Indian Journal of Science and Technology, *Vol 10(29), DOI: 10.17485/ijst/2017/v10i29/115603,* August *2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Reversible Video Steganography using Hybrid DWT- DCT with Secure Cryptographic Technique and GPU

Premanand P. Ghadekar[1] and Farah J. Iqbal[2]

[1]Department of Information Technology and Master in Computer Application, Vishwakarma Institute of Technology, Pune – 411037, Maharashtra, India; ppghadekar@gmail.com
[2]Department of Computer Engineering, Vishwakarma Institute of Technology, Pune – 411037, Maharashtra, India; farahiqbal1@gmail.com

Abstract

Objectives: To propose a system that allows hiding of a video as secret message under the cover medium for secured transfer. **Methods/Statistical analysis**: In early days most of the work is done to hide multimedia data such as text, images, audio by using Least Significant Bit (LSB) and Most Significant Bit (MSB) techniques. Use of LSB and MSB techniques for data hiding affects the quality of the cover medium also it allow to hide limited amount of data. **Findings:** Exchange of large amount of secret data is not possible when multimedia data is used as a secret message. So video steganography is used, which allows to hide large amount of secret data and to transfer it securely. Proposed system allows hiding video as secret message under the cover medium. This is used for hiding and transmitting significantly more amount of data securely as compared to that of the existing systems. In the proposed work, hybrid DWT-DCT is applied on each frame of both cover video stream and secret video stream. For embedding, SVD (Singular Value Decomposition) is applied on LL band of each frame. For reducing the execution time the proposed model is implemented using GPU (Graphics Processing Unit). From results of proposed system 2.09 MB video can be hidden under the 2.27MB video which shows quite high capacity for hiding than any other video steganographic existing system. Also the quality of video does not get affected even after embedding the secret video. **Improvements:** Further work can be done to enhance the image quality of retrieved secret video.

Keywords: Cryptographic Technique, GPU, Hybrid DWT-DCT, Reversible Video Steganography, SVD

1. Introduction

As the internet users are increasing day by day the amount of data being exchanged is also increasing. But not all the transmission medium provides secure exchange of data. So for transferring some confidential or sensitive data, some secured transmission medium is required. For this, a proper data hiding technique can be used, which will provide security during transmission. Steganography and cryptography are the two widely used data hiding techniques[1,2].

Steganography is the art and science of hiding a secret message into the cover medium without knowing the existence of the secret message. In other words, when a secret data is embedded in a cover medium, the output is known as stego-object[3].

Cryptography transforms the data into unreadable form which is called ciphertext[1,2]. Steganography totally hides the existence of secret message so that only the authorized persons can have access to it while cryptography scrambles the message into unreadable form so that intended users can process it[2,4].

In this paper, both steganography and cryptography are combined to get better security. For hiding the secret video stream under the cover video stream hybrid DWT-DCT algorithm is used. Each frame is decomposed into non-overlapping four sub-bands LL, HL, LH, HH[5,6] using

*Author for correspondence

Discrete Wavelet Transform (DWT). After this Discrete Cosine Transform (DCT) is applied to LL band to determine the frequency region, then SVD (Singular Value Decomposition) is used for embedding the secret data. AES cryptographic algorithm is used to scramble the secret video stream which provides more security.

The core objective of the proposed algorithm is to hide the secret video stream under the cover video stream using hybrid DWT-DCT. For security, confidentiality and authorized access AES cryptographic algorithm are used.

For steganography, a lot of work is proposed using different algorithms along with different methods. But each method has its own pros and cons depending upon the different factors such as hiding capacity for secret message, cover medium video quality, quality of recovered secret message, execution time, time required for embedding and extraction of the secret message, perceptual video quality of stego-video, time required for encryption and decryption, etc. Most of the work is done using Least Significant Bit (LSB) and also by using different algorithms.

Hiding of secret video under the cover video using LSB technique with sequential encoding and encrypted using[7]. However, the problem is that it takes more time for encryption by using XOR; there is a little bit distortion in the recovered secret video. Moreover, stego-video contains shadow after embedding the secret video.

In[8] proposed embedding of multimedia data such as text, audio, image in the original image using new chaos steganographic algorithm. Results show good quality of original image even after embedding. But it does not provide space for embedding large amount of data. Also, it is limited to text, audio, and images.

Algorithm for embedding text in the original video by using linked list method along with cryptography is done[9]. In this secret text is encrypted using feistel network and linked list is used for embedding the cryptographic key. In this paper, feistel network is used for cryptography, but it takes time for encryption and decryption though it provides security to secret data.

