SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Chaos Based Novel Video Encryption Scheme to Secure Video/Image Information from Any AI-Generated Attacks

Harshita Bajaj[1], Parnab Das[1], Santanu Mandal[1,*]

[1] School of Advanced Sciences, VIT-AP University, Andhra Pradesh 522237, India

ARTICLE INFO

Article history:
Received 5 November 2023
Received in revised form 30 May 2024
Accepted 16 June 2024
Available online 10 August 2024

Keywords:

Real-time video encryption; image encryption; scrambling; diffusion; secure communication

ABSTRACT

With the rise of data-intensive activities, methods such as video encryption have gained prominence, paving the way for quantum encryption and AI-powered strategies. It ensures content protection, supports compliance, and enables controlled sharing across sectors like security, satellite & medical imaging, and E-commerce. This study introduces a novel efficient and guarded scheme for encrypting videos as well as images using a 4D hidden chaotic system and application in AI-developed real-time video. A chaotic system is used for developing a unique scrambling process and for the diffusion process. Such an encryption method is rare in recent findings. Various performance analyses are employed to assess the efficiency and resilience of the algorithm. The large key range enhances the algorithm's security against brute force attacks and the careful adjustment of keys empowers the chaos to create different sequences of pseudo-random numbers, which significantly influences the proposed algorithm. The correlation coefficient is close to zero and NPCR is at least 99.62%, UACI is at least 33.50%. After encryption, the histogram is uniformly distributed, key space is extensive with 10^{135}, and the three-dimensional intensity plot of the encrypted image also exhibits uniformity. Moreover, the encryption algorithm can overcome several noise attacks such as salt and pepper noise, Gaussian noise additionally provides strong resistance against clipping attacks, underscoring the algorithm's effectiveness and resilience.

1. Introduction

With the rapid development of the Internet of Things (IoT) and communication technologies and with the accessibility of multimedia applications, videos have emerged as the predominant medium for conveying information in visual communication. Therefore, to prevent the transmitted video from unauthorized users the video should be encrypted before transmitting or storing. The video data is characterized by special features for instance bulk capability, high ratio of repetition, and its pixels are highly correlated to each other. As a result, performing the video encryption process is required to develop an efficient and secure video encryption algorithm. However, established encryption

* *Corresponding author.*
E-mail address: santanu.mandal@vitap.ac.in

https://doi.org/10.37934/araset.50.1.120

methods like the Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Data Encryption Standard (DES) are unfit for real-time applications [1].

In the Video complete encryption process, video is not considered as a total data format, it splits into frames and then the encryption process is applied and it also ignores the correlations between video frames. This leads to an augmentation in the algorithm's complexity, resulting in an enhanced level of security and effectiveness in the encryption process. In the recent era of advancement in IoT, Multimedia encryption can be utilized in medicine and healthcare [2-5], satellite video [6], science and technologies [7,8], online education content [9], military, and Judicial systems in protecting the witness, etc. Numerous multifaceted applications in modern life, have led to the development of several video encryption methods [10-14].

Due to the complex properties like ergodicity, non-convergence, non-periodicity, sensitivity to parameters, and initial condition, the chaotic system [15,16] attracts special attention in multimedia encryption methods. Several image encryption techniques based on chaotic maps have already been developed [17-19].

In 2020, Wang *et al.,* [20] developed an image encryption scheme based on Fisher-Yates scrambling and 5D fractional order cellular neural network, where the diffusion technique was controlled by the chaotic neural network system. In 2021, Rahman *et al.,* [21] proposed a chaotic system-based encryption process for grey-scale images. In 2022, by utilizing the Lorenz chaotic system and cellular automata and S-box as key tools Alexan *et al.,* introduced a colour image encryption technique [22]. In 2023, Alexan *et al.,* [23] by employing several discrete chaotic maps and KAA map, proposed a colour image encryption technique, specifically for square images. In 2023, Alharbi *et al.,* [24] developed an encryption technique for grey-scale images by utilizing an eight-dimensional chaotic system. To increase the effectivity of the algorithm some of these studies utilize higher dimensional chaotic systems. Though the higher dimensional systems increase the complexity of the encryption method than the lower dimensional system, it consumes lots of computational effort, which is not suitable for real-time application. Also, some of the techniques used several complicated techniques for the encryption processes, which increases the efficiency of the algorithm. Since these processes require a significant amount of computing work, they are not suitable in the extension for the real time video encryption techniques. However, the number of chaos-based video encryption methods is comparatively less.

In 2020 Liu *et al.,* [25] developed a video encryption technique based on integer dynamic coupling tent mapping. Several analysis results show that the algorithm is less efficient in the sense of key sensitivity and pixel correlations. In 2022 Benrhouma *et al.,* [26] proposed a video encryption technique based on singular value decomposition and a Chaotic system. Here the encryption is performed in a selective frame considered as an image, instead of the whole video, which is less secure, and the described algorithm was simulated only for grey-scale images. In both algorithms, the analysis for noise and clipping attacks has not been carried out, which is more necessary in dedicated encryption algorithms for remote communication systems. In 2022 El-Mowafy *et al.,* [27] developed two chaotic system-based video encryption techniques. The first algorithm is based on the chaotic map-based random keys and the second method has been proposed by using the chaotic system and both steganography and cryptography tools. Several discrete chaotic maps are utilized, which are lower dimensional, which are of lower complexity. As a result, the algorithm is less complex in the sense of the order of the chaotic map. In 2023 El-den *et al.,* [28] discovered a video encryption algorithm based on chaotic systems and skewed maps. The scrambling process is based on two chaotic linearly symmetric maps and one chaotic tent map. For the diffusion scheme, both linearly symmetric chaos maps and a distorted form of chaotic tent map are employed to create keys. In this

case, also, encryption is not performed for every frame, which indicates less security than, the whole video encryption by considering the video as a sequence of images.

Despite having some groundbreaking discoveries, these algorithms have a number of drawbacks. Therefore, to overcome these issues in this paper an efficient image encryption technique for colour images of any size has been developed, based on a four-dimensional chaotic system, which can provide comparatively less computational efforts with high complexity. The encryption method is complex in structure but consumes comparatively less computational effort and also has extended the encryption techniques for the videos, which can effectively encrypt real-time video in secure an efficient manner. Several analyses confirm the efficiency and reliability of the algorithm. It is observed that this image encryption part of the algorithm is efficient and more secure compared to other existing work [18,19,22,23,29,30].

This paper illustrates these subsequent key aspects:

i. The proposed video encryption algorithm is separated into three parts in the first part images are constructed from the video then an image encryption technique is developed for encrypting those images and in the last part an image sequence is developed to create an encrypted video.
ii. In this encryption method the images are constructed from consecutive cluster frames and a user input is taken for choosing the number of frames (one or more than one frame at a time), which enhances the complexity of the algorithm.
iii. A matrix is constructed to perform the bitwise XOR operation, with its columns consisting of pseudo-random numbers. The matrix size corresponds to the dimensions of the image.
iv. Videos of any dimension can be encrypted using this scheme.
v. Keyspace analysis, key sensitivity analysis, histogram analysis, three-dimensional pixel intensity and robustness analysis against external noise like salt and pepper noise, Gaussian noise, anti-clipping attack analysis are performed for a frame of the video to analyse the effectiveness and randomness of the algorithm and the image encryption technique is used for encryption a sample image which is used in adjacent correlation analysis, and analysis for differential attacks such as UACI (unified averaged changed intensity) and NPCR (number of changing pixel rate), which are executed to verify the algorithm's efficiency and effectiveness.
vi. Recently an AI-based powerful tool WALDO 2.0 is developed to detect objects extremely fast from drone footage. Which can efficiently capture the real footage of moving objects from very far distances. But it is also needed to secure that footage from unauthorized users. We have used the footage captured using this AI-based tool and available at https://www.linkedin.com/posts/aigpt_ai-will-be-tracking-our-every-move-you-are-ugcPost-7095231106177765376-4MKz?utm_source=share&utm_medium=member_android, to perform the proposed novel video encryption algorithm. Here the video is compressed into 256×256 size for easier demonstration and split into 844 frames.

The subsequent sections of this work are structured as: In section 2 a 4D chaotic system based novel video encryption scheme and the algorithm for video decryption are demonstrated. The application of the encryption algorithm in real-time application is demonstrated and some performance tests are also performed in section 3.

