Applied GIS

ISSN: 1832-5505
Vol-4 Issue-03 july 2016

A Review of DCT and LSB for Video Steganography

Shri Mata Vaishno, Kakryal, Katra, Jammu and Kashmir, India Jasiya Fayaz1, Sanjay Sharma2,
Devi University School of Computer Science and Engineering, Shri Mata Vaishno

***Abstract*—** Steganography is an effective method for concealing information in the form of text, images, sounds, or videos without compromising the integrity of the original material. A secure and reliable transmission of information from one medium to another may be obtained utilizing steganography and cryptography. Latterly video steganography has become a handy approach for delivering a big volume of data to be sent discreetly. Video steganography has been greatly influenced by the prevalence of video transmission on social networking sites like Facebook, YouTube, and many more. Given that video is essentially a compilation of still pictures, it offers additional opportunities to conceal sensitive data. Many steganographic methods have been invented, all of them produce statistically detectable changes in the characteristics of cover medium. Video steganography approaches might vary depending on factors like the compression algorithm used, the nature of the message to be encoded, the availability of cover files, and so on. The strength of a stenographic method lies in its ability to maintain the confidentiality of the sent message and the size of the data to be concealed. Despite the fact that several methods for video steganography currently exist, researchers are still exploring this area. In this study, we provide a comprehensive overview of the existing approaches and techniques in this field..

***Keywords*—** Data concealing, LSB, DCT, Steganography, and Cryptography**.**

INTRODUCTION

The term "steganography" is derived from the Greek for "covered writing," steganos, and "writing," graphia. Steganography refers to the practice of secretly concealing information inside a carrier file (text, image, audio, video) without altering the file's outward appearance[1]. The most common use of steganography is the hiding of data inside another file. Data is often not kept in its original format when steganography is used. Steganography and cryptography are both vital tools for protecting sensitive data. In steganography, only the sender and the recipient have access to the hidden information. Data concealment techniques are what cryptography is all about, making it another useful security tool[2]. The only people who know this algorithm are the sender and the recipient. Both approaches have a same goal, which is accomplished in distinct ways. Steganography is a method that may be used to four different media types: text, audio, images, and videos. The hidden information in text steganography might take the form of text, audio, images, or videos[3]. picture steganography involves the use of picture files to conceal other types of data (such text, audio, or video). To hide a video message. Using different techniques, we can conceal music, text, images (binary, grayscale, and colored), and more inside videos. The encoded or concealed data is revealed to the recipient through a secret key. Data may be concealed in either a single video frame or over many frames. It can be done in an almost infinite variety of ways. Due to the extensive availability of the internet, people from all over the globe are now able to instantly share and receive information. While there are benefits to this approach, there are also drawbacks to consider. Since the internet is available to anyone, the data may be accessed by anybody. Numerous individuals actively seek out targets on the internet in an effort to steal sensitive information, and they are often successful. So internet is a terrific site for interchange of secret information but also highly unsafe area for transferring the sensitive data. In this case, steganography is a workable solution[4].

Steganography entails concealing sensitive data inside a host file in a manner that renders it undetectable to the human eye. This technology is used to battle the insecurity of the data being sent across the internet. Any steganographic system's two most crucial factors are its embedding capacity and the embedding payload[4].

1.STEGANALYSIS

Steganalysis is the method of observing confidential data inside some media (image, text, audio, or video) using steganography. This is analogous to cryptanalysis which is a method used in cryptography. The idea behind steganalysis is to extract hidden message inside any media. Steganography is a practical method for communication. One can send its secret or confidential data using steganography. Steganography is used in comparison to cryptography as it changes the arrangement of data but it is an invisible (secret data remains hidden) technique[5].

Applied GIS

ISSN: 1832-5505
Vol-4 Issue-03 july 2016

TYPES OF STEGANOGRAPHY

• Image steganography: In image steganography secret data is hidden inside image. This secret data can be text, image or audio. The output of this steganography is stego image which is send to the receiver through transmission channel.

• Text steganography: Text steganography is a method of concealing confidential data inside text. When communication takes place, sender sends encrypted text to the receiver through secure communication channel. Any unauthorized user observes this text but they are not able to see the hidden text. At the receiver end, receiver encrypts this stego text using secret key. There are various techniques behind this method like a) linguistic method; b) random and statistical generation;
c) format based method.

- Audio steganography: Audio steganography engage with hiding confidential message in audio signals. It works by negligibly altering the binary sequence and hiding the confidentialdata.
- Video steganography: this technique deals with concealing any type of data into digital video format. Video (a set of moving frames) is selected as a host medium and in one of the frames secret message is embedded. We can select any frame for embedding depending on the technique used. Video steganography uses some of the video formats like AVI,MPEG etc.[6],[7].

