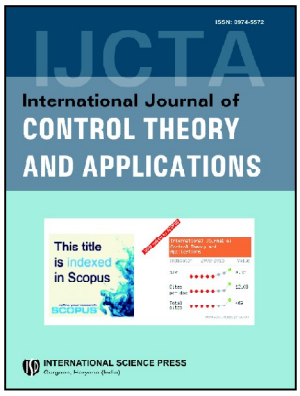


International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 10 • 2017

An Advanced and More Secure Steganography Algorithm for Hiding Image Over Video Using Various Algorithm in MATLAB

Navneet Kaur[1] and Bhupinder Kaur[2]

[1] *ME(CSE), Chandigarh University,Gharuan, Mohali,* E-mail: navneetsamplay9@gmail.com
[2] *Associate Professor, CSE, Chandigarh University,Gharuan, Mohali,* E-mail: erbhupinderkaur@gmail.com

Abstract: Steganography is a technique that is used to transmit hidden information by modifying an audio signal in an imperceptible manner and it is an art of hiding information in ways that avert the revealing of hiding messages. The secure data that is transmission over internet is achieved using Steganography. Video files are generally a collection of images. So most of the presented techniques on images and audio that can be applied to video files too. The great advantages of video are the large amount of the data that can be hidden inside and the fact that it is a moving stream of images. The network that provides a method of communication to distribute information to the masses. With the growth of data communication over computer network and the security of information has become a major issue. Steganography and the cryptography are the two different data hiding techniques. And cryptography, on the other hand obscures the content of the message. We propose a high capacity data embedding approach that is the combination of Steganography by using DWT and SVD algorithms.

Indexed Terms: Steganography, Data hiding, File Security, Frame Extraction, Consumer Videos, DWT, SVD etc.

INTRODUCTION

Text, images, audio, and video that can be represented as digital data. The explosion of Internet applications that leads people into the digital world, and communication via the digital data becomes recurrent. However, new issues also are arise and have been explored, such as data security in digital communications, copyright protection of the digitized properties and invisible communication via through digital media, etc. but rapid development of the Internet and the digital information revolution that caused significant changes in the global society that is ranging from the influence on the world economy to the way of people nowadays will communicate.[1] Broadband communication networks and multimedia data that is available in a digital format (images, audio, video) opened many challengesand opportunities for the innovation. Versatile and simple-to-use software and decreasing the prices of digital devices (e.g. digital photo cameras, camcorders, portable CD , mp3 players, DVD players, CD and DVD recorders, laptops, PDAs) have made it possible for the consumers side from all over the world to create, edit and exchange multimedia data. [1] [3] [7] In steganography, the object of communication that is the hidden message and the cover data are only the means of sending it. Secret information as well as cover the data can be any multimedia data like text, image, audio, video etc The objective of this work is to develop Compressed

Video Steganographic Scheme that can provide provable security with high computing speed, that embedded secret the messages into images without producing noticeable changes. Here we are embedding data in video frames. In the following sections, first a brief description of concepts and available methods is presented that is followed by a detailed description of proposed techniques and their implementation results. [6]

DWT

Discrete wavelet transform (DWT) is implementation of the wavelet transform that is using a discrete set of the wavelet scales and translations for obeying some defined rules. In other words, this transform decomposes the signal into the mutually orthogonal set of the wavelets, which is the main difference from the continuous wavelet transform (CWT), or its implementation for discrete time series sometimes called discrete-time continuous wavelet transform (DT-CWT).Wavelet can be constructed from a scaling of function which describes its scaling properties.

SVD

Singular value decomposition take a rectangular matrix of the gene expression data (defined as B, where B is n x p matrix) in which the n rows represents genes, and the p columns represents the experimental conditions. The SVD theorem states:

Bnxp= Unxn Snxp VTpxp

Where

UTU = Inxn

VTV = Ipxp (i.e. U and V are orthogonal)

The columns of U are the left singular vectors that are (gene coefficient vectors); S (the same dimensions as B) has a singular values and diagonal (mode amplitudes); and VT has rows are the right singular vectors (expression level vectors). SVD represents an expansion of the original data in coordinate system where the covariance matrix is diagonal.

