International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 1, January-2014, pp: (91-96), Impact Factor: 1.252, Available online at: www.erpublications.com

A Novel Lightweight Encryption Scheme for Multimedia Data

Special focus on Video Processing through Chaos Based Transformations

Rajan Gupta[1], Saibal K. Pal[2], Neeharika Chaudhary[1]
[1]Department of Computer Science, [2]SAG Lab
[1]University of Delhi, [2]DRDO, Delhi, INDIA

Abstract: The usage of Multimedia data has increased by many folds in recent years. And with so many different types of devices available to access the data, it becomes imperative to protect its sanctity. In this paper, a novel lightweight encryption scheme using a secret key has been proposed for multimedia data especially Videos. Chaos based maps has been used to provide an apt level of confusion and diffusion process at different levels of Video Processing. Proposed technique has a high encryption rate and performs well even with the videos with excessive redundant data. Security Analysis has been performed to validate the high security features against different types of Statistical and Differential attacks and helps to prove the effectiveness of proposed system.

Keywords: Chaotic maps, Lightweight Schemes, Multimedia Encryption, Security Analysis, Video processing.

I. INTRODUCTION

Cryptography [1, 2] is the science of hiding and sending the information in such a way that it cannot be deciphered by any middle person. It has been in practice since cave era for humans where it was used by early man to communicate secretly or to encrypt the whole message. The applications which developed for data security were related to Cryptography and Steganography (Data Hiding). Cryptography [3,4] deals with the development of techniques for converting information between intelligible and unintelligible forms. It deals with the content confidentiality and access control. The process by which the multimedia is changed into another form in intelligible manner is called Encryption. This process gives the encrypted data/cipher data. The process of recovering original data from encrypted data is called decryption process.

Since the data storage and communication was not too large during earlier days, so security was not a major issue with data storage and its retrieval. But with the rapid growth of computer networks and advancement in information technology and communications [5, 6], not only the regular data but also the amount of multimedia transmission over internet and wireless network has grown tremendously [7]. However, this convenience also causes substantial decrease in multimedia security as one can make thousands of identicalcopies of a piece of information stored electronically and each is indistinguishable from original. So, the security of multimedia data becomes very important for current environment and for the future data transmission as well.

There are three prominent applications of digital data protection [8, 9] from unauthorized eavesdropping, i.e. Cryptography, Steganography and Digital Watermarking. Among these, Cryptography is widely used to provide high level of data security. The traditional text encryption algorithms such as Data Encryption Standard (DES),Rivest, Shamir and Adleman (RSA) and Advanced Encryption Standard (AES) works strongly on textual data but are not preferred for multimedia data especially videos. This is accounted for two prime reasons. First one is that the video size is very large as compared to the simple text size therefore the traditional text cryptosystems take longer time to encrypt the video data. The second is that in the traditional cryptosystems the size of decrypted text must be equal to the original text size. However this requirement is not necessary for video data due to the characteristic of human perception, a smalldistortion in decrypted video is usually acceptable. In secure communications using cryptography, which is the main focus of the present work, the encryption and decryption operations are guided by one or more keys [10, 11].

Techniques that use the same secret key for encryption and decryption are grouped under private key cryptography. Alternately, encryption and decryption keys are different or computationally it may not be feasible to derive one key even though with the knowledge of other key, such cryptographic methods are known as public key cryptography.There are two common principles to design a cryptographic system: Confusion and Diffusion. Diffusion or Substitution is the increasing of independency of the statistics of cipher on the statistics of the plain text, while the Confusion or permutation is the shuffling of information from one into many, to hide the statistical structure of the message. Similarly chaos-based system developed to solve the purpose of permutation and substitution. Since chaotic systems has characteristic like ergodicity, sensitive dependency on initial conditions and random like behaviour, they came into good usage for data processing especially Multimedia. These properties are ofgreat importance in permutation and substitution process.The present work focuses on the development of private key chaos-based video cryptographic algorithm for providing high level of security [12, 13, 14].

The rest of the paper is organized as follows. Section 2 discusses the existing algorithm and in section 3 Proposed algorithm is discussed. In Section 3 the Security Analysis and Results are presented and finally Section 4 presents the conclusion.

