Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-4, February 10, 2012

A High Capacity Video Steganography Based on Integer Wavelet Transform

Lakshmi narayanan K
M.E (CSE), Dept. of CSE,
Annamalai University, Annamalai Nagar, Tamil Nadu, India
E-mail: lakshmi1076@gmail.com

Prabakaran G
Asst Professor,
FEAT,Annamalai niversity,
Annamalai Nagar,
Tamil Nadu, India
E-mail:gpaucse@yahoo.com

Bhavani R
Reader,
FEAT Annamalai University,
Annamalai Nagar,
Tamil Nadu, India

Abstract - Steganography is a data hiding technique and widely used in information security applications. It is the art of invisible communication. Steganography communication system consists of an embedding algorithm and an extraction algorithm. Video Steganography is a Technique to hide any kind of files in any extension into a carrying video file. The Application developed to embed any kind of data (file) in another file, which is called carrier file. The carrier file must be a video file. It concerned with embedding information in an innocuous media. A data hiding approach for embedding different types of data in video frames is presented. In our System we utilize Integer wavelet transformation in cover image so as to get the stego-image. The capacity of the proposed algorithm is increased as the only approximation band of secret image is considered. The extraction model is actually the reverse process of the embedding model. Experimental results show that our method gets stego-image with high capacity and security with certain robustness.

Keywords: *Video Steganography, Integer Wavelet Transform, Image quality.*

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. The steganography make the presence of the secret data appear invisible to eaves droppers. The steganography is used for secret data transmission. Steganography is derived from the Greek word steganos which means “covered” and graphia which means “writing”, therefore Steganography means “covered writing”.

In steganography the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. The digital images, videos, sound files and other computer files can be used as carrier to embed the information. The object in which the secret information is hidden is called the covert object. Stego image is referred as an image that is obtained by embedding the secret image into the cover image. The hidden message may be plain text, cipher text or images etc. SEncrypting data provides data confidentiality, authentication, and data integrity.

Video signal is a highly correlated signal, this correlation is from two sources. The first one is spatial correlation that results from inter pixel correlation within each frame of the video sequence. The second one is the temporal correlation that results from the slow time varying nature of the video signals. In this paper integer wavelet transforms are used to exploit the spatial and temporal correlation in and between the video frames or minimizing the embedding distortion. The main aspect of steganography is to achieve high capacity, security and robustness. Steganography is applicable to (i) confidential communication and secret data storing, (ii) protection of data alteration, (iii) access control system for digital content distribution, (iv) media Database systems etc.

1.1 Related Work

H.S. Manjunatha Reddy et al., [1] proposed a scheme embeds a larger-sized secret image while maintaining acceptable image quality of the stego-image and also improved image hiding scheme for grayscale images based on Integer wavelet transformation. K. B Raja et al., [2] have proposed a novel image adaptive stenographic technique in the integer wavelet transform domain called as the Robust Image Adaptive Steganography using Integer Wavelet Transform. According to information theoretic prescriptions for parallel Gaussian models of images, data should be hidden in low and mid frequencies ranges of the host image, which have large energies.

Steganalysis of current Steganography tools classification and features [3]. It explains about spatial domain based steganography Least Significant Bit (LSB), BPCS. Steganography tools includes in this paper “losseless steganography” on AVI five using swapping algorithm proposed. ., [4] have proposed a combination of three different LSB insertion algorithm on GIF image through stegcure system. The unique feature about the stegcure is being able to integrate three algorithms in one Steganography system. By implementing public key infrastructure, unauthorized user is forbidden from intercepting the transmission of the covert data during a communication because the stego-key is only known by the sender and receiver.

Gaetan Le Guelvoit [5] proposed a work which deals with public key Steganography in presence of passive warden. The main aim is to hide the secret information within cover documents without any preliminary secret key sharing. This work explores the use of trellis coded quantization technique to design more efficient public key scheme. Chine-Chen chang, et al.,[6] have presented a scheme embeds a larger sized secret-image and also improved image hiding scheme for grayscale images based on wet paper coding.

In [7],we focus spatial domain techniques to hide a significant amount of information in the cover file by using LSB, several of LSB insertion exist in Novel scheme of data hiding in binary images .

