

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 4, Issue. 7, July 2015, pg.502 – 512

RESEARCH ARTICLE

Safe Information Hiding Using Video Steganography

D.Nithya Kalyani¹, Dr. K.Mahesh²

M.Phil Scholar¹, Professor²

Department of Computer Science and Engineering, Alagappa University, Karaikudi

Mail id: pddevanithya96@gmail.com

Abstract:

The internet plays a major role in transferring information from one person to another person. But some users can access or modify valuable information by using some other techniques. Steganography is one of the data hiding technique that hides information in any medium. For hiding important data, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) methods were used. The data gets hidden in a video file and it can be extracted in a proper way. The video file is chosen as cover medium because large volume of data can get resided inside it. The psnr value obtained in this work is good when comparing to existing system.

Keywords: *Steganography, DiscreteCosineTransform, DiscreteWaveletTransform, Least Significant Bit.*

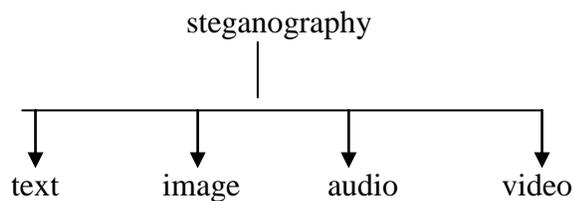
1. Introduction:

Lot of information gets exchanged through internet. The information can be sent from person to another person even in a second. Today the technology gets improved in a fast manner. When the valuable data is sent through communication channel, it can be accessed by unauthorized users. And they can modify the data. The illegal modification done by unauthorized users is termed as interception and therefore the security measures needs to get improved[15].Although many techniques are available for securing the data, information hiding technique plays an efficient

role. Information hiding means the secret information can be placed in the data source without making any changes to the quality of the medium. Information hiding technique involves imperceptibility, embedding capacity and robustness.

Information hiding technique includes cryptography, steganography and watermarking. In cryptography, the original text is converted into ciphertext which makes the person unable to detect the message. But the size of ciphertext is larger than the plaintext and it takes more time to encrypt the message. Steganography means the secret information can get hidden in some media. The media may be an image, audio or video file. Cryptography and steganography are used for security purpose, the difference between them is cryptography prevents the valuable data whereas steganography protects the cover of the message. The cover medium is referred as an object that holds the valuable information. The stego-object is the output that is sent to the destination. The key which is used to extract the hidden information from stego-object is known as stego-key [14].

Steganography is of four types: They are:



In text steganography, every n^{th} letter of a word of text message is replaced by secret data. Then in image steganography, the message gets hidden inside an image by modifying the cover source in some noisy areas. In audio steganography, the secret message is added to the audio signal that leads to changes to binary sequences of the audio file. The video steganography hides the message in a number of images which makes the person not able to detect the message. Digital watermarking is nothing but hides information in some digital objects, The digital object includes audio, video or an image file. It is not possible to remove watermark without affecting the quality of the valuable data of digital object. Imperceptibility and robustness gets improved with watermarking.[2]

2. Related work:

Majumder et al (2012) have been focused on image steganography approach. It deals with the algorithm based on hiding a large amount of data- image, audio, text file into color bitmap image. In their work it has been discussed that make use of Least Significant Bit(LSB) algorithm for embedding data into the Bitmap image. The LSB technique suggests that data can be hidden in the least significant bits of an image.[1]

BANOCI et al (2011) proposed novel steganographic method for embedding secret data in gray scale image. In their work it has been discussed that the embedding process is performed in transform domain of DWT in order to get good visual quality.[12]

Moon et al (2013) used computer forensics as a tool for providing security to the data stored in the video file. Text and image can be hid in a video file. Suitable algorithms such as 1 LSB,2LSB,4 LSB is used and 4 LSB method found to be good for hiding more secret information data.This paper deals with the idea of video steganography, cryptography and the use of computer forensics technique in both investigate and security manner.[10]

