Implementation of Videocryptography based on Sine and Cosine Chaotic Map

Nisarga J
M. Tech (VLSI Design and Embedded system)
Student
ECE Dept, BNMIT
Bangalore, India

Smt. Anuradha V Rao
Assistant Professor
ECE Dept, BNMIT
Bangalore, India

***Abstract*— Since advancement in technology, the chaos based cryptography algorithms of new and efficient have been existed to develop secure image and video encryption techniques. Digital video and image cryptography is based on non linear trigonometric functions sine and cosine chaotic map. The sine and cosine chaotic map is generated for high-intense of chaos over most regions of image to increase confidentiality of information. Confusion and Diffusion is performed through pixel shuffling and bit-plane separations before to XOR operations in order to attain a fast encryption process. Key of alphanumeric words which gives security is to be converted from ASCII code to floating number and it is used as initial conditions. Experiments will be performed in MATLAB using standard color video**

***Keywords*— Chaotic map, sine, cosine**

I. Introduction

Day by day, transfer of images and videos through internet been increased as technology advances. Encryption is one of the way to hide the data from unauthorisers. Till now plenty of encryption algorithms had been proposed and there are some conventional techniques also available to provide secured transmission. But still come across the leakage or hacking of video or image content due to swift growth of hackers. This paper says about video cryptography based on sine and cosine chaotic method which provides more secured encryption compared to other techniques. Since expanding of complexity in the encryption techniques, good encrypted videos or images can be obtained. Here sine and cosine functions will add the complexity to the encryption technique. The aim of the proposed technique is to make encryption more robust by adding still more complexity and hackers would be received failure as a result to their Ad-hoc tricks. Hope this proposed technique will reduce video leakage to certain extent and make the users happy.

Cryptography is a synonym of encryption. It is a process of transmuting the original information into a form, that can be comprehend one who has secret key to unlock it.

In image and video cryptography, there are two types conventional and chaotic. Conventional cryptography such as AES[2], DES, IDEA, RSA involves just shuffling of pixels so it leads to reduced security. Another technique is information splitting method has Shamir sharing[1] technique. Chaotic cryptography involves changing of pixels so that it gives elevated security. In chaotic there are 2 juncture are confusion and diffusion. The plenty of encryptions methods have been developing since decades. With the use of chaotic maps (is a map that gives chaos behavior which aids to cryptography) in encryption techniques increases complexity. As complexity increases, information security increases. Thus chaos based encryption plays an important role in protecting the privacy of the information i.e data confidentiality than conventional.

Chaotic map is a map that produces chaos behavior which helps in encryption techniques. There are so many types of chaotic maps they are logistic map[4], chybshev map.

Basically video encryption algorithms are of four types:-

Completely layered encryption:- in this type, first entire video is compressed later encrypted using any conventional encryption techniques as though AES,DES, RSA etc..

Encryption using permutation:- video encrypted using some permutation algorithm, here more focus on confusion stage compare to diffusion stage

Selective encryption:- only few selected bytes of video will be encrypted, not entire video as type first

Perceptual encryption:- video will be encrypted just by adding noise, video still be visible after encryption. Quality of the video will be decreased.

II. LITRATURE SURVEY

Classic encryption algorithms like AES[1], DES,RSA etc… are not feasible for video data because of its large size and high computational requirements. As a contradict measure, earlier encryption algorithms used simple scrambling mechanisms for huge video data. Evidently they are insecure.

In this paper, we can see selective encryption technique which is fast enough for real time but it is less secured. Proposed algorithm is predicated on sharing DC coefficients among AC and DC coefficients. Here first they applied DCT over image then made use of Shamir sharing technique for encryption. Shamir sharing is the process of splitting the information among the given number of participants. But it has the disadvantages that video length has been increased and this algorithm supports only MPEG-1 and MPEG-2.

As referred [2] First entire video is compressed using encoder H.264 then compressed I-frames is partially encrypted by AES block cipher. Decryption is the reverse process of encryption that is first decrypt the encrypted I-frame and the decode by H.264.

