Video Steganography using Curvelet Transform and Elliptic Curve Cryptography

Sonali Rout
Department of Computer Science and Engineering
National Institute of Technology, Rourkela
Rourkela, India
617cs6003@nitrkl.ac.in

Ramesh Kumar Mohapatra
Department of Computer Science and Engineering
National Institute of Technology, Rourkela
Rourkela, India
mohapatrark@nitrkl.ac.in

***Abstract*—Video steganography mainly deals with secret data transmission in a carrier video file without being visually noticeable by intruders. Video steganography is preferred over image steganography because a video carries more space in comparison to an image. The main concept of information hiding consists of a cover media, which is a greyscale or a color video, a secret data, which is an image or text, and a stego key. Here a secure video steganography method has been proposed which uses Curvelet Transform for secret data embedding, Elliptic Curve Cryptography for stego key encryption and a threshold algorithm for the determination of the amount of secret data to be encoded per frame. A video is a collection of various frames. The frames are selected randomly from the cover video and the frame number of the respective frames has been indexed in the stego key to find the secret data embedding location. Here, the selection of frames in a sequential manner has been avoided to improve security. For enhanced security, the stego key is also encrypted using Elliptic Curve Integrated Encryption Scheme (ECIES). Fast Discrete Curvelet Transform (FDCT) has been applied to the frames of the cover video and the curvelet coefficients have been modified to obscure the secret data to produce the stego video.**

***Index Terms*—Video Steganography, Fast Discrete Curvelet Transform, Elliptic Curve Cryptography, Stego Key**

I. Introduction

In this digital era of data communication, the transmission of private information through a secure channel is the main concern of researchers as well as security providers. Maintaining security and privacy of data can no longer be an afterthought and can not be conveyed through the traditional way of security solutions. Information Security is the branch of science that provides two main approaches cryptography and steganography to reach three goals confidentiality, integrity, and availability [1]. Cryptography focus on hiding the meaning of a message adding privacy whereas steganography refers to hiding the existence of the secret message. Hiding data with steganography methods adds an extra layer of security and protection to encryption using cryptography.

Steganography is the technique of embedding a secret message inside a medium that can be a text, an image, an audio or a video such that a third party can not realize its presence. To conceal secret information in the cover medium, it must contain some amount of distortions or noise [2]. In that noise, the secret data is replaced effectively without tampering its similarity to the original cover data. The limited ability of the Human Visual System (HVS) can not detect minor changes in the cover medium which encourages researchers to find out different methods to perform steganography in different media.

Steganography methods are targeted to achieve three major security concerns as imperceptibility, embedding capacity and robustness [3]. Imperceptibility means the intruder can never find the differences between the original and stego object. Embedding capacity targets to hide the maximum amount of data without hampering the originality of the actual cover medium. The high imperceptibility directs to low embedding capacity means good visual quality. And lastly, robustness called the strength of the steganographic method that is the degree of difficulty to destroy the secret message without destroying the cover media.

Based on the domain, there can be different types of steganography methods [4] but two of them are widely used, spatial domain techniques and Transform or frequency domain techniques. The spatial domain method which is also called the substitution method tries to hide data at redundant parts of the cover medium. It aims directly at the cover medium altering the pixels values. Least Significant Bit (LSB) technique is a very common method of data hiding in both image and video steganography. Transform domain methods convert the cover medium from time to frequency domain and then embed data into frequency coefficients. Some popular transform domain methods are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT) etc. Curvelet Transform [5] is also a transform domain technique that is used here for better sparser representation of cover medium as compared to previous methods.

Video steganography [6] received little attention as compared to image steganography. There are lots of methods and ideas have been discussed on the topic of image steganography incorporating spatial domain methods. Various researchers also have given the idea to implement spatial domain techniques in video steganography. However there are few discussions done on the transform domain methods.