II. EXISTING ALGORITHM

In the existing algorithm [6], video frame values are rearranged using Arnold's Cat map defined in Equation 1 and then these values are changed using the 1D-Logistic map defined by Equation 2.

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} \leftarrow \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} . \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod\ N) \quad (1)$$

$$X_{n+1} = 4 \times X_n \times (1 - X_n) \quad (2)$$

The values of 'a' and 'b' in Cat map are randomly generated from 0 to 256 using 256 bits encryption key. Cat map transformation is applied on Y component of YCbCr frames. Each pixel is XORed with $Zi = (X_n * 10^5) \bmod 256$, where X_n is generated using logistic map and X_0 is generated as initial input number in (0, 1) using encryption key. Diffused data is combined back with CbCr component. All the diffused frames are combined to form the encrypted video. A block diagram of existing scheme is show in Fig. 1.

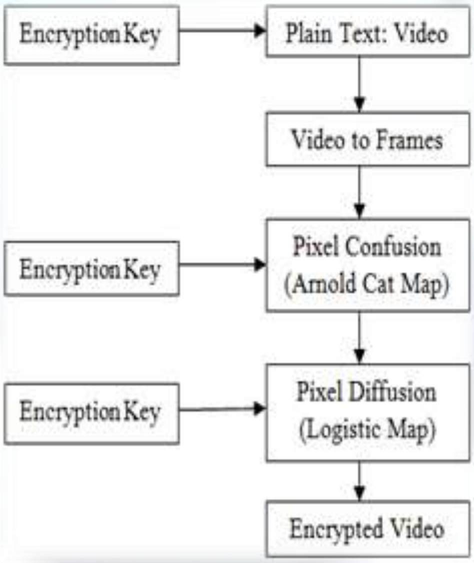

Figure 1.The Existing Algorithm

III. PROPOSED ALGORITHM

There exists a strong correlation among adjacent samples in frames of any video. To encrypt this video this strong correlation must be erased by using a symmetric key dependent process. The proposed encryption algorithm does this by modifying the pixel values of the frames as well as scrambling the bits of the resultant pixels of the frames, and reordering the frame sequence thereby providing multilayer security. Basic scheme is shown in Fig. 2.

The video is divided into frames which are selected one by one for the encryption process. The values are generated using a key and circle map for the diffusion process of pixels in a frame. This diffused matrix is used for the bit confusion process with help of another key B and Arnold cat map[6]. Now the bits are converted to decimal numbers in the range of 0-255 and the frames are now diffused with the help of Key C with Logistic map[6]. Finally frame shuffling id done using Key D and Logistic map. These all keys (A-D) are of256 bits and are generated from User Key.Step by step encryption method is show as follows:

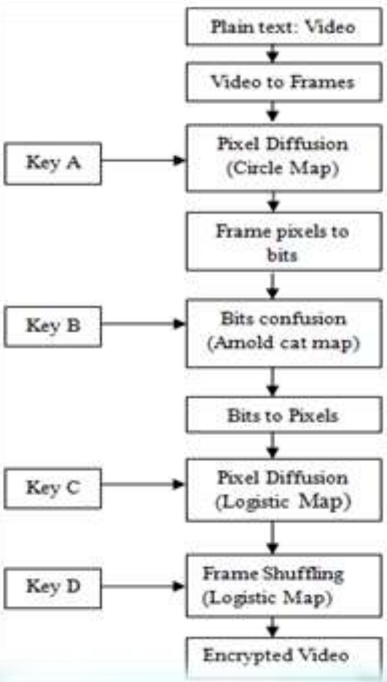
Plain text: Video
Video to Frames
Key A
Pixel Diffusion (Circle Map)
Frame pixels to bits
Key B
Bits confusion (Arnold cat map)
Bits to Pixels
Key C
Pixel Diffusion (Logistic Map)
Key D
Frame Shuffling (Logistic Map)
Encrypted Video

Figure 2.The basic 3 level of security scheme

Encryption (Video, User Key)

