IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# An Effective Video Steganography Technique Bases on Small Pixel Valve difference (SPVD).

[1]Sheikh Aasim Hussain, [2] Dr. Punam Rattan

[1] Student M.Tech Electronics and Communication, [2]Assistant Professor Computer Science Engineering
[1]Elecronics and Communication,
[1]CT University Ludhaina, Punjab, India.

*Abstract:* With the growth in internet it is easy to transfer data faster and accurately to the destination. There are high possibility that data we are transferring is not secure, this can be misused or modified. To overcome this various steganography techniques are used. For transmission of multimedia files there are already lot of security tools, but less efforts are made to secure text message. The purpose of this paper is to propose a new steganography technic to hide text message in a video file based on small pixel value difference (SPVD). This paper focuses on analyzing the various video steganography techniques which were proposed for securing text message. In this paper small pixel value difference of characters are used to embed data into the video file. On experiment this proposed method shows appreciable results and visual quality of stegno-video is better compare to other techniques used previously.

***Index Terms*** **- Video Steganography, image Processing, video frame, ASCII Value, SPVD, Information Hiding.**

## I. Introduction

Modern world is also called digital world because documents, audios, videos are present in digital form. With the growth in digitalization it must ensure safety of digital data. Privacy of data should be maintain and presentation from mass copying. To achieve this steganography techniques are used. Steganography is a technique of hiding secret information in such a way that hidden message can be detected by authorised person only. In steganography secret data is hidden in cover medium. Cover medium can be audio, video, audio or image.[10] [11] Steganography is a combination of two words "stegano" refers to "covered" and "graphic" means "Writing". Back in history steganography techniques were used around 440 B.C. Steganography was used during American Revolution, they use invisible ink to hide secret message which glows in heat. Britisher and Americans used this technique to communicate with each other.

With growth in technology steganography techniques were also changed. Now a days with the growth in internet, multimedia contents are not secure, their arises a need of new steganographic techniques to secure data. Steganography provides an important tool to secure data.

### Types of Steganography

Based on type of cover file in which secret message is hidden, steganography is of following 4 types:

1. Text Steganography.
2. Audio Steganography.
3. Video Steganography.
4. Image Steganography.

These are discussed as under:

1. **Text Steganography**

Text steganography is defined as hiding information in text file. In this method text file is used to hide data. Secret message is hide in the nth letter of each word. There are various ways of hiding information in a text file there are using free grammars from generate readable texts, to changing words within a text, to generate random character sequences, to changing the formatting of an existing text. Main difference between structure of a text document and structure of image document is that structure of text is same as what we observe while as structure of image document is different from what we observe. This difference between structures of text document and image document is the main advantage of text steganography over image steganography because secret data can be hidden without changing original output. Storing of text requires less memory than audio, video or any other file, it is faster and easier to communicate, this is why it is most preferable steganography technique than others. [12][13]

2. **Video steganography**

Video steganography is defined as a type of steganography in which video file is used as a cover file. Data which is to be hide is embedded into frames of host video. This type of data hiding is secure because of large size of video file. Embedding of data don't affect the quality of video due to large size of video file.[7]

3. **Image steganography**

Image steganography is a type of steganography in which secret data or information is hidden in image. In order to hide data in an image, grayscale image is first represented in X × Y matrix then stored in memory. In case of colour image, image is represented in X×Y×3 matrix. Intensity of pixels is represented by each entry. Steganography is done my altering some pixel value of an image. Image Stenography is achieved by following proper encrypted algorithm, to extract the hidden message from the image receipt of the image must know the same algorithm.[9] [14]

4. **Audio or sound steganography**

Audio steganography is type of hiding secret message in an audio file like WAV, AU or MP3 sound file. Audio steganography ensure copyright of audio file. Video and image steganography depends on the limitation of human visual system i.e. hidden data is visible to human eye while in case of audio steganography, it depends on listening capacity of human which is known as Human Auditory System (HAS). Proper algorithm must be followed for embedding of secret message as well as for extraction of secret message. [18] [19]

