Multimedia Tools and Applications (2021) 80:13253–13270
https://doi.org/10.1007/s11042-020-10395-6

Exponential fractional cat swarm optimization for video steganography

Meenu Suresh[1] · I. Shatheesh Sam[2]

Received: 3 April 2020 / Revised: 14 October 2020 / Accepted: 22 December 2020 /
Published online: 14 January 2021

Abstract

In this paper, an effective method named Exponential Fractional-Cat Swarm Optimization (Exponential Fractional-CSO) along with multi-objective cost function is proposed. The proposed method is designed by integrating the CSO with the fractional concept based on the Exponential parameters. Initially, an input video is selected from the database from which frames are generated. Key frames are chosen among the frames using the contourlet transform and Structural Similarity Index Measure (SSIM). Regions are formed on the selected key frames through the help of grid lines. Once the regions are formed, optimal regions are ascertained with the help of the proposed optimization algorithm along with multi-objective cost functions to hide the secret data. During the embedding process, the secret data is hidden in the optimal region using the lifting wavelet transform (LWT). The embedded video is then transmitted through the network to reach its intended receiver. The experimental results reveal that the proposed Exponential Fractional-CSO obtained a maximal correlation of 0.9931 by considering the frames, maximal Peak Signal-to-Noise Ratio (PSNR) of 89.70 dB and MSE of 0.00006 respectively. Hence, the proposed method shows greater effectiveness of hiding the secret data in the video sequence along with data security.

Keywords Video steganography · Cat swarm optimization · Lifting wavelet transform · Fractional concept · Exponential parameters

✉ Meenu Suresh
meenupillai1988@gmail.com

I. Shatheesh Sam
shatheeshsam@yahoo.com

[1] Deparment of Computer Science, Nesamony Memorial Christian College, affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamil Nadu 627012, India

[2] Department of PG Computer Science, Nesamony Memorial Christian College, affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamil Nadu 627012, India

1 Introduction

Steganography is widely used in various fields, like information integrity certification, identity authentication, confidential communication, and digital copyright protection [13]. Video steganography is an important field of research in industrial as well as military applications, due to its size and memory requirements. It is a process of hiding the secret information inside the video or image such that the hidden data is only known to the sender and the receiver. Steganography otherwise referred to as data hiding is an effective method used to protect the privacy and security of digital information, as it embeds the secret message in the digital media. The digital media contains secret information, which has some meaningful form. Hence, the privacy and security of embedded secret data is guaranteed, which prevent the attention of attackers [22]. In the past decades, various steganography methods were developed in the digital multimedia. The digital media contains various files, such as image, text, and video [17]. Among these media types, video is the most popularly used embedding framework, due to its wide range of applications in storage device, internet, surveillance camera etc. To save the storage space, coding model is applied for compressing the video sequences, as the video sequences has large file size [24]. The steganographic system uses various multimedia objects, namely audio, video and image as cover medium. Based on the category of cover medium, the steganography is categorized into image, video, audio, protocol, and text steganography [38].

The steganography method uses discrete cosine transform (DCT) coefficients, as it is the major transformation domain used for compressing the video files in order to embed the secret data into video coding structure [5, 22, 28]. It is the process used for embedding the secret data into digital media, such as video, text, and image [9, 14, 30]. The key role of the steganography procedure is to maximize the imperceptibility for increasing the level of security while dealing with the high embedding capability. Among different types of cover media, the video file plays a major attention in the area of research, as it provides large capacity. The existing video steganography techniques are classified into two different types, namely re-encoding embedding, and distortion compensated embedding [34]. Due to high complexity of computational process, the above methods are not effective in performing the data hiding mechanism. The existing data embedding techniques uses video coding structure that includes motion vector [31], DCT coefficient, and prediction mode for embedding the secret data [16]. The DCT coefficients utilize lesser modification and low amount of distortions. The present steganography method also uses various optimization techniques to get the best possible results. The well-known methods are genetic algorithm (GA) [7], particle swarm optimization (PSO) [12], monarch butterfly optimization (MBO) [6], artificial bee colony (ABC) [11], grey wolf optimization (GWO) [27], fractional-grey wolf optimization (Fractional-GWO) [29] etc.

In this paper, a novel video steganography method to hide the secret data using the Exponential Fractional-CSO is proposed. The proposed optimization framework involves three different phases to hide the secret data in the video sequence, namely key frame extraction, optimal region selection, and embedding of the secret data. Firstly, the key frames are extracted from the input video, and then grid lines are formed on the extracted key frame. Then, to select the optimal region proposed Exponential Fractional-CSO algorithm, which is developed using the CSO with the fractional concepts based on the Exponential parameter is used. The proposed optimization framework considers the factors, such as intensity, edge, wavelet energy, LBP energy, kurtosis, and neighborhood information associated with the multi-objective cost function before hiding the secret data. Once, the optimal region is selected then the embedding process is achieved using LWT to get the embedded image. After embedding all the frames are combined together to get the stego-video which is then transmitted through the network to the intended receiver. Upon receiving, extraction of the secret data is done from the stego image with the help of original image and optimal region.

The significant contribution of the proposed work are summarized as follows,

- This scheme employs optimal region selection for hiding the secret data using Exponential Fractional-CSO algorithm.
- The embedding process is achieved using LWT approach which increases the complexity level of security.
- The secret data is hard to find as it’s embedded in an optimal region which is calculated from the fitness measure. After going through a series of hiding procedure the hidden data is not degraded and is imperceptible.
- The system is simple yet robust even if any attacks happens.

The organization of this research is explained as follows: Section 2 elaborates the existing steganography methods. Section 3 explains the proposed optimization framework, Section 4 describes the results and discussion of the proposed model, and conclusion of this paper is made in Section 5.

2 Literature survey

Liu et al. [15] modeled a robust steganography model based on secret sharing to embed the secret message. It increased the robustness in message hiding. It improved the quality of video and achieved better performance. However, this method obtained low survival rate. Xue et al. [37] presented a secure steganographic scheme using quantized DCT coefficients. Here, the const function was constructed using the block distortion, texture complexity and bit rate change of DCT block. However, this method failed because of security performance and embedding capacity. Jalali et al. [10] proposed a video sparse representation method. This method exhibited better invisibility, and was highly robust against various attacks. However, it failed to increase the embedding payload.

