Computers, Materials & Continua
DOI: 10.32604/cmc.2023.030197
Article

Tech Science Press

Improved Video Steganography with Dual Cover Medium, DNA and Complex Frames

Asma Sajjad[1], Humaira Ashraf[1], NZ Jhanjhi[2,3,*], Mamoona Humayun[4], Mehedi Masud[5] and Mohammed A. AlZain[6]

[1]Department of Computer Science and Software Engineering, International Islamic University, Islamabad, Pakistan
[2]School of Computer Science, SCS, Taylor's University, Subang Jaya, 47500, Selangor, Malaysia
[3]Center for Smart Society 5.0, [CSS5], FIT, Taylor's University, Subang, Jaya, 47500, Selangor, Malaysia
[4]Department of Information Systems, College of Computer and Information Sciences, Jouf University, KSA
[5]Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif, 21944, Saudi Arabia
[6]Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
*Corresponding Author: NZ Jhanjhi. Email: noorzaman.jhanjhi@taylors.edu.my

Received: 21 March 2022; Accepted: 22 June 2022

Abstract: The most valuable resource on the planet is no longer oil, but data. The transmission of this data securely over the internet is another challenge that comes with its ever-increasing value. In order to transmit sensitive information securely, researchers are combining robust cryptography and steganographic approaches. The objective of this research is to introduce a more secure method of video steganography by using Deoxyribonucleic acid (DNA) for embedding encrypted data and an intelligent frame selection algorithm to improve video imperceptibility. In the previous approach, DNA was used only for frame selection. If this DNA is compromised, then our frames with the hidden and unencrypted data will be exposed. Moreover the frame selected in this way were random frames, and no consideration was made to the contents of frames. Hiding data in this way introduces visible artifacts in video. In the proposed approach rather than using DNA for frame selection we have created a fake DNA out of our data and then embedded it in a video file on intelligently selected frames called the complex frames. Using chaotic maps and linear congruential generators, a unique pixel set is selected each time only from the identified complex frames, and encrypted data is embedded in these random locations. Experimental results demonstrate that the proposed technique shows minimum degradation of the stenographic video hence reducing the very first chances of visual surveillance. Further, the selection of complex frames for embedding and creation of a fake DNA as proposed in this research have higher peak signal-to-noise ratio (PSNR) and reduced mean squared error (MSE) values that indicate improved results. The proposed methodology has been implemented in Matlab.

Keywords: Video steganography; data encryption; DNA embedding; frame selection

1 Introduction

Data security during transmission is one of the ever-increasing concerns in today's world; as a result, methods and means to address the challenges of data security are being investigated continuously. The field of cybersecurity safeguards data against a variety of threats and attacks.

Cyberattacks may disrupt, corrupt, or steal shared information. While there are other information security techniques available, cryptography and steganography tend to be the best when it comes to safely transporting data between the source and destination. Cryptography is the process of modifying a message in such a way that it becomes incomprehensible to a third party. A key is used in cryptography to encrypt and decrypt data. There are two types of cryptography: symmetric and asymmetric. DES, AES, RC4, IDEA and RSA are among the most extensively used encryption algorithms. Steganography is a technique that ensures the security of critical data by encapsulating it in a cover medium hence concealing its existence [1]. The ability of Human Visual Systems (HVS) to camouflage messages has been a widely used steganography technique for concealing critical information in still photos. Plain text steganography conceals the message within text using special characters, symbols, and the cover medium's white spaces. Video steganography is another emerging field that hides messages into a video exploiting HVSs less sensitivity to the minor changes in video scenes. Many approaches have been proposed in video steganography. The modification of the Least Significant Bit (LSB) is a well-known approach in digital image steganography. The LSB technique conceals the binary equivalent of the secret message within each pixel's least significant bit. This approach is extremely sensitive to attacks because of its simplicity. The discrete cosine transform (DCT) is applied to the LSB of an image's pixel values to generate a compressed steganography image. An emerging steganographic field based on DNA has been proposed by researchers as a new data hiding method [2]. One gram of DNA may hold up to 215 petabytes of data. The randomness of the building blocks forming the DNA, its enormous storage capacity, less computing power make it an ideal cover and storage medium. Many DNA steganography algorithms have been proposed for creating a fake DNA to be used as a cover medium. All these techniques require a message, a secret key, and a DNA sequence to be used as a cover medium. The technique is at times improved by first encrypting the message before embedding. This reduces penetration risk and produces a dual cover to the data. Another technique is the insertion of a random DNA strand XORed with a user-supplied key. In all these techniques a constant DNA strand is used. This strand if breached is vulnerable enough to aid in the decryption of the cipher text. Further, the fake DNA is embedded in random locations that produces visual artifacts in the stego video that give the first chances of presence of some data to any eavesdropper.

The purpose of this research is to provide an efficient technique using a combination of cryptography and steganography algorithms. This research proposes two new algorithms. The first one is for the creation of a fake DNA and second algorithm selects intelligent locations for embedding in the cover medium reducing the first chances of visual perceptibility. In our work, we have experimented on mpeg4 videos as the cover medium. The proposed approach has shown better results in terms of maintaining video perceptibility reduced MSE and PSNR.

2 Manuscript Layout

The paper is divided into five categories. Section 3 highlights the research contributions of this research. Section 4 discusses the literature review. Section 5 describes the recommended strategy in detail. Section 6, discusses the security analysis of the proposed technique. In Section 7 we discuss the experimental results, and Section 8 summarizes the proposed approach.

3 Research Contribution

The main contributions of this research are enumerated below:

1. A new technique has been introduced in DNA steganography for embedding the stego message within the DNA. Previously, DNA was used as a means of frame selection [3] or as a key for encryption and decryption.
2. Further, a novel frame selection mechanism has been introduced for embedding the stego message that maintains the perceptibility of frames by embedding only in complex frames. Thus hiding the first chances of visual perception.
3. The results of the proposed techniques are better both in terms of MSE and PSNR.

4 Literature Review

DNA characteristics are suggested by Kar et al. [2] for embedding secret message in a video. Selection of frames is based on the binary values of DNA, the number of codons, and a user-supplied key. For frame selection, a random number is generated by the linear congruential generator and then XORed with DNA. Burger chaotic map in combination with LGC i.e., linear congruential generator is utilized for pixel selection. LSB replacement strategy is used for concealing the data at arbitrary positions. In this scheme the selected frame is ultimately a random frame that might not be detected. But hiding data in random frames does not guarantee safety of the hidden message. Hiding in any random frame lacking analysis of the contents of the frame host artifacts in the frame that make the video itself perceptible.

