Indian Journal of Science and Technology, *Vol 7(7), 897–904, July 2014*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Video Steganography based on Integer Haar Wavelet Transforms for Secured Data Transfer

Mritha Ramalingam[1*] and Nor Ashidi Mat Isa[2]

Imaging and Intelligent System Research Team (ISRT) , School of Electrical and Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, Nibong Tebal 14300, Penang, Malaysia; mritha2011@gmail.com

Abstract

This paper proposes a video steganography algorithm based on Haar Integer Wavelet Transforms (IWT) and Least Significant Bits (LSB) substitution for data hiding and extraction in Red Green Blue (RGB) components of the video files. In this approach, the cover-video is divided into RGB frames and the text in binary form is embedded into the LSBs of IWT coefficients. The embedded text is extracted from stego-video using the reverse process of data hiding. The proposed system was implemented using Audio Video Interleave (AVI) files. The experimental results prove that the proposed system has shown imperceptible modifications in AVI videos that lead to high security and an eavesdropper's inability to detect hidden data. The proposed system is simple and therefore can be used to transfer highly confidential data like military secrets, hospital reports and other data.

Keywords: Data Hiding, Haar Integer Wavelet Transform, Imperceptibility, Security, Video Steganography

1. Introduction

The growing demand for today's digital communication has created a sturdy need for new approaches to protect the secret data from illicit usage. In some cases it is highly desired to have secret communication. This goal is achieved using two techniques namely cryptography and steganography. In cryptography, a sender scrambles the message using an encryption key and the intended receiver extracts the original data from scrambled message using the appropriate decryption key. But in steganography, the message is not scrambled; instead the existence of a message is hidden in a carrier usually called as cover-medium[1,2]. The carrier containing the hidden message is called as stego-medium.

Steganography is an art of hiding data without leaving invisible distortions in cover-medium. The major aim of steganography on any medium is that the mere existence of secret data is expected to be imperceptible after hiding. A basic steganography system is shown in Figure 1. Sender applies the steganography technique to hide the secret message in cover-medium to obtain stego-medium. The stego-medium is transmitted to the receiver. At the receiver side, the de-steganography technique is applied on stego-medium to extract the embedded message from stego-medium. Several steganography algorithms hide data in transform domain coefficients on any digital media files like text, image[3], audio[4], and video[5].

Video steganography is a process of hiding secret data in videos. We had opted videos for data hiding as they provide fairly high bandwidth and are frequently transferred online. Figure 2 illustrates the graphical view of a video steganography system. The figure depicts hiding a secret message inside a cover-video using the embedding algorithm and extraction of the hidden message using extraction algorithm.

**Author for correspondence*

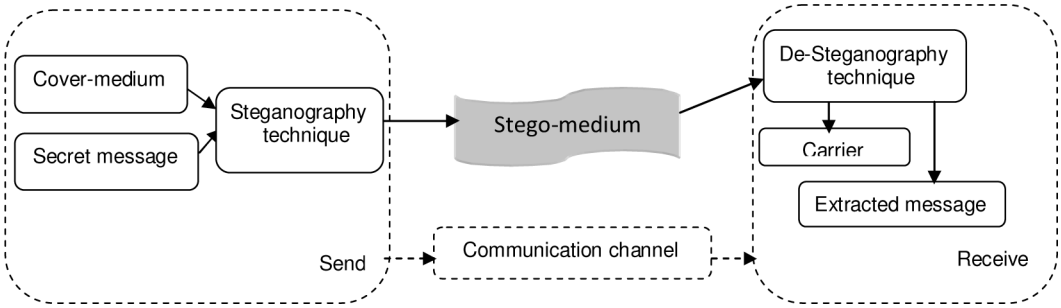


Figure 1. Basic steganography system.

