RESEARCH ARTICLE OPEN ACCESS

A novel chaotic system for Video Cryptography using 2D logistics Sine-Cosine maps

Manjunatha V G, Meharunnissa S P
Dept. of Electronics and Instrumentation, Dayanandasagar College of Engineering
Dept. of Electronics and Instrumentation, Dayanandasagar College of Engineering

Abstract
The astonishing developments have been occurring in the field of network communications for a long time and these advancement lead to a genuine and conspicuous need of image transfer and getting safely through the web. The web is not secure for the exchange of dependable data, for example, content, picture and video. Cryptographic procedures are vital to be improved to exchange data through web safely. Routine cryptography, for example, AES, DES, IDEA and RSA includes simply rearranging of pixels and henceforth will prompt decreased security for information protection. With a specific end goal to enhance the security, it is important to expand the intricacy in encryption. As an answer for this it is proposed to utilize confused maps in encryption methods which expand the multifaceted nature. As intricacy builds, data security increments. Thus, chaos-based encryption has its own significance in providing security for secret information i.e. data confidentiality than conventional.

Index Terms: Cryptography, Image Encryption, Image communication and Video Processing.

I. INTRODUCTION

In day by day life, exchange of pictures and recordings through the web has been expanding as innovation advances. Encryption is one of the approaches to conceal the information from unapproved clients. Till now a lot of encryption calculations had been proposed and there are some traditional methods additionally accessible to give secure transmission. Yet at the same time there is the spillage or hacking of video or picture content because of quick development of hacking methods by programmers. Cryptography is the procedure of transmitting the first data into a structure which can be comprehended by the person who has the mystery key. This paper is about video cryptography taking into account sine and cosine disordered system which gives more secured encryption contrasted with different strategies. Since growing of multifaceted nature in the encryption strategies, all around scrambled recordings or pictures can be got. Many-sided quality of the encryption method will be included by sine and cosine terms. The point of the proposed strategy is to make encryption more powerful by including still more complexity.

Advance enhancements in communication domain for a secured conveyance of data, for example, text,image and video in such a large number of areas, in communication systems, medical science, and so forth. The web does not give intense assurance to information exchange. So encrypting the multimedia is important to accomplish strong classification. Non-linear attributes of the ongoing frameworks are being examined and confused framework is likewise one of the nonlinear frameworks. Numerous turmoil based encryption calculations have been exhibited and talked about in the most recent couple of decades. Utilization of Bakers guide in the encryption has the weakness that it for the most part hand-off on the dissemination stage, if the dispersion stage is split, then effortlessly make out the disarray stage and it is not relying upon trigonometric capacity. When all is said in done, confused maps, to be specific tent, ikeda, standard make utilization of one and only trigonometric capacity, however here attempted with two trigonometric terms in a solitary disorganized guide. We built up a chaos based encryption procedure for a video utilizing secret key

II. LITERATURE SURVEY

Traditional encryption algorithms like AES [1], DES and RSA, etc… are not feasible for video data because of its high computational needs and large size. As a counter measure, old cryptography algorithms make use of simple bit rotation and shifting method abundant video information. Gradually old encryption techniques become insecure.

In paper [1], selective encryption technique can be seen which is fast enough for real time but it is less secure. The proposed algorithm is predicated on sharing DC coefficients among AC and DC coefficients. Here first DCT has been applied over image to compress it and then made use of Shamir sharing technique for encrypting. 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 in paper [2], first entire video is compressed using encoder H.264 to compress the video and then compressed I-frames are partially encrypted by AES block cipher which is a conventional cryptography method. Decryption is the reverse process of encryption that is first decrypted the encrypted I-frame and decode by H.264.The use of H.264 has the disadvantage that it requires high bit rates 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 a sequence of designated keys.

As mentioned in paper [3], the image has been compressed by Haar wavelet which is one of the transformations and it is a bipolar step function. Haar wavelet function is anti-symmetric in time is equal to half. It is discontinuous in time. Transformed image is divided into blocks and each block shuffle among themselves. The secret key is obtained by the logistic map method and it will be sent 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 paper [4], the secret key is alphanumeric, later it is converted into real number using some sort of equations. Three bytes from the image file has been taken by an algorithm. These three bytes indicate the value of the red, green and blue (RGB) color respectively, and combination of these three pixels from 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 in which each group consists of three values. Different type of operation has been assigned according to each of these groups to encrypt the image. This technique gives much more complex than other methods, but it is very much time consuming for large volume images and it takes more memory to store images for any of image compression methods have not applied.