**Steganography Techniques**

1. **Hiding of text using Small Pixel Valve difference (SPVD).**

This steganography technique is one of the simplest steganography technique in this method frame is divided into blocks having dimension of M × M. Then difference between pixel values of each block is calculated. Choose two smallest differences from each block, then from the given table the optimum range is obtained in which these differences lies. ASCII value of characters which is to be embedded is taken and is converted into binary code. Number of bits which is to be embedded is chosen from given table. Convert these bits into decimal number and add this decimal number with the lower range for computing new differences. Subtract this differences from the old difference to get new value. Divide this value by 2, add this value to pixel with high pixel number and subtract form pixel with lower pixel value. At last rearrange these blocks having new pixel valves into frames and reconstruct the video. [1][2]

2. **Steganography in Spatial Domain (LSB Substitution)**

The Least Significant Bit (LSB) substitution method, is a simple method but it is a effective one to hide information in an audio video or an image file. In this method the least significant bit or the most significant bit of each pixel of an image is used to embed. This embedded bits in an image forms a new image by combining with the original pixels of the image [06]. For Example Original Pixels of image: 10100111 and Embedded Pixel: 00111111.

New Image Pixel should be: 10110011. In order to get the message bits the count of bits used for storing secret image should be known. [15] [16]

3. **Discrete cosine transform**

Leurs in 2001 proposed that discrete cosine transform (DCT) is an important component in compression of JPEG images. In this technique image is divided into 8 x 8 squares, where each block is transformed. After transformation the output is a multi-dimensional array which has sixty four coefficients. Now coefficients which has small vale are rounded off to zero (0) and thus producing a coefficient array. By

using Huffman encoding scheme it is further compressed and then decompressed by an inverse DTC. Due to evenly distribution of hidden information in image, image is robust. [16]

### 4. Wavelet transform (DWT)

Wavelet transform is a steganography technique which uses wavelets to encode an image [7]. This technique is consider better than DCT, because of its high compression levels. This robust technique of information hiding is widely used in watermarking. In this technique wavelets compress high frequency details of an image and then separates it from lower frequencies and compresses the wavelets. After this quantization technique is applied and message is hidden in wavelet information. [16]

## II. Literature survey

Steganalysis is now a days emerging research field. Before late 1990's some research articles was published. As the time passed on more and more research was done on staganalysis which proposes techniques by which steganography is achieved. Some of these researches is based on steganography based on techniques using ASCII value of character which is to be embedded. [1] Proposed that an individual character can be stored into a single pixel by combining character's ASCII value with the RGB value of pixel. Advantage of this method is that it provide maximum payload capacity. [2] Proposed a method in which stego text is visibly indistinguishable from the original cover text based on steganography based on ASCII Mapping Technology on English. Advantage of this solution is that it is doesn't depend on the nature of data which is to be hidden this it is applicable to other languages as well. [5] Suggested the mechanism which uses the structure of omega network to hide secret data. This method is very useful to hide long text message as it have better execution time and better covering words. There are various other methods to hide text in a cover file. One research developed in Germany called microdot. Microdots contain full information of the page, they are the size of letter. These microdots are then printed on envelope or in a letter, due to their small size they are unnoticeable [4]. On studying further one author proposed a new method of hiding secret information, [3] by using white spaces between words and paragraphs to hide secret information. Main disadvantage of this method was that it requires large space to hide small bit of data. To overcome this they use space between words and space between paragraphs to hide information. LSB is another tool of hiding secret message in a cover file. By using this technique data can be hidden in both audio and video files with the help of key exchange. Probability of attack can be reduced by this proposed method [6]. Video is combination of frames of audio, text and images, data which is to be hidden is embedded into these frames. This can be achieved by using DWT and artificial intelligence. Artificial intelligence technique is used to enhance security of data transfer [7]. Combining steganography with cryptography provides more security to secret data, in this proposed method steganography provides security layer for the embedded data. This newly formed security layer changes the format of encrypted message. This encrypted message is then embedded into a multimedia cover file [8].