Kashyap et al (2012) have been focused on image watermarking .In their work, a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique. The watermarks generated with this algorithm are invisible, the quality of watermarked image and the recovered image are improved.[13]

Kelash et al (2013) proposed steganography algorithm based on color histograms for embed data into video clips directly, where each pixel in each video frame is divided into two parts, the number of bits which will be embedded in the right part are counted in the left part of the pixel. This proposed algorithm has the ability to hide large amount of data, extracting the written text without errors, besides it gives huge level of authentication to guarantee integrity of the frames being extracted.[11]

Kaur et al (2011) have been focused on DCT based watermarking scheme which provides higher resistance against attacks such as JPEG compression, noise, rotation, translation etc. In their paper it has been discussed that watermark is inserted by adjusting DCT coefficients of the image and by using private key. The same private key is used to extract the watermark.[9]

Hariri has been focused on audio steganography. In this paper it has been discussed about Least Significant Bit(LSB) coding, Parity Coding, Phase Coding, Spread Spectrum and Echo data hiding.[3]

Pal et al have been focused on Digital Watermarking. The aim of digital watermarking is hidden information added into multimedia content. In their paper it has been discussed that DCT technique is used and when size of image is increase then also increases PSNR without decreasing power of embedded factor in same format.[2]

Kumar et al(2014) have been focused on hiding secret image in video sequence. In their work, hiding and extraction method is used. The higher order coefficients maintains secret message bits, the hidden information will be in the form of gray scale image pixel values. The resultant binary values will be assigned to the higher order coefficient values of DCT of video frames. These experiments were successful.[14]

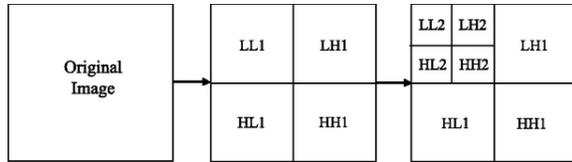
3. Least Significant Bit

Least significant bit is used for embedding secret information in a cover image. If the secret data is placed in the least significant bit of the frame , it is not easy for the human eye to detect the message.

4. Discrete Wavelet Transform

DWT is normally used for digital images. DWT is considered as better transform because it provides temporal resolution.DWT is of many types: They are haar wavelet, Daubechies wavelet, Dual-Tree wavelet, Complex wavelet, Fast haar wavelet. Many DWTs are available. For hiding text,, integer wavelet transform can be used. One of the simplest transform is haar transform. DWT is the multi resolution description of an image. DWT separates the signal into high and low frequency parts. The low frequency part is again separated into high and low frequency parts, where the high frequency part contains information about the edge components. When DWT transform is applied to an image it is decomposed into 4 sub bands: LL, HL, LH and HH. To perform a second level decomposition, again DWT needs to be applied to LL1 which decomposes the LL1 band into the 4 sub bands [15].

Haar Transform separates each signal into two components, one is called average or trend and the other one is called as difference or fluctuation.



Level 2D-DWT

The formula for the values of first average sub signal, $a = a_1, a_2, a_3, \dots, a_{n/2}$ at one level for a signal of length N i.e. $f = (f_1, f_2, \dots, f_n)$ is [15]

$$a_n = (f_{2n-1} + f_{2n}) / \sqrt{2}, n=1,2,3, \dots, N/2$$

And the first sub signal, $d^1 = d_1, d_2, d_3, \dots, d_{N/2}$, at the same signal is

$$a_n = (f_{2n-1} - f_{2n}) / \sqrt{2}, n=1,2,3, \dots, N/2$$

5. Discrete Cosine Transform

DCT are used for solving partial differential equations by using spectral methods. DCT transforms the time domain signal into its frequency components. Many frequency coefficients arise from DCT. They are single direct current DC coefficients, mid frequency coefficients, low frequency coefficients and high frequency coefficients. The middle frequency bands are chosen because it avoids the most visual important parts of the image without over exposing themselves through compression and noise attacks.

