Volume 6, Issue 1, January 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Information Hiding Techniques for Data Security Using FPGA

A. A. Prabhune, S. M. Joshi

Electronics and Telecommunications, Pune Institute of Computer Technology,
Pune, Maharashtra, India

Abstract--Steganography is defined as hiding the secret message within a cover-medium in such a way that others cannot discern the presence of the hidden message. The main aim of paper is to implement a data embedding algorithm which is capable of hiding more secret data while keeping the stego-image quality degradation imperceptible. In this paper, a video is taken as embedding media, then image frames and audio is extracted from video. Image frames are selected by using password entered for hiding data. The Diamond Encoding algorithm as reference for hiding the secret image and text file and DCT algorithm for hiding secret audio file. Original frame is replaced by stego-frame and stego video is form. At the receiver end user enters the password, if that password is correct then that authorize user can be able to extract data from video frame.

Keywords—Stegnography, stego-image, Diamond Encoding, DCT,stego-frame and stego video.

I. INTRODUCTION

Digital representation of information makes it possible to illegally produce an unlimited number of perfect copies. Especially for audio and video files, industry is strongly interested in hiding copyright information or serial numbers in the data in order to enforce copyright laws. Interest for information hiding techniques has grown in the last few years, but it should be kept in mind that steganography is by no means a new discipline. In fact, it has been excessively used throughout history.

In a large number of applications, it is desired that the communication to be done in secrete. Data should be more secured while transmitting it. Also, the steganography is the latest technique to send data safely to receiver. Such secrete communication ranges from the obvious cases of bank transfers, corporate communications, and credit card purchases, on down to a large percentage of everyday email. Steganography aims at hiding any data in a cover carrier in such a way that only receiver knows its existence. Steganography is the ancient art of embedding a secret message into a seemingly harmless message. A data hiding scheme in digital images with the diamond encoding by pixel value adjustment is used. This method is the extension of the exploiting modification direction (EMD) embedding scheme. The diamond encoding provides an easy way to produce a more perceptible result than those yielded by simple least-significant-bit substitution methods. The embedded secret data can be extracted without the original cover image.

II. BLOCK DIAGRAM

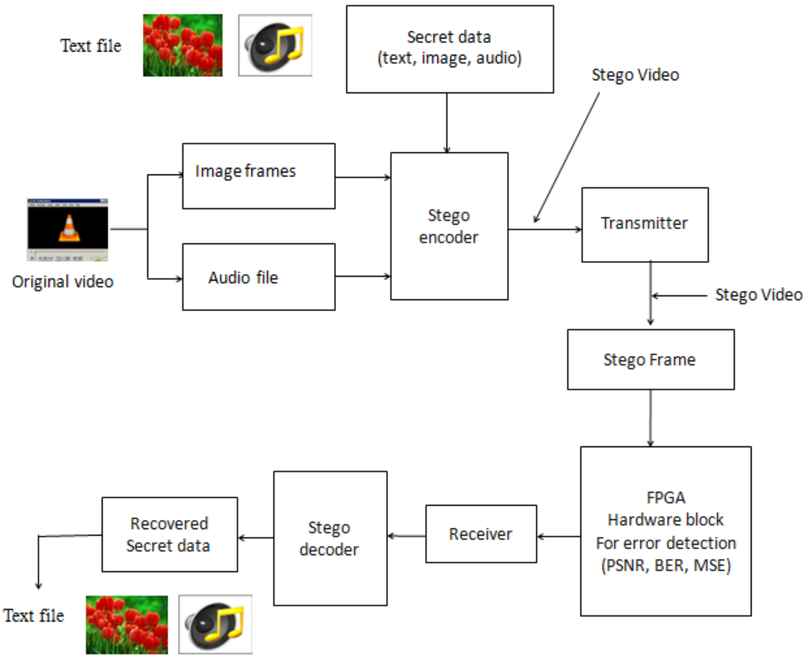


Fig 2.1 Block diagram of data hiding and recovering

This data or the video is needed to embed the secret data in it. The secrete message can be text, image or audio. This secret data is embedded into image frames of this video file with some password.