The modified least significant bit strategy of Ramalingam et al. [3] creates an encrypted and a non-encrypted avi file. The encrypted file contains the encrypted message using a symmetric key for encryption of text. Message is revealed by finding out the bit by bit difference between the two created files and then decrypting the message using a symmetric key which is altogether a compromised approach in terms of encryption using a symmetric key and using two files for transmission.

Cao et al. [4] suggested an embedding method based on the H.264 that uses motion vectors to store the secret message. To reduce the changes in motion vectors, linear block codes have been used. But this technique compromises the visual quality of the reconstructed images.

Yi et al. [5] introduced a steganography approach based on a motion vector through the use of matrix encoding. A motion vector component with a large amplitude that exists in both vertical and horizontal components are chosen to embed the coded message. The Human Visual System is capable of detecting changes in a slow moving object, but failing while when the same object travels quickly. Hence author utilizes large-scale motion vectors for the purpose of inserting the hidden message. No encryption of the embedded message has been proposed in this method.

Kelash et al. [6] concealed data within frames by splitting each pixel of the frame into two parts. The data is embedded into the pixels based on their color histograms. The frames chosen are on the bases of high threshold difference between RGB histograms of two frames. The pixels are embedded in a frame with a greater difference. This gives a clear clue to an eve's dropper when he sees these mild color changes due to pixel embedding compared to sharp color changes in a similar video.

The DNA insertion algorithm has been modified by Malathi et al. [7]. The algorithm makes use of two distinct keys. The message is encrypted using the first key. K2 being the second key is produced randomly and it segments the DNA into equal parts. At the beginning of each segment, the resulting cypher characters are inserted as binary bits one by one. A DNA rule-based dictionary is used to translate the binary sequence into DNA bases.

Wang et al. [8] encrypt the secret message prior to embedding using the vigenere cypher. The cypher text is then converted in to binary and hidden by means of DNA encryption approach, resulting in a better-quality video steganography technique and detection of modified frames in a stego-video. Jiao et al. [9] proposed using encryption to conceal data within living beings' DNA. The message is binary transformed from DNA bases or codons. 35 codons were employed in the implementation of this study. The position of the codons that are substituted by the message is presumed at first. The encryption allows for quiet DNA sequence mutation. The complement of encryption is performed during the decryption process in order to recover the hidden message.

In a cloud computing context, Abbasy et al. [10] suggested a data concealing approach in DNA sequences for resource sharing. This document protects data in the cloud that is accessible to the public. This approach uses complementary algorithm to combine the bases of used DNA and that of the DNA transformed message to form a complete message. The fictitious DNA is manufactured and stored in the cloud. The client downloads the false DNA and retrieves the data using the inverse of the complimentary process. The complimentary algorithm has a higher likelihood of cracking than the substitution approach.

According to Peterson et al. [11], the confidential message is concealed within a DNA sequence by substituting the character on the free consecutive bases of a DNA sequence. They assigned a codon to every letter. In case a letter appears multiple times it will be easy to decrypt. This characteristic can be used by an attacker to decrypt the communication. This is one of the pioneering works of concealing data within a DNA sequence and uses a very preliminary approach.

Liu et al. [12] concealed a secret message within DNA using insertion, substitution, and complementary techniques. Using the insertion approach, the message i.e., transformed in to a binary message is placed at the beginning of the binary transformed DNA sequence. This work likewise use the replacement approach in conjunction with the complementary rule to embed the concealed message in the sequence. The cracking probability of each approach is determined to ensure the algorithms' security. The insertion procedure is the least likely to result in cracking.

Agarwal et al. [13] employ substitution method using a DNA dictionary to camouflage the data inside the DNA. The proposed strategy improves the embedding capability and security of the present substitute method. Codons are utilized to conceal information inside the DNA sequence. Binary transformations are performed on the codons, and their lengths are tested for multiples of six. If it is a multiple of six, it is left alone; otherwise, it is appended to the binary string with additional zeros. Codons are used to convert the six-bit binary code to DNA. The altered DNA is then transmitted to the recipient. The receiver retrieves the data by reversing the algorithm.

Mumthas et al. [14] use 2D DCT steganography, Rivest–Shamir–Adleman (RSA), random DNA encryption, and Huffman encoding. The original message is converted to cypher text using the RSA technique, then random DNA encryption and compression are applied. A random DNA encryption technique is utilized instead of fixed DNA encryption. The mapping of codons against amino acids is through DNA-based random numbers. The positions of codons and amino acids are decided by a random permutation of accessible places. Each 8 × 8 block of the cover video's frame is subjected to DCT. The compressed message is concealed in the coefficients' less significant sections.

Khalifa et al. [15] suggested a steganography algorithm using DNA also. The proposed approach is divided into two distinct stages. In stage one, the secret message is originally encrypted using a DNA-based Playfair cypher. At stage two, the encrypted secret message is concealed within some reference DNA via a substitution approach. That is, the reference DNA's bases are substituted with the encrypted DNA in accordance with a generic two-by-two complementary rule. The performance of the presented algorithm is evaluated in terms of its ability to conceal data as well as its resistance to attacks. Hiding data in DNA makes advantage of a variety of biological properties and is not particularly efficient to execute economically.

To encrypt and disguise the user data in the video, Jose et al. [16] proposed a combination of cryptography and steganography. For generating keys, they developed SHA512-ECC, which combines the SHA512 hash function with the elliptic curve–ECC. They employed an upgraded version of the crow search algorithm, which they called CM-CSA, for pixel selection. The plain text is first taken as input, after which it is compressed and encoded using an improved version of the Huffmann Algorithm known as the IHA. SHA512-ECC algorithm is used to encrypt the DNA encoded data. Finally, these encrypted data is hidden into the optimal pixel points of the video frames using the CMCSA.

Fuad et al. [17] embedded text in the object motion regions by using motion analysis. Using DCT-psycho visual effects of hiding messages, the suggested technique picks six DCT coefficients in the intermediate frequency. The proposed approach is used to embed a message by altering middle DCT coefficients. Text is not encrypted which recovers the message once pixels are identified.

Arraziqi et al. [18] compressed text using ZIP algorithm. The proposed algorithm adds a compression and encryption algorithm to secret data before distributing. There are 2 proposed algorithms, embedding and extracting algorithms. Compression of secret data is done using ZIP algorithm. Encryption is done using AES algorithm. The compressed and encrypted secret data is embedded at the end of the frame evenly to produce stego FLV. This technique is only tested for flv codecs.

Hussein et al. [19] proposed an encryption using Turbo Code. Embedding is done using least two Significant Bit Technique. This strategy embeds a logo inside video frames by using the Turbo system and least two significant bit. It embeds the logo after converting the cover to the frequency domain by using Fast Fourier Transform. Although the technique promises good results but degrades the video quality.