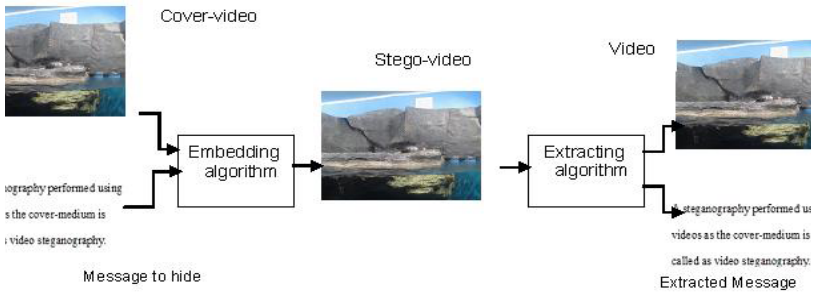


Figure 2. Graphical view of a video steganography system

One of the most important characteristics that differentiate steganographic systems is the domain in which the alterations for data hiding are applied. Image and video based steganography systems can be implemented in spatial domain and/or frequency domain[2,3]. In spatial domain, usually data is hidden in Least Significant Bits (LSB) of video images. The spatial domain based steganography provides larger space for data hiding, but it is insecure[6]. In frequency domain, the steganography can be applied on audio or video images that are transformed to frequency elements by using either frequency Fourier transform, discrete cosine transform or discrete wavelet transform. The data are embedded in some or all of the transformed coefficients. The frequency domain based steganography provides high embedding capacity and highly secures the data from eavesdroppers. The major disadvantage in these techniques is in the robustness of the systems[7,8]. The wavelet transform domain provides good robustness to perform efficient data hiding. The highlighting properties of Haar integer wavelets like, perfect reconstruction of transformed images and good correlating properties motivated us to employ the IWT in our proposed work. A brief introduction to wavelet transforms is provided in Section 2. The proposed algorithm is presented in Section 3. Experimental results are discussed in Section 4. The conclusion is drawn in Section 5.

2. Integer Wavelet Transform (IWT)

Wavelets are set of non-linear basis. When resembling a function in terms of wavelets, the wavelet basis functions are chosen according to the function being approximated. Wavelets utilize a dynamic set of basis functions that represents the input function proficiently. The secret data can be hidden in images using wavelets.

In many multimedia applications, the IWT maps an integer into another integer data. Fortunately the lifting scheme can be modified easily to a transform that maps integers to integers and it is reversible[4,10]. Lifting scheme is a method for decomposing wavelet transforms into set of elements. A simple example of lifting scheme is the Haar wavelet. Haar transforms the wavelets by a process of dilation and shifting. The wavelets are constructed from base wavelets using (1),

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right) \quad (1)$$

where a, b are scaling and shifting parameters respectively.

Haar wavelet operates on the input data by calculating the sums and differences of adjacent elements. This wavelet operates first on adjacent horizontal elements and

then on adjacent vertical elements. An excellent feature of the Haar wavelet transform is that the transform is equal to its inverse[10]. The wavelet transform is considered to be more robust for multi-resolution analysis that has been widely used in most of the steganography applications[11]. IWT splits the components into numerous frequency bands called sub bands known as LL – Horizontally and vertically low pass, LH – Horizontally low pass and vertically high pass, HL - Horizontally high pass and vertically low pass and HH - Horizontally and vertically high pass. Hiding in LL sub-band is much more sensitive to human visual system (HVS). Generally wavelet domain allows us to hide data in regions that the HVS is less sensitive to, such as the high resolution sub-bands, LH, HL and HH. Hiding data in these wavelet bands does not degrade video quality and allow us to increase the robustness while maintaining good visual quality. Though the authors[9] have improved the hiding capacity, the robustness is not encountered.

The one level IWT coefficients are integer values that are obtained using (2)

$$W(a,b) = d_i - \left\lfloor \frac{1}{2}(s_i + s_{i+1}) + \frac{1}{2} \right\rfloor \tag{2}$$

where d, s are the high-frequency and low-frequency components of an input signal respectively. Length of s and d is equal to 2^{n-1}. Simply, the transform results in two values, one is averages and the other is differences, differences are called as coefficients. For example, the one dimensional lifting scheme of an input signal of sequence, $x = (1, 2, 3, 4, 5, 6, 7, 8)$ can be calculated using lifting prediction. The length of the input is $2^3 = 8$. The single level IWT decomposition can be obtained using (3) and (4).

