Biosc.Biotech.Res.Comm. Special Issue Vol 13 No 13 (2020) Pp-52-57

BBRC
Bioscience Biotechnology
Research Communications

Application of Fisher Yates Data Shuffling and RSA Encryption in Transform Domain Video Steganography

Laxmi Gulappagol*[1,2] and K. B. Shiva Kumar[3]

[1]*Department of Electronics & Communication Engineering, Visvesvaraya Technological University, Jnana Sangama, Belgaum, Karnataka, India.*

[2]*Department of Electronics & Communication Engineering, Mangalore Institute of Technology and Engineering, Moodabidri, Karnataka, India.*

[3]*Department of Telecommunication, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India.*

ABSTRACT

Internet source and digital media tools have become daily requirements of the society. A major problem in digital communication is secured data transmission. Steganography is a technique of hiding confidential data in the media files such as audio, images and videos, in a cover model to provide secured communication. Video steganography process is an authenticated communication to hide secret information from unauthorized user(s) through a video file as cover medium. In this article, an architecture is developed to hide input secrete image into a cover video. The secret image is encrypted by RSA algorithm, further continued with data shuffling by using Fisher Yates algorithm. Then Discrete Cosine Transform is applied to generate 8*8 blocks. On the other side, video is discretized into frames which are applied with DCT to form 8*8 blocks which are embedded with earlier generated blocks that results in a stego-video. Performance analysis is also carried out to enhance embedding capacity, imperceptibility, robustness and security.

KEY WORDS: COVER VIDEO, DCT TECHNIQUE, FISHER-YATES DATA SHUFFLING ALGORITHM, RSA, STEGO VIDEO.

INTRODUCTION

Data communication is extremely challenging in the present era. Competition among the Nations has insisted the communication to be more secured and robust. Hence a lot of research has been carried out to develop secured data transmission through three major techniques such as Cryptography, Watermarking and Steganography. Steganography is a technique in which the sensitive data is hidden inside a picture, text or video records and transmitted to receiver. Video steganography under transfer domain has wide spread applications in data hiding. Bit Length Replacement Steganography Based on DCT Coefficients (BLSDCT) where the payload MSB is embedded into the cover image using segmentation, DCT and coherent bit length is one of the safest data hiding techniques. The payload from the stego image is retrieved by using adaptive reverse procedure of embedding (K B Shiva Kumar et al., 2010).

ARTICLE INFORMATION

*Corresponding Author: laxmigulappagol@gmail.com
Received 11th Oct 2020 Accepted after revision 30th Dec 2020
Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

Clarivate Analytics
crossref

NAAS Journal Score 2020 (4.31)
A Society of Science and Nature Publication,
Bhopal India 2020. All rights reserved.
Online Contents Available at: http//www.bbrc.in/
Doi: http://dx.doi.org/10.21786/bbrc/13.13/8

Cover object is media file in which data is hidden whereas hidden data is called payload or secret data. The unified data file obtained after embedding the payload into the cover image is called the stego image. The hidden data in the stego object cannot be recognized by a Human Visual System (HSV). In ancient periods the Greek historian Herodotus was the first one to develop steganography. Steganography can be classified into three types based on the cover media used for steganography: Text-based, Image-based and video-based steganography methods which are generally classified into two domain namely spatial domain which includes LSB technique and transfer/ frequency domain based schemes (Subramani et al 2020) which include DCT and DWT (Kousik Dasguptaa et al., 2013).

Hiding an encrypted text message inside random frames of video in a sequential pattern of "BBRGGB" is possible (Ramandeep Kaur et al., 2014). The technique of generating a sequence of steganographic network packet sequence by embedding encrypted secret message into video and to further embed a resultant file into the TCP/ IP headers with fisher Yates is also proposed (Shahzad Alam et al., 2014 and Amritha Sekhar et al., 2015). An algorithm that creates a magic rectangle applicable with third order iterative fisher Yates data shuffling is advantageous (C. Aishwarya et al., 2015 and Nithiya Devi.G et al., 2016). Video steganography method in DCT domain based on Hamming and BCH (7, 4, 1) error correcting codes is one of the newer techniques in data hiding (Ramadhan J et al., 2016).

Incorporation of a strategy which combines the ideas of RSA technique, random DNA encryption (Parameshachari, B. D et al. 2019), Huffman encoding and at last DCT steganography employing video as the cover for the safe communication of secret messages is the later development in the video steganography (Mumthas S et al., 2017). The presented literatures motivate to extend the research to hide the data more securely by video steganography based on transfer domain using data shuffling algorithm of Fisher Yate data shuffling with RSA encryption.