This paper proposes a novel video steganography based on the Curvelet Transform and Elliptic Curve Cryptography (ECC). Fast Discrete Curvelet Transform (FDCT) has been applied to the cover video frames for secret data embedding

process. Stego key has been generated where information regarding to the location of secret data hiding has been stored. This Stego key has been encrypted using Elliptic Curve Cryptography based Encryption Scheme called Elliptic Curve Integrated Encryption Scheme (ECIES). The encrypted stego key has been sent along with the stego video. The intended receiver has to generate all the possible frames and search for the stego key. From the stego key all the information of the location of the secret has been known to the receiver. The selected video frames are undergone curvelet transform to extract the secret data hidden in the stego video frames.

II. Related Work

In spatial domain video steganography, one of the most simple and common methods is the Least Significant Bit (LSB) technique. The video steganography method using the least significant bit method is given by Eltahir et al. [7] where 3, 3, 2 locations of least significant bits (LSB) of R, G, B color component of the 24 bits are used for secret data embedding. A new video steganography method with LSB technique is proposed by Yadav et al. [8] where the symmetric encryption method (i.e. XOR encryption) is used for encrypting the secret video data. The secret video frames are undergone through the sequential encoding (with BGRRGBGR predefined pattern) and LSB technique is used to hide the secret data in the cover video. Patel et al. [9] embedded a video in another video using LSB technique with the random byte hiding method, which ensures the secret data is being embedded in each line of the video frame at a different location. LSB technique shows good embedding capacity but it is an overworked method and easily detected by the adversary.

Transform domain video steganography methods comprises an improved method based on Discrete Wavelet Transform (DWT), which has been practiced on the color video to hide another color video given by Kolakalur et al. [10]. On the other hand, the method does not deliver lossless steganography and generates a stego video with large noise which is recognizable. A methodology based on Discrete Wavelet Transform was introduced by Balaji et al. [11] in which secret data is embedded in a selected video frame. In this method, the use of selected frames has been performed instead of sequential data embedding and an index key has been introduced. Along with secret data, the index key has been implanted inside the stego video frame to reduce the computational cost for searching the whole video at the receiver side. Thakur et al. [12] examined a new method of video steganography using DWT and Arnold transform where high PSNR is achieved. Another method of data hiding based on multiple object tracking and DWT-DCT has been given by Mstafa et al. [13] which uses the motion-based algorithm to find the region of interest in moving objects to hide data within it. A secure technique of video steganography was proposed by Yadav et al. [14] where a comparison between spatial domain, discrete wavelet transform, and integer wavelet transform has been shown. An improved method is proposed by Mumthas et al. [15] with RSA cryptography is added before video steganography using Random DNA encryption and Huffman coding for better security. Moreover, RSA uses 1024 bit key size which is computationally very extensive.

Curvelet transform has been used in several kinds of steganography methods. Jero et al. [16] proposed ECG steganography with Curvelet transform to watermark patient data as a secret. Leung et al. [17] introduced digital watermarking using curvelet transform with hamming codes. Zhang et al. [18] introduced multipurpose watermarking using curvelet transform in digital images. Borra et al. [19] embedded the patient's information in radiological images using curvelet transform and compressive sensing. Mittal et al. [20] proposed an image watermarking method using Gaussian filter and first-order differential matrix for finding surface blocks to embed data using curvelet transform. Curvelet transform has been used in various fields like multimodal image fusion proposed by Arif et al. [21], ECG steganography introduced by Goyal et al. [22], video surveillance suggested by Epsiba et al. [23], image based simulation in porous media propounded by Aljasmi et al. [24] etc.

It has been observed from the above review that many video steganography schemes have been proposed using LSB, DCT, DWT, IWT etc for hiding grayscale images. Further, it has been found that almost every method uses sequential frames for data embedding which requires more computational time to search all of the frames for secret data extraction at the receiver's side. Our proposed method promises to overcome two limitations, one is to use curvelet transform as the discrete wavelet transform lacks to identify curve edges in a 2-D image. Curvelet transform is capable of identifying angles with the orientation parameter and is good at defining curved edges as compared to wavelets [5]. As we know human eyes are less sensitive to the edges as compared to the smooth region, so that boundaries and edges of the cover frames has been analysed profoundly using curvelet transform to hide secret data. The second limitation is to avoid the use of sequential frames, so the secret data has been concealed in random frames. The respective frame numbers are stored in a stego key which is protected by ECIES encryption and sent along with stego video which adds an extra layer of security.