Chan et al. [4] proposed a hybrid method in which scene change analysis was used to embed the data and error correcting code is embedded as a watermark in the audio channel. In this approach, the compressed video is first decomposed into standard video format, embedding of the data is done in the video signal and finally the video is recompressed. The proposed method gave a good embedding capacity but takes a lot of computer processing time. Noda et al. [21] presented a video steganography algorithm employing bit-plane complexity segmentation (BPCS) and compressed video in wavelet domain. The DWT domain are used by two coding techniques namely, 3D set partitioning in hierarchical tress (SPIHT) and Motion-JPEG2000. The proposed technique gave a higher embedding payload however it is not sure that all types of cover-video will have enough of noise-like bit-plane regions. Moon et al. [20] proposed a new approach of video steganography algorithm for hiding secret data and for authentication computer forensic tool was used. The secret data prior to embedding using the LSB method is first encrypted and authenticated using a key. The secret data is hidden into the 4LSB of the cover frame of video. Since the method uses spatial domain it not robust against noise. Stanescu et.al [26] presented a video steganography algorithm called StegoStream which uses MPEG-2 video streams to embed the subtitle message without consuming any extra bandwidth. After the quantization process and when the predefined threshold T is reached, the bocks are selected for embedding the data. The secret subtitle message are embedded only in the I frames of the video stream blocks. However, this method failed as the video subtitle will not repeat continuously since for every one second the MPEG-2 video have 4–5 intra frames.

Wang et al. [35] developed a video steganography method based on Intra Prediction Mode (IPM) and effectively evaluated the probability distribution. It increased the performance of security but failed to increase the performance of coding efficiency. Younus et al. [39] introduced Knight Tour algorithm for video steganography. The secret message was encrypted using the mathematical equation such that the key specified was set of random numbers. It was highly reliable in terms of security, but failed to use the key for selecting the frames. In Song et al. [25] to avoid the difficulties of distortion drift, an improved scheme based on Multi-view coding (MVC) standard for 3D video was introduced. The selected coefficients of 4×4 Quantized Discrete Cosine Transforms (QDCT) is first modified and then the data are hidden into b4-frames thereby preventing distortion drift. The proposed method uses two random sequenced to maintain randomness. However, this method failed to ensure security of the hidden data.

Gurunathan et al. [8] presented a method named stegano-visual cryptography to embed the secret data within an input image. The cover image is splitted into $n$blocks of 8×8pixels and the secret data into n partitions to enhance the embedding capacity and quality of stego image. For finding an optimum result, Cuckoo Search (CS) optimization technique was employed. It helps to detect the best substitution matrix which change protected data into whole block but failed to find single optimum matrix for substitution. Banharnsakun et al. [2] proposed a LSB based image steganography which is enhanced with the help of an Artificial Bee Colony (ABC). To embed the confidential image inside an input image, the block is optimized by ABC. The ABC algorithm is updated using a using a block assignment list is also presented in this. Though, there was no improvement in the embedding capacity. Miri et al. [18] proposed to map the cover image to a frequency domain, adaptive wavelet transform and GA. Based on Kieu and Chang model, the encrypted data is embedded in the edges of the image by which there is least difference in the cover image. Still, this method did not much concentrate on the improving the time complexity.

The detailed study conveyed that the above issues affected the video quality and security level of the hidden data. To overcome these issues, a new model of data hiding using Exponential Fractional-CSO method to achieve improved video quality and security level is proposed.

3 Proposed exponential fractional-CSO for video steganography

The main objective of developing the video steganography algorithm is to find the optimal region for embedding the secret data into the cover image thereby improving the video quality and offering the best security to the secret data. The proposed scheme benefits from the goodness of the Exponential Fractional-CSO along with multi-objective cost function. Initially, an input video is selected from the database, and the key frames are effectively extracted by applying contourlet transform and SSIM measure. After extracting the key frame, regions are formed through the aid of grid lines. Then, optimal regions are selected with the help of proposed optimization algorithm based on the multi-objective factors, like intensity, edge, wavelet energy, LBP energy, kurtosis, and neighborhood information. The proposed Exponential Fractional-CSO algorithm is designed by incorporating the fractional concept with the CSO based on the Exponential concept. Once, the optimal region is selected, the secret data is embedded in the optimal location with the help of LWT which is an effective transform model to hide the secret data. Figure 1 portrays the schematic diagram of the proposed Exponential Fractional-CSO for video steganography.

3.1 Extracting key frames from the input video

The input video B_i is selected from the database in order to perform the key frame extraction process. The key frame extraction process is simple and is effective for summarizing the long video sequence. The key frames represent the salient information of a video shot and they are effectively extracted within a specified shot. The key frame extraction process reduces the hiding complexity in video by concentrating more on the particular frames. For extracting key frames, the input video is divided into various frames and the difference between each frames is calculated and finally, the key frames used for embedding process is extracted. The key frame that is extracted is represented as,

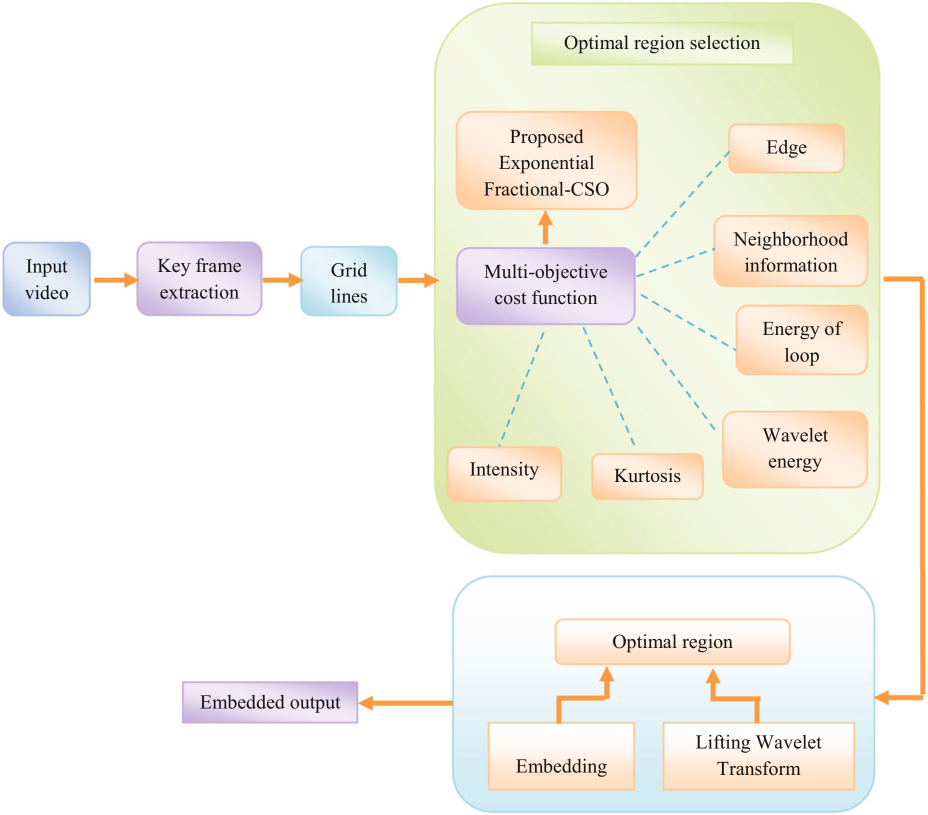


Fig. 1 Schematic diagram of the proposed Exponential Fractional-CSO for video steganography

$$FK = \{FK_1, FK_2, \ldots FK_i, \ldots FK_n\} \tag{1}$$

where, FK denotes the key frame, FK_n represents the number of key frames, and FK_i indicates the i^{th} key frame, respectively.

