Encryption of Text File in a Video Using Adaptive Compression of Video

Y. Satheesh[1], Shaik Taj Mahaoob[2]

[1] P.G Scholar, ECE, JNTUA College of Engineering, Pulivendula, A.P, India

[2]Assistant Professor, ECE, JNTUA College of Engineering, Pulivendula, A.P, India

Abstract: ***Steganography, is the art of providing security to text file by embedding into a carrier which can be a text or an multimedia file. This paper proposes a method for the real-time embedding of information in a compressed video. Unlike images Video files are generally a collection of images which can be more eligible than other multimedia files, because of its size and memory requirements. The great advantages of video files are the large amount of data that can be hidden inside and the fact that it is a moving stream of image. This paper provides a new technique that is motion vector is used to embed the data in the moving objects. We focus on the Least Significant Bit (LSB) technique is an important insertion technique for embedding data into video file and comparing the qualitative and quantitative performance of algorithms (compression).***

Keywords*:* Steganography, video processing, Motion vectors, DCT, DWT, LSB

1. Introduction

One of the reasons that intruders can be successful is that most of the information they acquire is in a form that they can read and comprehend. Hackers may reveal the information to others and modify it to misrepresent an individual or organization. One solution to this problem is the use of steganography. Steganography is a technique of hiding information in digital media. Data hiding and watermarking in digital images and raw video have wide literature. This paper targets video compression using DCT (Discrete Cosine Transform) and the DWT (Discrete Wavelet Transform) and chooses video as a carrier instead of image because of video contains amore number of frames compared to image. So text is embedded in any specified frames.

2. Literature Survey

Data hiding is the ability of embedding data into a digital cover with a minimum amount of perceivable degradation, i.e., the embedded data is invisible to a human observer. Data encryption consists of two sets of data, namely the cover medium and the embedding data, which is called the message. The cover medium may contain different types, i.e., text, audio, image and video files. This paper we target on video file as a cover medium. Here we can embedded the message bits by proper selection of motion vectors where the Motion vectors whose magnitude is above a predefined threshold, and are called candidate motion vectors (CMVs). The data bits of the message are hidden in some of the motion vectors whose magnitude is above a predefined threshold. A single bit is hidden in the least significant bit of the larger component of each CMV. The basic block diagram representation for steganography mechanism is shown in the below figure.

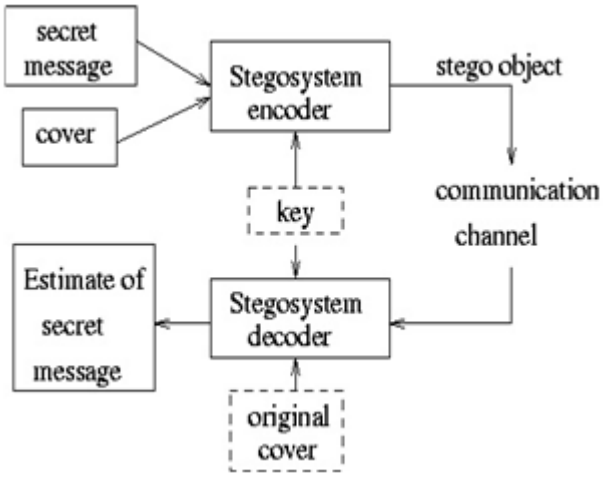

Figure 1: Steganography Mechanism

The above figure shows a simple representation of the generic embedding and extraction process in steganography. In this a message bits to be hide is being embedded inside a cover image, i.e., video file to produce the stego image. A key is often needed in the embedding process. The embedding procedure is done by using least significant algorithm by using the proper stego key and this process is done at sender side. The receiver can extract the original message bits in order to view the secret data by using the same key used by the sender.

