Video Steganography using Zero Order Hold Method for Secured Data Transmission

Shashidhara H. N.
M.Tech Student
Dept. of CSE, RVCE
Bengaluru, INDIA

Usha B. A., PhD
Assistant Professor
Dept. of CSE, RVCE
Bengaluru, INDIA

ABSTRACT
Steganography used for secure transmission of secret message. Message transmitted over the internet facing malicious attack. So, steganography is needed for secure transmission of secret message. There are two methods which are used for secure transmission. The first method cryptography, secret message which needs to be transmitted over the internet is encrypted using encryption key and sent over the communication channel and at the receiver side only right person with valid key can retrieve the secret message. The second method is steganography, in this method secret message hidden inside the cover media like image, audio, video etc. In this paper, we have presented video steganography using Zero Order Hold(ZOH) technique. Zero Order Hold is basically zooming method, it is used for image zooming. By applying ZOH method, secret information embedded in the cover video.

General Terms
Security, Algorithms, Encryption, Steganalysis.

Keywords
Video Steganography, Zero Order Hold, Peak Signal Noise Ratio, Mean Squared Error, Data Embedding.

1. INTRODUCTION
Using image steganography only limited amount of secret data can be hidden, due to its less embedding capacity video steganography being used. Using video steganography unlimited secret data can be stored in the video frames. Due to its unlimited hiding capacity video steganography applications used in many areas like industrial applications, copyright, military etc. And another advantage of video steganography is gets extra security due to fast moving of video frames, so attacker cannot notice differences between original and cover video.

There are various techniques of video steganography, in this project Zero Order Hold, a new technique being used to hide the secret data inside the video. The main goal of this technique is to hide a secret message in the pixels of the cover video in such a way that the human eyes are not able to differentiate between the original and the stego-video. ZOH method already used in image steganography [1], in our work we have extended this for video steganography.

System architecture of video steganography for secured data transmission is as shown in Fig 1.

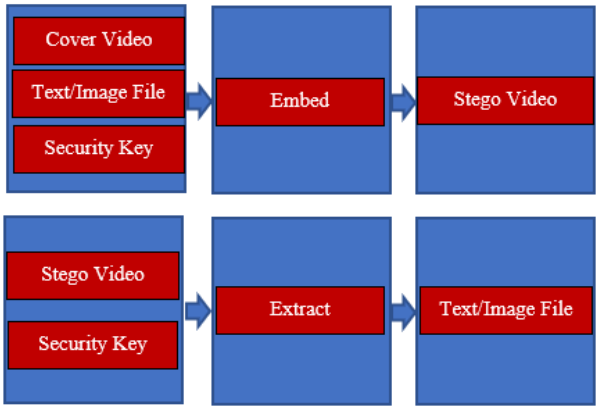

Fig 1: System Architecture of Video Steganography

The video steganography project developed using ZOH method hides any secret data provided in the text or image file. Encoding application allows user to select cover video, secret text or image file and encoding password. The secret data provided in the text or image file is converted into binary form using Braille character representation and embedded in the video frames of cover video and creates stego video. Encoding password will be used select the video frames randomly to hide the secret information. Decoding application allows user to select stego video and decoding password. Using valid decoding password, decoding application can extracts the secret information from the video frames and created text or image file based on the message type.

2. LITERATURE REVIEW
A lot of research work has been carried out on audio and video steganography which concentrate on secret data hiding in audio and video file without image distortion. Image zooming method (ZOH) used for image steganography [1], in this research work each secret character converted 8-bit binary form of its ASCII equivalent and embedded in the image pixels. In this research, limited information can be stored.

The work presented in paper [2] developed robust steganography system uses combination of techniques algorithm incorporates features from various existing techniques to form an efficient steganography algorithm which can help in cover communication. This method uses RSA cryptography method for secret data encryption. With this common encrypt method secret data can be easily decrypted.