3.2 Optimal region selection using the proposed exponential fractional-CSO

Once the key frames are extracted, the next step is the formation of grid lines on the specific key frames. The grid lines are formed on the extracted key frame in order to detect optimal region for hiding the secret data. Once the grid lines are formed, the region used to hide the secret data is selected using the proposed Exponential Fractional-CSO which is designed by incorporating the CSO [1] with the fractional concept [3] based on the Exponential parameter.

The selection of optimal region enables the proposed model to hide the secret data more effectively in such a way that the secret data is not visible to the third party. The optimal region selection is done using the proposed method along with multi-objective cost function, which is formed using the factors, like intensity, edge, wavelet energy, LBP energy, kurtosis, and neighborhood information. These functions are associated together to model the fitness function, which in turn is used to obtain the optimal result.

3.2.1 Solution encoding

Solution encoding is used to represent the grids for selecting the optimal region to hide the secret data. It specifies the solution vector, which comprises of $v$number of regions. The dimension of solution vector is specified as $[1 \times h]$ which indicates the total number of regions used to embed the secret data, where h takes the value 9. Figure 2 portrays the solution vector.

3.2.2 Fitness function

The fitness of the selected regions are computed using the multi-objective cost function factors like intensity, edge, LBP energy, kurtosis, neighborhood information, and wavelet energy. The fitness function is evaluated using the below Equation as,

$$F = A + (1-T) + (1-D) + E + L + P \tag{2}$$

where, Arepresents the wavelet energy, T specifies the intensity of pixels, D represents the edge, E denotes the energy of loop, L represents the kurtosis, and P indicates the average of pixels in the neighborhood information. The wavelet energy is represented as,

$$A = \frac{1}{h} \sum_{m=1}^{h} \lambda(G_m) \tag{3}$$

where, G_m represents the image corresponding to m^{th} region and the entropies of m are averaged to calculate the wavelet energy. To calculate the intensity, the intensity difference between the pixels of a block is done which is represented as,

1	2	………	h

Fig. 2 Solution encoding

$$T = \frac{1}{h \times R \times S} \sum_{m=1}^{h} \sum_{q=1}^{R} \left[\sum_{r=1}^{S} G_m^q - G_m^{q,r} \right] \tag{4}$$

where, R denotes the total number of pixels at m^{th} region, and S specifies the total number of neighbors. The intensity of q^{th} pixel at m^{th} region is represented as G_m^q, and $G_m^{q,r}$ specifies the intensity of r^{th} neighboring pixel with respect to q^{th} pixel of the m^{th} block. The edge of the block is calculated as,

$$D = \frac{1}{h \times R} \sum_{m=1}^{h} \sum_{q=1}^{R} D_{m,q} \tag{5}$$

The edge of pixel is denoted as $D_{m,\ q}$ such that the value of $D_{m,\ q}$ is one in case of edge pixel. The energy of the loop is calculated for each region by fixing the center pixel in the block. The difference between the center and the neighboring pixel is computed in such a way that if the difference is greater than or equal to zero, then the pixel value is updated by one otherwise the value is specified as zero. The energy of the loop is calculated as,

$$E = \frac{1}{h} \sum_{m=1}^{h} \lambda[J(G_m)] \tag{6}$$

where, $\lambda[J(G_m)]$ represents the entropy of the image corresponding to m^{th} region. The kurtosis of loop corresponding to the m^{th} region is calculated as,

$$L = \frac{1}{h} \sum_{m=1}^{h} \beta(G_m(q,z)) \tag{7}$$

where, the term $\beta(G_m(q, z))$ denotes the kurtosis of loop corresponding to m^{th} region such that $G_m(q, z)$ is represented as,

$$G_m(q,z) = \sum_{m=0}^{h} a(b_m - b_v).2^m \tag{8}$$

The condition used to specify the factor $a()$ is represented as,

$$a(\alpha) = \begin{cases} 1 & if \propto \geq 0 \\ 0 & otherwise \end{cases}$$

The average of pixels present in the neighborhood information is represented as,

$$P = \frac{1}{h} \sum_{m=1}^{h} T \tag{9}$$

where, T represents the intensity. The fitness value of intensity and edge should be minimal and in order to afford maximum value, the intensity and the edge factors are subtracted from one.

3.2.3 Proposed exponential fractional-CSO

The CSO algorithm is integrated with the fractional concept based on the Exponential parameter in order to design the proposed Exponential Fractional-CSO for embedding the secret data. The CSO algorithm operates using the behavioral characteristics of cats. The cat uses two modes in order to chase the prey, namely the tracing mode and seeking mode. In seeking mode, the cats take rest for a long time but with curiosity and high degree of alertness of the objects moving around them and in tracing mode it moves around to chase the prey. Based on these two modes, global solution is obtained for embedding the secret data. As, the cats spend less time for tracing, there exist minimum number of cats in this subgroup such that the number are defined using the mixture ratio (MR).

Once, the cats are sorted in any of the two modes, the best solution is derived and saved based on their position and fitness. The steps are repeated until a stopping criterion is attained. Thus, based on factor such as Self-Position Considering (SPC), Seeking Memory Pool (SMP) and Seeking Range of the selected Dimension (SRD) decides between the modes through which the position of the cats is updated. The algorithmic steps involved in the proposed Exponential Fractional-CSO are discussed as follows:

Initialization Let us consider N number of cats in the Z^{th} dimensional search space and the solution is represented as Y.

Evaluating the fitness The fitness of each solution is evaluated using Eq. (2) and the results are organized in ascending order with the maximal value of fitness. Finally, the function with the best fitness measure is declared as the optimal solution.