The sender first uses the steganographic application for encrypting the text file For this encryption, the sender uses text document in which the data is written and the video as a carrier file in which the secret message or text document to be embed. The sender sends the video as a carrier file and text document to the encryption phase for data embedding, in which the text document is embedded into the video file. In encryption phase, the data is embedded into carrier file which was protected with the password. Now the carrier file acts as an input for the decryption phase. The video in which data is hidden i.e. the carrier file is sent to the receiver using a channel. E.g. Web or e-mail. The receiver receives the carrier file and places the video in the decryption phase. In the decryption phase, the original text document can be revealed

using the same password which is used at encryption time. The decryption phase decrypts the original text document using the least significant bit decoding and decrypts the original message. Before the encryption of the text, the message can be watermarked in order to avoid unauthorised modification .As mentioned in the above block diagram, the data hiding and the data extracting will be done in three phases

3. Video Processing

Video signal is used to describe any sequence of time varying images. Movies (films) and television are both examples of video signals. Digital video has become very important form of information technology and is now used in many different areas, such as broad casting, teleconferencing, mobile telephone, surveillance, and entertainment. People now expect to access a video through a wide range of different devices and over various networks. To provide these kinds of services we must know what a video compression is, for storage and transmission. But A raw video contains a large storage space so as to compress this video to reduce the requirement of bandwidth in web. "Compressed" just means that the information is packed into a smaller space.

The first step in the compression process involves converting from the RGB color space to the YCrCb color space. YCrCb describes a color space where the three components of color are luminance, red chrominance, and blue chrominance. This switch is made because the human eye is less sensitive to chrominance than it is to luminance. Chrominance data can then be sampled at a quarter the rate of luminance data.

The next step in compression involves reducing spatial redundancy. This is done using essentially the same methods as JPEG. The image is divided into 16 x 16 pixel macroblocks. Each macroblock contains 16 x 16 luminance pixels, and 8 x 8 red/blue chrominance pixels. The luminance block is then split into 4 8 x 8 blocks. Now we have 6 8 x 8 blocks on which a DCT is performed. The DCT coefficients are quantized , filtered, and then stored.

The next step in compression is intended to reduce temporal redundancy. The first step in this process is to divide a series of frames into a group of pictures (GOP) and then to classify each frame as either I, P, or B. The usual method is to break a video into GOPs of 15 frames. The first frame is always an I frame. In a 15 frame GOP, it is common to have two B frames after the I frame, followed by a P frame, followed by two B frames, etc. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are the most commonly used transformation. DCT has high energy compaction property and requires less computational resources. On the other hand, DWT is multi resolution transformation.

- DCT (Discrete Cosine Transform),
- DWT (Discrete Wavelet Transform).

3.1 DCT (Discrete Cosine Transform)

One common technique for video or image compression is discrete cosine transform (DCT). DCT is a lossy compression algorithm that samples an image at regular intervals, analyzes the frequency components present in the sample, and discards those frequencies which do not affect the image as the human eye perceives it. DCT has been one of the most popular and widely used compression methods. Although hardware implementation for the JPEG using the DCT is simple, the noticeable "blocking artifacts" across the block boundaries cannot be neglected for higher compression ratio. In addition, the quality of the reconstructed images is degraded by the "false contouring" effect for specific images having gradually shaded areas. It is inter coding compression method and it has high energy compaction property and requires less computational resources.

The N ×N DCT of a N × N image sequence {x (m, n): m=t, t + , . . . , t + N-1; n = 0,1,. . . , N-1} is defined as

$$X_c(k,l,t) = \frac{2}{N} C(k)C(l)\sum_{m=t}^{t+N-1}\sum_{n=0}^{N-1} x(m,n) \cos\frac{\pi[2(m-t)+1]k}{2N} \cos\frac{\pi(2n+1)l}{2N}$$

Where

$$C(k) = \begin{cases} \frac{1}{\sqrt{2}} & if \quad k=0 \\ 1 & otherwise \end{cases}$$

There are different steps in DCT technique to compress the image.

Step1. The image is broken into N*N blocks of pixels. Here N may be 4, 8, 16,etc.
Step2. Working from left to right, top to bottom, the DCT is applied to each block.
Step3. Each block's elements are compressed through quantization means dividing by some specific value.
Step4. The array of compressed blocks that constitute the image is stored in a drastically reduced amount of space.

So first the whole image is divided into small N*N blocks then DCT is applied on these blocks. After that for reducing the storage space DCT coefficients are quantized through dividing by some value or by quantization matrix. So that large value is become small and it need small size of space. This step is lossy step. So selection of quantization value or quantization matrix is affect the entropy and compression ratio. If we take small value for quantization then we get the better quality or less MSE(Mean Square Error) but less compression ratio. Block size value also affects quality and compression ratio. Simply the higher the block size higher the compression ratio but with loss of more information and quality.

