International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

# Secure Transmission of Video using (2,2) Visual Cryptography Scheme and Share Encryption using Logistic Chaos Method

**Sangita Vishwakarma**[*1], **Shahana Qureshi**[2]
[*1]M. Tech Scholar, CSE, RITEE, Mandir Hasaud, Raipur, Chhattisgarh, India
[2]Assistant Professor, Computer Science Dept., RITEE Mandir Hasaud, Raipur, Chhattisgarh, India

## ABSTRACT

The crucial issue on World Wide Web is the security of communication and authentic transmission of confidential multimedia elements. Web has progressed towards becoming most ordinarily utilized media for communication and consequently message, voice, video, images and numerous more are transmitted through Internet. Cryptography is an important way of sending confidential information in a secret way. There are many cryptographic techniques available. One such variation is visual cryptography in which the image is divided into two or more shares in such a way that the original image cannot be recovered until all the shares are obtained and stacked together. In the present years, various algorithms of visual cryptography in image were considered and developed for the security of the image. In this paper, we have proposed visual cryptography in videos using pixel shuffling method as well as encrypting the videos shares using logistic chaos method. Experimental results and analysis show that the proposed technique can offer greater efficiency regarding the security of information transmission.

**Keywords :** Visual Cryptography, Chaotic Maps, Security, Video Encryption, Pixel Shuffling.

## I. INTRODUCTION

With the development in the field of information and technology over the period of time, new possibilities for communication among us are enlarged. E-Commerce being fast and more reliable method of providing services emerged as one of the most powerful way of interaction between end users like us and government agencies, banking fields and other organizations [1]. With the rapid advancement of network technology, internet has become the convenient media for transmission of multimedia information. Various confidential data are continuously being transmitted over the network. Various techniques have been developed to deal with these issues.

Visual cryptography is introduced by first in 1994 by Noar and Shamir [1]. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, hand written notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret image can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.

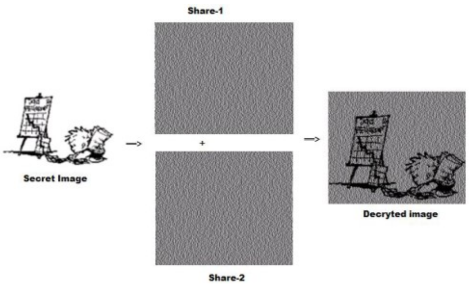


**Figure 1.** Basic visual cryptography scheme

For the case of electronic prints or images, the secret can be dealt directly or can be printed on transparencies and stacking is all required further to know results. According to Naor and Shamir [19], the presumption was that the whole message or image may consist of pixels that are black and white; therefore only two levels will exist. In addition, the white pixel will be transparent while black will be printed as such. This brings the problem of contrast ratio. The process was lossy in the terms of contrast ratio and this could have created a problem while human visual system decodes the secret. Contrast is an important parameter to determine the clarity of the imaging process.

Visual cryptography allows effective and efficient secret sharing between a numbers of trusted parties. The visual cryptography provides a very powerful technique by which one secret can be distributed into two or more shares. VCS is a cryptographic technique that allows for the encryption of visual information in such a way that decryption can be performed using the human visual system. We can achieve this by one of the following schemes.

1. (2, 2) Threshold VCS scheme- This is the simplest threshold scheme that takes a secret message and divides it into two different shares that reveal the secret image when they are overlaid.
2. (n, n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when all the n shares are combined, the secret image will be revealed.
3. (k, n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

There has been a lot of work seen in the area of visual cryptography in images. So the proposed algorithm applies visual cryptography in videos as well as encrypts the shares of the video. However videos generally possess a large amount of data and require extensive computations. In order to deal with the security issues of video data, we need a secure technique with the help of which videos can be sent securely over the network. The proposed scheme has been developed using the advantages and concepts of visual cryptography and chaotic map.
While performing visual cryptography on videos, two shares are generated that can be sent over the network. The shares exist in their normal form while they are being sent over the network. So there is a chance that the original can be obtained by the hackers if they succeed in getting all the shares. Therefore, to deal with this issue, it becomes important to encrypt the shares. Due to this reason, we have encrypted the shares after applying the visual cryptography scheme.

## II. CLASSIFICATION

Generally, the video encryption algorithms are broadly classified into four categories which are described as follows:

1. **Fully layered Encryption**: In this class, entire content of video is first compressed and afterward encrypted utilizing standard algorithms like DES, RSA, IDEA, AES and so forth. This method is not suitable for real time video applications because of heavy calculations and moderate speed.
2. **Permutation based Encryption**: In this class, the algorithms mostly utilize different permutation algorithms. These algorithms scramble the video contents. Each byte of the video is not necessarily scrambled. Some algorithms use permutation list as secret key to encrypt video contents.
3. **Selective Encryption:** The algorithms of this class selectively scramble the bytes of the video content. Since each byte of the video is not encrypted, the overall computational complexity is reduced.
4. **Perceptual Encryption:** This class of algorithms incompletely degrades the quality of visual data, which means that the encrypted contents are

still partially perceptible. Quality degradation needs to be controlled by a factor p.

## III. RELATED WORK

Basic visual cryptography was given by Naor and Shamir's [1] to share a binary image into two shares Share1 and Share2. If pixel is white, one of the above two rows of Figure 2 is selected to generate Share1 and Share2. Similarly if pixel is black, one of the below two rows of Figure 2 is selected to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each of share alone give noise whether it is white or black. Secret image is shown only when both of the images shares are superimposed.