Now split the signal x into even samples and odd samples,

$$X_{even} = S_1 = \{2 \quad 4 \quad 6 \quad 8\} = \{s_1 \quad s_2 \quad s_3 \quad s_4\}$$

$$X_{odd} = D_1 = \{1 \quad 3 \quad 5 \quad 7\} = \{d_1 \quad d_2 \quad d_3 \quad d_4\}$$

then the coefficients are calculated as follows,

$$d_1 = d_1 - \left\lfloor \frac{1}{2}(s_1 + s_2) + \frac{1}{2} \right\rfloor = 1 - \left\lfloor \frac{1}{2}(2+4) + \frac{1}{2} \right\rfloor = -2$$

$$d_2 = d_2 - \left\lfloor \frac{1}{2}(s_2 + s_3) + \frac{1}{2} \right\rfloor = 3 - \left\lfloor \frac{1}{2}(4+6) + \frac{1}{2} \right\rfloor = -2$$

$$d_3 = d_3 - \left\lfloor \frac{1}{2}(s_3 + s_4) + \frac{1}{2} \right\rfloor = 5 - \left\lfloor \frac{1}{2}(6+8) + \frac{1}{2} \right\rfloor = -2$$

$$d_4 = d_4 - \left\lfloor \frac{1}{2}(s_4 + s_5) + \frac{1}{2} \right\rfloor = 7 - \left\lfloor \frac{1}{2}(8+0) + \frac{1}{2} \right\rfloor = 3$$

$$s_1 = s_1 + \left\lfloor \frac{1}{4}(d_0 + d_1) + \frac{1}{2} \right\rfloor = 2 + \left\lfloor \frac{1}{4}(0 + (-2)) + \frac{1}{2} \right\rfloor = 2$$

$$s_2 = s_2 + \left\lfloor \frac{1}{4}(d_1 + d_2) + \frac{1}{2} \right\rfloor = 4 + \left\lfloor \frac{1}{4}(-2-2) + \frac{1}{2} \right\rfloor = 3$$

$$s_3 = s_3 + \left\lfloor \frac{1}{4}(d_2 + d_3) + \frac{1}{2} \right\rfloor = 6 + \left\lfloor \frac{1}{4}(-2-2) + \frac{1}{2} \right\rfloor = 5$$

$$s_4 = s_4 + \left\lfloor \frac{1}{4}(d_3 + d_4) + \frac{1}{2} \right\rfloor = 8 + \left\lfloor \frac{1}{4}(-2+3) + \frac{1}{2} \right\rfloor = 8$$

$$D_1 = \{d_1 \quad d_2 \quad d_3 \quad d_4\} = \{-2 \quad -2 \quad -2 \quad 3\} \tag{3}$$

$$S_1 = \{s_1 \quad s_2 \quad s_3 \quad s_4\} = \{2 \quad 3 \quad 5 \quad 8\} \tag{4}$$

Haar transforms are very appropriate for IWT based video steganography because of its exceptional properties like exploiting de-correlation and possible for better encoding.

3. The Proposed Video Steganography System

The main objective of the proposed video steganography system is to enhance the security and robustness of the secret communication. The system utilizes the IWT and Red, Green, and Blue (RGB) components of the cover-videos to perform efficient data hiding. For data hiding, we utilized the coefficients obtained by one level integer wavelet decomposition of the original cover-video. IWT ccoefficients are integer values that come as a result of wavelet function in (2). To exploit frequency masking effect, the high frequency sub-bands HL, LH and HH of IWT are used for data embedding.

Figure 3 illustrates the block diagram of data embedding and extraction processes in the proposed video steganography system. In this system, the secret data in binary form are hidden in the LSB of each RGB component of the cover-video sequences. The RGB color components are highly correlated. The use of this property of RGB components, ensure the robustness of the proposed algorithm. One dimensional (1 D) Haar IWT is applied on RGB frames of cover-video. The secret data are embedded in the LSB of each RGB components of the video. The Inverse IWT (IIWT) is applied on the resulting video frames to obtain the stego-video. To avoid the overflow / underflow that occurs by altering the IWT coefficients of some pixel blocks of the cover-video, it is necessary to normalize the video frames so that the