Stego-Encoder block deals with hiding data and ”covered writing”.This block encode required data to be sent. Select the best suited and most secured method for transmitting it to it’s destination and no one except sender will detect it.This primarily help to hide the fact that a communication is taking place between two parties. The sender embeds secret data of any type(image, text etc) using a key in digital cover file to produce a stego file, in such a way that an observer cannot detect the existence of the hidden message. The secrete message has to be converted into the binary data to hide it in the frames of video file.To minimize the difference between the original file and the one obtained after embedding the hidden data. Depending upon the application and transmission medium,will have to choose the appropriate encoding styles. Stego-video is the output of the stego-encoder block, which contains original video plus secrete data(text or audio or image).From this stegovideo the stego frame is selected by using the same key as that of at the transmitter and then this stego frame is given to the FPGA(Field Programmable gate array) block for further processing. This ensures that only authorized users are able to access the contents available in digital media.So,this block is for information security.In this block,we will measure the peak signal to noise ratio,mse, bit rate error etc. If these factors are upto the desired level then only it will allow,to transmit the stego object to the destination, Otherwise it won’t send the stego object to its destination.Hence, transmission is very much secured after checking these factors. Also it will see that our stego object is up to the level of the transmission and it is not distorted. Stego Decoder block deals with securing the original data to be captured by only authorized person. At the receiver end, the key of frame selection using which it will decode the original video and secret message hidden and use the decoding algorithm that of opposite to encoding. The key is known to only the desired receiver and others will unable to known the secured data. Hence, video steganography improves security. Also, this algorithm must be robust and are embedding in to video file so it is difficult for unauthorized person to identify the data is hidden in to it.so at the output of this block secret data obtained as it is, as that of transmitted by sender.

2.1 Steganography System

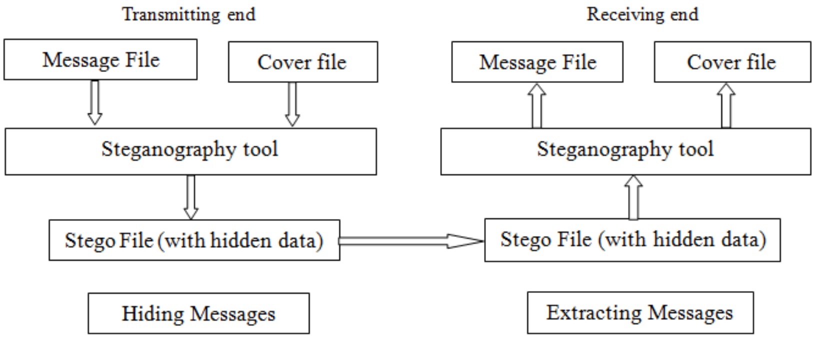


Fig 2.2 General Steganography System

2.2 Image Steganography Techniques

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain.

2.2.1 Image (spatial) domain

Image also known as spatial–domain techniques embed messages in the intensity of the pixels directly.Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as “simple systems”.

2.2.2 Transform Domain

Transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image. Steganography in the transform domain involves the manipulation of algorithms and image transforms. These methods hide messages in more significantareas of the cover image, making it more robust.

2.3 Steganalysis

The art of detecting steganography is referred to as steganalysis. To put it simply steganalysis involves detecting the use of steganography inside of a file. Steganalysis does not deal with trying to decrypt the hidden information inside of a file, just discovering it. There are many methods that can be used to detect steganography such as:

i) Viewing the file and comparing it to another copy of the file found on the Internet (Picture File.)There are usually multiple copies of images on the Internet, so you may want to look for several of them and try and compare the suspect file to them. For example if you download a JPEG and your suspect file is also a JPEG and the two files look almost identical apart from the fact that one is larger than the other, it is most probable your suspect file has hidden information inside of it.

ii) Listening to the file. This is similar to the above method used for trying to manually detect steganography in picture files. If you are trying to detect hidden information inside of a MP3 audio file you will need to find an audio file to compare it to that uses the same compression (MP3.) The same applies to finding hidden information inside Picture files.

III. ALGORITHMS USED IN PAPER

1. Diamond Encoding For hiding image as well as text file as a secret data into the image frame of video.
2. DCT algorithm for hiding audio into the image frame of video.