III. Background of the Proposed Approach

A. Video Steganography

Video is a collection of frames, hence it provides much more space in comparison to the image. In a video hardly some frames are required to hide data and video frames are shown with an extremely brief time frame, so it is very difficult to notice any kind of changes in the frames by Human Visual System (HVS). It is not focused as an image, so minor manipulation with pixel values are unrecognizable. It is the main reason why video steganography is preferred over image steganography [25]. Here a hybrid approach has been suggested which uses curvelet transform for implementation of video steganography and Elliptic Curve Cryptography (ECC) for stego key generation as well as encryption.

B. Curvelet Transform

The curvelet transform is a multiscale directional transform that allows an almost optimal non-adaptive sparse representation of 2D objects with limitations of traditional multiscale representation such as wavelets (DWT) [5]. Curvelet transform is a multi-scale pyramid with different directions and positions at each length scale and needle-shaped elements at fine scales. Therefore, curvelet transform can better represent the 2D images with curve singularities in high dimensions sparsely. Curvelet transform is used to extract the multi-scale and multi-direction image. Fast discrete curvelet Transform (FDCT) extracts various curvelet sub-bands with various frequency coefficients. The curvelet transform decomposes the image into concentric squares as different scales. Smaller squares represent low frequency and bigger squares define high frequency coefficients. The curvelet coefficients can be calculated using frequency wrapping as given in equation (1).

$$c(j,l,k) = \int f[t_1,t_2].\theta^D_{\langle j,l,k\rangle}[t_1,t_2] \tag{1}$$

Where,
c = curvelet coefficients of the cover frame.
j, l, and k are the parameters of scale, orientation and translation respectively.
$f[t_1,t_2]$ is the 2-D image.
$\theta^D_{\langle j,l,k\rangle}[t_1,t_2]$ is the digital curvelet waveform.

C. Elliptic Curve Cryptography (ECC)

It is a public key cryptography developed by Miller [26] in the year 1985. It is a plane curve defined by the equation (2) which is also known as Weierstrass equation.

$$y^2 = x^3 + ax + b \tag{2}$$

Here a and b are real numbers. The curve to become non-singular, the discriminant should satisfy the following condition.

$$4a^3 + 27b^2 \neq 0 \tag{3}$$

Cryptographic operations on elliptic curve are usually carried out using the points on the curve. Elliptic curve over finite field is given by the equation (4).

$$y^2 = x^3 + ax + b \mod p \tag{4}$$

where p is a prime number.

Since ECC is a public key cryptography, it requires both public key and private key. For sender and receiver, they have to agree on a common Elliptic curve and a generator g.

Let the sender is Alice and the receiver is Bob. The private keys of Alice and Bob are nA and nB respectively. These are calculated as follows.

$$P_a = nA * g \tag{5}$$

$$P_b = nB * g \tag{6}$$

Let the plain text is denoted as P_m. Using Bob's public key Alice finds the cipher text using the equation (7).

$$P_c = \{k * g, P_m + k * P_b\} \tag{7}$$

where k is a random integer. For every communication between Alice and Bob, the value of k is different. Thus, it makes an adversary difficult to decrypt the message which is being sent on insecure channel.

$$P_m = \{P_m + k * P_b - nB * k * g\} \tag{8}$$

Bob on the other hand use the above equation (8) to decrypt the message.

