Robust and Secure Video Steganography Method in Haar Wavelet Domain Based on Multiple Object Tracking and ECC

Roopa Raju

Department of Electronics& Communication
Jawaharlal College of Engineering &Technology
Palakkad, Kerala, India

Felix.M.Philip

Department of Electronics & Communication
Jawaharlal College of Engineering&Technology
Palakkad, Kerala, India

Abstract *—Video steganography has become a popular method for secret data communication. The performance of any steganography algorithm is based on the imperceptibility, embedding capacity, and robustness against attackers. In this paper, a new video steganography algorithm method in DCT-DWT domain based on the multiple object tracking algorithm and Error correction codes. We are using Haar Wavelet Transform in DWT domain. The proposed algorithm includes four different stages. First, the secret message is pre-processed using BCH and Hamming codes (n, k) to produce an encoded message. Second, a motion-based multiple object tracking algorithm is applied on cover videos to identify the regions of interest of the moving objects. Third, the data hiding process is performed by concealing the secret message into the DWT and DCT coefficients of all motion regions in the video depending on foreground masks. Fourth, the process of extracting the secret message from each RGB component of all moving regions.*

Keywords—*Video steganography, Multiple object tracking, DWT, ECC, DCT, Haar wavelet transform, Imperceptibility, Embedding capacity, Robustness* .

I. Introduction

In the modern world, there are many ways to transmit data using internet. The transmission of data is quite simple, fast and accurate, but main problem is that the confidential data has been hacked or stolen in different ways. The main objective of the project is to provide a secure data communication using steganography. The user can transmit secret data within cover media and provide a less suspicious means of data communication when compared to cryptography. Video Steganography is a technique used to hide multimedia files into a video file. Video steganography algorithms gain more attention to researchers due to size and memory requirements of video data, many of these algorithms lack preprocessing stages. Small distortions might unobserved by humans because of the continuous flow of information .The preprocessing stages are applied before embedding stage to enhance the security and robustness of the steganographic method. This steganographic method has the capacity to withstand against both noises and signal processing operations.

II. PROPOSED SYSTEM

In the proposed method we have used Haar wavelet transform and discrete cosine transform for converting image from its spatial domain to frequency domain. The main purpose of converting an image into frequency domain during steganography is that when we insert our secret information into frequency domain it is very difficult to detect steganography.

The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate, Vertical, Horizontal, and diagonal band. Significant part of the spatial domain image is in the approximation band, that is the low frequency wavelet coefficients .Other bands are called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image. HAAR wavelet transform is a fast wavelet transform which computes very fast. Haar wavelet Transform supports reliable coding efficiency, high compression ratio, and better image restoration quality compared with the traditional transforms.

Another transform used is DCT (Discrete Cosine Transform) which separates the image into parts (high, medium and low frequency components) and the secret message is hidden in the least significant bit of the medium-frequency components. DCT works by slightly changing each of the images in the video, only so much that it is not noticeable by the human eye. DCT alters values of certain parts of the images, it usually rounds them up. By concealing the secret data using both transform into coefficients of all motion regions in the video depending on foreground masks.

The proposed system of secure video steganography method in Haar Wavelet Transform and DCT domains based on multiple object tracking and error correcting codes and its methodology is divided into following four stages:

A. Preprocessing Stage

A defined text data is selected as the secret message and it is preprocessed earlier to the data embedding stage, which is ciphered and coded by Hamming and BCH (7, 4) codes. The characters in the text file are converted into ASCII codes in order to generate an array of binary bits. Then the binary array is encrypted by using a key (key 1) that represents the size of the secret message. This process will encode the message and protect it from attackers. Since the binary linear block of Hamming and BCH codes (7,4) are used ,the encrypted array is divided into 4 bit blocks. Then, every block is encoded by the hamming and BCH codes (7, 4) .The size of the message is extended by adding four parity bits into each block. Another key (key 2) is utilized to generate the randomized 7 bit numbers, and each number is XORed with encoded block. The security of the proposed algorithm will be improved by using two keys, XOR operation, BCH and Hamming codes. The process of encrypting and encoding secret message is represented in Fig 1.