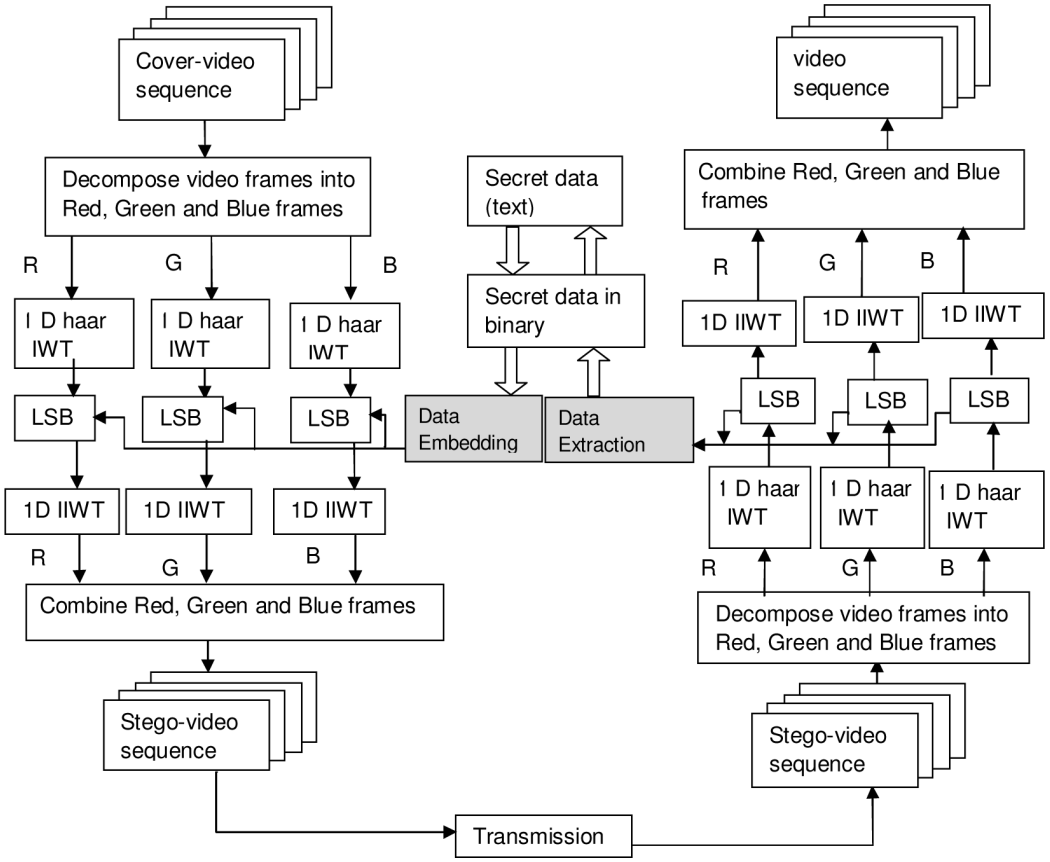


Figure 3. Block diagram of the proposed video steganography system.

possible pixel values may not exceed the upper bound (255 for an 8-bit video image) and/or the lower bound (0 for an 8-bit video image).

3.1 Embedding Algorithm

Figure 4 shows the block diagram of the embedding algorithm. Algorithm to embed the text data:

Step 1: Input cover-video.
Step 2: Decompose the cover-video into RGB components
Step 3: Normalize the cover-video frames to avoid underflow/overflow
Step 4: Divide the video frames into 8x8 blocks
Step 5: Obtain the wavelet coefficients of frames using 1 D Haar IWT.
Step 6: Read the text data to be embedded and convert the text to bits
Step 7: Use the LSB substitution technique on RGB component of each video frame to embed the secret data bits into the obtained coefficients.
Step 8: Calculate the inverse Haar IWT on RGB frames to produce stego-video sequence.

3.2 Extraction Algorithm

Figure 4 shows the block diagram of the extraction algorithm. Algorithm to retrieve the embedded text data:

Step 1: Input stego-video.
Step 2: Decompose the stego-video into RGB components
Step 3: Normalize the video frames to avoid underflow/overflow
Step 4: Divide the video frames into 8x8 blocks
Step 5: Obtain the wavelet coefficients of frames using 1 D Haar IWT.
Step 6: Use the LSB substitution technique on RGB component of each video frame to identify the bits containing hidden data bits and extract the secret data bits from the coefficients.
Step 7: Convert the retrieved data bits into text

Step 8: Calculate the inverse Haar IWT on RGB frames to produce video sequence.