Position update of search agents The cats update their position either in the tracing mode or in the seeking mode. The cats engaged in the seeking mode update their position using the below Equation as,

$$Y^{x+1} = (1 \pm O \times w) \times Y^x \tag{10}$$

where, Y^{x+1} represents the location of cat in the current iteration, Y^x indicates the location of cat in the previous iteration,$w$represents a random number and O denotes the Seeking Range of the selected Dimension (SRD) factor. The location of cat in the tracing mode is represented as,

$$Y^{x+1} = Y^x + g^{x+1} \tag{11}$$

Here, Y^x denotes the position of cat at x^{th} iteration and g^{x+1} denotes the velocity of cat in the current iteration. By substituting the velocity g^{x+1} in the above Equation we get.

$$Y^{x+1} = Y^x + g^x + w_1 \times s_1 \times Y^{bst} - w_1 \times s_1 \times Y^x \tag{12}$$

By integrating the fractional concept with the CSO algorithm, the above Equation is modified as,

$$g^{\mu}\left(Y^{x+1}\right) = g^x + w_1 \times s_1 \times Y^{bst} - w_1 \times s_1 \times Y^x \tag{13}$$

$$\begin{aligned} Y^{x+1} = {} & \mu.Y^x + \frac{1}{2}(1-\mu)Y^{x-2} + \frac{1}{6}(1-\mu)Y^{x-2} + \frac{1}{24}\mu(1-\mu)(2-\mu)Y^{x-3} + g^x + w_1 \times s_1 \\ & \times Y^{bst} - w_1 \times s_1 \times Y^x \end{aligned} \tag{14}$$

With the concept of Exponential Weighted Moving Average (EWMA), the term Y_d^x is represented as,

$$Y^x = \frac{Y_d^x - (1-\delta)Y_d^{x-1}}{\delta} \tag{15}$$

By substituting the above in Eq. (14), the resultant Equation is expressed as,

$$Y^{x+1} = \frac{\mu.Y_d^x}{\delta} -.\frac{\mu(1-\delta)Y_d^{x-1}}{\delta} + \frac{1}{2}(1-\mu)Y^{x-2} + \frac{1}{6}(1-\mu)Y^{x-2} + \frac{1}{24}\mu(1-\mu)(2-\mu)Y^{x-3} + g^x + w_1 \times s_1 \times Y^{bst} - \frac{w_1 s_1 Y_d^x}{\delta} -.\frac{w_1 s_1 (1-\delta)Y_d^{x-1}}{\delta} \tag{16}$$

The final updated equation for the proposed Exponential Fractional-CSO is presented in Eq. (16). The cat updates its position based on the position from the previous iterations Y^x,Y^{x-1},Y^{x-2} and Y^{x-3}, random numberw_1, a constant s_1, fractional constant μ, and the parameter δvaries from$0 < \delta \leq 1$.

Termination The above steps are repeated until an optimal solution is obtained or till it meets a condition criteria. The pseudo code of the proposed Exponential Fractional-CSO is explained below.

```
Input  :  Cat population, $Y$ with $N$ solutions.
Output :  Global optimal solution, $Y^*$
Begin
    Initialization
    While $(x < x_{\max})$
      Compute the fitness of the solutions and rank them
      Conclude the best solution
        For $(x < x_{\max})$
          If $(SPC = 1)$
          {
              Update the position of cat in the seeking mode using Eq. (10)
              else
              Update the location of cat in the tracing mode using Eq. (16)
          End If
        End For
      End While
Terminate
```

Pseudo code of the proposed Exponential Fractional-CSO

3.3 Embedding the secret data using lifting wavelet transform

Once the optimal region is identified using the proposed Exponential Fractional-CSO, then the embedding process to hide the secret data is carried out in the embedding phase to provide higher degree of security during data transmission. The secret data is embedded using the LWT, as it offers fast computation than the existing wavelet transforms. The cover image or the video frame $W_i$is used to embed the secret data with dimension of$[U \times V]$. Firstly, the image W_i is decomposed using LWT, which generates bands, such as LL, LH, HL, and HH that provides enhanced edge details of the image. The application of LWT to image W_i is composed of two levels of decomposition. The first level of decomposition is specified as,

$$\{LL, LH, HL, HH\} = K(W_i) \tag{17}$$

The lifting wavelet transform is denoted by K and $\{LL, LH, HL, HH\}$ denotes the wavelet coefficients of frame. The size of the individual bands are denoted as $\left(\frac{U}{2} \times \frac{V}{2}\right)$. Each bands of the image W_i is further send for second level of decomposition which generates 16 sub-bands, which are represented as,

$$\{LL_1, LH_1, HL_1, HH_1\} = K(LL) \tag{18}$$

$$\{LL_2, LH_2, HL_2, HH_2\} = K(LH) \tag{19}$$

$$\{LL_3, LH_3, HL_3, HH_3\} = K(HL) \tag{20}$$

$$\{LL_4, LH_4, HL_4, HH_4\} = K(HH) \tag{21}$$

The size of sub-bands from Eq. (18 to 21) is denoted as $\left(\frac{U}{4} \times \frac{V}{4}\right)$. In this research, the wavelet coefficients *LL* and *HH* are used to embed the secret data. The embedding process is specified as,

$$X_t(u, y) = W_t(u, y) + l{*}Z_j(u, y); selected\ optimal\ region \tag{22}$$

where, t and j denotes the total wavelet bands and it values ranges from 1 to 8. The watermarked image is $X_t\,(u, y)$, $W_t(u, y)$ denotes the lifting wavelet sub bands, $Z_j(u, y)$ indicates the secret data, and $l$denotes the embedding strength.

3.4 Inverse wavelet transform

Once, we get the embedded image from the previous step then inverse lifting wavelet transform is applied which helps in getting the original embedded image wherein the secret data is concealed. It also involves two levels of decomposition which is applied on the embedded image. The first level of decomposition is given as,

$$IDWT(X_t(u, v)) = B(u, v) = \{LL^{\bullet}, LH^{\bullet}, HL^{\bullet}, HH^{\bullet}\} \tag{23}$$

where, $IDWT(X_t(u, v)$ represents the inverse lifting wavelet transform of the embedded image. Then, the second level of decomposition follows and the outcome is denoted as $B^*\,(u, v)$, which is referred to as the stego image. All the frames along with the stego image frames are then combined together to get the stego-video.

3.5 Retrieval of secret data from the stego-video

The stego-video is then forwarded to the receiver through network for extracting the secret data. At the receiver end, the secret data can be retrieved using the original cover video, optimal regions and the embedded image. The lifting wavelet transform is applied to extract the secret data and the receiver extracts it from the optimal region. The process of extraction is represented as,

$$M(u,y) = W_t^*(u,y) - W_t(u,y) \tag{24}$$

Here, $M(u,y)$ represents the retrieved secret data.

The impact of video steganography developed in this paper gives robust data hiding, ensures perception quality and security of the data.

4 Results and discussion

4.1 Experimental setup

The performance of the proposed method is verified using two input videos taken from [32, 36] along with a manually generated secret data. The experimental work is implemented in MATLAB R2015a, Intel Core i7, CPU @2.60 GHz, 8GB RAM under the Windows 10 operating system.

