I. J. Computer Network and Information Security, **2021, 5, 40-54**
Published Online October 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2021.05.04

Selective Video Encryption Using the Cross Coupling of One-dimensional Logistic Maps

Rohit S Malladar
Jain Institute of Technology, Davanagere, 577004, India
E-mail: msrohit@jitd.in

Sanjeev R Kunte
J.N.N.College of Engineering, Shivamogga, 577204, India
E-mail: sanjeevkunte@jnnce.ac.in

Received: 22 February 2021; Revised: 14 April 2021; Accepted: 07 May 2021; Published: 08 October 2021

Abstract: H.264 videos have been the most shared type of video format in recent times and hence its security is a major issue. The techniques presented in the recent times incur complex computations. The major research objective is to design an efficient Chaotic Selective Video Encryption (CSVE) technique which can result in a better visual degradation of the encrypted video with less computational complexity. In the proposed work, in order to secure the H.264 videos, two one-dimensional logistic maps are cross coupled in the chaotic encryption technique which uses a lookup table for data conversion. The technique is evaluated using different performance metrics like Peak Signal to Noise Ratio (PSNR), entropy, statistical analysis etc along with the traditional logistic map. The work is compared with some recent techniques in terms of PSNR and was found out that the proposed technique has better encryption effect.

Index Terms: Encryption, computational complexity, JM 19.0 reference model, H.264, cross coupled logistic map.

1. Introduction

With the exponential advancement in internet and the innovative breakthrough in the technology, the video sharing is happening very smoothly at the satisfactory rate. Sensitive and personal information share the higher priority and hence, data must be protected against the interceptions [1]. Avoiding unauthorized access and securing the privacy can be achieved through video encryption. Video encryption is a technique to secure the contents of the video by converting the content of the video into unreadable form for the unauthorized users.

Information security has been the primary concern over internet as the illegal activities [2] are increasing with increasing users. Need for security is one of the driving forces behind the new techniques evolving in the field of cryptography. Innovation in the cameras [3] and swift advances in the storage capacity have been the reasons for increased movement of videos and also the reason behind increased quality of the videos. The encryption techniques have to preserve the quality of the videos to the maximum extent and hence the research is continued in increasing the quality of the video after the decryption.

The encryption techniques have to address the computational complexity incurred during the process along with the visual degradation. The full video encryption is a technique which fully encrypts the video and hence the time required to do so is very high. Instead of working on every bit of the video, selective video encryption technique choses few parameters for the process of encryption. The selective video encryption technique is a better solution than full video encryption and it can be used in the different applications of multimedia streaming like video conferencing, Video on demand (VoD), Pay Per View (PPV), etc. This technique can reduce the computational overhead so the time required for encryption is very less as compared to the full / naïve encryption technique. In the proposed work, H.264 compression technique is chosen for the encryption which is carried out during the compression technique itself. Chaos theory is used as the platform for encryption in which cross coupled logistic maps [4] are used for the conversion of data. The technique can be used in the various fields like medical data processing [5], online library systems, video conferencing, etc. Online streaming of the video content has been on the rise from last decade and the chaotic video encryption techniques have also been evolving from one-dimensional to

Contributions of the proposed work:

1. Cross coupling of the logistic maps to increase the security of the encryption technique.
2. Usage of congruence rules for the start state generation.

2. Previous Work

Chaos encryption has been evolving since the first work on the logistic map application in encryption was proposed by Baptista [6]. Since then, different types of multimedia have been encrypted by the chaos theory using many chaotic maps. The video encryption is explored using many chaotic maps like logistic map, sine map, henon map etc. Different properties of the chaos like ergodicity, unpredictability and sensitivity to the initial conditions are the reasons behind the chaos' usage in the field of encryption. Such a kind of the encryption technique when used on multimedia like video, can make the video very secure [7] and can withstand the attacks for a longer time. Video encryption has also evolved from the theory of full encryption to the partial / selective encryption. Selective video encryption is a technique which encrypts a part of the video to reduce the computational complexity incurred in the traditional encryption processes. The raw video, when undergoes the H.264 video compression, results in the bit stream which is a complex stream of syntax elements[8] which can only be decoded by the H,264 decoder.

Syntax elements such as Motion Vectors (MVs), trailing zeros, trailing ones, Motion Vector differences (MVDs), Intra Prediction Modes (IPMs), etc are encrypted using different chaotic maps. The proposed work encrypts few of the syntax elements using the concept of cross coupling of logistic maps. So far, the video encryption using chaos has been implemented using different sets of syntax elements. The time period of the compression process was chosen for the encryption by Lei Chen et al [9] for the encryption of the selected syntax elements in the video stream. The code trees viz., kth order Exp Golomb code (KEG), Fixed length (FL) codes and the Truncated Unary Code (TU) were selected for the encryption using the Piecewise Linear chaotic map. The KEG and FL codes contributed to the increase in the code length. The technique became complex due to the selection of all the code trees presentation and the selective choice of the code trees might have reduced the computational overhead. The technique failed to withstand against the different types of attacks, but it was also fast in encrypting the syntax elements.

A huge number of parameters such as levels of non-zero coefficients, Intra Prediction Modes (IPMs), number of zeros before non-zero coefficients, Trailing Zeros' sign and Motion Vector Differences (MVDs) were encrypted by Hui Xu et al[10]. The selection of the syntax elements resulted in the strong security but the technique suffered from the high computational complexity. A considerable key space of 2^{626} bits was used which is enough for the brute force attacks but the key space is small for the replay and differential attacks. Chaotic stream cipher was generated using the traditional Coupled Lattice Model (CML) without any modifications and hence if initial state is known then the subsequent states can be easily computed. The technique claimed to preserve the bit rate and compression ratio.

Very few syntax elements were chosen for encryption using multiple Renyi chaotic[11] maps and the pseudorandom bit sequence generated was strong enough to maintain format compliancy. 111-bit secret key was used in the technique which made the process weak against the brute force attacks. The technique was very secured due to the use of multiple maps. Five Renyi maps were used to generate the required random numbers which increased the computational complexity and the total key length was 128 bits which is very very low to withstand against any kind of attacks.

IPMs, residual coefficients and MVDs were used for selective video encryption using chaotic Qi system[12]. The Qi system was supported by the XOR operation to produce the random numbers based on the user provided key. For every slice in the frame, 256-bit keys were generated which made the technique to consume a lot of time to encrypt the syntax elements. A very huge key space of 2.4×10^{52} which sums to a key with length 174 bits is used in this technique. The trade-off between the security and computational complexity is well addressed in this technique

Coupled Lattice Model (CLM) was used to address the spatiotemporal behaviour of the chaotic system by [13]. Different parts of the bit stream like residual data, inter block mode selection and IPMs were converted to cipher data using the pseudo random numbers produced by the CLM. The scene change observed in the videos resulted in a large residual data and hence the encryption process consumed more time than expected. Bit rate of the encrypted file increased at an average of 1.98%, which is considerably low. Trailing ones and zeros with DCT coefficients, IPMs and MVs were used to encrypt the video stream by Hui Xu et al [4]. Modified LCM was once again used in the spatiotemporal domain but with different set of syntax elements for different frames. Payload in the Network abstraction layer was the region of encryption unlike encryption during the compression method. Header of every slice had to be parsed in order to encrypt and decrypt the data. This resulted in the increased security but also increased the file size and time consumed, since the metadata of the encryption had to be included in the encrypted bit stream.