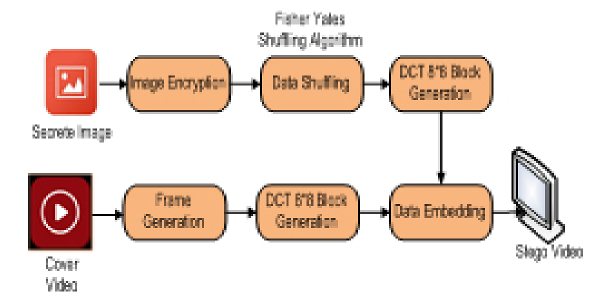
PROPOSED METHODOLOGY

The proposed methodology includes two phases, in which three different algorithms are used for data engrafting and data extraction. The sequence of the process is displayed below:

Phase-I: Secured data engrafting process
Input: Secret Image, Cover video
Output: Stego-video
RSA algorithm for secret image encryption
Fisher Yates algorithm for data Shuffling of encrypted secret image
2D-DCT transform for both shuffled secret image and cover video frame
Data engrafting of a secret data in the cover video

Phase-II: Secured data extraction process
Input: Stego-video
Output: Secret Image
Stego frame generation
2D-IDCT transform stego-frames
Data decryption
Data deshuffling
Data extraction of secret data from the stego-video

Figure 1: Proposed System Phase-I Architecture for Secured Data engrafting



Initially a suitable cover video is chosen for the given secret image. This cover video is segregated into frames which are transformed to 2D-DCT domain of 8x8 blocks. Encryption of secret image is made possible by RSA algorithm followed by Data Shuffling using Fisher Yates algorithm. Further 8x8 block generation is proceeded by DCT algorithm which results in Data engrafting. Thus enabling the construction of stego-video using stego-frames as depicted in Figure 1.

Figure 2: Proposed System Phase-II Architecture for Secured Data Extraction

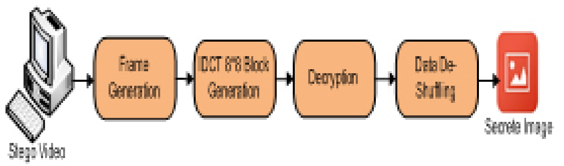
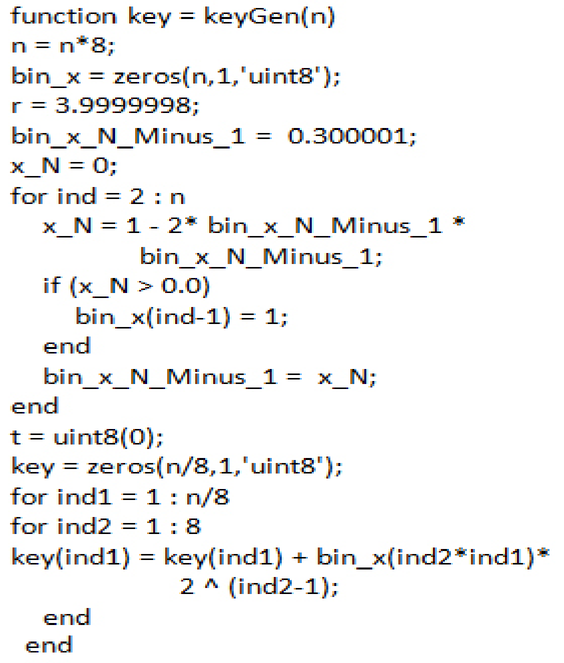