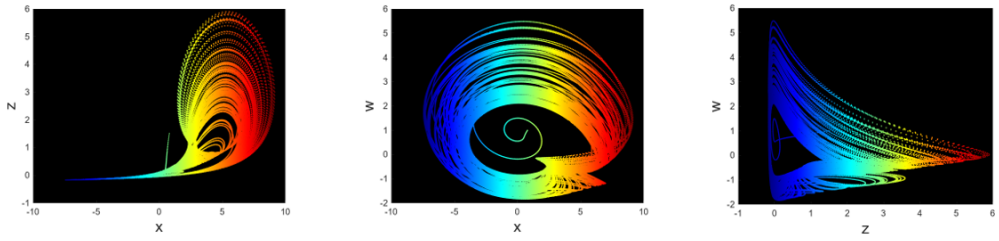
2. Methodology

2.1 Chaotic Map

To perform the encryption algorithm the four-dimensional chaotic map with four parameters proposed in [31] is used here. The chaotic system is as follows

$$\begin{cases} \frac{dx}{dt} = -y - z^2 \\ \frac{dy}{dt} = x + ay \\ \frac{dz}{dt} = bx - cz + xz \\ \frac{dw}{dt} = -dx - zw \end{cases} \quad (1)$$

The chaotic system Eq. (1) described in [31] has hidden type attractor with infinite equilibrium points and the phase portraits are shown in Figure 1, and show different dynamics for different parameter values, which indicates the sensitivity of the system with the parameter values. It also possesses fixed point and chaotic multistability. Which indicates that the system is also sensitive to initial conditions. The amplitude of the chaotic signal can be changed, without changing the chaotic structure, by coupling an amplitude control parameter. As a result, different chaotic attractors can be generated for fixed parameter values and initial conditions and different amplitude control parameters. Therefore, the system contains rich dynamics to apply in pseudo-random number generation in the video encryption process.



(a) (b) (c)

Fig. 1. Chaotic system's phase diagram by fixing $a = 0.38, b = 0.3, c = 5.7, d = 0.4$ and initial condition $(0.8, 0.05, 1.5, 1)$, in (a) *x-z*, (b) *x-w*, (d) *z-w* planes

2.2 The Suggested Encryption and Decryption Algorithm

2.2.1 Slicing the video

The methodology involved in extracting individual frames from a video comprises a step-by-step approach that has been widely applied in practical video analysis. The procedure, executed using the OpenCV library, starts with data acquisition and preprocessing, where the video dataset is prepared for analysis. Subsequently, the video file is loaded into the program, and the OpenCV VideoCapture function facilitates frame-by-frame traversal. The Mechanism of the algorithm is shown in Figure 2(a).

2.2.2 Merging image sequence into video

The procedure to convert an image sequence into a video involves leveraging OpenCV's capabilities for image processing and video creation. The essential libraries like cv2 for image and video manipulation and, an operating system for file and directory operations are imported. The

settings for the resulting video are specified, encompassing critical parameters such as the output video's title, resolution dimensions, frames per second (FPS), and the codec used for compression. The image files within the directory are organized sequentially so that the images are processed in the correct sequence to form a video. We have used the VideoWriter object to write the images into a video file. It iterates through all the image sequences and preprocesses it to form a converted video.

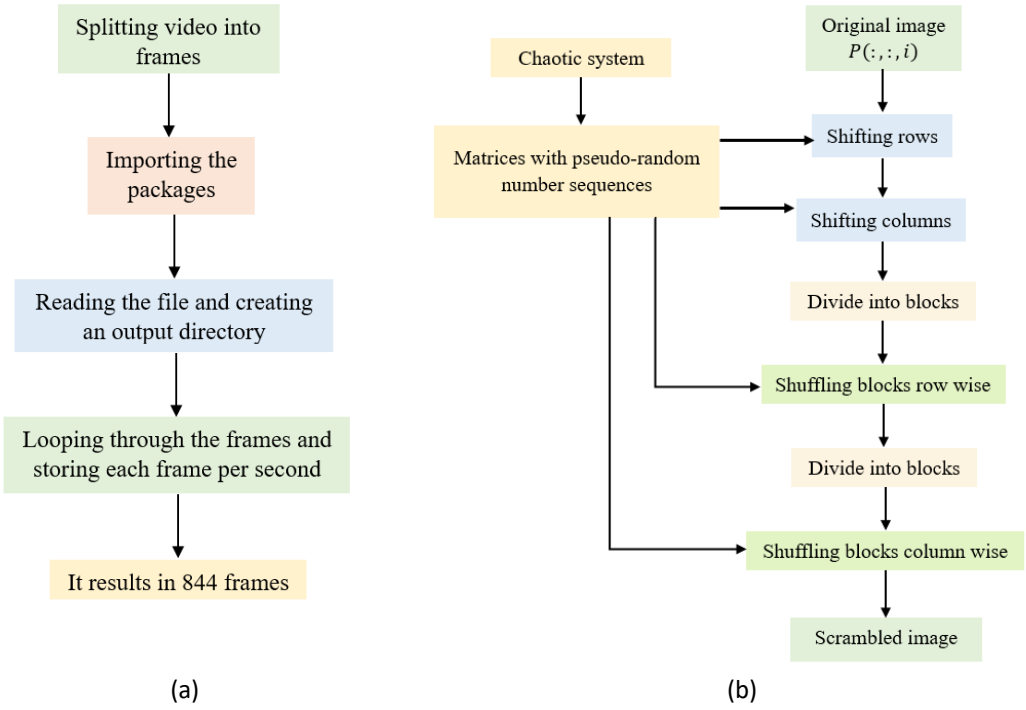


Fig. 2. (a) Mechanism of splitting video into frames, (b) flow chart for Scrambling (For scrambling repeat step 2 to last step 256 times)

2.2.3 Encryption algorithm

In these algorithms $floor(x)$ is used to round each element of x to the nearest integer which is less than or equal to that element, $mod(a,m)$ returns the remainder after the division of a by m, $ceil(x)$ rounds each element of x to the nearest integer greater than or equal to that element.

Algorithm 1: Generation of Pseudo Random Number for Scrambling
INPUT: Chaotic system, system parameters $a, b, c\ and\ d$, initial condition $\big(x(0), y(0), z(0)\text{ and }w(0)\big)$, height M and width N of the image from multiple consecutive cluster frame
OUTPUT: Matrices using pseudo-random number sequences, $T(:,i), D(:,i), F(:,:,i), G(:,:,i)$, $i = 1,2,3$
1. Solve the system using the parameters a, b, c, d and an initial condition $\big(x(0), y(0), z(0), w(0)\big)$ and store the solution set for x, y, z and w in the columns of the matrix $X(:,:)$.

2. for $i = 1:3$
3. $\quad E = mod(X(1:256:256 \times (M-1), i), M)$
4. $\quad a1$ is the position of the M elements of E by arranging them in ascending order.

5. $T(:,i) = a1$
6. end
7. for $i = 1:3$
8. $E = mod(X(1:256:256 \times (N-1), i), N)$
9. $a1$ is the position of the N elements of E by arranging them in ascending order.
10. $D(:,i) = a1$
11. end
12. for $i = 1:3$
13. $a1 = ceil(N/4)$
14. for $j = 1:a1$
15. $E = mod(X(1:256:256 \times (a1-1), i) + j^2, a1)$
16. $b1$ is the position of the elements of E by arranging them in ascending order.
17. $F(j,:,i) = b1$
18. end
19. end
20. for $i = 1:3$
21. $a1 = ceil(M/4)$
22. for $j = 1:a1$
23. $E = mod(X(1:256:256 \times (a1-1), i) + j^2, a1)$
24. $b1$ is the position of the elements of E by arranging them in ascending order.
25. $G(j,:,i) = b1$
26. end
27. End

