Journal of Computer Science

Original Research Paper

Discrete Hyperchaotic S-Box Generation for Selective Video Frames Encryption

Megala G. and Swarnalatha P.

School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Article history
Received: 23-11-2022
Revised: 25-03-2023
Accepted: 27-03-2023

Corresponding Author:
Swarnalatha P.
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India
Email: pswarnalatha@vit.ac.in

Abstract: Cloud computing has become a significant technology with rapid popularization offering many services with highly effective computation and large-scale storage solutions. As multimedia files are growing explosively, securely storing them for authorized access is a major task. Concentrating on video file storage in a public cloud environment, the security and privacy of those outsourced videos are the major concerns. A selective frame encryption approach is proposed to encrypt the semantic elements of the selected frames of High Efficiency Video Coding (HEVC) compressed videos by storing them in the cloud. The semantic elements of HEVC videos are extracted and encrypted by a modified Advanced Encryption Standard (AES) operation in CFB mode with a Substitution-Box (S-Box). A dynamic, nonlinear 2D discrete hyperchaotic mapping-based S-box generation method is proposed to enhance security by providing good confusion, diffusion, and scrambling. The performance analysis of generated S-box and experimental results show that the proposed selective encryption highly resists attacks and encrypts with reduced time complexity.

Keywords: Discrete Hyperchaotic Mapping, Nonlinear S-Box, Selective Encryption, Semantic Elements

Introduction

The cloud environment is grown enormously with numerous services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and security as a service. Several approaches to cloud technology and cloud services have reached a tremendous progression of computational clouds with constrained resources. Cloud users store their sensitive confidential information on cloud servers. Conventional encryption techniques are used for securing the outsourced media files to the cloud. The traditional encryption methods such as DES and AES (Awan *et al*., 2020) need to be enhanced to deal with current emerging security threats. The major tasks of deploying computational cloud services are to enhance security, reduce the utilization of resources and minimize delay. Though many traditional encryption standards are developed still there exist security issues and privacy concerns.

Encrypting a video is a time consuming process as a video file consists of a huge amount of information. Video encryption can either be performed as full (Naïve) encryption or selective encryption. The video files comprising smaller sizes can be encrypted completely which is known as full (Naïve) encryption. The more informative semantic elements of the video are intra prediction mode, inter prediction mode, non-zero coefficients of the Intra coded (I) frame in addition to the Predicted (P) frame, Motion Vector (MV), Motion Vector Difference (MVD) of macroblocks, Quantization Parameters difference (QP) and the residual coefficients. The larger sized videos can be selectively encrypted by extracting the semantic elements and encrypting them. The primary goal of video encryption is that it must satisfy the necessary conditions such as less computation complexity, less cost in time, no format compliance, and should not influence compression efficiency. Many existing techniques (Megala, 2021a) consume more time to encrypt/decrypt data blocks and there exists less security in stream ciphers. Shah *et al.* (2020) encrypted syntax elements of the HEVC videos and very high concern selectively. Though this method protects the visual contents, it is not suitable for real-time applications and there is a need for security enhancement. He *et al.* (2020) selectively encrypted the non-zero coefficients of DCT sign bits but it does not resist differential attack.

Zhang *et al*. (2018) deployed a lightweight encryption approach to secure the surveillance videos. The Region of Interest (RoI) contents of those surveillance videos are protected by applying cellular automata layered approach.

From the Group of Pictures (GoP) of video, the ROI of the I frame is alone encrypted and so there is leakage of data, and is vulnerable to attack. Ma *et al*. (2015) have also protected the ROI of Advanced Video Coding (AVC)/H.264 compressed videos. Due to the quantization process, the privacy content is distorted during encoding. Shah *et al*. (2019) have performed transcoding and decoding of video using XOR operation to encrypt and have not concentrated on syntax elements and rate distortion quality is not analyzed. A DNA-based encryption scheme is proposed by Namasudra *et al*. (2020) to encrypt the multimedia files uploaded to the cloud environment but the computation cost and latency are high. Kermani and Azarderakhsh (2018) discussed the GCM functionality to check the integrity of the information which are being encrypted. 128-bit block ciphers are authenticated using Galois Field (GF) finite multipliers. S-box, being one of the cryptographic core components, is vital in block ciphers and has been widely utilized in cryptographic standards such as DES and AES. Recent research indicates that using the nonlinear nature of chaos to create S-boxes is a fresh and interesting avenue. No other S-boxes relying on chaos come close to matching the excellent performance of the one employed in AES. There is still a significant performance gap between chaos-based S-boxes and traditional ones. Therefore, more development is required to enhance the functionality of chaos-based S-boxes. Using the chaotic maps' inherent random distribution property, chaos-based algorithms often produce robust S-boxes.

The major contribution of this study is to enhance video security by applying the proposed selective frame encryption, where the Pseudo Random Number Generator (PRNG) is used to generate the key; then AES in Cipher Feedback (CFB) mode is applied on the extracted MVD, IPM, QP elements to encrypt it. A modified 2D discrete hyperchaotic algorithm is proposed to generate an Substitution box (S-box) dynamically in AES-CFB operation to strengthen the security of video encryption by increasing nonlinearity and decreasing differential probability. Security of the Advanced Encryption Standard (AES) is enhanced by modifying the AES by using chaotic maps for substitution box generation and the speed of the encryption process is increased.

A selective video encryption scheme encrypts only a fraction of the video. Selective encryption is performed to minimize the computational overhead during the encryption process of an H.264 compressed video. Encoders are used to encode the syntax elements of the video. HEVC encoders use a quad tree structure of block partitioning (Megala, 2021b) with large inter/intra prediction blocks, efficient coding architecture, and high bit depth. HEVC encoder uses Context Adaptive Binary Arithmetic Coding (CABAC) encoding. It involves mainly three functions such as binarization step, context modeling, and arithmetic coding. In binarization, all the non-binary semantic elements of the video are transformed into binary symbols or strings (bin). The probabilities of bins are updated during the context modeling phase. Based on these probabilities, the bins are compressed into bits. During arithmetic coding, based on the estimated probability, bins are compressed to bits in two different modes such as regular mode or bypass mode. In regular mode, the probability is selected from the content based on previously encoded syntax elements whereas, in bypass mode, the fixed probability is used. The selective encryption is performed by using the bypass mode (Malladar and Kunte, 2021), ensuring format compliance and maintaining the bit rate of HEVC-encoded videos.