Chroma components were focused for encryption in different processes of H.264 compression like inter prediction, IPMs and Context Adaptive Variable Length Coding (CAVLC) by Khlif et al [14]. Couple of Piecewise Linear Chaotic Maps (PWLCMs) were practiced for the generation of the keys in the encryption process. The technique stood strong against the brute force attacks and the format compliance along with the compression ratio was preserved. The key space used by the technique was 10^{44} which is very high. The PWLCMs used in the technique are independent to each other which infer that, if any of the state of information is revealed then other state information can be found out without the interference of the other map. Random state interchange or the cross coupling of the maps could have increased the security of the technique. Security of the encryption techniques was strengthened by using multiple syntax elements by [15]. Scrambling operation was used along with chaotic encryption to support the confusion and diffusion

property of the encryption technique. Permutation process with S-box scrambled the DCT coefficients, AES with a modified S box was used to encrypt the non-zero coefficients and the chaotic logistic map was used to encrypt the trailing non zero coefficients. The security of the technique is very high but due to the multiple encryption techniques in the overall encryption process might be very time consuming. The order of the encryption technique starts with the permutation of the of DCT using the traditional S-box without any modification, the overall technique could have been stronger if the encryption started with a more complex encryption technique.

Yanije et al [16] proposed a Chaotic Selective Encryption Scheme (CSES) which uses two Key Stream Generation (KSGs). A big set of syntax elements including IPMs, coded block pattern, information regarding the synchronization of macro blocks and slices, non-zero quantized coefficients and inter prediction mode were encrypted using the CSES. Logistic maps were used in the KSGs and the technique claimed to be very fast and the technique was able to maintain the bit rate post encryption process.

Selection of the syntax elements can directly impact the encryption ratio and it was proved by [17]. This was achieved when the binarization step in Context Adaptive Binary Arithmetic Coding (CABAC) was represented using the Code Tree. Syntax elements like the IPMs and the reference frame indexes were encrypted using the Unary Code (UC) and Truncated Unary (TU) respectively. The technique used less time in the encryption process and the complexity of the overall technique was also very low. The security of the technique was limited to the key space of 128 bits and the technique used A 4-D hyperchaotic system [18] was used to encrypt each slice in the frame by selecting the syntax elements present such as the MVD, delta Quantization parameter, residual coefficient and IPM along with the cipher feedback mode of the Advanced Encryption Standard (AES). The effect of the encryption was better compared toother chaotic techniques and the process also consumed very less time.

Even though so many chaotic maps have been tried to secure the video content so far, the field of encryption still demands the novel techniques to strengthen the security of the encryption process. When assessed using the standard measures, the encryption techniques are expected to show good results in terms of visual degradation, resistance to attacks, signal to noise ratio, entropy, etc. In the proposed work, the concept of cross coupling of logistic maps is used to encrypt the syntax elements of the H.264 video. Motion vectors, IPMs and trailing ones are selected for the encryption which is aimed to make the process to consume less time and hence the process a lightweight encryption technique.

3. Proposed Work

As described in the previous section, the proposed CSVE technique uses a subset of the syntax elements available as per the H.264 guidelines. In order to reduce the computational complexity of the technique, the main advancing feature of the proposed technique is the cross coupling of two one-dimensional logistic maps to generate the cipher text. Fig 1 shows the basic encryption process used in the work. The cross coupling of the maps enhances the features of confusion and diffusion of chaos theory in the proposed technique.

The chaotic encryption technique [19] follows a recursive process in which the initial state carries a lot of importance. Every state of the chaotic encryption is derived from its previous state and hence initial state of this entire technique has to be highly secured. In addition to this property, two different logistic maps are coupled together to increase the security of the technique. The syntax elements are encrypted using the chaos theory which shall be described further in this section. The cipher text resulting in this encryption process are swapped with syntax elements in the bit stream and hence the process results in the encrypted video. The logistic map has been used in the video encryption because of its chaotic properties like ergodicity, confusion and diffusion. The generic equation of the logistic map is as shown in (1).

$$x_{n+1} = r\, x_n\, (1 - x_n) \tag{1}$$

Where,

x_n represents the start state of the system
r is the fixed non negative parameter
x_{n+1} represents the next state of the system

The cross coupling of the logistic maps is carried out with an added XOR operation which shall be detailed in the next section. The methodology used in the proposed technique includes many stages in addition to the processes described in the fig 1.

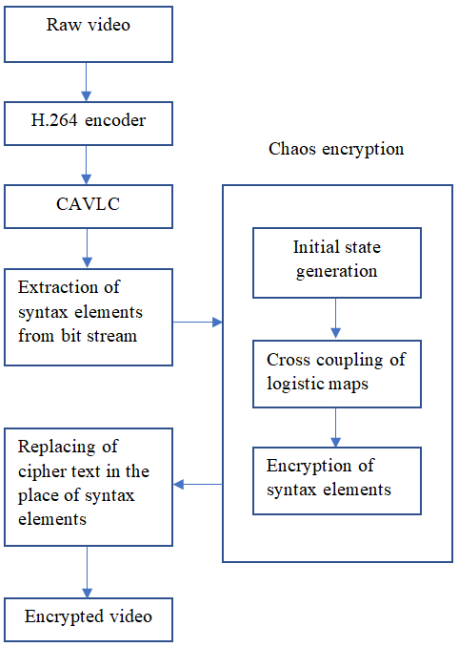

Fig.1. Block diagram of the proposed chaotic encryption

3.1. Research methodology

Methodology of the entire proposed work starts with the usage of the congruence rules for the generation of the start states for both of the logistic maps. The two logistic maps shall produce different states since the initial states are computed with different inputs. The logic behind using different start state is to impart another level security in addition to cross coupling the two maps. Step by step cross coupling of the two logistic map is carried out without leaving any loop hole in the encryption technique. With these states, the logistic maps are run with XOR operation to induce more security. The primary aim of using the chaotic maps in an encryption technique is to generate highly secure random numbers which are used directly in the encryption process or the random numbers can be associated with the range of values which are further used in the lookup tables as it is used in this work. Another reason behind using of lookup tables is that it eliminates any kind of added communication regarding the sharing of procedural information with the receiver. The lookup table makes the technique lightweight as the procedure to compute the table is very simple as shown in the upcoming sections. The randomness of the numbers generated in the process is also assessed in the results section.