III. SYSTEM DESIGN

This chapter says about chaos theory, cryptography, benefits of digital video and its process, chaotic map and steps carried out to design the system.

A. Chaotic Maps

The chaotic map is a map that produces chaos (confusion) behavior which helps in encryption techniques. In the chaotic map, individual description in trajectories makes ensemble description results in different formulation. Chaotic maps are discreet and continuous in nature so it can be used in analog system as well as in a digital system. Chaotic maps have the concept of chaos theory to have its chaotic behavior in it. Chaos theory is related to the deterministic and non-deterministic system whose behavior can be predictably or foreseen and unpredictable respectively. The behavior of chaotic systems can be predictable for sometime later it will be developed as random. The time taken to determine the behavior of a chaotic system depends on three things they are: uncertainty, accuracy, time scale. For instance, in the forecast, how much uncertainty can be tolerated, how accurately its current state can be measured, the dynamics of the system measured by time scale, called the Lyapunov time.

Property of chaotic systems is sensitivity to initial condition says that each point has unsurely very close approximation by next successive points with different future trajectories. Thus, unique behavior might be seen if there are small changes in current trajectory. Initially a system with some of its information, as time passes the system will not be predictable anymore, gives the concept of sensitivity to an initial condition. The sensitivity to initial conditions is measured by Lyapunov exponent. At the beginning, two trajectories are given in the phase space that are located very close to each other with initial distance δY0, diverge at the end with a rate given byEq.1

$$|\,\delta Y(t)\,| = e^{\gamma t}\,|\,\delta Y_0\,| \qquad (1)$$

Where time is denoted by t and the Lyapunov exponent is denoted by ɣ. The direction of the vector of initial separation judges the rate of separation between trajectories. The overall predictability of the system is determined by the maximum value lapunov exponent. System is chaotic if maximal Lapunov exponent is positive else system is nonchaotic.

B. Background theory on cryptography

Cryptography is the technique of transmitting the original information into a form which can be understood by the person who has the secret key only. Cryptography technique can be applied to text, images and videos. Cryptographic methods applied to videos has gained lot momentum for research basically due to security reasons.Fundamentally video cryptography algorithms are of four types:-

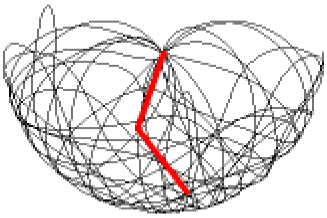


Fig. 1. Chaotic system (simple two pendulums) producing confusion behavior

1) Completely layered encryption

In this type, initially entire video is compressed and encrypted using any conventional encryption techniques namely AES, DES, RSA etc.

2) Encryption using permutation

Video is encrypted using some permutation algorithm, there is more focus on confusion stage compare to diffusion stage.

3) Selective Encryption

Only a few selected bytes of video will be encrypted, not the entire video as mentioned in completely layered encryption.

4) Perceptual encryption

Noise will be added to encrypt the video, video will be visible yet after encryption. The quality of the video will be decreased.

Under completely layered video cryptography algorithm, instead of using conventional algorithms, using chaotic maps gives elevated security by changing the pixel values and its position. Chaos based video cryptography is the encryption of the video by using chaotic maps instead of conventional methods and chaos based video cryptography algorithms are executed in two phases they are,

1. Confusion Phase

Confusion phase creates a link between the original information and encrypted information using the secret key. The goal of this process is to make it difficult to recover the original information, though encrypted information is available as the key used is highly secure and confidential. Proposed method of confusion phase involves generation of a chaotic map by using a random arrangement of the secret key. In other words, part of encrypted information depends on the part of the secret key. Confusion phase involves the generation of chaotic maps which gives confusion characteristics. For instance, Simple physical system of 2 pendulums in which one pendulum is connected to the end of another pendulum such that two pendulums are rotated in 360 degrees. Start moving in some direction (angle) initially as shown in Fig. 1. Here the initial angle is called initial condition.