Non-zero coefficients and sign bits of Quantized Transform Coefficients (QTC) are encrypted using stream cipher by performing XOR operation among plaintext and PRNG secret bits. The most important part of video construction is the Motion Vector (MV). It is often detected by using block matching algorithms. Instead of encrypting MV, the signs and magnitude of Motion Vector Difference (MVD) are coded in bypass mode and encrypted. The suffix value of the MVDs is XORed with the pseudorandom bits. Encrypting sign bits of QTC, MVD, and absolute suffix value of MVD bins in bypass mode ensures the format compatibility of the video and thus maintains the structure of the video in achieving the same bit rate. In HEVC encoding, the first two bins are encoded in regular mode and the remaining is encoded in bypass mode by employing Golomb rice and Exponential-Golomb (Exp-Golomb) for small values and large values respectively. Hong and Han (2014) extracted the MV and encrypted it with the RC4 stream cipher approach which has format compliance and increases in bits. In the early days, researchers focussed to extract the key frame information by video cut detection techniques and video analysis techniques. Mostly histogram comparison, pixel-wise comparison, ROI comparison, edge comparison, and threshold comparison are preferred to choose the keyframe, fragment it and then perform encryption. Later the recent works on selective encryption are focussed on detecting the key transitions and performing encryption techniques. Table 1 represents various encryption schemes.

The encryption technique provides the confidentiality of the outsourced data to the public clouds and protects the data from adversaries by applying distinct numerical systems and symmetric/asymmetric keys to transform digital information into meaningless ciphertext. The objective of security management is to provide data confidentiality, authentication of users/devices, integrity, and accuracy. Moreover, video based as well as image-based files require more time and power consumption for encryption as well as decryption.

Table 1: Summary of encryption schemes

Reference	Approach	Keyspace analysis	Comments
Liu and Kadir (2015)	Hash function	2^{512}	High computational cost
Jolfaei *et al*. (2012)	Stream cipher	2^{256}	Vulnerable to security attacks such as differential and statistical attacks
Lima *et al*. (2015)	Cos functional transformation	2^{160}	It is not dependent on keys generated
Kumar and Rana (2016)	Block cipher approach	2^{320}	Possibility of differential attacks due to a small number of round involved
Dong (2015)	DNA approach	2^{256}	Non-linear implementation leads to high computational complexity

Traditional Encryption Algorithm

Although it is recognized that statistics multimedia security gives extra protection and confinement, the concerns raised are due to vulnerable access to customer records. There are many security issues related to customers' data. Traditional encryption offers confidentiality, but it is not well suited for multimedia security. In recent encryption methods, users exclusively encrypt their data with their keys providing increased security. This involves the following steps.

Key_gen: Is the key generation procedure, which creates key *k* using PRNG or chaos parameters.

Encrypt (*k*, *pt*): Is the encryption procedure that encrypts or translates the plain text, *pt* with the help of key *k* and then generates the cipher text, *ct* in unreadable form.

Decrypt (*k*, *ct*): This is the decryption procedure that decrypts the cipher text, *ct* into plain text, *pt* of original form with the help of the same key *k*.

Tag_gen (*M*): Is the tag generation algorithm that outputs a tag value *T* for the message *M* which is useful to check the integrity of *M*.

The Advanced Encryption Standard (AES) algorithm is based on the principles of substitution and permutation. AES reads 128-bit sized plaintext chunks and encrypts them using various sizes of keys 128, 192, or 256 bits for 10, 12, or 14 rounds of operation respectively. This plaintext is replicated to the state array that is updated in each round and at the last phase, it is copied to the output. Each round performs mainly four different operations such as substitution bytes (S-box), shift rows, mix columns, and add round keys. These are the 4 stages of round transformations involving one permutation and three substitution functions. Initially, encryption begins with one add round key operation using the key. Add round key performs bitwise XOR of the current block with 4 words of an expanded key. The substitute byte stage uses a substitution box (S-box) to perform the substitution of bits in a block. Following a simple permutation in the shift rows stage is performed. The output of this stage is then passed to the mix column, substitution is performed using arithmetic multiplication over GF(2^8). These 4 stages of operations are performed for *n*-1 rounds and then the mix column is eliminated in the n^{th} round. All the stages provide confusion, diffusion, and nonlinearity and so it is secure. All these stages are reversible and so the decryption uses an expanded key in reverse order.

AES encryption algorithm can be implemented in four different modes of operation Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Counter (CTR) mode. In this study, the CFB method is preferred to encrypt the video fragments in a bit sliced approach. The same bit rate is accurately maintained by CFB and produces format compatibility. CFB mode divides the plaintext, *pt* into *k*-bit segments rather than *m* (128) bits. An Initialization Vector (IV) is initialized which is the m-bit shift register. It is similar to the stream cipher approach (Megala and Swarnalatha, 2022). The leftmost Most Significant Bit (MSB) is *k* bits of encryption function output which is being XORed together with the initial part of plaintext pt_1 towards generating ciphertext ct_1 and is transmitted. Meanwhile, the content of the shift register is moved towards the left for the *k* number of bit positions and ct_1 is restored in the rightmost Least Significant Bit (LSB) of *k* bits in the shift register. This procedure is repeated till the entire plaintext blocks are encrypted. The input register is renewed one block at a time with a feedback structure. CFB produces output depending on both plaintext and ciphertext. AES algorithm combined with GCM (Gueron and Kounavis, 2010) is motivating fast processing networks with high security in performance. It generates a 128-bit digest (hash) value from the encrypted blocks.

Chaotic Maps and Bijective Function

A chaotic system, a mathematical model consisting of more than one positive Lyapunov Exponent (LE) is said to be hyperchaotic. Hyperchaos is the new class of attractors raised with 4 dimensions as a minimum. This hyperchaotic attractor has at least two positives LE showing chaotic behavior and one negative LE ensuring the boundness of the solution. These hyperchaotic systems have complex algebraic structures which further makes it difficult to obtain the bounds. A new state variable can be introduced to the 2-D chaotic system to make a simple hyperchaotic system. The dynamic complex behavior of chaotic systems can be applied in the field of dynamics, cryptosystems, circuits, engineering, biochemical responses, stock exchanges, etc. Researchers have concentrated more on using hyperchaos behavior to increase nonlinearity.