3.2. Cross coupling of two logistic maps

The logistic map is coupled with another such map but with a different start state to impart higher level of confusion and diffusion into the crypto-system. The coupling of logistic maps is as shown in fig 2. In the proposed work, the two logistic maps are coupled mainly because such a coupling makes the cryptanalysis very difficult. The cipher obtained after the coupling has to be determined by the two different chaotic orbits. Since both the logistic maps are of same type, the encryption process increases the efficiency of the proposed technique. The coupling of the logistic maps is supported by the XOR operation which uses the first number in the mantissa part of the individual state value. Assume x_{n+1} is the second state of the first logistic map as shown in the (1) and its value is 0.48934.

Let the value, $x_{n+1} = r\,x_n\,(1 - x_n)$ = 0.48934 in the fractional part after the decimal point which is 48934, the first number i.e., 4 is taken as the key for XOR operation. Before cross coupling the states of two different logistic maps, the output of the states go through the XOR operation. Logistic maps by themselves are a safe to generate the random numbers and hence the proposed technique with cross coupling adds on to the security features of the technique.

Step 1: Find the first state of first logistic map 1, $x_{11} = r\,x_{10}\,(1 - x_{10})$.
Step 2: Extract the first number from the fractional part of the state x_1 and let this number be N_1.

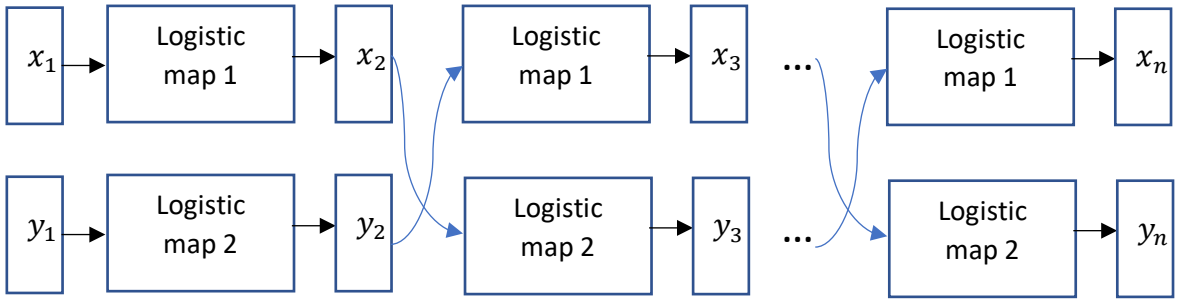

Fig.2. Cross coupling of logistic map 1 and logistic map 2

Step 3: Perform the XOR operation with the results of step 1 and 2.
Final state, $x_{11} = x_{11} \oplus N_1$
Step 4: Find the first state of first logistic map 2, $x_{21} = r\, x_{20}\,(1 - x_{20})$.
Step 5: Extract the first number from the fractional part of the state x_{21} and let this number be N_2.
Step 6: Perform the XOR operation with the results of step 1 and 2. Final state, $x_{21} = x_{21} \oplus N_2$
Step 7: Now the states x_{11} and x_{21} are cross coupled to each of the logistic maps and this process is continued till conditions for the lookup table are met.

Since the key for the XOR operation is taken implicitly by the technique from one of its states itself, there is no need to pass the key separately to the receiver. Following the roadmap of the encryption technique, the upcoming phases includes the start state generation and generation of lookup tables etc.

3.3. Generation of the start state

In order to generate the start state of the logistic maps X_0, the (2) is followed.

$$X_0 = \frac{1}{2}\sum_{i=0}^{255}\frac{b_i}{2^{i+1}} \tag{2}$$

Where, b_i is the random binary sequence.
X_0 is the start state.
Random binary sequence b_i is generated using the equivalence class rules merged with the congruence class rules theory in mathematics.
To generate binary sequence of logistic map 1, the congruence rule is shown in (3).

$$a \equiv b\ (\mathrm{mod}\ c)\ \forall\ c \mid c \geq 3 \tag{3}$$

where c = {3,4}
{a,b} ∈ E
E is the equivalence class for mod c. Between many equivalence classes that might be considered, for c = 3, the class considered for the first three remainders 0, 1 and 2 are considered to be c30, c31, c32. For c = 4, the respective classes are considered to be c40, c41, c42, c43. Consider the classes c30 and c40, which represent the classes for all the numbers whose division results in the remainder 0, 29 such numbers are taken from this class. These numbers are again binarized to form 128bit length key. Henceforth, the process is continued on c31 and c41 which represent the equivalence for all the numbers whose division results in the remainder 1 to form the 64bit key. The technique is continued till 256bit key length is reached.
To generate binary sequence of logistic map 2, the congruence rule is shown in (4).

$$i \equiv j\ (\mathrm{mod}\ k)\ \forall\ k \mid k \geq 5 \tag{4}$$

where k = {5,6}
{i, j} ∈ E
E is the equivalence class for mod k.
The procedure to form the 256bit length key for this map is similar to the one described for the logistic map1.

3.4. Encryption technique

Data changes rapidly from one process of the H.264 compression to another and the encryption techniques take the advantage of such change in a frame with reference to another frame within the same Group of Frame (GoP). Syntax

elements are the key elements which carry vital information of a frame which is referenced by other frames in the GoP. In the present work, the motion vectors along with the IPMs and trailing ones are selected for the encryption process. Look up tables are required to form the correlation among the intervals in the range of the logistic map in coordination to the plain text or syntax elements. The range of the cross coupled logistic map is between 0 and 1. This range is divided in to 'r' intervals where r = 256 which represents the maximum possible value of any parameters considered for the encryption. Now to decide the length of each interval in the range 0 to 1, an epsilon interval defined based on the maximum value as given by (5).

$$\varepsilon = \frac{1}{256} \tag{5}$$

The range [0,1] gets the interval length in form of $'\varepsilon'$. The role of each interval of this length in the range, is to get associated with each character in the syntax element. For example, the character '0' in the syntax element is linked to the interval 0 and ε , character '1' is linked to the interval ε and 2ε and so on. As shown in table 1, look-up table and the start state are two prerequisites for starting the encryption process. Considering each of the character in the syntax element s1, the range of the interval, r1-r2, using the epsilon is calculated and the cross coupled logistic map is run till the states of the map enters within the range.

Table 1. Look up table for the original data and range calculated

Syntax element	Interval range	Sample states	Iteration count
s1	r1 - r2	0.3178 – 0.3276	c1
s2	r3 – r4	0.3276– 0.3374	c2
s3	r5 - r6	0.3374 – 0.3472	c3

The number of the iterations, for eg c1, taken by the coupled map is recorded as the cipher text of the corresponding syntax element. Every bit in the syntax element is encrypted to create the stream of ciphers. One such lookup table for the coupled logistic map encryption is shown in the table 1.

