Video Steganography based on Scene Change Detection

[1]J.Mary Jenifer, [2]Dr.S.Raja Ratna

[1]PG Scholar, [2]Associate Professor
Computer Science and Engineering
VV College of Engineering, Tuticorin, India

***Abstract*— Video Steganography is a technique to hide the secret message inside a video. This is mostly useful in secret communications. In this system, the scene change detection method is proposed. The main objective of this method is to minimize the distortions in video and to increase the security of embedded message. The Discrete Cosine Transform coefficient is performed the scene change detection in the video for enhancing the security. The Least Significant Bit of scene change frame Discrete Cosine Transform coefficients are replaced by the message bit in the embedding process. In the Wavelet domain, the normalization operation is performed. This normalization process is used to increase the quality of the video. The proposed method offers high security and quality.**

***IndexTerms*— Communications, Least Significant Bit, Scene change, Security, Steganography.**

I. INTRODUCTION

After the growth of communication system it's simple to transfer the information among world [1], [2]. The information sharing is done by using both wired and wireless manners [3]. Cryptography is a method for secure communication of data. Many encryption and decryption methods are developed followed by cryptography. Most of the conventional methods are not provides security in sometimes. In order to provide security for secret information a technique called steganography is used [4], [5].

Steganography is a method that hides the secret information in the suitable carrier [6]. The carrier includes image, audio or video file. Steganography is coming from the Greek word and the meaning is covered writing [7], [8]. There are three things takes the important part in steganography technique. They are cover-medium, secret message and stego-medium. The cover-medium is used to carry the secret message. The secret message is the information to be inserted into the cover-medium and the medium has the secret message is called as stego-medium [9], [10].

The modern technologies describe that videos play an important role in sharing information. Videos are used in data hiding process because the hidden information is does not seen by the human visual system and the video gives additional space for hiding data [11]. In the proposed method, the video is used as a medium to convey the secret information. Undetectability, accuracy and security are the important properties of video steganography [12].

The paper proceeds as follows. Section II describes the related work. Section III explains the proposed method. Section IV presented the experimental result. Finally, Section V concludes the paper.

II. RELATED WORK

This related work describes the various techniques used in video steganography. These techniques are used to increase the protection of secret information.

In [13], the Tri-way Pixel Value Differencing (TPVD) technique is used for embedding the secret message. This technique is entirely performed in the compressed domain. The secret information is inserted in the macro blocks. This technique provides the high capacity to embed the data and no degradation in the quality of a video.

Ramadhan. et al [14] proposed a method for information hiding using BCH error correction codes. The secret data is embedded into the DCT coefficient of a video frame. This method is fast but less accurate.

Souvik Bhattacharyya. et al [15] explained a novel steganography approach using Pixel Mapping Method (PMM). All the processes are executed by using integer wavelet domain. The execution takes place in uncompressed domain. This method offers good video quality.

In [16], the new video steganography approach is proposed. Randomization and Parallelization technique perform the embedding operation in randomly chosen frame. It uses cryptography concept. The both encryption and decryption operation are performed in a parallel manner. It is one of the rapid techniques to perform the data hiding process. But the accuracy is low.

Anush Kalakular [17] described a video steganography approach using discrete wavelet transform. Least Significant Bit of wavelet band is replaced by the secret video frame. This technique offers high security for a secret message.

Tamer Shanableh [18] presented a data hiding approach using multi-variate regression and flexible macro block ordering. The message bits are predicted by using the decoder. The data hiding process is done by using flexible macro block ordering. This method causes less distortion in video. The demerit is poor video quality.

Tomas Filler [19] proposed a steganography approach using Syndrome-trellis codes. Replacement of individual bits produces the binary cases. This Syndrome-Trellis code is based on convolution codes. This Method is performed in high speed.

In [20] a secure steganography technique by using discrete wavelet transform and Arnold transform is proposed. In this technique, the cover video is separated into frames. The private-key is used to give the security in both the encoding and decoding process. This method offers high security and the Mean Square Error is low.

III. PROPOSED METHOD

The main goal of the proposed work is used to improve the security of inserted data by using scene change detection based data hiding and also help to increase the quality of video after embedding the secret information.

In the proposed Scene Change based Data Hiding (SCDH) method, the input is in the form of video and the secret information and the output is extracted message and the extracted video. This method is implemented in the transform domain. The Discrete Cosine Transform and Discrete Wavelet Transform coefficients are used for efficient processing. This data hiding process contains four steps (i) Video series parsing (ii) Embedding (iii) Normalization (iv) Extraction. The proposed system model is shown in Fig.1.