Algorithm 2: Scrambling each image obtained from multiple consecutive cluster frame (Figure 2(b))
INPUT: Image ($P(:,:,i)$) from multiple consecutive cluster frames of a particular colour channel with height M and width N, matrices using pseudo-random numbers
$T(:,i), D(:,i), F(:,:,i), G(:,:,i)$
OUTPUT: Scrambled image $I(:,:,i)$
1. Generate the sequence $T(:,i)$ from Algorithm 1.
2. Change the position of rows of $P(:,:,i)$ according to $T(:,i)$ and create a matrix $R(:,:,i)$.
(If $T(j,i) = g$, the j-th row of image $P(:,:,i)$ will be g-th row of $R(:,:,i)$)
3. Rotate $R(:,:,i)$ into 180^0.
4. Generate the sequence $D(:,i)$ from Algorithm 1.
5. Change the position of the columns of $R(:,:,i)$ according to $D(:,i)$ (similar to step 2) and create a new matrix $P1(:,:,i)$.
6. Rotate $P1(:,:,i)$ into 180^0.
7. Divide $P1(:,:,i)$ into 4×4 blocks, if 4 does not divide M or N then collect the remaining row wise or column wise. (e.g., if $M = 641$ and $N = 640$, then there will be 160 blocks in row wise and column wise 160, 4×4 blocks and the remaining one will be 1×4 block).
8. Generate the matrix $F(:,:,i)$ using Algorithm 1.
9. Shuffle blocks in j-th row using $F(j,:,i)$ and call it $P1(:,:,i)$.
(For each row use the similar method as described in step 2)
10. Divide $P1(:,:,i)$ into 4×4 blocks, similar to step 7.
11. Generate the matrix $G(:,:,i)$ using Algorithm 1.
12. Shuffle blocks in j-th column using $G(j,:,i)$ and call it $P1(:,:,i)$.
(For each row use the similar method as described in step 2)

13. Using the output from step 12 repeat step 1 to 12, 256 times to scramble the image efficiently. Call the scrambled image $I(:,:,i)$.

Algorithm 3: Generation of a matrix for diffusion
INPUT: Chaotic system, system parameters $a, b, c\ and\ d$ initial condition $\big(x(0), y(0), z(0)\text{ and }w(0)\big)$, height M and width N of the image from multiple consecutive cluster frame
OUTPUT: Matrix $A(:,:,i)$ whose entries are pseudo random numbers
1. Solve the system using the parameters a, b, c, d and the initial condition $(x(0), y(0), z(0)\ and\ w(0))$ and store the solution set for x, y, z and w, in the columns of the matrix $X(:,:)$.
2. $g = mod\big(floor\big((X(:,i)/256) \times 10^{15} + X(:,4) \times j \times 10^{14}\big), 256\big)$
3. A matrix $A(:,:,i)$ is constructed from g with the same size as the size of the video and the columns are a set of pseudo random number (PRN) sequences chosen from g.
4. The number of sets of generated PRN sequences is similar to the number of columns (width) of the video. Each PRN sequence comprises pixel values corresponding to the video's row number (height).In each column sequence, elements are from 0 to 255 and those are chosen from the pseudo random number sequence g.
5. For video of height M there will be $floor(M/256)$ complete sequence of PRN from 0 to 255 collected from g. The former 256 values are non-repeated 256 PRN from 0 to 255 collected from g and rest of the PRN values in g will be used for generating the next sequence of length 256 and using the similar method all the full sequences will be generated and rest of the portion will be covered by the remaining part of g using non-repeated PRN value from 0 to 255. (Demonstrated in Figure 3).

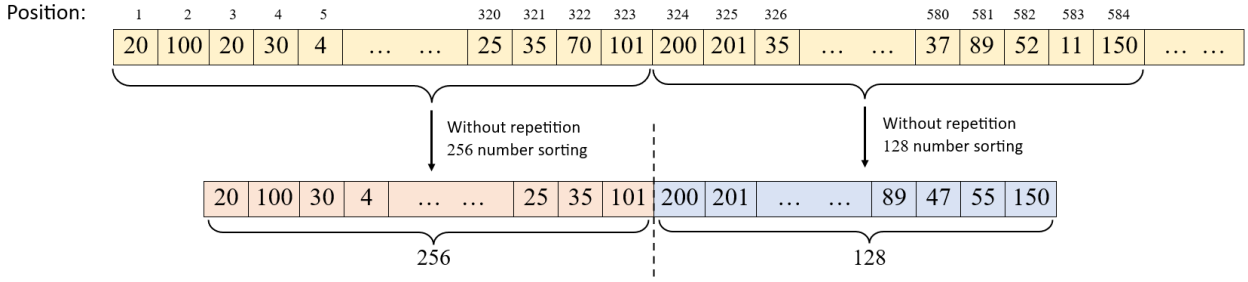


Fig. 3. Demonstration of generation of a column of length 384, Yellow shaded set denotes the Pseudo random number sequence, the red shaded set denotes the first 256 random numbers in that column and the blue shaded set denotes the last 128 random numbers of the column

Algorithm 4: Diffusion Process
INPUT: Matrix $A(:,:,i)$, the scrambled image $I(:,:,i)$ (obtained from algorithm 2)
OUTPUT: Diffused image $J(:,:,i)$.

for $j = 1:M$
  for $k = 1:N$
    if ($j == 1$) && ($k = 1$) // bitxor for first element
      $J(j,k,i) = A(j,k,i) \oplus I(j,k,i)$
    end if
    if ($j == 1$) && ($k > 1$) // bitxor for elements in first row except first element
      $J(j,k,i) = \big(A(j,k,i) \oplus I(j,k,i)\big) \oplus J(j,k-1,i)$
    end if
    if ($k == 1$) && ($j > 1$)
      $J(j,k,i) = \big(A(j,k,i) \oplus I(j,k,i)\big) \oplus J(j-1,k,i)$
    end if
    if ($k > 1$) &&($j > 1$) && ($k \leq floor(N/2)$)
      $J(j,k,i) = \Big(J(j,k-1,i) \oplus \big(A2(j,k,i) \oplus I(j,k,i)\big)\Big) \oplus J(j-1,k+1,i)$
    end if
    if ($k > floor(N/2)$)&& ($j > 1$)
      $J(j,k,i) = \Big(J(j,k-1,i) \oplus \big(A2(j,k,i) \oplus I(j,k,i)\big)\Big) \oplus J(j-1,k-1,i)$
    end if
  end for
end for

Algorithm 5: Video Encryption Process
INPUT: Original Video with height h and width w, Chaotic system, system parameters a, b, c and d, initial condition $\big(x(0), y(0), z(0) \text{and } w(0)\big)$, t (for making the image for encryption)
OUTPUT: Encrypted Video

1. First slice the video into frames, where each frame is of height h and width w.
2. Collect t (Ranging from 1 to the total count of divided frames) consecutive frames from the image sequence stating from first frame and by joining them make images in cluster form. If after collecting a group of t frames from the beginning, some frames (less than t) remain, then also collect the rest of the frames and make one image.
3. The encryption algorithm will be utilized in those images from multiple consecutive frame clusters.
4. For an image with height M and width N, split the image into three colour channels and apply the scrambling algorithm (Algorithm 2) for each one.
5. To perform the diffusion process, generate the matrix $A(:,:,i)$ from the chaotic system (Algorithm 3), which is of the same size as the image of step 4.
6. Perform the bitwise XOR operation (Algorithm 4) for each colour channel.
7. Combine all the colour channels and make an encrypted image.
8. Split the encrypted images into frames.
9. Merge the image sequence to make the encrypted video.

2.2.4 Decryption algorithm

The reverse method of the above Encryption algorithm is applied by using the keys as the system parameters a, b, c, d; $(x(0), y(0), z(0)$ and $w(0))$ as initial condition and a user input constant t. In the decryption process after slicing the video into frames the images from multiple consecutive frames need to be produced and each image will be decrypted using the back propagation method of the image encryption process for the original video the images will be split into frames and then by merging the image sequence the original video will be obtained.

3. Result

3.1 Application of the Scheme on a Real-Life Video Footage

The algorithm is simulated for the system parameter values $a = 0.38, b = 0.3, c = 5.7, d = 0.4$ and initial condition $(0.8,0.05,1.5,1)$ and $t = 1$, for the video described in introduction with dimension 256×256. The algorithm's simulation is illustrated in the Figure 4 and also the decrypted image is shown there.