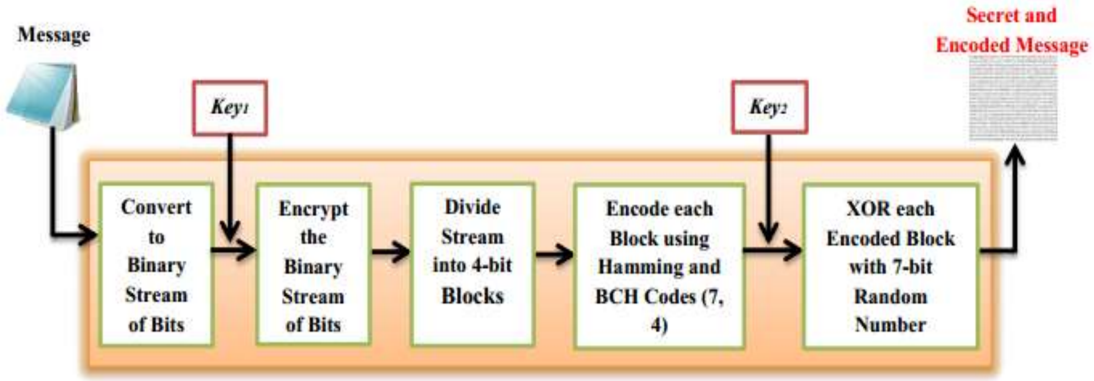
Message
Key1
Key2
Secret and Encoded Message
Convert to Binary Stream of Bits
Encrypt the Binary Stream of Bits
Divide Stream into 4-bit Blocks
Encode each Block using Hamming and BCH Codes (7, 4)
XOR each Encoded Block with 7-bit Random Number

Fig 1 Encrypting and Encoding input messages

B. Motion Based MOT Stage

Computer vision is one of the fastest emerging fields in computer science and has various applications. The detection and tracking of moving objects within the computer vision field has recently gained significant attention. The process of identifying the moving objects in the video frames must be carried out when motion object regions are utilized as host data. The process is achieved by detecting each moving object within an individual frame, and then associating these detections throughout all of the video frames. The tracking of moving objects is commonly divided into two major phases:

- Detecting the moving objects in an individual video frame, and
- Associating these detected objects in all video frames in order to construct complete tracks.

In the first phase, the background subtraction technique is used to detect the regions of interest such as moving objects. This technique is based on the Gaussian mixture model which is the probability density function that equals to a weighted sum of component Gaussian densities. The background subtraction method computes the differences between consecutive frames that generate the foreground mask. Then, the noises will be eliminated from the foreground mask by using morphological operations. As a result, the corresponding moving objects are detected from groups of connected pixels.

The second phase is known as data association. It is based on the motion of the detected object. A Kalman filter is used to detect the motion of each trajectory. In each video frame, the location of each trajectory is predicted by the Kalman filter. Moreover, the Kalman filter is utilized to determine the probability of a specific detection that belongs to each trajectory. The below figure shows a number of video frames that contain multiple objects and their foreground masks.

C. Data Embedding Stage

In our proposed method, the motion objects are considered as regions of interest. Fig 2 shows the block diagram of the data embedding stage of the proposed algorithm. By using the motion-based MOT algorithm, the process of detecting and tracking the motion regions over all video frames are achieved. The regions of interest altered in each video frame is dependent on the number and the size of the moving objects. In every frame, 2Dimensional-Haar Wavelet Transform (2D-HWT) is implemented on RGB channels of each motion region resulting LL, LH, HL, and HH subbands. In addition, 2Dimensional-Discrete Cosine Transform (2D-DCT) is also applied on the same motion regions generating DC and AC coefficients. Thereafter, the secret messages are concealed into LL, LH, HL, and HH of HWT coefficients, and into DC and AC of DCT coefficients of each motion object separately based on its foreground mask. Furthermore, both secret keys are transmitted to the receiver side by embedding them into the non-motion area of the first frame. Then, the stego video frames are rebuilt in order to construct the stego video that can be transmitted through the unsecure medium to the receiver.