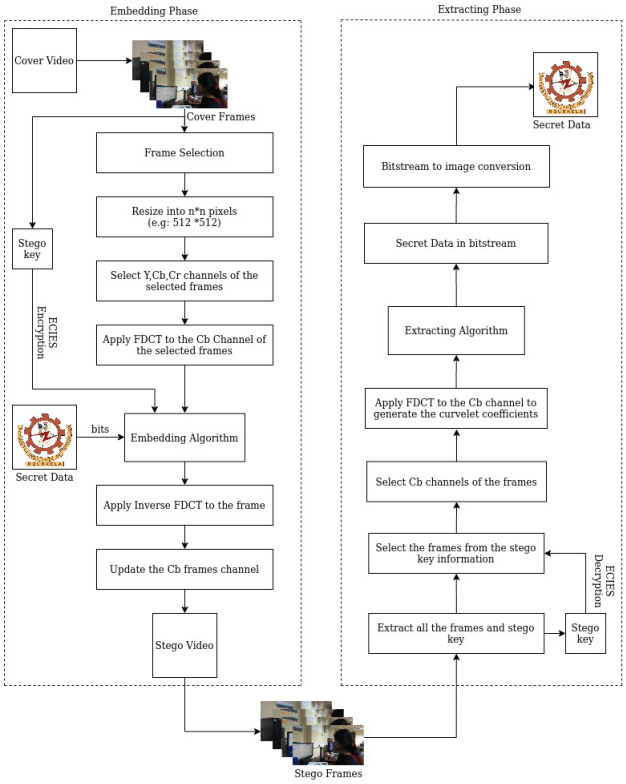

Fig. 1. Workflow diagram of the proposed method.

IV. PROPOSED METHOD

The proposed method consists of several steps as discussed below.

1) Frames Selection
2) Stego Key Processing
   - Stego key generation.
   - Stego key encryption using ECC.
3) Preprocessing
   - Accessing the pixels from the frame as 2D image.
   - Calculation of curvelet coefficients by applying Fast Discrete Curvelet Transform (FDCT) to the selected frame.
   - Obtaining the binary format of the secret image to embed in the curvelet coefficients.
4) Threshold selection
5) Secret data embedding
   - Selection of Scale 5 from the generated curvelet logs.

- The binary data from the secret message needs to be replaced with curvelet coefficients on scale 5.
- After embedding the secret data, Inverse Fast Discrete Curvelet Transform (IFDCT) to the cover frames to generate the stego frame.
- Stitch all the frames along with stego frames to generate the video.
- Send the encrypted stego key along with the stego video.

6) Stego key encryption and decryption
7) Secret data extraction
   - Take the stego video and generate frames.
   - Extract the stego key.
   - Decrypt the stego key using ECC decryption.
   - Select the frames corresponding to the stego key and get stego frames.
   - Apply FDCT to the stego frames to generate curvelet coefficients.
   - Compare and match the curvelet coefficients the stego frames with original frames of the actual cover medium.
   - Extract the manipulated curvelet coefficients.
   - From the extracted binary bits regenerate the secret image.

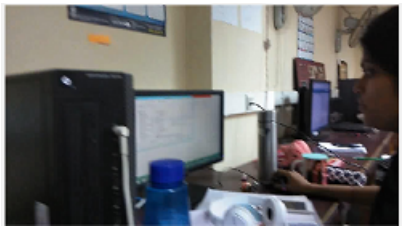

Fig. 2. Frame generated from the cover video with 720 × 1280 × 3 resolution.

A. Frame Selection

In this paper, a video has been taken as a cover video which is a color video of 720×1280 pixel resolution with 'RGB24' format and 24.895 frame rate. The total frames generated in this video taken for the experiment is 254. In Figure 2 we have shown a frame selected from the cover video, which is having a resolution of 720×1280×3 pixels.

In previous studies, it has been observed that the sequential frames have been used always for secret data hiding [8], [14]. It is more prone to steganalysis attacks and can be easily detected by the attackers. To avoid the usage of frames sequentially for data hiding we will hide secret data in the random frames. The random frame numbers are the index numbers that have been stored in the stego key as shown in Figure 3. To access the frame numbers from the receiver side, the stego key is required. Stego key has been created from the frame numbers used for secret data hiding which is discussed next.

5	17	241	151	9

Fig. 3. Stego Key Formation

B. Stego Key Generation

Stego key is generated by encrypting the frame numbers in which the secret data is embedded. In our experiment we have chosen a video with 254 frames out of which only randomly selected frames have been to embed the secret data. To ease the process of extracting, the frames at the receiver side, the frame numbers generated are represented with three digit with extra zero padding for single digit and double digit number. After the Stego key has been generated, the key is encrypted using ECIES for better security.