The technique used in [3] uses Hamming and BCH ECC codes for data hiding. Using this method an additional bit will be added along with secret message bits during data hiding.

Due to addition of extra bits, message hiding capacity will be reduced.

The work presented in [4] implements video steganography algorithm using frequency domain. In the transform domain algorithm, a true color image is transformed into IWT (Integer Wavelet Transform) domain using a wavelet called 'haar' wavelet. The wavelet transforms the image into four frequency bands, namely AC, HC, VC, and DC. The band AC is the approximation coefficient band and the other three are detail coefficients. The secret data are embedded in the DC component and the image is transformed back into original form by reverse transformation. The secret message is hidden only in one fourth part of the image. Hence the volume of information that can be hidden using this algorithm is less when compared to the spatial domain algorithm.

LSB is most commonly used algorithm in image/video steganography. Research carried out in [5] used Least Significant Bit (LSB) algorithm and along with Least Significant Frame(LSF) method. LSF method selects less significant frame using optical flow features. Using optical flow features, movement of the objects in the video is obtained, using this less significant frames is selected to hide to secret message.

In [6], LSB method is used to hide secret data in video frames and audio signals of audio-video file. Insertion position of the LSB is determined by using first 2 bits of the 24 bits WAV file and secret binary message is embedded until all the data embedded. Discrete wavelet transform value is used to select next frame to hide the data.

Shell based scheme used in [7] for data hiding that increase embedding capacity and with good visual quality of stego-image. This scheme called turtle, which uses hexagon shaped shell to update pixel pairs in the cover image. Using this scheme, it was noticed that embedding capacity stills needs to be improved.

In [8], Researcher used cryptography algorithms to provide extra security while hiding secret information in the image. In this image steganographic work various cryptographic techniques are experimented and its advantages are mentioned.

In the video steganography work [9], researchers used extended LSB method like 1LSB,2LSB and 4LSB used to hide the secret data in the video frames of the cover video.

In [10], researchers introduced method for video steganography based on motion vectors. This work model hides the secret information in the least significant bit of the motion vectors. Developed method tested with different types of video files by various motion vectors estimation methods.

Authors in [11], presented modified motion-vectors reversion based features and calibration-based approach for hiding data in the image or video frames. Proposed method is improved version of traditional motion vector, spatial or transform domain based method which violates data hiding principles.

Work carried out in [12], uses Sudoku puzzle to improve hiding capacity. Using Sudoku Puzzle, reference matrix was built that was used for data hiding and data extraction at both at sender and receiver side. In experimental results it was concluded that, Sudoku Puzzle improves the hiding capacity and quality of stego-image.

H. Aly et al [13] proposed data hiding method based on Motion Vectors of compression video. In this work data embedding in the compressed video. While encoding, forward predictive-frame and bidirectional frames are reconstructed using Motion Vectors. The secret data is encoded in the less significant bits of motion vector.

In [14], digital images are used as carrier media for communication of visual information. In proposed work authenticity of digital image is verified by different forensic techniques. The proposed forensic methods help in identifying others features like local and global contrast for the enhancement, histogram equalization and noise in the previously compressed images.

In the presented work [15], maze game used as carrier media to hide the secret message. In the maze game there are many paths along with solution path, all the paths cell or pixel values are used to hide the secret information. Secret information embedded using HKMG algorithm.

3. METHODOLOGY

Zero Order Hold is zooming method, basically it used for image zooming. In ZOH method, average of two adjacent pixels elements is found, and result is placed between two pixels. This procedure applied along row wise and then column wise. Below Fig 2 shows how image of dimensions 2 rows and 2 columns is zoomed using ZOH method.

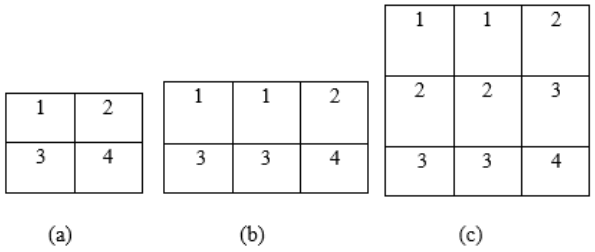

Fig 2: Zooming of 2*2 image using ZOH method. (a) Original 2*2 image (b) ZOH method applied row wise (c) ZOH method applied column wise.