3.2. DWT (Discrete Wavelet Transform)

Discrete Wavelet Transform (DWT) based coding, on the other hand, has been emerged as another efficient tool for image compression, mainly due to its ability to display image at different resolutions and to achieve higher compression ratio. It is requirement of large computational resources. Wavelet analysis can be used divided the information of an image into approximation and detailed sub signal. The approximation sub signal shows the general trend of pixel value, and three detailed sub signal show vertical, horizontal and diagonal details or changes in image. Discrete wavelet transforms. Wavelet analysis is computed by filter bank.

There is two type of filter

1) High pass filter: high frequency information is kept, low frequency information is lost.
2) Low pass filter: low frequency information is kept, high frequency information is lost.

Steps for compressing an image with Discrete wavelet transform is shown below.

Step1.First original image have to been passed through high pass filter and low pass filter by applying filter on each row.
Step2.now output of the both image l1 and h1 are combine into t1 = [l1 h1].
Step3. T1 is down sampled by 2.
Step4. Now, again T1 has been passed through high pass filter and low filter by applying on each Column.
Step5. Output of the step4 is supposed l2 and h2. Then l2 and h2 is combine into $t3 = \begin{bmatrix} l2 \\ h2 \end{bmatrix}$.
Step6. Now down sampled t3 by 2.

This is our compressed image. Though in DWT, we get very high compression ratio, we lose minimum amount of information. But if we do more than one level then we get more compression ratio but the reconstructed image is not identical to original image. MSE is greater if DWT apply more than one level. In nowadays, this technique is use in JPEG 2000 algorithm as one step of its.

4. Methodology and Approach

This Paper targets the First the video is divided into blocks and next the text file which is to be hidden is came in to existence therefore the text file is encoded in the least significant part of the block and is given as 16*16, 16*8, 8*8, 8*16 respectively. Therefore here in this scenario the data hiding is not a major task and also the data decoding is also not a major task but the main thing we are supposed to concentrate is on the clarity level or the mean square error (MSE) that is noise and also the loss of the data. Sometimes we may also call as a quantization errors therefore quantization is nothing but the setting the predefined values or may also be defined as the rounding off making it to the nearest value respectively. Therefore there is no problem at the time of the quantization at the encoding stage but the main challenge is at the receiver end at the time of the decoding of the data that is nothing but the dequantization of the data at the decoding stage so these comes under the quantization error. Due to this there is a lack of pixels and may lead to clarity loss etc. This paper proposes a least significant(LSB) algorithm to embed the text file in a video file.

LSB algorithm is very simple method to embed the secret data into video file. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. Embedding message is performed for two pixels *X* and *Y* of a cover image at a time and then adjusting one pixel of the (*X*, *Y*) to embed two secret bits message *s1 s2*. Embedding procedure is described as following:

Step 1. If the LSB of *X* is the same as *s1*, go to step 2.Otherwise, go to step 3.
Step 2. If the value of *f* (*X*, *Y*) is the same as *s2*, do not change any pixel. Otherwise, the value of pixel *Y* is increased or decreased by 1.
Step 3. If the value of *f* (*X* −1, *Y*) *is* the same as *s2*, the value of pixel *X* is decreased by 1. Otherwise, the value of pixel *X* is increased by 1.

4.1 Data Hiding Algorithm

Input: Video
Output: Stego video
Step 1: Read the input Video
Step 2: Perform frame separation
Step 3: Apply compression technique on each 8×8 block.
Step 4: Perform Zigzag Scanning on each 8×8 block.
Step 5: Apply Huffman coding to compress the frame.
Step 6: Apply secret key to hide the data.
Step 7: Apply LSB Algorithm to embed data
Step 8: Generate Stego video

4.2 Data Extraction Algorithm

Input: Stego video
Output: Hidden data
Step 1: Read Stego video.
Step 2: Perform decoding using inverse compression technique and Inverse Huffman coding.
Step 3: Extract hidden data using ILSB and Secret Key.

