Kumari *et al.*
Journal of Engineering and Applied Science (2024) 71:36
https://doi.org/10.1186/s44147-024-00376-z

Journal of Engineering and Applied Science

RESEARCH Open Access

A novel Cosine-Cosine chaotic map-based video encryption scheme

Sweta Kumari[1], Mohit Dua[1], Shelza Dua[2] and Deepti Dhingra[1*]

*Correspondence: deeptimona@gmail.com

[1] Department of Computer Engineering, National Institute of Technology, Kurukshetra, India
[2] Department of Electronics and Communication Engineering, National Institute of Technology, Kurukshetra, India

Abstract

The surge in online activities has led to the increasing popularity of sharing video data across diverse applications, including online education tutorials, social networking, video calling, and OTT platforms. Encryption prevents unauthorized access to the transmitted data over unreliable channels. The well-known features of chaos theory such as random behaviour, unpredictability, and initial parameters dependency facilitate its use in cryptography. Many security issues are faced by chaos-based cryptosystems because of their less complexity. Hence, a new Cosine-Cosine chaotic map characterized by intricate chaotic behaviour is designed in the current study. Additionally, we formulate an original video encryption scheme employing this Cosine-Cosine chaotic map. The encryption process involves five steps, beginning with the segmentation of the original video into frames based on its frame rate. In the second phase, a 384 bits pseudorandom key is generated that is further divided into three subkeys of 128 bits each. The novel Cosine-Cosine chaotic map-based sequence is generated. In the fourth step, red, green, and blue components are encrypted using the pseudorandom key and the chaotic sequence. In the last step, we combine encrypted frames to get cipher video. The security analysis validates that the proposed encryption protects against eavesdropping.

Keywords: Video encryption, Chaos, Statistical attack, Brute force attack, Cosine-Cosine map, Pseudorandom key

Introduction

With the swift advancements in communication technology, an enormous volume of image and video data is now exchanged through a multitude of applications, including webinars, video conferencing, meetings, online classes, and social media platforms, all facilitated over the Internet. Information security and privacy are the primary concern to avoid unauthorized access to the shared data on these platforms. There are many techniques available to protect the data from the invaders such as watermarking [1], steganography [2], and cryptography [3–5]. Encryption is considered as finest method to protect video in cryptography. It transfers the video data in an unrecognizable format and protects it from eavesdropping.

The inherent presence of substantial correlation and redundancy among pixels in both video and image data render traditional encryption methods unsuitable for securing such content. Classical techniques not only demand more time but also exhibit slower processing speeds. Consequently, researchers have increasingly turned to chaotic theory

[6–9] as an alternative for video encryption. Chaotic maps, known for producing diverse effects even with minute alterations in initial conditions, have become a focal point in encryption strategies. Primarily, chaos-based encryption approaches involve permutation and diffusion techniques. Permutation means scrambling the data. However, diffusion is the substitution of data [10–12].

Chaotic maps are categorized into two types, i.e., single and multi-dimensions [13–16]. A logistic map is a single dimension's chaotic function. Logistic map [17–19] is the most common and simplest among all the chaotic maps. The mathematical equation of logistic map is as follows:

$$L_{n+1} = \mu \times L_n \times (1 - L_n) \tag{1}$$

Here, μ represents the control parameter, and its values lie between 0 and 4. Sine map [20, 21] is a one-dimensional chaotic map that contains only one control parameter and generates using the sine function. Mathematically, the sine map can be represented by Eq. (2).

$$S_{n+1} = \alpha \times Sin(\pi \times S_n) \tag{2}$$

Where α is the control parameter in range (0, 1) [19–21]. The tent map with u as control parameter can be represented mathematically by Eq. (3).

$$X_{N+1} = \left\{ \begin{array}{c} u \times X_N, X_N < 0.5 \\ u \times (1 - X_N), X_N > 0.5 \end{array} \right\} \tag{3}$$

where u is the control value of the chaos map and its value is lies between 0 and 1.

Some existing one-dimensional chaotic maps have less complexity, a low level of unpredictability, and a narrow and discontinuous chaotic range with a stable window. Due to these reasons, such maps are not suitable to build strong cryptosystems. Therefore, in this current investigation, a new one-dimensional Cosine-Cosine chaotic map is defined. The map demonstrates high complexity in its chaotic behaviour and offers enhanced unpredictability over a broader and continuous chaotic range, thereby eliminating the stable window problem. Additionally, we employ the Cosine-Cosine chaotic map to formulate a video encryption strategy. The resultant video encryption scheme ensures both security and resilience against diverse types of attacks.

Related work

A number of chaotic maps have been created by researchers [22–26]. Kumar and Dua [27] used two different chaotic maps to encrypt audio using DNA encoding and dynamic diffusion. Erkan et al. [28] used the Schaffer function to introduce a two-dimensional hyperchaotic system. The map was used to design an image encryption scheme. Mansoor and Parah [29] used logistic map and tent to introduce a hybrid adaptive image encryption scheme. The author also integrates DNA computing into the scheme. The experiments validate the security provided by the approach.

Various video and image encryption algorithms based on chaotic maps has been developed in recent years [30–36]. Maolood et al. [37] proposed encryption algorithm using two chaotic maps for video encryption. The ChaCha20 algorithm has been used in the encryption process. An extensive security analysis has been done by the author

to validate the performance of the encryption strategy. Tabash and Izhrauddin [38] used the logistic map to encrypt real-time video stream.

Xu et al. [39] introduced an encryption strategy to encrypt H.264 compressed video stream. The encrypt scheme completely disordered the video data and transformed that into an unrecognizable form. Dua et al. [7] proposed a video encryption method using cosine transformed intertwining logistic map. The input video was divided into several frames in the first stage based on the video's duration and frames per second (FPS) value. To provide extra randomness during the encryption process, each frame was rotated 90° counterclockwise. In the last, frames were jumbled using a key.

Chiaraluce et al. [40] designed a novel video encryption strategy. XOR operation was used to encrypt the video data. Qin et al. [41] suggested a multimedia information end-to-end encryption approach that introduced several security mechanisms, such as selective encryption and selective integrity protection. This technique includes major activities such startup authentication and key distribution.

Hafsa et al. [42] developed the diffusion and confusion-based video encryption approach. The Henon chaotic map is used to provide randomness. The chaotic map initial conditions were created using the SHA-3 hash algorithm.