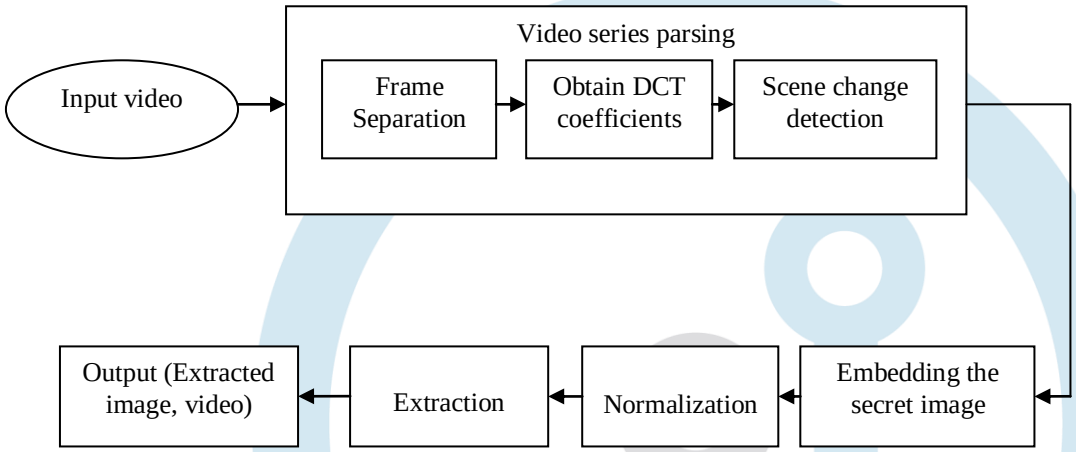

Fig.1. Proposed system model

In the first step, the video is separated into frames and the scene change point is detected by using DCT coefficient. In the second step, the secret message is embedded in the scene change point. This embedding process is used to raise the security level of hidden data. Inserting secret message at the scene change point of video causes the secret information hard to find. In the third step, the payload and video are normalized with the help of DWT coefficients. These coefficients are used to increase the quality of the video sequences. The following sub-topics describe the steps in the proposed method.

Video series parsing

In this step, the video is separated into frames for rapid computation. In the transform domain, the DCT coefficients are changed into blocks of pixel values. The two-dimensional DCT coefficient for a n×n image is achieved by using (1).

$$K(a,b) = \propto (a) \propto (b) \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} f(u,v) \cos\left[\frac{(2u+1)a\pi}{2n}\right] \cos\left[\frac{(2v+1)b\pi}{2n}\right] \quad (1)$$

For u, v= 0, 1, 2… n- 1.Where n represent the block size (i.e., if the block is 8×8 block then n is 8). Original image pixel value is represented by (u,v). Transformed image pixel values are in the form of (a,b).

In the video series parsing method, the scene change point is found by using frame difference. Generally, when a scene change of video frame appears, the brightness and color of one frame are differing from the previous frame. In the embedding process, the DCT coefficient values are replaced by the secret message pixel values.

Usually, the video is segmented into shots. Each shot represents the event or action. The sequence of frames obtained from the camera recording. The dissimilarity between frames also obtained to find scene change point. This point is identified by using (2).

$$D(f_k, f_{k+1}) = \sum_u \sum_v [C_k(u,v) - C_{k+1}(u,v)] \quad (2)$$

Where f_k and f_{k+1} represent the two continuous video frames. $f_k(u,v)$ is the pixel value at position(u,v). The DCTs of consecutive frames are represented by $C_k(u,v)$ and $C_{k+1}(u,v)$. The frame difference is represented by $D(f_k,f_{k+1})$.

Embedding

The key step of proposed SCDH method is embedding process. The embedding process is carried out when a scene change point is found. If the scene change point is greater than zero then the secret message is embedded into the frame of cover video. The scene change point denotes the changes in the scene when the consecutive shots of the video. The Algorithm 1 describes about secret message embedding process.

