Secure Video Steganography based on Discrete Wavelet Transform and Arnold Transform

Abhinav Thakur
Electronics and Communication Department, Baddi University

Harbinder Singh
Electronics and Communication Department, Baddi University

Shikha Sharda
Electronics and Communication Department, Panjab University

ABSTRACT
Internet has made so easy to transfer the large amount of data in different parts of the world. So, the security and safety of information has become the major concern. This problem has led to the development of steganography techniques. This paper deals with data hiding technique in which the secret data is embedded into the cover video. Firstly, cover video is decomposed into different frames. A single level Discrete Wavelet transform is applied on selected frame and on secret image. A private key is used during the process of encoding and decoding to provide high security. Then the Inverse Discrete Wavelet Transformation (IDWT) is applied to get the stego-video. The performance parameters like Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) can be calculated to determine the quality of stego video. The results show that the proposed algorithm for steganography is highly secured with good perceptual invisibility.

Keywords
Alpha Blending, Arnold Transform DWT, PSNR, Video Steganography.

1. INTRODUCTION
Data security deals with the protection of the secret data from eavesdroppers and unauthorized users. Cryptography and steganography are the two techniques used to deal with data security. The main objective of cryptography is to secure communications by changing the data into a form so that it cannot be understood by an eavesdropper. On the other hand, steganography techniques tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where exactly the message is.

The performance parameters that can used to measure the quality of the stego video or image are Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). One of the most important properties of the steganographic system is the statistical undetectability (imperceptibility) of the data, which shows how difficult it is to determine the existence of a hidden message. The other properties are the robustness which refers to how well the steganographic system resists the extraction of hidden data and capacity, which is the maximum information that can be safely embedded in a work.

Generally there are two approaches that can be used for video steganography, one is spatial domain and the other is frequency domain technique. In video steganography, secret data is embedded in cover video.

One of the simplest and common methods is Least Significant Bit (LSB) technique. In this method, LSB of cover video is replaced by secret data [1]. But this technique of hiding the secret data is not much effective as the data may lose after some file transformations [2] and [3]. A new method based on Discrete Cosine Transform (DCT) transformation has been introduced [4]. The main focus is to increase the capacity to hide the secret data.

A methodology based on Least Significant Bit (LSB) was introduced [5] in which secret data is embedded into the LSB of the host video frame. The quality of the stego video can be measured by using performance parameters like Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). A secure technique of video steganography was proposed [6]. This method provides index to secret data and the index is then placed in a video frame. At the receiving end, inspite of searching the whole video, the secret data can be retrieved from stego video with the help of index. This will reduced the computational time as compare to other existing methods. An improved method of data hiding based on back propagation neural network method was proposed [7]. In this method, neural network is used to perform XOR operation. Secret data is embedded into avi video format by using LSB substitution technique.

A high payload capacity video steganography method was introduced [8]. It uses Lazy lifting wavelet transform technique for hiding the secret information. Firstly wavelet is applied on the video frames and then LSB substitution method is used to hide data in the coefficients of video frames. A new data hiding technique based on Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT) was proposed [9]. This is based on the Markov-process in JPEG image steganalysis and used to detect the hidden message in stego video. A wavelet and Bit Plane Complexity Segmentation (BPCS) based video steganography method was introduced [10]. In this paper, 3-D SPIHT-BPCS steganography and motion-JPEG 2000-BPCS steganography are discussed. This technique results in high payload capacity.

This paper is organized as follows. Implementation of video steganography based on DWT and Arnold transformation is presented in Section 2. Experimental results and performance analysis are presented in Section 3. Finally, conclusions are drawn in Section 4.

2. IMPLEMENTATION OF VIDEO STEGANOGRAPHY BASED ON DWT
In this DWT based video steganography approach, two processes are used named as encoding and decoding. In this section, proposed work is discussed in detail.

2.1 Discrete Wavelet Transform (DWT)
DWT uses filter banks to perform the wavelet analysis. The discrete wavelet transform decomposes the signal into wavelet coefficients from which the original signal can be

reconstructed again. The wavelet coefficients represent the signal in various frequency bands.