The use of H.264 will let to have disadvantage that it requires high bit rate and become unrealistic for video content delivery and the use of AES gives weak security just by shuffling data and only sensitive to designated keys rather than sequence of designated keys.[3] Here image will be compressed by Haar wavelet which is one of the transformation and it is a bipolar step function. Haar wavelet function is antisymmetric with respect to time t=1/2. It is discontinuous in time. Transformed image is divided into blocks and each blocks shuffle among themselves. Secret key is obtained by logistic map method and it will be send by watermarking technique. Reverse operations will be performed to get decrypted image(decryption). Use of watermarking technique leaks security as if it is easy to remove by cropping watermarked region with the aid of image editing software and it is time consuming for large volume of images.

As mentioned in [4], secret key is alphanumeric, later it is converted into real number using some sort equations. Read the three consecutive bytes from the image file. These three bytes indicate the value of the red, green and blue (RGB) color respectively and together form a single pixel of the image. Divide the range [0.1,0.9] into 24 non-overlapping intervals and arrange them into eight different groups. Then assign different type of operation corresponding to each of these groups. This technique gives much more complexity than other methods but it is very much time consuming for large volume images and it takes more memory to store images since any of image compression methods have not applied.

III. PROPOSED ALGORITHM

Usually compression of video will be performed to make it to use less memory, later encryption algorithms will be applied. Compression is performed using different techniques or transformations such as wavelet[3],DCT[1] etc.., using compression formats such as H.265,H.264[2]. Proposed system consists of three important phases are:
First, bit plane slicing(confusion and diffusion process) of each frame of video which causes compression of video. Second, creation of chaotic maps using secret words. Third, carry out XOR operation between binary frames of video and chaotic maps. This paper incorporates both sine and cosine function to enhance the complexity of technique and security level of the information. Propounded technique has the following steps as shown in fig [1] and fig[2].

1) Take a video and extract frames
2) Take each frame and obtain RGB planes
3) Carry out bit plane slicing on all RGB planes to get binary images.
4) Take secret words and follow the sequence of latters (control parameter) as below, each letter represent its ASCII value

Table.1

X1 : A1A4A7A10A13A16A17	Y1 : A1 A3 A5 A7 A9 A11A18
X2 : A2A5A8A11A14A1A18	Y2 : A2 A4 A6 A5 A10 A12A17
X3 : A3A6A9A12A15A8A17	Y3 : A3 A5 A7 A9 A11 A13A18
X4 : A4A7A10A13A16A3A18	Y4 : A4 A6 A5 A10 A12 A14A17
X5 : A5A8A11A14A1A4A17	Y5 : A5A7A9A11A13A15A18
X6 : A6A9A12A15A2A5A18	Y6 : A6A8A10A12A14 A16A17
X7 : A7A10A13A16A3A6A17	Y7 : A7A9A11A13A15A1A18
X8 : A8A11A14A1A4A7A18	Y8 : A8A10A12A14A16A2A17

5) Each ASCII number represented in binary from and substitute in given formulae

$R_{Xm}=B_{X1}*2^0+B_{X1}*2^1+\ldots\ldots\ldots+B_{X48}*2^{55})/2^{56}$

$R_{Ym}=B_{Y1}*2^0+B_{Y1}*2^1+\ldots\ldots\ldots+B_{Y48}*2^{55})/2^{56}$

Where, m ranges from 1 to 8.

6) Calculate constants a and b using below formulae

$a_m=(R_{Xm}*R_{Ym})\bmod 1$

$b_m=(R_{Ym}*R_{Ym+1})\bmod 1$

7) Use the constants a and b to generate chaotic matrices where n is the number of pixels in each frame.
$x_{n+1}=\cos(a_m x_n)+\sin(b_m x_n)$ here cos and sine terms give more chaos behavior to the encryption as they are non linear function
8) Perform XOR operation between generated matrices and each binary frame to get new set of binary images called encrypted ones.
9) Carry out reveres of bit plane slicing to get RGB planes of each frame.
10) Concate each encrypted frames to get encrypted video.
Perform reverse operation of encryption (decryption) to get decrypted video.
Thus use of sine and cos terms, use of secret words as constants and sequence of secret words play an important role in encryption.