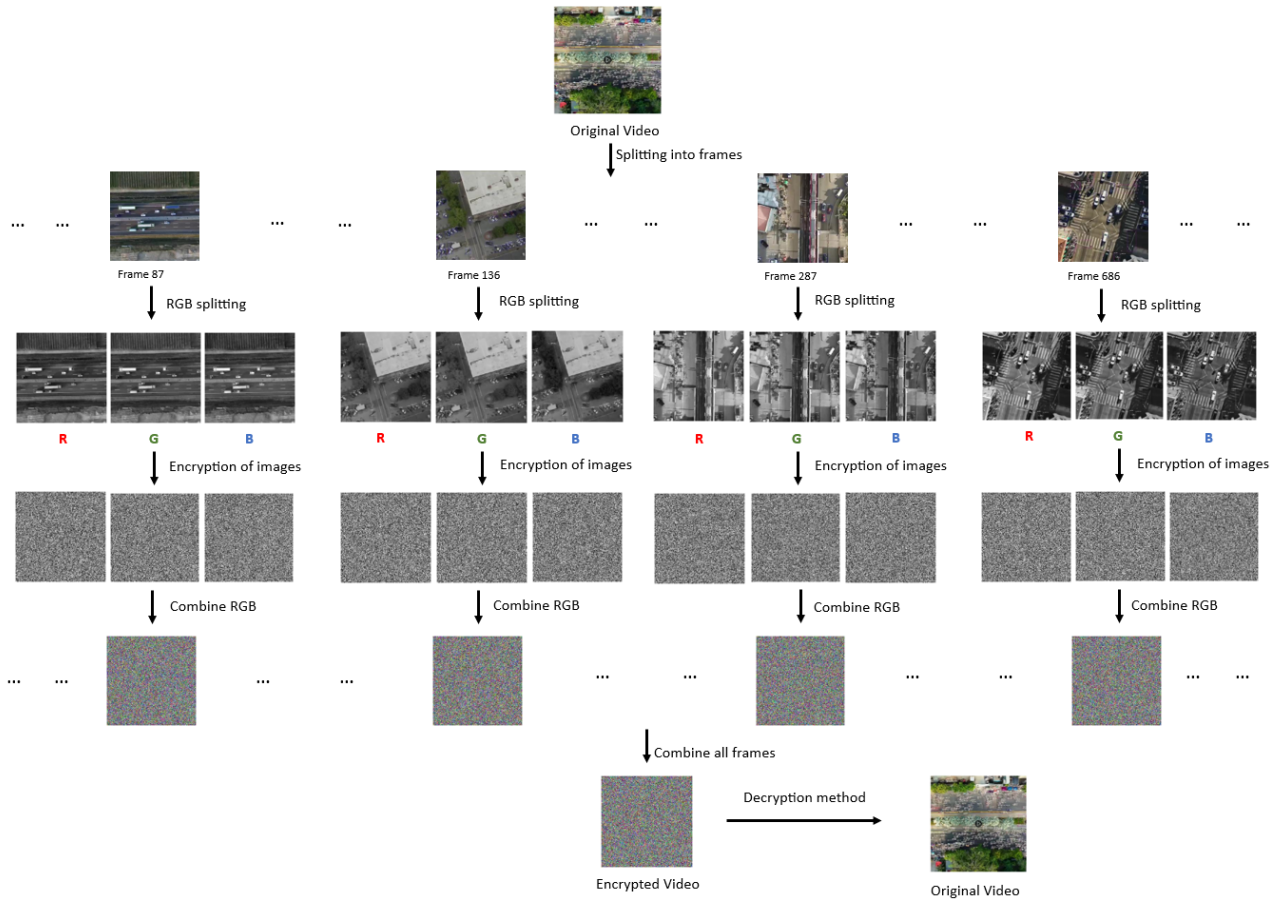


Fig. 4. Video encryption process and decrypted video for parameter values $a = 0.38, b = 0.3, c = 5.7, d = 0.4$ and initial condition $(0.8,0.05,1.5,1)$ and $t = 1$

3.2 Performance Analysis

3.2.1 Analysis for key space

The size of the key space is one of the important key characteristics to estimate the cryptosystem strength against brute force attacks [32]. To prevent this attack, the size of the key space must be at least 2^{100} [33]. The numerical keys for the algorithm introduced in this paper comprise of the four parameters a, b, c, d and $\big(x(0), y(0), z(0)\ and\ w(0)\big)$ as the initial point for the chaotic map in [31] and a user input key t and height and width of the video. As per [34], if the accuracy for the computing system is 10^{-15}, then key space size becomes at least $(10^{15})^9 = 10^{135}$ for the proposed video encryption scheme which is much higher than 2^{100}. Hence, the algorithm ensures protection against brute force attacks.

3.2.2 Analysis for key sensitivity

For any small perturbation in keys the change in encrypted image is known as key sensitivity. Since the chaotic system [31] is highly sensitive in parameter values and initial conditions, therefore, the generated pseudo-random number sequences from the chaotic system will be totally different for any tiny change in these values, which will affect the encryption process and the encrypted image will be totally changed. By evaluating UACI and NPCR key sensitivity can be utilized. Considering the encrypted image C1 for original one and C2 as an encrypted image with change in key, with dimension $m \times n$. For two encrypted images of the original Lena RGB image with different keys, NPCR and UACI are calculated (Table 1) using the formula given below (Eq. (2) and Eq. (3)). To assess the key's sensitivity during the encryption process, key $w(0)$ is slightly disturbed by adding 10^{-15}. After encryption using original and disturbed keys, both encrypted images are different from each other.

Table 1
NPCR and UACI values for small perturbations in keys

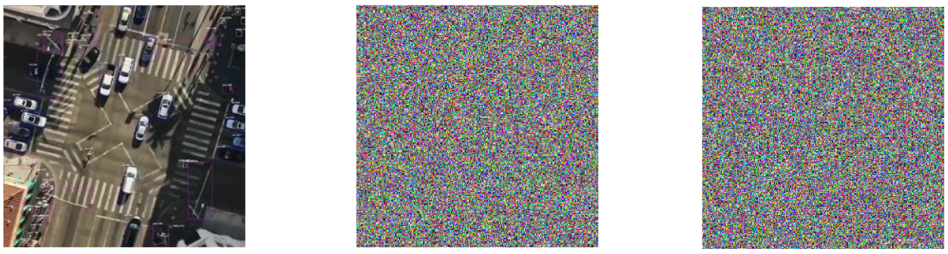
	NPCR (%)			UACI (%)		
Key handling	Red	Green	Blue	Red	Green	Blue
$w(0)$ $w(0) + 10^{-15}$	99.5987	99.6231	99.5895	33.4553	33.5743	33.4531

Figure 5 shows the different encrypted images ((b), (c)) for the keys $w(0) = 1$ and $w(0) = 1 + 10^{-15}$. To distinguish between two encrypted images NPCR and UACI are calculated. Since NPCR values are more than 99.589% and the UACI value is at least 33.453%. Therefore, for small changes in the keys, the encrypted image is totally changed. Which indicates the sensitivity of the keys in the algorithm.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100\% \tag{2}$$

$$D(i,j) = \begin{matrix} 1, C1(i,j) \neq C2(i,j) \\ 0, C1(i,j) = C2(i,j) \end{matrix}$$

$$UACI = \frac{\sum_{i,j}\big(C1(i,j) - C2(i,j)\big)}{255 \times m \times n} \tag{3}$$



(a) (b) (c)

Fig. 5. (a) The original image of frame 686 (b) Encrypted image for $w(0) = 1$, (c) Encrypted image for $w(0) = 1 + 10^{-15}$

3.2.3 Differential attack analysis

The attackers may decrypt an encrypted image by comparing it with another image which is encrypted with the same algorithm but with little change in the original one. NPCR and UACI [35] can explain the differences between two encrypted images to prevent differential attacks for any encryption scheme. An algorithm can effectively counter differential attacks when the NPCR and UACI values approach 100 and 34, respectively. The algorithm can encrypt the video by performing the encryption process in images produced from the slices, independently as an image encryption. Therefore, by using this algorithm an image also can be encrypted by utilizing the scrambling (Algorithm 2) and the diffusion (Algorithm 4) algorithms. The efficiency of the algorithm is shown by making a comparison of correlation coefficients and NPCR and UACI for differential attack with some existing image encryption algorithm for Lena RGB image. NPCR and UACI have been calculated for Lena RGB colour image of size 256×256 and those values are compared with some existing image encryption algorithms in Table 2 which confirms the efficiency of the proposed algorithm.