Karmakar et al. [20] use a dictionary to describe each video frame as a sparse matrix with only few substantial sparse coefficients. They compressed the video by encoding non-zero sparse coefficients along with their addresses. A 5D hyper-chaotic system is used in conjunction with DNA coding to generate a hyper-chaotic key, which is then incorporated into the encryption scheme to increase the security of video transmission. Due to the use of patch-based modification, the rebuilt frames exhibit a blocky appearance.

In the method used by Rout et al. [21], motion vectors were used to represent the displacement of the spatial video unit from one frame to reduce the temporal redundancy. To reduce inter frame temporal redundancy, macro blocks (MB) of B × B pixels were used in the motion model in the video compression methodology. The difference (error) frame in motion compensated frame prediction was determined as the difference between the actual frame and the predicted frame. There are often smooth regions with less motion in original video frames. As a result, the motion vectors and corresponding prediction error blocks are mostly homogeneous in these regions. These regions were targeted for embedding in this paper.

The aim of method proposed by Younus et al. [22] is to hide data in video and to ensure its security. This method begins with writing the message using the alphabets of English language then secured by encoding. During embedding, knight tour algorithm and LSB method was used. This process breaks the video into frames, these frames are then altered into images. Next step involves random selection of frames to be used as cover, knight tour algorithm was used to select pixels from selected frames. LSB method was used for hiding the cypher text in the selected pixels. After embedding, extraction process starts. The recipient divides the stego video into frames. Then using the same steps and knight tour algorithm used for embedding, pixels containing the data are identified and secret message is extracted using LSB method.

Method of Febin et al. [23] focuses on identifying violence or fights by filtering movements and motion boundary SIFT (MoBSIFT). Motion boundary SIFT (MoBSIFT) was an improved method for detecting violence. Extracted frames were converted to gray scale. Motion in each frame was detected through movement filtering. Only frames having motion will undergo feature extraction. Temporal derivative was an efficient method used for identifying violent videos. This research paper also discusses how nonviolence videos can be easily identified. There was still a need for more accurate method for feature selection.

Suresh et al. [24] devised a new method to hide data by the application of Fractional Grey Wolf Optimization. The optimization algorithm reads the fitness function derived from the cost function to find the global optimal region to embed the secret information. Encryption is accomplished through two steps: key generation and nonlinear diffusion.

Wan et al. [25] proposed method for removing redundant frames for video surveillance. His approach begins with the determination of the spatiotemporal interest points of each frame using the improved spatiotemporal interest point detection algorithm. Surround inhibition was then used in conjunction with local and temporal constraints to identify static interest points in the frame. In this way, by comparing the changes in the number of motion detection boxes, a large number of redundant frames in a long video can be removed which increases the speed of processing. Video segmentation was performed on the long video which doesn't have redundant frames and then SOI was extracted for retrieval of video event.

In Huang et al. [26] method, CapsNet was used to extract spatiotemporal features and generate inter-frame motion curves from video sequences. The purpose of this approach was to generate a summarized video for which key frames were selected. The key frames were chosen using the automatic shot segmentation method and the self-attention model.

Zhang et al. [27] proposed a technique for selecting pixels for embedding using a particle swarm optimization-based bacterial foraging algorithm. Zhang et al. [28] also suggested using Hurst Component for selecting appropriate pixels for embedding audio watermark.

Raju et al. [29] use the Mersenne Twister algorithm to hide information inside random pixels. They embed the AES encrypted test into the LSB locations achieving a PSNR 71.482 with MSE of 0.0046. The data is embedded in random pixel locations without looking at the contents of the frame, which generates visible artifacts in the stego video.

5 Proposed Approach

The proposed approach is a combination of cryptographic and steganographic techniques to make it more promising in terms of security. The solution comprises of multiple stages of processing that the data has to go through before being ready to be embedded. The first stage requires a cover medium, which in the proposed approach is an mpeg4 video. We initially separate our video into individual frames that will later be used for embedding. The second step after encryption is embedding the cipher text in a video. The raw data goes through multiple preprocessing stages such as encryption and DNA embedding before being embedded in the video. Once data is converted to cipher text it is embedded into selected video frames. This involves the selection of suitable frames. Without examining the contents of the frame, hiding information in any random frame [2] produces visible artefacts in the video that can help an attacker in the detection of message locations. The proposed solution aims to improve these issues by utilizing DNA as a cover medium for the cryptographic message and then using the chaotic map and linear congruential generator to strengthen our approach by further securing the embedded locations within the frames. For frame selection, we have a new algorithm that uses only the complex frames for embedding. The flow chart in Fig. 1 presents the overview of our proposed approach.

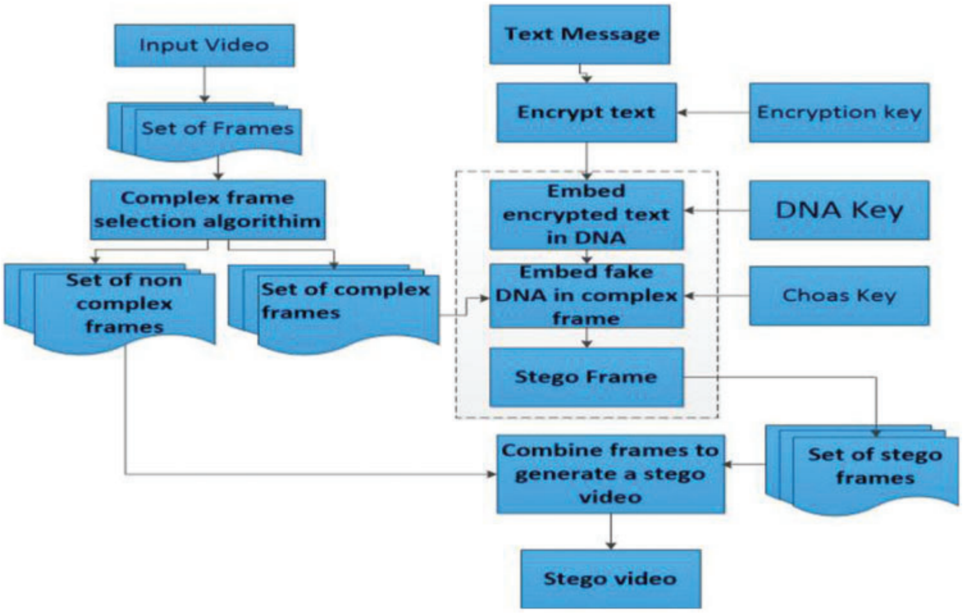

Input Video
Set of Frames
Complex frame selection algorithim
Set of non complex frames
Set of complex frames
Text Message
Encrypt text
Encryption key
Embed encrypted text in DNA
DNA Key
Embed fake DNA in complex frame
Choas Key
Stego Frame
Combine frames to generate a stego video
Set of stego frames
Stego video