D. Data Extraction Stage

In order to recover hidden messages accurately, the

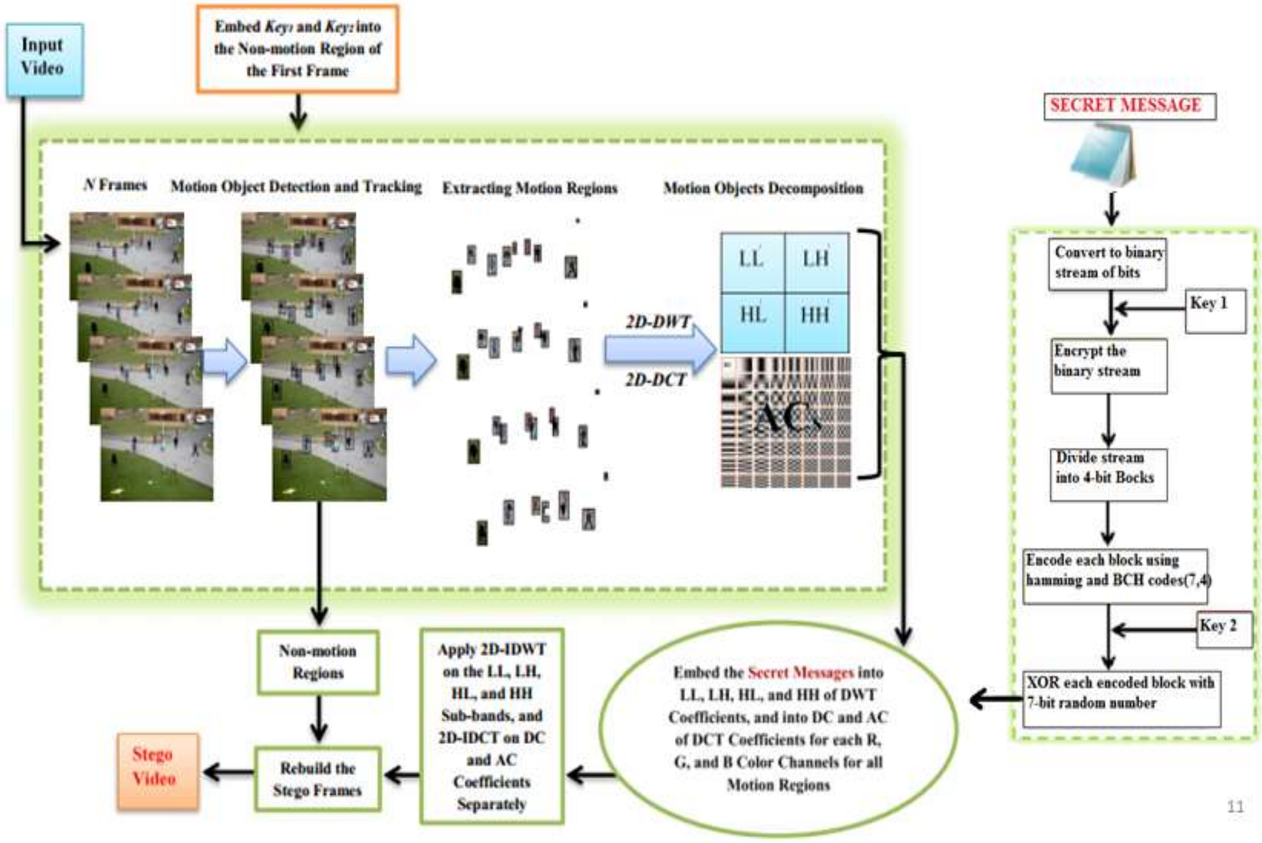
Input Video
Embed Key1 and Key2 into the Non-motion Region of the First Frame
N Frames
Motion Object Detection and Tracking
Extracting Motion Regions
Motion Objects Decomposition
2D-DWT
2D-DCT
LL
LH
HL
HH
ACs
SECRET MESSAGE
Convert to binary stream of bits
Key 1
Encrypt the binary stream
Divide stream into 4-bit Bocks
Encode each block using hamming and BCH codes(7,4)
Key 2
XOR each encoded block with 7-bit random number
Embed the Secret Messages into LL, LH, HL, and HH of DWT Coefficients, and into DC and AC of DCT Coefficients for each R, G, and B Color Channels for all Motion Regions
Apply 2D-IDWT on the LL, LH, HL, and HH Sub-bands, and 2D-IDCT on DC and AC Coefficients Separately
Non-motion Regions
Rebuild the Stego Frames
Stego Video
11