Algorithm 1: Algorithm for Embedding the secret image

Input: video frame, secret data
1: Start
2: Detect the scene change point
3: Determine the DCT coefficients
4: If the value of DCT is not zero and one
5: Evaluate the LSB value of each coefficient
6: LSB of DCT coefficient is replaced by the message bit
7: end if
8: Write the message bits in video frame
9: end
Output: Steganographic frame

In SCDH method the DCTs Least Significant Bit is replaced by the message bit. After the detection of scene change point, the secret message is embedded by using the algorithm. The small change in the scene also finds by using SCDH method. If no changes in video then the variable is set to zero. The secret message is embedded into scene change frame when the scene change point is greater than zero. The stego-video is normalized in the DWT domain.

Normalization

In the DWT domain, the cover-video and the payload are normalized. So the video frame pixel values are converted to standardized pixel values. This is in the range from 0 to 255. This normalization process produces the accurate pixel values. In the SCDH method, the signal is decomposed into wavelet functions. A one-dimensional wavelet transform equation is given in (3).

$$w(c,d) = \int_{-\infty}^{\infty} x(t)\psi_{c,d}(t)dt \quad (3)$$

Approximation band is the lower frequency band with video coefficients. In the Normalization process, both the cover video and payload pixel values do not exceed the higher value of 1. The fused result is obtained by merging the payload and video normalized versions. f is the cover video image. This is divided into four approximation parts.

$$f = f_m^{'} + (f_h^{'} + f_v^{'} + f_d^{'}) \quad (4)$$

Where, the horizontal, vertical and diagonal features are represented by $f_h^{'}$, $f_v^{'}$, $f_d^{'}$. The subsequent approximation level is denoted by $f_m^{'}$.

Extraction

The main goal of extraction procedure is to recover the secret message. It is the reverse procedure of embedding process. The Algorithm 2 is used to recover the secret message.

Algorithm 2: Algorithm for Extraction of secret image

Input: Steganographic frame
1: Start
2: Detect the scene change point
3: While for every block do
4: Find the DCT coefficient from parser
5: If the value of DCT is not zero and one
6: Determine the LSB of every coefficient
7: The message bits are extracted from the LSB
8: end if
9: Write the message bits
10: end while
11: end
Output: Extracted data, Video

After the detection of scene change point, the DCT coefficient of the frame is calculated. The value of DCT should not be zero and one then only the extraction process takes place. In the extraction process, the LSB of each coefficient is found then the message bits are extracted from the coefficient. Finally, the video and secret message is obtained as output.

Performance Measurement

The proposed method is estimated by using security and quality. Security denotes the inability of attacker's to detect the secret message in the video. Quality represents the good visibility of video without any distortions. The PSNR value of proposed method is obtained by using (5).

$$\text{PSNR} = 10 \log 10 \frac{R^2}{\text{MSE}} \quad (5)$$

Where R represents the peak signal level.MSE indicates the Mean Square Error. This MSE represents the average errors. The MSE is obtained by using (6).

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(C(i,j) - S(i,j)\right)^2 \quad (6)$$

Where cover video image size is represented by M×N. The intensity values of cover-video and stego-video are represented by C(i,j) and S(i,j).

IV. EXPERIMENTAL RESULT

In the scene change based data hiding method, the input is taken as color video. The proposed method is carried out in the transform domain. The input color video is shown in Fig.2.

Fig.2. Input Video

The input message is in the form of an image. The bit length of secret image should be less than the video frame pixels. The input image is shown in Fig.3.

Fig.3. Input Secret Message

The input video is segmented into frames. One individual frame represents the event or shot. This frame segmentation is the first step of data hiding process. The frame separation is shown in Fig.4.

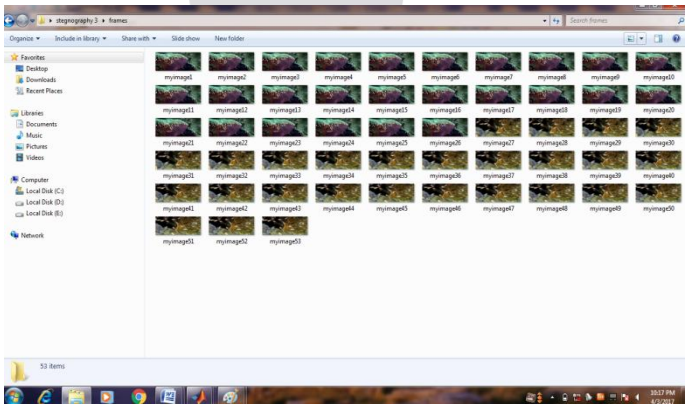

Fig.4. Frame segmentation

The scene change point is found by using frame difference between two consecutive frames. If the frame difference is greater than zero then it is taken as a scene change point. The scene change point is shown in Fig.5.