4. Experimental Results and Discussion

The proposed video steganography algorithm is tested using the AVI files in Table 1. The performance and robustness of the proposed video steganography system are discussed in this section. The proposed method is implemented using Java and Matlab. The AVI video files are used for testing the proposed method.

The performance of the proposed system is analyzed based on the variation in the size of the test videos that are used to hide secret data. We embedded text data in binary form into the cover-videos and observed the performance. Figure 6 shows the variation in the size of the test

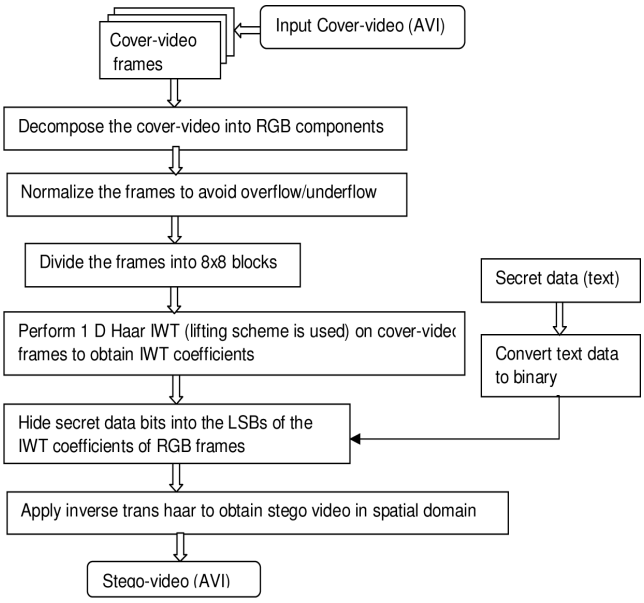


Figure 4. Block diagram of data embedding process.

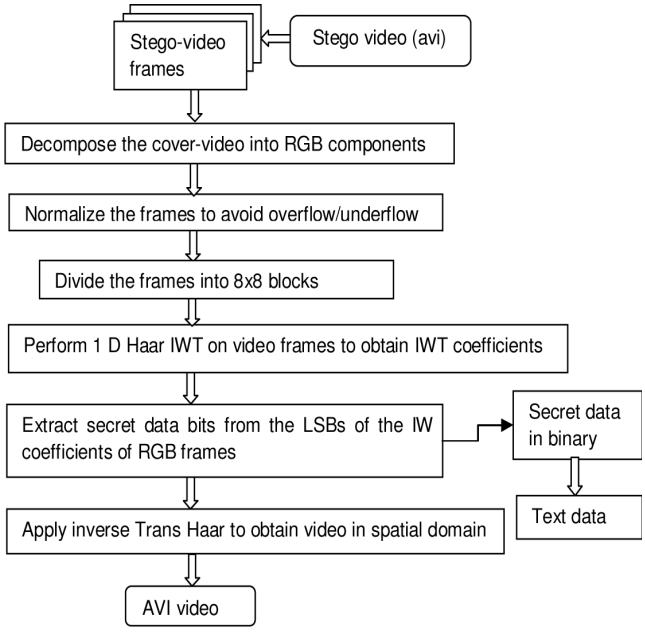


Figure 5. Block diagram of data extraction process.

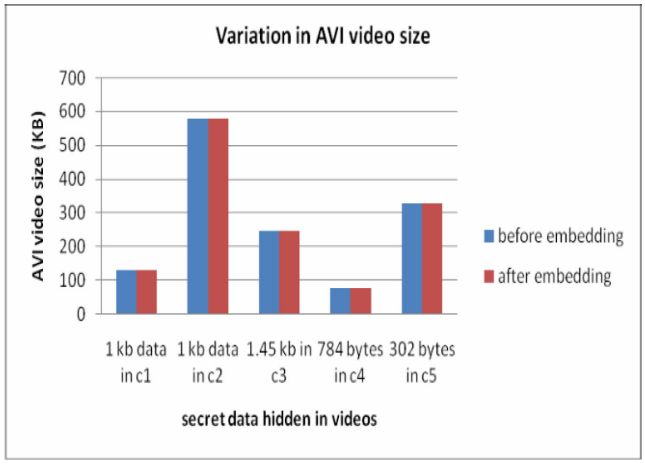


Figure 6. Variation in size of test video sequences before and after data embedding.