Fig 2 Block diagram of data embedding stage

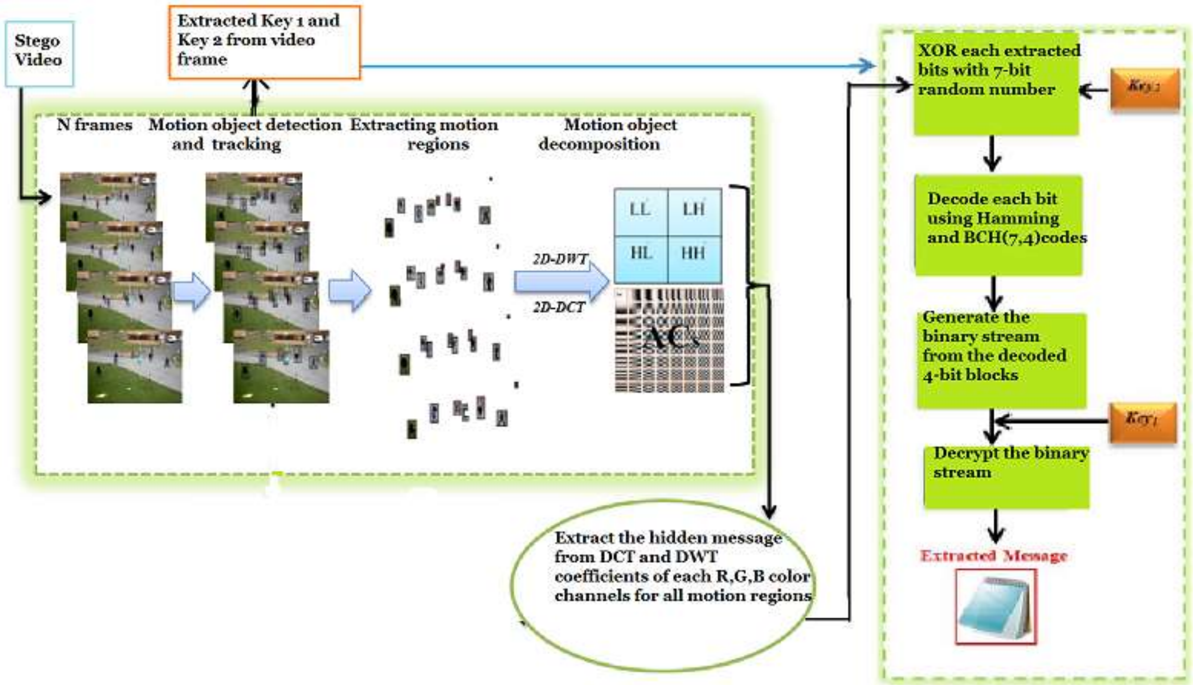
Stego Video
Extracted Key 1 and Key 2 from video frame
N frames
Motion object detection and tracking
Extracting motion regions
Motion object decomposition
2D-DWT
2D-DCT
LL
LH
HL
HH
ACs
Extract the hidden message from DCT and DWT coefficients of each R,G,B color channels for all motion regions
XOR each extracted bits with 7-bit random number
Key2
Decode each bit using Hamming and BCH(7,4)codes
Generate the binary stream from the decoded 4-bit blocks
Key1
Decrypt the binary stream
Extracted Message

Fig 3 Block diagram of data extraction stage

embedded video is separated into a number of frames through the receiver side, and then two secret keys are obtained from the non-motion region of the first video frame. Block diagram of the data extraction stage of the proposed algorithm is represented in Fig 3. To predict trajectories of motion objects, the motion-based MOT (Multiple Object Tracking) algorithm is applied again by the receiver. Then, 2D-HWT and 2D-DCT are employed on the RGB channels of each motion object in order to create LL, LH, HL, and HH subbands, and DC and AC coefficients, respectively. Next, the extracting process of the embedded data is achieved by obtaining the secret messages from LL, LH, HL, HH, DC, and AC coefficients of each motion region over all video frames based on the same foreground masks used in the embedding stage. The extracted secret message is decoded by Hamming and BCH (7, 4) codes, and then decrypted to obtain the original message.

III.PERFORMANCE EVALUATION PARAMETERS

All the steganographic methods have to observe some of the basic parameters, which are analyze through experimentation to measure the performance of the applied techniques. The parameters are as follows:

A. Imperceptibility

The Imperceptibility is the property in which a person should be unable to distinguish the original and the stego-image. Modern day steganalysis approaches are highly intelligent to detect slight modifications. High Imperceptibility has motivated researches to design steganalysis resistant video steganography methods. The imperceptibility of our proposed scheme is measured by utilizing a Peak Signal to Noise Ratio (PSNR) measurement, which is a well-known metric and can be calculated as follows:

$$\text{PSNR} = 10*\log\left(\frac{MAXa^2}{MSE}\right)\ \text{(dB)}$$

MSE represents Mean Square Error. *MAXA* is the highest pixel value of the frame A. Overall, the embedded video qualities are near to the host videos qualities because of the high values of PNSRs for our proposed algorithm.

