh, India
Department of Electronics & Comm Engg Sree Vidyaniketan Engineering College. Tirupati, Andhra Pradesh, India

Abstract
Internet which is ever more accessible to interference by not with authority people over the World. It is important to bring down a chance of Information being sensed while Transmitting is the major issue these days. To overcome these problems one of the solution is cryptography. There will be no solitude once it is decoded. So hiding data to make it confidential. Copyright is one of the ways for hiding data and it is security for digital media. Its significance and techniques used in executing hiding of data let us see in brief. The existing LSB modification technique as in this approach the bits are randomly distributes the bits of message in image so which will becomes complex for anonymous persons to extract original message information, it opens the gates for loosing important hidden information. Here hiding and extraction method is used for AVI (Audio Video Interleave). As Higher order coefficients maintains Secret message bits. The hidden information will be in the form of gray scale image pixel values. Grayscale value then converted into binary values .The resultant binary values will be assigned to the higher order coefficient values of DCT of AVI video frames. These experiments were successful. We can analyze the results using Mat lab simulation software.

Keywords: Image, Steganography, DCT, Video Data Hiding

I. INTRODUCTION

There is a need of transmitting data in securing manner as the popularity of internet and digital media going higher day by day. Even though there are numerous good techniques some of them already in practice .Without disturbing the perceptual Quality assigning the secret information within the data source are nothing but data hiding. The main intention is to hide a message in such a manner that only sender and respective recipient only having knowledge that there is an hidden message. In general, in data hiding ,actual information is converted into a relevant multimedia files such as image, video or audio which is undergoes hiding within another object So the actual information will not exists in its original format. The original message is departed from it and the recipient gets the supposed message via the network. Based on application the hiding of information varies .Sometimes it might be a company logo or else some secret message that indicates some important information. Even though there is need of higher security as internet is an open environment.

Cryptography and Information hiding are the two main methods of information security. In cryptography, it converts the data into inscrutable form [2]. This has capability to build back original data without any loss. Its main intention is to avoid unauthorized receivers from decryption. Steganography and digital watermarking are the two ways to conceal information. Steganography is the method of binding message, image or file within another message, image or file . Steganography and cryptography are alike and their main purpose is to provide the security for important information. The main variation between stenography and digital watermarking is, in stenography it will hide the information by which it shows there is no hidden information. At present word information hiding implies Stenography and digital watermarking [3]. Where as in digital watermarking it will conceals data within digital objects such as audio, video or image by which information is becomes robust for alterations and adjustments [2] [3]. Watermarking is the method in which mark itself is invisible and unnoticeable to human vision. Along with this it is impractical to remove watermark without downgrading the quality of digital object [5].

In other words stenography intended to conceal secret information within other cover media such as audio, video or image . In order to make persons insensible from the presence of information. Even though stenography is different form of cryptography but the both of them are employed to provide security to important data. In stenography carrier medium is termed as an object which carries the concealed information. Stego-object is the output of the stenography that is sent to intended destination. Now the concealed information from Stego-object can be extracted using a key called Stego-key. Data is encapsulated in different practical carriers such as audio files, document, file headers, digital images and video [1-5].

The embedded data is the message that one wishes to send secretly. It is usually hidden in an innocuous message referred to as a cover-text, or cover-image or cover-audio as appropriate, producing the stego-text or other stego-object. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data to parties who know it (or who know some derived key value). As the purpose of Steganography is having a covert communication between two parties whose existence is unknown to a possible attacker, a successful attack consists in detecting the existence of this communication [1].