Figure 1: Flow chart of the proposed DNA scheme

5.1 Frame Selection

The frame selection module is a critical component of our proposed solution for this problem. In this module, we, segregate complex frames of our video. Complex frames are those frames that involve any scene change. We will embed our data only in these frames. The reason behind using only complex frames for this purpose is to camouflage the secret data behind the motion estimation information. Frames involving scene change have object movement, color change, object infusion, and diffusion. So, taking advantage of this information secret text is infused only in these frames. For the detection of complex frames, we have used the key frame extraction technique mentioned in [30]. Discrete Cosine

Transform i.e., DCT coefficients are extracted from each frame of the video. Using the difference of the Mean of two consecutive frames, frames with scene change are segregated. If the mean of consecutive frames is not the same, it means there is some change between these frames. Hence that frame is selected as a complex frame. This is done for all frames of the video to achieve a subset of frames known as the complex frames. This procedure is given in the form of the algorithm in Tab. 1 below. Once complex frames are selected, the next step is preparing the data for embedding. This is done in the data encryption step.

Table 1: Frame selection algorithm

Algorithm 1: Frame selection algorithm

```
Frame selection algorithm:
Input: Video P
Output: An array of complex frames
for each frame i
    find DCT of frame i
    find MEAN of the DCT of each frame
    if MEAN of the frame(i) and frame($i - 1$) is not the same select the $i^{th}$ frame as a complex frame
        selected frame(ta)= frame(i)
    end
end
```

5.2 Data Encryption

Data encryption involves two phases of encryption. The first one is the encryption of the text message by a cipher. After this encryption, we add another layer of security by using the concept of DNA Cryptography. We embed our encrypted text in DNA using the technique referred to by [10]. We call this data encryption algorithm explained in Tab. 2. According to this algorithm, M is the encrypted message that will be embedded in the video and the final DNA encrypted message be M´´´. M´´´ is the encrypted message the receiver shall receive. This involves three phases to convert M to M´´´ before embedding in the video. This algorithm is shown in Fig. 2 First, the encrypted message is converted to fake DNA nucleotides by applying the DNA base pairing rules which give M´. Then M´ is converted to M´´ by applying DNA Complementary Rules on M´ which gives us M´´. In the final stage, using a reference DNA, we find index of each nucleotide pair in reference DNA Sequence and replace M´´ nucleotide pair with its index which gives M´´´. Now this M´´´ can be embedded in cover videos selected frames.

Table 2: Data encryption algorithm

Algorithm 2: Data encryption algorithm

```
Data encryption algorithm:
Input: Cipher Text M
Output: Fake DNA
Convert M to binary
for each binary pair $X_i$ in M´
    apply DNA complementary rule to get M´´
end
for each pair $X´´_i$ in M´´
    extract the index of each couple nucleotide using the reference DNA numerically
end
```

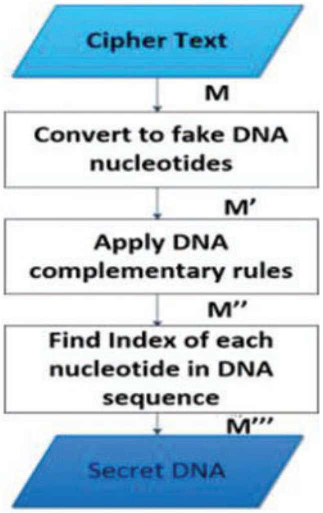

Cipher Text
M
Convert to fake DNA nucleotides
M'
Apply DNA complementary rules
M''
Find Index of each nucleotide in DNA sequence
M'''
Secret DNA

Figure 2: Conversion of cipher text to DNA code

Once the secret message is ready, the next step is its embedding in the video. We have added security here by embedding the encrypted message only in complex frames. To add further security and maintain video perceptibility a subset of the selected frames and pixels will be utilized. Out of the complex frames we further choose random pixels. These pixels are chosen by using a combination of pseudo-random generators, the Burger chaotic map and linear congruential generator [2]. As chaotic maps seed value always changes for each frame therefore the generated pixel set will always change making it unidentifiable for an attacker. Fig. 3 shows (a) the x-y plot of the pixels generated burger chaotic map, (b) shows the selected sub set for embedding.

Fig. 7 shows the chaotic map of selected pixels within frames and the selected sub pixels image; (a, b) shows the chaotic map of selected pixels rhinos and sub pixels image, (c, d) shows the forest map of selected pixels and sub pixels image, (e, f) shows the sky map of selected pixels and sub pixels image and (g, h) shows the school map of selected pixels and sub pixels image.

The pixel set generated by the chaotic map is fed to the linear congruential generator. Because of its relative ease of use, linear congruential generators are one of the most seasoned and well-known systems for producing random numbers [26]. The permutation cypher is used to embed 3 bits from each of red and green, and 2 from blue [2]. Fig. 9 shows the original and stego images of frame 70 of video titled rhinos, forest, sky and school respectively.

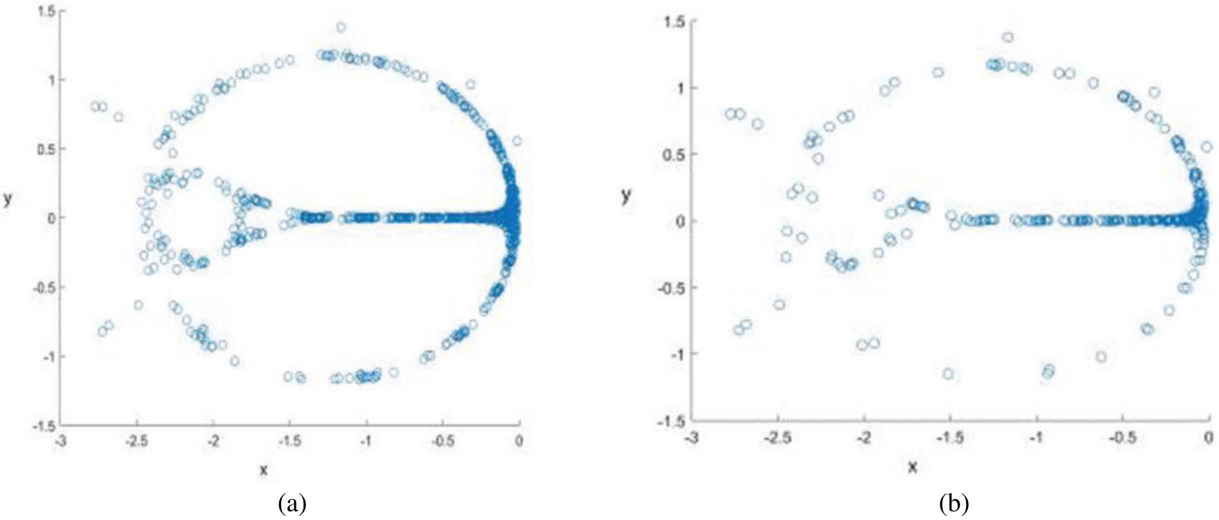
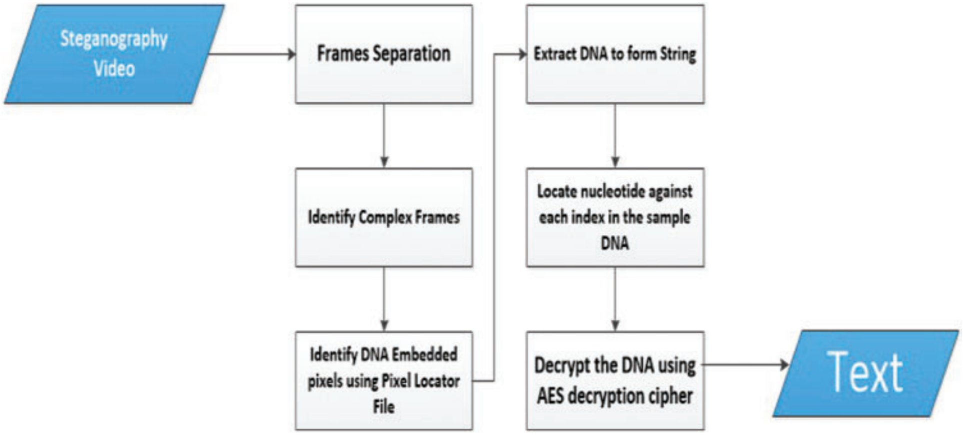