For video steganography, ZOH method will be applied only on row-wise, no additional rows created here, in this technique two adjacent pixels (i and i+1) average value is calculated to embed encrypted binary secret data and average with embedded secret data is placed in i+1 pixel, similarly next adjacent pixels (i+1, i+2) average calculated to embed next secret data and this procedure continues.

4. IMPLEMENATION

Video steganography project developed using ZOH method consists of encoding and decoding applications. Encoding application hides the secret information in the video frames of cover video and decoding applications extracts secret information from the stego video. This project developed using Java and used Xuggler library.

4.1 ZOH Data Embedding Algorithm

Below is algorithm for embedding the secret information using ZOH algorithm in the encoding application. In the pre-processing stage video frames extracted from the cover video and secret message converted into binary data using Braille character representation [20]. Video frames and binary secret message and message length are the input for the embedding algorithm. As earlier mentioned in this chapter, ZOH technique applied along row wise to embed the secret information.

Input: Secret Binary Data, Message Length, Video Frames from the Cover Video

Output: Stego Video Frames

Steps:

1. Get the value for Red(R1), Green(G1) and Blue(B1) from the i^{th} pixel of current row

2. Get the value of Red(R2), Green(G2) and Blue(B2) of $(i+1)^{th}$ pixel in the same row

3. Find the average values for Red (avgRed), Green (avgGreen) and Blue (avgBlue)

$$\text{avgRed} = (\text{R1} + \text{R2})/2$$
$$\text{avgGreen} = (\text{G1} + \text{G2})/2$$
$$\text{avgBlue} = (\text{B1} + \text{B2})/2$$

4. Embed the next secret bits in calculated average values

$$\text{avgRed} = \text{avgRed} \mid \text{Next Secret Bit}$$
$$\text{avgGreen} = \text{avgGreen} \mid \text{Next Secret Bit}$$
$$\text{avgBlue} = \text{avgBlue} \mid \text{Next Secret Bit}$$

5. Find the $(i+1)^{th}$ pixel values from the calculated average values

$$\text{nextPixel} = (\text{avgRed} \ll 16) + (\text{avgGreen} \ll 8) + (\text{avgBlue})$$
$$\text{pixel}(\text{i}+1) = \text{nextPixel}$$

6. $\text{i} = \text{i} + 1$

7. Repeat steps 1 to 6 until whole secret message embedded in the video frames

4.2 ZOH Data Extraction Algorithm

At the decoding application, secret binary information extracted from the stego video by applying reverse ZOH algorithm and extracted binary secret information converted into ASCI text using Braille character representation as mentioned in Table 2.1. Pre-processing stage of decoding application extracts video frames from the stego video and extracted frames and message length are given as input to the data extraction algorithm. Below is algorithm for extracting secret information using ZOH method.

Input: Video frames that contain Secret Data, Message Length

Output: Binary Secret data

Steps:

1. Get the value for Red(R1), Green(G1) and Blue(B1) from the i^{th} pixel of current row

2. Get the value of Red(R2), Green(G2) and Blue(B2) of $(i+1)^{th}$ pixel in the same row

3. Find the zooming values for Red (zoomRed), Green (zoomGreen) and Blue (zoomBlue)

$$\text{zoomRed} = (\text{R1} + \text{R2})/2$$
$$\text{zoomGreen} = (\text{G1} + \text{G2})/2$$
$$\text{zoomBlue} = (\text{B1} + \text{B2})/2$$

4. Extract the next secret bits from the zoomed values

$$\text{nextSecretBit} = \text{zoomRed}\%2$$
$$\text{nextSecretBit} = \text{zoomGreen}\%2$$
$$\text{nextSecretBit} = \text{zoomBlue}\%2$$

5. $\text{i} = \text{i} + 1$

6. Repeat steps 1 to 5 until whole secret message extracted from the video frames

5. EXPERIMENATAL ANALYSIS AND RESULTS

Evaluation metrics [16] are used to explain the performance of developed project, these metrics can be used to measure the quality of the software or software development method. Commonly used evolution metrics for the video steganography projects are Peak Signal Noise Ratio [17] and Mean Squared Error [18].