Cheng *et al*. (2020) employed a 4D hyperchaotic system, where the extracted syntax elements from each slice of video are first encrypted with the keys generated by PRNG. These encrypted elements are then inputted into the 4D hyperchaotic system performing DNA code selection and random matrix coding in the codeword substitution phase. Seven reference sequences from the group of pictures consisting of 300 frames are encrypted perceptually with four different sequences generated by the chaos system. Chaos-based multimedia encryption proposed by Yasser *et al*. (2020) with perturbation technique is included in all chaotic maps based on a Linear Feedback Shift Register (LFSR) consisting of 16 units where each of the units has 31 bits. Sallam *et al*. (2018) encrypted the MVD sign bits and DCT coefficients with a chaotic logistic map. 2D logistic maps use high computational costs. Qiao *et al*. (2020) paired the Chebyshev discrete chaos map and skew tent map to create a random sequence for introducing more confusion in S-box. Hamming distance and correlation analysis are measured to evaluate the confusion and diffusion property in image encryption. Silva-García *et al*. (2018) suggested a simple 1D chaos-based image encryption but the generated S-box is weak due to less nonlinearity and hence does not resist linear attack. Logistic sine chaotic maps are combined with DNA sequence-based permutation to encrypt the image (Chai *et al*., 2019). Though the proposed scheme generates a DNA matrix and performs an XOR operation to resist the known attacks, it does not provide high nonlinearity with good diffusion.

An image encryption scheme is the foundation of video encryption techniques where the encryption is done in a frame-by-frame manner. Some authors have used the chaotic map directly on the image to encrypt it. Based on the chaotic map, large pseudo random bit sequences are generated and then an XOR operation is performed on these bit sequences and the plain text stream to encrypt them. Valli and Ganesan (2017) implemented a pipeline for encrypting videos using an S-box with a high dimension of chaos and delay in the differential equation. But there exists key complexity and more time complexity for encryption. Xu *et al*. (2020) proposed an S-box generation using combined chaos algorithms. It is then optimized based on the genetic algorithm involving mutation and crossover stages. Hussain *et al*. (2019) constructed the substitution box based on Mobius transformation and logistic map providing nonlinearity to resist known attacks. Malik *et al*. (2020) have developed a dynamic S-box using a simples logistic chaotic map and the resulting S-box is then combined with affine transformation to perform rotational operations during key scheduling to increase the nonlinearity. The proposed work enhanced the AES security but with limited S-boxes. Hamidouche *et al*. (2017); Taha *et al*. (2017) have deployed a skew tent combined with a piecewise linear chaos map to generate a pseudo random sequence generator and encrypt the syntax elements of the video in block cipher and stream cipher approach respectively, but the computational cost was high.

Materials and Methods

A secure cloud framework is designed where the videos uploaded by the data owner or cloud user are secured in a block cipher feedback mode and stored. Video is represented as a group of pictures consisting of *I* frames, *B* frames, and *P* frames. The outsourced video data is first fragmented into several fragments and then each fragment is encrypted using the key pair generated at the owner side using modified Advanced Encryption Standard (AES). The existing approach of fragment then encrypting provides security but there is an increased risk of data loss. A 2D discrete hyperchaotic map-based dynamic S-box generation is proposed to perform selective frame encryption of video. The proposed framework for enhancing the secured storage of videos in the cloud is shown in Fig. 1. During the initial phase of AES encryption, the plaintext is XORed with the initialization vector used to generate the first ciphertext block of 128 bits. The current plaintext block is XORed with the ciphertext of the previous block and is performed to generate a new ciphertext block in the cipher block chain (CFB) mode of AES operation.

The process of selective frame video encryption is described in the following steps:

Step 1: Data owner uploads the video files for secured storage with protected access. This outsourced video file is fragmented into many fragments in frames in temporal and spatial frame space. The video file is passed to the fragmentation module with the parameters such as target_file_path, number_of_fragments, and output_location performs motion-based fragmentation which then produces sequential fragments with sequence ID

Step 2: I frame in the video are extracted using the Non-DCT algorithm (Megala, 2021b). Semantic elements of the *I* frames in a video such as codewords of Inter/Intra Prediction Mode (IPM), Moving Vector Difference (MVD), and signs of residual coefficients are extracted from these fragments using context adaptive binary arithmetic coding

Step 3: 2-Dimensional hyperchaotic operation is performed on the binary strings involving permutation and diffusion functions

Step 4: Chaotic mapping is performed to generate an adaptive encryption key generation and thus generates a chaotic sequence of S-box

Step 5: Cipher Feedback (CFB) mode of AES with the adaptive dynamic key is used to encrypt each slice and Galois Counter Mode (GCM) for the authentication code is used to preserve the integrity

Step 6: Objective video quality analysis is performed by measuring Peak Signal Noise Ratio (PSNR), Structural Similarity Index (SSIM), and information entropy value

