International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.06, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Dual Mechanism for Audio Data Guarding in Videos Using DWT

Dr.S.Padmapriya[1], J.Sakina Farveen[2], T.Noorea Salhma[3], M.Rishvana Farvin Nachiya[4], M.Raikana Farvin Nachiya[5]

1) Professor, Department of Computer Science and Engineering, A.V.C College of Engineering

2,3,4,5) Students, B.E Computer Science and Engineering, A.V.C College of Engineering

ABSTRACT

Steganography is the art of hiding text, image or audio within another text, image or video. It is useful in many fields as the hidden content is completely secured. In our paper, we are going to hide a secret audio message inside a video file based on DWT. Existing method implements a video steganographic algorithm using DCT. The major disadvantage of using DCT is less quality and it needs some more security. The proposed method uses double coding mechanism to secure the audio data inside the video. Double coding means using two kinds of codes on the same data one after another. The two codes are pseudo random code and morse code. It is more reliable and secured when compared to the existing methods. 2 D Discrete Wavelet Transform is used to compress the video. Pseudo random codes are generated by Linear Feedback Shift Register (LFSR). Then the morse codes are applied. The compressed data and the coded data are used to embed the audio data into the video file. Once the data embedding is over, inverse DWT is performed and the stego video is obtained. This video will be sent to the receiver. The receiver performs the reverse operation to extract the secret audio file from the stego video.

Keywords: Steganography, Double coding, DWT, Pseudo random code, morse code, Embedding, Extraction.

I. INTRODUCTION

Nowadays more and more data (mainly digital) is transmitted into the web due to development in all major technical fields. Data in the form of images is livelier and visual communication is an effective method of sharing information. There is an increasing need for security of images which contain an embedded research work, designed weapons, information regarding any data which should not be revealed.

Steganography is the area of science which does this work. Steganography is gleaned from Greek language for secret communication. It is a mixture of two words Steganos means 'concealed/covered' and graphy means 'writing'. It is an art of embedding data inside a cover medium such as text, images and videos. It's goal is to hide the fact that communication is taking place. Governments, military, businesses and private citizens all over the world now use steganography for security and privacy purpose.

The main goal of steganography is to hide secret information in cover file so that no one can predict the presence of secret information; the cover file and the secret data file can be any multi-media file i.e. image or video or audio file. Steganography, a branch of information security, Several research works being pursued to ensure high security. Steganography hides the secret message and make it invisible, while cryptography scrambles the message to make it unreadable, drawing the attention of eavesdroppers. After embedding secret data in cover medium,a stego image is obtained which modifies the cover image slightly. The main objectives of Steganography are imperceptibility, robustness and capacity of the hidden data which separate it from its relative techniques such as watermarking and cryptography.

Steganography is for preserving the privacy in secret communication, watermarking is for ownership protection and Cryptographic encryption is for data security. It has many application areas such as audio-video synchronization, copyright control, TV broadcasting, in defense forces and digital watermarking etc,. The combination of cryptography as well as steganography makes available great level of security to the secretive data.

Steganography techniques are categorized as spatial domain methods and transform domain methods. Transform domain approach is more secure whereas spatial domain provides more payload embedding. In Spatial domain simplest data hiding technique is least significant bit (LSB)substitution method, in which least significant bit of the pixel value is replaced with the value of secret data value. In transform domain there are wide varieties of tools such as Fourier Transform (FT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Apart from these two techniques another category is also there i.e. Adaptive steganography (AS), it can be applied either in spatial domain or in frequency domain.

A video is an electronic medium for showing the moving visual images. Video Steganography is a technique to hide any kind of files into a video file. Videos are the set of images. The number of still pictures per unit of time of video ranges from six to eight frames per second. In video steganography, some media is hidden inside a video.

The best embedding technique is that to hide secret message without affecting the quality of video, structure and content of video. After hiding a secret data in video create "stego" video

file which is sent to the receiver.