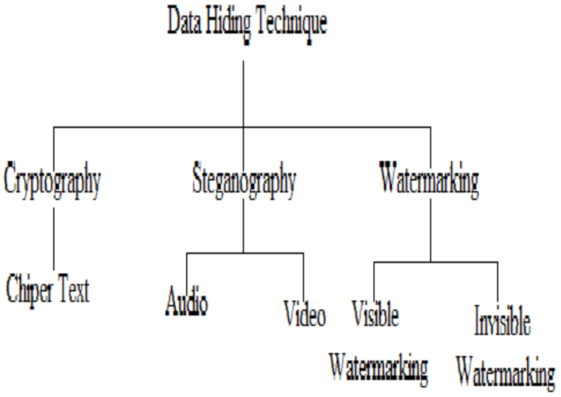

Fig1: A Technical Survey of Steganography Methods

II. PROPOSED SYSTEM

An AVI (Audio Video Interleave) is a file which consists of an array of high resolution images know as frames. All the frames can be collected in the form of bitmap images. Each and every frame contains 3 channels RGB. There after collecting frames it is possible to perform DCT (8x8 blocks) on any channel (Say R channel) of the frames. And it encloses the Secret information within selected higher order coefficients. AS Shown in Fig 6. Each Frame is handled by Inverse DCT block processing and it is merged to get AVI with hidden Image.

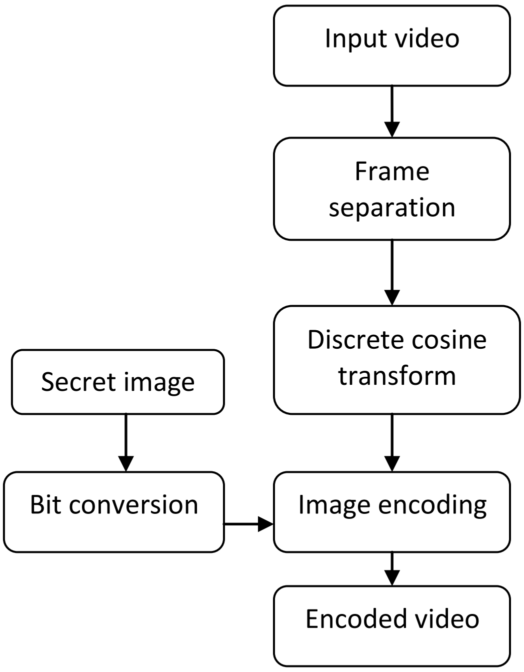

Fig:2 Data3AHiding

Let us consider input as video which in AVI format. There after extract frames from the video. Each from consists of three frames namely R, G, B-Channels. Among three channels one channel will be considered (say R-channel).consider any one of the frame among all frames. Now apply 8x8 DCT block processing to that frame. Higher order coefficients will be selected after processing 8x8 DCT block operation.

Now convert the secret image which you want to hide, into binary values. The converted binary values of the secret image will be embedded with higher order coefficients of the selected video frame using multiplier. The secret image data will be hidden among that frames. In order to get the reconstructed AVI video combine all frames together. A number of computer programs are available that will embed information in an image. Some of them just set the least significant bits of the image pixels to the bits of the embedded information. Embedded in this way may be invisible to the human eye but is trivial for an alert third party to detect and remove. Provide the high security here we can also use the secret keys system [6].

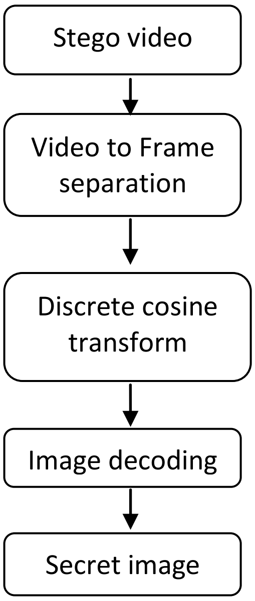

Fig: 3 Data Reconstruction

And Decryption is vice versa of Encryption as shown in fig 5. From creating each frame is extracted one by one. Implement 8x8 DCT Block Processing on Where the secret information was embedded previously (here R-channel). To obtain concealed bit information by subtracting from original DCT block Processed values. Now reconstructed AVI video consists secret image in it. The video which consists of secret image in it is called as Stego video. Now extract the frames from the reconstructed video. Each frames consists R, G, B channels .now consider any one the channel among them (here say R-channel).the secret image will be hidden among those frames. Now apply 8x8 block inverse DCT to those frames. Now separate the binary values and higher order coefficients by de-Multiplexing. Based on resultant binary values we will get back the secret image [6].