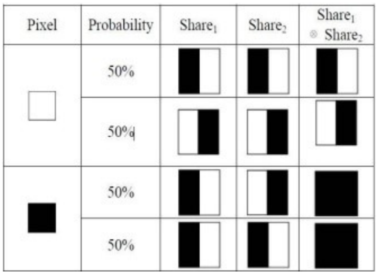


**Figure 2.** Naor and Shamir's scheme for encoding a binary pixel into two shares

Wu and Chen [2] were first researchers to present the visual cryptography schemes to share two secret images in two shares. They hide two secret binary images into two random Shares, namely A and B, such that the first secret can be obtained by stacking the two shares, denoted by $A \otimes B$, and the second secret can be obtained by first rotating A Θ anti-clock wise. Angle restriction of Wu and Chen's scheme [2] was overcome by Hsu et al. [3] who hide two secret images in two rectangular share images with arbitrary rotating angles. S J Shyu et al [5] were first researchers to implement the multiple secrets sharing in visual cryptography. This scheme encodes a set of $n \geq 2$ secrets into two circle shares. The secrets can be obtained one by one by stacking the first share and the rotated second shares with n different rotation angles. Mustafa Ulutas et al [8] advised secret sharing scheme based on the rotation of shares. In this scheme shares are rectangular in shape and are created in a fully random manner. First secret is reconstructed by stacking the two shares. Rotating the first share by 90° in a counter clockwise manner and stacking it with the second share reconstructs the second secret. Multiple image encryption schemes by rotating random grids, without any pixel expansion and codebook redesign was offered by Tzung-Her Chen et al [9].

Zhengxin Fu et al [11] intended a rotational visual cryptography scheme. It was based on correlative matrices set and random permutation that can be used to encode four secret images into two shares. Jonathan Weir et al [12] offered sharing multiple secrets using visual cryptography. A master key is generated for all the secrets; correspondingly, secrets are shared using the master key and multiple shares are obtained. First color visual cryptography scheme was developed by Verheul and Van Tilborg [13]. Colored secret images can be shared with the concept of arc. In color visual cryptography scheme, one pixel is transformed into m sub pixels, and each sub pixel is divided into color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacked sub pixels. Yang and Laih [14] improved the pixel expansion to c × 2 of Verheul and Van Tilborg [13]. But in both of these schemes shares generated were meaningless. Lukac and Plataniotis et al [17] introduced bit-level based scheme to share true-color image by operating directly on S-bit planes of a secret image. To hide a colored image into multiple colored cover images,

Wei Qiao et al [23] suggested visual cryptography scheme for color images based on halftone technique. K. Shankar and Dr. P. Eswaran [27] used Elliptical Curve Cryptography along with Differential Evolution Optimization technique that is applied in the private key generation phase to encrypt the shares. Elliptical Curve Cyptography provides minimal mathematical complexity and is more computationally efficient. DiShiau Tsi, Tzung-

Her Chen and Gwoboa Horng [28] incorporated Genetic Algorithm based Share Construction Method for preventing cheating where some participants can deceive the remaining participants by delivering forged transparencies. Shankar K and Eswaran P [30] suggested encrypting the shares using AES algorithm. The combination of visual cryptography and encryption of images made the process complex but provides high security to the shares generated. Hongjun Lia and Xingyuan Wang [32] proposed a bit level permutation and high dimension chaotic map to encrypt a color image. Any color image of size (MxN) is converted into grayscale image of size (Mx3N) and then transformed into a binary matrix. This matrix is permuted at bit level by scrambling mapping generated by Piecewise Linear Chaotic Map (PWLCM) and used Chen system to confuse and diffuse red, green and blue components simultaneously.

Aman Chadha, Sushmit Malik, Ravdeep Kaur, Ankit Chadha and M. Mani Roja [35] proposed a video encryption using RSA algorithm and Pseudo Noise (PN) sequence. The audio and video components separately undergo two layers of encryption. Encryption of video component involves applying RSA algorithm followed by PN-based encryption. The audio component is encrypted by PN and Then by Discrete Cosine Transform (DCT). Bhawna Shrivas and Shweta Yadav [36] implemented visual cryptography in videos by using Halftoning technique. Halftoning is a process of transforming an image with greater amplitude resolution to one with lesser amplitude resolution. Floyd and Jarvis method has been used for halftoning.

As we have seen most of the work in visual cryptography has been done in the field of gray level & color images. With time the problem of poor quality of recovered image and pixel expansion was improved but brought the issue of share protection & security. Using different encryption algorithms the security issue was solved. But all these concerns were for images. Very little emphasis has been given in the area of visual cryptography in videos. We need to implement a technique that can efficiently apply visual cryptography in videos & also deals with the security issues of the shares. Chaotic encryption has a crucial essentialness because of sensitive dependencies on initial conditions, system parameters, random behavior, non-periodic and topological transitivity, and so forth. In this paper we have proposed (2, 2) visual cryptography scheme for videos using pixel shuffling and used logistic chaos based encryption technique for encrypting the shares of video. We have described the proposed methodology and discussed the results in the following sections which proves the efficiency of the methodology on the basis of various parameters like encryption speed, encryption ratio, key space analysis, noise analysis, PSNR, MSE, pixel correlation, NPCR, UACI, entropy and histogram analysis.

