# Technique of Video encryption/scrambling using chaotic functions and analysis

[1]Jyoti S. Bowade, [2]Pawan khade, [3]Dr. M. M. Raghuwansh
[1]Student, [2]Professor, [3]Professor
[1]Department of computer science
[1]Rajive Gandhi college of engineering & research Nagpur, India

***Abstract*—Multimedia data security is very important for multimedia commerce on the Internet and real-time video multicast. However, traditional encryption algorithms for data secrecy such as DES may not be suitable for multimedia applications because they are unable to meet the real-time constraints required by the multimedia applications. In this paper a new video encryption algorithm presented where the encryption of video is done by shuffling and encryption of frames using 4D and 3D arnolds cat map and generate pseudorandom numbers by using chebyshev map. As both Arnold and chebyshev shows chaotic behavior and puedorandom number has an important role in cryptography it has been used for the generation of pseudo random numbers and it has been used as keys for encryption.**

***Index Terms*— Chaos; chebyshev map; arnolds cat map; video; shuffling; random numbers.**

---

## I. INTRODUCTION

In today's era of information we need to secure the multimedia data because large amount of traffic in network is either images or video. This project uses the multidimensional chaotic maps for encryption of the Videos[5].Chaotic functions are blessed with important characteristics which makes it excellent for practical use against any statistical attack that is they are very sensitive to initial condition or system parameter and it shows Pseudo-random behaviour which makes them desirable for encryption. Multidimensional chaotic functions will contain more than one parameters using which the video frames will be encrypted. To maintain a balance between security and computational time, we shuffles the video frames along with scrambling of frames[14]. The Large numbers of chaotic algorithms are being proposed for the image encryption now days. Many authors have proposed the image encryption algorithms based on low dimension chaotic functions. Security provided by these function is limited since these functions provide the limited key space and possesses some weakness[8] . 3 dimension functions are far more secure from cryptanalytic attacks and so as 4D functions. Here we are using the 3D Arnolds cat map for encryption of frames of the video and generating a 4D map which will be used for the encryption of video.

Cryptography uses two concepts, one is Encryption and the other is Decryption. In the process of video encryption and decryption the following basic steps are involved. First is key generation algorithm, second is Encryption algorithm and third is Decryption algorithm. So the key generation algorithm plays an important role in the process of encryption system. The generated random number is chaos based and unpredictable, hence one can use it as a key. Hence random numbers are generated using chaotic map for video Encryption system [4].the pseudo random number generators as the sequence of random numbers generated by the process depends upon a small initial value. There are several applications in different areas like the weather forecasting and cryptography where the pseudo random numbers are used. So in this paper the pseudorandom numbers generated by using chaotic maps is shown.

The security of video data is needed for many applications such as computer forensics, distant education and training, it needs encryption for no alteration of information. So this is the motivation to implement secure video encryption system [5].

## II. PRELIMINARY

In this section we first introduce the definition and properties of arnolds cat map and chebyshev map.

### *Arnolds cat map (ACM):*

The arnolds cat map is discrete system that stretches and folds its trajectories in phase space. Its important properties are it is invertible because the matrix has determinant 1; it is area preserving and its periodicity property.

Many authors have implemented image encryption using 2D arnolds cat map [4] and 3D arnolds cat map. Here the 3D arnolds cat map is used for video frame encryption and 4D for shuffling of frames.

3D arnolds cat map: In order to increase the security of the Arnold's cat map, many authors have proposed the 3 dimensional Arnold's cat map. 3D ACM which is improved by introducing four control parameters a, b, c & d as follows.

$$\begin{pmatrix} X` \\ Y` \\ Z` \end{pmatrix} = \begin{pmatrix} 1 & p & 0 \\ q & pq+1 & 0 \\ c & d & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \quad \text{mod } N \text{ [1].}$$

It can be written in equation form as follows:

$$X' = ( X + pY ) \bmod n$$
$$Y' = ( qX + (pq + 1) Y) \bmod n$$
$$Z' = (cX + dY + Z) \bmod m$$

where x', y' are the transformed location of pixel of frame, x,y is the original location of frame, z is the bit value of pixel before mapping and z' is bit value of image after mapping [5]. N is the size of frame and M is the maximum value of the intensity/color code of pixel that is M=256[1].