Table 2
NPCR and UACI values for Lena image

	NPCR (%)			UACI (%)		
	Red	Green	Blue	Red	Green	Blue
Our method	99.6246	99.6475	99.6384	33.5301	33.5017	33.5302
[18]	99.6121	99.6103	99.6182	33.4448	33.4316	33.5443
[19]	99.6094	99.6055	99.6122	33.4511	33.4850	33.5177
[22]	99.6109	99.6109	99.6375	33.4158	30.3902	33.2420
[23]	99.6254	99.6254	99.6254	33.0704	30.7620	27.8720
[29]	99.61	99.60	99.63	33.45	33.42	33.51
[30]	99.5712	99.5758	99.6094	33.1056	30.5178	27.5385

3.2.4 Histogram analysis

The histogram portrays how the grey values of the image are distributed within a specific colour channel. It shows a specific statistical pattern where the heights of pixel pics are different. The histogram plotting for the original image of frame 686 (Figure 6(a-c)) shows a pattern. But for the encrypted frame (Figure 6(d-f)) it patterns are uniform. which indicates that extracting any original image information from the encrypted one is challenging, confirming the encryption algorithm's effectiveness in preventing statistical attacks.

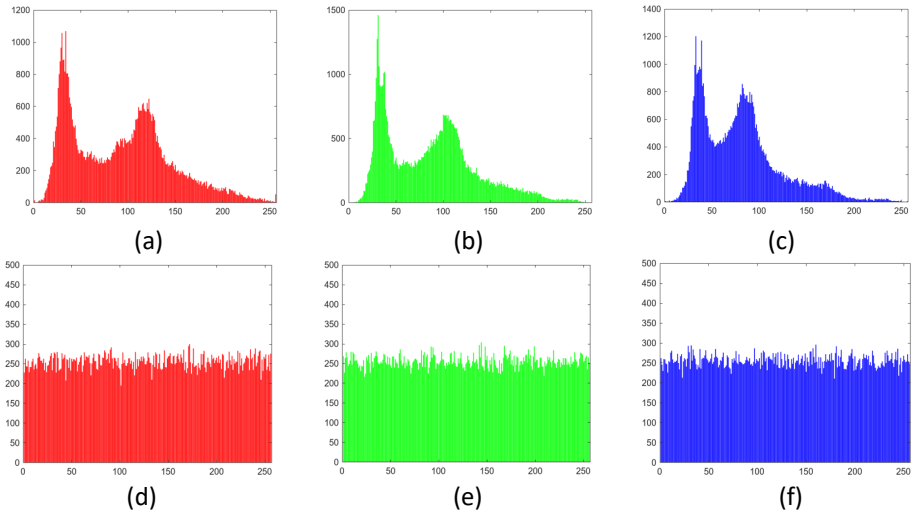


Fig. 6. Histogram of three colour panels of image frame 686 (a) - (c) and encrypted image (d) - (f)

3.2.5 Three-dimensional pixel intensity

The appearance of the video is controlled by its pixel values. For a digital video, the appearance of each point depends on the colour intensity. The intensity of the colour is nothing but the pixel values at that point for that colour channel. In three-dimensional pixel intensity plotting for the original frames of the video, there are ununiformed pick heights, but for the encrypted frames, the distribution is uniform. In Figure 7, the three-dimensional pixel intensity plots are presented for the original and encrypted image of frame 686 of the video. These diagrams confirm the algorithm's strength.

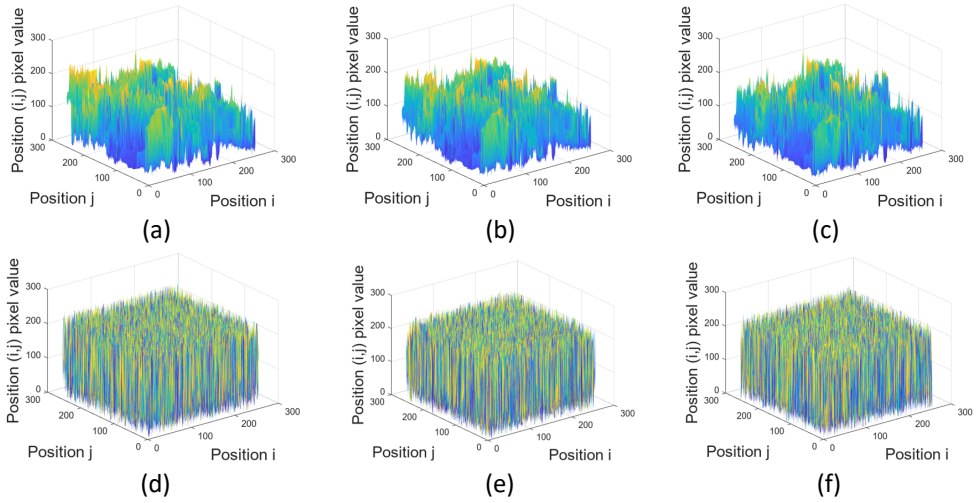


Fig. 7. Pixel intensity of colour images of frame 686, for the red channel (a) original, (d) encrypted, for green channel (b) original, (e) encrypted, for the blue channel of (c) original, (f) encrypted

3.2.6 Analysis of correlation between adjacent pixels

The values of pixels of the frames of the original video at horizontal, vertical and diagonal are highly correlated. This can be observed from the scatter plotting of the pixel values for the original image of frame 686 for three directions in Figure 8(g-i). But in order to prevent statistical attacks, it is imperative that the correlation coefficients of the encrypted frames approach zero which is observed in Figure 8(j-l) for the encrypted image of frame 686. The scatter plot is uniformly distributed all over the frame which confirms that the correlation of the adjacent pixels is almost zero. The correlation-coefficient r_{xy} [36] (Eq. (4)) between the adjacent pixels in a certain direction is defined as follows,

$$r_{xy} = \frac{cov(x,y)}{\sqrt{var(x)}\sqrt{var(y)}} \tag{4}$$

where x and y represent two adjacent pixels in that direction, $cov(x,y)$ denotes the covariance of two pixels, $var(x)$ is the variance.

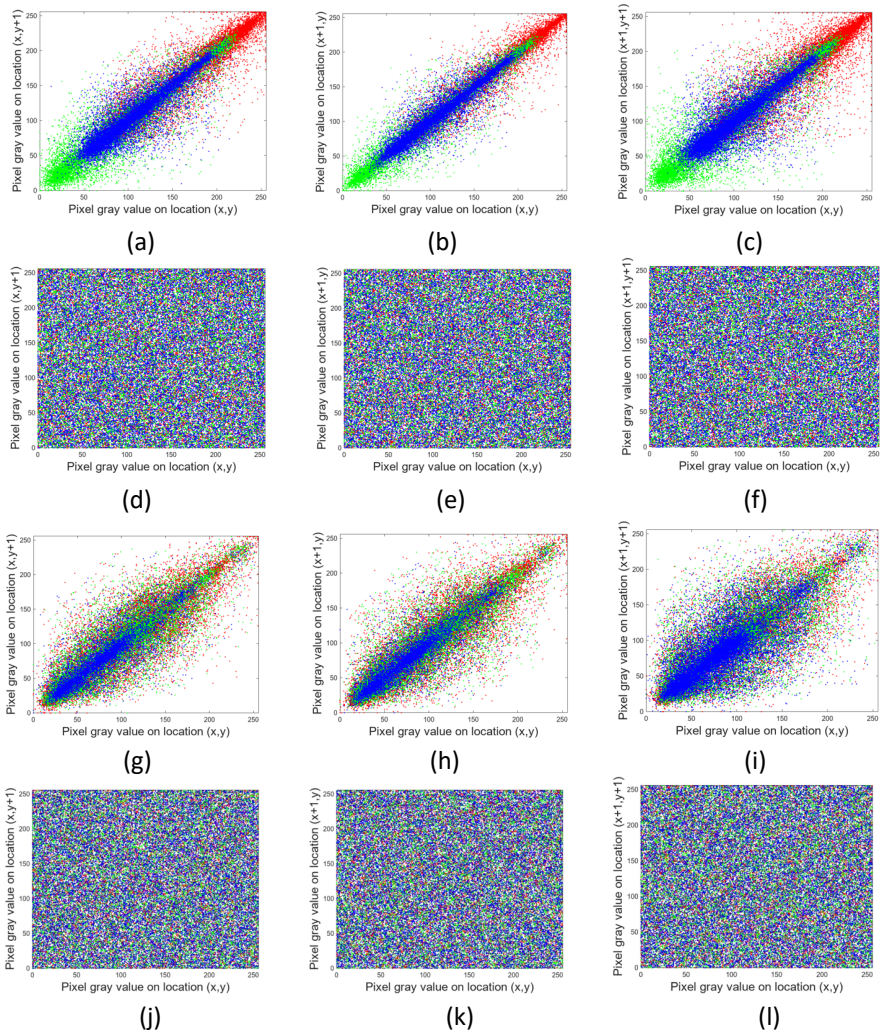


Fig. 8. Correlation plots for the original image of Lena are in (a) horizontal, (b) vertical, & (c) diagonal directions for three colour panels, the same analysis for the encrypted image is depicted in (d), (e) and (f). Correlation

plots of the image of frame 686 are in (a) horizontal, (b) vertical, and (c) diagonal directions for red green and blue colour panels, the same analysis for the encrypted image is depicted in (d), (e) and (f)

