IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DWT BASED DATA HIDING USING VIDEO STEGANOGRAPHY

S.Kamesh*, K.Durga Devi, S.N.V.P.Raviteja
Assistant Professor, ECE Department, Sasi Institute of Technology & Engineering, Tadepalligudem, Andhra Pradesh, India

DOI: 10.5281/zenodo.556248

ABSTRACT

Now a days transfer of information from one system to another system needs more security especially in some applications like militaty etc. It can sent to through different mediums such as audio,video. So to transmit information in secured manner, **Steganography** is used. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos meaning "covered, concealed, or protected", and graphein meaning "writing". But we cannot transmit more amounts of hidden data. So we go to the video Steganography using DWT method. In this paper, we propose a steganography technique which embeds the secret messages in frequency domain. According to different users demands on the embedding capacity and quality, the proposed algorithm consists of converting video into frmaes and embedding each secured data within each frame. So more amount of information hide in a single video. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform.

KEYWORDS: Steganography, Discrete Wavelet Transform (DWT), Secrete message, Secure key.

INTRODUCTION

The term digital image refers to processing of a two dimensional picture by a digital computer. In a broader context, it implies digital processing of any two dimensional data. A digital image is an array of real or complex numbers represented by a finite number of bits. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory. This digitized image can then be processed and/or displayed on a high-resolution television monitor. For display, the image is stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25 frames per second to produce a visually continuous display.

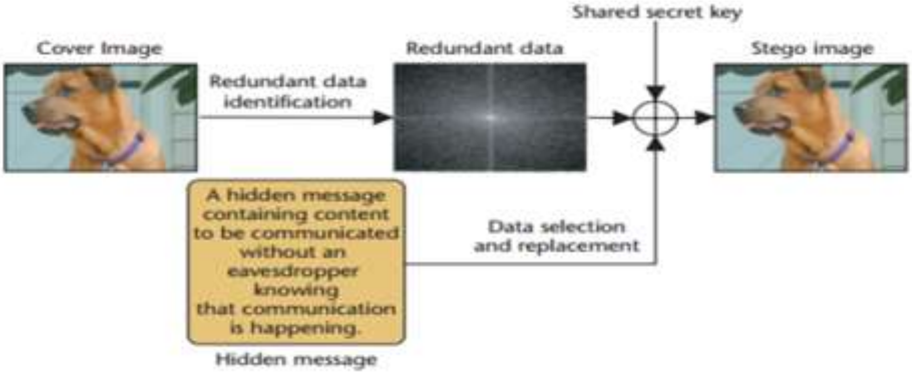

Shared secret key
Cover Image
Redundant data identification
Redundant data
Stego image
A hidden message containing content to be communicated without an eavesdropper knowing that communication is happening.
Data selection and replacement
Hidden message

Figure-1: Basic Steganography Model

It is very essential to transmit important data like banking and military information in a secure manner. Video Steganography is the process of hiding some secret information inside a video. The addition of this information to the video is not recognizable by the human eye as the change of a pixel color is negligible. This paper aims to provide an efficient and a secure method for video Steganography. The proposed method creates an index for the secret information and the index is placed in a frame of the video itself. With the help of this index, the frames containing the secret information are located. Hence, during the extraction process, instead of analyzing the entire video, the frames containing the secret data are analyzed with the help of index at the receiving end. When steganography by this method, the probability of finding the hidden information by an attacker is lesser when compared to the normal method of hiding information frame-by-frame in a sequential manner. It also reduces the computational time taken for the extraction process.

LITERATURE REVIEW

Anderson RJ, Petitcolas FAP[1] proposed steganography is andwhat it can do. We contrast it with the related disciplines ofcryptography and traffic security, present a unified terminologyagreed at the first international workshop on the subject, andoutline a number of approaches—many of them developed to hideencrypted copyright marks or serial numbers in digital audioor video. We then present a number of attacks, some new, onsuch information hiding schemes. This leads to a discussion ofthe formidable obstacles that lie in the way of a general theoryof information hiding systems.

J. Fridrich Proposed the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image,audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goalhere is always to conceal the very existence of the embedded data. [2] Steganography has various useful applications. However,like any other science it can be used for ill intentions.

Bailey K, Curran K [8] proposed a stegnography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image,audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goalhere is always to conceal the very existence of the embedded data. Steganography has various useful applications. However,like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies,government and through intellectual pursuit. Steganography's ultimate objectives, which are undetectability, robustness(resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors thatseparate it from related techniques such as watermarking and cryptography.