The coupled logistic maps are run until the states in the maps enter the epsilon intervals which are linked to the characters as described above. Once the iteration stops in an interval, the number of iterations taken by the coupled map is recorded as the cipher text. Every odd numbered iteration count account for the logistic map1 and the even number count accounts for the map2. The count of the iteration is not reset after the encryption of the first character in the syntax element, the count is continued for the next character and hence the dependency towards the start state in this encryption increases and strength of the crypto-process also increases. The encryption process described so far in this section distorts the visual quality of the video by selecting few of the syntax elements in the H.264 bitstream.

4. Experimental Setup

In the proposed work of selective video encryption, the chaotic encryption is carried out during the encoding process of H.264. Joint Model (JM) 19.0 reference model which encodes the raw CIF video sequences to H.264 videos is used for the encryption process. CAVLC process is selected as the encoding method. The base profile is selected with quantisation parameter set to 28. The encrypted video is studied and analysed using many performance metrics in the next section. The JM is run on Windows 10 OS with Intel core i3 processor and the work is examined with different CIF sequences like carphone, foreman, miss America, etc.

5. Results & Analysis

To analyse the encrypted video, different areas like key sensitivity, visual degradation and computational complexity are assessed. The proposed work is also compared with recent work and both are discussed. Key sensitivity is also assessed by bringing changes into the initial sequence. Many of the performance metrics which are applicable to the naïve encryption are also used in the work to depict the difference in the approach of both the full and selective video encryption. Performance metrics like Peak Signal to Noise Ratio (PSNR), entropy, NPCR (Number of Pixel Change Rate), UACI (Unified Average Change Intensity), Structural Similarity Index (SSIM), chi squared test are used to study the effect of the encryption on the video with the help of a stream analyser called Codec Visa. The proposed work is also compared with recent works and both are discussed.

5.1. Peak Signal to Noise Ratio (PSNR)

To assess the effect of the change in a frame due to the encryption, PSNR[20] can be very useful in measuring the error between the encrypted and the original frames. The lower value of PSNR reflects the higher noise and hence the more degradation due to encryption. The recorded values of in decibels(dB) for the different YUV sequences taken as

input is as shown in the table 2 below.

Table 2. Recorded PSNR for different inputs

CIF Sequences	QP = 28			QP = 34			QP=40		
	Original	LM	CCLM	Original	CCLM	LM	CCLM	LM	CCLM
Foreman	45.46	7.70	6.90	41.45	8.29	7.41	37.29	8.98	8.23
Akiyo	46.45	9.23	8.28	42.03	10.18	8.92	39.48	11.29	9.73
Carphone	45.21	9.15	7.36	40.5	10.43	8.69	36.14	11.58	9.94
Miss America	44.96	8.26	8.06	40.94	9.31	8.88	37.83	10.32	9.65

The foreman sequence has recorded the lowest PSNR of 6.9 compared to others indicating that the encryption has a good effect. The motion in the frame affects the PSNR too as rest of the frame remains same in the GoP. In the case of Akiyo, the motion is less and can notice the minor movement of the facial region. Average PSNR calculated for the one-dimensional logistic map is 8.585 and for the cross coupled logistic maps is 7.06 considering all the sequences used in the test. Overall, there is a change of 17.94 in PSNR due to the cross coupling which is very much considerable with the selected list of syntax elements. As more parameters are selected for the encryption, the encryption quality also increases but the computational complexity increases too.

5.2. Number of Pixels Change Rate (NPCR)

Encryption effect is analyzed based upon the amount of change the encryption brings on the data present in the frame. NPCR calculates the change in the encrypted frame with respect to the original frame using every pixel value in both the frames. So NPCR can be used as a tool to evaluate the encryption technique and ideally all the pixels are expected to be changed.

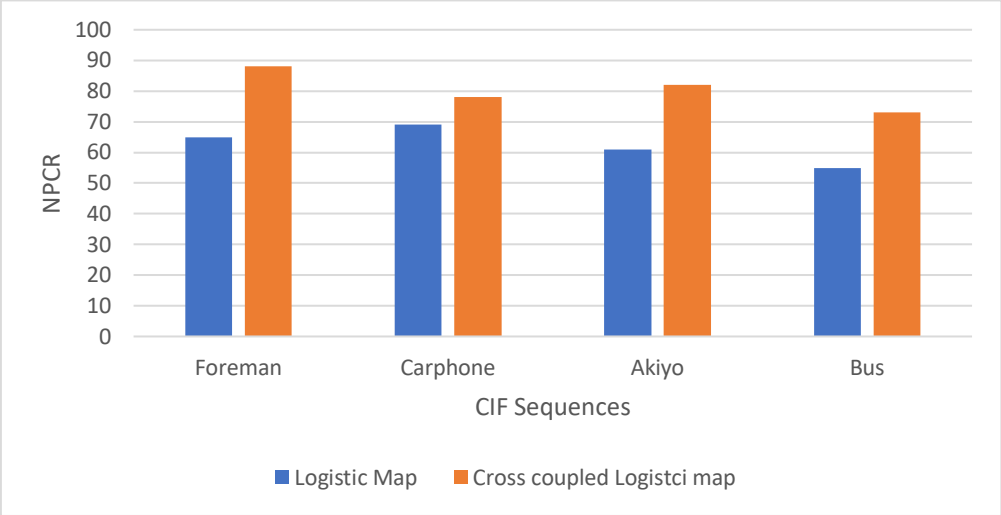

Fig.3. NPCR values for the P frame in GoP

The maximum value of NPCR achieved through the proposed technique is 88% for the foreman sequence and the lowest recorded is 69% for the bus sequence. The syntax elements selected same but their appearance shall vary for every different CIF sequence.

The observed value of NPCR for the different CIF sequences is shown in the fig 3. The number of motion vectors found in the foreman sequence shall be very different from Akiyo and other frames. The ideal value of the NPCR is not reached by the encryption technique described in this work due to the partial selection of the bit stream parameters. The one-to-one pixel information matched during the NPCR calculation results in a lesser value since only selected portions of the frame are encrypted.

5.3. Bitrate

The encryption technique should have very less impact in terms of number of bits processed per second. In the proposed work, the change in the bit rate[21] after the encryption depends upon the number of parameters selected for the process. In the proposed work, the number of bits processed by the encoder in a second is altered by the factors like calculations in the encryption technique as described earlier and magnitude of the values substituted due to the look up table reference. The proposed work encrypts a very small set of syntax elements and a very minor change in the bit rate

is observed. The table 3 shows the bit rates of the original and the encrypted frames with average due to the encryption technique.