Calculating the SVD consists of the finding the eigenvalues and eigenvectors of BBT and BTB. The eigenvectors of BTB make up the columns of the V , the eigenvectors of BBT make up the columns of U. Also, the singular values in S are square roots of the eigenvalues are from BBT or BTB. The singular values that are the diagonal entries of the S matrix and are arranged in the descending order. Singular values are always real numbers. If the matrix B is a real matrix, then U and V are also real.

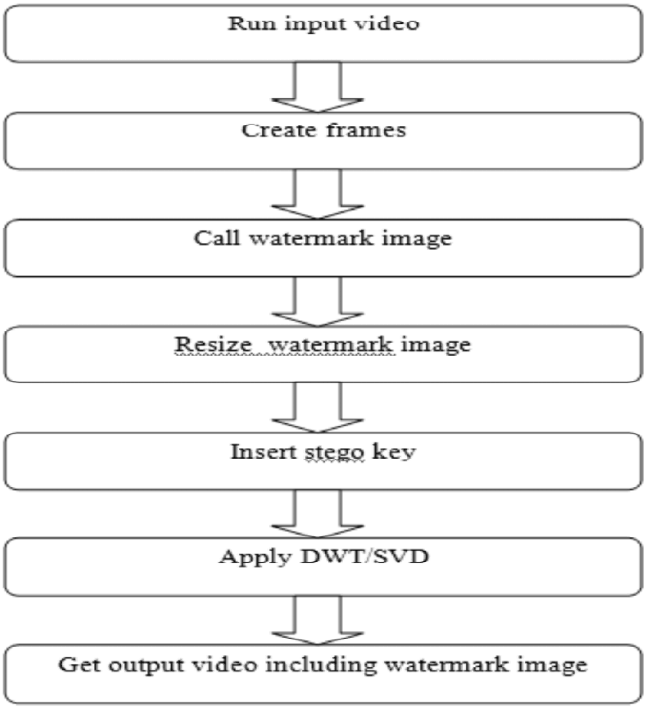
PROBLEM FORMULATION

Steganography techniques can be implemented easily but if someone tries to find out the tricks after knowing that someone using the stego video file then there are the good chances of finding out the hidden information. In order to avoid this some hybrid system can be used. In such a way that even through someone finds out one technique is used only on the few frames that contains different kind of stegnographic and hence total secrete message is not delivered. Issue occurs when the size of secrete image gets increased from the input images which causes problems over network.

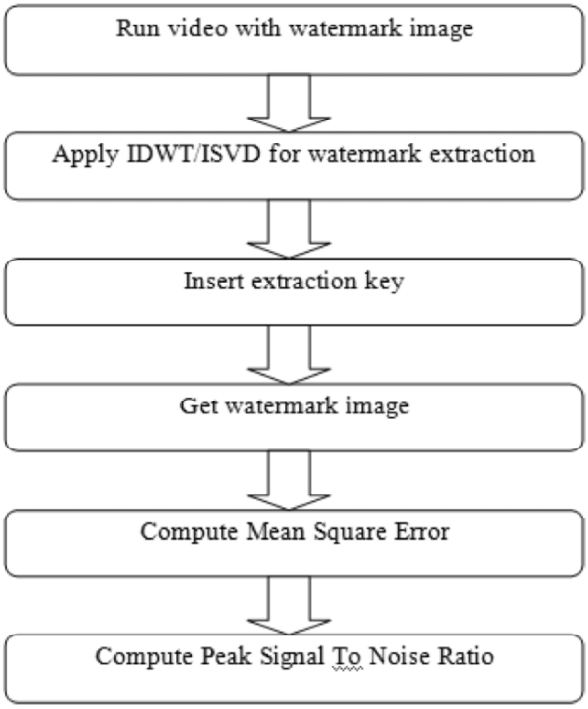
OBJECTIVES

1. To develop the more robust and secure algorithm for steganography.
2. To calculate computation time for algorithm.
3. To reduce error ratio and to improve peak signal to noise ratio

METHODOLOGY



Figure(i): Embedded Process



Figure(ii): Extraction Process

RESULTS

As per the implemented algorithm, results below are obtained. The steps of the implemented code are given below.