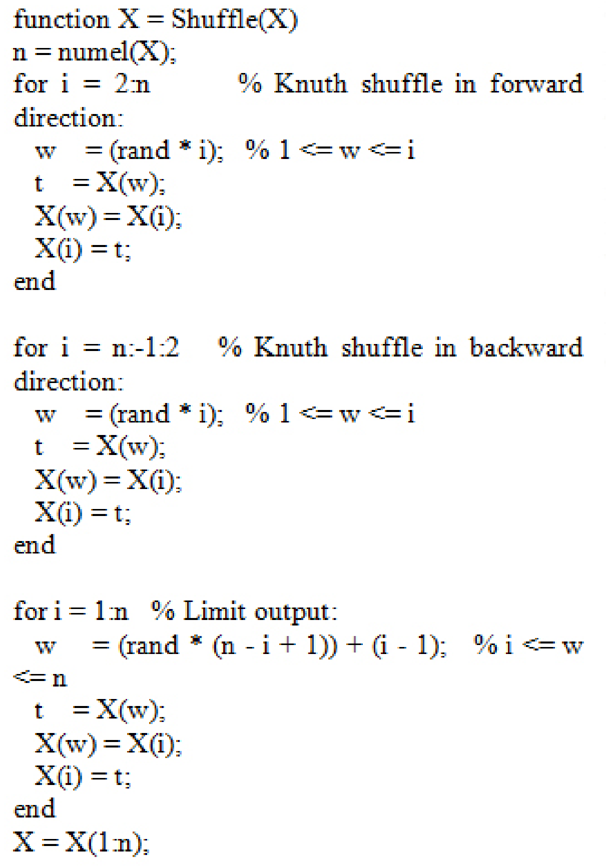
Figure 3: Key generation using RSA algorithm



```
function key = keyGen(n)
n = n*8;
bin_x = zeros(n,1,'uint8');
r = 3.9999998;
bin_x_N_Minus_1 =  0.300001;
x_N = 0;
for ind = 2 : n
   x_N = 1 - 2* bin_x_N_Minus_1 *
            bin_x_N_Minus_1;
   if (x_N > 0.0)
      bin_x(ind-1) = 1;
   end
   bin_x_N_Minus_1 =  x_N;
end
t = uint8(0);
key = zeros(n/8,1,'uint8');
for ind1 = 1 : n/8
for ind2 = 1 : 8
key(ind1) = key(ind1) + bin_x(ind2*ind1)*
                2 ^ (ind2-1);
   end
 end
```

The resulting stego-video obtained by the user is segregated into number of frames which are divided into 8x 8 blocks. 2D-IDCT is employed for each selected frame further preceded by data decryption and de-shuffling to obtain the original secret image as depicted in Figure 2. The different algorithms used in the proposed methodology are discussed below.

Figure 4: Pseudo code of Fisher Yates algorithm



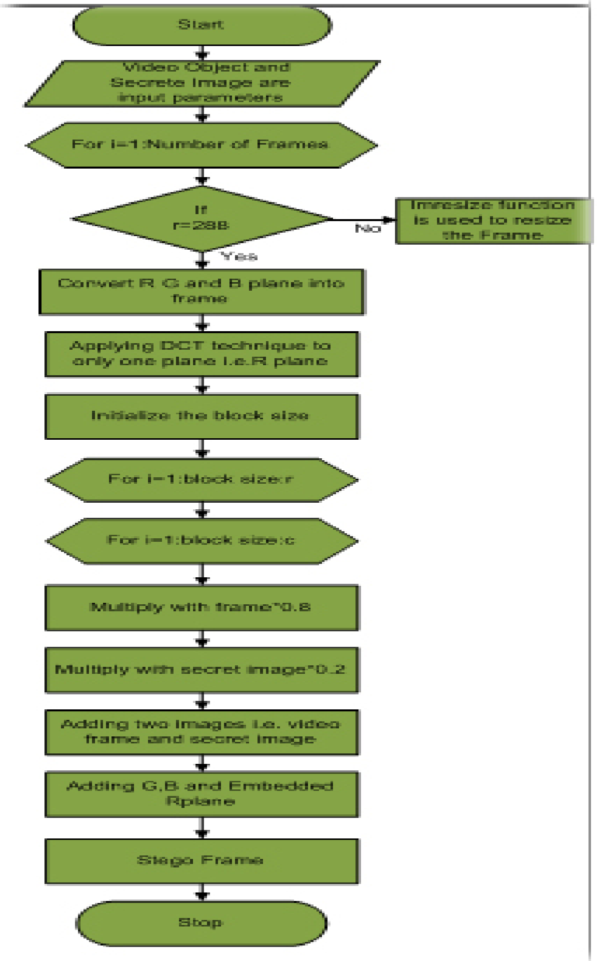
```
function X = Shuffle(X)
n = numel(X);
for i = 2:n         % Knuth shuffle in forward direction:
  w   = (rand * i);  % 1 <= w <= i
  t   = X(w);
  X(w) = X(i);
  X(i) = t;
end

for i = n:-1:2     % Knuth shuffle in backward direction:
  w   = (rand * i);  % 1 <= w <= i
  t   = X(w);
  X(w) = X(i);
  X(i) = t;
end

for i = 1:n   % Limit output:
  w    = (rand * (n - i + 1)) + (i - 1);   % i <= w <= n
  t   = X(w);
  X(w) = X(i);
  X(i) = t;
end
X = X(1:n);
```