B. Embedding Capacity

Embedding Capacity is the amount of secret information that can be embedded without degrading the quality of the image. Videos are getting popular due to their high embedding capacity and embedding efficiency. According to our suggested method has a high embedding capacity. Here, the average of the gained hiding ratio is 3.46% using DWT domain. The average sizes of secret messages in both domains varies when using one LSB, two LSBs, and three LSBs of DWT and DCT coefficients, respectively. The hiding ratio (HR) is calculated as follows:

$$\text{HR=}\ \frac{Size\ of\ embedded\ message}{Video\ size}\ X100\%$$

C. Robustness

Robustness is the third requirement which measures the steganographic method's strength against attacks and signal processing operations. That is it refers to the degree of difficulty required to destroy embedded information without destroying the cover image. These operations contain geometrical transformation, compression, cropping, and filtering. A steganographic method is robust whenever the recipient obtains the secret message accurately, without bit errors. An efficient steganography method withstands against both adaptive noises and signal processing operation. Similarity (Sim) index and Bit Error Rate (BER) metrics have been utilized. The Sim ($0 \leqslant Sim \leqslant 1$) and BER can be calculated. The algorithm used different attacks such as Gaussian noise, Salt & pepper noise, and median filtering. The highest robustness of our method can be achieved when the maximum Sim and minimum BER values are gained.

IV.RESULT& CONCLUSIONS

Robust and secure video steganography method in Haar wavelet Transform and DCT domains based on MOT and ECC is proposed in this paper. The proposed algorithm consists of 1) Preprocessing stage 2) the motion-based MOT algorithm, 3) data embedding, and 4) data extraction stages. The performance of our method is verified using experiments, demonstrating the high embedding capacity for DWT and DCT domains, respectively. An average PSNR of above 49.01 dB for DWT and DCT domains are achieved leading to a better visual quality for the proposed algorithm when compared to existing methods of the literature. The proposed algorithm has utilized MOT and ECC as the preprocessing stages which in turn provides a better confidentiality to the secret message earlier to embedding phase. The security and robustness of the method against various attacks have been confirmed through various experiments.

ACKNOWLEDGMENT

My endeavour stands incomplete without dedicating my gratitude to everyone who has contributed a lot towards successful completion of my work. First of all, I offer thanks to my parents for their blessings. I am indebted to God Almighty for blessing me with his grace and taking my endeavour to a successful culmination.

I specially acknowledge **Prof. C Venugopal**, Professor and Head of the Department and my project guide **Mr.Felix.M.Philip**, Assistant Professor, ECE for her technical support and guidance given to me and steering me to successful completion of this work.

REFERENCES

[1] N. Ke and Z. Weidong, "A video steganography scheme based on H. 264 bit streams replaced," in 4th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2013, pp. 447-450.

[2] R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes," in 2015 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2015, pp. 1-7.

[3] Mohammed Abd Al-Hassan Hussein, "Video steganography based on discrete cosine transform method", Thesis on Physics, 2014.

[4] X.-y. Wang,et al; "A robust blind color image watermarking in quaternion Fourier transform domain," Journal of Systems and Software, vol. 86, pp. 255-277, 2013.

[5] S. Islam, M. R. Modi, and P. Gupta, "Edge-based image steganography," EURASIP Journal on Information Security, vol. 2014, pp. 1-14, 2014.

[6] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "A secure and improved self-embedding algorithm to combat digital document forgery," Signal Processing, vol. 89, pp. 23242332, 2009.

[7]Poonam V Bodhak, Baisa L Gunjal, “Improved Protection in Video Steganography using DCT and LSB”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[8] M. Sajjad, et al., "Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices," Multimedia Tools and Applications, vol. 76, pp. 35193536, 2017.

[9] L. Guangjie, L. Weiwei, D. Yuewei, and L. Shiguo, "Adaptive Steganography Based on Syndrome-Trellis Codes and Local Complexity," in 2012 Fourth International Conference on Multimedia Information Networking and Security (MINES), 2012, pp. 323-327.

[10] A. Singh, B. Kumar, S. Singh, S. Ghrera, and A. Mohan, "Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network," Future Generation Computer Systems, 2016.