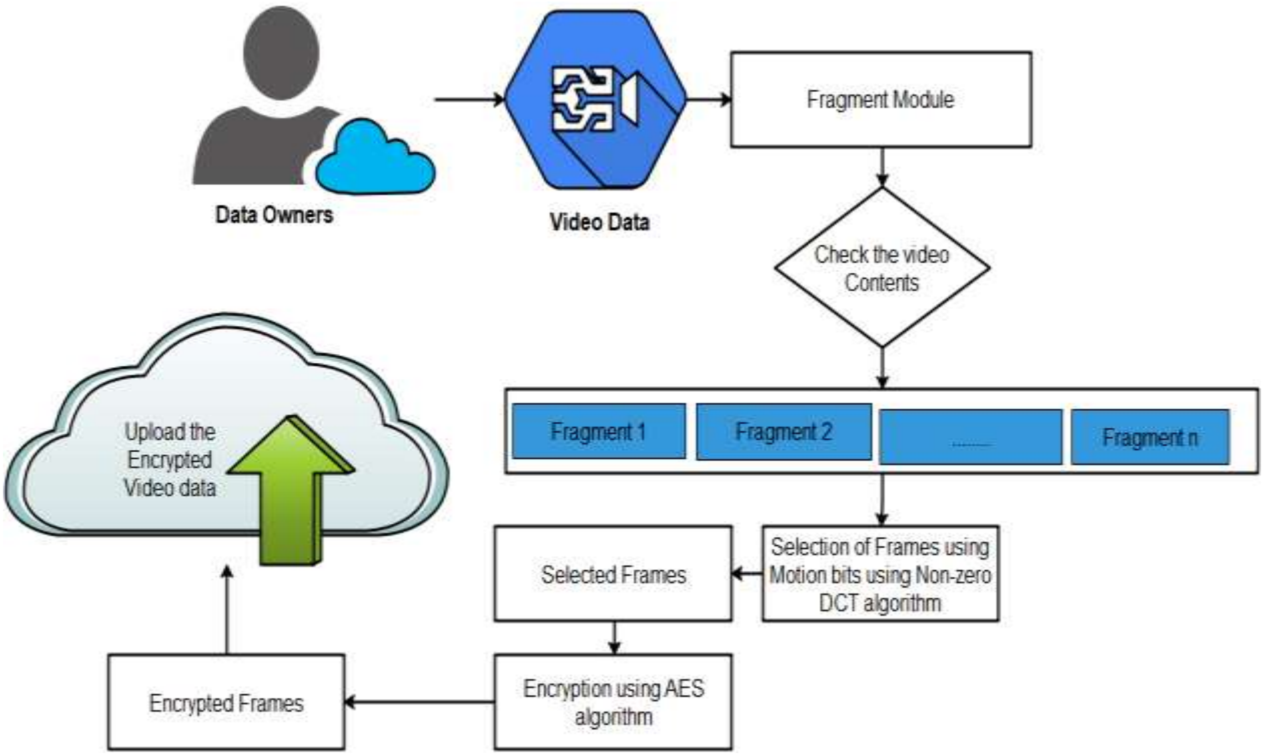


Fig. 1: Proposed framework of selective encryption

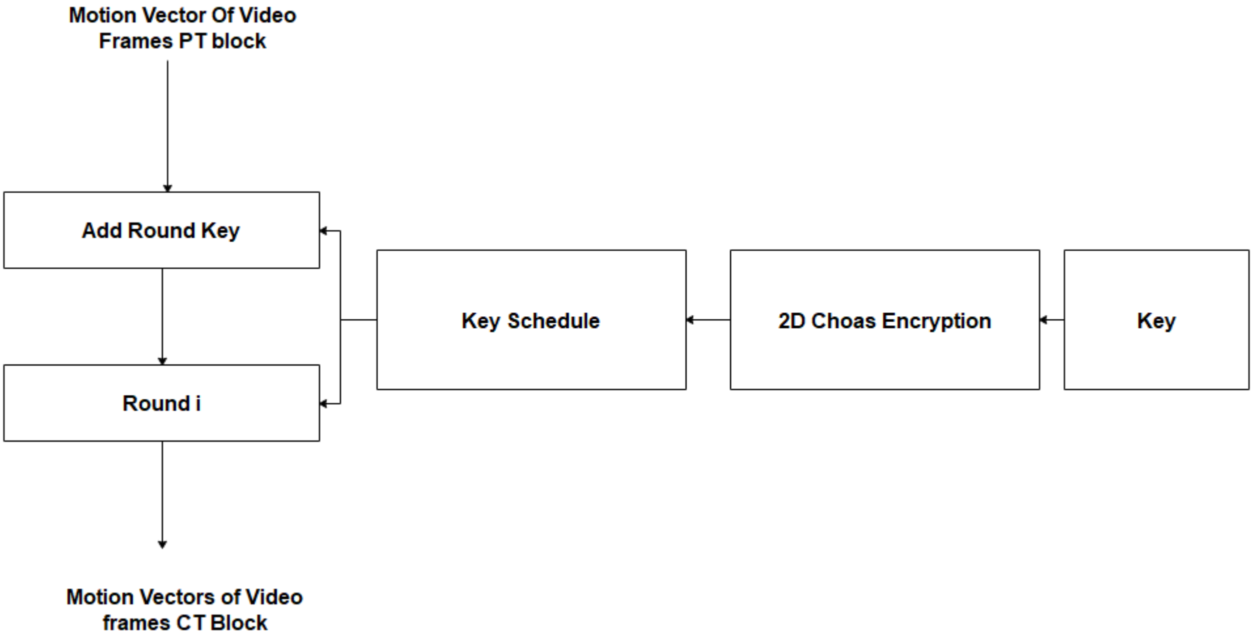

Motion Vector Of Video Frames PT block
Add Round Key
Round i
Key Schedule
2D Choas Encryption
Key
Motion Vectors of Video frames CT Block

Fig. 2: Modified AES encryption algorithm

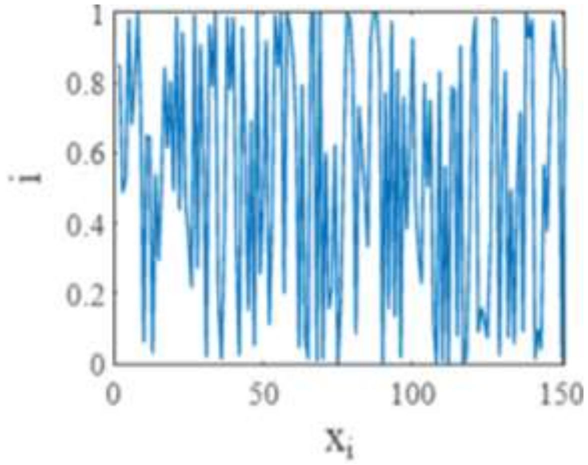


Fig. 3: Modified sine chaotic map

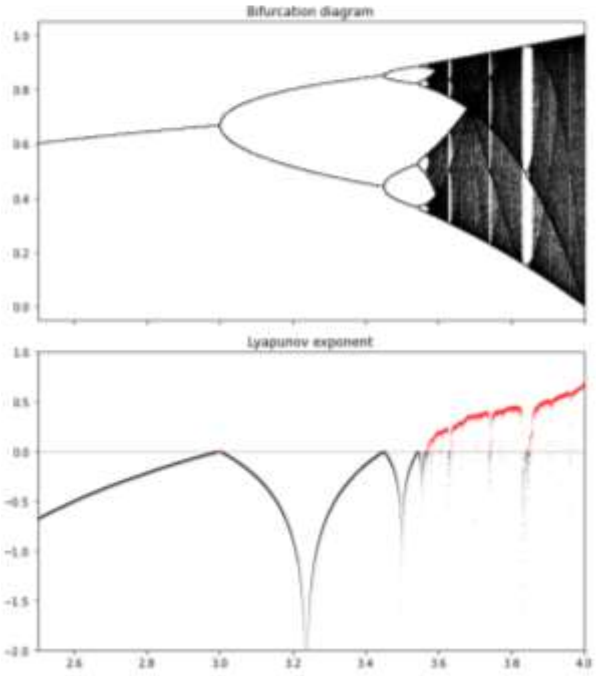


Fig. 4: Bifurcation diagram and lyapunov exponent of the chaotic map

AES algorithm in the Cipher Feedback (CFB) mode of operation is applied to selectively encrypt the extracted syntax elements. As the S-box in AES is vulnerable to a timing attack, a modified dynamic S-box is generated using 2D discrete hyperchaotic mapping. Modified S-box uses Chaos signals that are dynamic which poses a good characteristic of pseudorandom sequence. Also, it is highly complex, nonlinear, and unpredictable with good randomness. Figure 2 shows the modified AES encryption algorithm.