Figure 3: (a) Chaotic map of all pixels (b) chaotic map of selected pixels

5.3 Extraction Module

The original message from the stego video is extracted using the data extraction procedure as shown in Fig. 4. For this, the frames of the stego video will be separated again. This module uses the same parameters as in the encryption phase. For the data extraction separate the stego video into the same number of frames and under the same parameters as in the time of encryption.



Steganography Video
Frames Separation
Identify Complex Frames
Identify DNA Embedded pixels using Pixel Locator File
Extract DNA to form String
Locate nucleotide against each index in the sample DNA
Decrypt the DNA using AES decryption cipher
Text

Figure 4: Extraction of cipher text from DNA

Identify the complex frames in which the encrypted content was embedded using the frame embedding algorithm. Locate the embedded pixels within the stego frames using the pixel points given by the chaotic map. Each pixel's bits should be retrieved in the order 3, 3, 2, i.e., 3 bits each from red and green, and 2 from blue. The values retrieved are the index values in the reference DNA i.e., M´´´. Replace the nucleotide pair against each index with its nucleotide pair in the reference DNA, this will give M´´. M´´ is converted to M´ by applying DNA complementary rules. In the last step M´ is decrypted using AES encryption to reveal the hidden text.

6 Results and Discussions

For experimentation dataset used is the same as in [2]. Results are discussed for the sky.mpeg4 file that has a duration of 14 s and a file size of 2.91 Mb. In the input video file, there are 441 frames in total. The algorithm requires 2 security keys. One is for the encryption of data using the cipher and the other is a random DNA for embedding the encrypted text. Part of the DNA strand used is "GATCACAGGTCTATCACACCCT ATTACCACT". The text has been encrypted using AES. An example of the proposed method is shown below. $X_n = 2118$, $a = 21$, $c = 62$, and $m = 1000$ are the starting values for LCG. A series of random values will be generated by LGC i.e., the linear congruential generator using the seed value 10, $P = 408$, $Q = 408$. Starting with the fourth codon, a total of 204 codons are chosen. The codon for this experiment is GATCACAGGTCTATCACCCTATTAACCACTCACGGGAGCTCTCCATGCATTTGGTATTTT CGTCTGGGGGGTGTGCACGCGATAGCATTGCGAGACGCTGGAGCCGGAGCACCCTATGTCGCAGTATCTGTCTTTGATTCCTGCCTCATTCTATTATTTATCGC ACCTACGTTCAATATTACAGGCGAACATACCTACTAAAGT. The key for the AES cipher is = 12481632641282754, frame number = 7, and first value of chaotic map = 0.3. We have analyzed our method using Mean Squared Error, Peak Signal to Noise Ratio, histogram analysis and the quality of the steganographic video frames. Three videos of the same resolution and frame rate as in [2] were used as a comparison. Their detail is given in Tab. 3 below.

Table 3: Cover video details

File Mpeg 4	Duration (s)	Size (MB)[a]	Total frames	Selected frame
Forest	42	3.64	643	520
Rhino	7	0.29	114	88
School	26	1.08	787	101
Sky	14	2.91	447	31

6.1 Mean Squared Error (MSE)

Aggregating the differences between the corresponding pixel values of the original and the stego video frame mean square error is calculated. We calculate the difference between the original and the stego video frame, and divide the total by the frame's size using formula, $MSE_e = \sum_{n=1}^{h}\sum_{n=1}^{h}\left(C_{ij}^{c} - s_{ij}^{c}\right)$. Two bytes are selected of the color c at the (i, j) location from the original frame and stego frame here in called the C_{ij}^{c} *and* S_{ij}^{c} respectively, c is the color component, w = width of image, h = height of image. Tab. 4 shows the MSE values derived from video using the proposed algorithm and random frame selection strategies [2].

The Tab. 4 and Fig. 5 shows that the suggested approach gives improved result for the proposed approach as it has a lower MSE value than the algorithm [2] and algorithm [14].

Table 4: Results for MSE

Name of video file	Proposed mechanism	Algorithm [15]	Algorithm [3]
	MSE	MSE	MSE
Rhino	1.6526e-04	1.351e01	1.8181e-04
Forest	1.2049e-04	1.653e01	1.7484e-05
Sky	1.7606e-05	1.139e01	2.8247e-06
School	1.0102e-04	2.657e01	1.3753e-05

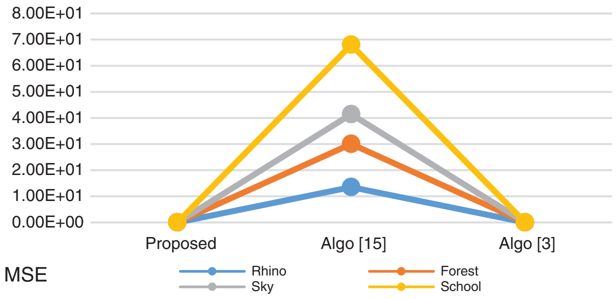


Figure 5: Results for payload

6.2 Peak Signal to Noise Ratio (PSNR)

The quality of an image corrupted due to noise and blur can be measured using PSNR. It is used to determine the degree of similarity between the original and stego frames by calculating the difference between them. Higher the value of PSNR, indicates higher the quality rate and more similarity between the two frames. MSE is indirectly proportional to the PSNR. PSNR is computed by using the following formula $PSNR = 10\log_{10} Maxl^2/MSE$. Where Maxl denotes the highest pixel value of a RGB image, (8 bits for each making one pixel is equal to 24 bits). PSNR is calculated separately for each of the three channels, resulting in a maximum value of (28–1) = 255. The suggested algorithm's results were compared to Video Steganography employing random frame selection techniques [2]. We created four videos with the same resolution and frame rate as for comparison as in [2]. Tab. 3 lists the video files and their descriptions. The PSNR of the proposed approach, algorithm [2], algorithm [5] and algorithm [14] are compared in Tab. 5. We may conclude that the suggested approach produced improved results, as shown in Tab. 5.