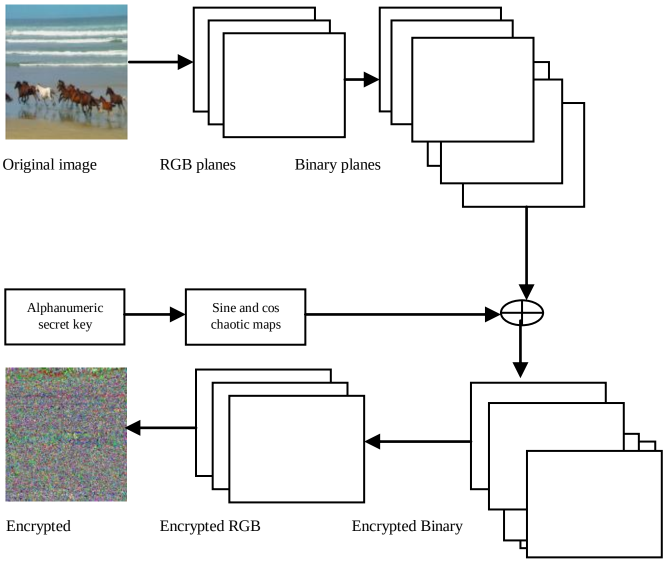


Fig-1 Encryption block diagram for single frame

Sequence of steps involved in encryption is shown in below using flowchart

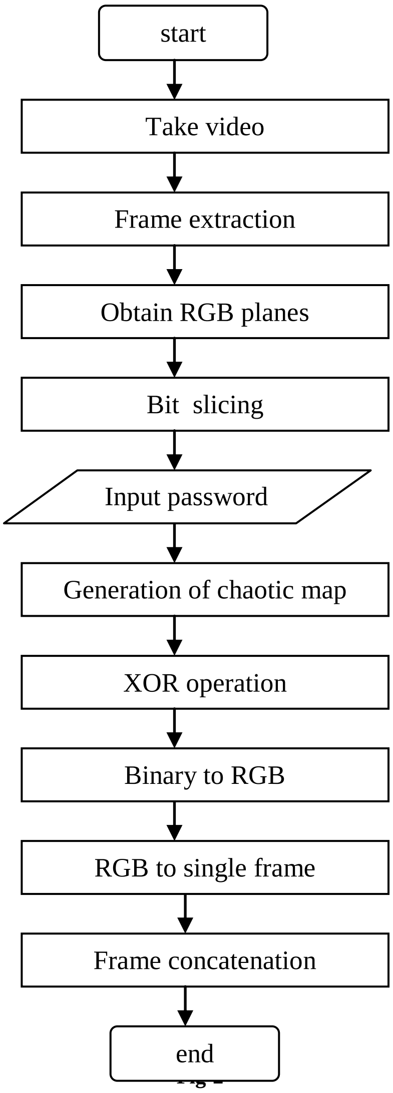


Fig-2

IV. RESULT AND ANALYSIS

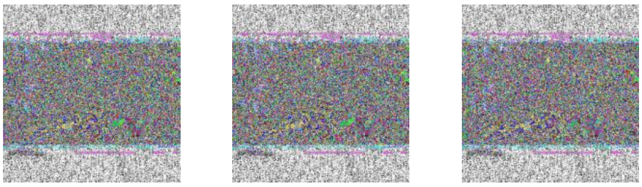
A. Result

Expected encryption and decryption result as shown in fig[3] below for few frames(original frames) of video.

Original frames

Frame No.1 2 9

Encrypted frames



1 2 9

Decrypted frames

1 2 9

Fig-3

B. Analysis(NPCR and UACI)

NPCR (Net Pixels Change Rate) is measures the different pixel values between encrypted and original image

For the encrypted images in which the corresponding original images have only one pixel difference are denoted by c1 and c2. Label the grey scale values of the pixels at pixel (i,j) in c1 and c2 by c1(i,j) and c2(i,j) respectively. Define a bipolar array d with the same size as images c1 and c2. D(i,j) is determined by c1(i,j) and c2(i,j). if c1(i,j)=c2(i,j) then d(i,j)=1 otherwise d(i,j)=0.

The NPCR is defined as

$$NPCR = \sum_{i,j} (d(i,j)/T)*100\%$$

$$UACI= \sum_{i,j}(|d(i,j)|/FT)*100\%$$

where, F denotes the largest pixel value compatible with the cipher image format.

The UACI concentrated on the averaged difference between original images and encrypted image.

The range of NPCR is [0,1]. When N(c1,c2)=0, it implies that all pixels in c2 remain the same values as in c1 . When N(c1,c2)=1 , it implies that all pixel values in c2 are changed compared to those in c1 . In other words, it is very difficult to establish relationships between this pair of ciphertext image c1 and c2. However,N(c1,c2)=1 rarely happens, because even two independently generated true random images fail to achieve this NPCR maximum with a high possibility, especially when the image size is fairly large compared to F . The range of UACI is clearly [0,1] as well. The UACI measures the average intensity of differences between two images.

