Robust Encryption of Uncompressed Videos with a Selective Frame Scheme

Rupali Hole[1], Megha Kolhekar[2]

[1,2]Fr.Conceicao Rodrigues Institute of Technology, Mumbai University, Department of Electronics and Telecommunication, Navi Mumbai Vashi-400703, India

Abstract: ***The wide use of video multimedia applications has made it important to improve the security of video information for streaming it over communication links. In this case cryptography techniques are necessary and the security of video information becomes essential. Existing video encryption scheme address this issue by using chaotic map or standard private key systems. In this paper, we propose an encryption scheme which uses a computationally simple technique like 'SDES' along with a novel frame selection scheme. The use of proposed 'frame selection mechanism and chaotic map encryption' makes the technique easy to implement. Robustness is achieved with the help of 'RSA' encryption on user key parameters. The proposed scheme is evaluated using unique feature such as 'UACI' and 'NPCR'. We tested proposed scheme on videos containing different videos of 'visual correlation' and we find that proposed scheme works reasonably well irrespective of level of 'visual correlation'.***

Keywords: Cryptography, Encryption, Chaotic map, Robust, frame selection mechanism.

1. Introduction

With the fast growth of multimedia applications like video surveillance, video conference, digital video broadcast, distance learning it becomes essential to provide a secure video data transmission. Military over worldwide communicate through private video information. These videos need to be secured from an undesired destination sources. Encryption is the best way to utilize for providing security of videos. Some standard encryption techniques like Data Encryption Standard (DES), Advance Encryption Standard (AES) can be implemented. Digital video is sequence of digital images known as frames. Encryption is performed on an individual frame. In this paper, Simplified DES (SDES) and chaotic map encryption are implemented. The proposed selective mechanism helps user to select frame either for SDES or chaotic map encryption. The selective scheme is easy to implement since it is based on Mean Square Error (MSE) and selection of frames is done within a short interval of time. Key exchange is achieved through Rivest-Shamir-Aldeman (RSA) encryption so as to make system robust.

1.1. Related Work

Most of the authors have reported implementation of compressed video encryption, selective video encryption and chaotic map encryption techniques [1-5]. In compressed videos (MPEG) video comprises of Group of Pictures (GOP) which is a set of Intra coded frames (I-frame), predictive coded frames (P-frame) and bidirectionaly predictive coded frames (B-frame). A frame can be subdivided into small blocks. Motion vector is used to represent block in a frame based on position of the similar block in another picture [17]. In selective encryption some authors have preferred to encrypt only selective part of video like I-frames, motion vectors etc. [2-4]. In chaotic map encryption the pixels are shuffled with respect to its positions. In [1], chaos based encryption is used so as to shuffle the frames. In [2], motion vectors are encrypted. Motion vectors are obtained by block matching using MSE and pixels are also encrypted. In [3], motion vectors with large difference of blocks in P, B frames are encrypted and key is generated through I frame. The encryption of frame is achieved by x-or operation of motion vectors and key. In [4], here only I frames are encrypted which is a selective encryption technique. In [5], encryption is performed on compressed videos in which Discrete Cosine Transform (DCT) coefficients are encrypted and the blocks of frames are shuffled. In [6], SDES encryption technique is discussed in detail.

1.2 Problem Statement

a) To encrypt and decrypt digital video using selective encryption scheme and techniques like SDES and chaotic map.
b) To provide privacy using RSA for key exchange.
c) To provide robustness and flexibility through key design.

1.3 Organization of Paper

Detail of SDES, RSA, proposed chaotic map encryption and decryption are covered in section 2. Ideas and implementations of proposed technique are described in section 3. In section 4, results of proposed techniques are discussed.

2. Preliminaries

2.1 SDES encryption

Simplified data encryption standard was invented by Edward Schaefer. S-DES is simplified version of DES, the only difference is the parameters block size, key sizes used in S-DES are smaller in length compared to DES. It is symmetric encryption scheme. A round of S-DES contains operations like shuffling of bits, permutation, ex-or, substitution, swapping. There are three permutations, initial permutation (IP), inverse of IP (IP^{-1}), expansion permutation(EP). IP achieved transpositions and there are S-boxes in special functionf_k. Swapping of bits and S-boxes are used for confusion and diffusion purpose.