Table 5: Results from DNA frame selection technique [1] and proposed algorithm for PSNR

Name of video file	Proposed mechanism	Algorithm [15]	Algorithm [3]	Algorithm [6]
	PSNR	PSNR	PSNR	PSNR
Rhino	33.2126	36.8241	32.1959	32.625
Forest	32.3982	33.8256	25.3075	30.519
Sky	42.1388	37.793	36.4644	36.118
School	35.8532	34.712	31.1546	32.951

The PSNR values obtained are higher than those obtained using random frame selection technique. The higher the PSNR value, the better the quality of the stego video. As a result, the proposed technique provides increased security and can produce a video that is as identical to the original cover-video as possible with minimal distortion. The proposed approach shows improved results in terms of payload as well, as shown by the payload comparison of proposed approach and algorithm [2] Tab. 6 and Fig. 6.

Table 6: Results for payload

Name of video file	Proposed mechanism	Algorithm [3]
	Payload	Payload
Rhino	1.1393	1.0174
Forest	1.0696	1.0087
Sky	1.0131	1.0016
School	1.0696	1.0087

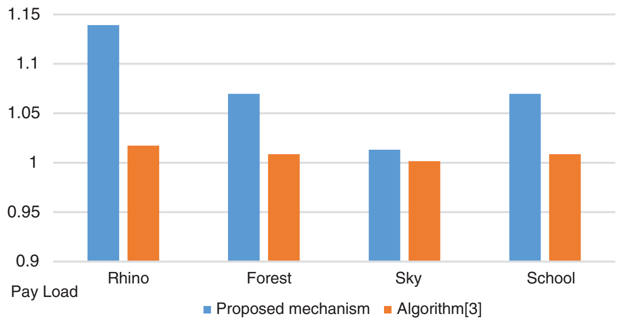


Figure 6: Results for payload

6.3 *Histogram Difference*

The histogram plots the frequency components in an image along horizontal and vertical axis. The horizontal axis indicates the pixel's RGB color level while the vertical axis indicates the number of times each color value in a pixel appeared in the frame. The pixel's range fluctuates between 0 and 255. We can see the distribution of intensities in the video frame by taking a histogram of each frame, which will display the amount of difference between the two frames and also give us an understanding of the video quality. Fig. 8 shows the histogram of selected frames of the sample stego videos rhinos, forest, and sky and their originals. The histogram of the frame where the scene changed abruptly, as opposed to the histogram of the frames where the scene changed gradually in all the stego frames, shows abrupt changes. The histograms show extremely mild changes due to distributed embedding in random locations among selected frames. As a result, stego video frame alterations relative to the original video frame will neither disclose nor reduce visual imperceptibility.

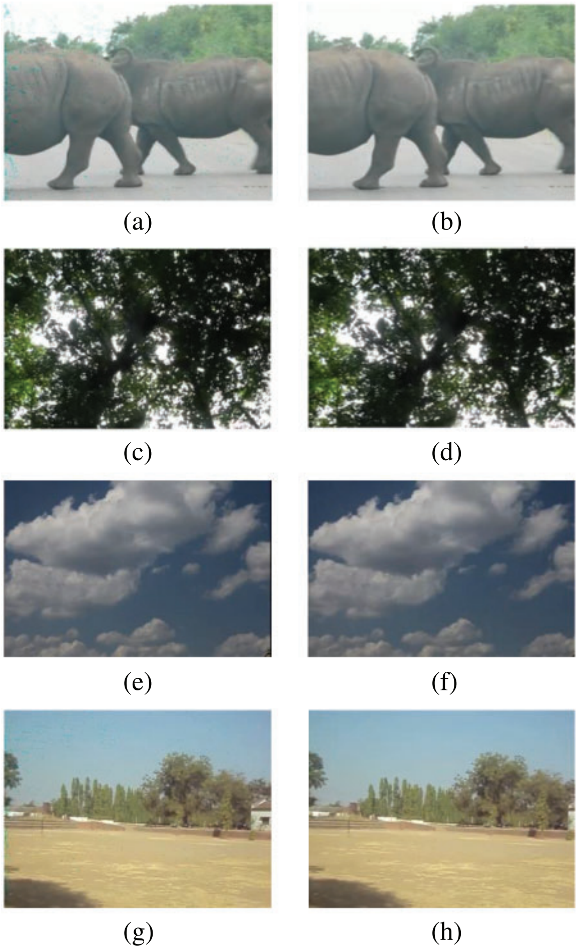
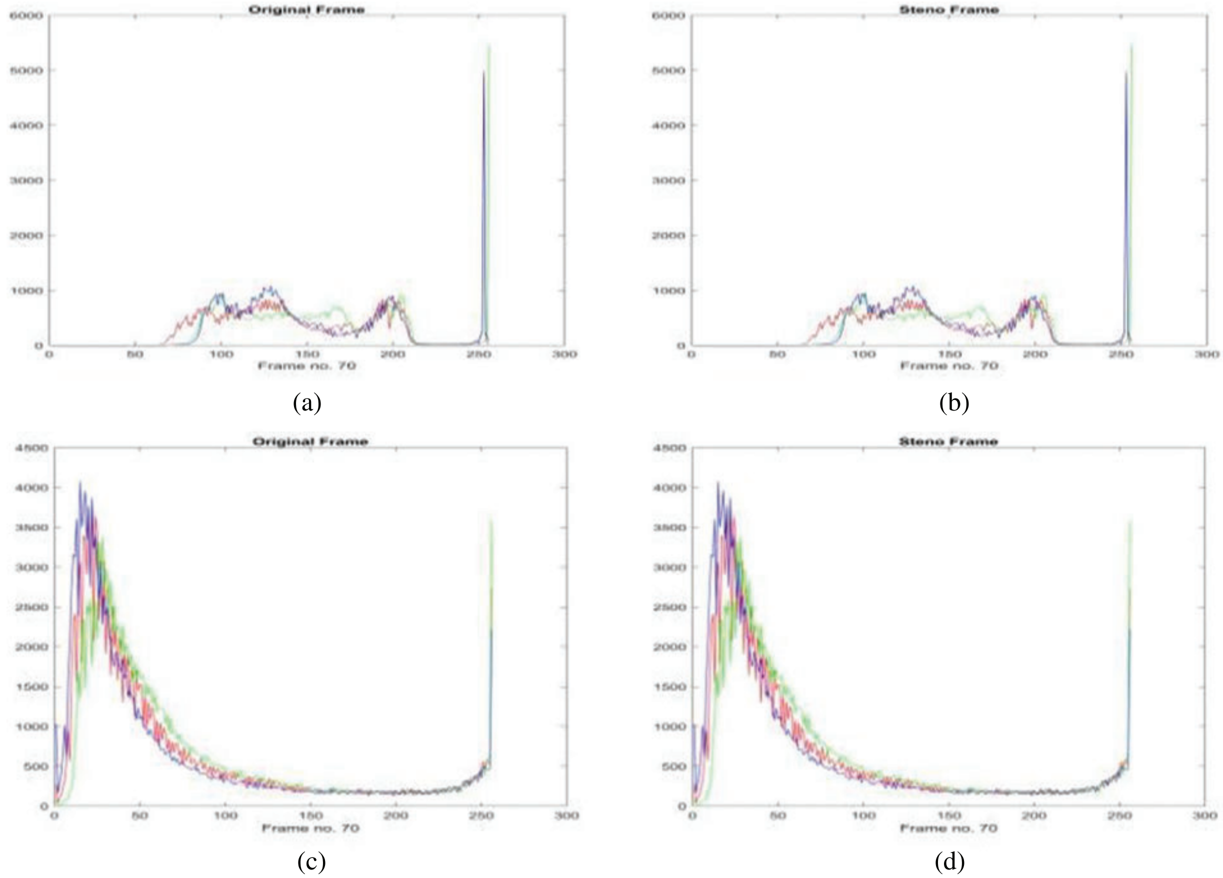