3.1 Flowchart for Data Embedding

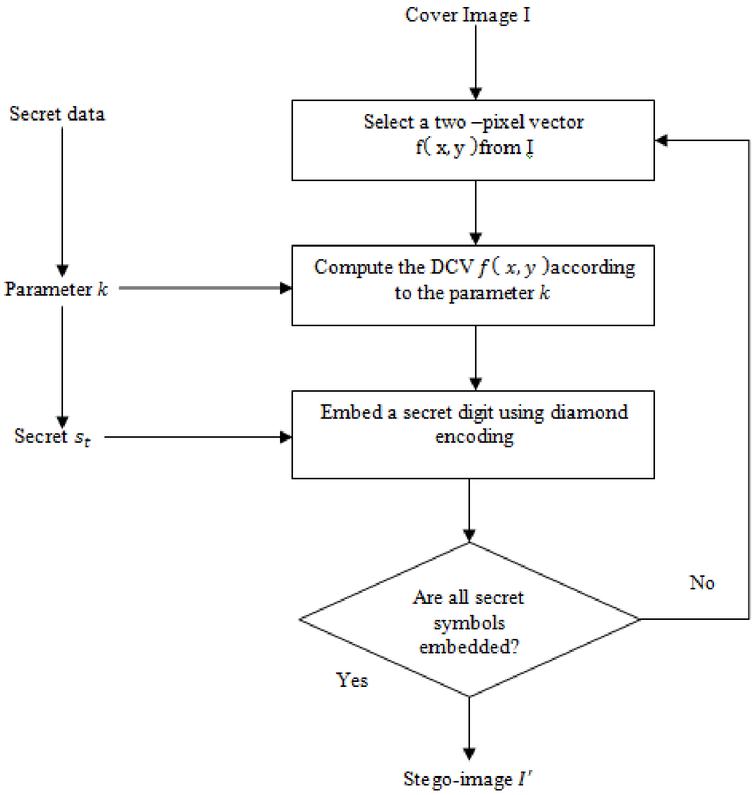

Cover Image I
Secret data
Select a two –pixel vector f(x, y)from I
Parameter k
Compute the DCV f(x, y)according to the parameter k
Secret s_t
Embed a secret digit using diamond encoding
Are all secret symbols embedded?
No
Yes
Stego-image I'

Fig 3.1: Data Embedding Process

3.2 Flowchart for Data Extraction

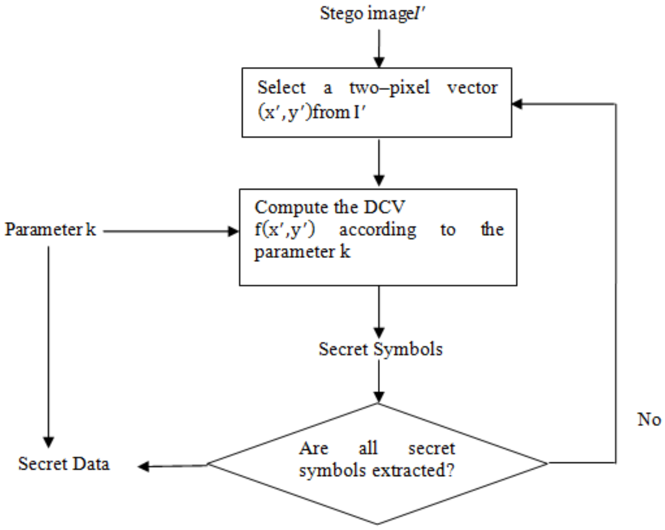

Stego imageI'
Select a two–pixel vector (x′,y′)from I′
Compute the DCV f(x′,y′) according to the parameter k
Parameter k
Secret Symbols
Are all secret symbols extracted?
No
Secret Data

Fig 3.2: Data Extraction Process

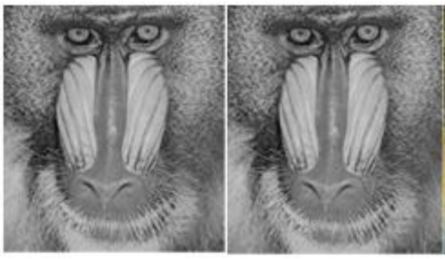
IV. SIMULATION RESULTS

(a) Lenna

(c) Stego-Lenna

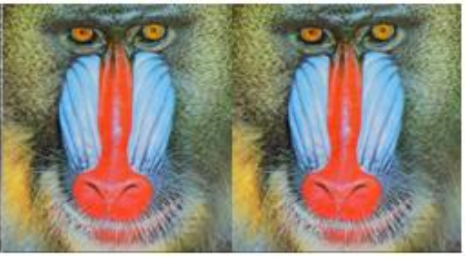
(e) Lenna

(g) Stego-Lenna



(b) Baboon (d) Stego-Baboon

Figure 4.1: Test images(a)–(b) and stego-images(c)–(d). For grey



(f) Baboon (h) Stego-Baboon

Figure 4.2: Test images(e)–(f) and stego-images(g)–(h). For colour

4.1 Results obtained for Embedding Image

Table 4.1 Results for Embedding Image

Video file	Size	Secret Image		EC (bits)	ER (bpp)	PSNR (dB)	MSE	BER	Correlation
		Format	Size						
.AVI	3.41MB	.bmp	190X190	288800	2.67	52.7031	0.348957	0.777	0.99
.WMV	5.6MB	.bmp	190X190	288800	2.67	53.1998	0.311245	0.655	1
.MP4	4.2MB	.bmp	190X190	28800	2.67	53.7446	0.274548	0.6006	1