4.2 Evaluation metrics

The assessment of the proposed system is done using different metrics like correlation, PSNR and MSE which is described in detail as follows:

4.2.1 Correlation

It specifies the relation which exists among the original frames and the embedded video frames, represented as,

$$\Re = \frac{M(\kappa,\lambda)}{\varpi_\kappa \varpi_\lambda} \tag{25}$$

where, ϖ_κ and ϖ_λ specifies the standard deviation of κ and λ, and M (κ,λ) denotes the covariance of κ and λ.

4.2.2 MSE

It specifies the error between the original video and the stego-video and is calculated as,

$$Ms = \frac{1}{No} \sum (W_t(u,y) - X_t(u,y))^2 \tag{26}$$

where, $W_t(u,y)$ specifies the original value, and $X_t(u,y)$ denotes the embedded pixels.

4.2.3 PSNR

It specifies the quality of embedded image that is calculated using embedded frames and the cover frames of video. However, the PSNR is expressed as,

$$P_s = 20\log_{10}\frac{W_{\max} \times \hbar \times \ell}{Ms} \tag{27}$$

where, $W_{\max}$ indicates the maximal energy with the size of image as $\hbar$ and ℓ and Ms is the MSE.

4.3 Comparative methods

The proposed approach is compared with the conventional methods, like Particle Swarm Optimization (PSO) [19], Multi-Objective Cat Swarm Optimization (MOCSO) [23] and Wavelet [33] to show the performance improvement.

4.4 Comparative analysis

This section describes the comparative analysis of the proposed Exponential Fractional-CSO with the existing methods based on various metrics.

4.4.1 Analysis based on correlation using video 1

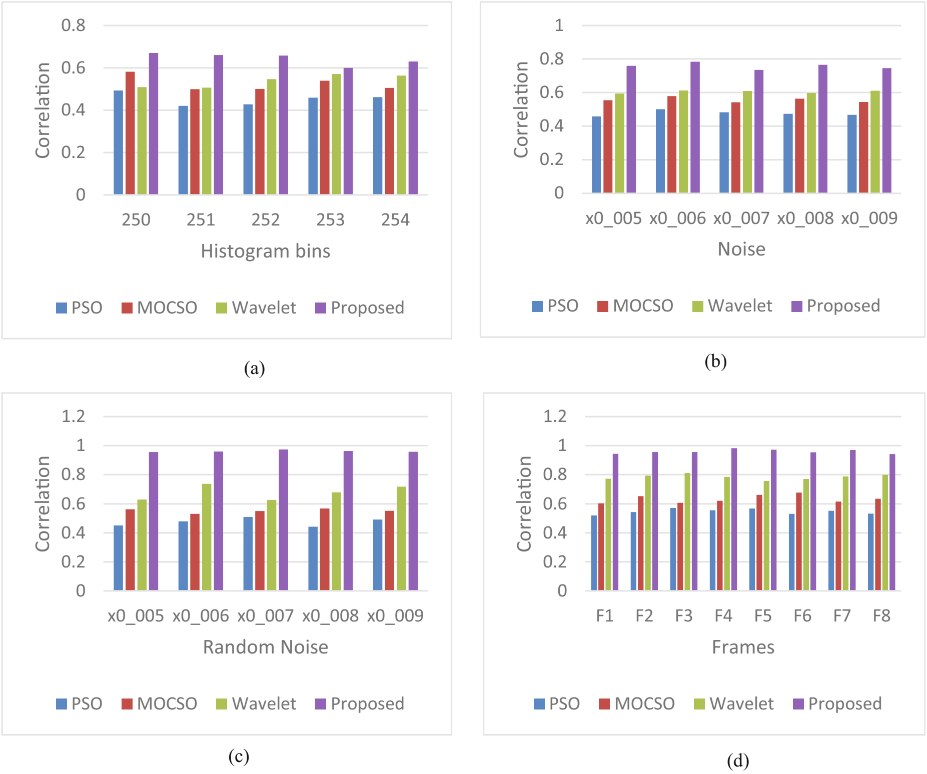
The above section presents the comparative analysis of the proposed Exponential Fractional-CSO method with the existing methods using video 1 in terms of frames, noise, random noise, and histogram respectively. When the histogram bins is 252, the methods, PSO, MOCSO, Wavelet and the proposed method acquired correlation of 0.4281, 0.5005, 0.5461, and 0.6579 respectively. It is clear from Fig. 3(a) that the proposed method rendered an accurate embedding through better security of the secret data.

When the noise level is 7×10^{-3} the methods, PSO, MOCSO, Wavelet and the proposed attained correlation of 0.4833, 0.5429, 0.6091 and 0.7356, respectively. Although the correlation declines with increase in noise levels, the proposed method acquired a higher value of correlation compared to other existing methods which is depicted in Fig. 3(b). When the random noise level is 7×10^{-3} the methods acquired correlation of 0.5091, 0.5501, 0.6249, and 0.9745, respectively as shown in Fig. 3(c). When the fourth frame is considered, the methods gained correlation of 0.5542, 0.6203, 0.7856and 0.9834 respectively. The analysis reveal that the proposed method acquired a higher correlation as portrayed in Fig. 3(d).

4.4.2 Analysis based on correlation using video 2

The comparative analysis using video 2 in terms of histogram, noise, random noise, and frames respectively are illustrated in this section. When the histogram bins is 252, the methods, PSO, MOCSO, Wavelet and the proposed method acquired correlation of 0.4244, 0.5289, 0.5421, and 0.6881 respectively. It is quite clear from Fig. 4(a) that the proposed method provided an accurate embedding through better security of the secret data.

When the noise level is 7×10^{-3} the methods, PSO, MOCSO, Wavelet and the proposed attained correlation of 0.4668, 0.5449, 0.6213 and 0.7845, respectively. Although the correlation declines with increase in noise levels, the proposed method acquired a higher value of correlation compared to other existing methods which is represented in Fig. 4(b). When the random noise level is 7×10^{-3} the methods acquired correlation of 0.5835, 0.6456, 0.7148, and 0.9914, respectively as shown in Fig. 4(c). When the fourth frame is considered, the methods



(a)

(b)

(c)

(d)