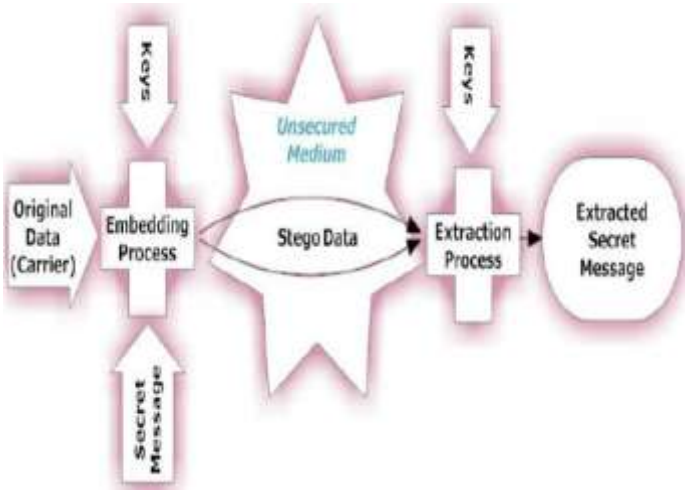


Fig 1: General block diagram of steganography algorithm

In our paper, we mainly concerned with hiding audio in videos, for that we propose a data embedding technique which uses double coding i.e. use of two coding methods on same data after performing wavelet transform and exposing stego videos to compression technique. These decomposed matrices are obtained by Discrete Wavelet Transform (DWT). Haar wavelet is used in DWT.

This paper is arranged in six sections. In section I contains introduction about steganography, Section II describes the related work, Section III elaborates about the Discrete Wavelet Transform (DWT), Section IV describes about the dual codes by LFSR and morse code, Section V is the important part that provides an algorithm to embed and extract audio data from video files, Section VI gives the conclusion and future scope of this proposed work.

II.RELATED WORKS

In May 2016, Madhuri R.Shende ,Prof. Amit Welekar and Prof S.V.Wajurkar presented an advanced Steganography For Hiding Data And Image Using Audio-Video[1]. In this paper they are combining cryptography and steganography for hiding data behind audio and image behind video in audio video file. For hiding image behind video used LSB replacement technique and for hiding data behind the audio used Parity coding algorithm. The Blowfish algorithm is used for more security purpose.

Chhaya Varade, Danish Shaikh, Girish Gund, Vishal Kumar and Shahrukh Qureshi presented a technique for data hiding using audio and video Steganography[2]. In this paper, the message is embedded in audio. For that they had used DES (Data Encryption System) algorithm. It did not make the change in the size of the file after encoding of data in an audio file. Encryption and Decryption techniques are used to make the security in data transmission.

M.I.Khalil discusssed an Image Steganography:Hiding Short Audio Messages Within Digital Images[3]. In this paper the steganography technique simply embed the audio message into the cover image without supplying any stego key. At this stage LSB technique used to insert the message bit into the image and extract the message from the stego image produced. This allow high perceptual transparency of LSB.

Mohamed Elsadig Eltahir,Miss Liha Mat Kiah and Bilal Bahaa zaidam presented a High Rate Video Streaming Steganography[4]. They used the LSB method on video images or frames, in addition to the usage of the human vision system to increase the size of the data embedded in digital video streaming.

Amol Bhujade and Prof. Sonu Lal presented a Advanced Steganography: Embedding HighCapacity Audio in Colour Image[5]. In this paper the bits of the secrete audio data are hidden in the only last bit of the cover image thus offers more key based secure data transmission and reception with same cover medium. It also applied for MPEGIII(mp3) file previously was applicable to only WAVE file, so provide flexibility and versatility to the user and it can cause no change in the image as per the human visual system.

Khaled Elleithy and Ramadhan J. Mstafa used A High Payload Video Steganography Algorithm In DWT Domain Based On BCH Codes (15, 11)[6]. In this paper, a secret message is first encoded by BCH(n,k,t) coding. Then, it is embedded into the DWT coefficients of video frames. As the DWT middle and high frequency regions are considered to be less sensitive data, the secret messages is embedded only into the middle and high frequency DWT coefficients. The result demonstrate better performance than the otheralgorithms.

Ketki Deshpande and Nagesh Kamble presented a Application Of Data Hiding In Audio-Video Using Advance Algorithm[7]. In this paper hide secret data in the audio and image of a video file. Video has so many still frames of image and audio, selected any frame for hiding the data. They proposed a new video data hiding method that makes use of correction capability of repeat accumulate codes and superiority of forbidden zone data hiding (FZDH). FZDH is used for no alteration is allowed while data hiding process.

Sumanth.C and Dr.M.BMeenavathi presented a Audio-Video Steganography Using Face Recognition Technique For Authentication[8]. The secret information hidden behind audio and recipient's face image behind the video. Select any frame of video to hide recipient's face image and audio for hiding our secret data as video

is an application of many still frames of images and audio. Suitable algorithm such as improved LSB used for image steganography and audio steganography, PCA algorithm is used for face recognition, hence the data security can be increased.