TECHNIQUES USED IN VIDEO STEGANOGRAPHY

There are number of techniques used in video steganography. The best among them is where quality of video is not eliminated.

In video steganography two techniques are mostly used which are more secure and vigorous. These are:

A. Spatial Domain Technique

In special domain method of video steganography confidential message is hidden in pixel values which means it is pixel based steganography technique. The secret message which we want to embed in inserted in the pixel values of carrier video based on some techniques or methods. Least Significant Bit (LSB) is the most favoured steganography technique based on spatial domain. LSB is easy in implementation, has high embedding capacity and has lowest embedding complexity. Using LSB as base technique, only LSB plane of the frame will be affected[8].so, the advantage of using LSB is that there is no intuitive difference between the original frame and the stego frame[9].

For example (applying 3-3-2 LSB)

We have a 24-bit RGB pixel as: 10101101 10010111 11101010 And the 8-bit secret message to be embedded is: 10010100

The stego pixel will be: 10101100 10010101 11101000

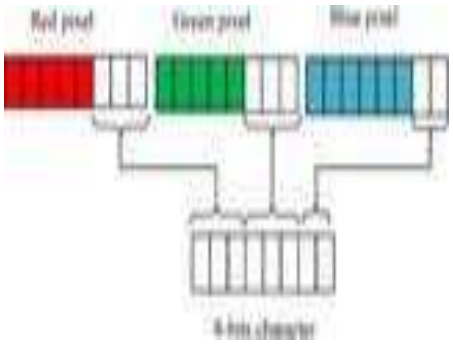

Fig. 1 24-BIT RGB PIXEL

B. Frequency Domain Technique

In frequency domain based technique of video steganography image is first transformed from spatial domain to frequency domain (by applying some techniques) and then embedding is performed. The well-known methods are Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

ISSN: 1832-5505
Vol-4 Issue-03 july 2016

DCT is very recurrent method of frequency domain steganography. This technique is applied to image pixels in spatial domain in order to convert them into frequency domain. DCT is a mechanism used in JPEG compression algorithm to transform 8*8 pixels of a block from spatial domain into 64 DCT coefficients each in frequency domain. If a single DCT coefficient is changed, it alters all image pixel[10],[11].
DCT process includes[12]:

- Initially the image is broken into blocks of pixels that are of size 8x8.
- The DCT is applied to each block from left to right then top to bottom.
- Through quantization each block is compressed.
- The array of blocks that are compressed that constitute the image is put in a significantly reduced amount ofspace.
- Through process of Inverse Discrete Cosine Transform (IDCT) image is reconstructed again.

1) DCT on an 8X8 block: Read the original image and get the values of the pixels from the image in the blocks. Since DCT is basically used to work on pixel values that range from -127 to 128. The block that is original is levelled off. It is done by subtracting 128 from every entry[13]. The discrete cosine transform is attained by

$$D = TMT'$$

Where T is the DCT matrix and M is the actual image matrix which is leveled off by subtracting 128.

2) Quantization: Block of DCT coefficients that is of size 8x8 is now sent for compression. This permits the person to decide the levels of quality starting from 1 to 100. DCT has predefined quantization matrix and is used to quantize the 8x8 blocks.

[16 11 10 16 24 40 51 61
12 12 14 19 26 58 60 55
14 13 16 24 40 57 69 56
14 17 22 29 51 87 80 62
18 22 37 56 68 109 103 77
24 35 55 64 81 104 113 92
49 64 78 87 103 121 120 101
72 92 95 98 112 100 103 99]

For less compression, higher image quality that is a quality level greater than 50, the standard quantization framework matrix is multiplied by (100-quality level)/50. For a quality level significantly less than 50 (more compression, lower image quality), the standard grid i.e. quantization matrix is multiplied by 50/quality level. The scaled quantization matrix is then adjusted and positioned accordingly to have only positive integer values that range from 1 to 255. Quantization is accomplished by dividing every element present in the transformed image matrix D by corresponding element in the quantization matrix, finally rounded to the integer value that is nearest.

3) Coding: All coefficients of C are changed to binary stream data by an encoder before storage (10011011...). To encode the data run-length encoding is used. To compress large runs of repeating items run-length encoding is used. Here only one item from the run is sent and a counter shows how many times this item has been repeated.
Discrete Wavelet Transform decays the signals into wavelet coefficients from which the original signal can be regenerated again. It is a wavelet transform for which wavelets are discretely sample. In DCT image is divided into four sub-bands: LL, HL, LH and HH. From which LL sub-band embeds the secret data.