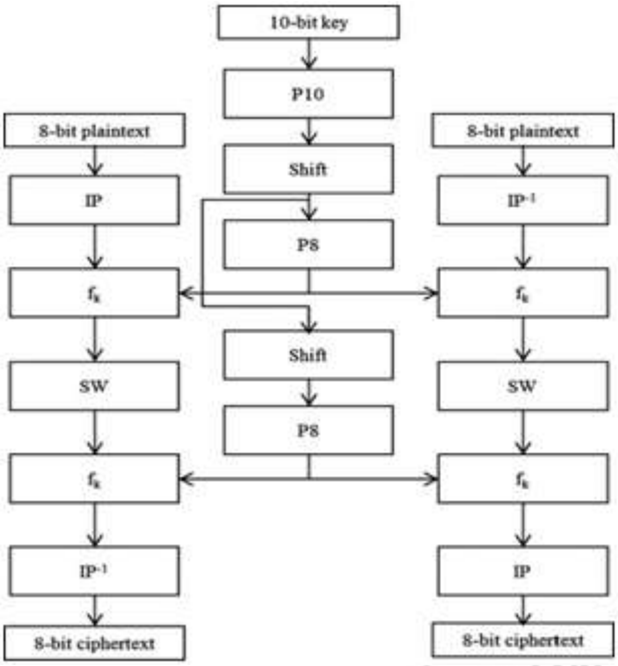

Figure 1: S-DES encryption scheme [25]

S-DES encryption involves following five functions:

a) Initial permutation(IP)
b) Function f_k that involves permutations, shifting and S-Box.
c) SW, switches the halves of the data
d) The function f_k is repeated again
e) Inverse initial permutation(IP^{-1})

Details of these functions are found in [6]

2.2 RSA encryption [7]

It is a public key cryptosystem that was originated in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA uses two keys one is private while other is public key. Private Key is kept secret between sender and desired receiver. RSA is based on modular arithmetic and integer factorization problem in cryptography.

Algorithm for RSA encryption and decryption

a) *p,q:* two distinct prime numbers
   Compute $n = pq$, choose p, q such that $n > M$ where M is original message.
   $\varphi = (p-1)(q-1)$, where φ is Euler's coefficient function
b) Choose e such that $\gcd(e, \varphi) = 1$
c) Choose d such that $mod(de, \varphi) = 1$
d) Compute encrypted message C, $C = M^e mod\ n$
e) To decrypt encrypted message compute, $M = C^d mod\ n$

2.3 Chaotic map encryption

It is a symmetric key encryption scheme in which pixels of a frame are mapped within itself by using some shifting parameters. Mapping is shifting of position of each pixel. This encryption technique takes less time compared to DES, S-DES and other techniques. Let the size of video be M× N. Pixels in a frame can be denoted by a vector. The Proposed chaotic map encryption technique is discussed in section 2.3.1

2.3.1. Methodology for encryption and decryption [1]

Choose x_1 and x_2 as shifting parameters for even and odd row number respectively in an original image. Such that $0 < x_1, x_2 < N$.

Compute transposed image, img1 using following transposition equations.

$$X'_{even\ row,\ k} = X_{even\ row,\ mod\ (j+x_1,\ N)}$$

$$X'_{odd\ row,\ k} = X_{odd\ row,\ mod\ (j+x_2,\ N)}$$

Where j is a column number

Now choose x_3 and x_4 as shifting parameters for even and odd column number respectively in img1. Such that $0 < x_3, x_4 < M$.