II. PROPOSED METHOD

2.1 Discrete Wavelet Transform

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time). Discrete wavelet transforms

(DWT) are applied to discrete data sets and produce discrete outputs. Transforming signals and data vectors by DWT is a process that resembles the fast Fourier transform (FFT), the Fourier method applied to a set of discrete measurements. Discrete wavelet transforms map data from the time domain (the original or input data vector) to the wavelet domain. The result is a vector of the same size. Wavelet transforms are linear and they can be defined by matrices of dimension n X n if they are applied to inputs of size n. Depending on boundary conditions, such matrices can be either orthogonal or "close" to orthogonal. When the matrix is orthogonal, the corresponding transform is a rotation in $\mathbb{R}^n$ in which the data (a n-typle) is a point in $\mathbb{R}^n$. The coordinates of the point in the rotated space comprise the discrete wavelet transform of the original coordinates.

An image that undergoes Haar wavelet transform will be divided into four bands at each of the transform level. The first band represents the input image filtered with a low pass filter and compressed to half. This band is also called ‘approximation’. The other three bands are called ‘details’ where high pass filter is applied. These bands contain directional characteristics. The size of each of the bands is also compressed to half. Specifically, the second band contains vertical characteristics, the third band shows characteristics in the horizontal direction and the last band represents diagonal characteristics of the input image. Conceptually, Haar wavelet is very simple because it is constructed from a square wave. Moreover, Haar wavelet computation is fast since it only contains two coefficients and it does not need a temporary array for multi-level transformation. Thus, each pixel in an image that will go through the wavelet transform computation will be used only once and no pixel overlapping during the computation

2.2 Integer Wavelet Transform

Integer to integer wavelet transforms maps an integer data set into another integer data set. This transform is perfectly invertible and yield exactly the original data set. A one dimensional discrete wavelet transform is a repeated filter bank algorithm. The reconstruction involves a convolution with the syntheses filters and the results of these convolutions are added. In two dimensions, we first apply one step of the one dimensional transform to all rows. Then, we repeat the same for all columns. In the next step, we proceed with the coefficients that result from a convolution in both directions.

Since the integer wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective. However, the used wavelet filters have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn't allow perfect reconstruction of the original image. However, with the introduction of Wavelet transforms that map integers to integers we are able to characterize

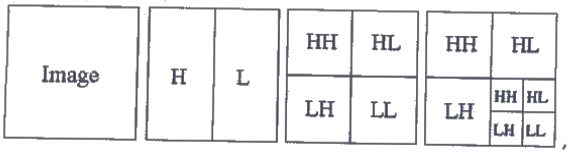

Figure 1: Two Dimensional Wavelet Transform

the output completely with integers. One example of wavelet transforms that map integers to integers is the *S-transform*.

Its smooth (*s*) and detail (*d*) outputs for an index *n* are given in (1) and (2) respectively. Note that the smooth and the detail outputs are the results of the application of the high-pass and the low-pass filters respectively. At the first sight it seems that the rounding-off in this definition of s(n) discards some information. However, the sum and the difference of two integers are either both odd or both even. We can thus safely omit the last bit of the sum since it equals to the last bit of the difference. The *S - transform* is thus reversible and its inverse is given in equations (3) and (4).

$$s(n) = \left\lfloor \frac{x(2n) + x(2n+1)}{2} \right\rfloor \quad (1)$$

$$d(n) = x(2n) - x(2n+1) \quad (2)$$

$$x(2n) = s(n) + \left\lfloor \frac{d(n)+1}{2} \right\rfloor \quad (3)$$

$$x(2n+1) = s(n) - \left\lfloor \frac{d(n)}{2} \right\rfloor \quad (4)$$

Generally, the 2D S-transform can be computed for an image using equations (5), (6), (7), and (8). Of course the transform is reversible, i.e., we can exactly recover the original image pixels from the computed transform coefficients. The inverse is given in equations (9), (10), (11), and (12). The transform results in four classes of coefficients: (A) is the low pass coefficients, (H) coefficients represent horizontal features of the image, (V) and (D) reflect vertical and diagonal information respectively. During the transform we ignore any odd pixels on the borders.

$$A_{i,j} = \lfloor (I_{2i,2j} + I_{2i+1,2j})/2 \rfloor \quad (5)$$

$$H_{i,j} = I_{2i,2j+1} - I_{2i,2j} \quad (6)$$

$$V_{i,j} = I_{2i+1,2j} - I_{2i,2j} \quad (7)$$

$$D_{i,j} = I_{2i+1,2j+1} - I_{2i,2j} \quad (8)$$

$$I_{2i,2j} = A_{i,j} - \lfloor H_{i,j}/2 \rfloor \quad (9)$$

$$I_{2i,2j+1} = A_{i,j} - \lfloor (H_{i,j}+1)/2 \rfloor \quad (10)$$

$$I_{2i+1,2j} = I_{2i,2j+1} - V_{i,j} - H_{i,j} \quad (11)$$

$$I_{2i+1,2j+1} = I_{2i+1,2j} - D_{i,j} - V_{i,j} \quad (12)$$

Where, $1 \leq i \leq x/2, 1 \leq j \leq y/2$

The presented transforms are not computed using integer arithmetic's, since the computations are still done with floating point numbers. However, the result is guaranteed to be integer [8] due to the use of the floor function and hence the invertetibility is preserved.