5.1 Experimental Datasets

The cover videos used for this project are in the MP4 or AVI format and secret images are in any format. Secret text files being used for the experiment are created by the user with any characters. Fig 3 to 7 shows cover videos and secret images used for experiment.

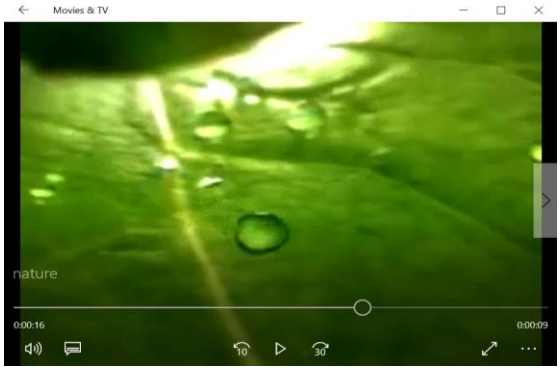

Fig 3: MP4 Format Cover Video

Fig 4: AVI Format Cover Video

Fig 5: Sample Secret Image

Fig 6: Sample Secret Image

Fig 7: Sample Secret Image

5.2 Performance Analysis

The performance of ZOH algorithm used in this project is evaluated using MATLAB [19] by finding PSNR and MSE values of cover video and stego video. Table 1 shows PNSR and MSE values between cover video (see Fig 3) and its stego video for different secret files.

Table 1: PNSR and MSE values for MP4 Cover Video

Secret File	Pay Load Size	MSE	PSNR
Image1 (Fig 5)	300*470	1.050312	48.165461
Image2 (Fig 6)	600*409	1.158077	49.181705
Image3 (Fig 7)	208*192	1.148571	47.647691
Text File	100 Pages (1,46,492 characters)	1.295432	48.092007

Table 2 shows PNSR and MSE values between cover video (see Fig 4) and its stego video for different secret files.

Table 2: PNSR and MSE values for MP4 Cover Video

Secret File	Pay Load Size	MSE	PSNR
Image1 (Fig 5)	300*470	1.167917	48.561012
Image2 (Fig 6)	600*409	1.265432	48.991012
Image3 (Fig 7)	208*192	1.248991	47.007691
Text File	100 Pages (1,46,492 characters)	1.395060	47.589964

6. CONCLUSION AND FUTURE SCOPE

The project on video steganography aimed at experimenting ZOH zooming method for video steganography. The main aim of this project is to experiment ZOH method for video steganography that improves the hiding capacity and the stego video quality in such a way that the human eyes are not able to differentiate between the original and the stego-video. This project provides the most secure approach using two layer of encryption the first is performed on the secret data itself and another on the video file during data hiding. Receiver should know both decryption keys extracts secret message from the stego video. The experimental results show that MSE and PSNR values of ZOH method for different data sets are satisfactory.

In this project ZOH algorithm applied only on row wise, in future, this work can be extended to apply ZOH algorithm along row and column wise and this will double the hiding capacity, this requires both data embedding, and extraction algorithms needs to be enhanced. Braille character representation method used for converting ASCII character into 6-digits binary form, an alternative character representation method can be found or used that will take less binary bits to represents a ASCII character so that hiding capacity can be increased.

7. ACKNOWLEDGMENTS

It is our privilege to acknowledge thanking all the department personals and sponsors who gave us an opportunity to present a paper at this level. We would like to place our deep sense of gratitude to all reference papers authors for their beneficial papers, books and websites etc.