Fig.5. Scene change frame

The second step is embedding process. The input message is in the form of an image. In the secret message embedding process, the message bit is inserted into the Least Significant Bit of DCT coefficients of the frame. This proposed method offers more security to secret information. The embedding step is shown in Fig.6.

Fig.6. Embedding process

Normalization is the third step. It is done in the wavelet domain. Normalization is the process of converted the pixel values of frames into standard pixel values. The normalization process is given in Fig.7.

Fig.7. Normalization

The final step is the extraction of secret message. It is the reverse procedure of data hiding process. If the scene change point is found then the secret image is extracted from the video. The output of proposed method contains secret image and video. The extraction process is shown in Fig.8.

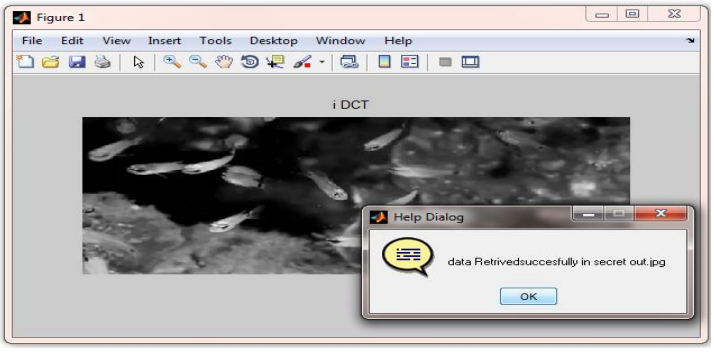

Fig.8. Extraction process

The output of proposed SCDH method is the secret message and cover video. This is shown in Fig.9.

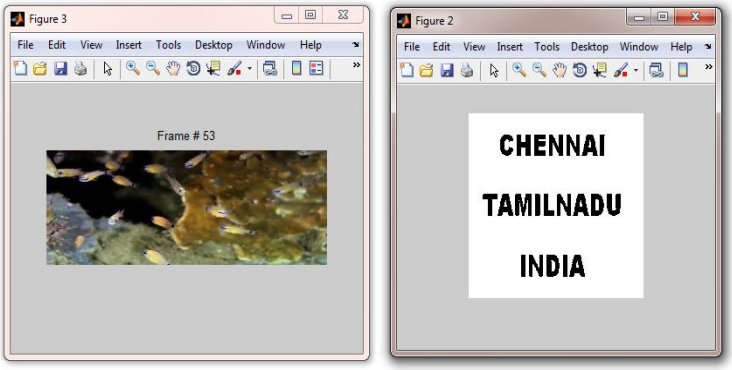

Fig.9. Output

The proposed method offers high security and reducing the distortions for good video quality. Security is the inability to find the secret image. The video with no distortion is called as quality. The peak signal to noise ratio for different images is shown in Fig.10.

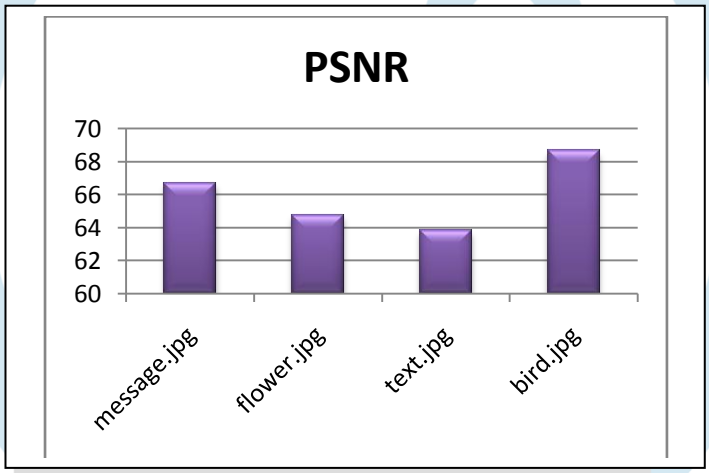

Fig.10. Performance graph of proposed work

The minimum mean square error rate defines the good performance of the proposed method. The mean square error rate for different images is shown in Table I.

Table I. Mean Square Error

Secret Image	MSE
message.jpg	0.014
flower.jpg	0.022
text.jpg	0.027
bird.jpg	0.009

Finally, the proposed SCDH method provides high security and reduces the distortions for improving the quality of the video.