4.2 Results obtained for Embedding Audio

Table 4.2 Results for Embedding Audio

Video file	Size	Secret Audio		EC (samples)	ER (spp)	PSNR (dB)	MSE
		Format	Size				
.AVI	3.42MB	.wav	236kb	212929	6.49	44.89	2.1705

4.3 Improved Results of this Algorithm

Table 4.3 Improved Results of this Algorithm

Diamond Encoding			Proposed method		
Parameter k	PSNR (dB)	Payload (bpp)	Parameter k	PSNR (dB)	Payload (bpp)
1	52.1	1.16	1	49.13	1.85
2	47.8	1.85	2	45.02	2.32
3	45.0	2.32	3	42.78	2.68
4	42.9	2.68	4	41.57	2.96

V. CONCLUSIONS

A Novel data hiding Diamond Encoding scheme in digital images is successfully implemented for video steganography.A DCT based Hiding algorithm is successfully implemented for audio hiding.In this paper audio wav file is converted into number of samples samples using in built functions in MATLAB. The most important point for DCT technique is changing the DCT coefficients will cause unnoticeable visual Artifices, they do cause detectable statistical changes.Diamond Encoding technique has high data embedding capacity in the range of 2 bpp.For steganography, the hiding capacity, visual quality of recovered image and security are three important parameters. It is seen that the original video and the final embedded video appear to be identical to the human eye. This experiment has been carried on bmp images. In this experiment, notational system used to convert secret data. The most important point for this technique is hiding a secret digit into two cover pixels and thereby achieving high embedding capacity of 2 bpp with very less distortion to original image. It is seen that this scheme is better than the other existing schemes in terms of payload and stego-image quality. A Diamond Encoding Steganography program can be customized for each user. Thus it guarantees Secret Internet communication. Steganography is a very strong information security technique, it can be applied to areas other than secret communication. FPGA is used as a hardware block to checks the all the parameters such as MSE, PSNR, NCC, BER etc. of received data which improves the security further.In conclusion, as more emphasis is placed on the areas of copyright protection, privacy protection, and surveillance,we believe that steganography will continue to grow in importance as a protection mechanism.

The software, **"**VIDEO STEGANOGRAPHY**",** employs an huge embedding capacity as it contains to many frames for data hiding , so that it can hide more no. of images ,large text files and even audio files while keeping the visual quality of video very high. The PSNR value for hiding image and audio is 52.70 dB and 44.89 dB respectively. The correlation between original and recovered data are 0.99 (approx. correlation =1) which add another layer of data security.The result proves that this embedding algorithm embeds the data with a very less distortion. Also the hidden data is recovered without much loss of data.

REFERENCES

[1] "Fundamentals of Digital Image Processing", A. K. Jain,Pearson Education

[2] Ruey-Ming Chao, Hsien-ChuWu, Chih-Chiang Lee, and Yen-Ping Chu "A Novel Image Data Hiding Scheme with Diamond Encoding," Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2009 .

[3] C.-M. Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "A High Quality Steganographic Method With Pixel-Value Differencing and Modulus Function," *The Journal of Systems and Software*, vol. 81, no. 1, pp. 150–158, 2008.

[4] X. Zhang and S. Wang, "Efficient steganographic embeddingby exploiting modification direction," *IEEE Communications Letters*, vol. 10, no. 11, pp. 781–783, 2006.

[5] P. L. Lin, C.-K. Hsieh, and P.-W. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery," *Pattern Recognition*, vol. 38, no. 12, pp. 2519–2529, 2005.

[6] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[7] D.-C. Lou and J.-L. Liu, "Steganographic method for secure communications," *Computers and Security*, vol. 21, no. 5, pp.449–460, 2002.

[8] Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure datahiding scheme for binary images," IEEE Transactions on Communications, vol. 50, no. 8, pp. 1227–1231, 2002.

[9] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proceedingsof the International Workshop on Multimedia and Security*, pp.27–30, Ottawa, Canada, October 2001.