Motivated by these works, we propose a new Cosine-Cosine chaotic map. We further apply the Cosine-Cosine chaotic map to introduce a video encryption scheme. The encryption method mainly takes five steps to produce cipher. The video is converted into frames in the first phase based on the frame rate of the video. We generate a pseudorandom key of 384 bits in the second step. The pseudorandom key is further divided into three sub-keys of 128 bits each. The third phase generates a chaotic sequence. The fourth stage involves dispersing the pixel values in every colour channel of the frame using both the pseudorandom key and the chaotic sequence. In the end, all encrypted frames are merged to form cipher video. The scheme's security is validated using several matrices.

The primary contributions and innovations of this study are as follows:

1. The work designed a new Cosine-Cosine chaotic map, demonstrating complex and unpredictable behaviour. Its chaotic characteristics have been validated through various metrics. The obtained results have been subsequently compared with those of established chaotic maps.
2. The created Cosine-Cosine chaotic map has been employed to formulate an innovative video encryption scheme. This strategy utilizes the chaotic values generated by the Cosine-Cosine chaotic map, in conjunction with a 128-bit pseudorandom key, to encrypt every colour component of the frame.
3. A novel diffusion procedure based on pseudorandom key, value generated using Cosine-Cosine chaotic map, XOR, and modulus operators has been introduced.
4. The proposed video encryption scheme's security has been assessed through diverse parameters, encompassing NPCR (number of pixel change rate), entropy, MSE (mean square error), correlation coefficient, PSNR (peak signal-to-noise ratio), and its resilience against differential and histogram attacks.

The paper is structured into distinct sections as outlined below: the "Cosine-Cosine chaotic map" section delves into the novel Cosine-Cosine chaotic map. The "Proposed

encryption scheme" section introduces the proposed encryption technique, while the "Results" section details the experimental setup and evaluates the results. Lastly, the "Discussion" section concludes the study.

Cosine-Cosine chaotic map

A newly introduced chaotic map, termed the Cosine-Cosine map, exhibits remarkably chaotic behaviour. The definition of the proposed Cosine-Cosine map is provided in Eq. (4).

$$X_{n+1} = |cos(\pi \times r \times cos(\pi(r + 3 \times X_n \times X_n)) * (r + 3 \times X_n \times X_n)| \tag{4}$$

where $r \epsilon [3, 7]$ and x_n, r represent the initial state and control parameter respectively.

Performance evaluation of Cosine-Cosine map

The Cosine-Cosine chaotic map exhibits good chaotic properties. These properties are analysed by various metrics.

Bifurcation diagram

In an effective chaotic map, these values should exhibit a uniform distribution across the entire range, with no gaps or stable windows in between [43]. Figure 1 displays the bifurcation diagram for several existing maps and the newly proposed Cosine-Cosine chaotic map. Notably, the proposed Cosine-Cosine chaotic map showcases a uniform and continuous bifurcation diagram within the range of 3 to 7.

Lyapunov exponent

The calculations of the maximal Lyapunov exponent give the best indications of predictability. The Lyapunov exponent of a chaotic map should be positive. The Lyapunov exponent of some existing maps and the proposed Cosine-Cosine map is given in Fig. 2. Figure 2d provides positive Lyapunov exponent of Cosine-Cosine chaotic map.

Proposed encryption scheme

Figure 3 depicts the proposed encryption algorithm. The novel Cosine-Cosine chaotic map and a pseudorandom key are responsible to change original frame into cipher frame. The decryption process follows the reverse order of these steps to retrieve the original video.

Encryption

The proposed method for encrypting videos involves a series of steps employing the novel Cosine-Cosine chaotic map. The process is outlined below:

1. Divide the original video into frames and determine the number of frames n using the formula $n = FPS \times$ video length in seconds, where FPS represents frames per second.
2. Generate a 128-bit pseudorandom key.
3. Create a chaotic sequence using the Cosine-Cosine chaotic map specified in Eq. (4).
4. Apply operations on the pseudorandom key and the generated chaotic sequence to change frame pixels.
5. Unite all the cipher frames to construct the encrypted video.

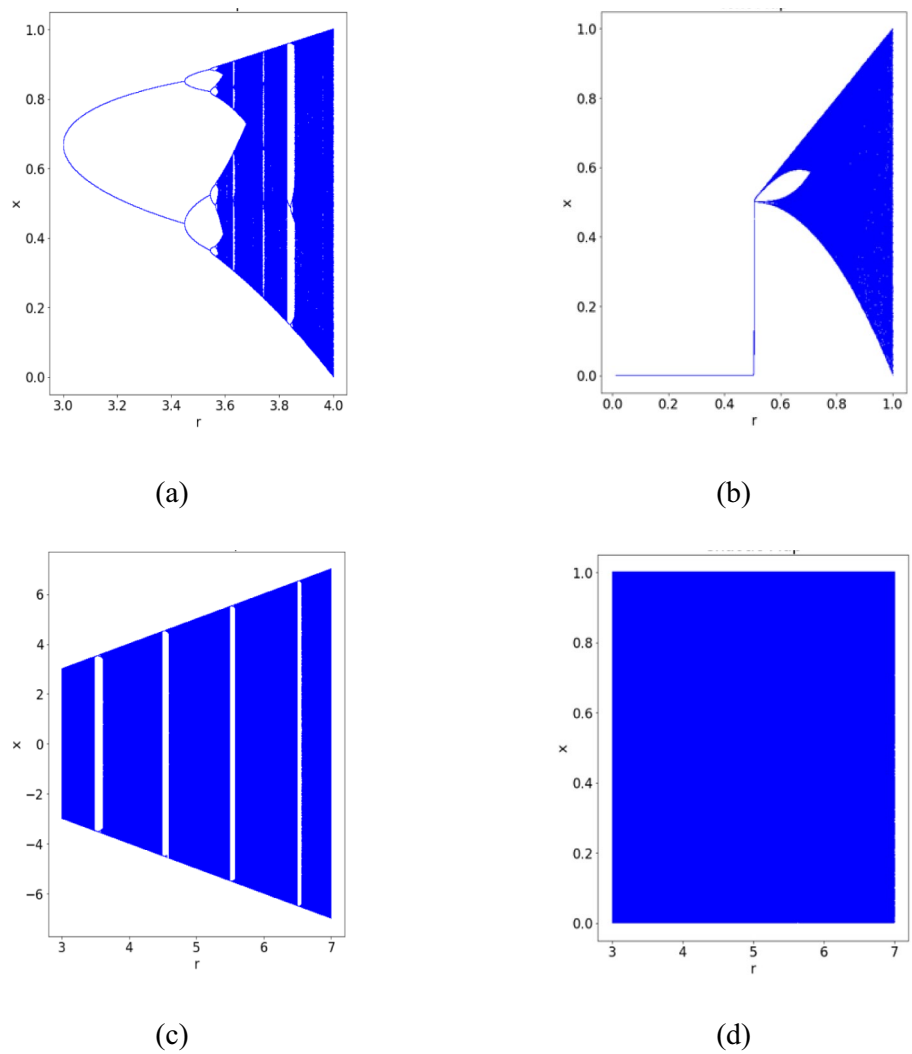


Fig. 1 Bifurcation diagram. **a** Logistic map. **b** Tent map. **c** Sine map. **d** Proposed Cosine-Cosine map

Function 1 represents the pseudocode to encrypt each frame. Function 1 is called in a loop to encrypt the complete video. The following subsections explain the encryption steps in detail.