Consider a subimage $g(x,y)$ of size $n \times n$ whose discrete transform $T(u,v)$, can be expressed in terms of general relation [15]

$$T(u,v) = \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} g(x,y) r(x,y,u,v) \quad [15]$$

$$r(x,y,u,v) = s(x,y,u,v) = a(u)a(v) \cos[(2x+1)u\pi / 2n] \cos[(2y+1)v\pi / 2n]$$

similarly $T(u,v)$, $g(x,y)$ can be obtained using inverse discrete transform [15]

$$g(x,y) = \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} T(u,v) s(x,y,u,v)$$

6. Existing system:

In existing system two techniques were used to provide security to data. They are steganography and watermarking. A video is taken and it is converted into number of frames. A particular image is chosen as cover image. A password is used for security purpose. Then the secret text is loaded. Then LSB technique is used and then the dct and dwt technique is applied, then watermarked video is produced and is transmitted through the internet and the secret text can be extracted by using the same password. The psnr value obtained in their work is 52.

7. Proposed system:

The proposed hiding technique has the following steps:

Embedding process:

Step 1: The original video is taken as cover video. Then convert the original video into number of frames. Then the frames can be selected. Choose a particular image as cover image. Totally the video file consists of 92 frames. We can hide data in any number of frames.

Step 2: A secret key is used for encoding secret text.

Step 3: A. In existing system a single text is taken as secret data and loaded into video file.

B. But in this work the secret data taken is the text file (40 KB). Every character in the text file is converted into its respective ASCII value. Then the ASCII values are converted into binary values and those binary values are loaded into the video file.

Step 4: Then the LSB technique is applied

A. In existing work, the LSB bit image pixel is replaced by binary data.

B. But in proposed work, the binary values of secret data are added to the least significant bit of the frames without altering any values inside an image.

Step 5: The combined DWT & DCT technique is then applied to stego image

Step 6: Then, the video gets transmitted through the internet.

Extracting process:

Step 1: Load the stego video.

Step 2: Use the same secret key to get the secret message.

Step 3: The inverse DWT and inverse DCT technique is applied to get the stego image.

Step 4: Then, apply the LSB technique on the stego image.

Step 5: Get the secret message and original video.

Here the input of frame is given as 7. Therefore the secret text can be hided in seven frames. The encoding and decoding time, message similarity and psnr value is shown below.

| Frames | Encoding time | Decoding time |
|--------|---------------|---------------|
| Frame1 | 1.299s | 0.534s |
| Frame2 | 1.043s | 0.738s |
| Frame3 | 1.045s | 0.539s |
| Frame4 | 1.043s | 0.546s |
| Frame5 | 1.043s | 0.550s |
| Frame6 | 1.060s | 0.506s |
| Frame7 | 1.061s | 0.526s |

| frames | psnr | Message similarity |
|--------|-------|--------------------|
| Frame1 | 29.55 | ~64.22 |
| Frame2 | 29.55 | ~45.72 |
| Frame3 | 29.80 | ~29.78 |
| Frame4 | 29.71 | ~15.11 |
| Frame5 | 29.67 | ~12.22 |
| Frame6 | 29.64 | ~15.72 |
| Frame7 | 29.57 | ~15.28 |

The psnr stands for peak signal to noise ratio. It is the difference between the original and the stego video. The formula used to calculate the psnr is:

$$\text{PSNR} = 20 * \log_{10} \left(\frac{255}{\sqrt{\text{mean}_2((a-b)^2)}} \right)$$

Likewise the data can be hidden upto 92 frames.

