ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 8, August 2015

A Secure Data Hiding In A Video

Dr. R. Muthammal

Associate Professor, ECE, Sriram Engineering College, Chennai, India

Abstract: This paper deals with data hiding in a carrier video. A new robust multi image digital watermarking scheme is proposed based on the frequency analysis of pixels intensity in the carrier video. The carrier video is divided into three basic color channels. Each channel is treated as a host image and broken into segments of equal sizes. A histogram is drawn for each segment in these channels formulating the number of pixels against intensity. The color characteristic in each is transformed to the corresponding blocks of each channel of the carrier video. The adopted key for embedding was by obtaining and modifying the intensity of pixels with the highest histogram in the segment. Each channel embeds one modulating image resulting into multi-watermarked image. The channels are then re-integrated back to form the watermarked image. Hence watermark bits values are distributed irregularly all over to each channels of the carrier video making it extremely difficult to be noticed or extracted unless the key is known. Therefore this method has proved to be very secured and robust against different types of noise, resizing and rotation.

Keywords: Water-marking, Histogram, Embedding, encoding and decoding

I. INTRODUCTION

Currently, images from various sources are frequently utilized and transmitted through the internet for various applications, such as online personal photograph albums, confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images usually contain private or confidential information so that they should be protected from leakage during transmission.

In existing, a new technique for secure image transmission is proposed, which transforms a secret image into a carrier video with the same size and looking like a preselected carrier video. The transformation process is controlled by a secret key, and only with the key can a person recover the secret image with minimum loss from the carrier video. Using this method the user is not allowed to select freely his/her favourite video for use as the carrier video. It is therefore desired in this study to remove this weakness of the method while keeping its merit, that is, it is aimed to design a new method that can transform a secret image into the carrier video of the same size that has the visual appearance of any freely selected carrier video without the need of the database. Hence, each channels of the freely selected carrier video is splitted into three colour characteristics (red, blue, green) and each secret image is embedded into each colour channels using watermarking technique. Watermarking is the process of embedding or hiding the digital information called watermark into the protected multimedia product such as image, audio or video. The embedded data can be detected later or extracted from the multimedia for identifying the copyright ownership.

II. IDEAS OF PROPOSED SYSTEM

The proposed method includes two main phase: watermarking image creation and secret image recovery.

Intensity histogram is commonly used technique for finding the distribution of gray levels, pixel rate within the image. Each histogram binary will represents a certain number of pixels with some intensity value. Each level will corresponds to one binary, often 256 levels histogram is used for watermarking technique.

For embedding watermarks in colour image, it makes use of intensity histogram technique. There are

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 8, August 2015

two main activities are performed one is modulation and the other is demodulation process.

First and foremost this technique will allow the three images to be embedded into single carrier video. It split the carrier video into three basic components, according to the frequency analysis of maximum amplitude occurrence evenly split the carrier video into all parts of the image. Then finally modulated image is obtained, by recombining these three watermark images shown in Fig.1. Reverse process can be done at the time of any required copyright conflicts; it is known as demodulation process.

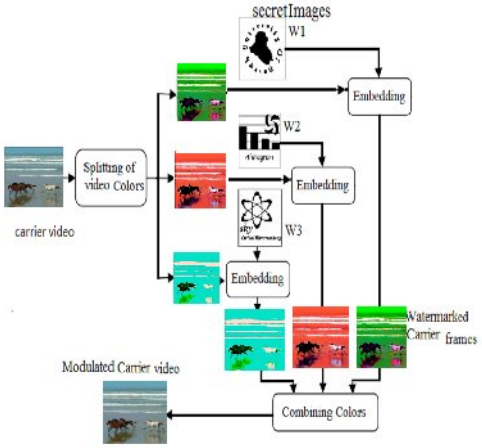


Fig.1.Block Diagram

A. Encoding technique

It is the process of putting a sequence of characters (or letters, numbers, punctuation and certain symbols) into a specialized digital format for efficient transmission or transfer. Any information which we sense and subsequently attempt to process store and later retrieve must be brought in through one of the senses and then transformed into some form that our mind understands. The process of getting into the memory for storage and later retrieval is encoding.

The encoding decoding flow is given in Fig.2. The encoding of a message is the production of message. It is a system of coded meanings in order to create that the sender needs to understand how the data is comprehensible to the members of the audience. Steps for encoding technique are as follows.

STEP 1: Read both the carrier video and the three modulating image each one of size 128x128 pixels.