Pseudorandom key generation

A pseudorandom key of 384 bit is divided into three sub-keys $\{key1, key2, key3\}$ of 128 bit each to encrypt the three-colour channels (red, green, and blue) of the plain frame. Figure 4 depicts the same.

The 128-bit *key* and initial value X are used to generate a pseudorandom key using the following equation for each colour component.

$$Pseudokey = Rightshift(X, d)\ OR\ Leftshift(X, d) \tag{5}$$

Here, the result of the logical OR operation is true if either or both of the input conditions are true and $d =$ count of the number of one's in the following equation:

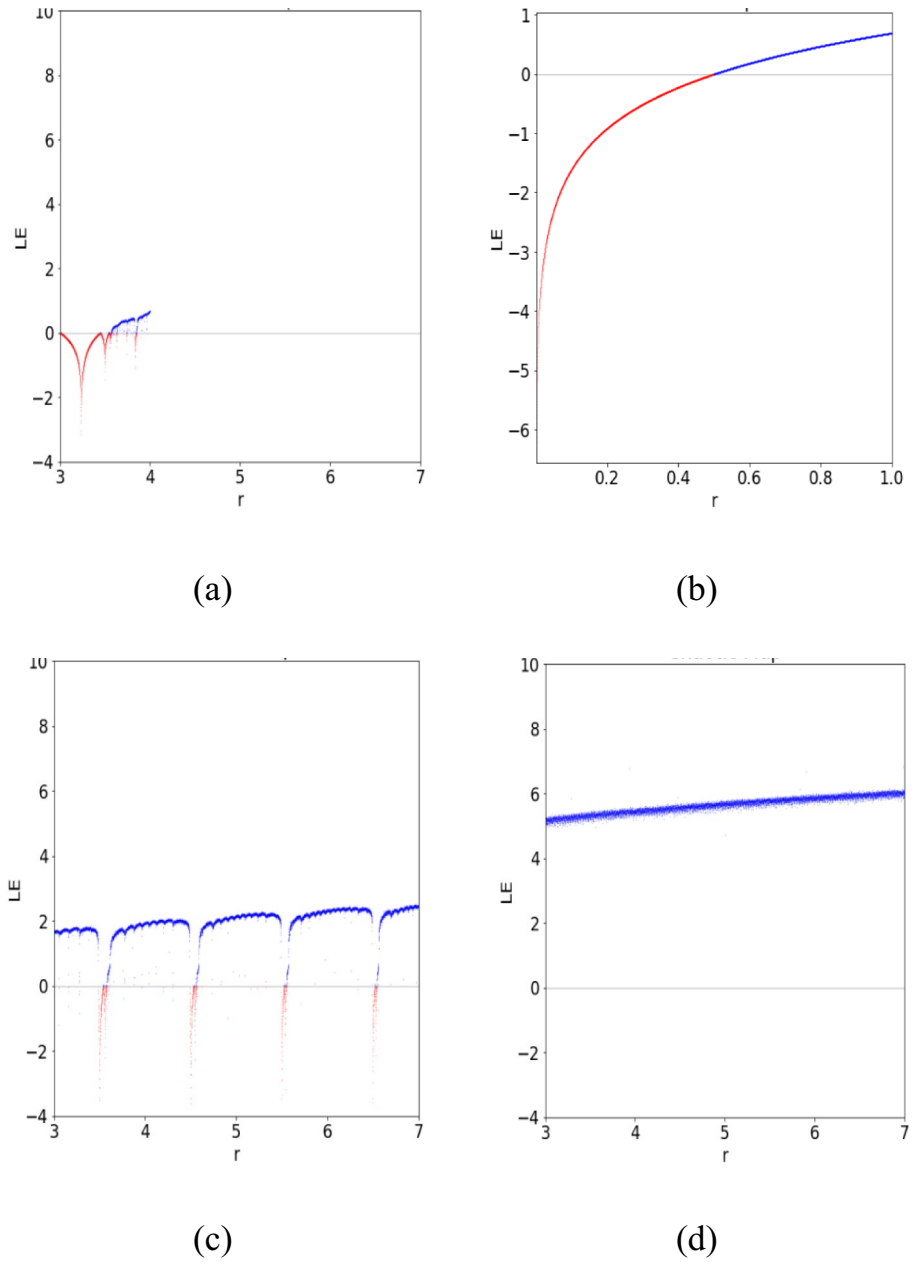


Fig. 2 Lyapunov exponent. **a** Logistic map. **b** Tent map. **c** Sine map. **d** Proposed Cosine-Cosine map

$$temp = Key \oplus X \tag{6}$$

The symbol $\oplus$ typically represents the bitwise XOR (exclusive OR) operation. Here, the bitwise XOR compares corresponding bits of *Key* and X and produces a result of 1 for each bit where the operands differ. If the corresponding bits are the same, the result is 0.