BLOCK DIAGRAM

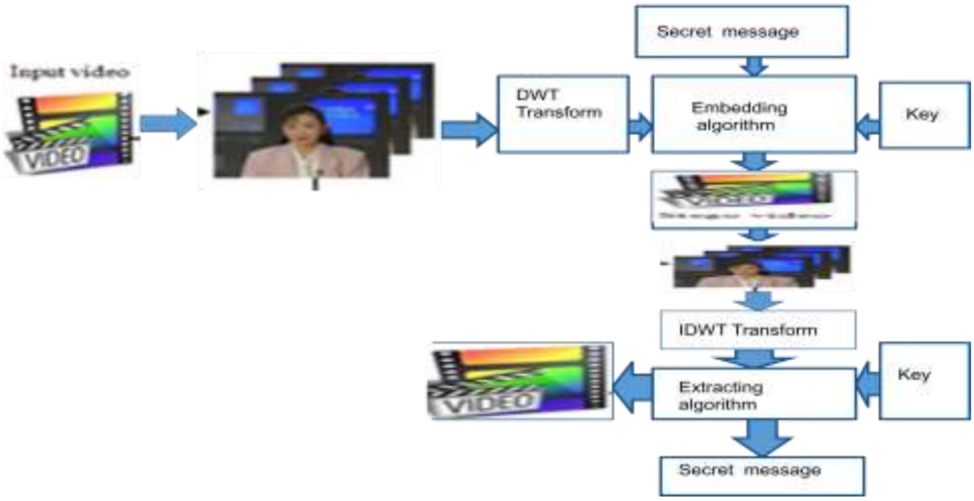


Figure-2: Block Diagram

The block diagram involves input video, frames, DWT transform. By using embedding algorithm method we are obtaining the stego video with the help of a secret key and calculating the peak signal to noise ratio. And at the receiving end extract the input video and secret message using extracting algorithm.

Video:

Video is an electronic medium for the recording, copying, playback, broadcasting, and display of moving visual media. Different types of video formats are there. Those are AVI (Audio Video Interleave), FLV (Flash Video Format), WMV (Windows Media Video), and MOV (Apple QuickTime Movie), MP4 (Moving Pictures Expert Group 4).

Frames:

Frame rate, (expressed in frames per second or FPS) is the frequency (rate) at which consecutive images called frames are displayed in an animated display. The term applies equally to film and video cameras, computer graphics, and motion capture systems. Frame rate may also be called the frame frequency, and be expressed in hertz.

DWT Transform:

Capacity and robustness of the Information- Hiding system features. The Discrete Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients that are generated by taking half of the difference of the same two pixels. The four bands obtained are LL, LH, HL, and HH.

Key:

Some specific key is used to hide the data. That specific key is too used to store the data as a background of the frames. They are having several number of keys are used. That type of similar keys is numerical bits, alphabets and etc.

IDWT Transform:

Once we arrive at our discrete wavelet coefficients, we need a way to reconstruct them back into the original signal (or a modified original signal if we played around with the coefficients). In order to do this, we utilize the process known as the inverse discrete wavelet transform.

Wavelet Transform

The wavelet transform is similar to the Fourier transform (or much more to the windowed Fourier transform) with a completely different merit function. The main difference is this: Fourier transform decomposes the signal into sins and cosines, i.e. the functions localized in Fourier space; in contrary the wavelet transform uses functions that are localized in both the real and Fourier space. Generally, the wavelet transform can be expressed by the following equation: where the * is the complex conjugate symbol and function ψ is some function. This function can be chosen arbitrarily provided that it obeys certain rules. As it is seen, the Wavelet transform is in fact an infinite set of various transforms, depending on the merit function used for its computation. This is the main reason, why we can hear the term “wavelet transforms” in very different situations and applications. There are also many ways how to sort the types of the wavelet transforms. Here we show only the division based on the wavelet orthogonality. We can use *orthogonal wavelets* for discrete wavelet transform development and *non-orthogonal wavelets* for continuous wavelet transform development.

$$F(a,b) = \int_{-\infty}^{\infty} f(x)\, \psi^{*}_{(a,b)}(x)\, \mathrm{d}x$$

Types of Wavelets

1. Haar Wavelets
2. Daubechies Wavelets
3. Biorthogonal Wavelets
4. Coiflets Wavelets
5. Symlets Wavelets
6. Morlet Wavelets
7. Mexican Hat Wavelets
8. Meyer Wavelets