5) Diffusion Phase

Diffusion process of conventional encryption method involves the horizontal and vertical rotation or shifting of rows and columns in the image, i.e. changing of pixel position, sometimes it involve a change in pixel value. So, a small change in one pixel value affects all the pixel values. Diffusion phase evaluates the technical complexity and dilute the correlation between pixels. In other words, it can be said that diffusion phase is scrambling of the image. For diffusion phase, chaotic encryption methods use bit plane slicing, arithmetic equations, permutation tables etc…Proposed technique of diffusion phase involves a bit plane slicing to spread the pixels of the image in it. The amount of information in each plane is

$$\mathrm{p(i)} = \frac{2^i}{\sum_{i=0-7} 2^i} \qquad (2)$$

C. *Encryption Process*

The major important phases of the proposed system are, Bit plane slicing, Generation of chaotic maps, XOR operation between binary images of video and chaotic maps. And Fig.2 depicts the process of encryption of the video.The propounded technique has the following steps.

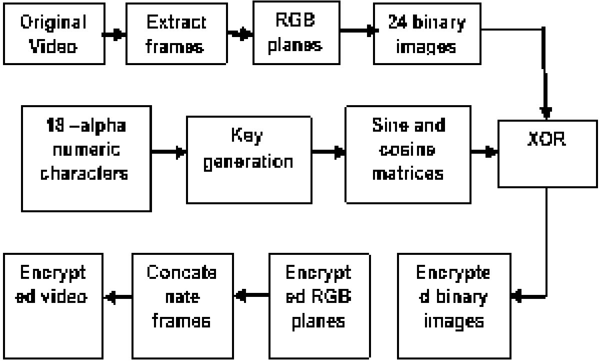


Fig. 2. Block diagram for Encryption

1) Step 1

At first a color video (set of frames) is changed over into still pictures of M*N*3 size, where M is height of the image, N is the image width, 3 demonstrates that an image comprises of 3 planes to be specific red, green and blue. The pixel has 24 bits, out of every 8 bit represents the composition of red green and blue intensity values, sothe original frame consists of 16777216 color values= $(28)^3$.

2) Step 2

Each frame is partitioned into three distinctive segment planes namely, Red component, Green component, Blue component using Matlab commands.

3) Step 3

Bit plane slicing of RGB planes has been performed to get parallel binary images. Bit plane slicing is performed to carry out diffusion process of each frame of video, which causes pixel spreading of the video. Bit plane slicing is the process of dividing the pixel values of 8 bits of gray scale image into a pixel value of a single bit of binary image so that eight binary images will be obtained as shown in Fig 3. MSB plane consists of most significant bits and least significant plane consists of least significant bits. Most significant plane has more information since most significant bits hold high intensity value. 0 in binary image denotes 0 in gray scale and 1 in binary image denotes 255 in gray scale.

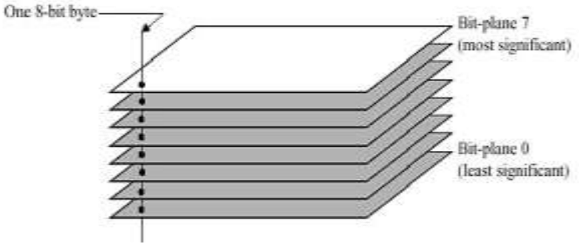


Fig. 3. Bit plane slicing

4) Step 4

Secret words of 18 alphanumeric characters has been considered to use as “hello world 2015n5” which act as external secret key arranged as shown in Table.1 and it is given to the key generation system to get internal secret keys, each letter represents its ASCII value. The arrangement of ASCII value is very random. Randomness gives confusion.