Table 1. Test videos used for testing the performance of the proposed system

Cover-video					Secret data	
id	Name (.avi)	Resolution	Frames per second	Size (KB)	Name	Size
c1	matl	104 × 104	15	130.1	data1.txt	1 KB
c2	buzz	352 × 288	25	578	data2.txt	1 KB
c3	Wildlife	104 × 104	30	247	mess.doc	1.45 KB
c4	rhinos	1380 × 960	20	76.8	secdat.doc	784 bytes
c5	cat	356 × 244	30	328.3	sec.txt	302 bytes

video sequences before and after embedding the secret data. We embedded different secret data on different cover-video sequences (refer Table 1). After embedding the secret data into respective cover-videos using the proposed algorithm, we observed that there is no variation in the size of the AVI videos. The size of the videos before and after embedding the data is similar. So hiding data in IWT coefficients of the videos did not vary the size of the test video files. For example, the secret data, data1.txt in binary form is hidden in the cover-video, c1 with a size of 130.1 KB. We observed that the size of c1 remains same even after the data is hidden into it.

We applied our algorithm on different AVI videos. Figure 7 shows the example illustration of the proposed algorithm on two cover-videos. Figure 7(a) shows the original cover-video (c1-matl.avi) frame before data hiding. Figure 7(b) shows the secret data to be embedded in c1. We embedded the text,

"Cyptography and steganography are related to each other. The main difference between cryptography and steganography is that cryptography scrambles the message so as to become difficult to understand, whereas steganography hides the very existence of a message. Steganography plays the central role in secret message communication [1] [2].Steganography is not intended to replace cryptography but to supplement it. Hiding a message reduces the chance of detecting a message."

in the cover-video, c1. The resulting stego-video (matl-steg.avi) frame after data hiding is shown in Figure 7(c). We observed that the original cover-video frame (matl.avi) and the video frame with hidden text (matl-steg.avi) look almost identical. The HVS can hardly notice the occurrence of this significant difference. Also, the proposed algorithm had shown good performance on the second example. Figure 7(d) shows the cover-video, c2-buzz.avi, Figure 7(e) shows the secret data to be hidden in c2, data2.txt and Figure 7(f) shows the resulting stego-video, stegbuzz.avi after hiding data2.txt in c2.

The imperceptible distortions that occurred in video by hiding data are measured using the statistical measurements like mean and median. The minor distortions were observed using the histogram results as shown in Figure 8. The figure illustrates the variation in statistical values between the cover-video and stego-video images. It can be observed that the minor difference occurred in the statistical values of the two video images does not affect the cumulative histogram, thus maintaining the good quality of the resulting video. Hence it is clearly noticed that the distortions occurred in the cover-video by applying the proposed algorithm is highly imperceptible to human eyes. This supports the robustness of the proposed scheme. The practical implementation of the proposed scheme ensures high security and robustness. The histograms of cover-video and stego-video are shown