## III. Proposed Scheme.

**Embedding**:

1. Take a video as a stenographic input for the proposed scheme.
2. Extract the video frames from input video.
3. Make blocks having dimensions of 2 × 2 for each frame of input video.
4. Select each block one by one for computing difference between pixels within each block
5. Choose two smallest differences from each blocks.
6. Find the optimum range from the table in which these smallest difference lie.
7. Converts each input text into ASCII code. After that this ASCII code is converted into binary code.
8. According to optimum range pick the number of bits from binary string and convert it into decimal number.
9. Add this decimal number with lower range for computing new difference.
10. Subtract new difference from old selected smallest difference for getting M.
11. Now compute

    m = M/2
12. Now add m with high pixel and subtract from lower pixel.
13. Now rearrange blocks into frames and reconstruct the video.

**Extraction**.

1. Receive the stenographic video.
2. Extract the video frame from the video.
3. Make blocks having dimension of 2 × 2 for each frame of video.
4. Select each block one by one for computing differences between pixels within the frame.
5. Choose two smallest differences from each blocks.
6. Convert these smallest differences into binary and concatenate these binary numbers to make a string.
7. Now convert this binary string into decimals and then convert this decimal into character.

## IV. Result and Conclusion

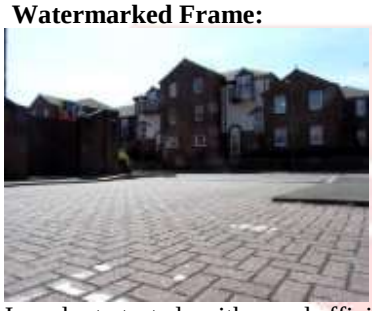
Below mentioned figures shows video stegnagraphy. One frame of video 1 and secret message which is to be embedded is taken as input. Text is embedded in frame using embedding algorithm. Figure 2 is a stegno image which is an output frame obtained after embedding text into a frame.

**Original Frame:**

**Text to be embedded:**

**THIS IS A SECRET MEESSAGE**

**Watermarked Frame:**



In order to test algorithm and efficiency of proposed technique four videos were taken. In terms of PSNR, BER, and MSE result comparison of all 4 videos is shown in below tables.

The PSNR has been calculated as below:

**PSNR:** $10 \log_{10}\left(\frac{MAX^2}{MSE}\right)$

Mean Square Error (MSE) between the host frame X and the watermarked Frame X' is defined as

$$MSE : \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{i=0}^{N-1} \left(X(i,j) - \left(X'(i,j)\right)\right)$$

Table 1: Matlab output of video1

| Video 1 | |
|---|---|
| PSNR | 82.207 |
| MSE | 0.00045 |
| BER | 125.02 |

Table 2: Matlab output of video2

| Video 2 | |
|---|---|
| PSNR | 83.220 |
| MSE | 0.00035 |
| BER | 123.08 |

Table 3: Matlab output of video3

| Video 3 | |
|---|---|
| PSNR | 79.807 |
| MSE | 0.00025 |
| BER | 89.021 |

Table 4: Matlab output of video4

| Video 4 | |
|---|---|
| PSNR | 72.067 |
| MSE | 0.00035 |
| BER | 65.08 |

**Conclusion:**

Video steganography techniques are used to hide secret message into a cover media so that any unauthorized access to secret message shall be prevented. There are various video steganography techniques used for this purpose, but less focus was made to hide text message into a video file. So the proposed method uses Small pixel value difference (SPVD) to embed text message into a cover video. The experimental result showed robustness against differ kinds of attacks also the text embedded was imperceptible to naked eye and the quality of the host video doesn't get effected by embedding the text in it. Main focus of this research is on security, by using this proposed techniques rate of security is enhanced in the realistic applications.