Compute transposed image, img2 using following transposition equations.

$$X'_{p,\ even\ column} = X_{mod\ (i+x_3,\ M),\ even\ column}$$

$$X'_{p,\ odd\ column} = X_{mod\ (i+x_4,\ M),\ odd\ column}$$

In case of decryption the shuffled pixels are relocated to its original position. Compute the transposed image, img3 with the help of following transposition equations applied on img2.

$$X_{i,\ even\ column} = X'_{mod\ (p-x_3,\ M),\ even\ column}$$

$$X_{i,\ odd\ column} = X'_{mod\ (p-x_4,\ M),\ odd\ column}$$

Now compute transposed image, img4 by applying transposition equations on img3 as follows:

$$X_{even\ row,\ j} = X'_{even\ row,\ mod\ (k-x_1,\ N)}$$

$$X_{odd\ row,\ j} = X'_{odd\ row,\ mod\ (k-x_2,\ N)}$$

After these computations of decryption img4 is a final decrypted image which is same as original image.

3. Proposed Algorithm

SDES is computationally more demanding compared to chaotic map encryption it is implemented on few selected frames. Digital color video is comprised of R-G-B components. In RGB all the three components contain visual information about the video, but encrypting all of them is computationally inefficient. Encryption can be made more efficient by working in Y-Cb-Cr domain and modifying only Y components. This makes scheme simple and flexible. In proposed work we give an easy to implement selection mechanism for selection of frames for SDES encryption. All the parameters are flexible and can be chosen by user.

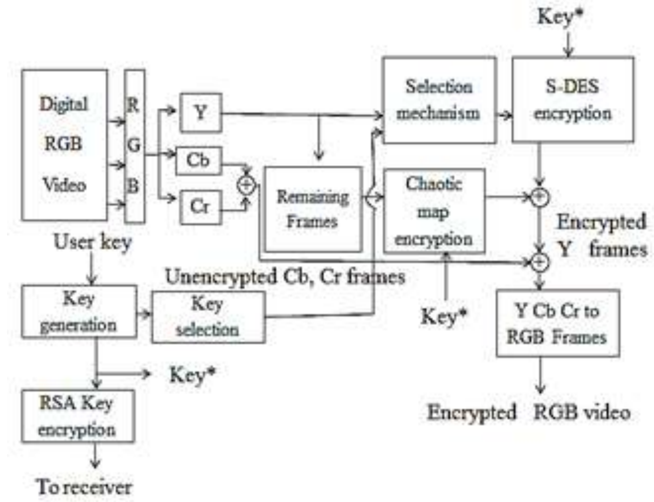

Figure 2: Encryption process

3.1 Selection mechanism

It is executed as follows:

a) Let F_V be a video which is a collection of K frames
$F_V = [F_1, F_2, F_3 \dots\dots. F_K]$
Each F_i can be treated as independent image.

b) F_I is subset of F_V with a selection parameter x
$F_I = [F_{i_0}, F_{i_1}, F_{i_2}, \dots. F_{i_n}]$
Where i_0 =1, $i_1 = 1 + x$, $i_2 = 1 + 2x, \dots.$ $i_n = 1 + (K - x)$

c) Compute adjacent frame MSE in set F_I to get vector F_{IMSE} as follows:
$F_{IMSE} = \{MSE(F_j, F_{j+1})\}\ \forall\ j\ \in \{i_0, i_1, i_2, \dots i_n\}$
Mean square error is given by:

$$MSE = \frac{\sum_{(i,j)}[x(i,j) - \hat{x}(i,j)]^2}{M \times N}$$

Where $x(i,j)$, the pixel at position (i,j) of the frame in vector F_I and $\hat{x}(i,j)$ is the pixel at position (i,j) of consecutive frame.

d) Let $A = median(F_{IMSE})$ and $C = maximum(F_{IMSE})$,
Choose frame in F_I having its MSE equal to B

$$(A - \Delta) \leq B \leq C \quad (1)$$

$$\Delta = \alpha_L + \frac{\alpha_H - \alpha_L}{100} \times \varphi \quad (2)$$

Where, $A \leq \alpha_H$, $\alpha_L \leq$ C and 0 <φ< 100.