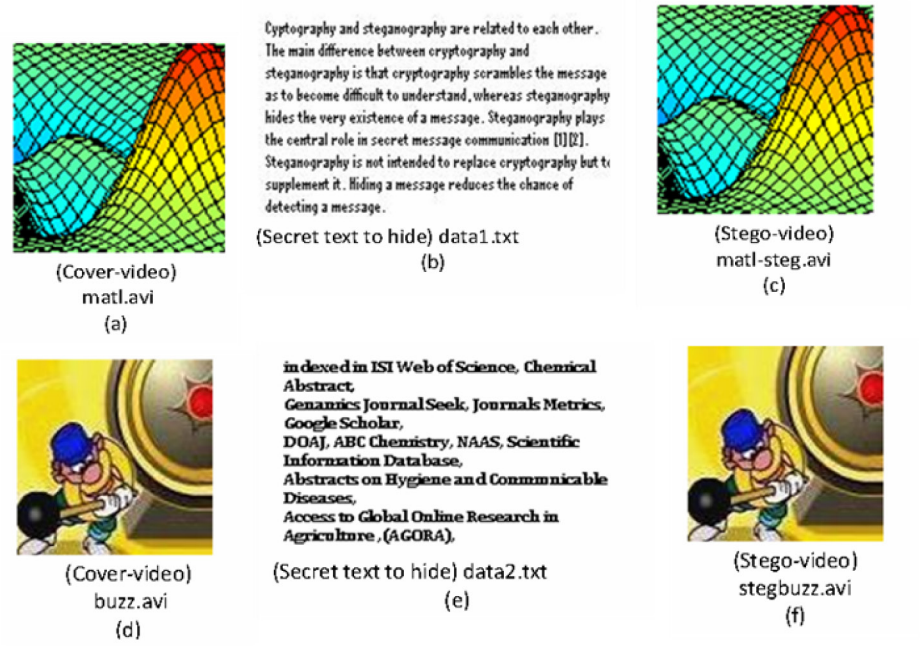
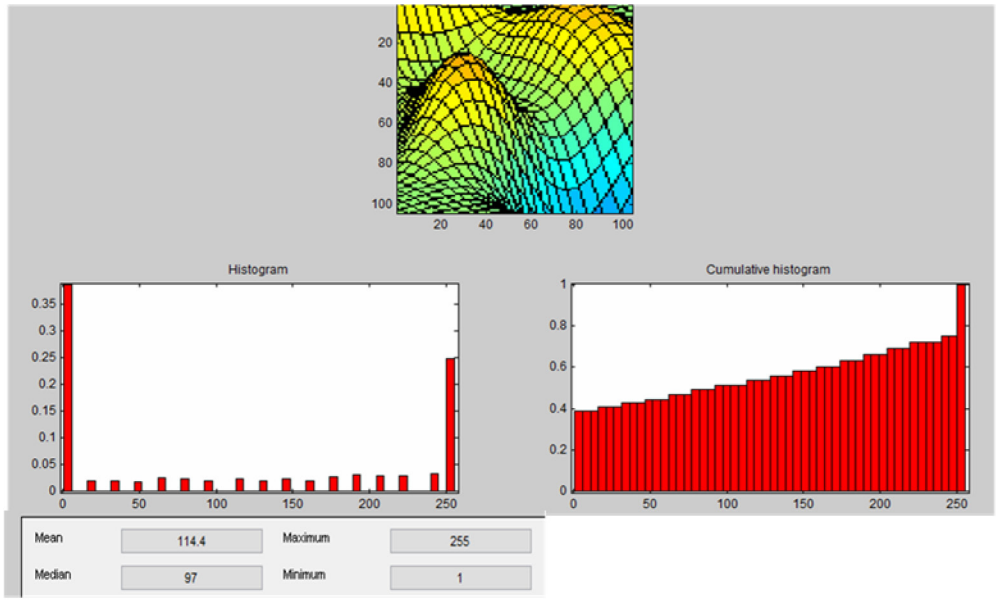
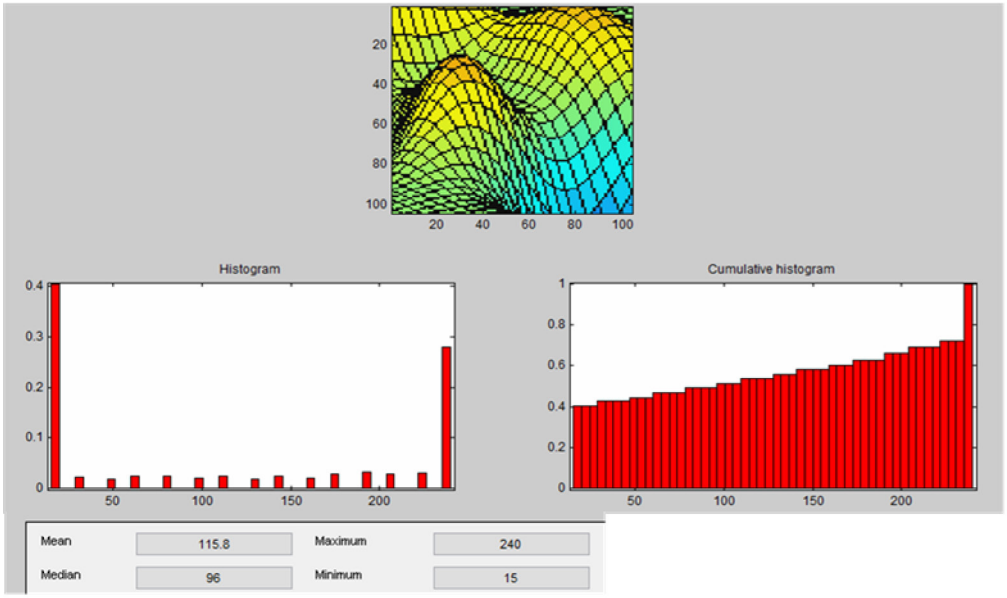