Chaotic sequence generation

The novel Cosine-Cosine chaotic map Eq. (4) has been used in the encryption process. The randomness and unpredictable nature of a chaotic map generates secure

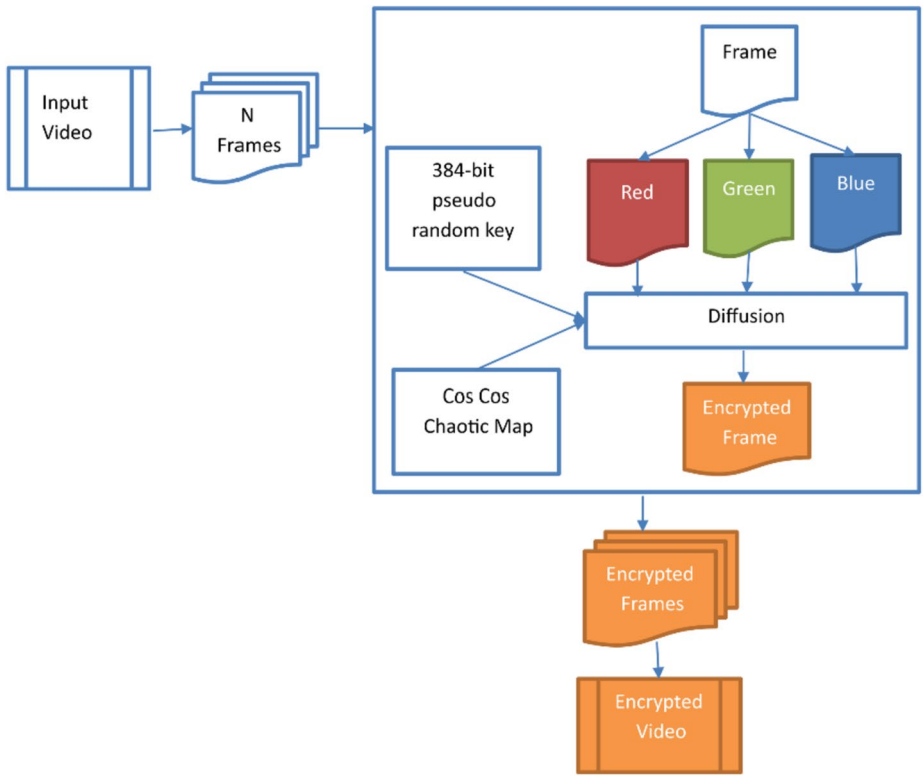


Fig. 3 Proposed video encryption algorithm

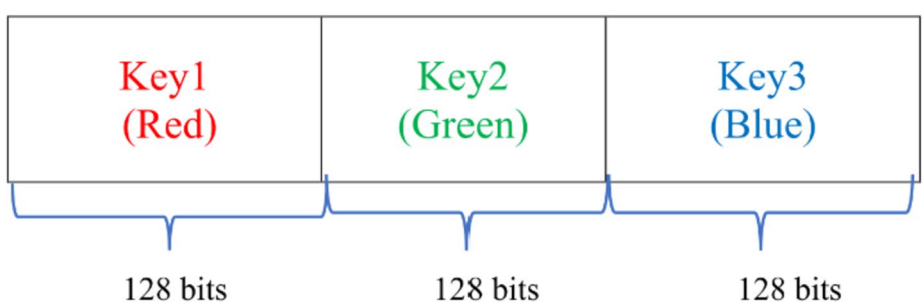


Fig. 4 Distribution of pseudorandom key

cryptosystems. In the proposed scheme, the random value generated by the Cosine-Cosine map in each iteration helps to change the pixels of the input frame.

Diffusion using pseudorandom key and chaotic sequence

We use a 128-bit pseudorandom key, the generated chaotic sequence, XOR, and modulus (% or mod) operator to diffuse the pixels of each colour component in a frame. The following equation is used to modify the pixels of the video frame.

$$cipherframe[row][column][i] = mod(((Plainframe[row][column][i])XOR(Pseudokey\%256))XOR(x_0 * X\%256)), 256) \tag{7}$$

where $cipherframe[row][col][i]$, $Plainframe[row][col][i]$ is the cipher, plain frame with row, column index, and i^{th} colour component. *Pseudokey* X is the pseudorandom key

and initial value for each colour channel, and x_0 represents the chaotic value generated during each iteration. The bitwise XOR compares corresponding bits of $(Pseudokey\%256)$ and $plainframe[row][col][i]$ and produces a result of 1 for each bit where the operands differ. If the corresponding bits are the same, the result is 0. The output of this intermediate result is again XORed with $(x_0 \times X\%256)), 256)$.

```
Function 1: Encryption_single_frame
Input: KeyRed, KeyGreen, KeyBlue, Initial value , rows, columns, color, orignalframe, r
Code:
1. Generation of Pseudorandom key
for i in range(0, color):
    if(color == 0): # Red value
      Key = KeyRed
      X = InitalRed
    else:
      if(color == 1): # Green value
        Key = KeyGreen
        X = InitalGreen
      else: # Blue value
        Key = KeyBlue
        X = InitalBlue
for row in range(0, rows):
for col in range(0, cols):
 temp = Key⊕X
d = Number of ones(temp)
Pseudokey = Rightshift(X, d)OR Leftshift(X, d)
2. Chaotic Sequence generation using Cosine − Cosine map
t = abs(cos(π * r * cos(π(r + 3 * x0 * x0)) * (r + 3 * x0 * x0)))
        if t < 0:
          x0 = −t
3. Diffusion Using Pseudorandom Key and Cosine − Cosine map
        cipherframe[row][col][i] =
                = mod(((Plainframe[row] [col][ i]) XOR (Pseudokey % 256))XOR( x0
                * X%256)),256)
          if t >= 0:
          x0 = t
        cipherframe[row][col][i] =
                = mod(((Plainimage[row] [col][ i]) XOR (Pseudokey % 256))XOR( x0
                * X%256)),256)
         X = temp
Output: cipherframe
```

Decryption

Figure 5 illustrates the decryption mechanism. The subsequent steps are used to decrypt the video.

1. The encrypted video is converted into encrypted frames.
2. Randomly generate a 128-bit key for each colour component of the frame.
3. Iterate the Cosine-Cosine chaotic map to produce a chaotic sequence employed during encryption.
4. Reverse the diffusion process by applying the same pseudorandom key and chaotic sequence to regenerate the original frame.
5. Finally, concatenate all decrypted frames to reconstruct the original video

Function 2 represents the pseudocode to decrypt a single video frame. Similarly, all the frames are encrypted by repeatedly calling Function 2.