V. CONCLUSION

The proposed scene change based data hiding method is performed in the transform domain and achieves scene change detection in videos. This proposed work uses Discrete Cosine Transform and Discrete Wavelet Transform coefficients of the video to increase the quality of the video and also helps to raise the security of secret message. The MATLAB simulation results indicate the good performance of the proposed SCDH method. Thus the small changes produced by the secret message embedding using scene change detection leads to the improvement of security.

REFERENCES

[1] Chen M, Zhang R, Niu Xinxin, YangY, "Analysis of current steganography tools: classifications &features", IEEE international conference on intelligent information hiding and multimedia signal processing;2006.
[2] Joseph, Princymol, and S. Vishnukumar. "A study on steganographic techniques" IEEE Global Conference on

Communication Technologies (GCCT), 2015
[3] Chang, Ko-Chin, Ping S. Huang, Te-Ming Tu, and Chien-Ping Chang."Adaptive image steganographic scheme based on tri-way pixel- value differencing", IEEE International Conference on Systems, Man and Cybernetics, pp. 1165-1170, 2007.
[4] Rig Das, Tuithung T, "A Novel steganography method for image based on Huffman encoding. "IEEE 3rd national conference on emerging trends and applications in computer science;2012.
[5] Jalab, Hamid, A. A. Zaidan, and B. B. Zaidan. "Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation." Journal of computing, vol. 1, no. 1, Dec. 2009.
[6] Al-Dmour, Hayat, and Ahmed Al-Ani. "A steganography embedding method based on edge identification and XOR coding" Expert systems with Applications-Elsevier,vol.46, 2016, pp. 293-306.
[7] H. Dadgostar and F. Afsari. "Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB" Journal of Information Security and Applications-Elsevier,vol. 30, 2016, pp. 94-104.
[8] Stanescu D,Stratulat M, Ciubotaru B, Chiciudean D,Cioarga R, Micea M, "Embedding data in video stream using steganography"
IEEE international symposium on applied computational intelligence information, vol.1,pp.241–4,2007.
[9] Li Z, Jiang J, Xiao G, Fang H, "An effective and fast scene change detection algorithm for MPEG compressed videos",Springer-Verlag;p.p.206–14,2006.
[10] Aly, A. Hussein "Data hiding in motion vectors of compressed video based on their associated prediction error." IEEE Transactions on Information Forensics and Security ,vol. 6,no.1 ,2011, pp. 14-18.
[11] Chen, Ming, et al. "Analysis of current steganography tools: classifications & features", IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing ,2006.
[12] Liao, Yi-Chun, et al. "Data hiding in video using adaptive LSB", IEEE Conferences on Pervasive Computing , 2009.
[13] A.P Sherly,and P. P. Amritha. "A compressed video steganography using TPVD" International Journal of Database Management Systems (IJDMS) Vol.2, 2010.
[14] Mstafa, J Ramadhan , and Khaled M. Elleithy. "A DCT-based robust video steganographic method using BCH error correcting codes" Long Island Systems, IEEE Conference on Applications and Technology, 2016.
[15] Bhattacharyya, Souvik, and Gautam Sanyal. "A novel approach of video steganography using PMM." Wireless Networks and Computational Intelligence. Springer", pp. 644-653, 2012.
[16] K.B Sudeepa , K. Raju, H. S Ranjan Kumar .and Ganesh Aithal , "A New Approach for Video Steganography Based on Randomization and parallelization", International Conference on Information Security & Privacy-Elsevier, vol. 78, pp. 483-490, Dec. 2015.
[17] Kolakalur, Anush, Ioannis Kagalidis, and Branislav Vuksanovic. "Wavelet Based Color Video Steganography." International Journal of Engineering and Technology, vol.8,no.3, 2016.
[18] Shanableh, Tamer. "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering." IEEE transactions on information forensics and security, vol. 7, no.2 2012, pp. 455-464.
[19] Tomas Filler, Jan Judas and Jessica Fridrich, "Minimizing Additive Distortion In Steganography Using Syndrome-Trellis Codes", IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, September 2011.
[20] Thakur, Abhinav, Harbinder Singh, and Shikha Sharda. "Secure Video Steganography based on Discrete Wavelet Transform and Arnold Transform."International Journal of Computer Applications, vol. 123, no.11, 2015.