1. Divide the input Video into frames and convert each frame to YCbCr domain. All operations are performed on Y component only.
2. Generate 4 different keys A, B, C & D from the User input key.
3. In order to disturb the high correlation among pixels, we adopt Circle map to diffuse the pixels of each frame. Key A and Circle map defined in (3), are used to
   $X_{n+1} = k_1^{1/2} + (k_2\times X_n) + \sin(2\pi\times k_3\times X_n)$ (3)
   wherek_1, k_2, k_3, X_0 are initial parameters randomly generated using Key A. An array of size equivalent to frame size is obtained from this step.
4. Frame matrix is XORed with the map generated from step 3.
5. Convert pixels into binary format and store them bit-wise.
6. Arnold Cat map, defined in (1), is applied to matrix obtained from step 5 for changing the bits position .Initial valuesof a, b and x_0 are generated from Key B.
7. The binary format is changed back to decimal numbers and new pixel values retained in matrix. Convert it into one dimensional data with M values.
8. Logistic map shown in (2) is used to generate M values .X_0 is random value from 0 to 1 depending upon the Key C.XOR each with pixel with $Z_i=(X_n*10^6)$ mod 256todiffuse its value. Convert diffused data into two dimensional array and recombine with CbCr component.
9. After each frame is encrypted, frames are reordered with the help of Key E and Logistic map shown in (2).
10. Frames are combined to get the encrypted video.
    We have used YCbCr color space as RGB signals are not efficient as a representation for storage and transmission, since they have a lot of redundancy. To create high level of confusion, pixels have been converted to bits level and then confused further. Similarly the decryption process has been used with same user keys to decrypt the video.

IV. Security Analysis and Discussion

The code has been developed in MATLAB 2013a [15] on an Intel core I3 processor with 4GB Ram and 320 GB Hard disk. Security analysis is the major challenge in any cryptosystem. A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute force attacks. The security of the proposed algorithms is investigated for video under the statistical attacks, and the differential attacks. Normal videos and white video has been analysed.

A. *Statistical Analysis*

To prove the robustness of the proposed algorithm, statistical analysis has been performed which demonstrates its superior confusion and diffusion properties and strongly resisting nature against the statistical attacks. This has been shown by using the Histogram and Correlation coefficient.

- Histogram*:* It illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. An attacker can analyse the histograms of an encrypted video frames by using some attacking algorithms to get some useful information of the original video. The histograms of selected plain frames and their corresponding encrypted frames are shown in Fig.3-7. It can be seen that, the histogram of the encrypted frame of proposed algorithm is fairly uniform.