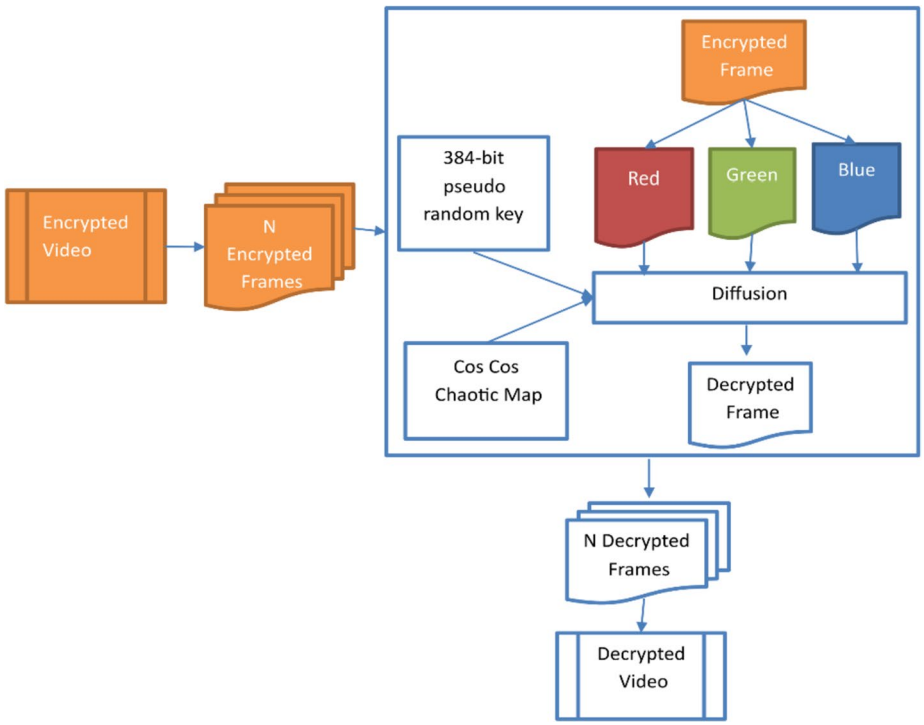


Fig. 5 Proposed video decryption method

Function 2: *Decryption_single_frame*

Input: *KeyRed, KeyGreen, KeyBlue, Initial value , rows, columns, color, cipher frame, r*

Code:

1. *Generation of Pseudorandom key*

```
for i in range(0, color):
    if(color == 0): # Red value
      Key = KeyRed
      X = InitalRed
    else:
      if(color == 1): # Green value
        Key = KeyGreen
        X = InitalGreen
      else:            # Blue value
        Key = KeyBlue
        X = InitalBlue
for row in range(0, rows):
for col in range(0, cols):
 temp = Key⊕X
d = Number of ones(temp)
Pseudokey = Rightshift(X, d)OR Leftshift(X, d)
```

2. *Chaotic Sequence generation using Cosine − Cosine map*

$t = abs(cos(\pi * r * cos(\pi(r + 3 * x_0 * x_0)) * (r + 3 * x_0 * x_0)))$

```
        if t < 0:
          x0 = −t
```

3. *Reverese Diffusion Using Pseudorandom Key and Cosine − Cosine map*

```
        Decrypted frame[row][col][i] =
                = mod(((cipherframe[row] [col][ i]) XOR (Pseudokey % 256))XOR( x0
                * X%256)),256)
          if t >= 0:
          x0 = t
        Decryptedframe[row][col][i] =
                = mod(((cipherframe[row] [col][ i]) XOR (Pseudokey % 256))XOR( x0
                * X%256)),256)
        X = temp
```

Output: *Decryptedframe*

Results

The experimental setup and performance evaluation of the introduced method are described in this section.

Experimental

To assess the effectiveness of our proposed approach, we utilized four video streams: Rhino.mp4, Train.mp4, Flamingo.mp4, and VipTrain.mp4 [44]. The implementation of our video encryption method was carried on a Windows 10 system equipped with an Intel Core i5 2370-M processor, 8 GB of RAM, and a 1-TB hard disk.

Security analysis

Various security parameters such as NPCR (number of pixel change rate), entropy, MSE (mean square error), correlation coefficient, PSNR (peak signal-to-noise ratio), and resistant against differential and histogram attacks are analysed in this section.

Entropy

Entropy serves as a metric for assessing the degree of randomness within an image. An entropy value of 8 signifies the utmost level of randomness [5]. The entropy of an encrypted frame is represented mathematically by Eq. (8):

$$E(i) = \sum_{j=0}^{G-1} p\left(i_j\right) \frac{1}{p\left(i_j\right)} \tag{8}$$

In the provided equation, $p\left(i_j\right)$ represents the probability of the occurrence of a symbol i_j. Here, $G = 2^k$, and $k = 8$ for a grayscale image or a frame. The entropy values of our test videos are documented in Table 1. Additionally, the entropy values for various frames of the rhino video are detailed in Table 2. The values validate the randomness property inherent in our proposed encryption scheme.

Correlation coefficient

The correlation coefficient (CC) gives the relation between two pixels within a video frame, ranging from −1 to 1, where 0 is considered optimal [45, 46]. The CC can be computed using Eq. (9).

$$c_{i,j} = \frac{cov\left(i,j\right)}{\sqrt{A(i)}\sqrt{B\left(j\right)}} \tag{9}$$

where,

$$cov\left(i,j\right) = \frac{1}{M}\sum_{k=1}^{M}(x_k - B(x))\left(y_k - B\left(y\right)\right) \tag{10}$$

$$A(x) = \frac{1}{M}\sum_{k=1}^{M}(x_k - B(x))^2 \tag{11}$$

$$B(x) = \frac{1}{M}\sum_{k=1}^{M} x_k \tag{12}$$

In this context, the CC between adjacent pixels i, j, M is contingent on the number of selected pixels. The CC values for the first video frame of the sample videos are detailed in Table 1. Specifically, for the VipTrain video frame, the CC in the diagonal direction is recorded as −0.0007, indicating a low correlation between pixels. Furthermore, Table 2 presents the CC values for various frames of the Rhino video.

PSNR

Peak signal-to-noise ratio (PSNR) computes the change in the quality of a video frame after encryption. To evaluate PSNR, we refer to the original frame as the signal and errors as noise produced due to encryption. For a good quality-decrypted video frame, the value of PSNR should be high.