Table 3. Bitrates for different CIF sequences

Sequence	Encrypted	Original	Change (%)
Foreman	339.47	332	2.25
Carphone	310.35	303.5	2.30
Akiyo	205.89	193.4	6.4
Bus	237.65	227	4.69

The maximum change in the bit rate is 6.4 % for the Akiyo and minimum change is 2.25 for foreman sequence. Since the number of syntax elements in a CIF sequence vary according to the data present in the frame, the bit rates presented in the table vary from each other. Considering the bit rates of original and encrypted frames, it can be inferred that the change in the bit rate is very minimal and considerable for the real time use. The change observed between the original and encrypted bit rate also reflects the minor change in the compression ratio. Average bit rate of the original sequences is 263.97 whereas the average bit rate of the encrypted stream is 273.34. The average change in the bit rate is found to be 3.91. The change in the bit rate shall directly affect the codec in terms of the decoding speed of the bit stream. The format compliancy of the technique is justified by the very minute average change in the bit rate.

5.4. Differential Attack

Average change in the intensity level of the pixels between the original and encrypted frame is measured to observe the changes brought by the encryption technique. UACI reflects whether the encrypted bit stream shows the non-random behavior or not. The Unified Average Change in the Intensity (UACI) is measured by (6).

$$\mathrm{UACI} = \sum_{i=0}^{m} \sum_{j=0}^{n} \frac{\left| \left(I_{orig}(i,j) - I_{encr}(i,j)\right) \right|}{255} * \frac{100}{m*n} \tag{6}$$

Where,

$I_{orig}(i, j)$ – gives the original intensity value at (i, j)

$I_{encr}(i, j)$ - gives the encrypted intensity value at (i, j)

m and n are the number of rows and column of the considered frames respectively.

Table 4. UACI of the proposed work for different CIF sequences

CIF sequences	LM	CCLM	Change in %
Foreman	38.63	41.23	6.4
Carphone	36.14	39.34	8.88
Bus	37.79	38.99	3.24
Akiyo	36.07	38.2	5.91

The UACI observed for the different sequences is as shown in the table 4. Since the encryption is partial in the proposed work, the average UACI of 39% is near to the ideal value [22] as it is proposed for the encryption. The average change in the in the intensity for the carphone is measured higher than the other three and the least change can be observed in the bus sequence. Even though the cross coupling of the maps has reflected in positive change as compared to the traditional usage of the logistic map in the encryption technique, the change is only due to the selective changes carried out due to the minimal set of the syntax elements.

5.5. Structural Similarity Index (SSIM)

Visual degradation of the video in less time using less computational resources can be a primary property of any video encryption technique. The SSIM is a very useful way of measuring this kind of visual degradation of the frame encryption. For an encryption technique to be very good, the SSIM value is expected to be near to zero. In the proposed work, the visual degradation can be easily noticed due to the encryption of the syntax elements. The proposed work has already been evaluated using PSNR which is calculated using the MSE, it only evaluates the absolute errors. But the inter-dependencies between the neighboring pixels is also to be evaluated. Collectively, these pixels account for the necessary information on the shape of the objects visually. The observed SSIM values in the proposed work is shown in the fig 4.

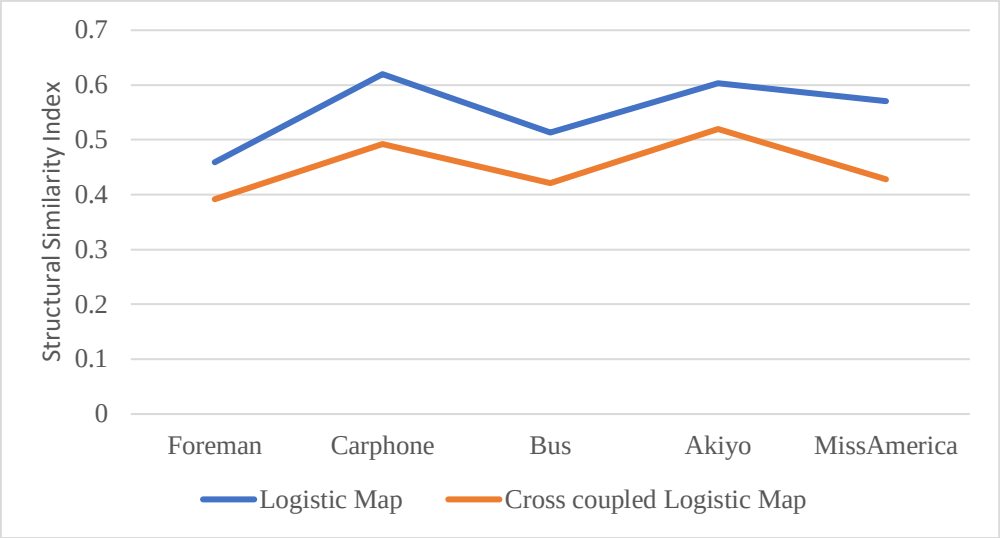

Fig.4. SSIM for the CIF sequences

The foreman sequence shows the SSIM 0.3918, the lowest in the fig 4 and the akiyo sequence with 0.5198 with highest SSIM. As described earlier, the change in the SSIM is common due to the individual properties of the videos. In the Akiyo sequence there is very less movement of the blocks since most of the blocks are static in the news presentation. Only the full encryption can achieve the ideal value of 0, but with the cost of time and computational resources. Having the lower SSIM for the sequence reflects the less dependency between the adjacent pixels and hence the visual identification of the objects is also differed. Having security as the primary objective of the proposed work, the lesser similarity index achieved through this result meets the necessary criteria. Hence the proposed work of selective video encryption justifies the recorded SSIM values.

5.6. Entropy Analysis

Entropy measure [23] reflects the amount of information present in the frame. The ability of the encryption technique to regenerate the data is very important because the encrypted data is rendered useless if the original data cannot be recovered from it. Entropy indicates the degree of re-generatability of the original information if applied on the encrypted stream. In the proposed work, the entropy analysis is carried out to evaluate the grade of uncertainty of the random sequence used in the chaotic sequence. Assuming that the variable 'a' is the information stream used in the calculation of entropy and the governing equation is given by (7).

$$\text{Entropy, } H(a) = \sum_{i=0}^{2^n-1} p(a_i) \log_2 \frac{1}{p(a_i)} \tag{7}$$

Here, p(a) indicates the probability of 'a' and the information linked with the occurrence of a_i is given by the logarithmic function. The entropy values of the encrypted stream of the proposed work are as given in the table 5. The entropy of the RGB channels being very near to the ideal value reflects the randomness and also the perseverance of information in the cipher stream. Hence the entropy assessment also shows that the encryption is strong enough to re-produce the data provided that right parameters are used in the chaos encryption.

The encryption effect given by the cross-coupling technique is equally supported by the subset of the syntax elements used, hence knowing the parameters under encryption and identification of the cross-coupling technique for the re-production of the bit stream becomes difficult.