EVALUATION MEASURES/ PERFORMANCE ANALYSIS

Many parameters are used to measure the performance of perceived stego image. In order to evaluate the imperceptibility of stego images and to measure the difference between original image and the cover image certain parameters are used like MSE (mean-squared error), PSNR (peak signal to noise ratio) and BER (bit error rate)[18].

A. PSNR

PSNR stands for peak signal to noise ratio. It may be defined as the ratio between the original frame and the stego frame. PSNRand MSE are inversely proportional to each other.

Mathematically:

$$\mathrm{PSNR} = 10 \times \lg\left(\frac{255^2}{\mathrm{MSE}}\right)$$

B. MSE

Mean-squared error (MSE) is the squared error between the original and stego frame and is given by:

$$\mathrm{MSE} = \frac{1}{M \times N}\sum_{i=1}^{N}\sum_{j=1}^{M}\left[I(i,j) - I'(i,j)\right]^2$$

C. BER

BER (bit error) is the number of bit errors per unit time and

$$\textit{Bit Error Rate, BER} = \frac{\textit{Number of errors}}{\textit{Total number of bits sent}}$$

is given by the equation:

ISSN: 1832-5505
Vol-4 Issue-03 july 2016

TABLE 1
COMPARISON TABLE

<table>
<tr><th>Author</th><th>Method/Technique Used</th><th>Parameter Calculated</th><th>Domain For Hiding data</th><th>Result</th></tr>
<tr><td>K. Dasgupta , J. K. Mondal, and P. Dutta</td><td>Genetic Algorithm and 3-3-2 LSB technique</td><td>PSNR IF</td><td>Uncompressed domain</td><td>
<table>
<tr><td>S no.</td><td colspan="2">Using GA</td><td colspan="2">Using 3-3-2 LSB</td></tr>
<tr><td></td><td>PSNR</td><td>IF</td><td>PSNR</td><td>IF</td></tr>
<tr><td>1</td><td>39.37</td><td>0.99</td><td>38.03</td><td>0.87</td></tr>
<tr><td>2</td><td>34.37</td><td>0.99</td><td>32.67</td><td>0.89</td></tr>
<tr><td>3</td><td>41.613</td><td>0.99</td><td>39.21</td><td>0.86</td></tr>
</table>
</td></tr>
<tr><td>A. A. Attaby, M. F. M. Mursi Ahmed, and A. K. Alsamma k [19]</td><td>DCT-M3 and LSB</td><td>Probability of change in DCT Coefficients</td><td>Compressed domain/ DCT</td><td>
<table>
<tr><td>Technique</td><td>No change</td><td>Change in 1 coefficient</td><td>Change in 2 coefficients</td></tr>
<tr><td>LSB</td><td>25%</td><td>50%</td><td>25%</td></tr>
<tr><td>DCT-M3</td><td>25%</td><td>66.7%</td><td>8.3%</td></tr>
</table>
</td></tr>
<tr><td>K. Dasgupta , J. K. [20] Mondal, and P. Dutta</td><td>HLSB</td><td>PSNR IF MSE</td><td>Spatial domain</td><td>
<table>
<tr><td>Sno</td><td colspan="3">Using HLSB</td><td colspan="3">Using LSB</td></tr>
<tr><td></td><td>PSNR</td><td>MSE</td><td>IF</td><td>PSNR</td><td>MSE</td><td>IF</td></tr>
<tr><td>1</td><td>44.34</td><td>0.34</td><td>0.23</td><td>48.56</td><td>0.42</td><td>0.32</td></tr>
<tr><td>2</td><td>45.67</td><td>0.34</td><td>0.25</td><td>52.34</td><td>0.52</td><td>0.34</td></tr>
<tr><td>3</td><td>42.66</td><td>0.34</td><td>0.35</td><td>48.56</td><td>0.38</td><td>0.38</td></tr>
</table>
</td></tr>
<tr><td>V. Kapoor and A. Mirza[21]</td><td>Enhanced LSB</td><td>PSNR MSE</td><td>Compressed domain</td><td>
<table>
<tr><td>S no</td><td colspan="2">Using enhanced LSB</td><td colspan="2">Using LSB</td></tr>
<tr><td></td><td>PSNR</td><td>MSE</td><td>PSNR</td><td>MSE</td></tr>
<tr><td>1</td><td>52.94</td><td>0.33</td><td>51.33</td><td>0.38</td></tr>
<tr><td>2</td><td>52.22</td><td>0.39</td><td>50.89</td><td>0.42</td></tr>
<tr><td>3</td><td>51.55</td><td>0.45</td><td>50.31</td><td>0.48</td></tr>
</table>
</td></tr>
</table>