III. SYSTEM WORKING FLOW

A. Secret Message Acquisition

In this context let image be our secret message (imported from mat lab library) which is grey scale image. It is representing pixel value 8x8 of 297 x169 size images. After that the intensity of pixel values converted into equivalent binary values. As the size of car image is 297 x169 hence 297x169x8 401544 bits will be hidden in video frame.

Fig: 4 Input secret image

Shows conversion of original secret image into binary value. The intensity pixel values converted into binary value. For each 8x8 block produces 64x8 matrixes along with 1 and -1 in it .Now converting 0’s to -1 which gives binary values. Now multiply each bit with α (α=0.01).In order to reduce its strength there by the amount of distortions goes down...

B. Frame separation and hiding Secret data

In this scenario traffice.avi is considered as a cover or host video and all frames were extracted (31 frames).324x244 is the resolution of original AVI. For encoding secret message made use of R-channel. There after performing DCT on frames. But the original size is of the image is 297x169 so 297x169x8 bit should be encoded in this video frames per 8x8 DCT Higher order coefficients we can embed max of 16 bits. And in intended frame we can embed. Here we taken input AVI video pixel size is 324x244 is divided by 8x8 block size and after multiplied by 16 will get 1264896 bits. The secret image size is 297x169 x8 is divided by 1264896 and hence nearly will be getting 31 frames.

Fig: 5 Input Video Sequences

There after the frames which are extracted, each and every R-channel frame is block processed by 8x8 DCT. Now higher order DCT coefficient of each block consists of 16-bit secret message which are embedded into it.

To achieve the AVI video file along with secret message embedded in it by combining R-channels of frames after Encoding. As we can see from figure 8.It represents the frames of video frame after embedding secret message. And it clear that there is not much more distortions in the video.

The JPEG process is a widely used form of lossy image compression that centers on the Discrete Cosine Transform. The DCT works by separating images into parts of differing frequencies. During a step called quantization. Where part of compression actually occurs, the less important frequencies are discarded, hence the use of term “lossy”. Then, only the most important frequencies that remain are used retrieve the image in the decompression process. As a result, reconstructed images contain some distortion; but as we shall soon see, these levels of distortion can be adjusted during the compression stage. The JPEG method is used for both color and black and white images, but the focus of this article will be on compression of the latter.

The JPEG Process

1. The image is broken into 8x8 blocks of pixels.
2. Working from left to right, top to bottom, the DCT is applied to each block.
3. Each block is compressed trough quantization.
4. The array of compressed blocks that constitute the image is stored in a drastically reduced amount of space.
5. When desired, the image is reconstructed through decompression, a process that uses the Inverse Discrete Cosine Transform (IDCT).

Doing the DCT on An 8x8 Block

Before we begin, it should be noted that the pixel values of a black and white image range from 0 to 255 in steps of one, where pure black is represented by 0,and pure white by 255.Thus it can be seen how a photo, illustration, etc. Can be accurately represented by these 256 shades of gray.

Since an image comprises hundreds or even thousands of 8x8 of pixels, the following description of what happens to one 8x8 block is a microcosm of the JPEG process. what is done to one block of image pixels is done to all of them. Now, let’s start with a block of image pixel values. This particular block was chosen from the very upper left hand corner of an image. Because the DCT is designed to work on pixel values ranging from -128 to 127, the original block is leveled off by subtracting 128 from each entry. We are now ready to perform the Discrete Cosine Transform, which is accomplished by matrix multiplication.