Table 1 Security analysis of the first frame of video

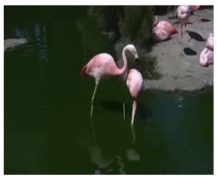
Video Sequence	Entropy	CC			PSNR	NPCR	UACI
		CCH	CCV	CCD			
 Rhino.mp4 (#1)	7.99922	8.92	0.0076	0.0013	37.9973	99.61	50.0
 Train.mp4 (#1)	7.9989	-0.0016	-0.0005	0.00381	37.959	99.68	50.0
 Flamingo.mp4 (#1)	7.9900	0.0007	-0.0089	0.0053	38.036	99.61	50.1
 cookies.mp4 (#1)	7.9992	0.0040	0.0020	-0.0007	37.976	99.657	50.0

Table 2 Encryption analysis of rhino video

Video Fame	Encrypted Image	Entropy	CC	PSNR	UACI	NPCR
		7.99922	0.0013	37.9973	50.0	99.61
		7.9992	0.0018	37.9701	50.02	99.66
		7.9992	0.0052	38.0073	50.01	99.64
		7.9987	0.0083	38.0179	50.02	99.59
		7.9992	0.0016	38.03948	49.91	99.58

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

where MAX_I represents the maximum value a pixel can have in a video frame or an image. MSE stands for mean square error. For an 8-bit representation of pixels in a frame, the value of MAX_I is 255. The PSNR value for the first frame of our sample videos is outlined in Table 1. Additionally, Table 2 provides the PSNR values for various frames of Rhino.mp4.

Differential attack

The resistance against differential attack can be analysed by using metrics NPCR and UACI, which stands for unified averaged change intensity, which are metrics designed to quantify the alterations that take place in a pixel when a single pixel is modified [47, 48]. It mainly emphasizes the pixels that change after an attack. Equations (14)–(16) give the mathematical formula to evaluate NPCR. The NPCR should be nearly equal to 100 for a good encryption algorithm.

$$NPCR = \frac{100}{A \times B} \sum_{m=1}^{A} \sum_{n=1}^{B} U(m,n) \tag{14}$$

where $U(m,n)$ is defined as follows:

$$U(m,n) = \begin{cases} 0, c1(m,n) \neq c2(m,n) \\ 1, otherwise \end{cases} \tag{15}$$

UACI, on the other hand, computes the average intensity of the changes that occur between two cipher images or video frame (UACI) [49, 50], and the formula for the same is as follows:

$$UACI = \frac{1}{A \times B} \sum_{m=1}^{A} \sum_{n=1}^{B} \frac{|E_1(m,n) - E_2(m,n)|}{255} \times 100\% \tag{16}$$

where $E(m,n)$ represents the pixel value located in the mth row and n^{th} column of E and where $E1$ and $E2$ denote the encrypted images. The UACI and NPCR values for various frames of Rhino.mp4 are documented in Table 2. The UACI and NPCR for the first frame of our test video samples are listed in Table 1, indicating a significant alteration in pixel values within the encrypted frame. In the Flamingo video frame, the UACI is 0.501, signifying a minimal difference between neighbouring pixels.

Histogram analysis of rhino video

A uniform histogram pattern indicates a robust encryption method that poses a significant challenge to decryption attempts [51–54]. The analysis in Table 3 illustrates the histograms of five randomly selected frames from the Rhino video. Notably, all the encrypted frames demonstrate a uniform distribution, indicating the efficacy of the proposed approach in handling statistical attacks.

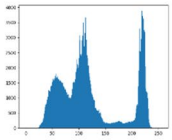
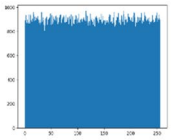
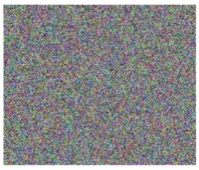
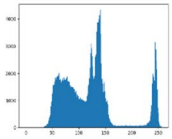
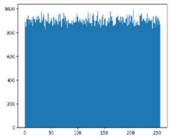
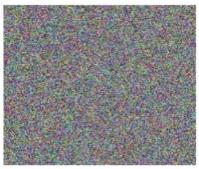
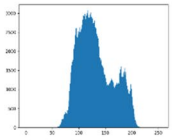
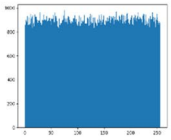
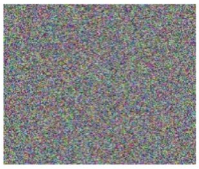
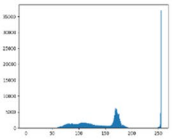
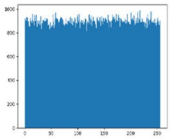
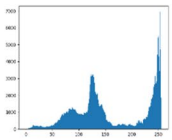
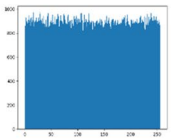
Keyspace analysis

An unauthorized party systematically tests all conceivable combinations of the secret key in an effort to gain access to confidential information. In the proposed scheme, each frame is encrypted using a 384-bit pseudorandom key. As a result, an attacker would be required to explore 2^{384} combinations to breach a single encrypted video frame. If the video consists of n frames, the attacker would need to test $n \times 2^{384}$ combinations to compromise the entire video.

Comparison analysis with different schemes

An encryption method is considered as good if it encrypts the data without any security risk. The size of the frames is a key aspect in determining how time-consuming the suggested strategy is. In comparison to smaller pictures, images with larger dimensions require longer encryption and decryption time. We have compared the results obtained on Rhino.mp4 with the other existing method in Table 4. The value of parameters obtained by our method is more favourable than the other approaches. Moreover, the Cosine-Cosine chaotic map designed in our work has wider chaotic range and more intricate and random features with no stable window problem. The robustness of any

Table 3 Histogram analysis of rhino video

Original Frame	Cipher frame	Original Frame Histogram	Cipher Frame Histogram
 Frame#1			
 Frame#10			
 Frame#40			
 Frame#80			
 Frame#100			

encryption scheme depends on the intricate nature of the chaotic map. Consequently, we assert that our encryption scheme offers substantial safeguard against various attacks, surpassing the effectiveness of other existing methods.

Discussion

The research introduces a newly devised chaotic map termed the Cosine-Cosine chaotic map. The chaotic nature of this map has been substantiated through both the bifurcation diagram and the Lyapunov exponent. The bifurcation analysis of the proposed map reveals a more extensive and uniformly distributed range [3, 7] as compared to other chaotic maps. The consistently positive Lyapunov exponent across the range [3, 7] affirms the randomness and intricate behaviour characteristic of the chaotic map. The study further explores the utilization of this novel map in formulating a video encryption

Table 4 Comparison with the existing approaches

Criteria	Valli et al. [37]	Dua et al. [43]	Ranjith et al. [44]	Proposed scheme
Video	Rhino.mp4	Rhino.mp4	Rhino.mp4	Rhino.mp4
Frame dimensions	-	352 × 192	-	128[a]128
NPCR	99.4518	99.61549	99.51	99.68
UACI	33.63	33.23251	33.54	50.0
CCH	0.0181	0.009020	0.0324	0.0040
CCV	0.0140	−0.01490	0.0261	0.0020
CCD	0.0107	0.000101	0.0263	−0.0007
Entropy analysis	-	7.99757	-	7.99922
Histogram	Uniform	Uniform	Uniform	Uniform
PSNR	-	31.423453	-	37.9701
Keyspace	Size[a]2^{128}	360	2^{212}	384

[a] The "-" values in the table indicate that the respective data is unavailable

strategy. The calculated average entropy value, representing the randomness in the pixels of the video frame, is 7.99683. This entropy value approximates the ideal value of 8, indicating a high degree of randomness. The value of CC is reduced to −0.0007 in the cipher frame that secures it from statistical attacks. The calculated average PSNR value (as shown in Table 1) is 38.00642, suggesting that the encryption scheme introduces randomness, rendering the content indistinguishable from noise. The average NPCR and UACI values (also in Table 1) are 99.63625 and 50, respectively, demonstrating the scheme's resistance to differential attacks.