Let S_I be set of frames that satisfy condition (1) and S_{NI} be a set of frames that does not satisfy condition (1) and S_{NO} be a set of frames those are not a part of vector F_I.
Frames in S_I are encrypted using ten bits key SDES as discussed in section 2.1. While frames in vector S_{NI} and S_{NO} are encrypted using proposed chaotic map encryption schemes as discussed in section 2.3.

In selection mechanism selection of frames is done based on difference between consecutive frames. By applying MSE selection mechanism becomes easy to implement and computationally efficient.

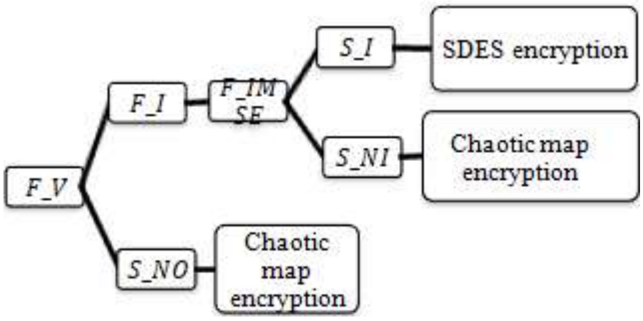

Figure 3: Sequence to Execute Set and Sub set of Frames in Selection Mechanism

3.2 RSA key encryption

The key parameters applied on SDES and chaotic map encryption is kept confidential by applying RSA public key cryptosystem as discussed in section 2.2. After encryption of parameters those key values are shared with intended receiver.After overall encryption all Y-Cb-Cr frames are merged together and transformed to RGB domain so as to get RGB encrypted video.

3.3. Run Length Encoding (RLE)

In order to communicate SDES encrypted frames and other frames to the intended receiver. Bit one is assigned to frames in S_I and bit zero is assigned to frames in S_{NI} and S_{NO}. RLE is performed on this sequence of 1's and 0's so as to extract selected framesS_I . RLE is explained in [8].

3.4. Decryption scheme

Choose the frames same as in vector S_I for SDES decryption by applying RLE decoding function. Corresponding frames with zero bits are encrypted using chaotic map. SDES and chaotic map encryption are symmetric key encryption. SDES requires key K and chaotic map requires x_1, x_2, x_3, x_4.

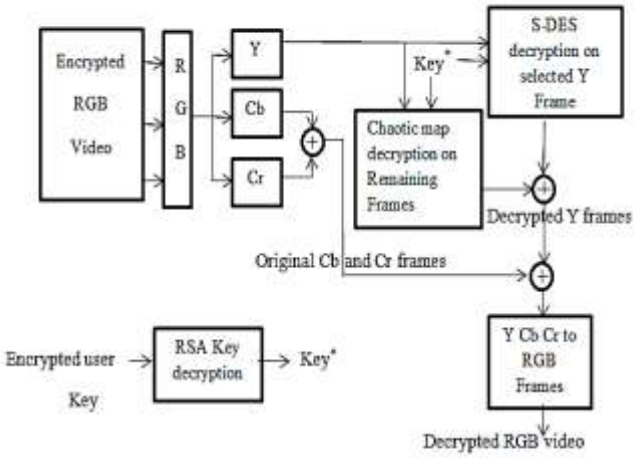

Figure 4: Decryption process

User key parameters are selection parameter$x$, key for SDES K, shifting parameters for chaotic map x_1, x_2, x_3, x_4. The key structure of proposed scheme becomes as shown in table1.

Table 1: User key and its length

Sr. no.	User key parameters	Length of maximum Number of bits
1	x	5
2	K	10
3	x_1	$\log_2 N$
4	x_2	$\log_2 N$
5	x_3	$\log_2 M$
6	x_4	$\log_2 M$

In table 1, M is number of rows and N is number of columns of video.

4. Implementation, Results and discussions

Experiment was carried out on five videos and noted as follows. Implementation is in MATLAB R2009a with processor Intel core i5 @ 1.80 GHZ speed.