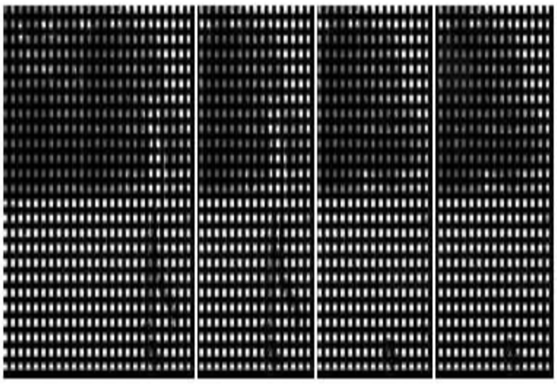

Fig: 6 DCT Transformation & Data Hided Video

C. Data Extraction from the Stego Video

1. Extraction of video frames.
2.8x8 blocks DCT processes the R-channel Frames
3. In order to get secret message the 8x8 block processed R-channel original frame values are subtracted.
4. The image will be reconstructed from the extracted secret message.

As we can see from figure 7 the construction of secret image which is embedded within the host video is reconstructed with fewer amounts of distortions.

Fig: 7 Recovered Secret Image

IV. CONCLUSION

So far we saw how can the data concealing method is applied on AVI video which is intended to insert a picture confidentially along with more perceptually lose of info to the cover media. By the making use of input video and discrete cosine transformation applying for frames and input image binary conversion then adding the image binary values to the video frames But as of now we used it is experimented for 31 frames only by embedding 297x169 image. Even though if there is much more information to hide, we can make use other channel of frame which is more capable of hiding data. Not discussed much more about robustness of a scheme here. The original signal and the quality of the video after encoding is almost similar perceptually.

REFERENCES

[1] F.A.P Peticolas, R.J. Anderson and M.G. Kuhn, “*Information Hiding – A Survey*”, in proceeding of IEEE, pp. 1062-1078, July 1999.

[2] A.A.Zaidan, B.B.Zaidan, Fazidah Othman, “*New Technique of Hidden Data in PE-File with in Unused Area One*”, International Journal of Computer and Electrical Engineering (IJCEE), Vol.1, No.5, ISSN: 1793-8198, 2009, pp 669-678.

[3] *Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standared and Distortion Techniques*”, International Journal of Computer Science

and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, 2009, P.P73-78.

[4] G. Sahoo and R. K. Tiwari, " *Designing an embedded Algorithm for Data Hiding using Steganographic Techniques by File Hybridization* International Journal of Computer Science and Network Security (IJCSNS),Vol.8,No.1,January 2008.

[5] S. Katzenbeisser, F. Petitcolas, "*Information Hiding Techniques for Steganography and digital watermarking*", 2000, pp 17-76.

[6] Saurabh Singh and Gaurav Agarwal, "*Hiding image to video: A new approach of LSB Replacement*", International Journal of Engineering Science and Technology, Vol. 2(12), pp. 6999-7003, 2010.

[7] Balaji R, Naveen G, "*Secure data transmission using video Steganography*", 2011 IEEE International Conference on Electro/Information Technology (EIT), pp. 1-5, 15-17 May 2011.

[8] Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb, "*A Secure Covert Communication Model Based On Video Steganography*", Military Communications Conference .(MILCOM), pp. 1-6, 16-19 November IEEE 2008.

[9] R.Kavitha, A. Murugan, "*Lossless Steganography on AVI File using Swapping Algorithm*", International conference on Computational Intelligence and Multimedia Applications, pp. 83-88, 2007 IEEE.

[10] AshishT.Bhole Rachna Patel, "*Design and Implementation of Steganography Over Video File*", the Indian Journal of Technical Education, Special Issue for NCEVT' 12, pp. 69-72, April 2012.

[11] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, *Attacks on copyright marking systems."* In Aucsmith [148], pp. 218{238, ISBN 3-540-65386-4.