Yugeshwari Kakde, Priyanka Gonnade and Prashant Dahiwale presented a Audio-Video Steganography[9]. This paper proposed an algorithm for hiding image in selected video sequence which is an image-hiding technique based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) and Least Significant Bit (LSB) method. It hides secret text information inside audio of the video file. It reduced embedding distortion of the host audio. It focused the idea of computer forensics technique which is used as a tool for authentication and data security purpose and its use in video steganography in security manner.

S.Kamesh, K.DurgaDevi and S.N.V.P. Raviteja presented a Dwt Based Data Hiding Using Video Steganography[10]. This paper proposed 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 frames 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.

III.WAVELET TRANSFORM

A wavelet is a mathematical function useful in image compression and digital signal processing . The principles are similar to those of Fourier analysis, which was first developed in the early part of the 19th century.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.

Types of Wavelets:

1. Haar Wavelets
2. Meyer Wavelets
3. Daubechies Wavelets
4. Morlet Wavelets
5. Mexican Hat Wavelets

6. Biorthogonal Wavelets

7. Coiflets Wavelets

8. Symlets Wavelets

original image. The LH band indicate horizontal features, while the HL band indicate vertical features in the original image. Finally, the HH band tends to isolate localized high-frequency point features in the image.

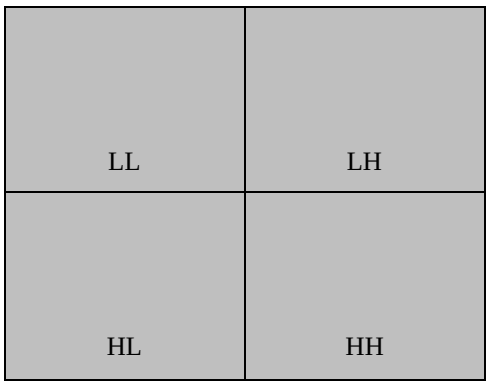


Fig 2: 1 level 2D DWT

The applications of two-dimensional DWT is in the field of computer vision and image processing, and is a relatively straight forward extension of the one-dimensional DWT.The results demonstrate the first level of decomposition.

DISCRETE WAVELET TRANSFORM

Discrete Wavelet Transform (**DWT**) ,which transforms a discrete time signal to a discrete wavelet representation.

The discrete wavelet transform is valuable way designed for signal exploration as well as picture handling, briefly in multi-resolution description.DWT is good method for signal decomposition in steganography a well as image processing.

The first level of the 2D-DWT image decomposition is applied to the cover video frame. It splits the frame into four sub-bands:LL (approximation), LH (horizontal), HL (vertical), and HH (diagonal) using both a low pass

filter and a high pass filter for the decomposition process.

In the second level of image decomposition, the 2D-DWT is applied to the LL sub-band, producing four new sub-bands. Here, L stands for low-pass filtering, and H stands for high-pass filtering The LL band corresponds roughly to a down-sampled (by a factor of two) version of the

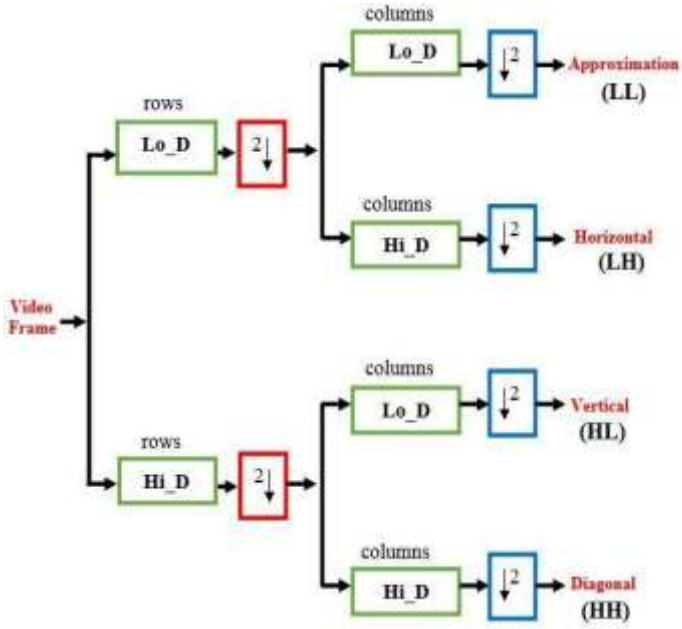


Fig 3: 2D-DWT

IV.DUAL CODINGS

The dual codes are pseudo random code and morse code. First pseudo random codes are used which can be generated by Linear Feedback Shift egister (LFSR) and then morse codes are used. This approach will give more security to the data.