Table 2: The encryption and decryption time of videos [18-22]

Video	Total number of frames (N)	Number of SDES encrypted frames(n)	Encryption time in seconds ($E_{time\,1}$)	Decryption time in seconds ($D_{time\,1}$)
1	300	1	249.47	191.73
2	400	2	286.77	274.14
3	240	4	445.75	317.95
4	500	5	890.50	603.81
5	300	13	1321.84	1204.89

As observed from table 2, encryption time is directly proportional to n .

$$E_{time\,1} \propto n$$

Encryption time increases with n hence overall time for encryption also raises. Images are statistical objects hence pixels of different frames in a same video has no correlation amongst them. Therefore $E_{time\,1}$ does not depend on N. These observations are plotted in a graph as shown in figure 5.

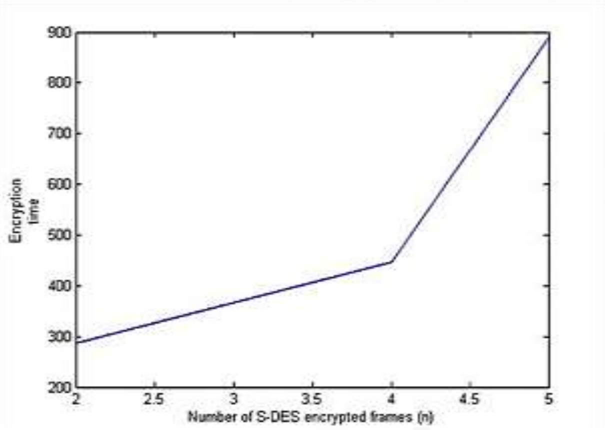

Figure 5: Graph of Encryption time v/s number of S-DES encrypted frames

By choosing the different values of selection parameter x the number of frames in S_I and total encryption time and decryption time are noted in table 3.

Table 3: The encryption and decryption time for different x values [22]

Sr. no.	x	Number of SDES encrypted frames(n)	Encryption time in seconds ($E_{time\,2}$)	Decryption time in seconds ($D_{time\,2}$)
1	15	17	1445.10	1392.31
2	20	13	1321.84	1204.89
3	25	11	1001.59	826.87
4	30	10	831.81	791.94
5	40	7	684.06	554.23

According to table 3, as value of x increases the encryption time reduces.

$$E_{time\,2} \propto \frac{1}{x}$$

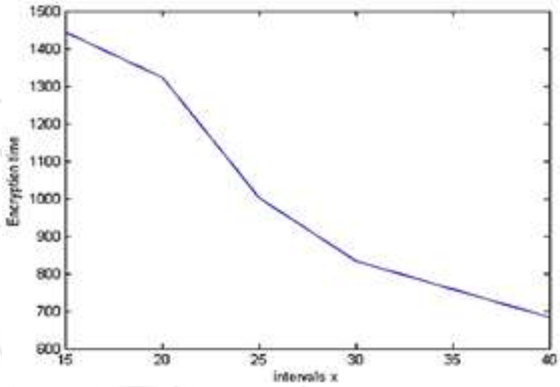

Figure 6: Analysis of Encryption time for certain values of interval values x

From table 2, video [21] was encrypted using MATLAB R2009a that gives results as shown in figure 7 for SDES encryption and decryption of frame.

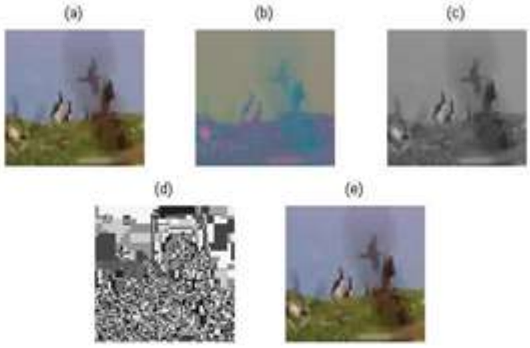

Figure 7: (a) Original RGB frame, (b) converted Y-Cb-Cr frame, (c) Y frame, (d) S-DES encrypted Y frame, (e) Decrypted frame

The results for same video [21] using chaotic map encryption of frame are given in figure 8.