ISSN: 1832-5505
Vol-4 Issue-03 july 2016

R. J. Mstafa and K. M. Elleithy	DCT Hamming and BCH codes	PSNR	Compressed domain/ DCT	PSNR=40.73 dB

LITERATURE SURVEY

Video steganography can be considered as the extension of image steganography as video file is primarily composed of images known as frames. Mostly used technique in video steganography is Least Significant Bit (LSB) technique. In this technique, first of all the carrier file (video, audio, image, text) is converted to 8 bit value then the LSB of 8 bit value is used for embedding the secret data. LSB method is also used in video steganography[22]. In video steganography firstly the video is converted into framesand 8 bit pixel value of each frame or some of the frames can be used for hiding secret data. It is the simplest technique which has less security as the secret data can be compromised by some file transformation operations. Another widely used technique is discrete cosine transform technique on which more research work is going on to improve performance[23].

Kousik Dasgupta, JK mondal [19], in the year 2012 suggested a hash based least significant bit (HLSB) technique for video steganography in which eight bits of secret message is divided into 3,3,2 and embedded into the RGB pixel of the cover video respectively. Here author has used random distribution of bits so that robustness is increased. The parameters calculated are PSNR, MSE and image fidelity (IF) and the results shows minimal degradation of video file. Vipula Madhukar wajgade, Dr Suresh Kumar, in the year 2013, had used AES and SHA-1 algorithm for video steganography to make it more secure and robust. These two algorithms are applied on secret message so that stenographic system is made more secure. AES has symmetric block cipher hence uses same key for encryption and decryption. SHA-1 is used to provide more restriction as it generates hash function with key which helps to make secret data more secure. After performing these steps actual steganography is performed, that is, data is embedded into the cover video.

And then, Kousik Dasgupta, Jyotsna Kumar mondal, paramartha dutt, in the year 2013, devised a 3-3-2 LSB based techniques has been used as a base technique for video steganography. Frames are extracted from cover video using splitter module and one or more frames which are used as carrier are given as input to embedder. The embedding is done using 3-3-2 LSB based technique. Now the stego frame(s) are given to the optimizer which optimizes the stego frame(s) so that it is indistinguishable from the original frame(s). Optimizer uses Genetic Algorithm (GA) as optimization algorithm. Anti-steganalysis test is also performed. Next the stego frames(s) are given to merger module which merges all the stego frame(s), non-stego frame(s) and audio in order toget the stego video.

Another contribution came in 2014 by M. Suresh Kumar, G. Madhavi Latha[10], in this paper author formulated a DCT based secret image hiding method in which only R channel is used to hide data. 297x169 sized image is used as a secret message, this message is first converted to binary format. As the size of image is 297x169 hence 297x169x8=401544 bits will be embedded in video frames. Then the carrier video is selected having resolution as 324x244, the number of frames extracted is 31. Lately DCTis applied to cover video so that 410544 bits will be embedded in higher order DCT coefficients. The original signal and quality ofvideo after encoding is almost similar. Heena Goyal, Preeti Bansal[24], in the year 2015, used Genetic Algorithm (GA) and Neural Network (NN) for steganography. Authors have divided the video stenographic system into two parts. In the first part GA algorithm and DCT is used in which DCT is used for optimization and segmentation of selected frames of cover video. Genetic Algorithm uses fitness function to optimize the sample images so that useless data is removed. In the second part Neural Network (feed forward) is used for classification purpose. NN distinguishes pixels in less sensitive areas from more sensitive areas in orderto embed the secret data.

Abdelhamid Awad Attaby[19],in the year 2017, proposed a methodology of transform domain JPEG image transformation technique. This method provides high embedding capacity while change in carrier image is minimized. The idea here is to use an algorithm named DCT-M3. This algorithm uses modulo 3 of the difference between two DCT coefficients for embedding. In order to minimize the change in cover medium author uses two methods, the former one is to compress the cover data and the laterone is to use DCT-M3 algorithm for embedding.

CONCLUSION

In the era of emerging technologies and fast exchange of confidential information over internet, steganography has played a vital role. This paper provides a review on various methods of steganography. All the methods have advantages and disadvantages like LSB has high embedding capacity while DCT is robust against attacks. On the other hand DCT has low embedding capacity. HLSB is also present which is efficient than LSB. The future scope is to use combination of these techniques so that robustness is achieved along with high embedding

ISSN: 1832-5505
Vol-4 Issue-03 july 2016

capacity. Optimization Algorithm will be used alongside in order to optimize the stego frames.