(a)

(b)

Fig 1: (a) Original Lena image and (b) Lena image after wavelet decomposition

In Figure 2.1, the two dimensional signal (usually image) is divided into four bands: LL (left-top), HL (right-top), LH (left-bottom) and HH (right-bottom).

2.2 Scrambling Based on Arnold Transform

Arnold transformation is proposed by V. I. Arnold in the research of ergodic theory. The transform is a process of clipping and splicing that realign the pixel matrix of digital image. A two dimension Arnold Transform is shown as follows [11].

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (ModN)$$

Where *x* and *y* are the coordinates of the pixel; *N* is the height or width of the square image processed; *x*' and *y*' are the coordinate of the scrambled image. The transform changes the position of two pixels, and if it is done several times, a disordered image can be generated.

2.2.1 Encoding

In the encoding process, the secret image is embedded into the cover video. The cover video is separated into different frames and a specific frame (image) is used to hide the secret image by using DWT and alpha blending process. Then modified frame is integrated with rest of the frames to get stego-image. Schematically it can be represented as:

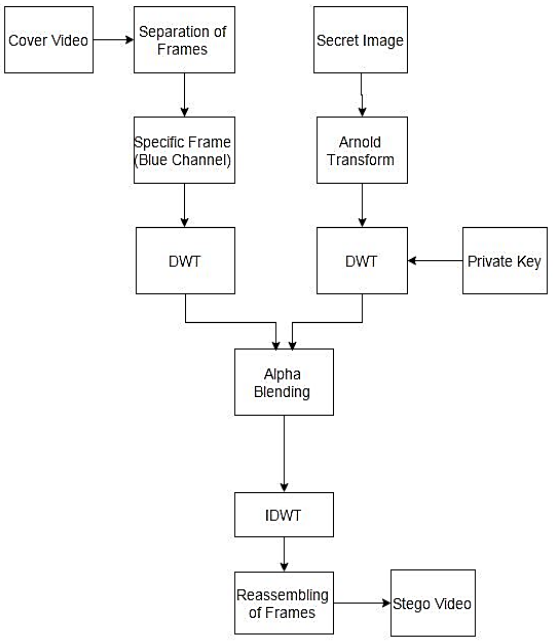


Fig 2: Encoding process

2.2.1.1 Algorithm for encoding process:

Step 1: Rhinos.avi video is taken as the cover video. The frames of the cover video are separated and save individually as .tif images.

Step 2: A specific frame (image) is accessed. That frame is divided into different channels named as red, green and blue. Now, the blue channel is used for embedding the secret image.

Step 3: Single level 2D-DWT is performed on the cover image (selected frame). It decomposes the whole image into four different coefficients such as approximation coefficient, horizontal coefficient, vertical coefficient and diagonal coefficient.

Step 4: A private key with Arnold transformation is applied on image S and Scrambled Secret Image is obtained (SS).

Step 5: Again 2D-DWT at level 1 is performed on the image SS.

Step 6: The approximation coefficient (cA), horizontal-coefficient (cH), vertical coefficient (cV) and diagonal coefficient (cD) of the stego-image is obtained as:

Approximation co-efficient of the stego image = (l-a)*Approximation coefficient of the cover + a* Approximation coefficient of the secret image similarly the same is used to find the horizontal coefficient, vertical coefficient and diagonal co-efficient of the stego-frame.

Step 7: Finally IDWT is performed to get blue channel of selected frame.

Step 8: Then the modified frame (with data) is integrated with the rest of the frames to get a stego video.

2.2.2 Decoding

In decoding process, blue frame is taken separately from the cover video and stego video. DWT is applied on the specific frame and then alpha blending operation is applied. Next, IDWT is performed to rebuild the scrambled secret image. Finally the original secret image is recovered by using the private key. Schematically it can be represented as:

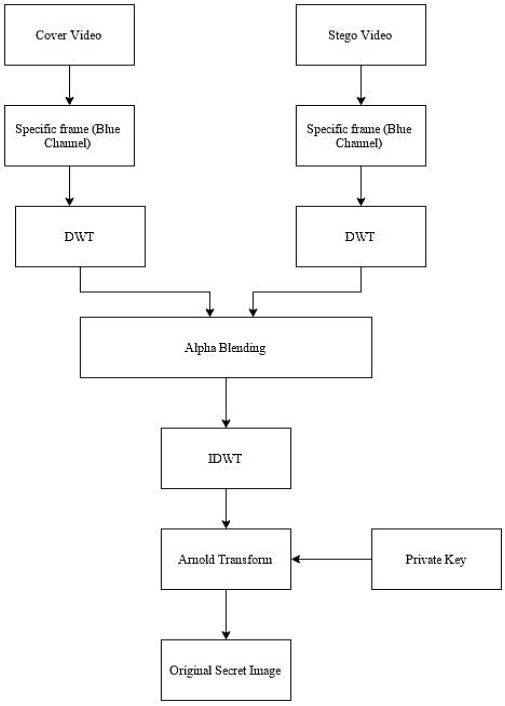


Fig 3: Decoding process

2.2.2.1 Algorithm for decoding process:

Step 1: Cover video and stego video is taken. The frames of the cover video and stego are separated and save individually as .tif images.

Step 2: A specific frame (image) is accessed. That frame is divided into different channels named as red, green and blue. Now, the blue channel is used.

Step 3: 2D- DWT is performed on selected frames (blue channel of both cover and stego video).

Step 4: Alpha blending is applied. To find the approximation co-efficient horizontal coefficient, vertical co-efficient and diagonal co-efficient of the secret image use the formula:

Approximation co-efficient of the secret image = (Approximation coefficient of the embedded image – (1-a)*Approximation coefficient of the embedded image) /a. Similarly the same is used to find the horizontal co-efficient, vertical coefficient and diagonal coefficient of the embedded image.

Step 5: IDWT is performed to reform the SS.

Step 6: Finally, Arnold transformation is performed with private key and secret image is obtained.

3. EXPERIMENTAL RESULTS AND ANALYSIS

The stego-video after embedding and recovered secret image is shown in the figure below. 2D Daubechies DWT is used for embedding and extracting. Results are obtained by using MATLAB R2012a. The value of alpha is taken as 0.01.

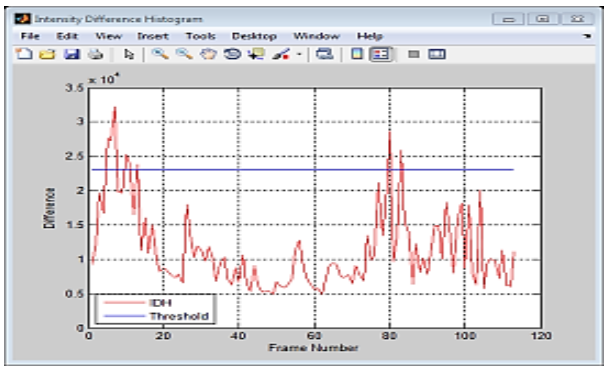
(a)

(b)

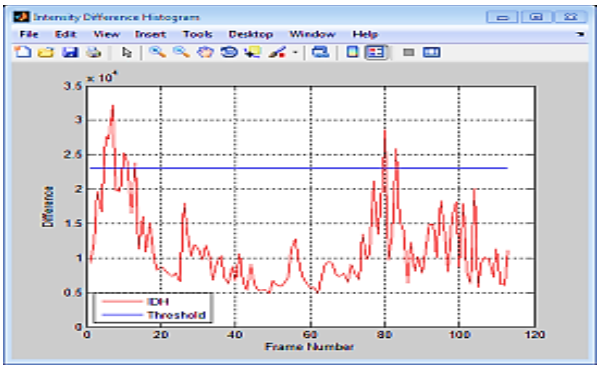
(c)

(d)

Fig4: (a) Cover video (Rhinos.avi) (b) Secret image (House.tif) and stego frame (c) Stego video (d) Extracted secret image



(a)



(b)

Fig 5: Intensity difference histogram (a) Cover video (b) stego video

3.1 Performance Analysis

There are five different image quality parameters named as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Maximum Difference (MD), Structural Content (SC) and Normalized Absolute Error (NAE) that are used to measure the quality of stego-video [12].