Discrete Wavelet Transform

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

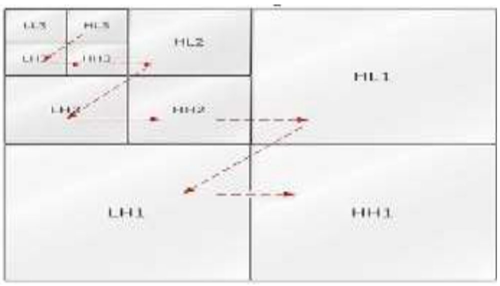
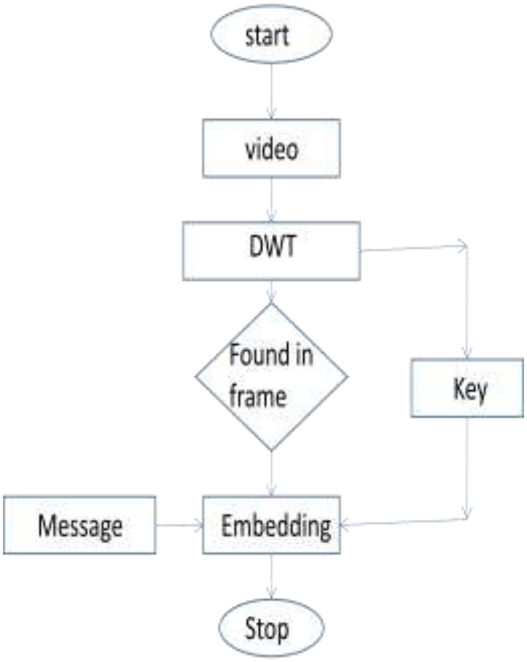


Figure-3: Wavelet Decomposition

FLOWCHART

First the video is taken as an input. Then video is converted into frames. Now, apply the DWT method for the selected frame for the conversion of frequency domain to spatial domain. Then, embedded the secret messge and selected frame with some specified key by the help of LSB algorithm. So, we get the stego video.



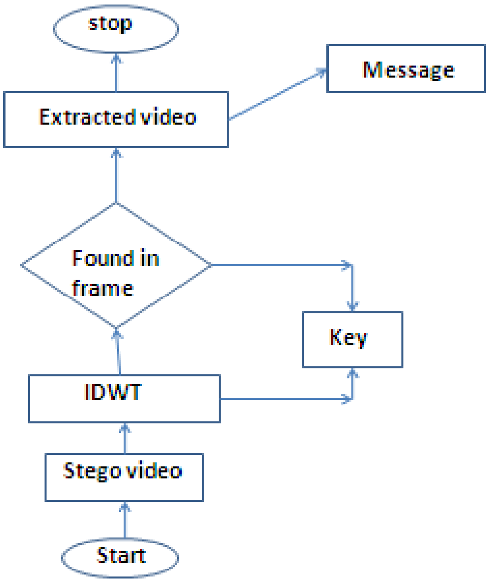
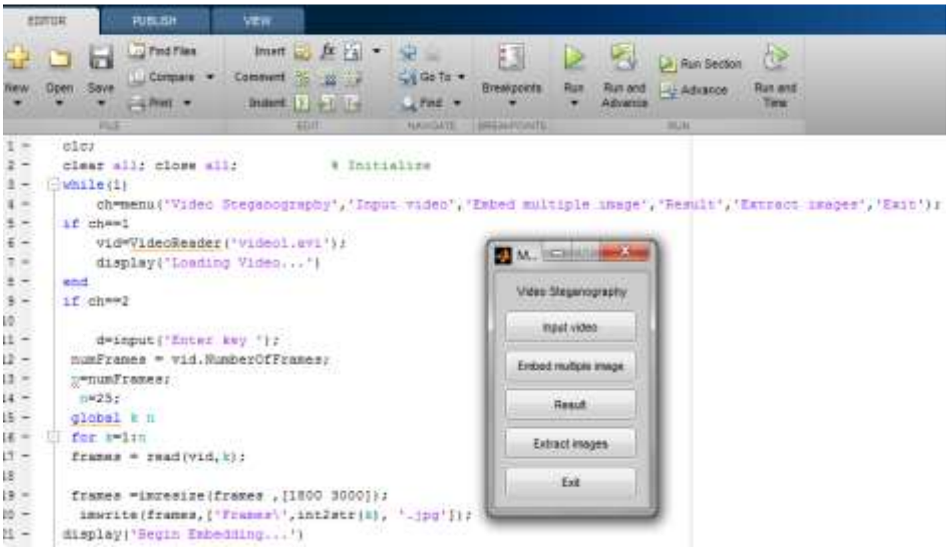