Table 3 provides a comparison of the correlation coefficients for adjacent pixels of 256×256 RGB Lena image with various established image encryption algorithms. Figure 8 presents scatter plots for both the encrypted and original Lena images.

Table 3
Correlation coefficients for Lena's original and encrypted image and comparison with other algorithms

		Horizontal	Vertical	Diagonal
Lena Original	Red	0.9474	0.9750	0.9262
	Green	0.9496	0.9758	0.9296
	Blue	0.9033	0.9507	0.8685
Our proposed method	Red	−0.00046703	−0.0003218	−0.0003281
	Green	−0.00007605	0.0002713	−0.0006954
	Blue	−0.0008137	0.0003974	−0.0006579
[18]	Red	0.0018	−0.0015	0.0011
	Green	0.0002	0.0042	−0.0015
	Blue	−0.0051	−0.0069	−0.0036
[19]	Red	−0.0048	0.0031	−0.0029
	Green	0.0016	1.5975×10^{-4}	-2.4794×10^{-4}
	Blue	0.0022	-6.4675×10^{-4}	−0.0039
[22]	Red	−0.00364	0.000697	0.00016
	Green	0.000118	−0.0011	0.00177
	Blue	−0.00164	0.006041	−0.00523
[23]	Red	0.00073	0.00311	−0.00508
	Green	−0.00054	0.00076	0.00331
	Blue	0.00147	−0.00147	0.006219
[29]	Red	0.0028	0.0019	−0.0011
	Green	−0.0001	−0.0013	0.0024
	Blue	0.0022	−00006	−0.0010
[30]	Red	0.00771152	0.00199022	−0.003263
	Green	−0.000053	−0.003507	0.0026447
	Blue	−0.000962	0.00259674	−0.004093

3.2.7 Analysis of robustness
3.2.7.1 Analysis of anti-noise attack
3.2.7.1.1 Salt and pepper noise attack

After adding Salt and pepper noise to the encrypted video, the impact on the decrypted output video is presented in Figure 9 with various noise densities for frame 686. For decrypted images, the quality gradually decreases with the increase in the salt and pepper noise density.

(a) (b) (c)

Fig. 9. Decryption after adding Salt and Pepper- noise to encrypted image, when density= (a) 0.01, (b) 0.1 and (c) 0.2 respectively

Evaluation of decrypted image quality is executed using the Peak Signal to Noise Ratio (PSNR). If P be the $H \times W$ image, D be a reference image with the same dimension, then Eq. (5) describes the mean square error (MSE) and the PSNR [37].

$$\begin{cases} MSE = \frac{1}{H \times W} \sum_{i,j} \left(P(i,j) - D(i,j) \right)^2 \\ \text{PSNR} = 10 log_{10} \frac{(2^n - 1)^2}{MSE} \end{cases} \quad (5)$$

For different densities of noise 0.001, 0.01, 0.1, and 0.2, the change in PSNR is presented in Table 4. Higher values of PSNR signify better quality of the image. For PSNR value $>$ 40 decibels (dB), the quality of the image becomes extraordinary; it shows good quality for the value within $30 - 40$ dB; image quality is poor but acceptable within the range $20-30$ dB; the quality of the image becomes undesirable for the value $<$ 20 dB.

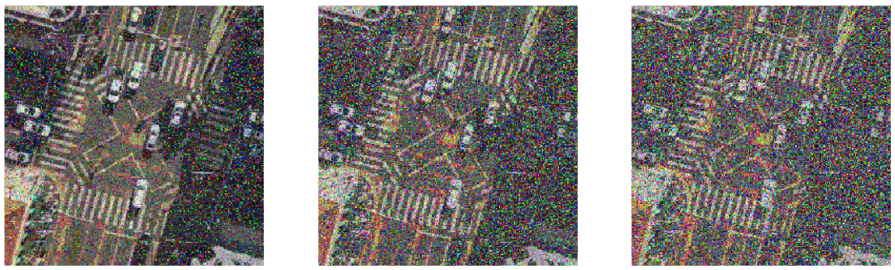
From Table 4, it is clear that when noise density is less than 0.01, the image quality under the proposed encryption scheme is acceptable.

Table 4
PSNR(dB) values with different salt and pepper noise densities

Noise density	Red	Green	Blue
$\mathbf{0.001}$	35.5452	33.6991	34.5174
$\mathbf{0.01}$	23.4838	23.4883	23.6652
$\mathbf{0.1}$	14.0453	14.001	14.1522
$\mathbf{0.2}$	11.4511	11.3788	11.4284

3.2.7.1.2 Gaussian noise attack

The effective resistance of the proposed digital video encryption algorithm against the Gaussian noise attack has been performed by decrypting the encrypted image of frame 686 with mean 0 and variances 0.001, 0.005, 0.01 (Figure 10), which ensures the recognition of the decrypted image even when subjected to such noise attacks.



(a) (b) (c)

Fig. 10. Adding Gaussian noise to encrypted image with mean = 0 and variances (a) 0.001, (b) 0.005 and (c) 0.01 respectively

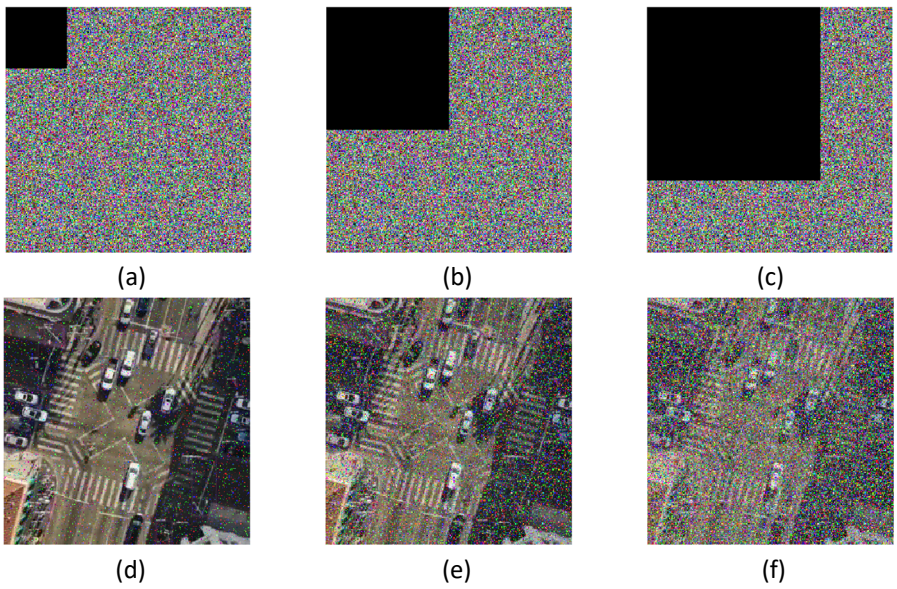
The PSNR values for each channel after decryption are presented in Table 5.