5) Step 5

Each ASCII number has been represented in binary format and those binary numbers have been substituted in given formulae (Eq.3 and Eq.4) to get real numbers RX$_m$ and RY$_m$. The use of floating numbers in chaos encryption method creates complexity in computation compared to use of integers in conventional encryption methods, once again this results in complexity in the encryption process. Where, m ranges from 1 to 8.

$$RX_m = \frac{B_{X1} * 2^0 + B_{X1} * 2^1 + \dots\dots.. B_{X48} * 2^{55}}{2^{56}} \quad (3)$$

$$RY_m = \frac{B_{y1} * 2^0 + B_{y1} * 2^1 + \dots\dots.. B_{y48} * 2^{55}}{2^{56}} \quad (4)$$

6) Step 6

Values of a and b have been calculated using Eq.5 and Eq.6 which act as internal secret keys using below formulae. In a chaotic system, sensitivity to initial condition says that each point has unsurely very close approximation by next successive points with different future trajectories.

$$a_m = (R_{Xm} * R_{Ym}) \quad (5)$$

$$b_m = (R_{Ym} * R_{Ym+1}) \quad (6)$$

7) Step7

Calculated a and b have been used in the below Eq.7 to generate chaotic matrices. This project incorporates both sine and cosine function to enhance the complexity of the technique and the security level of the information. These trigonometric terms have been given more chaos and dynamic behavior to the encryption as they are nonlinear and non-periodic function. Where n denotes number of pixels in each frame and x denotes pixel position. 10π is added to a and b to increase the chaos behavior, according to Lyapunov exponent.

$$x_{n+1} = \cos(10 \prod a_m x_n) + \sin(10 \prod a_m x_n) \quad (7)$$

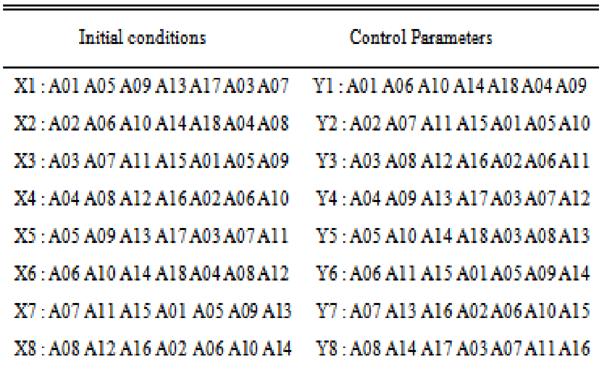
8) Step 8

Xor operation between generated chaotic matrices and each binary frame has been performed to get a new set of binary images in which pixel values changed to some other value called encrypted binary images. Chaotic matrix (C) xor binary image (B) = encrypted image (E).

9) Step 9

Bit plane combining has been carried out to get RGB planes of each frame. Bit plane combining is the process of collecting the single bit pixel values from eight binary images to get gray scale images of 8 bit pixel value. And finally each encrypted frame has been concatenated to get encrypted video.

Table I
Summary of 18-Characters Input Ascii Codes For Setting Initial Conditions And Control Parameters



Initial conditions	Control Parameters
X1 : A01 A05 A09 A13 A17 A03 A07	Y1 : A01 A06 A10 A14 A18 A04 A09
X2 : A02 A06 A10 A14 A18 A04 A08	Y2 : A02 A07 A11 A15 A01 A05 A10
X3 : A03 A07 A11 A15 A01 A05 A09	Y3 : A03 A08 A12 A16 A02 A06 A11
X4 : A04 A08 A12 A16 A02 A06 A10	Y4 : A04 A09 A13 A17 A03 A07 A12
X5 : A05 A09 A13 A17 A03 A07 A11	Y5 : A05 A10 A14 A18 A03 A08 A13
X6 : A06 A10 A14 A18 A04 A08 A12	Y6 : A06 A11 A15 A01 A05 A09 A14
X7 : A07 A11 A15 A01 A05 A09 A13	Y7 : A07 A13 A16 A02 A06 A10 A15
X8 : A08 A12 A16 A02 A06 A10 A14	Y8 : A08 A14 A17 A03 A07 A11 A16

D. *Decryption Process*

Fig.4 shows the block diagram for decryption process. Reverse operation of encryption (decryption) is carried out to get decrypted video i.e. encrypted video has been taken and individual frames have been extracted. RGB planes of a single encrypted frame have been obtained and performed a bit plane slicing to get 24 binary images. Same external secret keys “hello world 2015n5” are given to key generation system which has used the same arrangement of ASCII letters during encryption processes to generate internal secret keys. Later xor operation between encrypted binary images and chaotic maps has been performed to get decrypted binary images then bit plane combining has done to obtain decrypted RGB planes, RGB planes are concatenated to get decrypted single frame. All these procedure has been performed on every encrypted frame to get final decrypted video. Thus use of sine and cosine terms, use of sequence of secret words play an important role during encryption and decryption.