This representation is equivalent to→

$$\begin{pmatrix} X` \\ Y` \\ Z` \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \quad \text{Mod N , where p=1, q=1, c=1, d=1.}$$

ACM perform the dual encryption, firstly it performs the shuffling using regular ACM and secondly it will perform the substitution of grey/ colour values according to the positions and original grey/colour values of pixels using z component[1]. 3D ACM is implemented; following is result for colour image.

The 3D ACM is more secure than that of 2D ACM because of two factors. First, presence of additional constants c and d that can take any random values and secondly 2D ACM can only shuffle the pixel location but 3D ACM can perform the additional substitution and make distribution of colour/gray value uniform [3].

***4D arnold cat map*:** When taking all the values 1, following is the matrix.

$$\begin{pmatrix} X' \\ Y' \\ Z' \\ V' \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} X1(K) \\ X2(k) \\ X3(K) \\ X4(K) \end{pmatrix} \quad \text{mod n}$$

$$X` = (X+Y+Z+V) \bmod n$$
$$Y` = (X+2Y+Z+V) \bmod n$$
$$Z` = (X+Y+2Z+V) \bmod n$$
$$V` = (X+Y+Z+2V) \bmod n$$

Here this fourth equation is used for video frame shuffling. By modifying this last equation we can write it as $V` = (X + 2V) \bmod n$ because X+Y+Z will be any constant value.

B. *chebyshev map:*

Chebyshev map[6] is a chaotic map and these maps are the form of chebyshev polynomials. The chebyshev polynomials associated with the de moivre's formula are the a sequence of orthogonal polynomials. To introduce chebyshev map following trigonometric functions are given.

$$\cos 0\theta = 1$$
$$\cos 1\theta = \cos\theta$$
$$\cos 2\theta = 2\cos^2\theta - 1$$
$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$
$$\cos 4\theta = 8\cos^4\theta - 8\cos^2\theta + 1$$
$$\cos 5\theta = 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta$$

From the above the chebyshev polynomial can be defined as follows:
$T_n(x) = 2xT_n(x) - T_n(x)$, where n is an integer and $-1 \le x \le 1$, If we consider $x = \cos\theta$ then $T_n(\cos\theta) = \cos n\theta$ and we get the following equations:

$$T_1(x) = x$$
$$T_2(x) = 2x^2 - 1$$
$$T_3(x) = 4x^3 - 3x$$
$$T_4(x) = 8x^4 - 8x^2 + 1$$
$$T_5(x) = 16x^5 - 20x^3 + 5x.$$

The proposed algorithm uses $T_2(x)$, $T_3(x)$, $T_4(x)$ and $T_5(x)$ to generate keys.

## III. PROPOSED METHODOLOGY

Videos in simple terms are a collection of frames. Video is made up of frames and each frame is like a still image. Here in this paper we will see how each frame will be encrypted by using the Arnolds 3D cat map with the help of frame shuffling[13] concept to provide more security to the video.

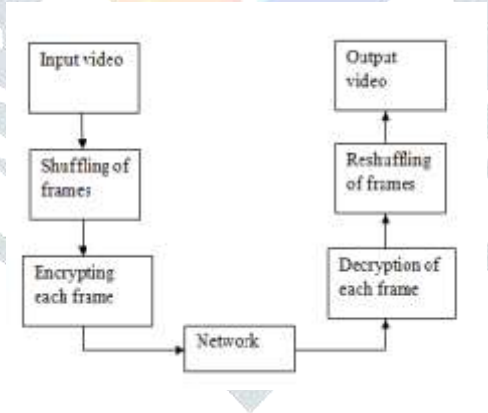


Fig. 1. Proposed system architecture

First take a video for the process of encryption. Then the shufflingof frames of the video is done by using the fourth equation we got from the 4D Arnolds cat map. The equation is v'=(x+2v) mod n where v is the original location of frame, v' is the shuffled location of frame, x is any constant number and n is the total number of frames of the video. this equation is used when the total no of frames i.e. n is odd number, if n is even then we are using v'=(x+3v) mod n.