- Mean Square Error (MSE)

  $$MSE = \sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2$$

- Peak Signal to Noise Ratio (PSNR)

  $$PSNR = 10 \log\left(\frac{C_{max}^2}{MSE}\right)$$

- Maximum Difference (MD)

  $$MD = \text{Max}(|C_{xy} - S_{xy}|)$$

- Normalized absolute error (NAE) is defined as

  $$NA = \sum_{x=1}^{M}\sum_{y=1}^{N}|C_{xy} - S_{xy}| \Big/ \sum_{x=1}^{M}\sum_{y=1}^{N}|S_{xy}|$$

- Structural content (SC) is defined as

  $$SC = \sum_{x=1}^{M}\sum_{y=1}^{N}(C_{xy})^2 \Big/ \sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy})^2$$

Where x and y represents image coordinates, M and N are the image dimensions, S_{xy} is the stego image obtained after encoding and C_{xy} is the cover image. C_{max}^2 is the maximum value in the image. Greater the value of PSNR better is the image quality.

The summary of various quality measurements has been given in Table 1.

4. 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 many algorithms of steganography have been proposed. In this paper a wavelet based video steganography is introduced. The use of private key along with Arnold transform makes this system more secure as compared to other methods. Experimental results show that the stego video looks unaltered and have better PSNR value. Research can be extended in video steganography based on DWT. In future this method can be used with other wavelets. The various combinations of wavelets like Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT) can be applied on cover image and secret image and comparison can be made for different image quality parameters

Table 1: Comparison of various quality measurements on cover video and stego-video

Cover Video	Secret image (256x256)	MSE	PSNR	NAE	MD	SC
Rhinos.avi	House.tif	0.0000	99.9028	0.0047	0.0084	0.9996
Rhinos.avi	Lena.tif	0.0000	97.9201	0.0062	0.0083	1.0065
Rhinos.avi	Monarch.tif	0.0000	97.3706	0.0064	0.0087	1.0052
Rhinos.avi	Cameraman	0.0000	98.8700	0.0057	0.0090	1.0023

5. REFERENCES

[1] C.S. Lu, "Multimedia security: steganography and digital watermarking techniques for protection of intellectual property". *Artech House, Inc.* (2003).

[2] J.J. Chae and B.S. Manjunath, "Data hiding in Video" Proceedings of the 6th *IEEE International Conference on Image Processing, Kobe, Japan* (1999).

[3] Provos, N., Honeyman, P., "Hide and Seek: An Introduction to Steganography" *IEEE Security & Privacy Magazine 1* (2003).

[4] Y. Wang, E. Izquierdo, "High-Capacity Data Hiding in MPEG-2 Compressed Video", *9th International Workshop on Systems, Signals and Image Processing, UK,* 2002.

[5] Mrudul Dixit, "Video Steganography" *International Conference on Pervasive Computing (ICPC)* 2015.

[6] Balaji R., "Secure Data Transmission Using Video Steganography", *IEEE international conference on Electro/Information Technology (EIT)* 2011

[7] Richa K., "Video Steganography by LSB Technique using Neural Network", *Sixth International Conference on Computational Intelligence and Communication Networks* 2014.

[8] Patel, K., "Lazy Wavelet Transform Based Steganography in Video", *International conference on communication systems and network technologies (CSNT)* 2013.

[9] Qingzhong Liu,"Video Steganalysis Based on the Expanded Markov and Joint Distribution on the Transform Domains Detecting MSU Stego video" *ICMLA '08. Seventh International Conference on Machine Learning and Applications*2008.

[10] Noda, H., "Application of BPCS steganography to wavelet compressed video", Image Processing, 2004. *ICIP* '04. 2004 International Conference on (Volume:4)

[11] Lingling Wu et al., "Arnold Transformation Algorithm and Anti-Arnold Transformation algorithm", the 1st*International conference on information Science and Engineering* (ICISE2009).

[12] Prabakaran. G and Bhavani .R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform", 2012 *International Conference on Computing, Electronics and Electrical Technologies [ICCEET*].