REFERENCES

[1] H. Trivedi and P. A. Rana, "A Study Paper on Video Based Steganography," *Int. J. Adv. Res. Ideas Innov. Technol.*, vol. 3, no. 1, pp. 612–615, 2017.

[2] V. M. Wajgade and S. Kumar, "Enhancing Data Security Using Video Steganography," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 4, pp. 549–552,2013.

[3] K. B. Sudeepa, K. Raju, H. S. Ranjan Kumar, and G. Aithal, "A New Approach for Video Steganography Based on Randomization and Parallelization," *Phys. Procedia*, vol. 78, pp. 483–490, 2016.

[4] I. Naidu, P. Deepak, and K. Xaxa, "A Novel Video Steganography Algorithm for Secure Data Hiding," pp. 1569–1575, 2017.

[5] L. N. Meghanathan Natarajan, "Steganalysis algorithm for detecting the hidden information in images, audio and video cover media," *Proc. Seventh Int.Conf. Inf. Qual.*, vol. 2, no. 1, pp. 18–30, 2002.

[6] S. A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Comput. Electr. Eng.*, vol. 70, pp. 380–399, 2018.

[7] P. Shinde and T. B. Rehman, "International Journal of Advanced Research in A Novel Video Steganography Technique," no. March, 2016.

[8] A. Nissar and A. H. Mir, "Classification of steganalysis techniques: A study," *Digit. Signal Process. A Rev. J.*, vol. 20, no. 6, pp. 1758–1770, 2010.

[9] P. V Swetha V, "Data Hiding Using Video Steganography -A Survey," vol. 5, no. 6, pp. 206–213, 2015.

[10] M. S. Kumar and G. M. Latha, "DCT Based Secret Image Hiding In Video Sequence," *Int. J. Eng. Res. Appl.*, vol. 4, no. 8, pp. 5–9, 2014.

[11] R. J. Mstafa and K. M. Elleithy, "An ECC/DCT-Based Robust Video Steganography Algorithm for Secure Data Communication," *J. Cyber Secur.Mobil.*, vol. 5, no. 3, pp. 167–194, 2017.

[12] S. Gujjunoori and B. B. Amberker, "DCT based reversible data embedding for MPEG-4 video using HVS characteristics," *J. Inf. Secur. Appl.*, vol. 18,no. 4, pp. 157–166, 2013.

[13] A. Khamrui and J. K. Mandal, "A Genetic Algorithm based Steganography Using Discrete Cosine Transformation (GASDCT)," *Procedia Technol.*, vol.10, pp. 105–111, 2013.

[14] P. Malathi, M. Manoaj, R. Manoj, V. Raghavan, and R. E. Vinodhini, "Highly Improved DNA Based Steganography," *Procedia Comput. Sci.*, vol. 115,pp. 651–659, 2017.

[15] P. Sethi and V. Kapoor, "A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography," *Procedia Comput. Sci.*, vol. 87, pp. 61–66, 2016.

[16] K. Dasgupta, J. K. Mondal, and P. Dutta, "Optimized Video Steganography Using Genetic Algorithm (GA)," *Procedia Technol.*, vol. 10, pp. 131–137,2013.

[17] A. Khamrui, E. Scholar, and K. Univerasity, "A Report on Genetic Algorithm based Steganography for Image Authentication."

[18] L. Rossi, F. Garzia, and R. Cusani, "Peak-shaped-based steganographic technique for JPEG images," *Eurasip J. Inf. Secur.*, vol. 2009, 2009.

[19] A. A. Attaby, M. F. M. Mursi Ahmed, and A. K. Alsammak, "Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3," *Ain Shams Eng. J.*, 2016.

[20] J. . M. and P. D. Kousik Dasgupta, "Hash Based Least Significant Bit Technique Foe Video Steganography (HLSB)," *Procedia Comput. Sci.*, vol. 10,no. 3, pp. 1–11, 2016.

[21] V. Kapoor and A. Mirza, "An Enhanced LSB based Video Steganographic System for Secure and Efficient Data Transmission," *Int. J. Comput. Appl.*,vol. 121, no. 10, 2015.

[22] S. Sahand, M. Ziabari, and V. U. Amsterdam, "Video Steganography Title Video Steganography in the compressed area Seyed Sahand Mohammadi Ziabari January 2017," January, 2018.

[23] M. I. S. Reddy and A. P. S. Kumar, "Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm," *Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 62–69, 2016.

[24] P. B. Henna Goyal, "VIDEO STEGANOGRAPHY USING NEURAL," vol. 1, no. 9, pp. 7–14, 2015

[25] .