005	017	241	151	009

Fig. 4. Final stego Key formation after zero padding

Stego key is the secret information that strengthens the steganography process. Here in our proposed steganographic technique, the stego key is the sequence of frame numbers which has been shown in Figure 4. In our experiment, five frames have been used for data embedding. Here the frame numbers are arranged as the order of data embedding is done. Then extra zero digits have been added to the frame number to distinguish the frame numbers from the string. As the maximum digit of the frame number in the video taken for the experiment is three (as the last frame number is 254 in the video taken for the experiment). So we have added extra two zeroes to the single-digit frame number and an extra zero to the double-digit frame number to make it three-digit numbers. So that from the first three-digit of the stego key, it is considered as the first cover frame and so on.

The arrangement of the frame numbers has been shown in Figure 3 at the initial stage and Figure 4 shows the stego key after the extra zero digit padding to the frame numbers.

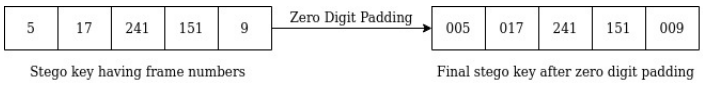

Fig. 5. Stego Key Formation

To secure the stego key of a 15 digit number, it is needed to be encrypted using ECIES. The encrypted number has to be sent as a ciphertext along with the stego video. The receiver needs to decrypt the ciphertext to retrieve the stego key to calculate the frame number sequence and fetch the frames that have been used for secret data hiding. The zero digit padding has been shown in Figure 5. Elliptic Curve Integrated Encryption System (ECIES) has been used to encrypt the 15 digit stego key.

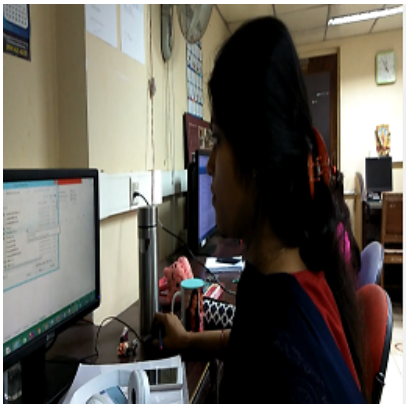

Fig. 6. Cover Frame of the Input Video which is resized to 512×512 pixels to apply FDCT.

C. Preprocessing

After selecting the frames to be used as a cover frame, Fast discrete curvelet transform has been applied to generate curvelet coefficients. FDCT converts the cover frame from the time domain to the frequency domain using the 2D Fast Fourier Transform.

The cover frame is subjected to the Curvelet transform by Fast discrete curvelet transform (FDCT) using frequency wrapping technique using MATLAB 18(a) and Curvelab 2.0.

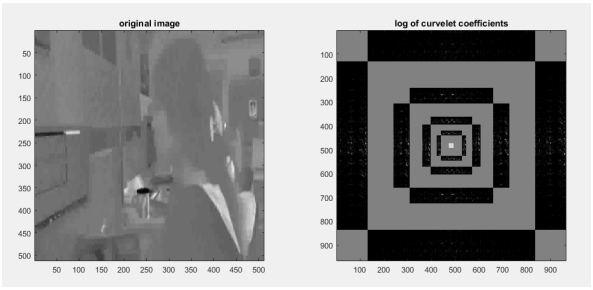

Fig. 7. Curvelet Transform applied to the cover frame which is shown in Figure 4.

D. Secret Data Embedding

Here secret data is an image shown in Figure 9. The secret image has been converted into bitstream which results into an 1-D array having all the pixels of the secret image converted into binary form. α is the embedding factor which has been empirically taken 0.5 in this experiment. It has been found that α depends on the pixel intensity value of the cover image which has been studied in [17].

This binary data has to be hidden by using the equation(9).