Figure 7: (a, b) Chaotic map of selected pixels rhinos and sub pixels image (c, d) forest map of selected pixels and sub pixels image (e, f) sky map of selected pixels and sub pixels image (g, h) school map of selected pixels and sub pixels image



(a)

(b)

(c)

(d)

Figure 8: Histogram of frame 70 of cover and stego frame (a,b) rhinos (c,d) forest

6.4 Pixel Correlation

Images have high data redundancy. As a result, pixels exhibit significant correlations with their neighboring pixels. These correlations should be broken by a competent picture encryption scheme. Data correlation is defined mathematically by the formula, $Corr = \sum_{ij} \frac{(i - \mu i)\,(j - j)\,\rho\,(i,j)}{\sigma i \sigma j}$

Here µ, is the average value i.e., the mean and σ is the standard deviation calculated over the mean for any two data sequences i and j. The correlation value of two sequences i and j is near to one if their correlations are large aside from that, it’s close to zero. We examined the correlation between the cover frame and the embedded frame. The cover image has a correlation value of 1 and the stego image has a correlation value of 0. Hence, it can be stated that the suggested algorithm’s encrypted image has a very low correlation.

7 Analysis of Security and Attack Vulnerabilities

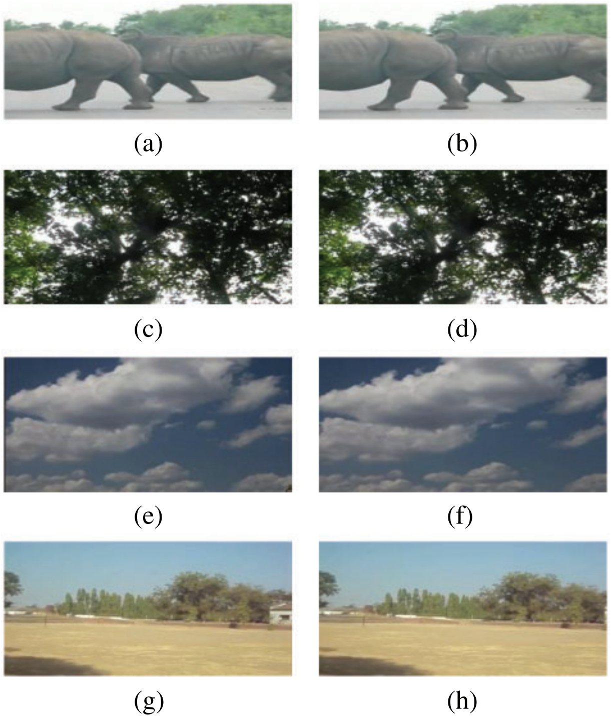
This algorithm’s resistance to plain text attack and man in the middle attack has also been evaluated.

7.1 Plain Text Attack

The first attack addressed is the Plain Text Attack. It is a relatively simple attack where the sender transmits data for encryption and the attacker may intercept portions of that plaintext. The key is also sent through a secure channel, hence the attacker never learns it. The attacker attempts to build the encryption technique utilized for the cipher text using some known cyphers and plaintext. This method is then used to decrypt the cipher text further. The proposed solution sends no plaintext across the network so only cipher text is sent. As key is never communicated over the network, this attack becomes very unlikely. Even if the attacker captures few frames, this attack is hard to execute since the text is encrypted and distributed in random pixels in complex frames throughout the video.

7.2 Man in the Middle Attack

A man in the middle attack is possible if the attacker can intercept the two parties' secret conversation. In this scenario, an attacker may intercept video transmission between the two parties, but the footage obtained will be encrypted. The encrypted data may be decoded only if both the key and the algorithm for encryption is well-known. As private key is being utilized in this scenario, it is very difficult to determine the key since the private key is never sent across a network. If the secret key is unknown, it becomes quite difficult for an unauthentic individual to retrieve the data that strengthens the suggested approach's security.


(a) (b)

(c) (d)

(e) (f)

(g) (h)

Figure 9: Original and stego images of frame 70 (a,b) rhinos (c,d) forest (e,f) sky and (g,h) school

8 Conclusion

This research introduces an improved method of video steganography by using a dual cover medium and a new frame selection algorithm. The dual cover medium consists of creation of fake DNA by embedding encrypted data in DNA using DNA cutting properties. This fake DNA is then embedded in selected frames of a cover video that are chosen using proposed frame selection algorithm involving scene change detection. After frame selection, the fake DNA is embedded in random pixel locations generated using linear congruence generator, burger chaotic map and RGB channel. The proposed technique has shown better results in terms of maintaining video perceptibility that reduces the every first chances of perception. Further, a high embedding efficiency, reduced MSE and reduced PSNR show the success of this technique in comparison with the techniques discussed. This paper proves that without an intelligent frame selection many embedding scheme fail to maintain video perceptibility giving the first signs of some abnormal activity in a video. Therefore a combination of an intelligent frame selection technique and improved embedding techniques we can transmit our steganographic videos securely over any communication medium.