**V. References**

[1] Keshav Joshi, "*A New Approach of Text Steganography Using ASCII Values*", International Journal of Engineering Research & Technology (IJERT), Vol. 7 Issue 05, May-2018

[2] Souvik Bhattacharyya, Pabak Indu and Gautam Sanyal, "*Hiding Data in Text using ASCII Mapping Technology (AMT)*", International Journal of Computer Applications, Volume 70– No.18, May 2013.

[3] L. Y. Por, B. Delina, "*Information Hiding: A New Approach In Text Steganography",* WSEAS intentional. Confrence on Applied Computer & Applied Computational Science, April 2008.

[4] Dhanarasi G. and Prasad A. M., "*Image Steganography Using Block Complexity Analysis*", International Journal of Engineering Science andTechnology (IJEST), vol. 4, 2012.

[5] Abdullah M. Hamdan and Ala Hamarsheh, "*An algorithm of text in text steganography using the structure of omega network*", Security and communication networks, February 2017.

[6] Sateesh Gudla, Suchitra Reyya, Aswini Kotyada and Aditya Sangam, "*Key Based Least Significant Bit (LSB) Insertion for Audio and Video Steganography*", International Journal of Computer Science Engineering Research and Development (IJCSERD), March 2013.

[7] Shivani Gupta, Gargi Kalia and Preeti Sondhi, "*Video Steganography Using Discrete Wavelet Transform and Artificial Intelligence*", International Journal of Trend in Scientific Research and Development (IJTSRD), Volume: 3, Issue: 4, May-Jun, 2019.

[8]Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay, and Tai-hoon Kim, "*Text Steganography: A Novel Approach*", International Journal of Advanced Science and Technology, Vol. 3, February, 2009.

[9] Abhishek Koluguri, Sheikh Gouse, Dr. P. Bhaskara Reddy, "*Text Steganography Methods and its Tools*", International Journal of Advanced Scientific and Technical Research , Issue 4 volume 2, March-April 2014.

[10] K. H. Jung, "*Dual image based reversible data hiding method using neighbouring pixel value differencing,*" Imaging Science Journal, vol. 63, no. 7, pp. 398–407,2015.

[11] S. Atawneh and P. Sumari, "*Hybrid and blind steganographic method for digital images based on DWT and chaotic map,*" Journal of Communications, vol. 8, no. 11, 2013.

[12] Ammar Odeh, Khaled Elleithy, Miad Faezipour "*Steganography in Text by Using MS Word Symbols*".

[13] Khaled Aedh Alaseri and Adnan Abdul-Aziz Gutub, "*Merging Secret Sharing within Arabic Text Steganography for Practical Retrieval*", IJRDO - Journal of Computer Science and Engineering, Volume-4 | Issue-9 | Sept, 2018.

[14] Ashadeep Kaur, Rakesh Kumar, Kamaljeet Kainth, "*Review Paper on Image Steganography*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016

[15] Naveen Verma, Preeti Sondhi, Gargi Kalia, "*LSB Based Steganography to Enhance the Security of an Image*", International Journal of Trend in Scientific Research and Development (IJTSRD), Volume: 3 | Issue: 4 | May-Jun 2019

[16] Roshidi Din, Massudi Mahmuddin, Alaa Jabbar Qasim, "*Review on Steganography Methods in Multi-Media Domain*", International Journal of Engineering & Technology, 8 (1.7) (2019)

[17] Vipul Sharma, Sunny Kumar, "*A New Approach to Hide Text in Images Using Steganography*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

[18] Shilpi Mishra, Virendra Kumar Yadav, Munesh Chandra Trivedi and Tarun Shrimali, "*Audio Steganography Techniques: A Survey*", Research Gate, January 2018.

[19] Pooja P. Balgurgi and Sonal K. Jagtap, "*Audio Steganography Used for Secure Data Transmission*", Springer India 2013.

[20] V.Yamini Priya, K.Priyadharshini, K.Sowndharya, S.Swathi and K.Swetha, "*Hiding Data in Video Sequences using RC6 Algorithm*", International Journal of Computer Science and Mobile Computing, Vol. 9, Issue. 1, January 2020.