



A SECURE VIDEO STEGANOGRAPHY BASED ON OCTONARY PVD

M.KALYANI¹, D.SRIHARI²

¹PG Student, Dept. of ECE, SEAGI, Tirupati, Andhra Pradesh

²AssociateProfessor& HOD, Dept. of ECE, SEAGI, Tirupati, Andhra Pradesh



M.KALYANI



D.SRIHARI

ABSTRACT

Information security has become the area of concern as a result of widespread use of communication medium over the internet. Therefore different video steganography algorithms like least significant bit substitution (LSB), pixel value differencing (PVD) have been proposed to hide large amount of information inside a video but these methods provide less secure of information. So new Octonary PVD approach is proposing to improve the efficiency and Data security in video Steganography with high embedding capacity while concurrently sustaining the video quality.

In this approach, frames in video are selected using pseudo random order to hide the data and within a frame it performs pairing a pixel with all of its neighbors in all the eight directions to increase the embedding capacity and the number of bits embedded in each pixel is based on the nature of its region to enhance the perceptual quality. MATLAB tools are used to implement this proposing technique.

Keywords: Data hiding, video steganography, pseudo random sequence, Pixel value differencing.

©KY PUBLICATIONS

I.INTRODUCTION

In cryptography, the information is scrambled to transmit it securely but hacker may know the presence of secret data. In view of this, steganography provides the secure transmission of data without knowing even the presence of data. In steganography, the information is hidden inside any one of the cover file like image, video, audio etc. Image steganography hides the information inside an image which hides less information and others also can detect the artifacts if more information is hidden. So video steganography is proposed to hide much more information because video is a set of frames or still images. The artifacts are not detectable if a cover is a video.

The frames in the video act as still images so the image steganography techniques are used to hide information in each selected frame. The basic steganographic technique is LSB replacement [3] where every pixel least significant bit is replaced with the secret message bit and it results low hiding capacity. Other technique is PVD(Pixel Value Differencing)[1] where the difference is calculated between neighboring pixels to hide the secret information. It hides much information than LSB replacement. .Tri way PVD [4] is extension of PVD technique which increases the hiding capacity by calculating the difference of pixels in three directions. A novel technique is proposed to hide much more

information without degrading the quality of a cover file by calculating the difference of pixels in eight directions [2].

II. PROPOSED METHOD

A. Embedding Phase

The video is a collection of frames and in proposed method only some of the frames in video are selected based on PN sequence to provide more security. After selecting the frames OPVD embedding technique is directly applied to hide the secret information. Finally all the frames in video, both stego frames and original frames are added to form stego video which is similar to that of original video with hidden information.

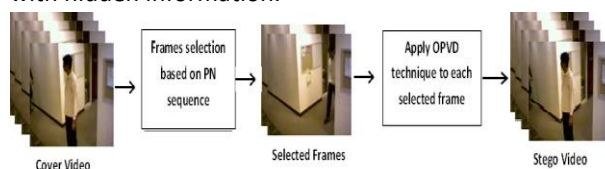


Fig 1: Block diagram of Video steganography Using OPVD

PN Sequence Generation: The steganography method (OPVD) is applied to each selected frame. The pseudo random sequence is generated to select the frames in video and based on tap weights the selection of frames is varied. The generation of PN sequence is shown in fig 1a. The PN sequence is generated using LFSR (Linear Feedback Shift Registers) and exclusive OR gate circuits [7].

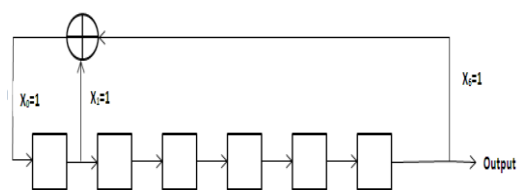


Fig 1a: Generation of PN sequence of length 63

The length of PN sequence must be greater than number frames in a given video. The 'n' numbers of shift registers generate PN sequence of length N.

$$N=2^n-1$$

The predefined tap weights for generating PN sequence are shown in table 1. For more security, the different taps also used to select the different frames.

Table 1: Tap weights for generating PN sequence of different lengths

n	N	Tap weights
5	31	[5 2 0] or [5 4 3 2 0]
6	63	[6 1 0] or [6 5 2 1 0]
7	127	[7 3 0] or [7 3 2 1 0]
9	511	[9 4 0] or [9 6 4 3 0]
10	1023	[10 3 0] or [10 8 3 2 0]
11	2047	[11 2 0] or [11 8 5 2 0]

B. OPVD Embedding Phase: In embedding phase of OPVD[8], the cover frame is divided into non-overlapping blocks of some size and each block is shifted by an angle of some degrees θ to obtain the shifted frame. That shifted image is used to hide the secret data to provide high security which improves the perceptual quality. Again the same shifted frame is divided into non-overlapping blocks of size 3×3 , each with nine pixels in pre-processing phase. The eight neighboring pixels form eight pixel pairs with the center pixel. The proposed approach hide more number of bits in edge areas than smooth regions [5, 6] so first the regions are identified to hide the data in region identification phase. Subsequently, the number of hiding bits in each pixel pair is determined by referring range table. After utilizing all the edge regions, smooth regions are used to hide the data. The range table is constructed by dividing [0 255] range into different levels. Data is hidden based on OPVD algorithm. The exceeded pixel values are adjusted to get the pixel values within the range in pixel readjustment phase. Finally the post processing phase is used to obtain the stego frame.