A comparative assessment with other existing methods (as detailed in Table 4) substantiates that our proposed scheme surpasses the performance of alternative methods.

Conclusion

In this study, we introduced a new chaotic map named the Cosine-Cosine chaotic map. Using this map, we presented a video encryption scheme. The scheme involves the generation of a unique pseudorandom key and chaotic sequence using the Cosine-Cosine map to encrypt video frames. The resulting chaotic sequence and pseudorandom key alters the pixel values. The analysis of results demonstrates that the proposed video encryption technique is resilient against diverse attacks.

Abbreviations

DNA	Deoxyribonucleic acid
CC	Correlation coefficient
UACI	Unified average change intensity
NPCR	Number of pixel change rate
PSNR	Peak signal-to-noise ratio
SHA-3	Secure Hash Algorithm 3
XOR	Exclusively OR
FPS	Frames per second
CCH	Correlation coefficient horizontally
CCV	Correlation coefficient vertically
CCD	Correlation coefficient diagonally
MSE	Mean square error

Acknowledgements
Not applicable.

Authors' contributions
Ms. S designed the proposed scheme, Dr. MD implemented and analysed the work, Dr. SD performed the result analysis, and Ms. DD was a major contributor in writing the manuscript. All authors read and approved the final manuscript.

Funding
The work did not receive any funding from any resource.

Availability of data and materials
Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 21 June 2023 Accepted: 22 January 2024
Published online: 08 February 2024

References

1. Liu Q, Yang S, Liu J, Xiong P, Zhou M (2020) A discrete wavelet transform and singular value decomposition-based digital video watermark method. Appl Math Model 85:273–293
2. Paul G, Davidson I, Mukherjee I, Ravi SS (2017) Keyless dynamic optimal multi-bit image steganography using energetic pixels. Multimed Tools Appl 76:7445–7471
3. Yasser I, Mohamed MA, Samra AS, Khalifa F (2020) A chaotic-based encryption/decryption framework for secure multimedia communications. Entropy 22(11):1253
4. Wang R, Du P, Zhong W, Han H, Sun H (2020) Analyses and encryption implementation of a new chaotic system based on semi tensor product. Complexity 2020:1–13
5. Elrefaey A, Sarhan A, El-Shennawy NM (2021) Parallel approaches to improve the speed of chaotic-maps-based encryption using GPU. J Real-Time Image Process. 18(6):1897–1906
6. Asgari-Chenaghlu M, Balafar M-A, Feizi-Derakhshi M-R (2019) A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation. Signal Processing 157:1–13
7. Dua M, Makhija D, Manasa PYL, Mishra P (2022) 3D chaotic map-cosine transformation based approach to video encryption and decryption. Open Comput Sci 12(1):37–56
8. Patro K, Acharya B, Nath V (2019) Secure multilevel permutation-diffusion based image encryption using chaotic and hyper-chaotic maps. Microsyst Technol 25(12):4593–4607
9. Pankaj S, Dua M (2021) A novel ToCC map and two-level scrambling-based medical image encryption technique. Netw Model Anal Health Inform Bioinform 10(1):48. https://doi.org/10.1007/s13721-021-00324-4
10. Kumar A, Dua M (2021) Novel pseudo random key & cosine transformed chaotic maps based satellite image encryption. Multimed Tools Appl 80(18):27785–27805. https://doi.org/10.1007/s11042-021-10970-5
11. Liu H, Kadir A, Li Y (2016) Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys. Optik (Stuttg) 127(19):7431–7438. https://doi.org/10.1016/j.ijleo.2016.05.073
12. Liu J, Tang S, Lian J, Ma Y, Zhang X (2019) A novel fourth order chaotic system and its algorithm for medical image encryption. Multidimensional Systems and Signal Processing. 30(4):1637–1657. https://doi.org/10.1007/s11045-018-0622-0
13. Liang Q, Zhu C (2023) A new one-dimensional chaotic map for image encryption scheme based on random DNA coding. Optics Laser Technology 160:109033
14. Aslam MN, Belazi A, Kharbech S, Talha M, Xiang W (2019) Fourth order MCA and chaos-based image encryption scheme. IEEE Access 7:66395–66409
15. Guesmi R, Farah MAB (2021) A new efficient medical image cipher based on hybrid chaotic map and DNA code. Multimed Tools Appl 80(2):1925–1944. https://doi.org/10.1007/s11042-020-09672-1
16. Nkandeu YK, Tiedeu A, Abanda Y, Pone JRM (2022) Image encryption using the logistic map coupled to a self-synchronizing streaming. Multimed Tools Appl 81(12):17131–17154
17. Rupa C, Harshita M, Srivastava G, Gadekallu TR, Maddikunta PKR (2022) Securing multimedia using a deep learning based chaotic logistic map. EEE J Biomed Health Inform 27(3):1154–1162
18. Song X-H, Wang H-Q, Venegas-Andraca SE, Abd El-Latif AA (2020) Quantum video encryption based on qubit-planes controlled-XOR operations and improved logistic map. Physica A Statistical Mechanics and its Applications. 537:122660
19. Panwar K, Purwar RK, Srivastava G (2021) A fast encryption scheme suitable for video surveillance applications using SHA-256 hash function and 1D sine–sine chaotic map. International Journal of Image and Graphics 21(02):2150022
20. J. Sethi, J. Bhaumik, and A. S. Chowdhury, "Chaos-based uncompressed frame level video encryption," in Proceedings of the Seventh International Conference on Mathematics and Computing : ICMC -2021, Springer Singapore 2022, pp. 201–217.
21. B. D. Parameshachari and H. T. Panduranga, "Medical image encryption using SCAN technique and chaotic tent map system," in Recent Advances in Artificial Intelligence and Data Engineering, Springer, 2022, pp. 181–193.
22. B. Liu, X. Li, H. Yu, and J. Lv, "A light chaotic encryption algorithm for real-time video encryption," in 4th EAI International Conference on Robotic Sensor Networks, 2022, pp. 111–118.
23. Adhikari S, Karforma S (2021) A novel audio encryption method using Henon-Tent chaotic pseudo random number sequence. Int J Inform Technol 13(4):1463–1471