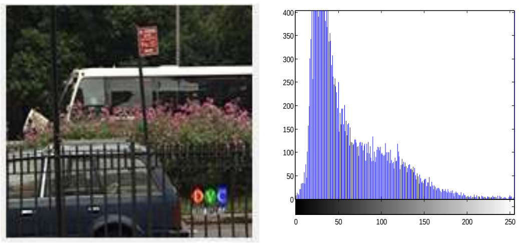

Figure 3.The First Frame of Video and its Histogram

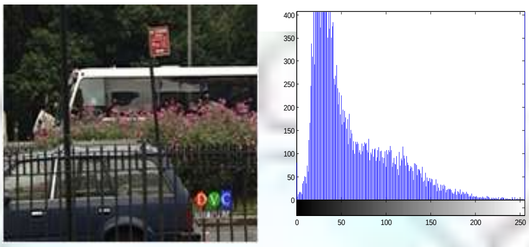

Figure 4.The Second Frame of Video and its Histogram

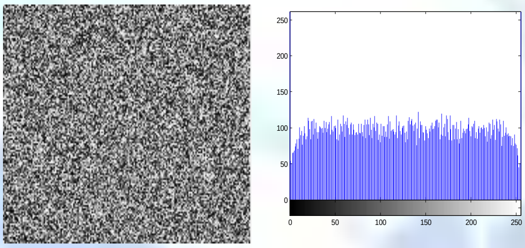

Figure 5.The First Encrypted Frame of Video and its Histogram

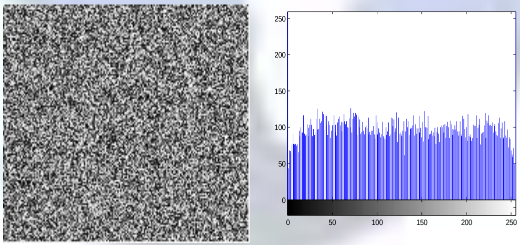

Figure 6.The Second Encrypted Frame of Video and its Histogram

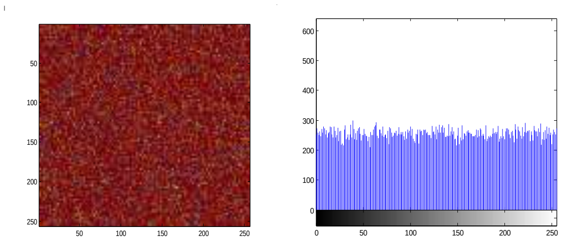

Figure 7.The Encrypted White Image and its Histogram

- Correlation Coefficient: Correlation coefficient is a measure of the strength and direction of the linear relationship between two variables. For this calculation, we have used the following two formulas:

$$r_{xy} = \mathrm{cov}(x,y) / (D(x)D(y))^{1/2} \tag{4}$$

$$\mathrm{cov}(x,y) = E\{ (x-E(x)) \times (y-E(y)) \} \tag{5}$$

Where E(x) is the estimation of mathematical expectations of x, D(x) is the estimation of variance of x,andcov(x, y) is the estimation of covariance between x and y considering x and y are pixel values of two adjacent pixels in the frame. The correlation coefficient between two vertically as well as horizontally adjacent pixels in the original and Encrypted frames is calculated using (4).It is clear from Table I that two adjacent pixels in the original frames are highly correlated. On the other hand, the pixels in the proposed algorithm have negligible correlation. If we interchange the order of sub-algorithms i.e. Arnold cat map performed on pixels followed by circle map performed on bits still get negligible correlation. Correlation close to zero reflects that the proposed algorithm is highly secure.

TABLE I. Correlation Coefficient of Original and Encrypted Frame

Frame	**Adjacent Pixel Orientation**		
	Horizontal	***Vertical***	***Diagonal***
Original Frame 1	0.8908	0.8365	0.7537
Existing Algorithm[6] Frame 1	-0.0116	-0.0206	-0.0001
Proposed Algorithm Frame1	-0.0097	-0.0041	0.0032
Original Frame 2	0.8893	0.8367	0.7513
Existing Algorithm[6] Frame 2	-0.0134	-0.0142	-0.0047
Proposed Algorithm Frame 2	0.0001	0.0092	0.0072

B. *Differential Analysis*

In general, a desirable property for an encrypted video frames is being sensitive to the small changes in plain frames (e.g., modifying only one pixel). The attacker may make a slight change in the input frame and observe the changes in the encrypted frame. In this way, he/she may be able to find some meaningful relationship. We have measured the number of pixels change rate (NPCR) as well as unified averaged changed intensity (UACI) to see the influence of changing a small percentage of pixels in the original frame on the encrypted frame produced by the proposed algorithm. To calculate NPCR, consider two ciphered frames C1 and C2, whose corresponding plain frame have only one pixel difference. The values of each pixels in C1 or C2 is labelled C1(i, j) and C2(i, j) respectively. If we define a bipolar array D with the same size as frame C1 or C2, with D(i, j) being determined by C1(i, j) and C2(i, j): if C1(i, j) = C2(i, j) then D(i, j) = 0, otherwise D(i, j) = 1. Then calculating NPCR (Number of Pixels Change Rate) by

$$\text{NPCR}= ((\textstyle\sum_{i,j} D(i,j) / (W\times H))\times 100\% \qquad (6)$$

Where W is width and H is height of C1 or C2. Test is performed on one-pixel change influence on video. NPCR is approximately 99.06% in both frames, which indicates that with a swift change in the original video, the ciphered video will be significantly changed. The UACI, on the other hand, measures the average of intensity – difference between the pixels of two ciphered images – and is defined by the following equation.

$$\text{UACI} = \textstyle\sum_{i,j} | C1(i,j) - C2(i,j) | /255 \ \times (1/W\times H)\times 100\% \qquad (6)$$

The UACI for proposed algorithm is found to be 33.49% using (6) indicating that the rate of influence due to one-pixel change in original frame is high. The result of these two tests shows that the proposed cipher is sensitive to a minor change in original frame.