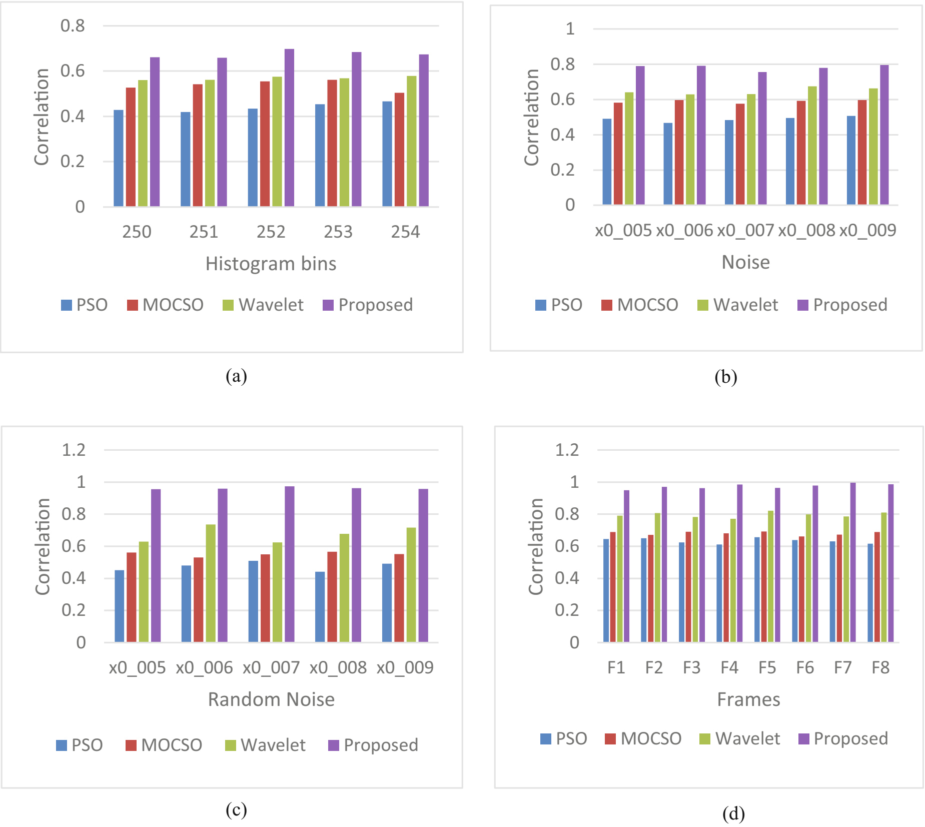
Fig. 3 Results of video steganography with video 1 based on Correlation, (**a**), varying histogram bins, (**b**) varying salt and pepper noise, (**c**) varying random noise, (**d**) varying the number of frames

gained correlation of 0.6109, 0.6818, 0.7713, and 0.9854 respectively. The analysis reveal that the proposed method acquired a higher correlation as portrayed in Fig. 4(d).

4.4.3 Analysis based on correlation using video 3

The comparative analysis in terms of histogram, noise, random noise, and frames respectively using video 3 are explained in this section. When the histogram bins is 252, the methods, PSO, MOCSO, Wavelet and the proposed method acquired correlation of 0.4344, 0.5548, 0.5752, and 0.6981 respectively. It is quite evident from Fig. 5(a) that the proposed method provided a precise embedding through better security of the secret data. When the noise level is 7×10^{-3} the methods, PSO, MOCSO, Wavelet and the proposed attained correlation of 0.4832, 0.5759, 0.6313 and 0.7567, respectively which is represented in Fig. 5(b).

When the random noise level is 7×10^{-3} the methods acquired correlation of 0.5935, 0.6634, 0.7394, and 0.9974, respectively as shown in Fig. 5(c). When the fourth frame is considered, the methods gained correlation of 0.6209, 0.6918, 0.7934, and 0.9754 respectively. The analysis reveal that the proposed method acquired a higher correlation as portrayed in Fig. 5(d).



(a)

(b)

(c)

(d)

Fig. 4 Results with video 2 based on Correlation, (**a**), varying histogram bins, (**b**) varying salt and pepper noise, (**c**) varying random noise, (**d**) varying the number of frames

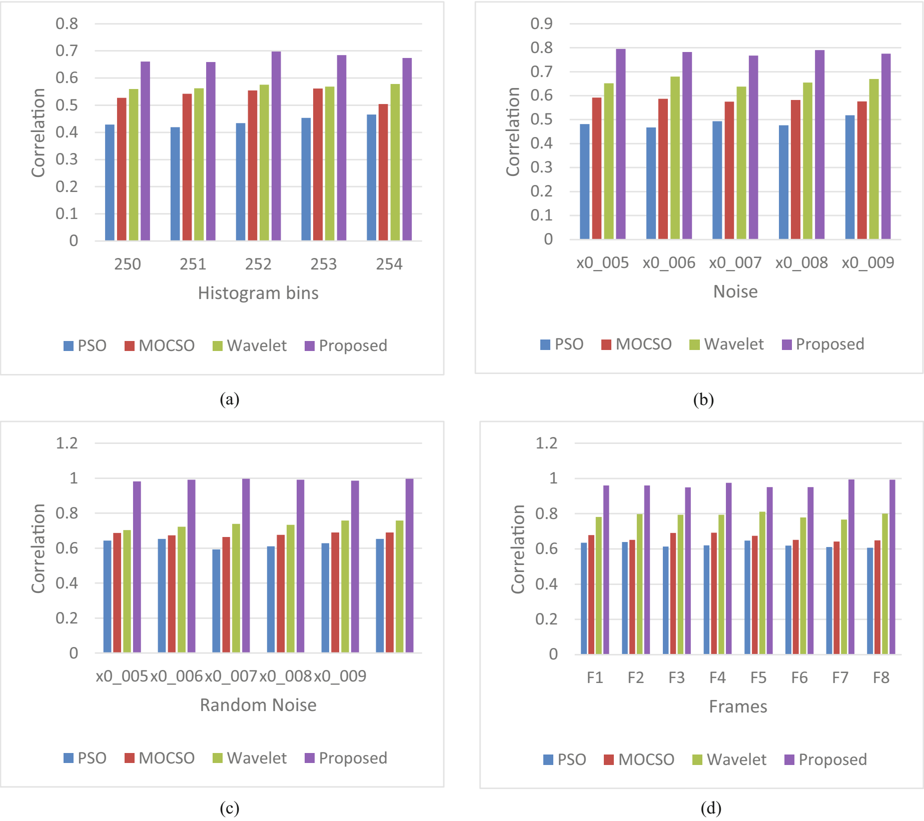
4.4.4 Analysis based on correlation using video 4

The comparative analysis in terms of histogram, noise, random noise, and frames respectively using video 4 are explained in this section. When the histogram bins is 252, the methods, PSO, MOCSO, Wavelet and the proposed method acquired correlation of 0.4549, 0.5481, 0.56521, and 0.6881 respectively. It is quite evident from Fig. 6(a) that the proposed method provided a precise embedding through better security of the secret data.

When the noise level is 7×10^{-3} the methods, PSO, MOCSO, Wavelet and the proposed attained correlation of 0.5078, 0.5629, 0.6591 and 0.7563, respectively which is represented in Fig. 6(b)**.** When the random noise level is 7×10^{-3} the methods acquired correlation of 0.5181, 0.5201, 0.7242, and 0.9785, respectively as shown in Fig. 6(c). When the fourth frame is considered, the methods gained correlation of 0.5934, 0.6956, 0.8156, and 0.9889 respectively. The analysis reveal that the proposed method acquired a higher correlation as portrayed in Fig. 6(d).