## IV. PROPOSED METHODOLOGY

The main idea behind the proposed methodology is to create two shares of the secret video and encrypt those shares.

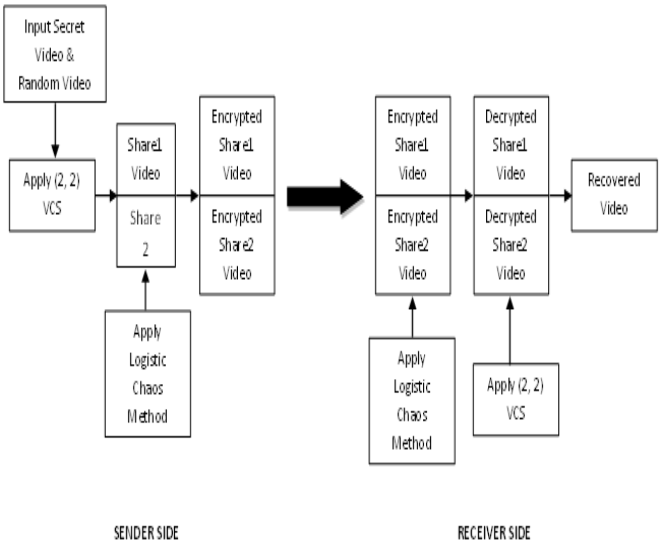


**Figure 3.** Basic visual cryptography scheme

The shares of the video are generated using the (2, 2) visual cryptography scheme with the help of a cover video and the frames of the video shares are encrypted using logistic chaos method.

Main reason for using the encryption is to enhance the security of the visual cryptographic shares. During decryption process, the shares are recovered using the same logistic chaos method and then the original video is obtained using the (2, 2) visual cryptography technique.

## V. SHARE GENERATION

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel. When the shares 1 and 2 are stacked together, it results in the form of complete black or gray (it's partially white and black but visualizes as gray). Because of this when the shares are overlaid, the white in original secret image becomes gray in the stacked result.

In this proposed scheme, a secret video and a cover video are taken as inputs and frames are obtained. Each frame undergoes the process of channel division into red, green & blue channels. The R, G & B components of secret video frames are pixel shuffled with the help of key & then they are complemented. The R, G & B components of cover video frames are also complemented.

After this the corresponding red, green & blue channels of the video frames are ORed, complemented & then combined to get the first share video. The second share video is obtained by ANDing the complemented corresponding R, G & B components of cover video frames & pixel shuffled R, G & B components of cover video frames. Reverse method is required to reconstruct the original video.

The algorithm for generating the shares of video is given below.

**Step 1** Input the random or cover video and divide into frames.

**Step 2** Input the secret video and divide into frames. Separate the red, green and blue channels of frames of random video.

**Step 3** Separate the red, green and blue channels of frames of secret video.

**Step 4** Apply **pixel shuffling operation** using **Key1** on the red, green and blue channels of secret video frames.

**Step 5** Perform complement operation of the red, green and blue channels obtained in step 3.

**Step 6** Perform complement operation of the red, green and blue channels obtained in step 5.

**Step 7** Perform OR operation between red, green and blue channels obtained in step 6 and red, green and blue obtained in step 7.

**Step 8** Perform complement operation on red, green and blue channels obtained in step 8 and combine the resultant channels to obtain the **share1 video**.

**Step 9** Perform AND operation between the red, green and blue obtained in step 5 and red, green and blue obtained in step 6 and combine resultant channels to obtain the **share2 video.**

## VI. SHARE ENCRYPTION

Chaotic scheme has been chosen for the encryption of shares because of the simplified key management as requires assuring the security of the private key transmission in which parameters and initial states of chaotic system are included. The horizontal axis shows the possible values of the parameter r while the vertical axis shows the set of values of x visited asymptotically from almost all initial conditions by the iterates of the logistic equation with that r value. The chaotic map is viewed as a wise decision for encrypting data as a result of its randomness, blending property, high affectability to the underlying conditions, high deterministic properties and high unpredictable arbitrary behaviours [44– 49].

The steps below show the algorithm for encryption of share videos.

**Step 1** Input share1 & share2 video.
**Step 2** Divide both the videos into frames.
**Step 3** Separate the red, green and blue channels of share1 & share2 video.
**Step 4** Apply Logistic Chaos Encryption method on red channel of share1 & share2 video frames using Key2.
**Step 5** Apply Logistic Chaos Encryption method on blue channel of share1 & share2 video frames using Key2.
**Step 6** Apply Logistic Chaos Encryption method on green channel of share1 & share2 video frames using Key2.
**Step 7** Combine the red, green & blue channels obtained in steps 4, 5 & 6 to get the encrypted shares.

**Algorithm for Logistic Chaos Encryption & Decryption method**

**Step 1** Input the frame F.
**Step 2** Calculate the dimension of frame, N = a x b.
**Step 3** Initialize the Key2, i. e., m = 0.3.
**Step 4** For each pixel value, calculate the new values of m by using Logistic Map function

$$m(i+1) = 4*m(i)\ (1 - m(i))$$

**Step 5** Now compute the m as m = mod (1000*m, 256), where m are the values obtained in the step 4.
**Step 6** Apply XOR operation between each frame pixel and the corresponding value of m calculated for that pixel in step 4 to get the encrypted frame.