24. Yang F, An X (2022) A new discrete chaotic map application in image encryption algorithm. Physica Scripta 97(3):35202
25. Wang X, Xu D (2014) Image encryption using genetic operators and intertwining logistic map. Nonlinear Dynamics 78(4):2975–2984. https://doi.org/10.1007/s11071-014-1639-z
26. Dua M, Wesanekar A, Gupta V, Bhola M, Dua S (2020) Differential evolution optimization of intertwining logistic map-DNA based image encryption technique. Ambient Intelligence and Humanized Computing 11:3771–3786
27. Kumar A, Dua M (2023) (2023), "Audio encryption using two chaotic map based dynamic diffusion and double DNA encoding." Applied Acoustics 203:109196
28. Erkan U, Toktas A, Lai Q (2023) 2D hyperchaotic system based on Schaffer function for image encryption. Expert Systems with Applications 213:119076
29 Mansoor S, Parah SA (2023) HAIE: a hybrid adaptive image encryption algorithm using chaos and DNA computing. Multimed Tools Appl 82(1–28):2023
30. Suri S, Vijay R (2019) A synchronous intertwining logistic map-DNA approach for color image encryption. Ambient Intell Human Comput 10(6):2277–2290
31. Bouteghrine B, Tanougast C, Sadoudi S (2021) Novel image encryption algorithm based on new 3-d chaos map. Multimed Tools Appl 80:1–23
32. J. Sethi, J. Bhaumik, and A. S. Chowdhury, "Fast and secure video encryption using divide-and-conquer and logistic tent infinite collapse chaotic map," in International Conference on Computer Vision and Image Processing, 2022, pp. 151–163.
33. Benrhouma O, Alkhodre AB, AlZahrani A, Namoun A, Bhat WA (2022) Using singular value decomposition and chaotic maps for selective encryption of video feeds in smart traffic management. Appl Sci 12(8):3917
34. Shanableh T (2022) HEVC video encryption with high capacity message embedding by altering picture reference indices and motion vectors. IEEE Access 10:22320–22329
35. Ma H, Ma Y, Zhang W, Zhao X, Chu P (2022) Development of video encryption scheme based on quantum controlled dense coding using GHZ state for smart home scenario. Wireless Person Commun 123(1):295–309
36. Al-Hazaimeh OM, Abu-Ein AA, Al-Nawashi MM, Gharaibeh NY (2022) Chaotic based multimedia encryption: a survey for network and Internet security. Bulletin of Electrical Engineering and Informatics 11(4):2151–2159
37. Maolood AT, Gbashi EK, Mahmood ES (2022) Novel lightweight video encryption method based on ChaCha20 stream cipher and hybrid chaotic map. Int J Electric Comput Eng 12(5):2088–8708
38. Tabash FK, Izharuddin M (2019) Efficient encryption technique for H.264/AVC videos based on CABAC and logistic map. Multimed Tools Appl 78(6):7365–7379. https://doi.org/10.1007/s11042-018-6494-3
39. Xu H, Tong X, Wang Z, Zhang M, Liu Y, Ma J (2020) Robust video encryption for h. 264 compressed bitstream based on cross-coupled chaotic cipher. Multimed Syst 26(4):363–381
40. Chiaraluce F, Ciccarelli L, Gambi E, Pierleoni P, Reginelli M (2002) A new chaotic algorithm for video encryption. IEEE Transactions on Consumer Electronics 48(4):838–844
41. Qin L, Zhang G, You L (2022) Application of CSK encryption algorithm in video synergic command systems. Journal of Organizational and End User Computing (JOEUC) 34(2):1–18
42. Hafsa A, Fradi M, Sghaier A, Malek J, Machhout M (2022) Real-time video security system using chaos-improved advanced encryption standard (IAES). Multimed Tools Appl 81(2):2275–2298
43. Dua M, Makhija D, Manasa PYL, Mishra P (2022) D chaotic map-cosine transformation based approach to video encryption and decryption. Open Comput Sci 12(1):37–56
44. Dua M, Kumar A (2022) Multiple image encryption approach using non linear chaotic map and cosine transformation. Int J Inform Technol 14(3):1627–1641
45. Kumar CM, Vidhya R, Brindha M (2021) An efficient chaos based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function. Appl Intell 52(3):2556–2585
46. Dua M, Suthar A, Garg A, Garg V (2021) An ILM-cosine transform-based improved approach to image encryption. Complex Intell Syst 7(1):327–343
47. Jaroli P, Bisht A, Dua M, Dua S (2018) A color image encryption using four dimensional differential equations and Arnold chaotic map. Proceedings of the International Conference on Inventive Research in Computing Applications, ICIRCA 2018:869–876. https://doi.org/10.1109/ICIRCA.2018.8597310
48. Bisht A, Dua M, Dua S (2018) A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random transform. Ambient Intelligence and Humanized Computing 10(9):3519–3531. https://doi.org/10.1007/s12652-018-1072-0
49. P. Deshmukh and V. Kolhe, "Modified AES based algorithm for MPEG video encryption," in International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp. 1–5.
50. D. Ganeshkumar, A. Suresh, and K. Manigandan, "A new one round video encryption scheme based on 1D chaotic maps," in 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019, pp. 439–444.
51. Wen D, Jiao W, Li X, Wan X, Zhou Y, Don X, Han W (2023) The EEG signals encryption algorithm with K-sine-transform-based coupling chaotic system. Inform Sci 622:962–984
52. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, & X. Tang, X. "EFR-CSTP: encryption for face recognition based on the chaos and semi-tensor product theory. Inform Sci. 2023;621:766-781.
53. Dhingra D, Dua M (2023) Medical video encryption using novel 2D cosine- sine map and dynamic DNA coding. Med Biol Eng Comput 62:1–19
54. Dhingra D, Dua M. A chaos-based novel approach to video encryption using dynamic S-box. Multimed Tools Appl. 83:1-31.

Publisher's Note