Acknowledgement: Taif University Researchers Supporting Project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Funding Statement: Taif University Researchers Supporting Project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Kumar and K. Pooja, "Steganography-A data hiding technique," *International Journal of Computer Applications*, vol. 9, no. 7, pp. 19–23, 2010.

[2] N. Kar, K. Mandal and B. Bhattacharya, "Improved chaos-based video steganography using DNA alphabets," *ICT Express*, vol. 4, pp. 6–13, 2018.

[3] M. Ramalingam, "Stego machine–video steganography using modified LSB algorithm," *World Academy of Science, Engineering and Technology*, vol. 74, pp. 502–505, 2011.

[4] Y. Cao, H. Zhang, X. Zhao and H. Yu, "Video steganography based on optimized motion estimation perturbation," in *Proc. 3rd Association for Computing Machinery*, New York, NY, United States, pp. 25–31, 2015.

[5] Z. L. Yi and Z. W. Dong, "A novel steganography algorithm based on motion vector and matrix encoding," in *Proc. IEEE 3rd Int. Conf. on Communication Software and Networks*, Xian, China, pp. 406–409, 2011.

[6] H. M. Kelash, O. F. A. Wahab, O. A. Elshakankiry and H. S. El-sayed, "Hiding data in video sequences using steganography algorithms," in *Proc. Int. Conf. on ICT Convergence (ICTC)*, IEEE, Jeju, South Korea, pp. 353–358, 2013.

[7] P. Malathi, M. Manoaj, R. Manoj, V. Raghavan and R. E. Vinodhini, "Highly improved DNA based steganography," in *Proc. Computer Science, ICACC 2017*, Kochi, Kerala, India, vol. 115, pp. 651–659, 2017.

[8] Z. Wang, X. Zhao, H. Wang and G. Cui, "Information hiding based on DNA steganography," in *IEEE 4th Int. Conf. on Software Engineering and Service Science*, pp. 946–949, 2013.

[9] S. H. Jiao and R. Goutte, "Hiding data in DNA of living organisms," *Natural Science*, vol. 1, no. 3, pp. 181–184, 2009.

[10] M. R. Abbasy, P. Nikfard, A. Ordi and M. Torkaman, "DNA base data hiding algorithm," *International Journal of New Computer Architectures and their Applications (IJNCAA)*, vol. 1, pp. 183–193, 2012.

[11] I. Peterson, “Hiding in DNA,” in *Proc. of Muse*, pp. 22, 2001.

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

[13] R. Agrawal, M. Srivastava and A. Sharma, “Data hiding using dictionary based substitution method in DNA sequences,” in *Proc. 9th Int. Conf. on Industrial and Information Systems*, Tangier, Morocco, pp. 1–6, 2014.

[14] S. Mumthas and A. Lijiya, “Transform domain video steganography using RSA, random DNA encryption and huffman encoding,” in *Proc. Computer Science*, Cochin, India, vol. 115, pp. 660–666, 2017.

[15] A. Khalifa and A. Atito, “High-capacity DNA-based steganography,” in *8th Int. Conf. on Informatics and Systems (INFOS)*, Giza, Egypt, pp. 76, 2012.

[16] A. Jose and K. Subramaniam, “DNA based SHA512-ECC cryptography and CM-CSA based steganography for data security,” in *Proc. Materials Today*, 2020. https://doi.org/10.1016/j.matpr.2020.09.790.

[17] M. Fuad and F. Ernawan, “Video steganography based on DCT psychovisual and object motion,” *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 1015–1023, 2020.

[18] D. Arraziqi and E. S. Haq, “Optimization of video steganography with additional compression and encryption,” *Telkomnika*, vol. 17, no. 3, pp. 1417–1424, 2019.

[19] A. A. Hussein and O. Q. Jumah Al-Thahab, “Design and simulation a video steganography system by using FFTturbo code methods for copyrights application,” *Eastern-European Journal of Enterprise Technologies*, vol. 2, no. 9, pp. 104, 2020.

[20] J. Karmakar, A. Pathak, D. Nandi and M. K. Mandal, “Sparse representation based compressive video encryption using hyper-chaos and DNA coding,” *Digital Signal Processing*, vol. 117, pp. 103143, 2021.

[21] S. Rout and R. K. Mohapatra, “Video steganography using curvelet transform and elliptic curve cryptography,” in *Proc. 11th Int. Conf. on Computing Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, pp. 1–7, Jul. 2020.

[22] Z. S. Younus and G. T. Younus, “Video steganography using knight tour algorithm and LSB method for encrypted data,” *Journal of Intelligent Systems*, vol. 29, no. 1, pp. 1216–1225, Feb. 2019.

[23] I. P. Febin, K. Jayasree and P. T. Joy, “Violence detection in videos for an intelligent surveillance system using MoBSIFT and movement filtering algorithm,” *Pattern Analysis and Applications*, vol. 23, no. 2, pp. 611–623, May 2020.

[24] M. Suresh and I. S. Sam, “Optimized interesting region identification for video steganography using fractional grey wolf optimization along with multi-objective cost function,” *Journal of King Saud University-Computer and Information Sciences,* vol. 34, pp. S15319157820304456, 2020.

[25] S. Wan, X. Xu, T. Wang and Z. Gu, “An intelligent video analysis method for abnormal event detection in intelligent transportation systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4487–4495, Jul. 2021.

[26] C. Huang and H. Wang, “A novel key-frames selection framework for comprehensive video summarization,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 2, pp. 577–589, Feb. 2020.

[27] X. Zhang, W. Zhang, W. Sun, X. Sun and S. K. Jha, “A robust 3-D medical watermarking based on wavelet transform for data protection,” *Computer Systems Science and Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[28] X. Zhang, X. Sun, X. Sun, W. Sun and S. K. Jha, “Robust reversible audio watermarking scheme for telemedicine and privacy protection,” *Computers, Materials & Continua,* vol. 71, no. 2, pp. 3035–3050, 2022.

[29] B. Raju and P. K. Sathish, “Randomized pixel selection for concealing the AES encrypted text message inside a video file,” in *Computer Vision and Robotics,* Springer, Singapore, pp. 165–174, 2022.

[30] S. Biswas, S. R. Das and E. M. Petriu, “An adaptive compressed MPEG-2 video watermarking scheme,” *IEEE Transactions on Instrumentation and Measurement*, vol. 54, no. 5, pp. 1853–1861, 2005.