2.1 RSA algorithm for Data Encryption and Decryption: Encryption is a process of encoding a message so that its meaning is not easily perceived by human and decryption is the reverse process of encryption. RSA is a asymmetric cryptosystems as different keys are used for encryption and decryption, which has come to be known by the acronym from the author's names R. Rivest, A. Shamir, and L. Adleman, the RSA cryptosystem. The key generation of proposed algorithm is shown in Figure 4.

2.2 Fisher Yates algorithm for data Shuffling and De-shuffling: Data shuffling is also called as a data masking algorithm where secret data is protected by shuffling. Fisher Yates shuffling algorithm is utilized in proposed methodology for data shuffling which is the essential technique for generating the arbitrary numeral 1to N. To shuffle the 'n' elements of arrays the conclusion rate is measured as (n-1). It presents unique randomness for each shuffle. It is relatively well-organized indeed, its asymptotic period and gap complication which are optimal. Shared with a high-quality unbiased arbitrary numeral basis, it is also definite to create unbiased outcomes. The benefit of Fisher Yates shuffle algorithm is its superior speed and accuracy in estimating the randomness of the information. The Pseudocode of Fisher Yates algorithm is shown in Figure 4.

2.3 Block generation using 2D-DCT and 2D-IDCT algorithm: Data hiding can be efficiently performed in the frequency domain. Steganographic method in frequency domain is performed using DCT technique (Discrete Cosine Transform).DCT permits a image to be divided into three frequency groups like the LF (Low-frequency) group, HF (High-frequency) group and MF (Mid-frequency) group. In this approach, the covert information is fixed into the DCT chunk which contains MF (Mid frequency) sub group apparatus where the high frequency sub group apparatus stay idle. The following mathematical expression represents the two dimensional discrete cosine transform (2D-DCT) for image of size N*N.

Figure 5: Flow Chart of Embedding


Start
Video Object and Secrete Image are input parameters
For i=1:Number of Frames
If r=288
No
Imresize function is used to resize the Frame
Yes
Convert R G and B plane into frame
Applying DCT technique to only one plane i.e.R plane
Initialize the block size
For i=1:block size:r
For i=1:block size:c
Multiply with frame*0.8
Multiply with secret image*0.2
Adding two images i.e. video frame and secret image
Adding G,B and Embedded Rplane
Stego Frame
Stop

$$F(j,k) = a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} f(m,n)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \qquad (1)$$

The equivalent inverse conversion, whether 2D-IDCT is represented as,

$$f(m,n) = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} a(j)\, a(k) F(j,k) \cos\left[\frac{(2m+1)j\pi}{2N}\right] \cos\left[\frac{(2n+1)k\pi}{2N}\right] \tag{2}$$

Where, $a(j) = a(k) = \sqrt{\frac{2}{N}}$

2.4 Embedding Process: This process is carried out at sender side in which, a secret message is embedded inside the cover video using embedding algorithm and generate a stego video or stego frame. The secret image is encrypted by RSA algorithm, further continued with data shuffling by using Fisher Yates algorithm. Then Discrete Cosine Transform (DCT) is applied to generate 8*8 blocks. On the other side, video is discretized into number of frames, each frame is extracted into R ,G and B plane and R-plane is applied with DCT to form 8*8 blocks which are embedded with earlier generated blocks to results in a stego-video. The detailed flow chart of embedding process is shown in Figure 5.

3.5 Extraction Algorithm

The extraction process is carried out at receiver side to extract secret message. The following steps are followed for performing extraction process.

Input: Stego video
Output: Hidden data
Step-1: Select stego video and convert it into Frames
Step-2: In this step frame generation takes place, next step to apply Inverse Discrete Cosine Transform (IDCT) 8×8 block generation method.
Step-3: Decrypt the extracted image.
Step-4: Display final secret image as output.
Step-5: Exit.