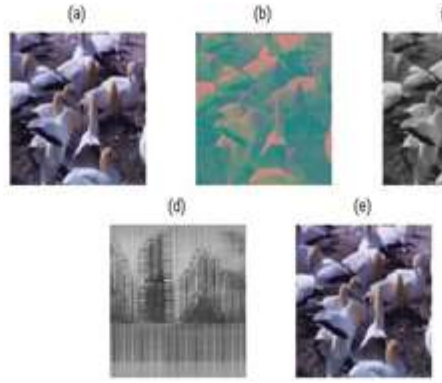

Figure 8: (a) Original RGB frame, (b) converted Y-Cb-Cr frame, (c) Y frame, (d) chaotic map encrypted Y frame, (e) Decrypted frame using chaotic map.

Table 4: Tasks performed while encryption and their respective computational time for video [21] with 500 frames

Sr. no.	*Tasks performed*	*Computational time (seconds)*
1	Selection mechanism	0.2
2	SDES encryption	194.336
3	Chaotic map	94.22

4.1 Evaluation parameters

4.1.1 Number of pixel change rate (NPCR)

It is a common measure used to check the effect of one pixel change on the entire image [10].

$$NPCR = \sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times \frac{100}{M \times N}$$

Where, $D(i,j) = 0$ if $Io(i,j) = IENC(i,j)$ if not then $D(i,j) = 1. I_O(i,j)$and $I_{ENC}(i,j)$ are the pixels values of original and encrypted images at position(i,j). M is number of rows and Nis number of columns.

4.1.2 Unified average changing intensity (UACI)

UACI is helpful to identify the average intensity of difference in pixels between the two images [10].

$$UACI = \sum_{i=1}^{M}\sum_{j=1}^{N} [I_0(i,j) - I_{ENC}(i,j)] \times \frac{100}{M \times N}$$

Results for NPCR and UACI are given in table 5.

Table 5: Evaluation parameters for videos [18-21]

Video	*NPCR*	*UACI*
1	4.4792 e^6	765
2	7.9702 e^6	1020
3	2.8766 e^6	612
4	1.7465 e^7	1.5198 e^3
5	4.4968 e^6	765

The higher value of NPCR shows the factor by which original and encrypted video differs. Value of NPCR should be high.Even if encrypted and original video differs visually its intensity should be almost similar hence The value of UACI parameter should be low [10]. These observations are noted in table 5.

4.2 Visual correlation

We estimate visual correlation in a video by number of scene changes in it and the number of consistent frames in one scene we call video to be highly correlated, if it contains a reasonable number of frames of same scene. If it does not, we call it low correlated video and otherwise moderate correlated.

4.2.1 Implementation on different video

The encryption is applied on Y-frames hence results for Y frames are shown in figure 9, figure 10 and figure 11.

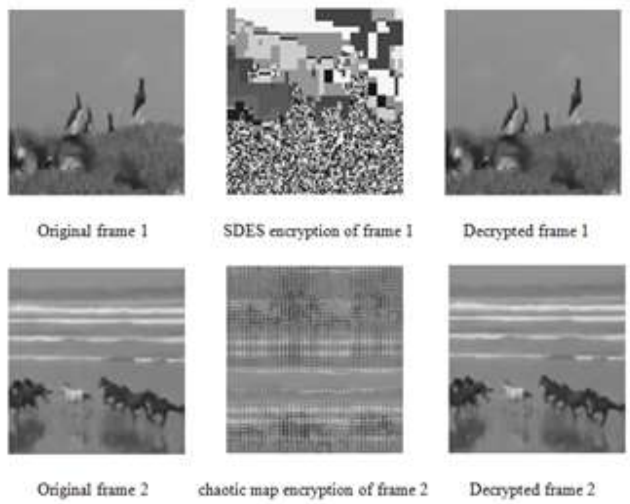

Figure 9: Results of encryption and decryption for highly correlated video 'wildlife.mpg' [21]