The model by[10] consists of various techniques RSA encryption, edge detection, identical matches' technique and 4th LSB substitution. In this secret message is embedded in selected cover video frames by detecting edges from RGB frame using canny edge detector. Then 4th LSB is used along with identical match technique for hiding the data. There is some distortion in the output as secret data is embedded in 4th LSB this affects the video quality. Also embedding of secret data in RGB layers of cover medium affects the quality of image.

2. Proposed Work

Objectives of proposed algorithm are:

- To hide a huge amount of secret data under the cover medium.
- To embed the secret data with better quality of cover medium.
- To retrieve secret data with good and acceptable quality.
- To encrypt and decrypt secret data with less execution time.
- To decompose the image frames efficiently and reduce time complexity by using GPU.

2.1 Proposed Algorithm

Figure 1 shows the block diagram of proposed work.

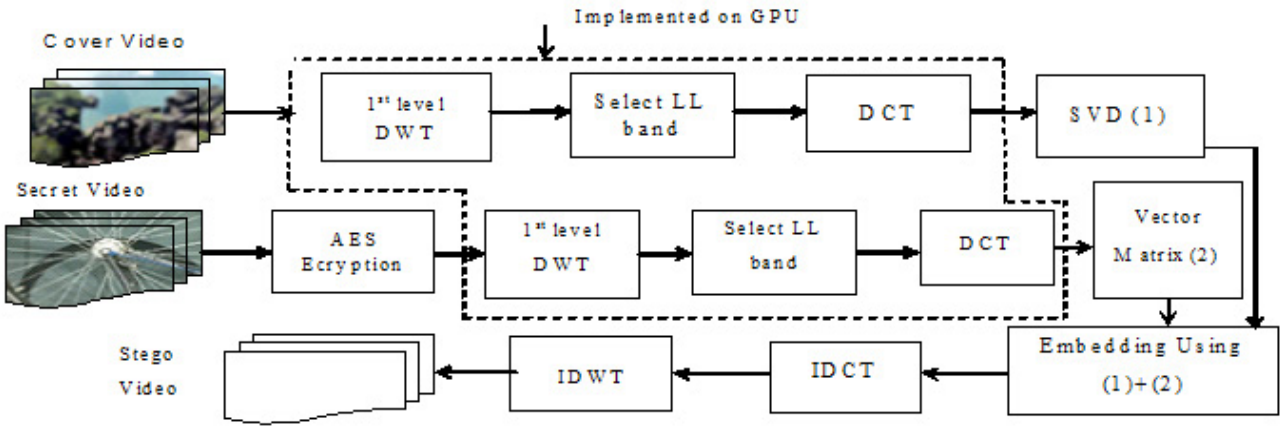

Figure 1. Proposed model using hybrid DWT-DCT for embedding secret video stream into cover video.

2.1.1 Phases of Proposed Work

2.1.1.1 Pre-Processing

First both cover and secret videos are broken into number of images. Then zigzag scanning is done over each image to group the low frequency co-efficient in the images.

2.1.1.2 AES Encryption

Secret video images are encrypted using AES encryption algorithm. Use of AES provides faster encryption and high level security. AES does not use feistel network so encryption is done in less amount of time. Also AES is robust against different cryptographic attacks such as cipher text attack, known plaintext attack, chosen plaintext attack, dictionary attack and brute force attack.

2.1.1.3 Hybrid DWT-DCT

It is applied on each image frame of both cover and secret video for decomposing it into LL, LH, HL, HH bands. Out of these bands, LL is selected as it contained low-frequency coefficient and it is similar to original image. After this DCT is applied over LL band of cover image frames for dividing it into low-frequency, middle-frequency, high-frequency components and compressing the secret image frames. Out these components middle-frequency components are selected because it allows embedding large amount of data and providing robustness.

2.1.1.4 Vector Matrix and SVD

Each secret video frame is converted into vector matrix ranging from 0-255

SVD is the tool used for mapping one vector matrix into the other. SVD is matrix of size m×n consisting of 3 matrices $G = USV^T$ where U is orthogonal matrix of size m×m and $U^TU = I$ (I is identity matrix) in U columns are orthonormal containing eigenvectors of GGT. Similarly V is orthogonal matrix of size n×n and $V^TV = I$ (I is identity matrix) in V rows of V^T are eigenvectors of GTG. GG^T is the left singular vector of U and G^TG is the right singular vector of V. And S is the diagonal matrix is same G. Diagonal entries consist of $\lambda 1$, λ_2, λ_3…..λ_n and are non zero. In SVD U, S, V represents the shape of the image.