1.LFSR(Linear Feedback Shift Register)

LFSRs are known to produce (binary) sequences with good pseudorandom properties. In computing,

LFSR whose input bit is a linear function of its previous state. The commonly used linear function of single bits is exclusive-OR (XOR). Register bits that do not need an input tap, operate as a standard shift register. The input taps determines how many values there are in a given sequence before the sequence repeats. The seed is the initial value of the LFSR, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current (or previous) state. An LFSR feedback function can produce a sequence of bits that is random and has a very long cycle.

Linear feedback shift registers make extremely good pseudorandom pattern generators. when the LFSR is clocked, it will generate a pseudorandom pattern of 1s and 0s.

Applications of LFSRs include generating pseudo-noise sequences, whitening sequences, fast digital counters and pseudo-random numbers. The implementations of LFSRs are common in both hardware and software.

2. MORSE CODE

Morse code is a method of transmitting text information as a series of on-off tones, lights, or clicks that can be directly understood by a skilled listener or observer without special equipment. Morse codes are the standardized sequences of "Dots" and "Dashes"**.** Morse codes are available for alphabets, numbers and prosigns. The prosigns are combinations of two letters sent together with no space in between.

The following shows the morse codes for alphabets and numbers:

Fig 4: Morse code

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.06, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

V.PROPOSED METHODOLOGY

1. EMBEDDING OPERATION

This part describes the steps for hiding audio in video

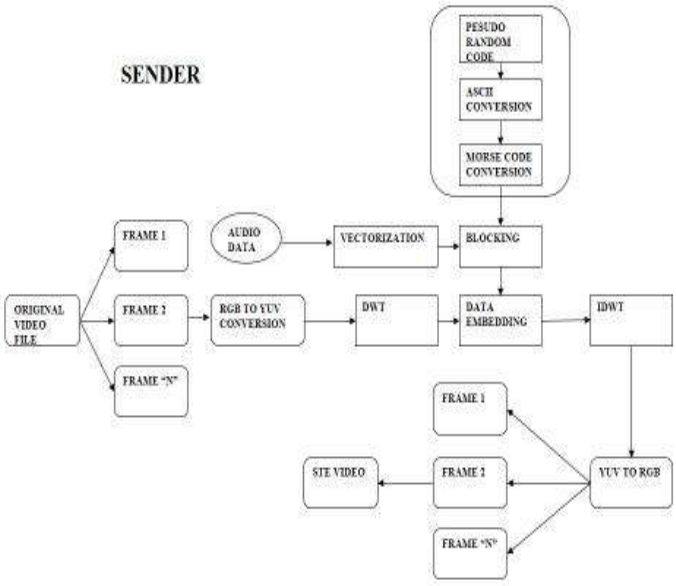


Fig 5: Hiding secret audio in video.

The step by step procedure of hiding audio in video is as follows:

Step 1: First upload the video and then extract all the frames from the video file.

Step 2: Perform RGB to YUV color conversion. Human eye is more sensitive to changes in illumination rather than chrominance. Thus during compression, it is more easier to reduce the bit requirement for the color components and store the luminance properly.

Here we use only Y-frame because these will not reflect any processing change after dada hiding.

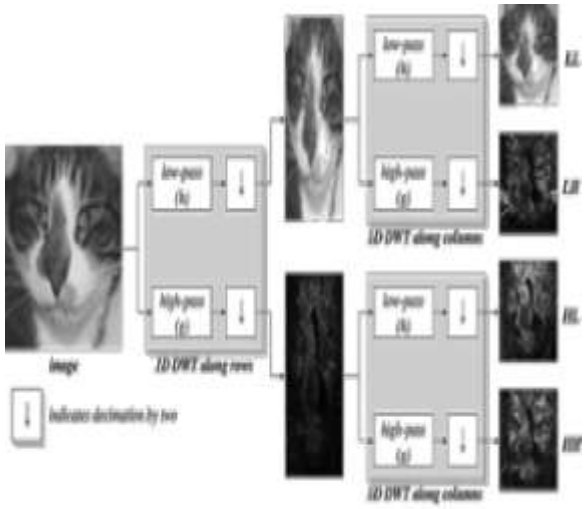
Formula for converting RGB to YUV:

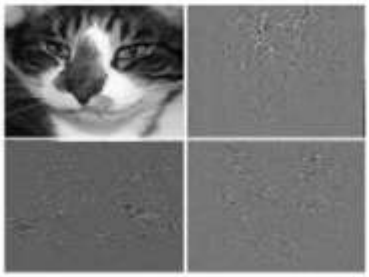
$Y = 0.299R + 0.587G + 0.114B$

U = -0.147R - 0.289G + 0.436B

V = 0.615R - 0.515G - 0.100B

Step 3: Apply Haar two-dimensional (2-D) DWT to the converted frames and compute approximated coefficients and detailed coefficients. These coefficients are placed in sub matrices named as LL, LH, HL & HH.





$$\begin{pmatrix} 0\,0\,1\,0\,1\,1\,0\,0 \\ 1\,0\,1\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,1\,0\,1\,1 \\ 1\,1\,0\,1\,0\,1\,0\,0 \end{pmatrix}$$

Step 4: Take the audio file that is to be hidden. Then extract the audio information from the audio file.

Consider the extracted audio data as 0010 1101 0010 1110

Step 5: Generate the pseudo random code by using LFSR(Linear Feedback Shift Register). The output of LFSR is in binary form. Convert the binary into ASCII.

Let us consider the random code as

0100110101010010010101110100010001010010

……

After converting the random code to ASCII format, it will be

MRRMRGMDRI

Step 6: Write corresponding morse code for the ASCII value. Convert the morse codes into a combination of 0's and 1's by placing 0 in the place of dot and 1 in the place of dash. By this, a block matrix will be composed.

Convert the ASCII into appropriate morse

code

_ _ . _ . . _ _ _ . . . _ . _ _

. _ . _ _ . _ _ _ . . . _ . . .

Fig 6: 1 level 2D DWT

This is 1-level 2D DWT. From these, we get decomposed sub matrices. Among these, we can use any matrix for embedding.

Let us take the submatrix as

Write the morse code in the form of 0's and 1's

$$\begin{pmatrix} 1\,1\,0\,1\,0\,0\,1\,1 \\ 1\,0\,0\,0\,1\,0\,1\,1 \end{pmatrix}$$

0 1 0 1 1 0 1 1

1 0 0 0 1 0 0 0

Step 7: Choose the position as 0 or 1 in the block matrix for placing the audio vector values. Fill the block matrix with the audio vector values.

Here choose 1 to place audio data

$$\begin{pmatrix} 0\,0\,0\,1\,0\,0\,0\,1 \\ 1\,0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0\,0\,1\,1 \\ 1\,0\,0\,0\,0\,0\,0\,0 \end{pmatrix}$$

Step 8: Embed the audio with video frame by adding sub matrix with block matrix.

After embedding, it will be like

$$\begin{pmatrix} 0\,0\,1\,1\,1\,1\,0\,1 \\ 0\,0\,1\,0\,1\,1\,1\,1 \\ 0\,0\,1\,1\,1\,0\,0\,0 \\ 0\,1\,0\,1\,0\,1\,0\,0 \end{pmatrix}$$

Step 9: Apply 2-D inverse DWT (IDWT) to the embedded form. Perform the color conversion process by converting YUV back into RGB.

Formula for converting YUV into RGB:

$$R = Y + 1.140V$$

$$G = Y - 0.395U - 0.581V$$

$$B = Y + 2.032U$$

Step 10: Finally reconstitute all the frames to make the stego video. Stego video is nothing but our video containing the secret audio.

\

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.06, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

2. EXTRACTION OPERATION

This part describes the steps for extracting audio from video.

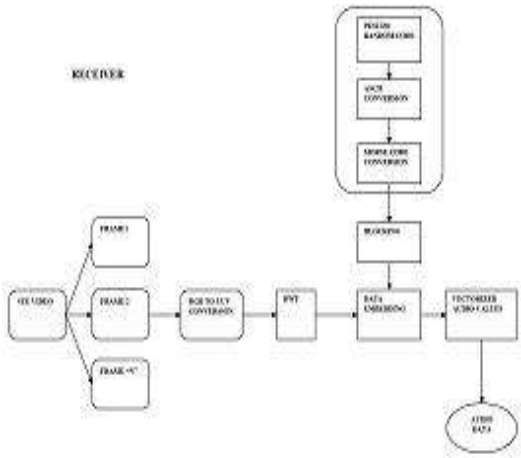


Fig 7: Extracting secret audio from stego video

The step by step procedure of extracting audio from the video is as follows:

Step 1: From the stego video, extract all the frames.