Figure-4: Embedding Process ***Figure-5: Extraction Process***

RESULTS

After writing the code in the MATLAB editor folder we need to browse the location of the images in the current folder and save file. After saving the file we need to run the code. Then it will display a menu having title as face recognition system with contents as shown in the figure-6.



```
clc;
clear all; close all;            % Initialize
while(1)
    ch=menu('Video Steganography','Input video','Embed multiple image','Result','Extract images','Exit');
if ch==1
    vid=VideoReader('video1.avi');
    display('Loading Video...')
end
if ch==2

    d=input('Enter key ');
 numFrames = vid.NumberOfFrames;
 n=numFrames;
  n=25;
 global k n
 for k=1:n
 frames = read(vid,k);

 frames =imresize(frames ,[1800 3000]);
  imwrite(frames,['Frames\',int2str(k), '.jpg']);
display('Begin Embedding...')
```

Figure-6: Menu for Video Steganography

Now select the required option from the menu obtained. If we select **'input video'**, then it will go to video folder and it interfaces the video to the MATLAB software and the video streaming gets started. After the streaming was started then select the 'Embedded multiple image' to start the embedded function. After that we get the embedded frames successfully.

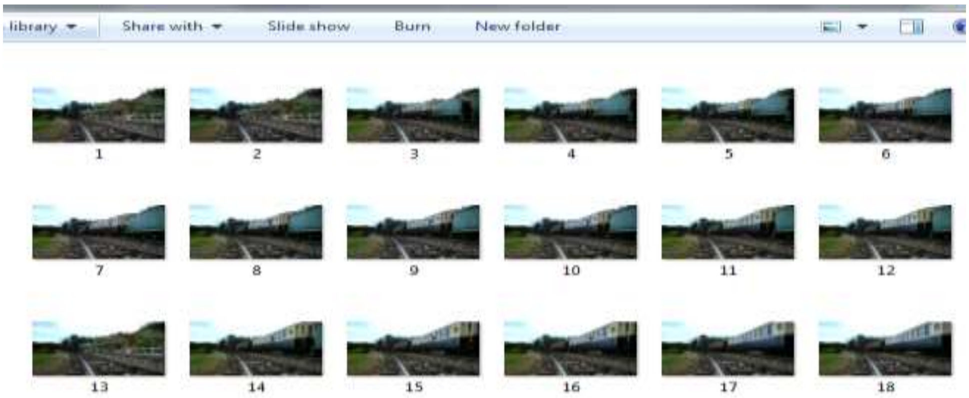


Figure-7: Decomposition of Frames

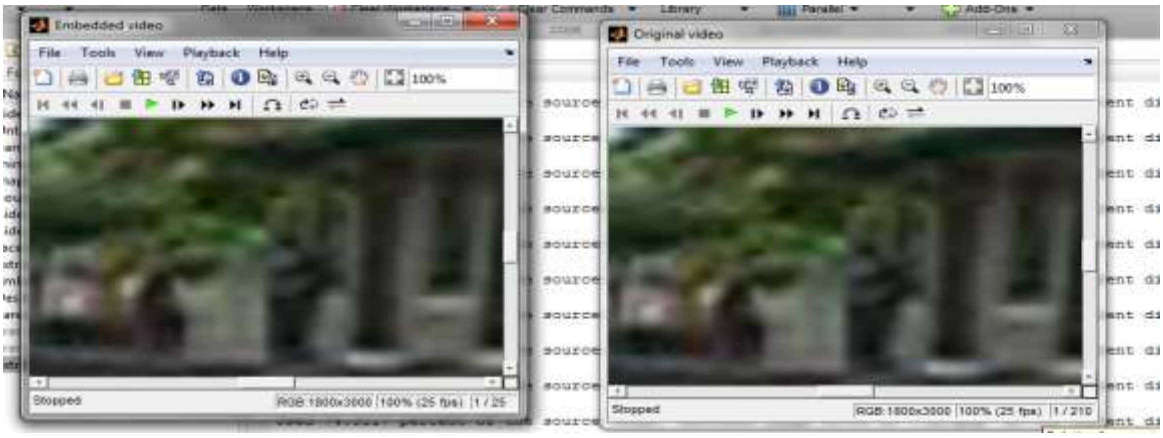


Figure-8: Embedded Video & Original Video

After the embedded video generation click on **'Extract images'** to start the extraction, then we get the extracted images on extracted images folders as shown in figure-9.