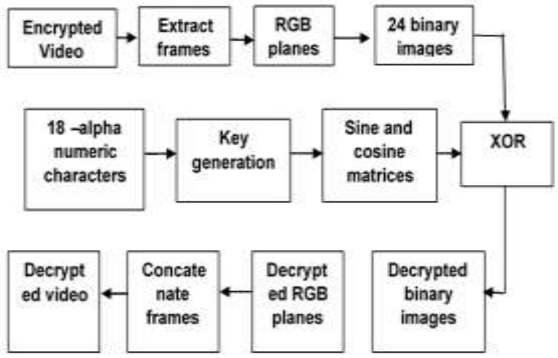


Fig. 4. Block diagram for Decryption process

IV. RESULTS AND ANALYSIS

This section discuss about how a video is encrypted by the proposed strategy for cryptography utilizing Matlab. Fig.5 and Fig.6 describes the three channel of a single frame

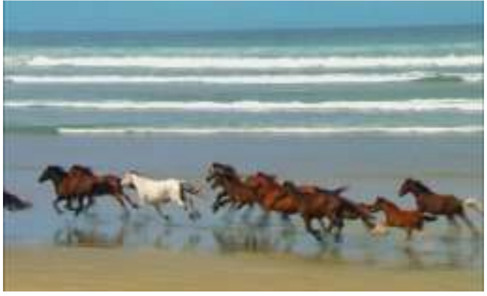


Fig. 5. Single frame extracted from video

Fig.6 shows the binary images of R and G planes. These are obtained by bit plane slicing. The least significant plane is denoted by one and the most significant plane is denoted by eight. The least significant plane has less information about the image and most significant plane has more information about the image.

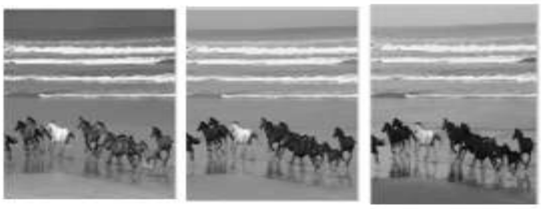


Fig. 6. Red, Green and Blue planes

Finally encrypted binary images of RGB as shown in Fig.7 is obtained after xoring between chaotic matrices and binary images of the original image. Encrypted colored plane as shown in Fig.8 is obtained by performing bit plane combining of encrypted binary images and then concatenation of encrypted RGB planes gives the final encrypted image.

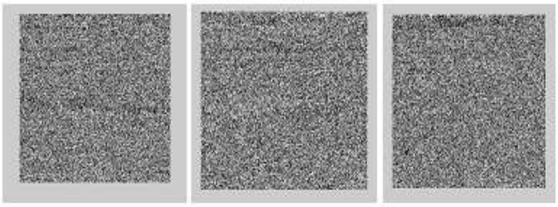


Fig. 7. Encrypted Red, Green and Blue planes

A. Histogram and Power spectrum analysis

A histogram of the image is the graph where the number of pixels distributed at different intensity values i.e. versus pixel value. The histogram is one of the ways to judge characteristics and attributes (brightness and contrast) of the image. For dark images, Histogram has more number of pixels on the side of lower gray level values and for bright images, the histogram has more number of pixels on the side of high gray level values. In the histogram of low contrast images, pixels are concentrated in regions of mid gray level values, but in the histogram of high contrast images pixels are distributed on the side of high gray level values and also on the side of lower gray level values by bifurcating the graph. Histograms for three components such as R, G, B is shown in Fig.9.