Table 5. Entropy of the color components

Color	R	G	B
Foreman	7.5981	7.9143	7.3573
Carphone	7.4319	7.4837	7.3041
Coastguard	7.1985	7.9002	7.8148
Miss America	7.3198	7.7638	7.2939

5.7. Randomness test

Randomness factor of the key sequence generated during the chaos encryption is measured using the National Institute of Standards and Technology (NIST) test suite. The test checks many factors of a sequence to be concluded as a random sequence for eg: checking the proportion of ones and zeros, number of 1s within a given block, sequence of

uninterrupted sequence of identical bits, longest runs of ones, etc. For each of the tests in NIST, the output, the p\P value is expected to be greater than or equal to 0.01. The recorded results for the proposed work are as shown in the table 6

Table 6. NIST test suite results

Statistical Test	P-value	Result
Frequency	0.29812	Pass
Block Frequency	0.33019	Pass
CumulativeSums	0.48217	Pass
Runs	0.52912	Pass
LongestRun	0.20298	Pass
Rank	0.43913	Pass
FFT	0.51873	Pass
Approximate entropy	0.68154	Pass
RandomExcursions	0.21498	Pass
RandomExcursionsVariant	0.39821	Pass
Serial	0.61834	Pass

In order to evaluate the uniform distribution of the bits, the threshold value of acceptance is kept 0.01 which was selected due to the cross coupling of the maps. But all the achieved values are well above the mark set and the cross-coupling technique is expected to withstand against the stronger attacks. The occurrence of zeros and ones determined by the frequency test resulted in 0.298, which exhibits the required randomness in the technique. To assess the frequency of ones in a N-bit is expected to be N/2 for absolute randomness, the output p-value of 0.330 reflects that the block frequency is near to N/2 for the different combinations of ones.

Further the cumulative sums, runs and the longest runs results in the 0.482, 0.529 and 0.202. The linear dependency of the bits between the fixed length substrings given by the rank gets the impressive score of 0.439 and it shows that not only the fixed block of N bits, but also the fixed length of the substrings exhibits the randomness. The observed values for different tests result are in the favor of the proposed work, as the P value for the tests are above 0.01. This implies that the start sequence generated using the congruent rules resulted in a strong sequence to make the entire process stronger.

5.8. Statistical Analysis

Statistical relationship between the encrypted and the original frames is measured by the correlation coefficient of the frames which takes the help of mean of the pixels and its standard deviation. The correlation coefficient is given by the (8).

$$\text{CorrelCoeff} = \frac{\sum_{i=0}^{r*c}(x_i - x_{mean})(y_i - y_{mean})}{\sqrt{\left[\sum_{i=0}^{r*c}(x_i - x_{mean})^2 (y_i - y_{mean})^2\right]}} \tag{8}$$

Where,

r and c refer to the resolution of the frames under consideration.

x_i refers the intensity value in the original frame

y_i refers to the intensity value in the encrypted frame

x_{mean} refers to the average value of all the pixels in original frame

y_{mean} refers to the average value of all the pixels in encrypted frame

In the naïve techniques of encrypting the H.264 videos, the ideal value of no correlation or zero correlation can be achieved since entire data found in the frame undergoes the encryption. The recorded values of correlation for the proposed work is as shown in the table 7.

Table 7. Correlation coefficients of the different sequences

CIF sequence	Horizontal	Vertical	Diagonal	Average
Foreman	0.4529	0.5928	0.4040	0.4832
Coastguard	0.5195	0.5388	0.6111	0.5564
Carphone	0.5005	0.6960	0.6982	0.6315
MissAmerica	0.5998	0.5210	0.7109	0.6105

The pixel correlation in all the possible directions of vertical, horizontal and diagonal is assessed to show the non-correlation of the data present in the encrypted frame. The range of average score recorded in the test is 0.4832-0.6315

being far from the ideal value of 0 demands more parameters to be considered for the encryption. But the technique presented in this work ties to achieves the required visual degradation which is shown in the other results. The higher range of correlation achieved in this test is due to the presence of the non-encrypted parts of the video and for the proposed work of selective video encryption, the range can be treated satisfactory.

Selective video encryption may have to compromise with computational complexity to achieve the ideal value of the correlation coefficient which would fail the actual purpose of partial encryption. As it is evident from the table 7, a huge gap can be observed between the values recorded and the ideal value which is due to the kind of encryption proposed in the work. The tradeoff between the computational complexity and the parameters selected for encryption has to be modulated according to the need of the application.

5.9. Original and Encrypted images

In order to meet the ideal conditions of encryption, the parameters selected for the encryption of the videos may have to be increased to the maximum possible extent. This also affects the computational complexity of the technique. But limiting the parameter selection considering the tradeoff between the time taken, computational complexity and visual degradation, the proposed work encrypts a small set of syntax elements whose effect is as shown in the fig 5.

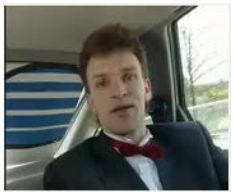

Fig.5a. Original carphone

Fig.5b. Coastguard original

Fig.5c. MissAmerica original

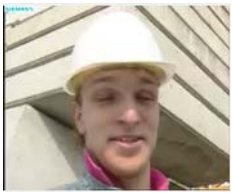

Fig.5d. Foreman original

Fig.5e. Encrypted carphone

Fig.5f. Encrypted coastguard

Fig.5g. Encrypted MissAmerica

Fig.5h. Encrypted Foreman

Fig.5. Original and encrypted frames

The encryption process has been lightweight in the proposed work due to the one-dimensional maps in the technique. Fig 5 reflects the considerable visual degradation because of very small portion of the syntax elements encrypted in the process. Majority of the frame which remains motion-less has very less degradation since the IPMs and trailing ones have less impact without the motion of the blocks.

The visual degradation is one of the primary objectives of the proposed work and it is achieved through the coupling technique described in the earlier section. The results achieved in the PSNR, correlation coefficient, SSIM, etc along with the fig 5 justify that the required encryption is carried out in the proposed work.

5.10. Key Sensitivity analysis

In the chaos encryption, since the start state holds the key to the subsequent states of the chaotic map, the start state must be strong enough to withstand attacks for a maximum time. Sensitivity of the key is assessed by bringing some minor changes to the key sequence and the impact of the change is shown in fig 6.

The analysis based on the experiments of the change in the start state provides evidence to the meeting of the research objectives set in the earlier sections. Being chaotic by itself is a reflection of the high sensitivity towards the initial states. As it can be observed in the Fig.6, the incremental changes brought in to the start state results in the change of encrypted video to a greater extent. The position of the blocks is highly distorted and the more noise can be observed in the encrypted frames. The total length of the key sequence in order to generate the same start state used in the proposed work is 256 * 256 which is equal to 65536 bits. Each of the logistic map need 256-bit length key and the coupling of the logistic maps doubles the requirement. Hence the key space of the overall encryption process is 2^{65536}.