$$c^*(i,j) = \alpha|c^D(i,j)|w \tag{9}$$

where,
α = embedding factor
w = 1, if secret data bit = 1

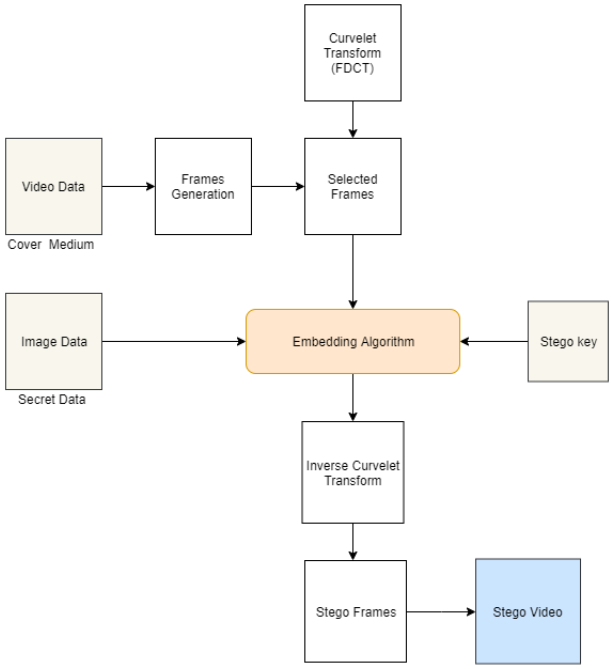

Fig. 8. Embedding Process

Fig. 9. Secret Image

w = -1, if secret data bit = 0

Fig. 10. Stego Frame

E. Encryption and Decryption of Stego Key

The Stego key is encrypted using the Elliptic Curve Integrated Encryption Scheme (ECIES) [27]. ECIES is a public-

key authenticated encryption scheme based on ECC. Encryption of the stego key has been implemented using Python 3.6.

- Input: Stego key of 15 digit number as shown in Figure 3 that is Plaintext: 005017241151009
- Private key: 0xa7ceb8fa710f11137e041fbe3231aec929 a8369cfe38042011afbs87d6048cL
- Public key: (0x44e6122bebcb7263f9f59838d146fa12882f 4f3c0f22a0089215cebb8da0ffbc,0xd57a2ed6 abfbd2e90aafea3cb406eefb46553d14fd516e5 2a5dd2456242c4fcf)
- Encryption Key: 113075403949594835401608705833884881918 144047314495459279970901424378686486722
- Encrypted: 4645526d7638364c556177746f4d4d7a3259737 147773d3d
- Decrypted: 005017241151009

F. Secret Data Extraction

Upon transmission of the stego video, the cover stego frames are extracted from the decrypted stego key and subjected to the FDCT to get the modified coefficients. The hidden image data can be extracted using the following equation.

$$w_r = 1, if \;\; \hat{c}(i,j) < 0 \tag{10}$$

$$w_r = 0, if \;\; \hat{c}(i,j) > 0 \tag{11}$$

w_r is the extracted secret data bit.
$\hat{c}(i,j)$ is the retrieved coefficient.

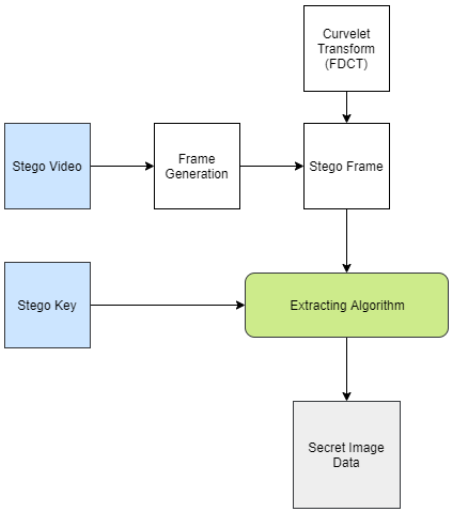

Fig. 11. Secret Data Extraction

The extracted secret data bits has been retrieved in binary bits one by one, which is again rearranged in m × n pixels array (which is the size of the secret image with m is height and n is width) to be read as an 2D image.

V. Results and Analysis

A. Evaluation Metrics

To measure the performance of our steganographic method, PSNR and MSE has been calculated. A good steganographic scheme requires high PSNR and low MSE. The main objective of the video steganography is to hide secret data inside the video without the knowledge of the eavesdropper. The concealing of the secret data inside the carrier video file should be imperceptible. To measure the changes in the original video file and stego video file, some performance metrics have been taken as described below.