After the shuffling is done, the encryption of individual frames will be done by using the 3D Arnold's Cat map which behaves chaotically, whose equations are given below:

$$X' = ( X + pY ) \bmod n$$
$$Y' = ( qX + (pq + 1) Y) \bmod n$$
$$Z' = (cX + dY + Z) \bmod m$$

Before applying these equations to the frames we have to generate the key values i.e. p, q, c and d. these keys are generate by using chebyshev map $T_2(x)$, $T_3(x)$, $T_4(x)$ and $T_5(x)$ respectively [6].

***Key generation:***

1. Select a random number x between (-1,1).
2. Select a random frame of the video.
   -add the diagonal pixels value of that frame and convert it in such a way that after adding it to x we will get the value between -1 and 1 and consider it as dr.
3. Add dr and x: x=x+dr.
4. Give input x to the equations T2(x), T3(x), T4(x), T5(x) and iterate them for n times.
5. After above four process we will get the four keys T2(x)=A, T3(x)=B, T4(x)=C, T5(x)=D.

But here we need the integer values and we got A, B, C and D in decimal form, then its converted into there digit or four digit form as per requirement and then used.

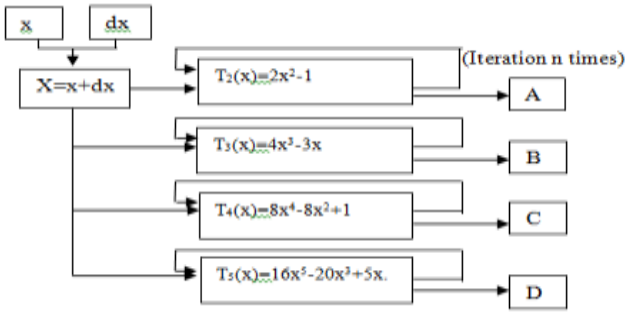


Fig. 2. Generated keys

Then by using these four keys we have encrypt all the frames and at last we got the encrypted video.

Decryption is known as reverse of encryption. Now the process of decryption is done by using the inverse Arnolds cat map which used to decrypt the frames and for reshuffling the reverse of the shuffling equation is used i.e.v=((v'-x) mod n)/ 2. After applying this equation on the video we will get the original video.

***Public Key Encryption***: The encryption process creates multiple text files which contain the key and other security parameters like number of iterations and so on, and their secure communication with the other party is necessary. This can be provided by using the public key encryption[12] of the generated text files. This public key encryption[6] using the Chebyshev map using El Gammel public key encryption for floating point numbers can be used for the encryption of video. The Chebyshev map possesses the semi group property which lead to TsTr= TrTs. Here A Chebyshev polynomial map $T_n : R \rightarrow R$ of degree n is defined using the following recurrent relation: $Tp+1(x) = 2xT_n(x) - Tp-1(x)$[11]. This can be implemented using iterative method.

## III. ALGORITHM FOR ENCRYPTION & DECRYPTION

The proposed Algorithm used for the process of encryption and decryption using both Arnold's CAT map and the chebyshev map is given below,

**A.** ***Encryption algorithm****:*

1. The original video is chosen for the process of encryption.
2. The shuffling of frames is bone by using the forth equation of 4D Arnolds cat map
3. Generation of key values or pseudo random numbers using chebyshev map with the help of video data.
4. Encrypt all the frames using 3D Arnolds cat map with the help of key values.
5. Encrypted video is ready and encryption process over.

**B.** ***Decryption algorithm****:*

1. The encrypted video which got from the process of encryption is chosen for the process of decryption.
2. Reshuffle the frames of video by using the reverse equation.
3. Generation of key values or pseudo random numbers using chebyshev map with the help of video data.
4. Decrypt all the frames by using inverse 3D Arnolds cat map with the help of keys.

5. Original video is obtained from the encrypted video and decryption process is over.

**C.** ***key exchange algorithm****:*

**Alice, in order to generate the keys, does the following:**

1. Generates a large integer s.
2. Selects a random number $x \in [-1,1]$ and computes Ts(x).
3. Alice sets her public key to (x,Ts(x)) and her private key to s.