The key scheduling process involved in the system creates and arranges all session keys for encryption and decryption. The key space of a traditional key scheduling technique based on 2D cubes is insufficient to withstand attacks and is easily exploitable. A key schedule process is introduced to expand the smaller master key to a larger expanded key for encryption and decryption. Further, Substitute byte operation in AES involves a chaos-based S-box that processes hyperchaotic behavior. The proposed modified AES with a 2D-discrete hyperchaotic system has been simulated and tested with different parameters.

Figure 3 illustrates the generated modified chaotic map. Figure. 4 represents the bifurcation diagram of the chaotic map and the lyapunov exponent of the discrete hyperchaotic map.

S-Box Generation Algorithm

The algorithm to create a dynamic nonlinear S-box involved in AES is outlined as follows:

Algorithm 1: Dynamic S-box generation

Step 1: Initialize the parameters of the 2D discrete hyperchaotic map such as control parameter, $r = [0.904,1]$, constant $a = 3$, $x_0 = 0.11$, and $y_0 = 0.14$.

Step 2: Iterate the map and generate chaotic sequences *xi* and *yi* based on the defined mapping Equations:

$$x_i = r\left(\sin(\pi y_{i-1}) + a\right).x_{i-1}\left(1 - x_{i-1}\right)$$

$$y_i = r\left(\sin(\pi x_i) + a\right).y_{i-1}\left(1 - y_{i-1}\right)$$

where, r is the control parameter that shows the hyperchaotic actions while its value remains in a range of [0.904,1].

Step 3: Generate a random sequence (p_i) between 0 to 255 to match the length of the S-box by converting *xi*.

$$p_i = floor(x_i \times 10^6)\, mod\, 256$$

Step 4: Sort the sequence y_i and make a note of its location as an index sequence (Q).

Step 5: Select the value in P that corresponds to Q and make sure it already appears in the S-box. If not, insert the P-value to the S-box until its length (256) gets filled with unrepeated values. 1024 S-boxes are randomly generated.

Step 6: Scramble the generated S-box.

Step 7: Return the final S-box

Hence S-box is generated based on the above mentioned steps and is nonlinear and highly efficient. The strength of the AES cryptographic algorithm depends on the strong S-box that resists known attacks. The S-box is reversible and hence during the decryption process, inverse the of the S-box is applied with inverse diffusion and inverse scrambling. The S-box strengths are analyzed which depend on algebraic structure nonlinearity, bijective, Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), linear probability, and linear cryptanalysis and differential cryptanalysis. There are 1024 boxes generated with 112 non-linearity. Therefore, more randomness is produced from the nonlinear S-box.

The integrity of the block transmitted is verified using Galois Counter Mode (GCM) which is parallelizable providing high throughput with less latency and low cost. GCM is used for authenticated encryption in a stream ciphering approach. GCM involves two functions namely, GHASH and CTR function to check the integrity. As the proposed framework uses the CFB block cipher mode of modified chaos-based AES, the GCM uses only the GHASH function (Méloni *et al.*, 2010) to include an authentication tag for the transmitted data. GHASH takes input plaintext (*pt*) as a 128-bit string, and hash key and then performs XOR operation (modulo-2 addition) also multiplication in Galois field. It outputs a 128-bit sized tag which is appended to the ciphertext. At the receiver end, this received tag can be used to check whether the data received is tampered with or not by comparing it with a newly computed tag using the same GHASH function.

Let pt_1, pt_2, $pt_3 \ldots pt_m$ denote the unique block sequences such that:

$$pt = pt_1 \| pt_2 \| pt_3 \| \ldots \| pt_m \tag{1}$$

Let, t_0 be a block of 128 zeros. For all values of $i = 1$ to m, compute the tag as:

$$t_i = \left(t_{i-1} \oplus pt_i\right).H \tag{2}$$

where, H is the hash key. This then returns the t_m tag value which is appended to the cipher block.

GCM constructs error detection to prove authenticity. If the output of the block cipher is incorrect, the associated tag derived using that information results in an inaccurate tag. If the GHASH function is broken, the ciphertext will be accurate but the tag will be incorrect, resulting in authentication failure. An incorrect ciphertext and tag are generated for the unrelated outputs. GCM is applied in a parallel fashion for q times of add-multiplication. For m number of data blocks, added authenticated blocks are combined with the encrypted blocks. GHASH function Hq is applied where $\log_2 q$ times the multiplication is performed which reduces the complexity in construction. Thus, the selective frame encryption and authentication to verify integrity are performed by implementing modified AES with dynamic S-box and GHASH respectively. Those encrypted videos are decrypted in the reverse fashion using the same chaotic map-based AES operation.

The decryption process of encrypted video is illustrated in Fig. 5. The chaotic function is applied to the encrypted media to decrypt it by involving diffusion and confusion stages.

Experimental Results and Discussion

The proposed selective frame encryption of videos is implemented in a cloud application by creating microservices and adding frontend web components using ReactJS, a cloud-native technique based on the Go language. The simulator is developed using cloud-native react as the front end with the support of the library system security which is implemented within JavaScript and uses the default settings. The performance analysis is done on the created S-box by measuring, nonlinearity, Strict Avalanche (SAC), Bit Independence Criteria (BIC), approximation of differential probability, and linear probability. To evaluate the objective video quality, Mean Square Error (MSE), Information Entropy value, Peak Signal to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM) are measured for the encrypted frame. Differential properties of the S-box are analyzed as it is intended to resist differential attacks.