Fig.6a. Original Image

Fig.6b. Original encryption

Fig.6c. Encrypted frame with 0.5% change in start state

Fig.6d. Encrypted frame with 1% change in start state

Fig.6e. Encrypted frame with 1.5% change in start state

Fig.6f. Encrypted frame with 2% change in start state

Fig.6g. Encrypted frame with 2.5% change in start state

Fig.6. Effect of change in start state on the encrypted frames

5.11. Chi squared test

Real time use of video data needs the faster rendering of the video which can be possible if the encryption technique is lightweight. The one-dimensional logistic maps with XOR operation make the proposed technique to use less resources of the system. But, to analyze the impact of the encryption technique, the variance between the recorded and the actual frequencies is calculated using the Chi squared (χ^2) test which is represented by (9).

$$\chi^2 = \sum_{k=1}^{256} \frac{(R_k - A_k)^2}{A_k} \tag{9}$$

Where, R_k is the recorded frequency of the pixels in the encrypted frames
A_k is the expected/actual frequency of the pixels encrypted frames

As per the assumption, the significant level considered in the proposed work is 0.05 and the chi square values are taken as χ^2 (255, 0.05) = 292.27. In order to achieve the uniform distribution, the governing condition $\chi^2_{examined} < \chi^2$ (255, 0.05) is expected to hold true. Autonomous observations are expected when the distribution is followed. The recorded results for the different CIF sequences are shown in the table 8.

Table 8. Chi square Test results

CIF sequences	Chi square values	
	$\chi^2_{examined}$ values	Result
Foreman	248.12	Accepted
Carphone	224.51	Accepted
Coastguard	252.48	Accepted
MissAmerica	233.74	Accepted

The expected theoretical value of 255 against the observed values listed in the table 8 mirrors the correctness of the encrypted data. Assuming that the maximum encrypted value that can be accommodated in the frame is 255, the encrypted values and the frequencies used in the (9) have produced the nearby values comparing to the theoretical data. The scores achieved in table 8 are the result of cross-coupling technique with XOR operation used in the proposed work.

5.12. Comparison

The presented work in this paper selectively choses a small sub set of the syntax elements present in the H.264bit stream. The work is compared with two other recent works which use the chaotic encryption technique to encrypt the videos. When compared with [5] which encrypts considerably big set of syntax elements, the coupling of the logistic maps in the present work has greater impact on the encryption according to the PSNR when compared with the [9] which uses a larger set of syntax elements. The proposed work records the lowest PSNR compared to the other works and is the result of the selected syntax elements and the cross coupled logistic map encryption.

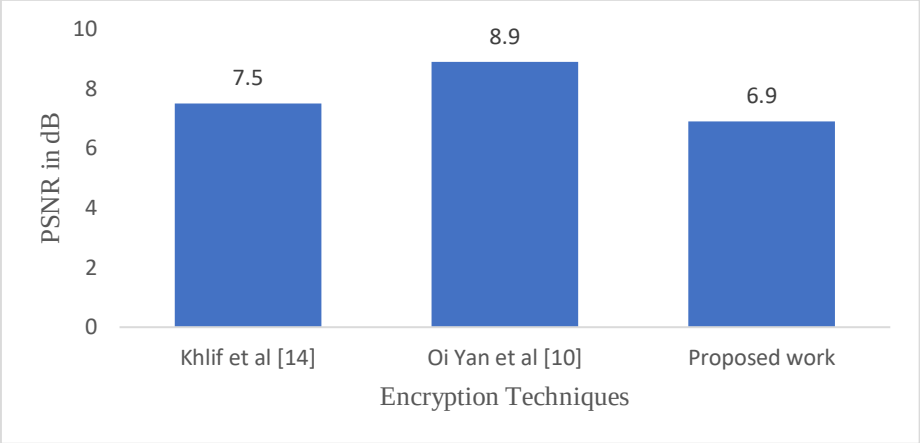

Fig.7. Comparison with the recent works.

Fig 7 shows the comparison of the proposed work with some of the recent works which use the similar set of the syntax elements used in the proposed work.

The encryption technique proposed in this work have been used to explore the properties of the chaotic technique used in the proposed work. The confusion property of the technique is addressed by the key sensitivity analysis and randomness tests, which reflects the degree of unpredictability in the technique.

Property of diffusion is shown by PSNR, NPCR, SSIM and statistical analysis, which also show that the necessary visual degradation is resulted due to the cross-coupling technique. Overall, the results achieved in this section scientifically prove that the proposed encryption technique is robust and can be used in the real time applications.

6. Conclusions

A novel selective video encryption technique to secure the H.264 videos is presented in this work. The present state of the work employs the logistic map has been used in many encryption techniques but in this paper the map is cross coupled with another similar map with different entry conditions. One of the unique properties of the chaotic encryption being the dependence on the start state is efficiently addressed in this work. The congruence rules are used to generate the unique sequence to generate the start states of the both the logistic maps. The results of the proposed work are analyzed using different metrics showing the change in the encryption status with respect to the standalone chaotic maps and cross coupled maps and the work is compared with some of the recent works. The average the present state of the research in video encryption broadly uses standalone chaotic maps, whether it is a three-dimensional or four-

dimensional map, but the analysis presented in this work hints that the cross-coupling technique is an effective way of encrypting the H.264 videos. The proposed technique can be used in the different media streaming applications like medical video conferencing, surveillance videos, Video on Demand (VoD), Pay Per View (PPV), etc. The future work may include priority-based encryption level regulating system which can select the number of syntax elements to be encrypted based on the needs of the application. Further, cross coupling of 4D hyperchaotic systems can be used to generate random more interdependent random numbers for the encryption technique.

References

[1] J. Yun and M. Kim, "JLVEA: Lightweight real-time video stream encryption algorithm for internet of things," *Sensors (Switzerland)*, vol. 20, no. 13, pp. 1–14, 2020, doi: 10.3390/s20133627.

[2] H. K. Arachchi, X. Perramon, S. Dogan, and A. M. Kondoz, "Adaptation-aware encryption of scalable H.264/AVC video for content security," *Signal Process. Image Commun.*, vol. 24, no. 6, pp. 468–483, 2009, doi: 10.1016/j.image.2009.02.004.

[3] S. Sin Myat Than, "Secure Data Transmission in Video Format Based on LSB and Huffman Coding," *Int. J. Image, Graph. Signal Process.*, vol. 12, no. 1, pp. 10–17, 2020.

[4] H. Xu, X. Tong, Z. Wang, M. Zhang, Y. Liu, and J. Ma, "Robust video encryption for H. 264 compressed bitstream based on cross - coupled chaotic cipher," *Multimed. Syst.*, no. 0123456789, 2020, doi: 10.1007/s00530-020-00648-7.