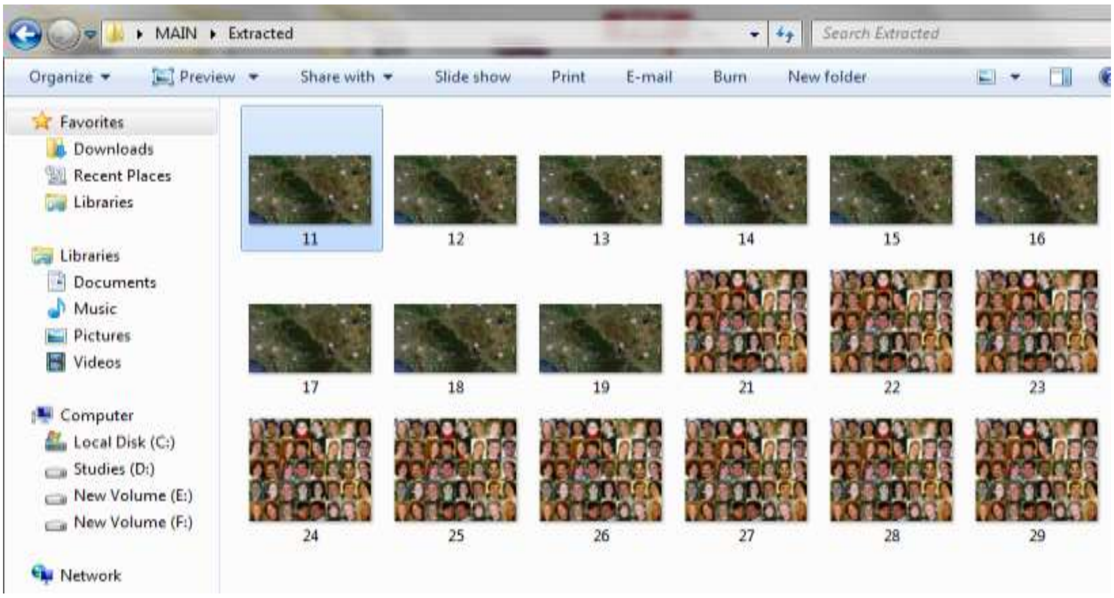


Figure-9: Extraction of Frames

CONCLUSION

In today's scenario of high speed internet, people are worried about the information being hacked by attackers. So order to overcome this problem many algorithms of steganography havebeen proposed. In this project, a wavelet based video steganography is introduced. Using this, an input logo hidden under one video frame by embedding algorithm and secret key. At the receiver, by using same key, logo and input video were recovered. Research can be extended in video steganography based on DWT and measured the values of MSE, PSNR for different wavelets.

Future Scope

In future, this method can be tested with other wavelet transform techniques with various image quality measurements and also implemented for videos of more length in less amount of time.

APPLICATIONS

Steganography is applicable to, but not limited to, the following areas.

1) Confidential communication and secret data storing

2) Protection of data alteration

3) Access control system for digital content distribution

4) Media Database systems

REFERENCES

[1] Anderson RJ, Petitcolas FAP (1998) On the limits of steganography. IEEE J Sel Areas Commun 16(4): 474-481.

[2] J. Fridrich, Application of data hiding in digital images, Tutorial for the ISSPA'99, Brisbane, Australia,August 22-25 1999.

[3] N.K. Abdulaziz and K.K. Pang, Robust data hiding for images, in: Proceedings of IEEE International Conference on Communication Technology, WCC-ICCT'02, 21-25 Aug. 2000, vol. 1, pp. 380-383.

[4] R.J. Hwang, K.T. Shih, C.H. Kao, Lossy compression tolerant steganography, in: Proceedings of the 1st International Conference on The Human Society and the Internet-Internet Related Socio-Economic Issues, Lecture Notes In Computer Science, 2001, vol. 2105, pp. 427-435.

[5] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy, 01 (3)(2003)32-44.

[6] S.B. Sadkhan, Cryptography: Current status and future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Damascus, Syria, April 19-23, 2004, pp. 417-418.

[7] P. Moulin and R. Katter, Data-hiding codes, Proceedings of the IEEE, 93 (12) (2005)2083-2126.

[8] Bailey K, Curran K (2006) An evaluation of image based steganography methods. Multimed Tools Appl 30(1):55–88.

[9] R.T. McKeon, Strange Fourier steganography in movies, in: Proceedings of the IEEE International Conference on Electro/Information Technology (EIT), 17-20 May 2007, pp. 178-182.

[10] A.A. Abdelwahab and L.A. Hassan, A discrete Wavelet transform based technique for image data hiding,in: Proceedings of 25th National Radio Science Conference, NRSC 2008, Egypt, March 18-20 2008, pp.1-9.

[11] M.W. Chao, C.H. Lin, C.W. Yu and T.Y. Lee, A high capacity 3D steganography algorithm, IEEE Transactions on Visualization and Computer Graphics, 15(2)(2009) 274-284.