Table 5
PSNR(dB) values with different Gaussian noise variances

Variances	Red	Green	Blue
0.001	14.7629	14.8763	15.1889
0.005	12.1153	12.1745	12.3684
0.01	11.0795	11.1826	11.3096

2.7.2 Analysis of anti-clipping attack

The proposed algorithm's effectiveness in handling data loss is examined by decrypting cropped encrypted images. Specifically, the encrypted image of frame 686 is trimmed from both the upper left corner & centre. The sizes of the cropped portion in the encrypted image are 16×16, 32×32, 64×64, 128×128, 50% of the image areas. The decrypted image's quality decreases as the size of the cropped region increases, irrespective of the upper left corner (Figure 11) or from the centre (Figure 12).



(a) (b) (c)

(d) (e) (f)

Fig. 11. Cropped areas (a) 64×64, (b) 128×128, (c) 50% from the upper left corner of encrypted image, related decryption outcomes (d), (e) and (f) respectively

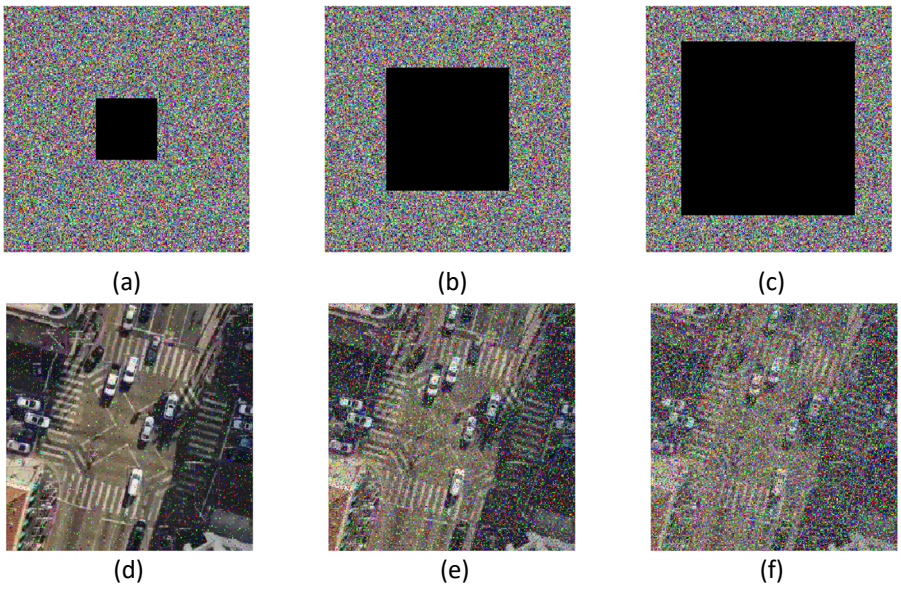


Fig. 12. Cropped areas (a) 64×64, (b) 128×128, (c) 50% from the centre of the encrypted image and related decryption outcomes (d), (e) and (f)

Decryption quality is examined by calculating PSNR values for the decrypted images, which are given in Table 6 (for cropping upper left corner) and Table 7 (for cropping in the centre). Even though 50% of image information is missing in the encrypted image the proposed decryption technique recovers the outline of the original image, illustrating the approach's capability against anti-clipping attacks.

Table 6
PSNR(dB) values after cropping (from the left upper corner) of the encrypted image

Cropped box size	Red	Green	Blue
16×16	31.9571	31.8874	31.7758
32×32	26.1273	26.1039	25.8867
64×64	20.2735	20.3387	20.3022
128×128	14.2360	14.2811	14.3012
50%	11.2778	11.2969	11.2766

Table 7
PSNR(dB) values after cropping (from the centre) of the encrypted image

Cropped box size	Red	Green	Blue
$\mathbf{16 \times 16}$	31.6569	31.7062	31.4229
$\mathbf{32 \times 32}$	26.0243	25.9889	29.7935
$\mathbf{64 \times 64}$	20.080	20.1703	20.1672
$\mathbf{128 \times 128}$	14.2510	14.2396	14.2134
$\mathbf{50\%}$	11.3041	11.2733	11.2400

4. Conclusions

This paper aims to propose a 4D chaotic map-based video encryption scheme, with real-time application. The encryption procedure incorporates the utilization of chaotic system-based scrambling and pixel diffusion. Various performance metrics, including histogram analysis, adjacent pixel correlation, UACI, NPCR, noise attack resilience, recovery of loss of data, and key space analysis, are utilized to assess the efficiency of the proposed method. The values for the correlation coefficient of the encrypted sample image are almost zero, signifying strong protection against statistical attacks. The evaluation of histograms indicates even distributions, indicating the algorithm's capacity to prevent unintended information disclosure.

The key space value reaches 10^{135}, ensuring a large value for security against a brute force attack. The NPCR value is measured at least 99.62%, and the UACI value is at least 33.50% for differential attack analysis, further indicating the efficiency of the encryption approach. Additionally, assessments involving noise attacks and cropping attacks affirm the resilience of the suggested scheme. The comparative analyses against alternative existing algorithms substantiate the enhanced effectiveness of the proposed video encryption method.

Acknowledgement
This research was not funded by any grant.

References
[1] Fang, Pengfei, Han Liu, Chengmao Wu, and Min Liu. "A survey of image encryption algorithms based on chaotic system." *The Visual Computer* 39, no. 5 (2023): 1975-2003. https://doi.org/10.1007/s00371-022-02459-5
[2] Chen, Rong, Xiaomeng Li, Lin Teng, and Xingyuan Wang. "Selective region medical image encryption algorithm based on cascade chaos and two-dimensional Joseph traversal." *Physica Scripta* 98, no. 3 (2023): 035227. https://doi.org/10.1088/1402-4896/acbcf8
[3] Chin, Wen Jun, Kai Sheng See, Yu Han Ng, Jie Ling Gan, and Sing Yee Lim. "Technologies for Indoor Noise Attenuation: A Short Review." *Progress in Energy and Environment* (2019): 1-10.
[4] Ibrahim, Muhammad Shafiq, Seri Rahayu Kamat, and Syamimi Shamsuddin. "The role of brain wave activity by electroencephalogram (EEG) in assessing cognitive skills as an indicator for driving fatigue: A review." *Malaysian Journal on Composites Science and Manufacturing* 11, no. 1 (2023): 19-31.
[5] Shameli, Kamyar, and Mariani Abdul Hamid. "Gold Nanoparticles from Plant Materials: Green Extraction, Biological Synthesis and Its Beneficials Properties for Cosmeceutical Applications." *Journal of Research in Nanoscience and Nanotechnology* 2, no. 1 (2021): 12-29. https://doi.org/10.37934/jrnn.2.1.1229
[6] Al-Khasawneh, Mahmoud Ahmad S., Muhammad Faheem, Eman A. Aldhahri, Abdulrahman Alzahrani, and Ala Abdulsalam Alarood. "A MapReduce based approach for secure batch satellite image encryption." *IEEE Access* 11 (2023): 62865-62878. https://doi.org/10.1109/ACCESS.2023.3279719
[7] Li, Hao, Zhaoquan Gu, Lianbing Deng, Yi Han, Cheng Yang, and Zhihong Tian. "A fine-grained video encryption service based on the cloud-fog-local architecture for public and private videos." *Sensors* 19, no. 24 (2019): 5366. https://doi.org/10.3390/s19245366
[8] Liang, Vernon Yeoh Sheng, Nur Irwany Ahmad, Diyya Hidayah Abd Rahman, Aimi Athirah, Hazwani Zaidi, Saidatul Shema Saad, Nazrul Azril Nazlan, Habibah Mokhtaruddin, and Baseemah Mat Jalaluddin. "Development of Solar Tracking Robot for Improving Solar Photovoltaic (PV) Module Efficiency." *Journal of Advanced Research in Applied Mechanics* 61 (2019): 13-24.
[9] Nor, Siti Rohani Mohd, Adina Najwa Kamarudin, and Nurul Aini Jaafar. "Comparison on the Student's Performances during Physical and Online Learning in Financial Mathematics Course." *International Journal of Advanced Research in Future Ready Learning and Education* 28, no. 1 (2022): 1-8.
[10] Yun, Junhyeok, and Mihui Kim. "JLVEA: Lightweight real-time video stream encryption algorithm for internet of things." *Sensors* 20, no. 13 (2020): 3627. https://doi.org/10.3390/s20133627
[11] Wahab, Osama Fouad Abdel, Ashraf AM Khalaf, Aziza I. Hussein, and Hesham FA Hamed. "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques." *IEEE access* 9 (2021): 31805-31815. https://doi.org/10.1109/ACCESS.2021.3060317