2.1.1.5 Data Hiding

For embedding vector matrix of secret image is added to left and right singular vectors i.e. U and V of cover image frame i.e. G. This is done because slight variation in values of U and V does not affect image quality also data can be embedded efficiently. It can be define as G' = VM + G where G' is stego image SVD, VM is the vector matrix of secret image and G is the cover image SVD.

2.1.1.6 Stego–Video

After embedding the data, Inverse Discrete Cosine Transform (IDCT) and Inverse Discrete Wavelet Transform (IDWT) is applied over each stego image. All stego images are combined together to get stego video as output.

2.1.1.7 Extraction

For the extraction of secret message from stego video first it is divided into number of images than zigzag scanning is done to rearrange the images. After that first level DWT is applied than LL band is selected from it. Using DCT middle frequency region selected of LL band. Then SVD is calculated of stego image. Secret message is extracted from SVD and decrypted using AES decryption algorithm.

2.2 Embedding Process

1. Take the cover video stream as input and divide it into a number of frames (X_1, X_2, X_3… X_N) where 'N' is the number of frames.
2. Rearrange the cover frames using zigzag scanning to get Rearranged Cover (RC) image frames.
3. Apply hybrid DWT-DCT algorithm:

   i. Using DWT divide the each image frame in LL, LH, HL, HH bands.

   ii. Out of which select LL band.

   iii. Apply DCT over LL band and divide it into low frequency, medium frequency, high-frequency components.

   iv. Select middle frequency region.

4. SVD is applied on middle frequency component to get $G_1=USV^T_1$, $G_2=USV^T_2$, $G_3=USV^T_{3..}$, $G_n= USV^T_n$ where U and V are orthogonal matrix, S is the diagonal matrix, n is the number of the matrix for each frame. $U^TU = I$, $V^TV = I$ where I is the identity matrix.
5. Now take the secret video stream as input and divide it into a number of frames (Z_1, Z_2, Z_3… ZN) where N is the number of frames.
6. Rearrange the secret frames using zigzag scanning to get Rearranged Secret (RS) image frames.
7. Encrypt the secret video frames using AES algorithm.
8. Apply hybrid DWT-DCT algorithm:

i. Using DWT divide the each image frame in LL_1, LH_1, HL_1, HH_1 bands.
ii. Out of which select LL band.
iii. Apply DCT over LL band and compress it.

9. Vector matrix is generated from each compressed secret image to get VM_1, VM_2, VM_3,…,VM_n where n is the number of the matrix for each frame.

10. Create stego image matrix SI_1, SI_2, SI_3,…,SI_n as given below:
i. Compute USV^T for G
ii. Convert U to U^T so that $SI_n = VM_n + |G_n|$
iii. Compute $SI^T = U^T SV^T$
iv. Resulting SI^T is the stego-image.

11. Apply IDCT to low band LL_1. Apply IDWT on LL, LH, HL and HH bands.

12. Use inverse zigzag process to arrange the original position of images and finally get stego video images.

13. Combine the stego-video images to get the video.

2.3 Extraction Process

1. Take stego-video as input.
2. Rearrange the stego-images by applying zigzag scanning process to get Rearranged Image (RI).
3. Use single level DWT on RI to decompose it into four sub-bands LL*, HL*, LH* and HH*.
4. Select LL* band of RI.
5. Apply DCT to LL band.
6. Then apply SVD to LL* band to get SI_1*, SI_2*,…,SI_n*
7. Modify SI_1*, SI_2*,…,SI_n* by using $SV_n = SI_n - G_n$.
8. Construct modified SVD matrix LL*.
9. Apply IDCT to LL* band.
10. Use IDWT to all bands to get secret video images.

Figure 2. Comparison of (a) cover video frames and (b) stego video frames.