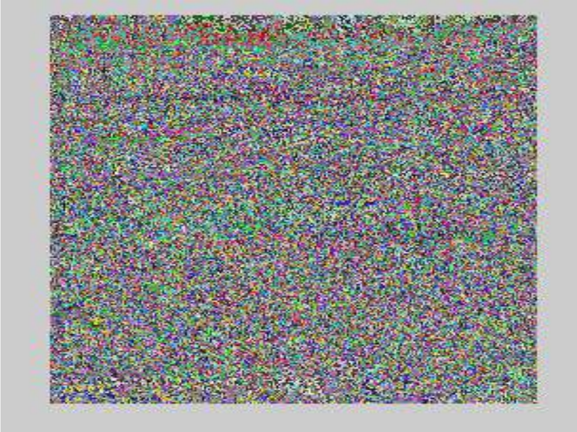


Fig.8 Encrypted Frame

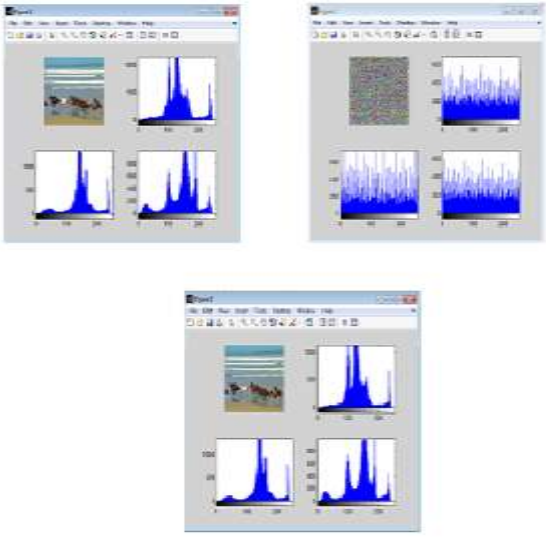


Fig.9. Histogram of original, encrypted and decrypted single frame

The Fourier transform converts image from spatial domain information into frequency domain information. The power spectrum shows the variation in magnitude of frequency components of the image. In the power spectrum of the original image, the magnitude of low frequency components has large value and these can be found in corners, whereas the magnitude of high frequency components has small values and these can be found at the center. Encrypted image has a flat spectrum, since the magnitude of high and low frequency components are at same values. The power spectrum of decrypted image with right secret key resembles the power spectrum of the original image, but power spectrum of decrypted image with wrong key almost resemble the power spectrum of encrypted image since high frequency and low frequency component amplitudes are not at their original values is as shown in Fig 10.

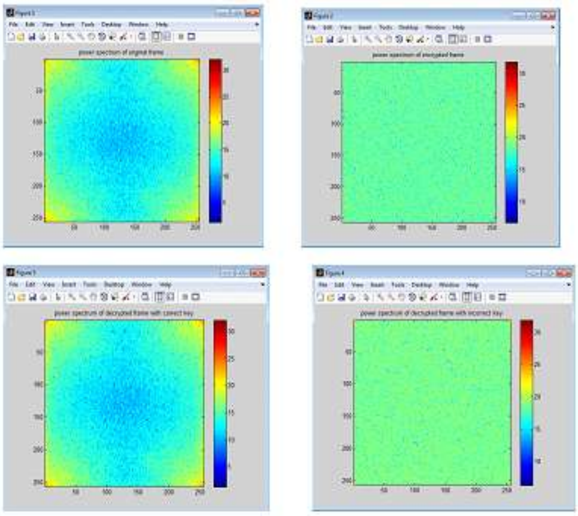

power spectrum of original frame
power spectrum of encrypted frame
power spectrum of decrypted frame with correct key
power spectrum of decrypted frame with incorrect key

Fig. 10. Power spectrum of original, encrypted, decrypted with wrong key decrypted single frame with right key