Logistic mapping is a paradigmatic illustration of chaotic scheme that is a non-linear map given by

$$x_{n+1} = r\,x_n\,(1 - x_n)$$

Appling under the following conditions:

•$x_n$ take value from interval 0, 1.

• r is a control parameter, r € [0,4]

• Initial value $x_0$ = 0.3.

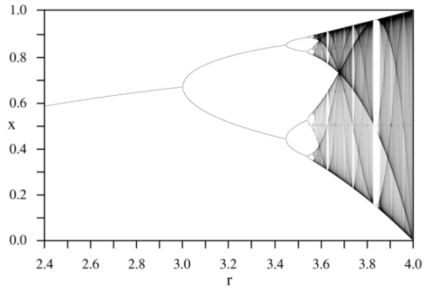
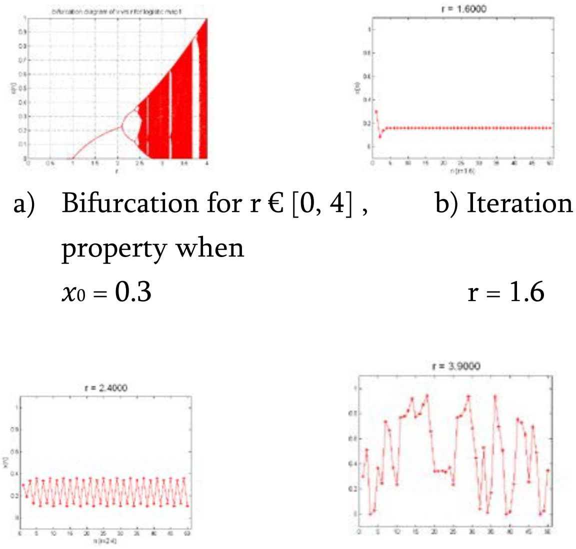


**Figure 4.** Bifurcation Diagram

A property of these maps is that their corresponding function has one maximum point. The system has different characteristics with different values of r, called the bifurcation parameter. For r > 3.564 starts the process of bifurcation. It may be noted that the closer the value of 4, the more chaotic the system response will be. Figure 3.1 shows the different characteristics for the values of $x_n$.

In addition, we use MATLAB software to graph the bifurcation diagram of logistic chaotic map1 as show in figure 4.



a) Bifurcation for r € [0, 4] , property when $x_0$ = 0.3

b) Iteration r = 1.6

c) Iteration property when property when r = 3.8

d) Iteration r = 2.4

**Figure 5.** Analysis of logistic chaotic map

## VII. EXPERIMANTAL RESULTS AND ANALYSIS

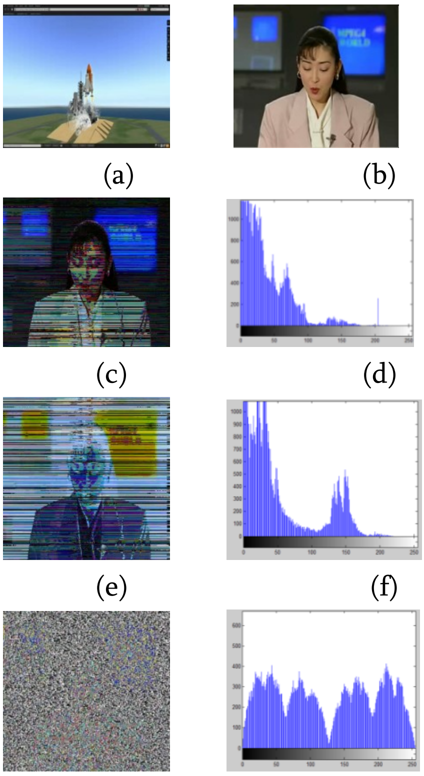
A good encryption technique should be stable through various attacks like brute-force attack and statistical attacks. This section proves the efficiency of the proposed algorithm based on various analyses.

### Statistical Analysis

A perfect cipher should be robust against any sort of statistical attacks. In order to prove their robustness, various statistical analyses have been performed on the proposed algorithm which includes histogram analysis, correlation coefficient analysis, entropy analysis, PSNR analysis, speed analysis.

### A. Histogram Analysis

Histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. We have calculated and analyzed the histograms of random frames of original shares and encrypted shares. Figure 5(a) and (b) show the frame from the secret video and random video respectively. Figure 5(c) and (d) show the original frames of the two video shares and Figure 5(e) and (f) shows their encrypted frames. Figure 5 (g), (h), (i) and (j) show their histograms. We observe that the histograms of the original and encrypted frames are different and the histograms of the encrypted frame are uniform.

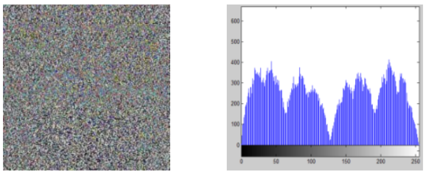


(a) (b)

(c) (d)

(e) (f)

(g) (h)



(i) (j)

**Figure 5.** Histogram analysis

### B. Correlation Coefficient Analysis

In this analysis, the horizontal, vertical and diagonal correlation coefficient of the pixels studied. Horizontal, vertical & diagonal Correlation coefficients $r_{(x,y)}$ of two adjacent pixels can be calculated using the following equations

$$r_{(x,y)} = \frac{COV(x,y)}{\sqrt{D(x)D(y)}},$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \sum_{i=1} x_i)^2 ,$$

$$COV(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big),$$

$$E(z) = \frac{1}{N}\sum_{i=1}^{N} z_i$$

Where x and y are gray-scale values of two adjacent pixels in the image. A correlation coefficient approaching to 1 indicates a strong correlation while the coefficient close to 0 means extremely low correlation.