Figure 1: Opening GUI

First code will be open;GUI design will appear when the program starts. The GUI will be used to interact with the videos in which we have to hide data.

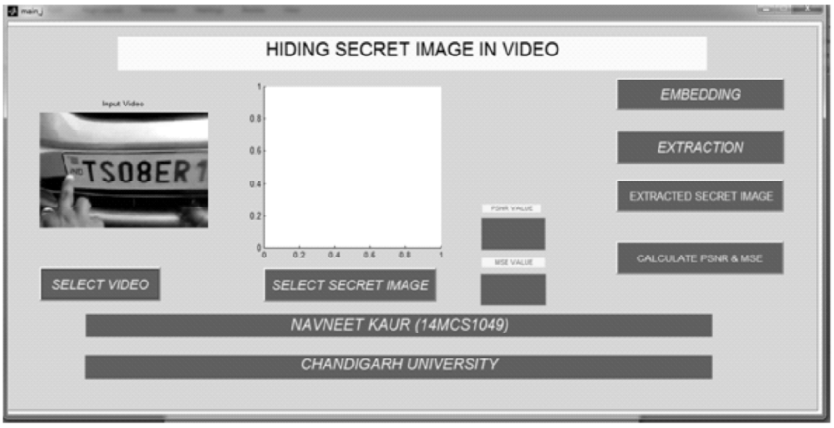


Figure 2: Input video

In this part of GUI, the video which will be selected will run in GUI player. Video is played to collect frames for hiding the data.

Figure 3: Hiding Image

This part of GUI will appear when some image will be called for hiding in video.

Figure 4: Hiding Image in frame

In this part the pop up window will appear. In this pop up window the image will be hiding in the frame which frame will be selected

Figure 5: Embedding Image

Figure 6: Extracting video

In this section, the video will be playing in matlab video player, the video will be played for extraction purpose.

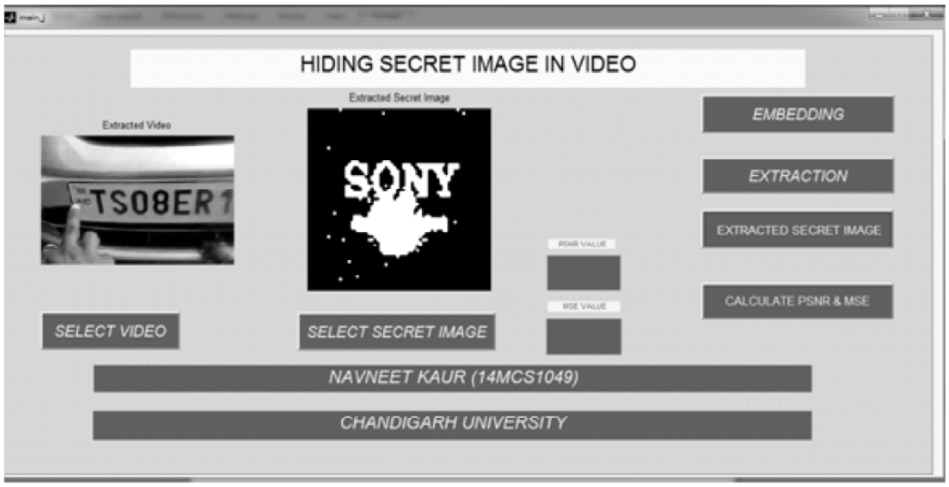


Figure 7: Extracting Image

In this section the image will be embedded in the video.