[5] Md. Minhaz Ur Rahman, Mahmudul Hasan Robin, Abu Mohammad Taief, " A New Framework for Video- based Frequent Iris Movement Analysis towards Anomaly Observer Detection", International Journal of Image, Graphics and Signal Processing, Vol.13, No.1, pp. 13-27, 2021.

[6] M. S. Baptista, "Cryptography with chaos," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 240, no. 1–2, pp. 50–54, 1998, doi: 10.1016/S0375-9601(98)00086-3.

[7] A. Shifa *et al.*, "MuLViS: Multi-Level Encryption Based Security System for Surveillance Videos," *IEEE Access*, vol. 8, pp. 177131–177155, 2020, doi: 10.1109/access.2020.3024926.

[8] S. Shafiq, S. Hanif, F. U. Rehman, K. Tariq, and A. Nawaz, "Video Encryption Techniques: A Review," *Proceeding 2019 Int. Conf. Digit. Landscaping Artif. Intell. ICD 2019*, pp. 174–177, 2019, doi: 10.1109/ICD47981.2019.9105707.

[9] L. Chen, N. Shashidhar, and Q. Liu, "Scalable secure MJPEG video streaming," *Proc. - 26th IEEE Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2012*, pp. 111–115, 2012, doi: 10.1109/WAINA.2012.163.

[10] H. Xu, X. Tong, and X. Meng, "An efficient chaos pseudo-random number generator applied to video encryption," *Optik (Stuttg).*, vol. 127, no. 20, pp. 9305–9319, 2016, doi: 10.1016/j.ijleo.2016.07.024.

[11] O. Y. Lui, C. H. Yuen, and K. W. Wong, "Chaos-based selective encryption for AVS video coding standard," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7674 LNCS, pp. 501–512, 2012, doi: 10.1007/978-3-642-34778-8_47.

[12] F. Peng, X. W. Zhu, and M. Long, "An effective selective encryption scheme for H.264 video based on chaotic Qi system," *Int. J. Digit. Crime Forensics*, vol. 5, no. 2, pp. 35–49, 2013, doi: 10.4018/jdcf.2013040103.

[13] S. Li, G. Wang, Y. Wang, and Y. Ning, "Selective encryption for format compliance of MPEG based on coupled map lattice," *Proc. - 2010 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010*, vol. 6, no. 2, pp. 453–458, 2010, doi: 10.1109/ICCSIT.2010.5564070.

[14] N. Khlif, A. Masmoudi, F. Kammoun, and N. Masmoudi, "Secure chaotic dual encryption scheme for H.264/AVC video conferencing protection," *IET Image Process.*, vol. 12, no. 1, pp. 42–52, 2018, doi: 10.1049/iet-ipr.2017.0022.

[15] M. Altaf, A. Ahmad, F. A. Khan, Z. Uddin, and X. Yang, "Computationally efficient selective video encryption with chaos based block cipher," *Multimed. Tools Appl.*, vol. 77, no. 21, pp. 27981–27995, 2018, doi: 10.1007/s11042-018-6022-5.

[16] Y. Song, Z. Zhu, W. Zhang, and H. Yu, "Efficient protection using chaos for Context-Adaptive Binary Arithmetic Coding in H.264/Advanced Video Coding," *Multimed. Tools Appl.*, vol. 78, no. 14, pp. 18967–18994, 2019, doi: 10.1007/s11042-019-7253-9.

[17] Lei, B. Y. and Lo, K. T. and Lei, Haijun, "A New H.264 Video Encryption Scheme Based on Chaotic Cipher 2," International Conference on Communications, Circuits and Systems, (ICCCAS), pp. 373–377, 2010.

[18] S. Cheng, L. Wang, N. Ao, and Q. Han, "A selective video encryption scheme based on coding characteristics," *Symmetry (Basel).*, vol. 12, no. 3, 2020, doi: 10.3390/sym12030332.

[19] X. Zhang, S. Yu, P. Chen, J. Lü, J. He, and Z. Lin, "Design and ARM-embedded implementation of a chaotic secure communication scheme based on H.264 selective encryption," *Nonlinear Dyn.*, vol. 89, no. 3, pp. 1949–1965, 2017, doi: 10.1007/s11071-017-3563-5.

[20] Erwin, Dwi Ratna Ningsih, " Improving Retinal Image Quality Using the Contrast Stretching, Histogram Equalization, and CLAHE Methods with Median Filters", International Journal of Image, Graphics and Signal Processing, Vol.12, No.2, pp. 30-41, 2020.

[21] Qiang Xiao, Liang Chen, Ya Wang, "An Efficient Dimension Reduction Quantization Scheme for Speech Vocal Parameters", International Journal of Information Technology and Computer Science, vol.3, vo.1, pp.18-25, 2011.

[22] S. Etemadi Borujeni and M. Eshghi, "Chaotic image encryption design using tompkins-paige algorithm," *Math. Probl. Eng.*, vol. 2009, 2009, doi: 10.1155/2009/762652.

[23] Padmavathi C, Veenadevi S.V, "An Automated Detection of CAD Using the Method of Signal Decomposition and Non Linear Entropy Using Heart Signals", International Journal of Image, Graphics and Signal Processing, Vol.11, No.2, pp. 30-39, 2019.

Authors' Profiles

Rohit S Malladar received his B.E Degree (Computer Science & Engineering) in 2009 and M. Tech (Computer Science & Engineering) in 2011 from Visvesvaraya Technological University.

He is working as an Assistant Professor, dept of Computer Science & Engineering, Jain Institute of Technology, Davangere, India and has 9 years of experience in teaching. He is certified by Google in mobile application development and has conducted many workshops on Java application development and mobile application development. His technical papers are published in IEEE explore and Springer Lecture Notes series. His areas of interest include image processing, android applications and information security.

R Sanjeev Kunte received his B. E. Degree in Computer Science from Kuvempu University, M.Tech Degree in Computer Science from Visvesvaraya Technological University, PhD Degree in Computer Science from University of Mysore in 2009.

He has 22 years of experience in teaching and research. He has published more than 50 technical papers in reputed Conferences and Journals. His areas of interest include Image Processing, Pattern Recognition, Computer Vision, and Information security. Reviewer for several International Journals and Technical Committee member, Program Committee member for several International Conferences. Resource person for many short-term training programs. Currently he is working as Professor and Head, Department of Information Science & Engineering, in J.N.N. Engineering college, Shivamogga, Karnataka, India.

How to cite this paper: Rohit S Malladar, Sanjeev R Kunte, "Selective Video Encryption Using the Cross Coupling of One-dimensional Logistic Maps", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.5, pp.40-54, 2021. DOI: 10.5815/ijcnis.2021.05.04