The table below shows the correlation coefficient of the original and encrypted frame.

**Table 1.** Correlation Coefficient Of The Original And Encrypted Frame

| VIDEOS | | HC | VC | DC |
|---|---|---|---|---|
| Shuttle.avi | Original Share 1 | 0.9402 | -0.3433 | 0.9086 |
| | Encrypted Share 1 | 0.0487 | -0.0346 | 0.0484 |
| | Original Share 2 | 0.9540 | 0.5051 | 0.9388 |
| | Encrypted Share 2 | -0.0100 | -0.0214 | -0.0843 |

As shown in above table, the correlation coefficients of the original image are close to 1 while those of the encrypted image are around zero. This further verifies that the encrypted image has good randomness and its adjacent pixels have extremely low correlation.

### C. Entropy Analysis

Entropy is defined as

$$H = -\sum_{k} p_{k \log_2(p_k)}$$

It shows the randomness of the data. According to the given equation, we can get the ideal H = 8, which shows that the information is random. Hence the information entropy of the encrypted image should be close to after encryption. The closer it gets to 8, the less possible for the cryptosystem to divulge information. Below table shows the entropy values, as we can find that they are all close to the ideal value 8.

**Table 1.** Enropy Of The Original And Encrypted Frame

| VIDEOS | | ENTROPY |
|---|---|---|
| Shuttle.avi | Original Share 1 | 6.3900 |
| | Encrypted Share 1 | 7.9983 |
| | Original Share 2 | 6.8695 |
| | Encrypted Share 2 | 7.9954 |

### D. PSNR & MSE Calculation

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. Given a noise-free m*n monochrome image I and its noisy approximation K, MSE is defined as

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{i=1}^{n}\left(I(i,j)-K(i,j)\right)^2$$

The PSNR (in dB) is defined as

$$PSNR = 10.\log_{10}\left(\frac{MAX_i^{\,2}}{MSE}\right)$$

Here, $MAX_i$ is the maximum possible pixel value of the image.

The below table gives the values of MSE & PSNR for the video shuttle.avi.

**Table 3.** Psnr &Mse Of The Original And Recoveed Video

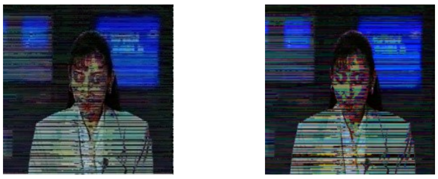
| VIDEOS | | MSE | PSNR |
|---|---|---|---|
| Shuttle.avi | Between Original Video & Encrypted Video | 1.5000e-005 | 96.3699 |

### Sensitivity Analysis

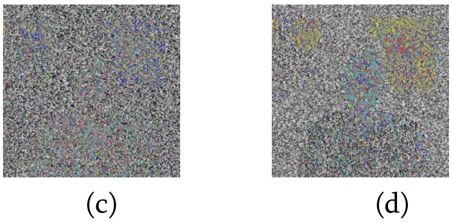
An ideal image encryption procedure should be sensitive to any small change in plain image and secret key.

### A. Key Sensitivity

A good encryption process ought to be sensitive towards little changes of key. This implies that a one-bit change in key causes an altogether different outcome. In this paper, one bit of the key was changed and the encrypted frame was decrypted with the new key. As a result, this new decrypted frame is entirely different from the original frame. In order to test the key sensitivity of the proposed algorithm, we have generated the video shares with exact key and slight different key whose frames are shown in figure 6(a) and 6(b). The video shares are encrypted using two slightly different control parameters whose frames are shown in figure 6(a) and 6(b). These outputs are compared for equality and the outcomes prove that the results obtained using different keys are different.



(a) (b)



(c) (d)

**Figure 6.** Key sensitivity analysis: (a) Frame of the video share generated using exact key (K) (b) Frame of the video share generated using different key (K’) (c) Encrypted frame using exact key (K) (d) Encrypted frame using different key (K’)

**B. Plain Image Sensitivity**

In encryption, the cipher resistance to differential attacks is commonly analyzed via the NPCR and UACI tests. The NPCR and UACI are designed to test the number of changing pixels and the number of averaged changed intensity between cipher images, respectively, when the difference between plain images is subtle.

Consider two images, whose corresponding plain images and encrypted images; be denoted by Io and Ienc. A bipolar array, D with the same size as images Io and Ienc is defined. Then, D(i,j) is determined by Io(i,j) and Ienc(i,j), namely, if Io(i,j) = Ienc(i,j) then D(i,j) = 0; otherwise, D(i,j) = 1.

NPCR is defined as

$$NPCR = \sum_{i=1}^{M}\sum_{j=1}^{N} D(i.j) * \frac{100\%}{M * N}$$

Where

$$D(i.j) = \begin{cases} 0, \ if\ Io(i,j) = Ienc(i,j) \\ 1, if\ Io(i,j)\ \neq Ienc(i,j) \end{cases}$$

The NPCR measures the percentage of different pixel numbers between the plain image and the cipher image.