Figure 8: PSNR & MSE Extracted

The button on the GUI will be clicked and peak signal to noise ratio and mean square error will appear in GUI window.

The Graphs for PSNR and MSE are given below.

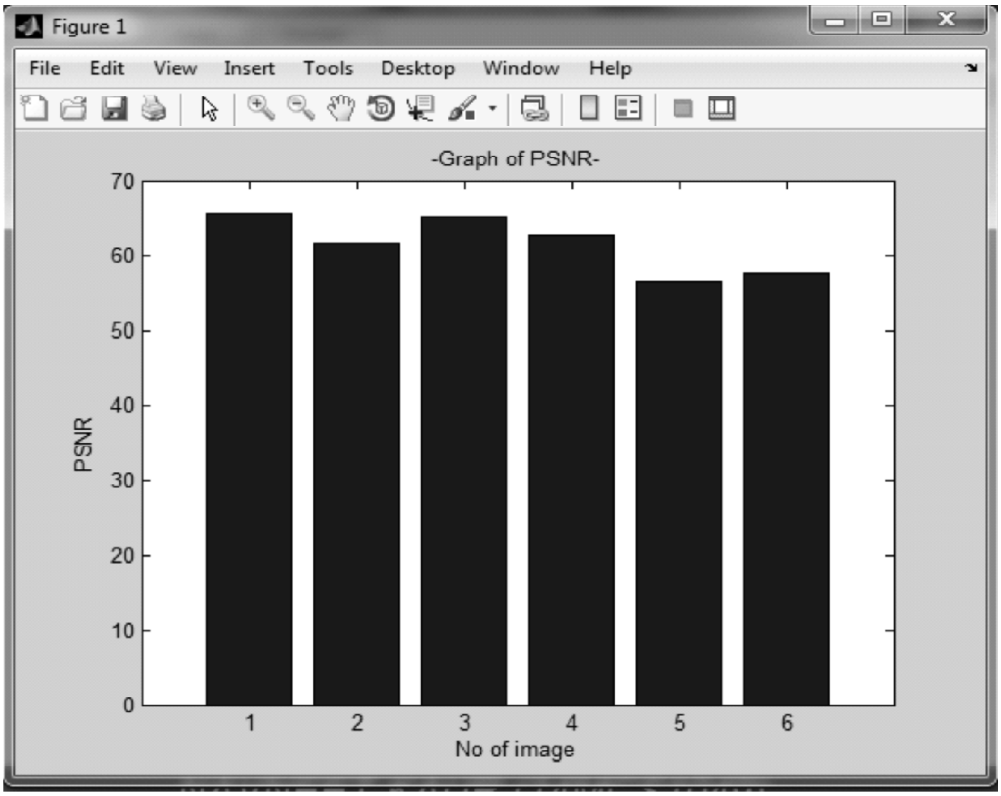


Figure 9: Graph of PSNR

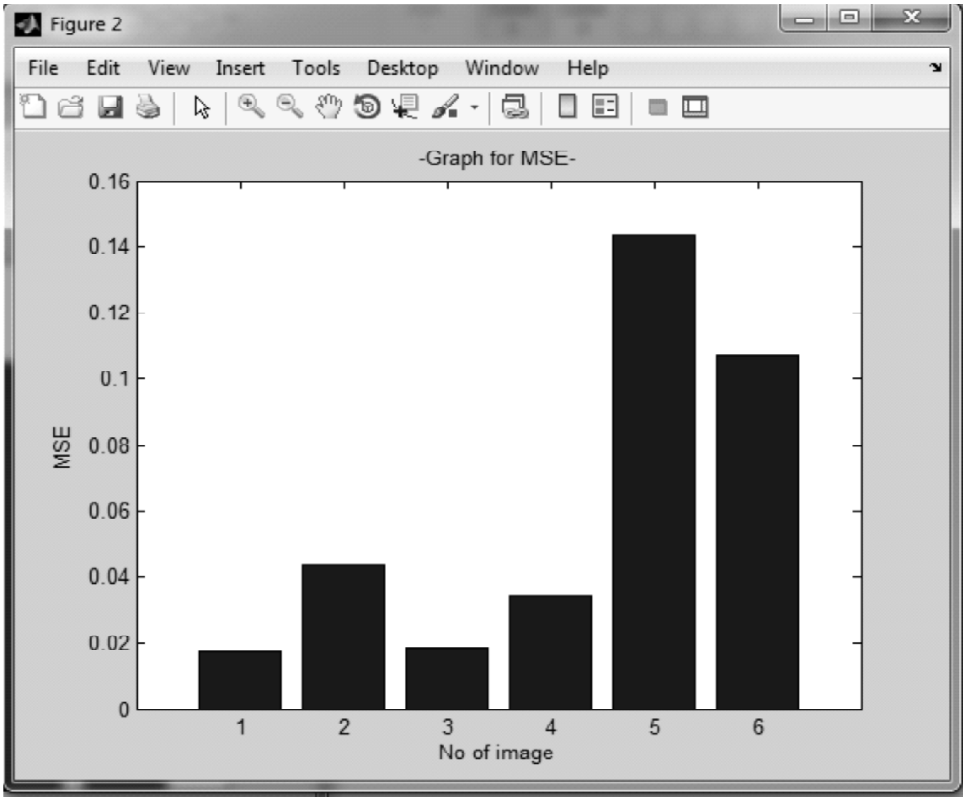


Figure 10: Graph of MSE

PSNR and MSE are computed using mathematical formulas, the graph for PSNR and MSE are given above and table for both is given below.

S.No	*Input video file name*	*Input image name*	*PSNR*	*MSE*	*Elapsed Time(sec)*
1.	VIDEO.avi	logo(6)	63.8029	0.0273	1.6079
2.	VIDEO.avi	logo(8)	61.8383	0.0429	0.3026
3.	VIDEO.avi	Logo	65.5248	0.0183	0.2898
4.	VIDEO.avi	wmrk	62.8369	0.0341	0.3220
5.	VIDEO.avi	wmrk1	56.5992	0.1434	0.3687
6.	VIDEO.avi	wmrk2	57.8709	0.1070	0.3164

CONCLUSION

The Steganography is used for secrete communication. In this paper High Capacity and Security Steganography using different algorithms is reviewed. The DWT and SVD technique is best suited algorithm for the watermarking or steganography. These techniques are used for video watermarking, audio watermarking and other security applications.

FUTURE SCOPE

This design is easily understandable. In future someone can use to implement some other algorithm to implement the same design.PSNR and MSE can also be improved and some more parameters for quality check could be implemented.

REFERENCES

[1] MamtaJuneja, Parvinder Singh Sandhu, " Information Hiding using Improved LSB Steganography and Feature Detection Technique" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[2] Mamta.Juneja and Parvinder S. Sandhu, "An improved LSB based Steganography with enhanced Security and Embedding/ Extraction", 3rd International Conference on Intelligent Computational Systems (ICICS'2013) January 26-27, 2013 Hong-Kong (China).

[3] Pritish Bhautmage, Prof. AmuthaJeyakumar, AshishDahatonde, "Advanced Video Steganography Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January - February 2013, pp.1641-1644.

[4] Poonam V Bodhak, Baisa L Gunjal, "Improved Protection In Video Steganography Using DCT & LSB", ISSN: 2277-3754 International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[5] Balaji R, Naveen G, "Secure data transmission using video Steganography", 2011 IEEE International Conference on Electro/ Information Technology (EIT), pp. 1-5, 15-17 May 2011.

[6] Saurabh Singh and GauravAgarwal, "Hiding image to video: A new approach of LSB Replacement", International Journal of Engineering Science and Technology, Vol. 2(12), pp. 6999-7003, 2010.

[7] NielsProvos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography", University of Michigan, IEEE 2003.