1) Mean Squared Error (MSE): Mean Squared Error is the cumulative squared error between the cover frame and the stego frame. Let A be the cover frame and B is the stego frame with a, b are the dimensions of the respective videos and c refers to the RGB color components.

$$MSE = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}\sum_{k=1}^{c}\left[A\left(i,j,k\right) - B\left(i,j,k\right)\right]^2}{a \times b \times c} \tag{12}$$

2) Peak Signal to Noise Ratio (PSNR): Peak Signal to Noise Ratio (PSNR) is used to find the difference in visual quality in the original video and stego video [28]. PSNR is calculated using the Mean Squared Error (MSE). High PSNR value implies slight distortion in the stego video. PSNR (in dB) has been calculated using the below formula:

$$PSNR = 10 \times log_{10}\left(\frac{MAX_A^2}{MSE}\right) \tag{13}$$

Here MAX_A is the maximum luminance value of the pixel of the frame A.

B. Experimental Results

A comparison table has been provided to show the embedding capacity, robustness in terms of PSNR, MSE in Table I. Here our method shows remarkably high PSNR and low MSE from other methods. It was found that our method performs well as compared to other techniques.

VI. Conclusion

Fast Discrete Curvelet Transform (FDCT) has been applied to the selected frames generated from the cover video to generate curvelet coefficients. Scale 5 has been considered to hide our secret image data for imperceptibility. It has been studied that more data embedding requires more modification of the coefficients in Cover frames which results in more deterioration of cover data. In future secret data can be chosen as a color video which is intended to hide in a cover color video. For more improvement Deep learning techniques may be applied to our proposed method. The process of lossless secret data retrieval and security issues can be improved for robust video steganography.

TABLE I
COMPARISON OF PROPOSED SCHEME WITH OTHER SCHEMES

Ref no.	Technique Used	PSNR (in dB)	MSE
Eltahir et al. (2009) [7]	Video Steganography with 3,3,2 location of Least significant bit of R, G, B channel	not given	not given
Yadav et al. (2013) [8]	Video Steganography with XOR Encryption and Least significant bit (LSB) Technique	34.43	not given
Thakur et al. (2015) [12]	Video steganography with Discrete Wavelet Transform and Arnold Transform to hide a secret image	97.3	not given
Kolakalur et al. (2016) [10]	Color video steganography using Discrete Wavelet Transform(DWT)	35.20	19.6
Jangid et al. (2017) [29]	Video Steganography using Multi-Clustering Algorithm	53.81	0.29
Yadav et al. (2018) [14]	Video Steganography using Discrete Wavelet Transform and Integer Wavelet Transform	29.58	72.16
Proposed Method	Video Steganography using Curvelet Transform and Elliptic Curve Cryptography	47.36	18.60

ACKNOWLEDGEMENT

This work is accomplished by the project "Information Security Education Awareness (ISEA)" Phase-II funded by the Ministry of Electronics and Information Technology (MeitY), Government of India.

REFERENCES

[1] B. A. Forouzan, *Cryptography & network security*. McGraw-Hill, Inc., 2007.

[2] G. C. Kessler, "An overview of steganography for the computer forensics examiner," *Forensic science communications*, vol. 6, no. 3, pp. 1–27, 2004.

[3] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and steganography*. Morgan kaufmann, 2007.

[4] C. Sumathi, T. Santanam, and G. Umamaheswari, "A study of various steganographic techniques used for information hiding," *arXiv preprint arXiv:1401.5561*, 2014.

[5] E. Candes, L. Demanet, D. Donoho, and L. Ying, "Fast discrete curvelet transforms," *Multiscale Modeling & Simulation*, vol. 5, no. 3, pp. 861–899, 2006.

[6] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: A review," *Neurocomputing*, vol. 335, pp. 238–250, 2019.

[7] M. E. Eltahir, L. M. Kiah, B. B. Zaidan, and A. A. Zaidan, "High rate video streaming steganography," in *2009 International Conference on Information Management and Engineering*. IEEE, 2009, pp. 550–553.

[8] P. Yadav, N. Mishra, and S. Sharma, "A secure video steganography with encryption based on lsb technique," in *IEEE International Conference on Computational Intelligence and Computing Research*. IEEE, 2013, pp. 1–5.