UACI measures the average intensity of differences between the two images which is defined as

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{[Io(i,j) - \ Ienc(i,j)]}{255}\right] * \frac{100\%}{M * N}$$

**Table 4.** Npcr & Uaci Values Of The Original And Encrypted Frame

| VIDEOS | | NPCR | UACI |
|---|---|---|---|
| Shuttle. avi | Share 1 & Encrypted Share 1 | 99.5001 | 39.5896 |
| | Share 2 & Encrypted Share 2 | 99.5181 | 28.9621 |

We can find that the NPCR is over 99% and the UACI is around 33%, the results show that the proposed algorithm is very sensitive to tiny changes in the plain image.

**Key Space Analysis**

The strength of the key depends on the size of the key that is used for encryption and decryption. Having a large key space ensures a strong resistance against brute-force attacks. In our proposed scheme, we have used two keys for securing the video. One is used during the share generation process that is considered to be of 80 bits. Therefore the key space is $2^{80}$ . The key size for logistic chaos based encryption results from two parameters. One is the control parameter $r$ and other is the initial condition $x_0$. Their values can be changed to enhance the security. They all are stored in double data type and the required memory space of one parameter is 8 bytes or 64 bits. Therefore the key size for logistic chaos based encryption is 128 bits, so the key space is $2^{128}$ . For an unknown set of $r$ and $x_0$, decryption is not possible. The strength of the two keys together is quite sufficient against brute force attacks.

## VIII. CONCLUSION

Through this paper, we have provided an encryption methodology that serves to securing video data utilizing the concepts of visual cryptography and logistic chaos method. The proposed scheme utilizes the confusion and diffusion properties to achieve high security level. The confusion step deals with pixel shuffling operation and the diffusion step applies the XOR operation. The proposed method is tested for robustness and efficiency by calculating entropy, NPCR & UACI, PSNR & MSE, correlation coefficient, histogram analysis, key space and key sensitivity analysis. The results of these analysis show that the proposed scheme is effective and secure for transmission of video data over network. For future enhancement, it is proposed that the encryption time can be reduced by applying video compression, as we have not compressed the video before encryption. Further, we will be taking audio component also into consideration and we will be creating more than two shares of the input video. Future research will be to decrease the encryption time and to increase the security of the encryption.

## IX. REFERENCES

[1]. Moni Naor and Adi Shamir, "Visual Cryptography", Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, Vol. 950, Springer, Berlin, 1995, pp. 1–12

[2]. C.C. Wu, L.H. Chen, "The Comparative Study on Visual Cryptography and Random Grid Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[3]. H.-C.Hsu, T.-S. Chen,Y.-H.Lin, "The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing", in Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp.996– 1001, March 2004.

[4]. H.-C.Wu, C.-C.Chang, "Sharing Visual Multi-Secrets Using Circle Shares", Comput. Stand. Interfaces 134 (28), pp.123–135, (2005).

[5]. S.J.Shyu, S.Y.Huanga, Y.K.Lee, R.Z.Wang, and K.Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol.40, Issue 12, pp.3633-3651, 2007.

[6]. Wen-Pinn Fang, "Visual Cryptography In Reversible Style", IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2007), Kaohsiung, Taiwan, R.O.C, 2007.

[7]. Jen-Bang Feng, Hsien-ChuWu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, "Visual Secret Sharing For Multiple Secrets", Pattern Recognition 41, pp.3572–3581, 2008.

[8]. Mustafa Ulutas, Rıfat Yazıcı, Vasif V.Nabiyev, Güzin Ulutas, (2, 2)- "Secret Sharing Scheme With Improved Share Randomness",978-1-4244-2881-6/08,IEEE,2008.

[9]. Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple-Image Encryption By Rotating Random Grids", Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256, 2008.

[10]. Wen-Pinn Fang,"Non-Expansion Visual Secret Sharing In Reversible Style", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009.

[11]. Zhengxin Fu, Bin Yu, "Research on Rotation Visual Cryptography Scheme", International Symposium on Information Engineering and Electronic Commerce, pp 533-536, 2009.

[12]. Jonathan Weir, Wei Qi Yan, "Sharing Multiple Secrets Using Visual Cryptography", 978-1-4244-3828-0/09, IEEE, pp509-512, 2009.

[13]. E. Verheuland H. V. Tilborg, "Constructions and Properties of K Out Of N Visual Secret Sharing Schemes" Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.

[14]. C. Yang and C. Laih, "New Colored Visual Secret Sharing Schemes". Designs, Codes and cryptography, 20, pp. 325– 335, 2000.

[15]. C. Chang, C. Tsai and T. Chen, "A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27, July 2000.

[16]. Chin-Chen Chang, Tai-Xing Yu, "Sharing A Secret Gray Image In Multiple Images",

Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.

[17]. R. Lukac, K.N. Plataniotis, "Bit-Level Based Secret Sharing For Image Encryption", Pattern Recognition 38 (5), pp. 767–772, 2005.

[18]. R.Youmaran, A. Adler, A. Miri, "An Improved Visual Cryptography Scheme For Secret Hiding", 23rd Biennial Symposium on Communications, pp. 340-343, 2006.

[19]. S.J. Shyu, "Efficient Visual Secret Sharing Scheme For Color Images", Pattern Recognition 39(5) ,pp. 866–880, 2006.