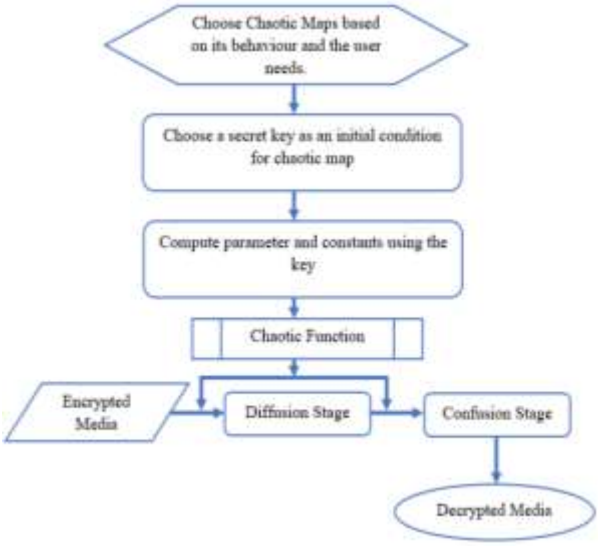
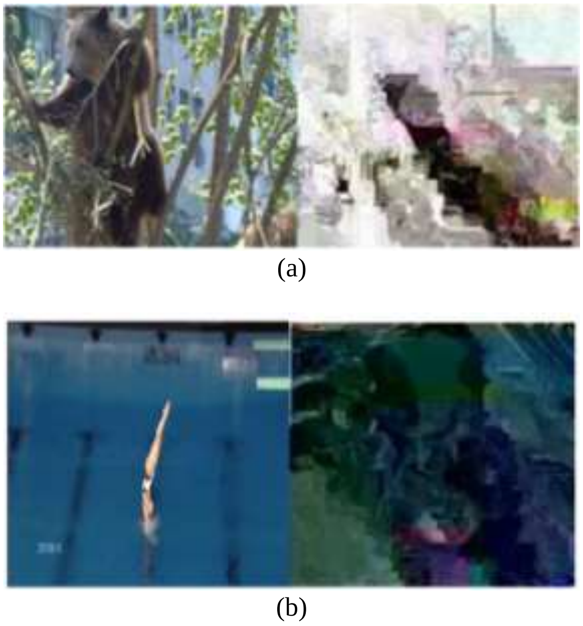

Choose Chaotic Maps based on its behaviour and the user needs.
Choose a secret key as an initial condition for chaotic map
Compute parameter and constants using the key
Chaotic Function
Encrypted Media
Diffusion Stage
Confusion Stage
Decrypted Media

Fig. 5: Process of media decryption


(a)

(b)

Fig. 6: Encrypted videos of different datasets; (a) Bearpark_climbing video and encrypted video frame; (b) Diving side video frame and encrypted video frame

Mean Square Error (MSE)

MSE is calculated as the averaged sum of squared pixel values difference between the original frame as well as the resultant frame and hence the error difference of image pixels for each frame is computed. It can be expressed as:

$$MSE=\frac{1}{N\times M}\sum\nolimits_{n=1}^{N}\sum\nolimits_{m=1}^{M}\left(f_i\ (n,m)\right)-f_o\ (n,m))^2 \tag{3}$$

where, f_i is the input original frame and f_o is the output resultant frame.

Peak Signal to Noise Ratio (PSNR)

The quality of the reconstructed image in a particular frame associated with the original frame is estimated by computing the degree of the MSE value. *PSNR* is estimated as:

$$PSNR = 10\ \log\frac{s^2}{MSE} \tag{4}$$

where, s = 255 for an 8-bit image. A higher *PSNR* value of the image in a frame indicates good quality whereas a lesser *PSNR* value indicates the low quality of the frame.

Structural Similarity (SSIM) Index

Based on the structural distortion measurement, the structural similarity metric is calculated among two frames. The value of SSIM lies between 1 to 1 indicating the quality degree of the video frame. A higher SSIM value indicates a good similarity between the original and reconstructed frame. The average value of SSIM of the input videos is around 0.05 which affirms that the proposed method is efficient in selective frame encryption. Fig. 6 illustrates that selective frames are encrypted using the proposed approach. Table 2 shows the objective video quality analysis performance metrics of the proposed algorithm for particular frames of the given video. The average entropy observed in the input video is 7.9436, the average PSNR is 9.7363 and the average MSE is 1.41.

Nonlinearity

The nonlinearity of a function $f(x)$ is described as the least possible hamming distance among the functions f and H, where H represents the collection of the entire linear functions in addition to affinal functions. Here $f(x)$ is a Boolean function of the Galois field GF(2^n). The Nonlinearity of the generated S-box is computed as:

$$N_{f(x)}=\min_{h\in H^n} d(f,h) \tag{5}$$

A higher value of nonlinearity indicates a stronger S-box that resists linear attacks. The proposed chaotic S-box produces nonlinearity as 112 which is efficient in resisting nonlinear attacks.

Table 2: Performance evaluation in objective quality analysis

Input	Entropy	PSNR (DB)	MSE	SSIM
Video 1	7.8682	10.23770	1.50	0.130
Video 2	7.9795	9.89790	1.47	0.021
Video 3	7.9833	9.07340	1.26	0.015

Table 3: Comparison of S-boxes

	Bijection	Nonlinearity	Avg SAC	BIC nonlinearity
Hussain *et al*. (2011)	128	105.12	0.5046	104.35
Hussain *et al*. (2019)	128	106.27	0.5037	103.45
Wang *et al*. (2015)	128	102.75	0.4914	103.67
Tian and Lu (2016)	128	103.00	0.5029	100.28
Özkaynak (2019)	128	106.40	0.5014	104.21
Proposed	128	112.00	0.5062	105.21

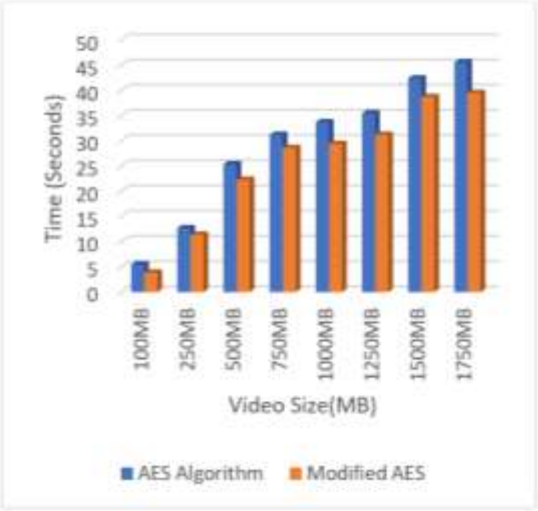


Fig. 7: Time consumption

Strict Avalanche Criterion (SAC)

The avalanche effect of the Boolean function is quantitatively analyzed by the SAC (Tian and Lu, 2016). It is defined as the one-bit difference in the given input Boolean function that must alter at least one-half of the output bit values (i.e., the changing probability should be 0.5). The dependency matrix or correlation is calculated to evaluate the SAC in which each element of the matrix will be 0.5. The average of all the elements in the matrix will be closer to 0, indicating that it holds SAC.