STEP 2: Split the carrier video into three channels according to the original colours (red, green and blue).
STEP 3: Convert the modulating images into black and white colour space. Now it is possible to map each regional segment from the carrier video into one bit of modulating image as in the following steps.
STEP 4: Segment each channel of the carrier video into blocks of equal dimensions and draw the histogram for the number of pixels versus intensity for each block, then select the pixel with maximum frequency of occurrence (i.e. the intensity that has the maximum value of pixels). The embedding process is performed depending on the bit value of the watermark binary image, if it is 1, the intensity is increased by 1 but if it is 0 then the intensity is decreased by 1. Then resemble these new blocks into new image.
STEP 5: The above step is replaced for the three watermarks involved to be embedded into the three colour channels.
STEP 6: Integrate the resulted images of the three channels of steps 4&5 into single modulated carrier video. Save this modulated image and the resized modulating image.

B. Decoding technique

It is the conversion of a digital signal into a original sequence of character. The decoding of a message is how an audience member is able to understand and interpret the message. Decoding is the process of translating received messages into code words of a given code. There have been many common methods of mapping messages to code words. These are often used to recover messages sent over a noisy channel, such as a binary symmetric channel.

The terms encoding and decoding are often used in reference to the process of analog to digital conversion and digital to analog conversion.

For the ownership proof, the proposed technique requires both the original carrier video and the modulated video. To extract the watermarks, the steps below are followed.

STEP 1: Read the original video and the modulated video.

STEP 2: Divide the carrier video into three channels and treat each channel as a single video. Each channel is then segmented into equal blocks and find the intensity that has the maximum value of pixels in histogram for each block.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 8, August 2015

STEP 3: Divide the modulated video into three channels and treat each channel as a single video then each channel is segmented into blocks and find the intensity for each block after embedding.

STEP 4: Apply equation in order to determine pixel values of the watermark.

Pixel _ value = (-1/4*D + 1 /2)

where, D is the difference between the maximum value of the two histogram.

STEP 5: Save the extracted watermark image.

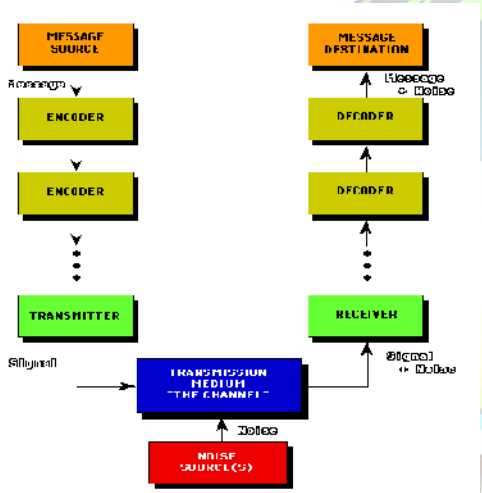


Fig.2. Encoding and Decoding process

III. Implementation And Explanation

Frames are collected in bitmap format. Each channel will have three RGB channel. After collecting the frames DCT will be performed on three channel of the frames and based on the higher order coefficient embed the secret image. Then the decoding ,which is the reverse process of encoding is done. It will perform IDCT on the three channel, where the image is embedded and the secret image is decoded from the carrier video. The different images are illustrated in Fig.3.

C. Secret image formulation

Here secret image is an image taken as a gray level image. Pixels values of first 8x8 of 128x128 size image. Thus the each pixel intensity is converted into equivalent binary values.

As if the size of the secret image is 128 x 128, we got 128x128x8=131072 bit.

a. Secret image b. Target image c. Mosaic image

Fig.3. Different Images

D. Frame extraction and embedding secret image

Here we have freely selected video has a cover video or host video. All fames are extracted (28 frames). The resolution of the original video is 128x128 pixels. The RGB channel is used for encoding secret image after performing block DCT on these frames. The size of original secret image is 128 x128. We have to encode a total 128x128 into 8 bits in the video frame.

In this we embed 16 bits per 18 to 8 DCT higher order coefficient and in a particular frame we can embed 120x160/8x8 bits.

Here 28 frames can accommodate our secret image bits. After extracting frames each RGB channel frame is block processed by 8x8 DCT and 16 image bits are embedded into higher order DC coefficient of each block. After combining all the three channels of frames we combine those to get the video AVI file with the secret image embedded. The distortion is very low in the resultant video.

E. Decoding and reconstruction of secret image .

STEP 1: First video frames are extracted .
STEP 2: RGB channel frames are proposed by 8x8 block DCT.
STEP 3: 8x8 block processed RGB channel original frame value as a packet to get secret image.
STEP 4: From the video secret image is extracted.