[20]. Mohsen Heidarinejad, Amirhossein Alamdar Yazdi and Konstantinos N. Plataniotis Algebraic Visual Cryptography Scheme For Color Images", ICASSP, pp. 1761-1764, 2008.

[21]. Haibo Zhang, Xiaofei Wang,Wanhua Cao, Youpeng Huang, "Visual Cryptography For General Access Structure By Multi-Pixel Encoding With Variable Block Size", International Symposium on Knowledge Acquisition and Modeling, pp. 340-344, 2008.

[22]. F. Liu1, C.K. Wu X.J. Lin, "Colour Visual Cryptography Schemes", IET Information Security, vol. 2,No. 4, pp 151-165, 2008.

[23]. Wei Qiao, Hongdong Yin, Huaqing Liang, "A kind Of Visual Cryptography Scheme For Color Images Based On Halftone Technique", International Conference on Measuring Technology and Mechatronics Automation 978-0-7695-3583-8/09, pp. 393-395, 2009.

[24]. Du-Shiau Tsai, Gwoboa Horng, Tzung-Her Chen, Yao-TeHuang, "A Novel Secret Image Sharing Scheme For True Color Images With Size Constraint", Information Sciences 179 3247–3254 Elsevier, 2009.

[25]. Daoshun Wang, Feng Yi, XiaoboLi, "On General Construction For Extended Visual Cryptography Schemes", Pattern Recognition 42(2009), pp 3071– 3082, 2009

[26]. Jung-San Lee, T.Hoang Ngan Le, "Hybrid (2, N) Visual Secret Sharing Scheme For Color Images", 978-1-4244-4568-4/09, IEEE, 2009.

[27]. K.Shankar and Dr. P. Eswaran, "ECC Based Image Encryption Scheme with aid of Optimization Technique using Differential Evolution Algorithm", International Journal of Applied Engineering Research, ISSN 973-4562, Vol 10, No. 55 (2015).

[28]. DiShiau Tsi, Tzung-Her Chen and Gwoboa Horng, "A Cheating Prevention Scheme for Binary Visual Cryptography with Homogeneous Images ", The Journal of Pattern Recognition Society, pattern Recognition 40 (2007) 2356-2366.

[29]. R. Anushiadevi, Padmapriya Praveen Kumar, John Bosco and Rengarajan, "Revolving of pixels and bits in Pixels-Plan (E) Tary Encryption ", Reserch Journal of Information Technology, ISSN 1815-7432, DOI: 10.3923/rjit.2017.25.31.

[30]. Shankar K and Eswaran P, "Sharing a secret image with Encapsulated Shares in Visual Cryptography", 4th International Conference on Eco-friendly Computing and Communication System, ICECCS, 2015, Procedia Computer Science 70 (2015) 462 – 468.

[31]. Zhou, K. Panetta, S. Agaian and C. L. P Chen, "Image Encryption Using P – Fibonacci Transform and Decomposition", Optics Communication, 285: 594-608.

[32]. Hongjun Lia and Xingyuan Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system", Optics Communications, 284 (2011) 3895–3903, August 2011.

[33]. Obaida M. Al-Hazaimeh, Nouh Alhindawi, Sofyan M. A. Hayajneh and Ammar Almomani, "HANON Chaotic Map-Based New Digital Image Encryption Algorithm", MAGNT Research Report (ISSN. 1444-8939) Vol.2 (4). PP: 261-266, August 2014.

[34]. Paul A.J, P. Mythili and K. Paulose Jacob, "Matrix based cryptographic procedure for efficient image encryption", Conference Paper ·

September 2011, DOI: 10.1109/RAICS.2011.6069296.

[35]. Aman Chadha, Sushmit Malik, Ravdeep Kaur, Ankit Chadha and M. Mani Roja, "Dual-Layer Video Encryption using RSA Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, April 2015.

[36]. Bhawna Shrivas and Shweta Yadav, "Visual Cryptography in the Video using Halftone Technique", International Journal of Computer Applications (0975 – 8887) Volume 117 – No.14, May 2015.

[37]. Noora Shihab Ahmed, Halabja University, " Multi-Image Encryption Technique Based on Permutation of Chaotic System", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:16 No:01

[38]. Rezvaneh Babazade Gorji ,Mirsaeid Hosseini Shirvani, Farhad Ramezani Mooziraji, "A new image encryption method using chaotic map", Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 3159-0040 Vol. 2 Issue 2, February – 2015

[39]. Hossam Eldin H. Ahmed, Ayman H. Abd El-aziem, "Image Encryption Using Development of Chaotic Logistic Map Based on Feedback Stream Cipher", Recent Advances In Telecommunications, Informatics And Educational Technologies, ISBN: 978-1-61804-262-0.

[40]. Kamal Jadidy Aval, Morteza Sabery Kamarposhty, Masumeh Damrudi, "A Simple Method for Image Encryption Using Chaotic Logistic Map", Journal of Computer Science & Computational Mathematics, Volume 3, Issue 3, September 2013

[41]. Nicole Kengnou Telem, ColinceMeli Segning,Godpromesse Kenne and Hilaire Bertrand Fotsin, "A Simple and Robust Gray Image Encryption Scheme UsingChaotic Logistic Map and Artificial Neural Network", Hindawi Publishing Corporation, Advances in Multimedia Volume 2014, Article ID 602921, 13 pages, http://dx.doi.org/10.1155/2014/602921

[42]. Liguo Fang, BinYu, "Research On Pixel Expansion Of (2,n) Visual Threshold Scheme", 1st International Symposium on Pervasive Computing and Applications ,pp. 856-860, IEEE.