[9] R. Patel and M. Patel, "Steganography over video file by hiding video in another video file, random byte hiding and lsb technique," in *2014 IEEE International Conference on Computational Intelligence and Computing Research*. IEEE, 2014, pp. 1–5.

[10] A. Kolakalur, I. Kagalidis, and B. Vuksanovic, "Wavelet based color video steganography," *International Journal of Engineering and Technology*, vol. 8, no. 3, p. 165, 2016.

[11] R. Balaji and G. Naveen, "Secure data transmission using video steganography," in *2011 IEEE International Conference on Electro/Information Technology*. IEEE, 2011, pp. 1–5.

[12] A. Thakur, H. Singh, and S. Sharda, "Secure video steganography based on discrete wavelet transform and arnold transform," *International Journal of Computer Applications*, vol. 123, no. 11, 2015.

[13] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "A robust and secure video steganography method in dwt-dct domains based on multiple object tracking and ecc," *IEEE Access*, vol. 5, pp. 5354–5365, 2017.

[14] S. K. Yadav and R. K. Bhogal, "A video steganography in spatial, discrete wavelet transform and integer wavelet domain," in *2018 International Conference on Intelligent Circuits and Systems (ICICS)*. IEEE, 2018, pp. 258–264.

[15] S. Mumthas and A. Lijiya, "Transform domain video steganography using rsa, random dna encryption and huffman encoding," *Procedia computer science*, vol. 115, pp. 660–666, 2017.

[16] S. E. Jero, P. Ramu, and S. Ramakrishnan, "Ecg steganography using curvelet transform," *Biomedical Signal Processing and Control*, vol. 22, pp. 161–169, 2015.

[17] H. Y. Leung, "Study of digital image watermarking in curvelet domain," Ph.D. dissertation, City University of Hong Kong, 2009.

[18] C. Zhang, L. L. Cheng, Z. Qiu, and L.-M. Cheng, "Multipurpose watermarking based on multiscale curvelet transform," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 611–619, 2008.

[19] S. Borra, R. Thanki, N. Dey, and K. Borisagar, "Secure transmission and integrity verification of color radiological images using fast discrete curvelet transform and compressive sensing," *Smart Health*, vol. 12, pp. 35–48, 2019.

[20] M. Mittal, R. Kaushik, A. Verma, I. Kaur, L. M. Goyal, S. Roy, and T.-h. Kim, "Image watermarking in curvelet domain using edge surface blocks," *Symmetry*, vol. 12, no. 5, p. 822, 2020.

[21] M. Arif and G. Wang, "Fast curvelet transform through genetic algorithm for multimodal medical image fusion," *Soft Computing*, vol. 24, no. 3, pp. 1815–1836, 2020.

[22] L. M. Goyal, M. Mittal, R. Kaushik, A. Verma, I. Kaur, S. Roy, and T.-h. Kim, "Improved ecg watermarking technique using curvelet transform," *Sensors*, vol. 20, no. 10, p. 2941, 2020.

[23] P. Epsiba, N. Kumaratharan, and G. Suresh, "A novel discrete curvelet transform and modified whog for video surveillance services," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 4, p. e5046, 2020.

[24] A. Aljasmi and M. Sahimi, "Efficient image-based simulation of flow and transport in heterogeneous porous media: Application of curvelet transforms," *Geophysical Research Letters*, vol. 47, no. 2, p. e2019GL085671, 2020.

[25] N. Singh and V. K. Yadav, "Trends in digital video steganography: a survey," *International Journal of Computer Applications*, vol. 975, p. 8887, 2017.

[26] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology — CRYPTO '85 Proceedings*, H. C. Williams, Ed. Springer Berlin Heidelberg, 1986, pp. 417–426.

[27] V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila, "A survey of the elliptic curve integrated encryption scheme," *Journal of Computer Science and Engineering*, vol. 2, 2010.

[28] Q. Huynh-Thu and M. Ghanbari, "The accuracy of psnr in predicting video quality for different video scenes and frame rates," *Telecommunication Systems*, vol. 49, no. 1, pp. 35–48, 2012.

[29] S. Jangid and S. Sharma, "High psnr based video steganography by mlc (multi-level clustering) algorithm," in *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, 2017, pp. 589–594.