4.4.5 Analysis based on PSNR and MSE

This section portrays the analysis based on the PSNR and MSE values of the proposed method with the existing work. The PSNR using video 1 for the methods PSO, MOCSO, Wavelet and



(a)

(b)

(c)

(d)

Fig. 5 Results using video 3 based on Correlation, (**a**), varying histogram bins, (**b**) varying salt and pepper noise, (**c**) varying random noise, (**d**) varying the number of frames

the proposed method is 53.233, 61.504, 71.931, and 84.176, respectively. The MSE for the methods are 0.30887, 0.04599, 0.00416, and 0.00024. Likewise, the PSNR and MSE values for video 2, video 3, and video 4 is illustrated in Table 1. It is quite evident that the proposed Exponential Fractional-CSO method acquired maximal PSNR with much lesser MSE values compared to the existing methods.

4.4.6 Analysis based on computational complexity

It is clear from Table 2 that the proposed method achieves low computational complexity than the other existing methods.

5 Conclusion

In this paper, an effective method named Exponential Fractional-CSO is developed to hide the secret data in the video sequence. The proposed steganography process involves three different phase, such as key frame extraction, formation of grid lines, and optimal region selection to hide the secret data in the video sequence. Initially, the input video is collected from the

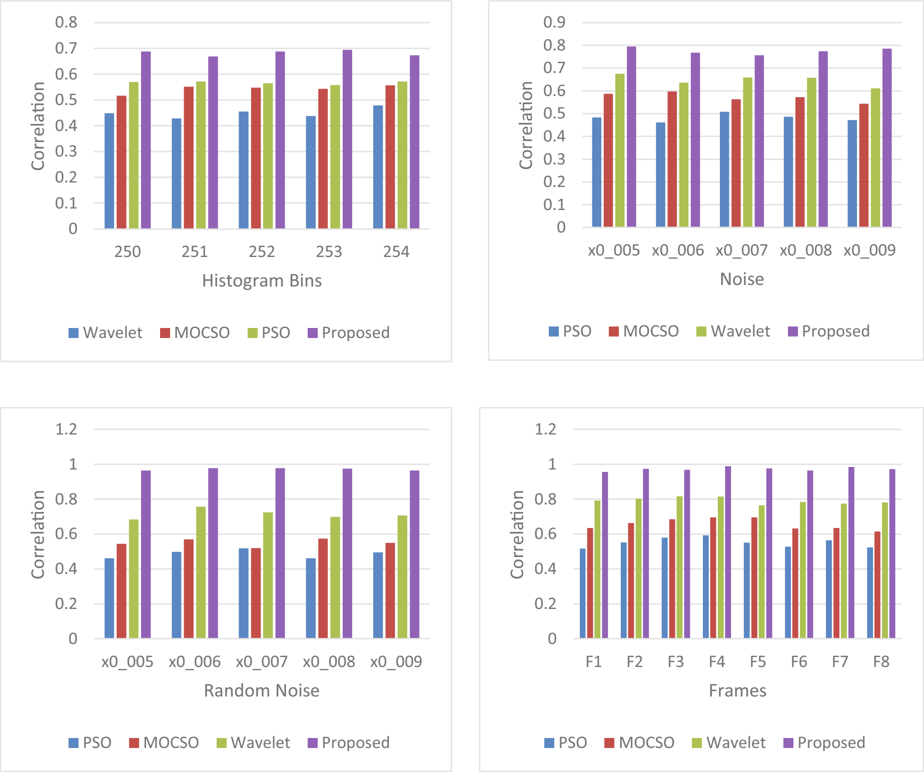


Fig. 6 Results using video 4 based on Correlation, (**a**), varying histogram bins, (**b**) varying salt and pepper noise, (**c**) varying random noise, (**d**) varying the number of frames

Table 1 Comparative discussion based on PSNR and MSE

Metrics/Methods		PSO	MOCSO	Wavelet	Proposed
Video 1	MSE	0.30887	0.04599	0.00416	**0.00024**
	PSNR (dB)	53.233	61.504	71.931	**84.176**
Video 2	MSE	0.09586	0.01873	0.00113	**0.00006**
	PSNR (dB)	58.142	65.233	77.490	**89.700**
Video 3	MSE	0.37981	0.03364	0.00266	**0.00018**
	PSNR (dB)	52.335	62.861	73.872	**85.382**
Video 4	MSE	0.15786	0.02277	0.001732	**0.00011**
	PSNR (dB)	55.976	64.384	75.572	**87.563**

Table 2 Computational complexity of proposed method along with conventional methods

Methods	Embedding time (s)	Extraction time (s)	Complete computational complexity (s)
Proposed	0.7901	0.2012	0.9913
Wavelet	1.1868	0.4638	1.6506
MOCSO	1.2653	0.4822	1.7475
PSO	1.2911	0.4894	1.7805

database and the key frames are retrieved from the input video. After extracting the key frames, the optimal region used to hide the secret data is selected through the grid lines. The selection of optimal region is carried out using the proposed Exponential Fractional-CSO, which is designed by integrating the CSO with the fractional concept using the exponential parameter. The optimal solution is evaluated using the fitness measure, which in turn uses the multi-objective cost function based on the constraints, like intensity, edge, wavelet energy, LBP energy, kurtosis, and neighborhood information. After determining the optimal region, the embedding process is achieved to hide the secret data using the lifting wavelet transform. The proposed Exponential Fractional-CSO obtained maximal correlation of 0.9931 by considering the frames, maximal PSNR of 89.70 dB, and MSE of 0.00006 respectively. In future, the performance of the video steganography process can be increased using different optimization model and also by encrypting the secret data prior to embedding.