Table.2

Frame No.	NPCR	UACI
1	0.99189	0.4426469
2	0.99167	0.44264277
3	0.99176	0.44267352
4	0.99176	0.44292608
5	0.99189	0.44222098
6	0.99204	0.44301221
7	0.99215	0.44261189
8	0.99191	0.44221674
9	0.99280	0.49185549
10	0.99252	0.49119015

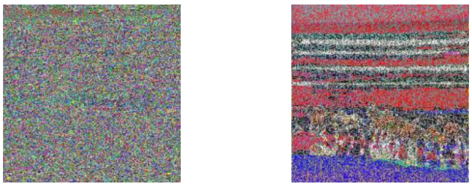
NPCR and UACI values for 10 frames of video

The average of NPCR value is 99.2039% and UACI average value is 45.2399% which indicates this algorithm has high resistance against attacks and performed best encryption of video so that we will get high secured video

C. Secret key analysis

If we give wrong key in decryption then we won't get decrypted video. Illustrated below in fig[4].

Key given during encryption is 'hello world 201525'. If we give 'hello great 201515' during decryption then we won't get decrypted video.

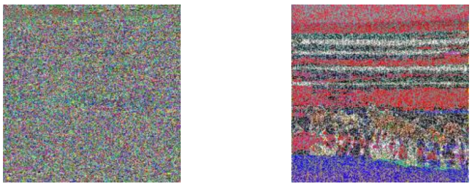


Encrypted Decrypted (wrong)

Fig-4

If we give correct key but arrange of words have been wrong then also we won't get decrypted video, Illustrated below.

Key given during encryption is 'Hello World 201525'. If we give 'world hello 201515' during decryption then it does not give decrypted video as shown in fig[5]



Encrypted Decrypted(wrong)

Fig-5

D. Video length analysis

Video length will be same as original after encryption process since size of all frames are same before and after the encrption, and same will be observed during decryption so the video length in entire encryption and decryption process will be same as original length. So that here there is no loss of information and decryption does not take more time compare to encryption as referred in[1].

Table.3

Frame No.	Original video frames size	Encrypted video frames size	Decrypted video frames size
1	192kb	192kb	192kb
2	192kb	192kb	192kb
3	192kb	192kb	192kb
4	192kb	192kb	192kb
5	192kb	192kb	192kb
6	192kb	192kb	192kb
7	192kb	192kb	192kb
8	192kb	192kb	192kb
9	192kb	192kb	192kb
10	192kb	192kb	192kb

Comparision between proposed algorithm and reference[1]

Table-4

Test Videos	No. of frames	Encrypted frames	%increase in video length
Car and man	775	775	0
Horse	760	760	0

Table-5

Test Videos	No. of frames	Encrypted frames	% increase in video length
Athletic	184	396	46.46
Penguin	801	2468	32.45

Table[4][5] shows that there is no increase in video length in proposed technique compare to reference[1]

ACKNOWLEDGMENT

The kind support from college, guide and friends is gratefully acknowledged.

REFERENCES

(1) Narsimha Raju C, UmaDevi Ganugula, Kannan Srinathan, C. V. Jawahar, "*A Novel Video Encryption Technique Based on Secret Sharing*" International Institute of Information Technology-Hyderabad,India, Hyderabad.

(2) 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, Vol. 2, No. 2 April, 2010.

(3) Nidhi Sethi and Deepika Sharma, " *A New Cryptology Approach for Image Encryption*", 2nd IEEE International Conference,2012.

(4) N.K. Pareek a,b, Vinod Patidar a, K.K. Sud, "*Image encryption using chaotic logistic map*", Image and Vision Computing 24 (2006) 926–934.

(5) Oge Marques, *Practical Image and Video Processing using MATLAB*, Florida Atlantic University,A Jhon Wiley and Sons,Inc Publication,2011.

(6) Rudra Pratap, *Getting Started with MATLAB*, Oxford University, Newyork,2010.

(7) S Jayaraman, S Esakkirajan, T Veerakumar, *Digital Image Processing*, Eleventh Edition, 2013.