F. Discrete Cosine Transform

DCT is the most popular for image compression. It is a standard for jpeg which is the main reason for its popularity.DCT is used for transforming a signal from

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 8, August 2015

spatial domain to frequency domain. Hence it is used in jpeg standard. DCT encoding and decoding are depicted in Fig.4 and Fig.5.

In this paper an image is hidden into a carrier video using DCT transform. A Carrier video is a file which consists of an array of high resolution images. All the frames can be collected in the form of bitmap format. Each and every frame consists of three channels RGB. Then after collecting the frames it is possible to perform DCT on each three channel of the frames. And it encloses the secret information within selected higher order coefficients. Each frame is handled by IDCT block processing and it is merged to get modulated carrier video with hidden three secret images.

Frames are extracted from video. Now apply 8x8 DCT block processing to all frames. Higher order coefficient will be selected after processing DCT operation. Then the secret images are converted into binary values.

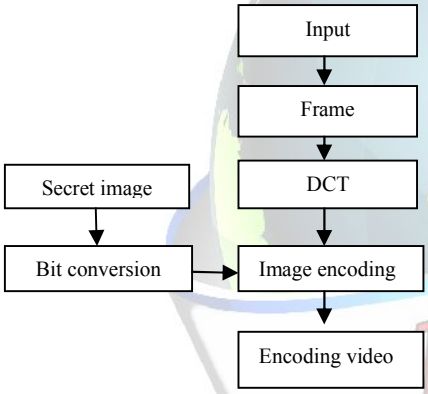
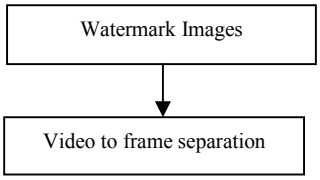


Fig.4. DCT Encoding.

The converted binary values of the secret images will be embedded with higher order coefficients of the selected video frame using multiplier. The secret image data will be hidden among these frames. In order to get the reconstructed video combine all three frames together. Some of the computer programs set the LSB of the image pixels to the bits of embedded information. Embedding may be invisible to the human eye, and we can also make use of secret key for security purpose.



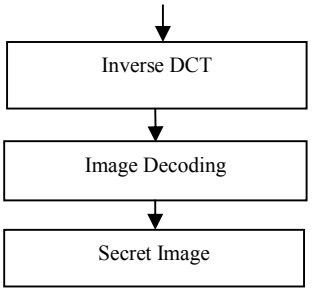


Fig.5. Reconstruction of video

Decryption is the reverse process of encryption. Initially each frame is extracted one by one and 8x8 DCT block is implemented. To obtain the bit information the values are subtracted from original DCT block. Now the video consists of secret image in it and is known as watermarked video. Extract the frames from reconstructed video. Applying inverse DCT in these frames the secret images can be obtained using the binary values.

IV. CONCLUSION

It is a secure data hiding video technique with lossless information using color characteristics. It is used for various applications like medical field, military, highly confidential areas etc..,. More information can be hidden and the quality of the video after encoding the image is almost similar as the original carrier video. Bit rate and quality of the image can be enhanced by changing the coding technique used.

REFERENCES

[1]. A.Z. Tirkel, R.G. Van Schyndel, C.F. Osborne, A digital watermark,Proceedings of ICIP 1994, Austin Convention Center, Austin, Texas, Vol. II, 1994, pp. 86–90.

[2]. W. Bender, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3/4) (1996) 313–336.

[3]. T.S. Chen, C.C. Chang, M.S. Hwang, A virtual image cryptosystem based upon vector quantization, IEEE Trans. Image Process. 7 (10) (1998) 1485–1488.

[4]. Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Hiding data in images by optimal moderately signi7cant-bit replacement, IEE Electron. Lett. 36 (25) (2000) 2069–2070.

[5]. Chi-Kwong Chan, L.M. Cheng, Improved hiding data in images by optimal moderately signi7cant-bit replacement, IEE Electron. Lett. 37 (16) (2001) 1017–1018.

[6]. Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2001) 671–683

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 8, August 2015

[7]. L.M. Marvel, C.G. Boncelet, C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process. 8 (8) (1999) 1075–1083.

The author R. Muthammal received her UG Degree in Electronics and Communication Engineering from Government college of Technology, Coimbatore and Masters Degree in Communication Engineering from IIT Madras. Now she has completed her Ph.D and she is a member of ASDF. Her current research interest includes VLSI System design and networking. She has published papers in ten international journals and twelve national journals.