[12] Zhang, Lingyu, and Deyuan Chen. "The large capacity embedding algorithm for H. 264/AVC intra-prediction mode video steganography based on linear block code over Z4." *Multimedia Tools and Applications* 79 (2020): 12659-12677. https://doi.org/10.1007/s11042-019-08528-7
[13] Alhasany, Rose M., and Lahieb M. Jawad. "A new technique for determining region of interest in selective video protection approach." *Iraqi Journal of Information and Communication Technology* 4, no. 2 (2021): 33-49. https://doi.org/10.31987/ijict.4.2.135
[14] Chen, Chen, Xingjun Wang, Guanze Huang, and Guining Liu. "An efficient video encryption algorithm based on the pseudorandom number generator of zipf distribution." *Security and Communication Networks* 2022 (2022). https://doi.org/10.1155/2022/1415505
[15] Ghosh, Indranil, Md Sazzad Hossien Chowdhury, and Suazlan Mt Aznam. "Numerical treatment on a chaos model of fluid flow using new iterative method." *Journal of Advanced Research in Fluid Mechanics and Thermal Sciences* 96, no. 1 (2022): 25-35. https://doi.org/10.37934/arfmts.96.1.2535
[16] Senin, Nor Halawati, Nor Fadzillah Mohd Mokhtar, and Mohamad Hasan Abdul Sathar. "Chaotic convection in a ferrofluid with internal heat generation." *CFD Letters* 12, no. 10 (2020): 62-74. https://doi.org/10.37934/cfdl.12.10.6274
[17] Arif, Jameel, Muazzam A. Khan, Baraq Ghaleb, Jawad Ahmad, Arslan Munir, Umer Rashid, and Ahmed Y. Al-Dubai. "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution." *IEEE Access* 10 (2022): 12966-12982. https://doi.org/10.1109/ACCESS.2022.3146792
[18] Chen, Xiaoyang, Jun Mou, Yinghong Cao, Huizhen Yan, and Hadi Jahanshahi. "A chaotic color image encryption scheme based on improved Arnold scrambling and dynamic DNA encoding." *Multimedia Tools and Applications* 82, no. 28 (2023): 43797-43818. https://doi.org/10.1007/s11042-023-14826-y
[19] Liu, Jia, Haiping Chang, Weiyu Ran, and Erfu Wang. "Research on Improved DNA Coding and Multidirectional Diffusion Image Encryption Algorithm." *Entropy* 25, no. 5 (2023): 746. https://doi.org/10.3390/e25050746
[20] Wang, Xingyuan, Yining Su, Chao Luo, and Chunpeng Wang. "A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling." *Plos one* 15, no. 7 (2020): e0236015. https://doi.org/10.1371/journal.pone.0236015
[21] Rahman, Zain-Aldeen SA, Basil H. Jasim, Yasir IA Al-Yasir, and Raed A. Abd-Alhameed. "High-security image encryption based on a novel simple fractional-order memristive chaotic system with a single unstable equilibrium point." *Electronics* 10, no. 24 (2021): 3130. https://doi.org/10.3390/electronics10243130
[22] Alexan, Wassim, Mohamed ElBeltagy, and Amr Aboshousha. "Rgb image encryption through cellular automata, s-box and the lorenz system." *Symmetry* 14, no. 3 (2022): 443. https://doi.org/10.3390/sym14030443
[23] Alexan, Wassim, Marwa Elkandoz, Maggie Mashaly, Eman Azab, and Amr Aboshousha. "Color image encryption through chaos and kaa map." *IEEE Access* 11 (2023): 11541-11554. https://doi.org/10.1109/ACCESS.2023.3242311
[24] Alharbi, Sarah, Amr Elsonbaty, A. A. Elsadany, and Fatma Kamal. "Nonlinear dynamics in the coupled fractional-order memristor chaotic system and its application in image encryption." *Mathematical Problems in Engineering* 2023 (2023). https://doi.org/10.1155/2023/8994299
[25] Liu, Bo, Jiandong Liu, Shuhong Wang, Ming Zhong, Bo Li, and Yujie Liu. "Hevc video encryption algorithm based on integer dynamic coupling tent mapping." *Journal of Advanced Computational Intelligence and Intelligent Informatics* 24, no. 3 (2020): 335-345. https://doi.org/10.20965/jaciii.2020.p0335
[26] Benrhouma, Oussama, Ahmad B. Alkhodre, Ali AlZahrani, Abdallah Namoun, and Wasim A. Bhat. "Using singular value decomposition and chaotic maps for selective encryption of video feeds in smart traffic management." *Applied Sciences* 12, no. 8 (2022): 3917. https://doi.org/10.3390/app12083917
[27] El-Mowafy, M. A., Sawsan Morkos Gharghory, M. A. Abo-Elsoud, M. Obayya, and MI Fath Allah. "Chaos based encryption technique for compressed h264/avc videos." *IEEE Access* 10 (2022): 124002-124016. https://doi.org/10.1109/ACCESS.2022.3223355
[28] El-den, B. M., Walid A. Raslan, and Ahmed A. Abdullah. "Even symmetric chaotic and skewed maps as a technique in video encryption." *EURASIP Journal on Advances in Signal Processing* 2023, no. 1 (2023): 40. https://doi.org/10.1186/s13634-023-01003-4
[29] Man, Xinpeng, and Yinglei Song. "Encryption of Color Images with an evolutionary framework controlled by chaotic systems." *Entropy* 25, no. 4 (2023): 631. https://doi.org/10.3390/e25040631
[30] Alexan, Wassim, Nader Alexan, and Mohamed Gabr. "Multiple-layer image encryption utilizing fractional-order chen hyperchaotic map and cryptographically secure prngs." *Fractal and Fractional* 7, no. 4 (2023): 287. https://doi.org/10.3390/fractalfract7040287
[31] Das, Parnab, Nune Pratyusha, and Santanu Mandal. "New 4D Chaotic System with Infinite Equilibrium and Secure Colour Image Encryption." In *2023 5th International Conference on Energy, Power and Environment: Towards Flexible Green Energy Technologies (ICEPE)*, pp. 1-5. IEEE, 2023. https://doi.org/10.1109/ICEPE57949.2023.10201626

[32] Mishra, Mina, and V. H. Mankar. "A Chaotic encryption algorithm: Robustness against Brute-force attack." In *Advances in Computer Science, Engineering & Applications: Proceedings of the Second International Conference on Computer Science, Engineering & Applications (ICCSEA 2012), May 25-27, 2012, New Delhi, India. Volume 2*, pp. 169-179. Springer Berlin Heidelberg, 2012. https://doi.org/10.1007/978-3-642-30111-7_17

[33] Alvarez, Gonzalo, and Shujun Li. "Cryptographic requirements for chaotic secure communications." *arXiv preprint nlin/0311039* (2003).

[34] Lambić, Dragan. "Cryptanalyzing a novel pseudorandom number generator based on pseudorandomly enhanced logistic map." *Nonlinear Dynamics* 89, no. 3 (2017): 2255-2257. https://doi.org/10.1007/s11071-017-3583-1

[35] Mohammad,Siti Nurul Hatikah and Arif Mandangan. "Colour Image Encryption and Decryption using Arnold's Cat Map and Henon Map." *International Journal of Advanced Research in Computational Thinking and Data Science* 1, no. 1 (2024): 41-52. https://semarakilmu.com.my/journals/index.php/CTDS/article/view/8986

[36] Wang, Xingyuan, Xiaomeng Qin, and Chuanming Liu. "Color image encryption algorithm based on customized globally coupled map lattices." *Multimedia Tools and Applications* 78, no. 5 (2019): 6191-6209. https://doi.org/10.1007/s11042-018-6326-5

[37] El-Khamy, Said E, Noha O Korany and Marwa H El-Sherif. "Chaos based secure image hiding in variable bit rate CELP speech coding systems." *Journal of Advanced Research in Computing and Applications* 8, no. 1 (2017): 15-21. https://www.akademiabaru.com/submit/index.php/arca/article/view/5045