**Encryption Algorithm: Encryption requires five steps:**

Bob, in order to encrypt a message , does the following:

1. Obtain Alice's authentic public key (x,Ts(x)).
2. Represents the message as a number $M \in [-1,1]$.
3. Generates a large integer r.
4. Computes Tr(x),Tr·s(x) = Tr(Ts(x)) and X = M·Tr·s(x).
5. Sends the ciphertext C = (Tr(x),X) to Alice.

**Decryption Algorithm: Decryption requires two steps:**

Alice, to recover the plaintext M from the ciphertext C, does the following:

1. Uses her private key s to compute Ts·r = Ts(Tr(x)).
2. Recovers M by computing M = X/Ts·r(x)

## V. EXPERIMENTAL ANALYSIS


Fig. 3. The video is selected for encryption.

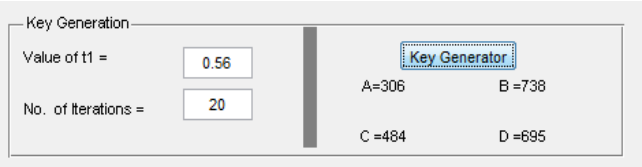


Fig. 4. Keys generated for video encryption.

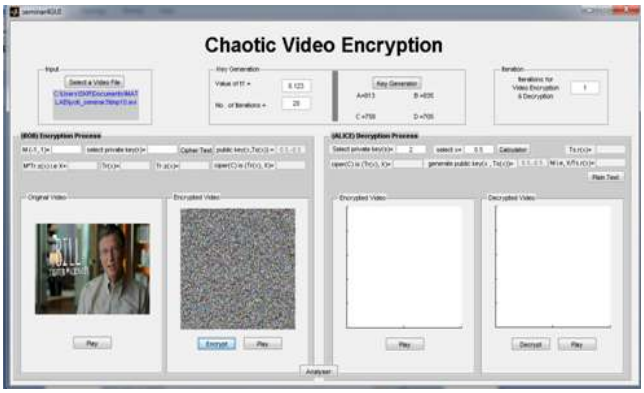


Fig. 5. Encryption of video is done by using keys.


Fig. 6. Key exchange process is shown here.

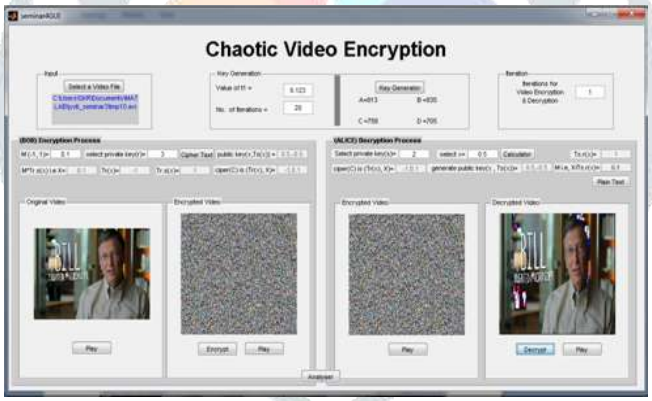


Fig.7. decryption of video is done after getting keys from other side.

From the above result analysis it gets clear that, shuffling and encryption of the video is done by using chaotic functions. But here in the last fig.7 the decrypted video has lost some of its data which could be corrected.

Some analysis is done which shown below like is histogram, entropy value and the correlation value.

Entropy value: original image= 7.77138, Encrypted image= 7.90009

Correlation values: original image= 0.923, Encrypted image= 0.918


Fig.8.select frame of video and its encrypted frame.

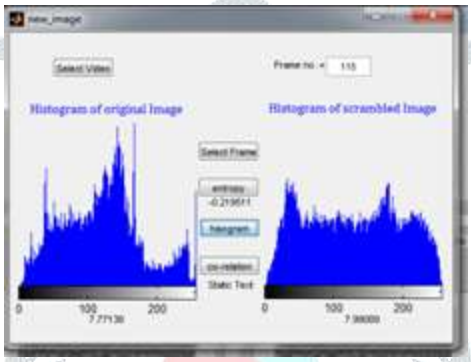


Fig.9. histogram of both the images and entropy values.