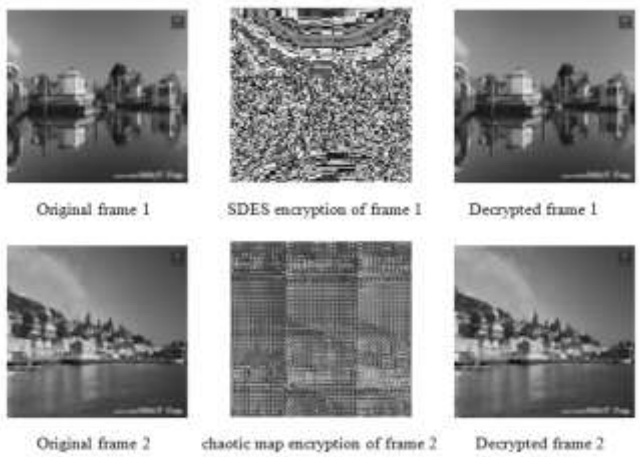

Figure 10: Results of encryption and decryption for moderately correlated video 'River.mpg' [23]

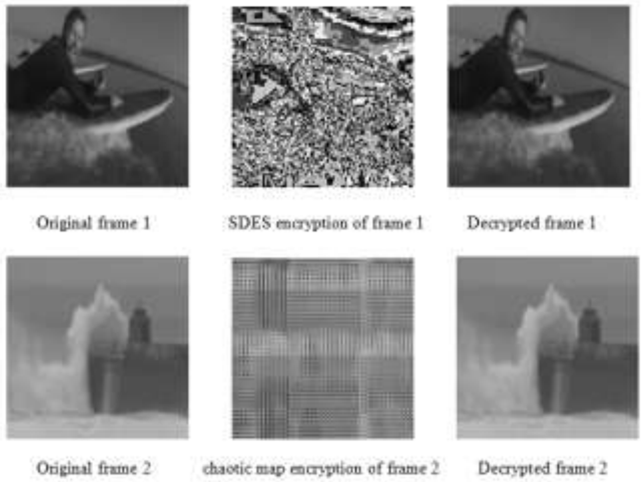

Figure 11: Results of encryption and decryption for low correlated video 'British.mpg' [24]

If key used while SDES encryption is changed by one bit while performing decryption on same video it gives the result as shown in figure 12, which shows if correct key is not known to user then it is difficult to decrypt and obtain original video information. Hence the scheme is found to be reasonably robust for one bit change in the key.

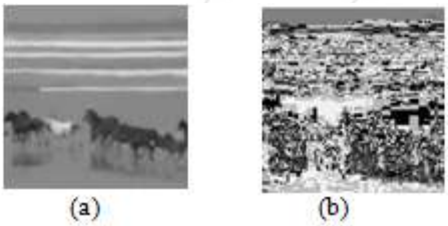

Figure 12: (a) Perfectly decrypted frame with correct key (b) Wrong decryption of frame using wrong key [21]

5. Conclusion

In this paper, we proposed selective encryption mixed scheme for digital videos which uses SDES and proposed chaotic map for encryption. The proposed scheme is found to be easy to implement due to a simple selection mechanism, simplified DES and shuffling maps. Robustness is added by using RSA for key transfer. Time taken for conversion from R-G-B to Y-Cb-Cr including proposed scheme takes approximately 10 minutes for 500 frames for 100×100 size. . Speed for encryption also depends on speed of microprocessor of a system. Evaluation parameters show very good performance as far as NPCR, UACI is concerned.