RESULTS AND DISCUSSION

The proposed method is simulated using MATLAB; the input to the process is secret image which is concealed into a cover video. Two evaluation parameters are considered for performance analysis - Mean Square Error (MSE) to measure distortion rate in the received stego-image using Equation 10 and Peak Signal to Noise Ratio (PSNR) to measure the embedding quality of stego-image in dB using Equation 11.

$$\mathrm{MSE} = \sum_{x=1,y=1}^{p,q} (\mathrm{Pix}_{\mathrm{BEx}} - \mathrm{Pix}_{\mathrm{AEx}})(\mathrm{Pix}_{\mathrm{BEy}} - \mathrm{Pix}_{\mathrm{AEy}})/(p * q) \tag{10}$$

$\mathrm{Pix}_{\mathrm{AE}}$ = Pixel values after image embedding

$\mathrm{Pix}_{\mathrm{BE}}$ = Pixel values before embedding

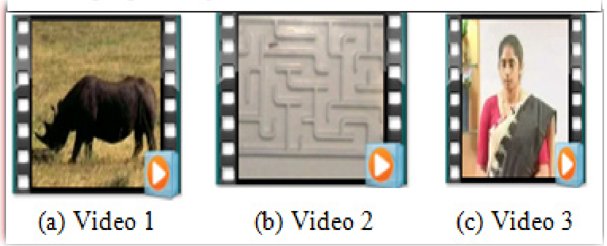
p*q = Image size

$$\mathrm{PSNR} = 10\log_{10}(2^q - 1/\mathrm{MSE}) \tag{11}$$

Figure 6: Different Secrete Images concealed in the proposed system

(a) Pirate (b) Lena (c) Woman-Blonde (d)Woman-Dark Hair

Figure 7: Different Cover videos used for concealing in the proposed system



(a) Video 1 (b) Video 2 (c) Video 3

Figure 8: Embedding process (a) Cover video (b) Woman-Dark Hair Secrete Image (c) Encrypted Image (d) DCT Image (e) Stego Frame

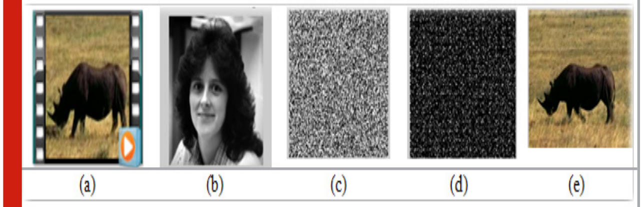
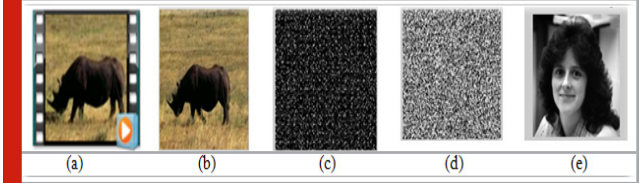


Figure 9: Extraction process (a) Stego video (b) Stego frame (c) Decrypted Image (d) IDCT Image (e) Secrete Image.



The secret images that are conceal in the different video are shown in Figure 6.Three cover videos are considered for testing the results are shown in Figure 7. Figure 8 and Figure 9 depict the process of embedding and extracting the secret image respectively. In each of the cases, secret image is encrypted, transformed to DCT image and then embedded into cover frame. The resultant embedded image is stego image frame. Then reverse embedding process is carried at the destination to retrieve the secret image. In the proposed system, performance analysis of secret image and cover video is presented in the Table 1. For all the cover videos, the value of PSNR is less for the image of Pirate in which pixel intensity variation is more when compared with other three images.

Table 1. Proposed System Performance Analysis for Secret Images

Sl. No.	Cover Videos Names	Video resolution (color)	Secrete Images Names	Secrete Images Sizes	PSNR (dB)	MSE
1	Video 1	352×288	Pirate	128×128	54.6253	0.22416
			Lena	128×128	56.1955	0.15615
			Woman-Blonde	128×128	56.0900	0.15999
			Woman-Dark hair	128×128	59.0632	0.08067
2	Video 2	352×288	Pirate	128×128	53.6140	0.23410
			Lena	128×128	55.1955	0.21408
			Woman-Blonde	128×128	55.1900	0.15469
			Woman-Dark hair	128×128	56.0632	0.15873
3	Video 3	352×288	Pirate	128×128	55.6201	0.21376
			Lena	128×128	55.1989	0.15
			Woman-Blonde	128×128	56.0173	0.15999
			Woman-Dark hair	128×128	57.5027	0.080679
				Average	55.78131	0.165583

Table 2. Comparison Table for Proposed and Existing Method of PSNR (dB)

Sl. No	Title	Method	Video Name	PSNR (dB)
1	A Novel Video Steganography Algorithm in DCT Domain based on Hamming and BCH Codes [8]	Existing Method	Video 1 Video 2 Video 3	40.21 38.95 40.55
2	A Novel Approach for Hiding Data in Videos Using Transform Domain	Proposed Method	Video 1 Video 2 Video 3	56.245 55.015 56.084

Table 3. Performance Analysis for different types of attack by considering video 1 and Pirate secret image.