B. Analysis on NPCR and UACI values

This analysis is performed to check the correlation of pixel values. The pixel difference values between encrypted and original image is measured by NPCR (Net Pixels Changing Rate). The original image and its encrypted image have only one pixel difference is indicated by p1 and p2. The pixel values at pixel position (m,n) is denoted by p1(m,n) and p2(m,n) respectively. Bipolar array d is defined with same size p1 and p2. d(m,n) is obtained by p1(m,n) and p2(m,n). d(m,n)=0 if p1(m,n)=p2(m,n) else d(m,n)=1. The range of NPCR is [0,1]. When N(p1,p2)=0, it implies that all pixels in p2 remain the same values as in p1 . When N(p1,p2)=1 , it implies that all pixel values in p2 are changed compared to those in p1, that means it is very difficult to establish relationships between these image p1 and p2. However, N(p1,p2)=1 happens very rare, because even two separately generated true random images fail to attain this NPCR maximum with a high possibility, especially when the image size is large compared to the largest pixel value in cipher image. The UACI (Unified Average Changing Intensity) deals with the averaged difference between original images and encrypted image. The range of UACI should also be in [0,1]. Values of UACI and NPCR for 15 frames are tabulated in Table 2. The average intensity of differences between two images is measured by UACI. The average of NPCR value is 95.67% and UACI average value is 28.89% which indicates this algorithm has high resistance against attacks.

C. Secret key analysis

Secret analysis is performed to check the sensitivity of the secret key.

1) Case 1:- Wrong key

Key selected during encryption is ‘hello world 2015n5’. If a wrong key is chosen as ‘hello great 152015’ during decryption then the decrypted frame thus obtained will not be the correct one as shown in Fig 11.

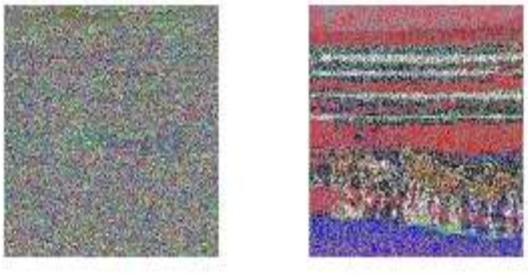


Fig. 11. Encrypted and Decrypted incorrect decrypted frame using wrong key

2) Case 2:- Interchanging secret words

Key selected during encryption is ‘hello world 2015n5’. Correct decrypted video will not be obtained when arrangement of secret words chosen wrongly as ‘world hello 2015n5’ during decryption is as sown in Fig.12

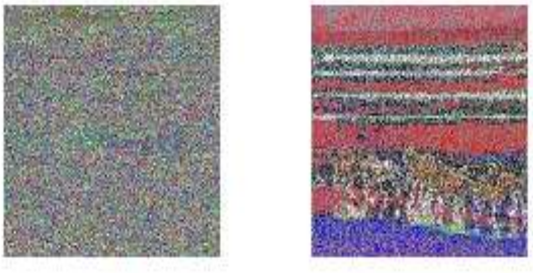


Fig. 12. Encrypted and Decrypted incorrect decrypted frame using interchanging words

V. CONCLUSION

Video cryptosystem implemented in this project, performs video encryption and decryption by changing the pixel values not only by a random arrangement of pixels and also gives high security against hackers. Random arrangements of cipher words (password) are also one of the main keys, that adds complexity. Video cryptosystem is coded and simulated using MATLAB software. NPCR-UACI analysis shows that the average of NPCR value is 93.61% and UACI average value is 27.56%, which indicates that the proposed algorithm has high resistance against attacks so that high secured video is obtained, increased speed as it has moderate computational complexity. The result of giving wrong key and right key during decryption is also shown. But it requires more memory space since no compression technique has been implemented. The encryption technique can be enhanced using more secret words as keys so that hackers cannot decrypt the video easily and can try with different trigonometric functions. Compression techniques can be used to compress the video that helps in faster transmission in communication and provide less memory usage.

REFERENCES

[1] NarsimhaRaju C, UmaDeviGanugula, KannanSrinathan, C. V. Jawahar, “A Novel VideoEncryption 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] NidhiSethi and Deepika Sharma, “ A New Cryptology Approach for Image Encryption”, *2nd IEEE International Conference*,2012.

[4] N.K. Pareeka,b, VinodPatidar a, K.K. Sud, “Image encryption using chaotic logistic map*”, Image and Vision Computing* 24 (2006) 926–934.

[5] M.K Mohsinai and Robin Abraham, “Enhanced chaotic image encryption algorithm based on trigonometric functions”, *Department of P.G, Applied Electronics, ICET*,Mulavoor.

[6] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law, “A Fast Image Encryption Scheme based on Chaotic Standard Map”, Department of Electronic Engineering, City University of Hong Kong.