Bit Independence Criterion (BIC)

Let the two distinct Boolean functions be f_i and f_k where ($i \neq k$) and these two are the outputs of the S-box with high nonlinearity. The output of $f_i \oplus f_k$ representing the correlation coefficient value is nearly 0 when one bit is changed or reversed. The proposed method outcome is verified by a change in the one-bit value of the input that must satisfy both the SAC and nonlinearity using BIC. The results of the proposed dynamic S-box are compared with other s-boxes of a block cipher in terms of Bijection, nonlinearity, SAC, and BIC values shown in Table 3.

Differential and Linear Probability

Differential Probability (DP) is calculated based on the XOR distributions of input and outputs of Boolean functions to analyze how far the S-box created can resist different attacks. It computes the maximum likelihood of differential outputs for the given inputs with a total of 2^n elements. The smaller value of DP indicates that the S-box generated highly resists differential attacks.

Linear Probability (LP) is determined by estimating the maximum amount of linearity of the S-box. The inputs and outputs of the S-box are masked and the maximum number of linear estimates are analyzed. Based on the probability equations (Yang *et al*., 2021), the DP and LP values are calculated for the generated S-box, and their values are 0.0383 and 0.142 respectively. Thus, the generated S-box strongly resists linear and differential cryptanalysis attacks. A smaller value of LP indicates that the S-box generated highly resists linear attacks.

Time Consumption

The existing symmetric algorithm and the proposed modified AES with chaos-based dynamic S-box are compared to check the time consumption of each while encryption and decryption. Figure 7 shows the time consumed by the proposed chaos based modified AES for different video data sizes such as 250, 500 MB, and 750 up to 1050 MB. The time consumption graph indicates that the proposed algorithm has less time complexity in encrypting and decrypting varying size videos. It also proves that the proposed algorithm has less time complexity for the encryption and decryption process.

Conclusion

In this study, a selective video frame encryption approach is proposed to encrypt the extracted semantic elements of the videos using a dynamic S-box. In the proposed approach, a novel dynamic chaos-based S-box generation algorithm is used to produce a pseudo-bit sequence and dynamically substitute random bits in video frame encryption. Designed S-box also performs self-scrambling and provides good diffusion which obtains a high nonlinear degree with large chaotic behavior. The performance analysis of the proposed approach with chaos-based S-box is evaluated using metrics such as MSE, PSNR, SSIM, nonlinearity, SAC, and BIC which affirms that it has high resistance to security attacks. The results confirm that the proposed selective video frame encryption scheme has a superior impact with less time complexity. In the future, statistical tests and rate distortion optimization can be performed while decoding the videos.

Acknowledgment

We express our thanks to Vellore institute of technology for their support.

Funding Information

The authors have not received any financial support or funding to report.

Author’s Contributions

Megala G.: Conceptualization, methodology, software, data curation, written original drafted, visualization, investigation, software, validation, written reviewed, and edited.

Swarnalatha P.: Supervision.

Ethics

This article is an original research work. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Awan, I. A., Shiraz, M., Hashmi, M. U., Shaheen, Q., Akhtar, R., & Ditta, A. (2020). Secure framework enhancing AES algorithm in cloud computing. *Security and Communication Networks*, *2020*, 1-16. https://doi.org/10.1155/2020/8863345

Chai, X., Gan, Z., Yuan, K., Chen, Y., & Liu, X. (2019). A novel image encryption scheme based on DNA sequence operations and chaotic systems *Neural Computing and Applications*, *31*, 219-237. https://doi.org/10.1007/s00521-017-2993-9

Cheng, S., Wang, L., Ao, N., & Han, Q. (2020). A selective video encryption scheme based on coding characteristics. *Symmetry*, *12*(3), 332. https://doi.org/10.3390/sym12030332

Dong, C. E. (2015). Asymmetric color image encryption scheme using discrete-time map and hash value. *Optik*, *126*(20), 2571-2575. https://ui.adsabs.harvard.edu/abs/2015Optik.126.2571D/abstract

Gueron, S., & Kounavis, M. (2010). Efficient implementation of the Galois Counter Mode using a carry-less multiplier and a fast reduction algorithm. *Information Processing Letters*, *110*(14-15), 549-553. https://doi.org/10.1016/j.ipl.2010.04.011

Hamidouche, W., Farajallah, M., Sidaty, N., El Assad, S., & Deforges, O. (2017). Real-time selective video encryption based on the chaos system in scalable HEVC extension. *Signal Processing: Image Communication*, *58*, 73-86. https://doi.org/10.1016/j.image.2017.06.007

He, J., Xu, Y., Luo, W., Tang, S., & Huang, J. (2020). A novel selective encryption scheme for H. 264/AVC video with improved visual security. *Signal Processing: Image Communication*, *89*, 115994. https://doi.org/10.1016/j.image.2020.115994

Hong, S. S., & Han, M. M. (2014). The study of selective encryption of motion vector based on the S-box for the security improvement in the process of video. *Multimedia Tools and Applications*, *71*, 1577-1597. https://doi.org/10.1007/s11042-012-1287-6

Hussain, I., Anees, A., Al-Maadeed, T. A., & Mustafa, M. T. (2019). Construction of S-box based on chaotic map and algebraic structures. *Symmetry*, *11*(3), 351. https://doi.org/10.3390/sym11030351

Hussain, I., Shah, T., Gondal, M. A., & Wang, Y. (2011). Analyses of SKIPJACK S-box. *World Appl. Sci. J*, *13*(11), 2385-2388. https://www.researchgate.net/publication/277559481_Analyses_of_SKIPJACK_S-box

Jolfaei, A., Vizandan, A., & Mirghadri, A. (2012). Image encryption using HC-128 and HC-256 stream ciphers. *International Journal of Electronic Security and Digital Forensics*, *4*(1), 19-42. https://doi.org/10.1504/IJESDF.2012.045388