[43]. M. Yang, N. Bourbakis, and S. Li, "Data-image-video encryption," IEEE Potentials, vol. 23, no. 3, pp. 28–34, 2004.

[44]. Y. Mao and G. Chen, Chaos-Based Image Encryption, Springer,Berlin, Germany, 2005.

[45]. G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," Pattern Recognition etters, vol. 31, no. 5, pp. 347–354, 2010.

[46]. S. Fu-Yan, L. Shu-Tang, and L. Zong-Wang, "Image encryption using high-dimension chaotic system," Chinese Physics, vol. 16,no. 12, pp. 3616–3623, 2007.

[47]. V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitutiondiffusion based image cipher using chaotic standard and logistic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 14, no. 7, pp. 3056–3075, 2009.

[48]. Y. Wu, J. P. Noonan, G. Yang, and H. Jin, "Image encryption using the two-dimensional logistic chaotic map," Journal of Electronic Imaging, vol. 21, no. 1, Article ID013014, 2012.

[49]. Y. Wu, J. P. Noonan, and S. Agaian, "A wheel-switch chaotic system for image encryption", Proceedings of the International Conference on System Science and Engineering (ICSSE '11), pp. 23–27, June 2011.

[50]. D. Valli and K. Ganesan, "Chaos based video encryption using maps and Ikeda time delay system", THE EUROPEAN PHYSICAL JOURNAL PLUS (2017) 132: 542 DOI 10.1140/epjp/i2017-11819-7.

[51]. Saumya Batham, Anuja Kumar Acharya, Virendra Kumar Yadav, Rahul Paul, "A New Video Encryption Algorithm Based on Indexed Based Chaotic Sequence", Confluence 2013:

IEEE, The Next Generation Information Technology Summit (4th International Conference), June 2014, DOI: 10.1049/cp.2013.2307.

[52]. Franco Chiaraluce, Lorenzo Ciccarelli, Ennio Gambi, Paola Pierleoni and Maurizio Reginelli, "A NEW CHAOTIC ALGORITHM FOR VIDEO ENCRYPTION", IEEE Transactions on Consumer Electronics, Vol. 48, No. 4, NOVEMBER 2002.

[53]. Saumya Batham, Virendra Kumar Yadav, Amit Kumar Mallik, "ICSECV: An Efficient Approach of Video Encryption", IEEE, 2014 Seventh International Conference on Contemporary Computing (IC3), DOI: 10.1109/IC3.2014.6897211.

[54]. Ms. Pooja Deshmukh, Ms. Vaishali Kolhe, "Modified AES Based Algorithm for MPEG Video Encryption", IEEE, 2014 International Conference on Information Communication and Embedded Systems (ICICES), DOI: 10.1109/ICICES.2014.7033928.

[55]. Aya Khalid Naji, Saad Najim Alsaad, " Data (Video) Encryption in Mobile Devices", Kurdistan Journal of Applied Research (KJAR), Print-ISSN: 2411-7684 – Electronic-ISSN: 2411-7706, Volume 2, Issue 3, August 2017, DOI: 10.24017/science.2017.3.17.

[56]. Ping Zhen, Geng Zhao, Lequan Min, Xiaodong Li, IEEE, 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, DOI 10.1109/3PGCIC.2014.69.

[57]. ROHITH S, K N HARI BHAT, A NANDINI SHARMA, "Image Encryption and Decryption using Chaotic Key Sequence Generated by Sequence of Logistic Map and Sequence of States of Linear Feedback Shift Register", IEEE, 2014 International Conference on Advances in Electronics, Computers and Communications(ICAECC), DOI: 10.1109/ICAECC.2014.7002404.

[58]. Zeinab Fawaz, Zeinab Zbib, Ayman Khalil and Samih Abdul-Nabi, "Chaos-Based Video Encryption for Network Coded Wireless Systems", IEEE, 2013 25th International Conference on Microelectronics (ICM) DOI: 10.1109/ICM.2013.6734982.

[59]. Dhananjay M. Dumbere, Nitin J. Janwe, "Video Encryption Using AES Algorithm", IEEE, 2nd International Conference on Current Trends in Engineering and Technology, ICCTET’14, DOI: 10.1109/ICCTET.2014.6966311.

[60]. W. Hamidouche, M. Farajallah, M. Raulet, O. D´eforges and S. El Assad, "SELECTIVE VIDEO ENCRYPTION USING CHAOTIC SYSTEM IN THE SHVC EXTENSION", 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), DOI: 10.1109/ICASSP.2015.7178273

[61]. Keshav S. Kadam, Prof. A. B. Deshmukh, "Video Frame Encryption Algorithm using AES", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 5 Issue 06, June-2016.

[62]. Min Long, Li Tan, "A chaos-based data encryption algorithm for image/video", IEEE,2010 Second International Conference on Multimedia and Information Technology (MMIT), DOI: 10.1109/MMIT.2010.27.

[63]. Pradeep Pai T, Raghu Me, Ravishankar K C, "Video Encryption For Secure Multimedia Transmission - A

[64]. Layered Approach", 2014 3rd International Conference On Eco-Friendly Computing And Communication Systems, Doi: 10.1109/Eco-Friendly.2014.101.