References

1. Bahrami M, Bozorg-Haddad O, Chu X (2018) Cat swarm optimization (CSO) algorithm. In: Bozorg-Haddad O (ed) Advanced optimization by nature-inspired algorithms. Springer Singapore, Singapore, pp 9–18
2. Banharnsakun A (2018) Artificial bee colony approach for enhancing LSB based image steganography. Multimed Tools Appl 77:27491–27504. https://doi.org/10.1007/s11042-018-5933-5
3. Bhaladhare PR, Jinwala DC (2014) A clustering approach for the l -diversity model in privacy preserving data mining using fractional calculus-bacterial foraging optimization algorithm. Adv Comput Eng 2014:1–12. https://doi.org/10.1155/2014/396529
4. Chan PW, Lyu MR, Chin RT (2005) A novel scheme for hybrid digital video watermarking: approach, evaluation and experimentation. IEEE Trans Circuits Syst Video Technol 15:1638–1649. https://doi.org/10.1109/TCSVT.2005.856932
5. Chandel B, Jain DS (2016) Video steganography: a survey. 7
6. Feng Y, Wang G-G, Deb S et al (2017) Solving 0–1 knapsack problem by a novel binary monarch butterfly optimization. Neural Comput & Applic 28:1619–1634. https://doi.org/10.1007/s00521-015-2135-1
7. Goldberg DE, HOLLAND JH (1998) Genetic algorithms and machine learning. Kluwer Academic Publishers
8. Gurunathan K, Rajagopalan SP (2020) A stegano - visual cryptography technique for multimedia security. Multimed Tools Appl 79:3893–3911. https://doi.org/10.1007/s11042-019-7471-1
9. Hussain M, Wahab AWA, Idris YIB et al (2018) Image steganography in spatial domain: A survey. Signal Processing: Image Communication 65:46–66. https://doi.org/10.1016/j.image.2018.03.012
10. Jalali A, Farsi H (2019) A new steganography algorithm based on video sparse representation. Multimed Tools Appl. https://doi.org/10.1007/s11042-019-08233-5
11. Karaboga D, Basturk B (2007) A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm. J Glob Optim 39:459–471. https://doi.org/10.1007/s10898-007-9149-x
12. Kennedy J, Eberhart R (1995) Particle swarm optimization. In: paper presented at the proceeding of the IEEE international conference on neural networks, Perth, Australia, 27 November–1 December
13. Khadam U, Iqbal MM, Alruily M et al (2020) Text data security and privacy in the internet of things: threats, challenges, and future directions. Wirel. Commun. Mob. Comput. 2020:1–15. https://doi.org/10.1155/2020/7105625
14. Li Y, Wang H-X (2019) Robust H.264/AVC video watermarking without intra distortion drift. Multimed Tools Appl 78:8535–8557. https://doi.org/10.1007/s11042-018-6942-0
15. Liu S, Xu D (2020) A robust steganography method for HEVC based on secret sharing. Cogn. Syst. Res. 59:207–220. https://doi.org/10.1016/j.cogsys.2019.09.008
16. Liu Y, Li Z, Ma X (2012) Reversible data hiding scheme based On H.264/AVC without distortion drift. JSW 7:1059–1065. https://doi.org/10.4304/jsw.7.5.1059-1065
17. Liu S, Bai W, Liu G et al (2018) Parallel fractal compression method for big video data. Complexity 2018:1–16. https://doi.org/10.1155/2018/2016976

18. Miri A, Faez K (2017) Adaptive image steganography based on transform domain via genetic algorithm. Optik 145:158–168. https://doi.org/10.1016/j.ijleo.2017.07.043
19. Montes de Oca MA, Stutzle T, Birattari M, Dorigo M (2009) Frankenstein's PSO: a composite particle swarm optimization algorithm. IEEE Trans Evol Computat 13:1120–1132. https://doi.org/10.1109/TEVC.2009.2021465
20. Moon SK, Raut RD (2013) Analysis of secured video steganography using computer forensics technique for enhance data security. In: 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013). IEEE, Shimla, India, pp 660–665
21. Noda H, Furuta T, Niimi M, Kawaguchi E (2004) Application of BPCS steganography to wavelet compressed video. In: 2004 International Conference on Image Processing, 2004. ICIP '04. IEEE, Singapore, pp 2147–2150
22. Noorkami M, Mersereau RM (2007) A framework for robust watermarking of H.264-encoded video with controllable detection performance. IEEE Trans Inform Forensic Secur 2:14–23. https://doi.org/10.1109/TIFS.2006.890306
23. Pradhan PM, Panda G (2012) Solving multiobjective problems using cat swarm optimization. Expert Syst. Appl. 39:2956–2964. https://doi.org/10.1016/j.eswa.2011.08.157
24. Shanableh T (2012) Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering. IEEE Trans Inform Forensic Secur 7:455–464. https://doi.org/10.1109/TIFS.2011.2177087
25. Song GH, Liu H (2020) An improved high capacity and efficient data hiding scheme for 3d videos without distortion drift. IEEE Access 8:143464–143478. https://doi.org/10.1109/ACCESS.2020.3013033
26. Stanescu D, Stratulat M, Ciubotaru B et al (2007) Embedding data in video stream using steganography. In: 2007 4th International Symposium on Applied Computational Intelligence and Informatics. IEEE, Timisoara, Romania, pp 241–244
27. Suresh M, Sam IS (2020) Optimal wavelet transform using Oppositional Grey Wolf Optimization for video steganography. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-09330-6
28. Suresh M, Shatheesh Sam I (2018) High secure video steganography based on shuffling of data on Least significant DCT coefficients. In: 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, Madurai, India, pp 877–882
29. Suresh M, Shatheesh Sam I (2020) 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 S1319157820304456. https://doi.org/10.1016/j.jksuci.2020.08.007
30. Tew Y, Wong K (2014) An Overview of Information Hiding in H.264/AVC Compressed Video. IEEE Trans Circuits Syst Video Technol 24:305–319. https://doi.org/10.1109/TCSVT.2013.2276710
31. Tsai Y-S, Tsai P (2011) Adaptive data hiding for vector quantization images based on overlapping codeword clustering. Inf. Sci. 181:3188–3198. https://doi.org/10.1016/j.ins.2011.03.017
32. Video Watermarking using DWT - File Exchange - MATLAB Central. https://in.mathworks.com/matlabcentral/fileexchange/52225. Accessed 24 Mar 2020
33. Wagdarikar AMU, Senapati RK (2019) Design and development of a multiobjective cost function for robust video watermarking using wavelet transform. J Intell Syst 28:873–891. https://doi.org/10.1515/jisys-2017-0264
34. Wang W, Farid H (2009) Exposing digital forgeries in video by detecting double quantization. In: Proceedings of the 11th ACM workshop on Multimedia and security - MM&Sec '09. ACM Press. USA, Princeton, New Jersey, p 39
35. Wang J, Jia X, Kang X, Shi Y-Q (2019) A Cover Selection HEVC Video Steganography Based on Intra Prediction Mode. IEEE Access 7:119393–119402. https://doi.org/10.1109/ACCESS.2019.2936614
36. Xiph.org :: Derf's Test Media Collection. https://media.xiph.org/video/derf/. Accessed 24 Mar 2020
37. Xue Y, Zhou J, Zeng H et al (2019) An adaptive steganographic scheme for H.264/AVC video with distortion optimization. Signal Process. Image Commun. 76:22–30. https://doi.org/10.1016/j.image.2019.04.012
38. Yang H, Kot AC (2004) Text document authentication by integrating inter character and word spaces watermarking. 2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763). IEEE, Taipei, Taiwan:955–958
39. Younus ZS, Younus GT (2019) Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data. J. Intell. Syst. 29:1216–1225. https://doi.org/10.1515/jisys-2018-0225