III. PROPOSED MODEL

3.1Fusion Encoder

The main idea behind the proposed algorithm is the Integer wavelets transform based fusion. The figure 3 shows the embedding algorithm, it involves merging wavelets decomposition of the normalized version of both the cover images and secret image into a single fused result. Both cover images and secret image into IWT domain. Further apply IWT on the secret image to increase the security level. The single fused resultant matrix is obtained by the addition of wavelet coefficient of the respective sub bands of the cover images and secret image is given by the equation [13]

$$F(x,y) = \alpha\, c(x,y) + \beta\, s(x,y) \qquad (13) \qquad \alpha + \beta = 1$$

Where, c(x,y) - Cover Image, S(x,y) - Secret Image, α, β = Fusion Parameters

Once fusion is done we apply Inverse. Integer wavelets transform to get the stego images in the spatial domain.

3.1.1 Algorithm of Data Embedding

Step 1: Get a video of (.avi) as and input of time 2 seconds.
Step 2: Sequence of cover image c and secret image s are taken from the video.
Step 3: Take the one frame as the cover image and hide secret image into cover image.
Step 4: Apply IWT on both the cover image and secret image.
Step 5: Secret image 2 level decomposition is fused into cover image.
Step 6: Apply Inverse Integer Wavelet transform on that image.
Step 7: Stego image is generated

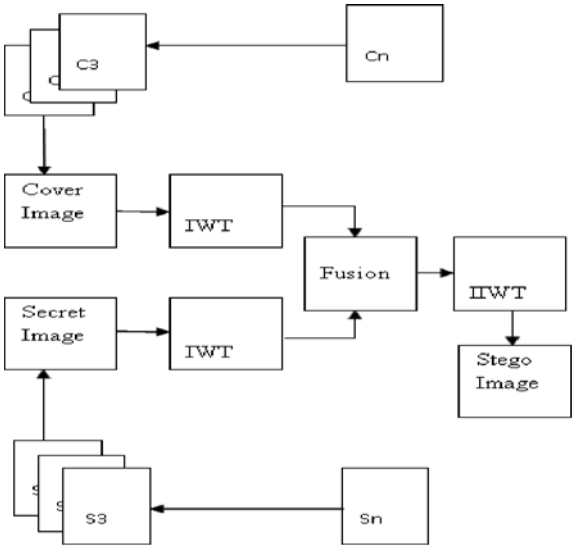

Figure 2 : Shows the Image Fusion Encoding Process

3.2 Fusion Decoder

From the decoder fig 3 it shows the retrieval of secret image from the stego image. The stego image is normalized, and then IWT is taken. The extraction process involves subtracting the IWT coefficient of the original cover image from IWT coefficient of stego image. It is then followed for decryption of subtracted coefficient. The first step of IIWT on these coefficients is applied by second IIWT, and coefficient of secret image is found.

3.2.1 Algorithm of Data Extraction

Step 1: Receive the Stego image as the input of decoder.
Step 2: Apply the IWT for the original cover image and the secret image.
Step 3: Apply Fusion process for stego and cover image.
Step 4: Apply the Inverse IIWT for secret image.
Step 5: The secret image is obtained.

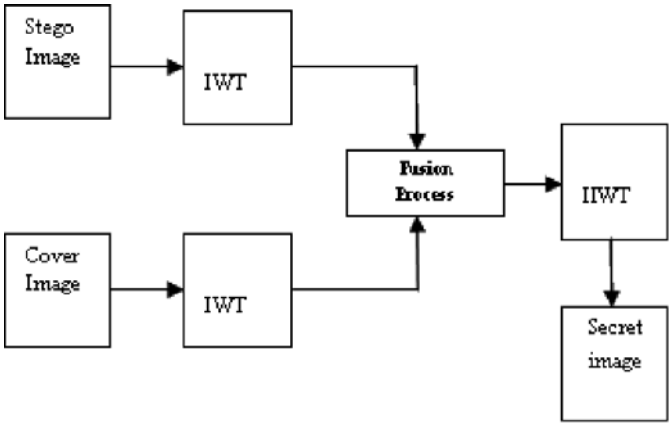

Figure 3: Shows the Image Fusion Decoding Process

IV. PERFORMANCE ANALYSIS

For performance analysis we consider the secret image is embedded into the cover image to derive the stego at the sending end. The secret image is recovered from the stego image at the destination with minimum distortion.