Also the value of existing algorithm [6] was shown to have improvement over traditional schemes like AES for multimedia security, so we can say that the proposed scheme is better than traditional scheme too as it is an enhanced version of the existing scheme.

V. CONCLUSION

The result shows good readings for various types of attacks. The algorithm not only exploits the properties of chaotic functions but also dissipate pixels into different level for better security of the algorithm. The role of key is important and the space has been kept large so that it becomes difficult for the attacker to attack the cipher frame.

The future scope includes the usage of chaotic functions in a more rigorous ways to exploit the process of encryption more. And the applications of the process are in all forms of Image and video processing for purpose of cryptography, Digital Image Processing and Steganography.

REFERENCES

[1]. Stinson, D.R. Cryptography: Theory and practice. Ed 3rd, 1, Chapman & Hall, 2005.
[2]. Menezes, A.J.; Oorschot P.C.van & Vanstone, S. The handbook of applied cryptography, CRC Press, 1997.
[3]. William Stallings,Cryptography and Network Security,Prentice Hall,2011
[4]. John E. Canavan, " The Fundamentals of Network Security," Artech House, February 2001, 350 pages.
[5]. M.A. Mohamed, F.W. Zaki and A.M. El-Mohandes**,"**Novel Fast Encryption Algorithms for Multimedia Transmission over Mobile WiMax Networks **",** IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 3, November 2012,p.60-67.
[6]. M.A. Mohamed, F.W. Zaki and A.M. El-Mohandes**,** "Enhanced Diffusion Encryption for Video Transmission over Mobile WiMax Networks" **,** IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013,p.213-220.
[7]. Ajay Kumar Dubey,Chandra Kant Shukla, Chaos based Encryption and Decryption of Image and Video in Time and Frequency Domain,IJCA Special Issue on "Network Security and Cryptography" NSC, 2011
[8]. Fuwen Liu and Hartmut Koenig,Puzzle-A Novel Video Encryption Algorithm J. Dittmann, S. Katzenbeisser, and A. Uhl (Eds.): CMS 2005, LNCS 3677, pp. 88 – 97, 2005.
[9]. Narendra K. Pareek , Vinod Patidar , Krishan K. Sud , "Diffusion–substitution based gray image encryption scheme" Digital Signal Processing 23 (2013),Elsevier,p.894-901
[10]. Anchal Jain , Professor Navin Rajpal , A Two Layer Chaotic Network Based Image Encryption Technique,IEEE 2012 National Conference on Computing and Communication Systems.
[11]. Gaurav Bhatnagar, Q.M. JonathanWu, and Balasubramanian Raman ,A Novel Image Encrytpion Framework Based on Markov Map and Singular Value Decompostion, Springer-Verlag Berlin Heidelberg 2011,M. Kamel and A. Campilho (Eds.): ICIAR 2011, Part II, LNCS 6754, pp. 286–296
[12]. Gaurav Bhatnagar , Q.M. Jonathan Wu. Shell,Selective image encryption based on pixels of interest and singular value decomposition, Digital Signal Processing 22 (2012) ,Elsevier,648–663
[13]. Daniel Socek, Spyros Magliveras, Dubravko ´ Culibrk, OgeMarques,Hari Kalva,and Borko Furht ,Digital Video Encryption Algorithms Based on Correlation-Preserving Permutations ,Hindawi Publishing Corporation ,EURASIP Journal on Information Security,Volume 2007, Article ID 52965, 15 pages
[14]. L. Kocarev, and S. Lian, Chaos-Based Cryptography, Verlag Berlin Heidelberg: Springer, 2011.
[15]. Oge Marques ,Practical Image and Video Processing UsingMATLAB,IEEE,Wiley 2011.