Step 2: Convert RGB into YUV and take only the Y-frame.

Step 3: Apply 2-dimensional DWT on the frame.

Step 4: Perform the reverse mathematical operation on the sub matrix and already available original video Y frame. The resultant matrix will be said as sub-1 matrix.

On subtracting the stego video frame from original video Y frame, we get

$$\begin{pmatrix} 0\,0\,0\,1\,0\,0\,0\,1 \\ 1\,0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0\,0\,1\,1 \\ 1\,0\,0\,0\,0\,0\,0\,0 \end{pmatrix}$$

Step 5: Generate the pseudo random code by the LFSR and write the morse code for them.

$$\begin{pmatrix} 1\,1\,0\,1\,0\,0\,1\,1 \\ 1\,0\,0\,0\,1\,0\,1\,1 \end{pmatrix}$$

0 1 0 1 1 0 1 1

1 0 0 0 1 0 0 0

Step 6: Compare the morse code matrix and sub-1 matrix. Whenever 1 is there at the morse code matrix, the corresponding position in the sub-1 matrix is extracted.

By doing this, we get

0010 1101 0010 1110

Step 7: The above gives the audio vector value. Convert the values into audio signal. Hence the secret audio is extracted.

The original frame before hiding audio is:

The frame containing audio hidden inside it

Fig 8

VI.CONCLUSION AND FUTURE WORK

CONCLUSION

In today's scenario of high speed internet, people are worried about the information being hacked by attackers. So in order to overcome this problem, our proposed method has been employed for applications that require more security. The video steganography is a technique to hide information inside video file for the secure data transmission from the sender to receiver through the internet. When transfer or download big video will take more time and storage space, so we used compression method with steganography to reduce storage size of video. This method introduces and adds an extra security level barrier by using double codes in the way of avoiding attacks by the attacker. This provides more security and reliability to the hidden data into video. As security is the most important matter of concern in present data communication scenario, thus our proposed method provides satisfactory results. Dual coding mechanism assures complete security of the secret audio.

FUTURE WORK

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.

REFERENCES

1. Miss Madhuri R.Shende ,Prof. Amit Welekar and Prof S.V.Wajurkar, "Advanced Steganography For Hiding Data And Image Using Audio-Video", International Conference on Modern Trends in Engineering Science and Technology (ICMTEST May 2016).
2. Chhaya Varade, Danish Shaikh, Girish Gund, Vishal Kumar and Shahrukh Qureshi,"A Technique For Data Hiding Using Audio And Video Steganography", International Journal of Advanced Research in Computer Science and Software Engineering,volume 6, February 2016.

3. M.I.Khalil,"Image Steganography: Hiding Short Audio Messages Within Digital Images",JCS&T Vol. 11 No. 2 October 2011.
4. Mohamed Elsadig Eltahir,Miss Liha Mat Kiah and Bilal Bahaa zaidam , " High Rate Video Streaming Steganography",2009 International Conference on Information Management and Engineering.
5. Amol Bhujade and Prof. Sonu Lal," Advanced Steganography: Embedding HighCapacity Audio in Colour Image", International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering,Vol. 4,July 2015.
6. Khaled Elleithy and Ramadhan J. Mstafa," A High Payload Video Steganography Algorithm In DWT Domain Based On BCH Codes (15, 11)", Conference Paper, April 2015.
7. Ketki Deshpande and Nagesh Kamble," Application Of Data Hiding In Audio-Video Using Advance Algorithm", International Journal of Computer Science and Mobile Computing,Vol. 5, June 2016.
8. Sumanth C and Dr. M B Meenavathi**,** **"**Audio-Video Steganography Using Face Recognition Technique For Authentication", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 5, May 2016.
9. Yugeshwari Kakde, Priyanka Gonnade and Prashant Dahiwale, "Audio-Video Steganography", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15.
10. S.Kamesh, K.DurgaDevi and S.N.V.P. Raviteja," Dwt Based Data Hiding Using Video Steganography", International Journal Of Engineering Sciences & Research Technology.