Figure 7. Examples of applying proposed steganography method on test video sequences.



(a) Original cover-video frame before data hiding, its histogram and cumulative histogram.



(b)Stego- video frame with embedded data its histogram and cumulative histogram.

Figure 8. Histogram and statistical analysis of video images before and after data hiding.

in Figure 8(a) and 8(b) respectively. The difference in the histogram results of the cover-video and stego-video frames clearly prove that the algorithm successfully hides the data into the video without making noticeable difference to the HVS.

The advantage of the proposed algorithm is that it provides high security as the data is hidden in wavelet transform domain. This system provides good quality resulting videos. Hence the proposed video steganography method is proved to be apparent to transfer highly confidential data like medical reports, banking details, military data and other important data.

5. Conclusion

We proposed a video steganography algorithm for secured data transmission with imperceptible distortions in the resulting AVI videos. We embed secret data bits in

the IWT coefficients of RGB components of the cover-video. Also, the proposed method extracts the data 100%, without any loss in quality and size of the original video files. The overall process is performed with less computational complexity. Our algorithm is simple and provides better security with less or equal distortions in test videos. To further improve on the video steganography method, future revisions include hiding multiple data at the same time and hiding different types of secret data in different types of video files without disguising the quality of the video files. Also, the data to be embedded and the secret key can be encrypted before hiding, which would enhance further security.

6. References

1. Provos N, Honeyman P. Hide and seek: an introduction to steganography. IEEE Computer Society. 2003; 32–44.
2. Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: survey and analysis of current methods. Int J Signal Process. 2010; 90(3):727–52.
3. Almohammad A, Ghinea G, Hierons RM. JPEG steganography: a performance evaluation of quantization tables. International Conference on Advanced Information Networking and Applications, AINA '09; 2009. p. 471–78.
4. Shahadi HI, Jidin R, Way WH. Lossless audio steganography based on lifting wavelet transform and dynamic Stego Key. Indian Journal of Science and Technology. 2014; 7(3):323–34.
5. Balaji R, Naveen G. Secure data transmission using video Steganography, IEEE International Conference on Electro/ Information Technology (EIT); 2011.
6. Habes A. 4 least significant bits information hiding implementation and analysis, ICGST Int Conf on Graphics, Vision and Image Processing (GVIP-05); 2005.
7. Zeng X, Ping L, Li Z. Lossless data hiding scheme using adjacent pixel difference based on scan path. Journal of Multimedia, 2009; 4(3):145–52.
8. Daubechies I. The wavelet Transform, time-frequency localization and signal analysis. IEEE Transactions on Information Theory. 1990; 36:961–1005.
9. Ghasemi E, Shanbehzadeh J, Fassihi N. High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm. Proceedings of the International Multiconference of Engineers and Computer Scientists; 2011.
10. Yang CY, Hu WC, Lin CH. Reversible data hiding by coefficient-bias algorithm. Journal of Information Hiding and Multimedia Signal Processing. 2010; 1(2):100–09.
11. Yang CY, Lin CH, Hu WC. Reversible data hiding by adaptive. IWT-coefficient adjustment, Journal of Information Hiding and Multimedia. 2011; 2(12):24–32.