4.1 MEAN SQUARE ERROR (MSE)

The experimental results obtained are subjected to various statistical techniques to evaluate the performance parameters of steganography images.
Mean Square Error is calculated as in (14)

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x_{j,k}\right)^2 \qquad (14)$$

Where, m X n size of the image with j=0, 1…….M & k=0, 1……N

4.2. PEAK SIGNAL TO NOISE RATIO (PSNR)

The Peak Signal to noise ratio (PSNR) is used in experiment to evaluate the quality of the container image and after embedded stego Image.

$$PSNR = \frac{10 \log_2 (255)^2}{MSE} \qquad (15)$$

The some of the image quality measurement has been illustrated in table and corresponding tested results shown in the table 1.

Table 1: Comparison of Various Quality Measurements on Cover-Images with Secret Images

Cover Image	Secret Image	MSE	PSNR
Car 320x240	Cat 320x240	0.8009	49.0949
Cute 320x240	Lady 960x720	1.0970	47.7287
Girl 320x240	Manisha 646x288	0.5516	50.7149
Hill 320x240	Benz 320x180	0.5886	50.4330

The image quality factors MSE, PSNR and other quality measurement are observed. The effectiveness of the stego image formation proposed has been studied by calculating MSE and PSNR for the two digital images. The result data shows that for less MSE and High PSNR value. Embedding capacity of the proposed method has been computed which is better than the most cases compared to the existing methods. The MSE and PSNR value is also better than existing methods after embedding of secret image in various coefficient of cover image.

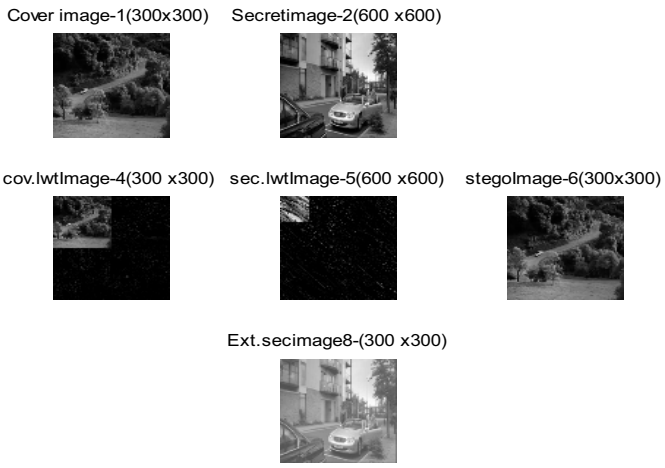

Figure 4: Shows the Cover Image and Stego Image with Secret Image

V. CONCLUSION

We achieved a new enhanced Video steganography methodology along with a suitable encryption scheme. Also it involves merging wavelets decomposition of the normalized version of both the cover images and secret images into a single fused result both cover images and secret image into IWT domain further apply IWT on the secret image to increase the security level. In this paper integer wavelet transforms are used to exploit the spatial and temporal correlation in and between the video frames or minimizing the embedding distortion. This algorithm is to achieve high capacity security and certain robustness. Another achievement of a wavelet basis is that it supports multi resolution. In future, this technique is applied to multiple wavelet transform and extended to color images.

REFERENCES

1. H.S Manjuatha Reddy and K.B Raja. “High Capacity and Secirity Steganography uing Integer Wavelet Transform”, International journal of Computer Scince and Security, (IJCSS), Volume(3): Issue (6), 2010.
2. K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal,L. M. Patnaik, “Robust Image Adaptive Steganography using Integer Wavelets” Internationalconference on Communication Systems Software, pp. 614-621, 2009.
3. A.J. Mozo, M.E.Obien, C.J.Rigor, D.F.Rayel, K.Chua, G.Tangonan “Video steganography using flash video (FLV)”. 12MTC 2009 International Instrumentation and Measurement Technology Conference Singapore, pp.5-7, May-2009
4. L. Y. Por, W. K. Lai, Z. Alireza, T. F. Ang, M. T. Su, B. Delina, “StegCure: A Comprehensive Steganographic Tool using Enhanced LSB Scheme,” Journal of WSEAS Transctions on Computers,vol. 8, pp. 1309-1318, 2008.
5. Gaetan Le Guelvouit, “Trellis-Coded Quantization for Public-Key Steganography,” IEEE International onference on Acostics, Speech and Signal Processing, pp.108-116, 2008.