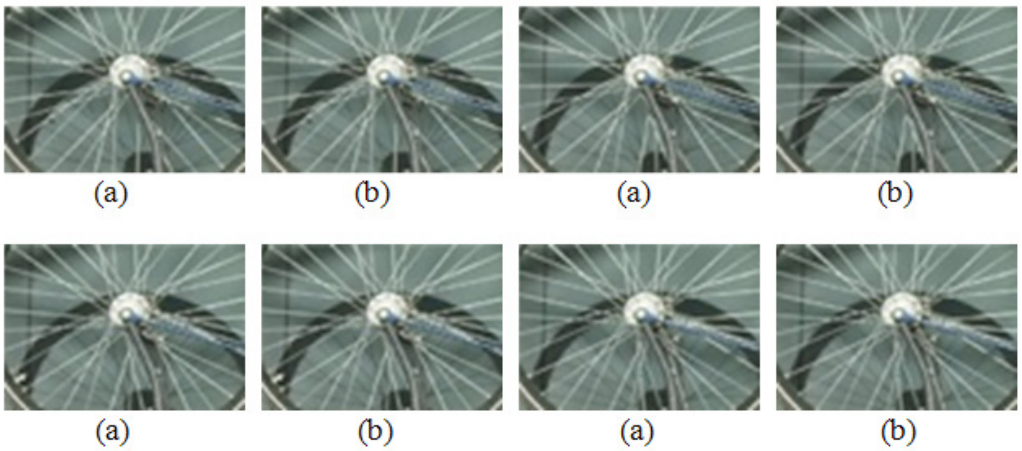

Figure 3. Comparison of (a) secret video frames and (b) recovered embedded video frames.

11. Decrypt secret video images using AES decryption algorithm.

3. Experimental Results

Embedding of the secret video stream into the cover video stream leads to some distortion in both cover medium and a secret message. Hence, for this, there is a need for some quality evaluation parameter such as Peak Signal to Noise Ratio (PSNR) to know the imperceptibility between the images of the proposed work. It is measured for both cover medium and video stream as well as for secret video stream.

$$PSNR = 10 \log 10 \frac{I^2}{MSE}$$

Where 'I' is the image pixel intensity, and MSE is mean squared error.

For testing the above proposed steganographic algorithm, two video streams cover video (120 frames) and the secret video (73 frames) are used. Stego video contains both embedded secret video and cover video.

Figure 2 shows frame by frame comparison of cover video and stego video. From Figure 2 there is a perceptual similarity between cover video frames and stego video frames. Table 1 shows all PSNR values are nearly around 40 dB which shows the similarity between cover video and stego video frames. Figure 3 illustrates the comparison of secret video and recovered secret video there is much similarity between the two images. The quality of images is acceptable and without much distortion, PSNR value is nearly 38 dB. In the existing system, secret data of 12 frames can be embedded in cover video stream. But in the proposed work secret data of 246 frames can be hidden efficiently under the cover video of 741 frames.

Table 2 shows PSNR value of different sample videos for cover video and secret video. Grass video is embedded

Table 1. PSNR value comparison between proposed system, existing system of cover video, stego video and Secret video, recovered secret video

PSNR Values	Existing System (12 frames) (LSB)		Proposed System (246 frames) (DWT+DCT)	
	Cover video and stego video	Secret video and recovered secret video	Cover video and stego video	Secret video and recovered secret video
Maximum Value	37.76 dB	34.43 dB	40.01 dB	35.20 dB
Average Value	36.45 dB	34.45 dB	38.91 dB	34.63 dB
Minimum Value	34.75 dB	33.75 dB	36.88 dB	35.79 dB

Table 2. PSNR value for different sample videos of cover video and secret video

PSNR value of proposed System (DWT+DCT)					
Sample Cover Videos	Original Cover video	Stego Video	Sample secret video	Original secret video	Extracted secret video
Ponds	70.12 dB	39.10 dB	Grass	68.19 dB	34.12 dB
Nature	72.01 dB	37.98 dB	Lake	64.32 dB	33.96 dB
Rain	69.32 dB	38.88 dB	Birds	61.95 dB	32.01 dB
Ocean	73.11 dB	40.01 dB	Ponds	60.44 dB	31.56 dB
Mountain	68.89 dB	36.91 dB	Flame	62.49 dB	32.54 dB

in ponds video after embedding there is little variation in PSNR value as compare to original one. While lake and birds video are embedded in nature and rain video. Flame video as a secret message was embedded in mountain video.

CPU consist of a small number of cores used for serial processing while GPU consist of thousands of small cores which is used for parallel processing. In the proposed work a combination of CPU+GPU has used the code with serial portion is executed on CPU while a parallel portion is executed on GPU. Hybrid DWT+DCT is implemented on GPU, which reduces the execution time. Figure 4 shows the execution time graph of CPU and CPU+GPU test on different videos. Table 3 shows the execution time required for CPU is more than the CPU+GPU. Configuration list of proposed model using CPU and CPU+GPU is:

CPU: Intel(R) Core(TM) i5-4210U, CPU clock: 1.70 GHz, RAM memory: 4 GB.