Kermani, M. M., & Azarderakhsh, R. (2018). Reliable architecture-oblivious error detection schemes for secure cryptographic GCM structures. *IEEE Transactions on Reliability*, *68*(4), 1347-1355. https://doi.org/10.1109/TR.2018.2882484

Kumar, P., & Rana, S. B. (2016). Development of modified AES algorithm for data security. *Optik*, *127*(4), 2341-2345. https://doi.org/10.1016/j.ijleo.2015.11.188

Lima, J. B., Madeiro, F., & Sales, F. J. (2015). Encryption of medical images based on the cosine number transform. *Signal Processing: Image Communication*, *35*, 1-8. https://doi.org/10.1016/j.image.2015.03.005

Liu, H., & Kadir, A. (2015). Asymmetric color image encryption scheme using 2D discrete-time map. *Signal Processing*, *113*, 104-112. https://doi.org/10.1016/j.sigpro.2015.01.016

Ma, X., Zeng, W. K., Yang, L. T., Zou, D., & Jin, H. (2015). Lossless ROI privacy protection of H. 264/AVC compressed surveillance videos. *IEEE Transactions on Emerging Topics in Computing*, *4*(3), 349-362. https://doi.org/10.1109/TETC.2015.2460462

Malik, M. S. M., Ali, M. A., Khan, M. A., Ehatisham-Ul-Haq, M., Shah, S. N. M., Rehman, M., & Ahmad, W. (2020). Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. *IEEE Access*, *8*, 35682-35695. https://doi.org/10.1109/ACCESS.2020.2973679

Malladar, R. S., & Kunte, S. R. (2021). Selective Video Encryption Using the Cross Coupling of One-dimensional Logistic Maps. *International Journal of Computer Network & Information Security*, *13*(5). https://doi.org/10.5815/ijcnis.2021.05.04

Megala, G. (2021a). State-of-the-art in video processing: Compression, optimization and retrieval. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(5), 1256-1272. https://doi.org/10.17762/turcomat.v12i5.1793

Megala, G. (2021b). A Comprehensive Analysis on Efficient Multimedia Storage Mechanism in Public Cloud Environment with Secured Access. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(5), 1273-1280. https://doi.org/10.17762/turcomat.v12i5.1794

Megala, G., & Swarnalatha, P. (2022). Efficient high-end video data privacy preservation with integrity verification in cloud storage. *Computers and Electrical Engineering*, *102*, 108226. https://doi.org/10.1016/j.compeleceng.2022.108226

Méloni, N., Négre, C., & Hasan, M. A. (2010). High performance GHASH function for long messages. In *Applied Cryptography and Network Security: 8th International Conference, ACNS 2010, Beijing, China, June 22-25, 2010. Proceedings 8* (pp. 154-167). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-13708-2

Namasudra, S., Chakraborty, R., Majumder, A., & Moparthi, N. R. (2020). Securing multimedia by using DNA-based encryption in the cloud computing environment. *ACM Transactions on Multimedia Computing, Communications and Applications (TOMM)*, *16*(3s), 1-19. https://doi.org/10.1145/3392665

Özkaynak, F. (2019). Construction of robust substitution boxes based on chaotic systems. *Neural Computing and Applications*, *31*(8), 3317-3326. https://doi.org/10.1007/s00521-017-3287-y

Qiao, Z., El Assad, S., & Taralova, I. (2020). Design of secure cryptosystem based on chaotic components and AES S-box. *AEU-International Journal of Electronics and Communications*, *121*, 153205. https://doi.org/10.1016/j.aeue.2020.153205

Sallam, A. I., El-Rabaie, E. S. M., & Faragallah, O. S. (2018). Efficient HEVC selective stream encryption using chaotic logistic map. *Multimedia Systems*, *24*, 419-437. https://doi.org/10.1007/s00530-017-0568-3

Shah, R. A., Asghar, M. N., Abdullah, S., Fleury, M., & Gohar, N. (2019). Effectiveness of crypto-transcoding for H. 264/AVC and HEVC video bit-streams. *Multimedia Tools and Applications*, *78*, 21455-21484. https://doi.org/10.1007/s11042-019-7451-5

Shah, R. A., Asghar, M. N., Abdullah, S., Kanwal, N., & Fleury, M. (2020). SLEPX: An efficient lightweight cipher for visual protection of scalable HEVC extension. *IEEE Access*, *8*, 187784-187807. https://doi.org/10.1109/ACCESS.2020.3030608

Silva-García, V. M., Flores-Carapia, R., Rentería-Márquez, C., Luna-Benoso, B., & Aldape-Pérez, M. (2018). Substitution box generation using Chaos: An image encryption application. *Applied Mathematics and Computation*, *332*, 123-135. https://doi.org/10.1016/j.amc.2018.03.019

Taha, M. A., Assad, S. E., Queudet, A., & Deforges, O. (2017). Design and efficient implementation of a chaos-based stream cipher. *International Journal of Internet Technology and Secured Transactions*, *7*(2), 89-114. https://doi.org/10.1504/IJITST.2017.087131

Tian, Y., & Lu, Z. (2016). S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm. *Journal of Systems Engineering and Electronics*, *27*(1), 232-241. https://ieeexplore.ieee.org/abstract/document/7424939

Valli, D., & Ganesan, K. (2017). Chaos based video encryption using maps and Ikeda time delay system. *The European Physical Journal Plus*, *132*, 1-18. https://doi.org/10.1140/epjp/i2017-11819-7

Wang, Y., Lei, P., & Wong, K. W. (2015). A method for constructing bijective S-box with high nonlinearity based on chaos and optimization. *International Journal of Bifurcation and Chaos*, *25*(10), 1550127.

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. *Multimedia Systems*, *26*, 363-381. https://doi.org/10.1007/s00530-020-00648-7

Yang, C., Wei, X., & Wang, C. (2021). S-box design based on 2D multiple collapse chaotic map and their application in image encryption. *Entropy*, *23*(10), 1312. https://doi.org/10.3390/e23101312

Yasser, I., Mohamed, M. A., Samra, A. S., & Khalifa, F. (2020). A chaotic-based encryption/decryption framework for secure multimedia communications. *Entropy*, *22*(11), 1253. https://doi.org/10.3390/e22111253

Zhang, X., Seo, S. H., & Wang, C. (2018). A lightweight encryption method for privacy protection in surveillance videos. *IEEE Access*, *6*, 18074-18087. https://doi.org/10.1109/ACCESS.2018.2820724