8. REFERENCES

[1] Abdelmgeid, Tarek, Al-Hussain, Shaimaa," New Image Steganography Method using Zero Order Hold Zooming, IJCA, Volume 133, Jan 2016.

[2] Swadhin, Kaustubh and Chirag, "Video Steganography Using Encrypted Payload for Satellite Communication",2017 IEEE Conference,978-1-5090-1613-6/17/31.00.

[3] Ramdhan J. Mstafa and Eman Abdelfattah, "Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC", 2017 IEEE International Conference, VOLUME 5, 2017.

[4] K.Rosemary Euphrasi and M. Mary Shanthi Rani, "A Comparative Study On Video Steganography in Spatial and IWT Domain", 2016 IEEE International Conference on Advances in Computer Applications (ICACA)".

[5] Achmad Solichin and Painem,"Motion-based Less Significant Frame for Improving LSB-based Video Steganography", 2016 International Seminar on Application for Technology of Information and Communication.

[6] Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale, "Audio-Video steganography," in IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems [Online]. pp. 1-6. 2015.

[7] C.C. Chang, Y. Liu and T.S. Nguyen, A Novel Turtle Shell Based Scheme for Data Hiding, Proc. Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing,2014.

[8] Monu U. Ragashe l, Sneha M. Ramteke2, " Combine use of steganography and visual cryptography in computer forensics", Discovery, Volume 18, Number51, May7, 2014.

[9] S. K. Moon and R. D. Raut, "Analysis of secured video steganography using computer forensics technique for enhance data security," Second International Conference on Image Information Processing, pp. 660-665, 2013.

[10] Keren Wang., Hong Zhao., Hongxia Wang., "Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value", vol.9, no.5, pp.741-751, 2014.

[11] Yun Cao., Xianfeng Zhao., Dengguo Feng. ,"Video Steganalysis Exploiting Motion Vector Reversion-Based Features", vol.19, no.1, pp.35-38, 2012.

[12] Pasumarthy Saradha and Bala Swamy, "Improving Image Data Hiding Capacity Scheme using Sudoku Puzzle in Color Images", International Journal of Engineering Research and Applications, Vol. 2, No. 3, pp. 2741-2744, May-June 2012.

[13] H. Aly, "Data hiding in motion vectors of compressed H. Aly, "Data hiding in motion vectors of compressed, "IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 14–18, Mar. 2011.

[14] Hung min Sun, Chi Yao Weng, Chin Feug Lee. "Anti-Forensics with steganography data embedding in digital images" IEEE journal on selected areas in Communication vol. 29. no.7 pp. 1392- 1403. August 2011.

[15] Hui-Lung Lee, Chia-Feng Lee and Ling-Hwei Chen, "A Perfect Maze Based Steganographic Method", The Journal of Systems and Software, Vol. 83, No. 12, pp. 2528-2535, July 2010.

[16] Stephan W. Thomas, Bram Adams, Ahmed E. Hassan and Dorothea Blostein" Validating the Use of Topic Models for Software Evolution", IEEE, 14 October 2010.

[17] Kamaldeep Joshi, Rajkumar Yadav and Sachin Allwadhi, "PSNR and MSE based investigation of LSB", ICCTICT, INSPEC Accession Number-16156341,2016.

[18] Soosan Beheshti , Masoud Hashemi and Ervin Sejdic , "Mean Square Error Estimation in Thresholding", IEEE,Volume-18,Issues-2,Ferbruary-2011.

[19] Brian Hahn and Daniel Valentine, "Essentials Matlab for Engineers and Scientist",4th edition, **e**Book ISBN: 9780080952116,2009.

[20] Anupam Kumar Garg, "Braille-8 The unified braille Unicode system: Presenting an ideal unified system around 8-dot Braille Unicode for the braille users world-over", IEEE, 6-9 Nov. 2016.