GPU card: GeForce GT 545, Cuda cores: 144, Processor clock: 871 MHz.

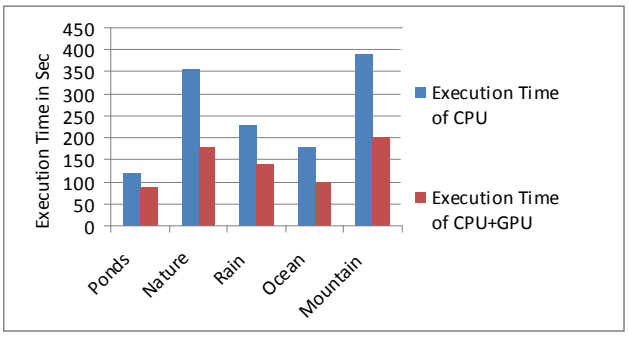

Figure 4. Execution time using CPU and CPU+GPU.

Table 3. Execution time comparison of proposed model on CPU and CPU+GPU

Sample videos	CPU Execution Time (in Sec)	CPU+GPU Execution time (in Sec)	Speed Up (%)
Ponds	119.44	88.92	1.34
Nature	355.89	181.05	1.96
Rain	230.18	139.50	1.65
Ocean	180.54	99.89	1.81
Mountain	389.61	200.01	1.94

4. Conclusion

Video steganography using hybrid DWT-DCT followed by SVD along with cryptographic technique has been proposed. The proposed scheme hides the secret video stream under the cover medium which allows hiding large capacity secret data. Both cover video stream and secret video stream are broken into a number of frames, then each frame of cover video is decomposed into four LL, LH, HL, HH bands. DCT is applied on the LL band and used to divide the image into different frequency regions and compression. In middle-frequency region, secret data is embedded frame by frame using SVD. For the security and authorized access of secret video stream, AES cryptographic algorithm is used. To reduce the execution time, proposed model is implemented on GPU. The result shows good hiding capacity for a secret message. It allows to hide 2.09 MB video under the 2.27MB video which is quite high than any other video steganographic existing system. Also, the quality of the cover video stream and secret video stream is good and is not much affected after embedding. It is tested against various cryptographic attacks and gives satisfactory result. Further work can be done to increase the hiding capacity to hide a large amount of secret data.

5. References

1. Gupta R, Gupta S, Singhal A. Importance and techniques of information hiding: a review. International Journal of Computer Trends and Technology (IJCTT). 2014 Mar; 9(5):260–5. Crossref.
2. Shakar A K. Enhancing the data security features of communication by means of media files through improvising the cryptographic and steganographic techniques. ASM's International E-Journal on Ongoing Research in Management and IT; 2013.
3. Venkatraman S, Abraham A, Paprzycki M. Significance of steganography on data security. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) International Conference on Information Technology: Coding and Computing, Las Vegas, NV, USA. 2004 Apr 5–7; 2:347–51. Crossref.
4. Agarwal M. Text steganography approaches: a comparison. International Journal of Network Security and its Applications (IJNSA). 2013 Jan; 5(1):91–106. Crossref.
5. Ghadekar P P, Chopade N B. Content-based dynamic texture analysis and synthesis based on SPIHT with GPU.

Journal of Information Processing System. 2016 Mar; 12(1):46–56.

6. Ghadekar P P, Chopade N B. Modelling nonlinear dynamic textures using hybrid DWT–DCT and kernel PCA with GPU. Journal of The Institution of Engineers (India): Series B Electrical Electronics and Telecommunication and Computer Engineering. 2016 Dec; 97(4):549–55.
7. Yadav P, Mishra N, Sharma S. A secure video steganography with encryption based on LSB technique. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) International Conference on Computational Intelligence and Computing Research, Enathi, India; 2013 Dec 26–28. p. 1–5. Crossref.
8. Tayel M, Shawky H, Hafez ADS. A new chaos steganography algorithm for hiding multimedia data. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) 14th International Conference on Advanced Communication Technology (ICACT), PyeongChang, South Korea; 2012 Feb 19–22. p. 208–12.
9. Selvigrija P, Ramya E. Dual steganography for hiding text in video by linked list method. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) International Conference on Engineering and Technology (ICETECH), Coimbatore, India. 2015 Mar 20. p. 1–5. Crossref.
10. Kaur R, Pooja, Varsha. A hybrid approach for video steganography using edge detection and identical match techniques. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India; 2016 Mar 23–25. p. 867–71. Crossref.