Attacks Types	PSNR(dB)	
	Secret Image	Cover Image
Salt & Pepper	35.5155	45.4178
Gaussian	35.9832	40.9055
Poisson	35.5143	47.7659
speckle	35.5131	40.4604

Also the PSNR is more for the image of Woman-dark hair where pixel intensity variation is less. For all the secret images, it is observed that the average PSNR for the cover videos is 60.7091 dB which is beneficiary when compared with PSNR 40.73 dB of the existing system [8] which is shown in Table 2.

The four different types of noise attack such as Salt and pepper, Gaussian, Poison and Speckle are introduced into secret image to check the robustness of the proposed algorithm. The performance analysis for both secret and cover image has been done as shown in Table 3. It is clear from the table that the Speckle attack has more influence on PSNR.

CONCLUSION

This paper presents a new approach which binds the ideas of video steganography based on RSA data encryption, Fisher Yates data shuffling algorithm, DCT (Discrete Cosine Transform) technique. The application of data shuffling algorithm enhances data hiding level in the cover video. The proposed scheme has put forth a robust and secure video steganography method which would be able to hide data into a video file that provides a robust and secure way of data transmission. The overall system is implemented using MATLAB Tool. The performance of the system has been tested using PSNR. It is observed that the proposed system is beneficiary when compared with the results of existing system by Ramadhan J et al., [8]. Moreover the security and robustness of the method against various attacks have been confirmed.

REFERENCES

K B Shiva Kumar, K B Raja, R K Chhotaray, Sabyasachi Pattanaik (2010) Bit Length Replacement Steganography Based On DCT Coefficients. International Journal of Engineering Science and Technology, 2(8): 3561-3570.

Subramani, Prabu, Ganesh Babu Rajendran, Jewel Sengupta, Rocío Pérez de Prado, and Parameshachari Bidare Divakarachari. ”A Block Bi-Diagonalization-Based Pre-Coding for Indoor Multiple-Input-Multiple-Output-Visible Light Communication System.” Energies 13, no. 13 (2020): 3466.

Kousik Dasguptaa, Jyotsna Kumar Mondalb and Paramartha Dutta (2013) Optimized Video Steganography Using Genetic Algorithm (GA). International Conference on Computational Intelligence, Elsevier 10:131 - 137.

Ramandeep Kaur and Pooja (2014) XOR Encryption Based Video Steganography. International Journal of Science and Research, 2(11): 2319-7064.

Shahzad Alam, S. M. Zakariya and Nadeem Akhtar, ”Analysis of Modified Triple A Steganography Technique Using Fisher Yates Algorithm”, pp. 207-212. IEEE, 2014.

Amritha Sekhar, Manoj Kumar and M. Abdul Rahiman (2015) A Novel Approach for Hiding Data in Videos Using Network Steganography Methods. Procedia Computer Science, Elsevier, 70: 764-768.

C. Aishwarya and J. R. Beny (2015) Novel Architecture for Data – Shuffling Using Fisher Yates Shuffle Algorithm. International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), 1(6): 387-390.

Nithiya Devi.G, Sharmila.S, Saranya.N, Rajkumar.K.K, and Gomathi (2016) Novel Architecture for Data – Shuffling Using Enhanced Fisher Yates Shuffle Algorithm. International Journal of Engineering Science and Computing (IJESC), 6(5): .4932-4935.

Ramadhan J. Mstafa and Khaled M. Elleithy (2016) A novel video steganography algorithm in DCT domain based on hamming and BCH codes. IEEE: 208-213.

Parameshachari, B. D., Rashmi P. Kiran, P. Rashmi, M. C. Supriya, Rajashekarappa, and H. T. Panduranga. ”Controlled partial image encryption based on LSIC and chaotic map.” In ICCSP, pp. 60-63. 2019.

Mumthas S and Lijiya A (2017) Transform Domain Video Steganography Using RSA, Random DNA Encryption and Huffman Encoding. International Conference on Advances in Computing & Communications, Elsevier, 115: 660–666.