C. OPVD Extraction Phase: The block diagram for extracting the secret information from video is shown in Fig 3. The stego frame is taken as input and the same PN sequence generator is used here for getting the stego frames. Stego frames are used to extract the secret information by using OPVD technique extraction phase. After extracting the secret information from stego frames, all the frames are added to form an original video.

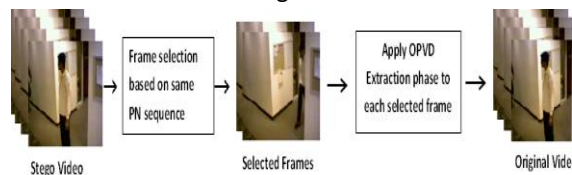


Fig 3: Extraction of video steganography using OPVD

III.RESULTS AND PERFORMANCE EVALUATION

Any Steganography technique is characterized mainly by two attributes, imperceptibility and capacity. Imperceptibility means the embedded data must be imperceptible to the observer (perceptual invisibility) and capacity means maximum number of bits can be hidden inside a cover file.

The perceptual imperceptibility of the embedded data is indicated by comparing the original image or video to its stego counterpart so that their visual differences, if any, can be determined. Additionally, as an objective measure, the Mean Square Error(MSE) and Peak Signal to

Noise Ratio (PSNR) between the stego frame and its corresponding cover frame are studied. The quantities are given as below,




$$MSE = \frac{1}{H * W} \sum_{i=1}^H (P(i,j) - S(i,j))^2$$

Where MSE is mean square error, H and W are height and width of a frame, P(i,j) and S(i,j) represent original frame and corresponding stego frame.

$$PSNR = 10 \log_{10}(L^2/MSE)$$

Where PSNR is peak signal to noise ratio and L is maximum gray level and is 255.

Table 2: Quality Parameter Analysis

Video file	No. of frames selected for hiding data	Results obtained using OPVD		Results obtained using PVD	
		PSNR	Payload(bits)	PSNR	Payload(bits)
News.wmv 	143	59.87	982696	57.59	982696
Car.avi 	143	57.74	1068000	55.09	1068000
	36	54.51	718560	52.89	718560
Rhinos.avi 	36	63.72	102240	62.87	102240
	60	53.44	1068000	50.46	1068000
	60	63.73	102240	61.07	102240

The proposed method is applied to uncompressed video formats only. From above table, the proposed technique hides much information inside a video without degrading the quality of a video compared to PVD technique.

IV.CONCLUSION

In this paper a new steganography method OPVD along with PVD and Triway PVD method was proposed, implemented and analyzed for a video. The proposed method selects video frames based on pseudo random order for security purpose and hides data by calculating the difference of pixels with center pixel in every hiding unit. The technique is applied to any video file formats. For video files like

MPEG the video needs to first decompress then the technique can be applied to the uncompressed video.

V.REFERENCES

- [1]. J. K. Mandal and Debashis Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain", International Journal of Information Sciences and Techniques (IJIST), Vol.2, No.4, July, 2012
- [2]. C. Balasubramanian, S. Selvakumar & S. Geetha "High payload image steganography with reduced distortion using octonary pixel pairing scheme" Springer Science+Business Media New York 2013

- [3]. Chan C-K, Cheng LM (2004) "Hiding data in images by simple LSB substitution". Pattern Recogn 37(3):469–474, 4
- [4]. Chang K-C, Chang C-P, Huang PS & Tu T-M (2008) "A novel image steganographic method using tri-way pixel-value differencing". J Multimedia 37(2):44, 6
- [5]. Zhang X & Wang S (2004) "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security". Pattern Recognit Lett 25:331–339, 46
- [6]. Yang CH, Weng CY, Wang SJ & Sun HM (2008) "Adaptive data hiding in edge areas of images with spatial LSB domain systems". IEEE Trans Inf Forensic Secure 3(3):488–497, 45
- [7]. Alka Sawlikar & Manisha Sharma, "Analysis of different Pseudo Noise sequences", International Journal of Computer Technology and Electronics Engineering (IJCTEE), Volume 1, Issue 2, OCT 2011
- [8]. V. Navya, T. Ravi Kumar Naidu & T. V. S. Gowtham Prasad, "Novel and Secure Image Steganography Using OPVD with High Capacity", International Journal of Engineering Trends and Technology (IJETT) – Volume 14 Number 3 – Aug 2014

AUTHORS BIOGRAPHY

Ms. M.Kalyani, P.G Student, Dept of ECE, Siddartha Educational Academy Group Of Institutions Integrated campus, C.Gollapalli, Tirupati received B.Tech in Electronics and Communication Engineering from YITS, Tirupati. Interesting Areas: Digital Signal Processing, Image Processing, Embedded Systems, Digital Communications.

D.Srihari is an Associate Professor & HOD, Dept of ECE, SEAGI, Tirupati. Obtained B.E degree in electronics and Communication Engineering from University of Madras, Chennai. M.E degree in Applied electronics from university of Madras, Chennai. M.E degree in Electronics and Instrumentation from Andhra University College of Engineering, Andhra University.