8. Conclusion:

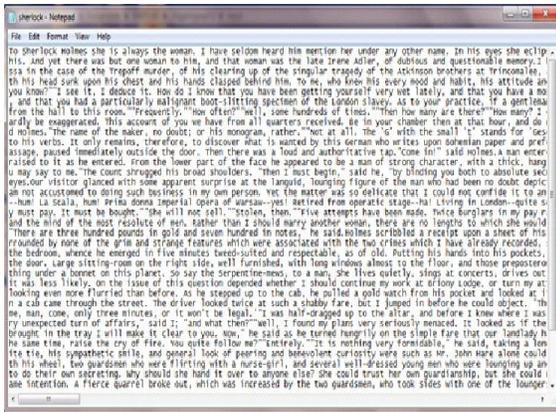
Advantages of proposed work:

Improvement in the encoding time and decoding time consumption. The psnr value obtained in proposed work is 29. This is far better than the existing work. In existing work, the psnr value obtained is 52. The difference between the original and the stego video is much better. The message similarity is also found to be good. The quality of video is also good.

Results:



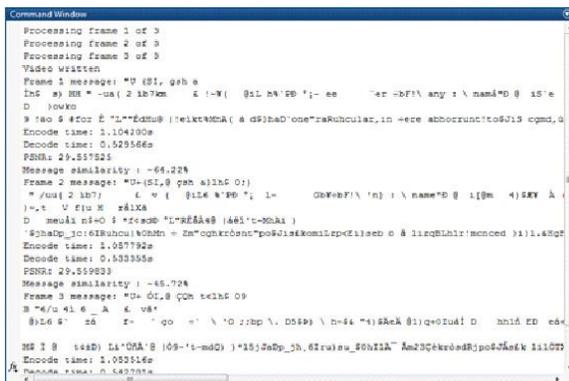
Original video



Secret text file



Stego video



Output window

REFERENCES

1. Majumder J, Mangal S, 2012, 'An Overview of image steganography using LSB Technique', IJCA.
2. Pal U, Chandra D, 2012, 'Survey Of Digital Watermarking Using DCT', IJCSE Volume 4.
3. Hariri MNRKM , 2012, 'Audio Steganography: A Survey on Recent Approaches' , World Applied Programming, Vol (2), No (3).
4. Karim S.M.M, Rahman M.D.S, Hossain M.D.S , 2011, 'A New Approach for LSB Based Image Steganography using Secret Key', IEEE.
5. Bhardwaj A, Ali R ,2009 , 'Image compression Using Modified Fast Haar Wavelet Transform', World Applied sciences Journal 7(5).
6. Paul R.T, 2011, 'Review of Robust video watermarking Techniques', IJCA.
7. Chandra M, Pandel S, Chaudhar R , 2010, 'Digital Watermarking Technique for Protecting Digital Images' , IEEE.
8. Anju R, Vandana , 2013, ' Modified algorithm for Digital Image Watermarking Using Combined DCT and DWT ',IJICT, Volume 3, no 7.
9. Kaur B, Kaur A, Singh J, 2011,'Steganographic approach for hiding image in dct domain', IJAET, Vol 1, Issue 3.
10. Moon S.K, Raut R.d, 2013,'Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security', IEEE.
11. Kelash H.M, Abdel wahab O.F, Elshakankiry ,Etsayed H.S, 2013, 'Hiding Data in Video Sequences Using Steganography Algorithms' IEEE.
12. BANOCI V, BUGAR G, LEVICKY Dusan, 2011, 'A Novel Method of Image Steganography in DWT Domain' IEEE.
13. Kashyap N, Sinha G.R, 2012,'Image Watermarking using 3-level Discrete Wavelet Transform (DWT)' IJMECS.
14. Kumar S, Latha M, 2014, "DCT Based Secret Image Hiding in video sequence" IJERA
15. Khosla S, Kaur P, 2014, "Secure Data Hiding Technique using Video Steganography and Watermarking" IJCA.
16. Poonam V, 2012, :Improved protection in video steganography using DCT & LSB".

17. Kaur M, Kaur² A, 2014, “Improved security mechanism of text in video by using steganographic technique: A Review” IJARCSSE.
18. Shraddha K, Varsha R, Mayuri S, 2014, “Secure Video Data Hiding” IJARCSSE.