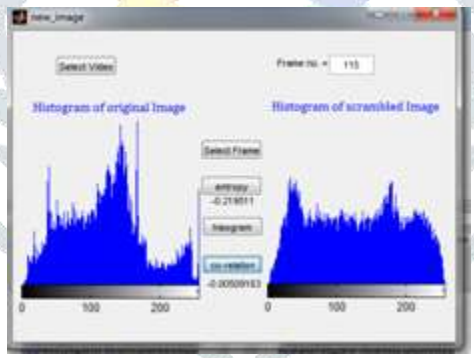


Fig.10. correlation value difference between two images.

Table.1. Analysis of encryption process.

| process | parameter | Arnold 2D | Arnold 3D |
|---|---|---|---|
| **encryption** | Time required (sec) | 25.957762 | 41.364911 |
| | Memory required | 2×2 bytes | 4×3 bytes |
| | Disk space | 4.32MB | 4.32MB |
| **decryption** | Time required (sec) | 38.357324 | 69.232926 |
| | Memory required | 2×2 bytes | 4×3 bytes |
| | Disk space | 4.32MB | 4.32MB |

## VI. CONCLUSION

This paper describes the video encryption technique using the chaotic functions. Arnolds Cat Map and chebyshev map ae the chaotic functions used for video encryption. In this algorithm the pseudo random numbers are generated by using chebyshev map and encryption of frames by using 3D arnolds cat map. Then again a shuffling technique is introduced here to make encryption of video more secure against the chosen attacks. The shuffling is done by using 4D arnolds cat. This encryption of video makes it more secure and robust also difficult for any intruder to crack the original video.

## V. REFERENCES


[1] A. Sethi Arumugal, D. Kiruba Jothi. "Image Encryption Algorithm Based on Improved 3D Chaotic cat map", 2010 IEEE International ConferenceOn computational intelligence and computing research(ICCIC).

[2] Bergamo, P.; D'Arco, P.; De Santis, A.; Kocarev, L.; "Security of public-key cryptosystems based on chebyshev polynomials", IEEE Transactions on Circuits and Systems I:Regular Papers 2005.

[3] Shahui Chen, Zengqiang Chen, Zhazhi Yuan" A Compound Video Encryption Algorithm Based on Hyperchaos"2008 IEEE

[4] Agyan Kumar Prusty, Ashutosh Pattnaik, Swastika Mishra"An image Encryption and Decryption approach based on pixel shuffling using Arnolds cat map and Henon map"2013 IEEE (ICACCS)

[5] Pooja Deshmukh, Vaishali Kolhe"Modified AES Algorithm For MPEG Video Encryption" ICOCES 2014 IEEE

[6] Ya-Fen chang, Wei-Liang Tai, Wei-Nawu, Wei-Han Li and Yung-Chi Chan"comments of on chaotic maps –based password-authenticated key agreement using smart cards " 2014 IEEE international conference on intelligent information hiding and multimedia signal processing.

[7] Gan Yu, Yongjun Shen, Guidong Zhang, Yanhua Yang"A Chaos-based Color Image Encryption Algorithm" Sixth International Symposium on Computational Intelligence and Design ,2013

[8] Kunal Kumar Kabi, Chittaranjan Pradhan, Bidyut Jyoti Sana, Ajay Kumar Bisoi"Comparative Study of Image Encryption Using 2D Chaotic map"2014 IEEE

[9] Bose, R. and Banerjee, "implementating symmetric cryptography using chaos functions" advanced computing & communication conference, 1999

[10] Min Long; Li Tan; "A Chaos-Based Data Encryption Algorithm for Image/Video ", Second International Conference on Multimedia and Information Technology (MMIT), 2010.

[11] Ljupco Kocarav , Shingao Lian; "Chaos-based Cryptography theory algorithms and applications" , Studies in Computational Intelligence,Volume 354,2011.

[12] Ganesan, K.; Singh, I.; Narain, M.; "Public Key Encryption of Images and Videos in Real Time Using Chebyshev Maps ",Fifth International Conference on Computer Graphics, Imaging and Visualisation, 2008. CGIV '08.

[13] Ajay kulkarni, Saurabh Kulkarni, Ketaki Haridas, Ankit More"Proposed Video Encryption Algorithm v/s Other Existing Algorithm: A Comparative Study"International Journal of Computer Applications , March 2013