References

[1] Manish Kumar, D. C. Mishra et al., "A first approach on an RGB image encryption", Optics and Lasers in Engineering 52 (2014) 27–34, 28.
[2] Hwa Young Um, "Selective video encryption of distributed video coded bit streams and multicast security over wireless networks", A Thesis Submitted to the Faculty of Purdue University, Aug 2006, 48, 55, 62
[3] Dinesh Goyal, Naveen Hemrajani, Suresh Gyan Vihar, "Novel Selective Video Encryption for H.264 Video", international journal of information security science 220-221
[4] M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan. "Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard", International Journal of Computer Theory and Engineering, 221
[5] Qiuhua Wang, Xingjun Wang, "A New Selective Video Encryption Algorithm for the H.264 Standard", International Conference on Progress in Informatics and computing 2014, pp. 277.
[6] Dr. K. S. Ooi, Brain Chin Vito, "Cryptanalysis of S-DES", University of Sheffield Centre, Taylor's College, April 2002, 8-13.
[7] Nentawe Y. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment", IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013, 2-11.
[8] Árpád Huszák, Sándor Imre, "Analysing GOP Structure and Packet Loss Effects on Error Propagation in MPEG–4 Video Streams", Fourth International Symposium on Communications, Control and Signal Processing (ISCCSP), IEEE 2010, pp. 1-2
[9] Haojie Shen, Li Zhuo, Yingdi Zhao, "An efficient motion reference structure based selective encryption algorithm for H.264 videos", Published in IET Information security, 2013, 199-200.
[10] Lini Abraham, Neenu Daniel, "Secure image encryption algorithms: a review", International journal of scientific & technology research volume 2, issue 4, April 2013. Pp. – 187-188
[11] Steven Gordan "Block Ciphers and DES, security and cryptography", 25 November 2009.
[12] William Stallings, "Cryptography and Network Security", Fourth edition 2006
[13] Seohyun Jeong, Eunji Lee, Sungju Lee, Youngwha Chung, Byoungki Min, "Slice-Level Selective Encryption for Protecting Video Data", The International Conference on Information Networking, IEEE 2011, 54-55.
[14] Priyanka Agrawal, Manisha Rajpoot, "Fast and Secure Selective Encryption Scheme using Grid Division Method", International Journal of Computer Applications, August 2012.
[15] Saurabh Sharma et al. "A Study on Different Approaches of Selective Encryption Technique", International Journal of Computer Science & Communication Networks, Vol 2(6), 658-662, pp. -660.
[16] Jayshri Nehete et al., "A Real-time MPEG Video Encryption Algorithm using AES", Bharat Electronics Ltd.
[17] Khalid Sayood, "Introduction to data compression", Third edition, 571, 592-594.
[18] https://www.youtube.com/watch?v=21rQEKKN0OA&feature=youtu.be
[19] https://www.youtube.com/watch?v=BSSBbeeuV5c&feature=youtu.be
[20] https://www.youtube.com/watch?v=SF_xhxvSOLA&feature=youtu.be
[21] https://www.youtube.com/watch?v=a3ICNMQW7Ok&feature=youtu.be

[22] https://www.youtube.com/watch?v=vPz4Akw0Fdw&feature=youtu.be
[23] https://youtu.be/IVx6ZlksMJw
[24] https://youtu.be/nCncIgF7Pfc
[25] SDES encryption algorithm http://ars.els-cdn.com/content/image/1-s2.0-S1566253513000298-gr5.jpg

Author Profile

Ms. Megha Kolhekar received her B.E. (Electronics) from Nagpur University in 1993 and M. Tech. in communication from IIT Bombay in 2005. She has been with Fr. C. Rodrigues Institute of Technology, Mumbai University, since 1997, where currently she is Associate Professor with the Electronics and Telecommunication Engineering Department. Her interests include Image Processing, Video Encryption-Decryption and Wireless Sensor Networks.

Ms. Rupali Hole obtained her bachelor of engineering degree in Electronics and Telecommunication Engineering from Mumbai University in 2015. She is pursuing Masters of Engineering in Electronics and Telecommunication Engineering from Fr. Conceicao Rodrigues Institute of Technology in 2017. Her research interest includesvideo processing, Image processing, Cryptography.