4.3 Secret Key Generation Algorithm

Step 1: Take a key which is a prime number
Step2: Generate two prime numbers p, q nearer to given key.
Step3: Calculate n=p*q;
Step 4: Calculate m= (p-1) (q-1).
Step 5: Generate e
Assume e=1; x=1;
While (mod (m , e) ==0)
e = e+1;
Step 6: Generate d
Take s=1+x*m;
While (mod (s , e) ~= 0)
x = x+1;
s=1+x*m;
d=s/e

5. Results & Discussion

Peak Signal To Noise Ratio (PSNR): PSNR is derived by setting the mean squared error (MSE) in relation to the maximum possible value of the luminance (for a typical 8-bit value this is 2^8 -1= 255) as follows:

$$psnr = 20 . \log_{10}\left(\frac{255}{\sqrt{MSE}}\right)$$

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[(f(x,y) - F(i,j)]^2}{M.N}$$

Table1: Comparison of Parameters

Parameters	DCT	DWT
Compression Ratio	42.6759	86.2516
PSNR	120.9806	112.5893
Encryption Time	7.53365	28.4701
Decryption Time	18.6799	13.7091

6. Conclusion

In the present world, the data transfers using internet is rapidly increasing because it is so easier as well as faster to transfer the data to destination. Security is an important issue while transferring the secret data using internet because any unauthorized individual can hack the data and make it useless or obtain information un- intended to him. The proposed approach in this project uses a new steganographic approach called video steganography. In this application personal data is embedded and is protected with a password which is highly secured. The proposed approach provides higher security and can protect the message from stego attacks. The compression is Classified in to two types they are lossy compression and the loss less compression respectively, here in the above algorithm or implementation of the above paper we are going for the lossy compression rather than the lossless compression.By doing experiments to compress the video we conclude that DCT , DWT both techniques have its own advantage and disadvantage. From our experiments show that DWT technique gets high compression ratio than DCT. DWT takes more time to processing than DCT. But performance time wise DCT is better than DWT.

7. Future Scope

I used the Least Significant Bit algorithm in this project for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithms. The future work on this project is to improve the compression ratio of the video to the text.. The security using Least Significant Bit Algorithm is good but we can improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption.

References

[1] Karen Lees "Image compression using Wavelets", *Report of M.S.* 2002.
[2] Andrew B. Watson, NASA Ames Research, “Image Compression Using the Discrete Cosine Transform”, Mathematica Journal, 4(1), 1994, p. 81-88.
[3] Swastik Das and Rashmi Ranjan Sethy, “A Thesis on Image Compression using Discrete Cosine Transform and Discrete Wavelet Transform”, Guided By: Prof. R. Baliarsingh, dept of Computer Science & Engineering, National Institute of Rourkela.
[4] Wong, P. and Memon, N., “Secret and public key image watermarking schemes for image authentication and ownership verification,” *IEEE Trans. Image Process.*, pp. 1593–1601, 2001.
[5] Bender, W., “Techniques for Data Hiding”, IBM Systems Journal, Vol. 35, Nos 3+4, Pgs 313-336, 1996
[6] Petitcolas, Fabien A.P., “Information Hiding: Techniques for Steganography and Digital Watermarking.”, 2000.
[7] Technique for Image Data Hiding”, Communications in Computer and Information Science, Springer, June, 2009, Vol. 29, pp. 151-159.
[8] Steganography and Steganalysis, J.R. Krenn, January 2004.
[9] Debnath Bhattacharyya, P. Das, S. Mukherjee, D. Ganguly, S.K. Bandyopadhyay, Tai-hoon Kim, “A Secured Technique for Image Data Hiding”, Communications in Computer and Information Science, Springer, June, 2009, Vol. 29, pp. 151-159.

Author Profile

Y. Satheesh is pursing M. Tech in Electronics & Communication Engineering from JNTUA College of Engineering Pulivendula. He is presently working on his project under the guidance of Assistant Professor Shaik Taj Mahaboob.

Miss Shaik Taj Mahaboob, working as Assistant Professor, Department. of ECE, JNTUA college of Engineering Pulivendula, graduated in the year 2004 with ECE specialization and completed post graduation in the year 2009 with specialization of Digital Systems and Computer Electronics and now pursuing her Ph. D in the field of Digital Image Processing. She has teaching experience of 9 years and published 3 papers in International conferences and 3 papers in national conferences. Her areas of interest are Digital Image Processing, Digital System Design, Microcontrollers and microprocessor and their applications, Embedded System design.