Chaos based Encryption and Decryption of Image and Video in Time and Frequency Domain

Ajay Kumar Dubey
Department of Computer Science and Engineering, United College of Engineering and Research, Allahabad, India

Chandra Kant Shukla
Department of Computer Science, Government Girls Polytechnic, Amethi, India

ABSTRACT
Encryption is one of the well known technique to provide security in transmission of multimedia contents over the internet and wireless networks. The simplest way of encrypting multimedia content is to consider the three-dimensional image or video stream as a one dimensional stream and to encrypt the entire content using standard block ciphers like AES, DES, IDEA etc. But the main flaw of this approach is, it requires too much processing time. So here new method of encrypting the multi-media content is proposed. In the following chaotic map based encryption scheme, we propose the combination of two dimensional chaotic map and discrete cosine transform method for encryption of video data. The proposed encryption scheme is more secure. Since chaos possesses many interesting properties, such as deterministic but random-like complex temporal behavior, high sensitivity to initial conditions and ergodicity etc. These properties have been found to be very useful in cryptographic designs.

General Terms
Encryption, Decryption, Security etc.

Keywords
Chaos, Permutation, Confusion, Diffusion, Chaotic map etc.

1. INTRODUCTION
Nowadays the applications like video telephony, video on demand, network based DVD recorders and IP television etc. are very common. Since digital images and videos are now transmitted over internet and wireless networks very frequently. So the security of digital images and videos are very important. Encryption is one of the most important technologies which ensure the security of digital images and videos.

Encryption is the process of converting the data into legible form to illegible form so that the message is kept secret. The main aim of cryptography is to provide an easy and inexpensive means of encryption and decryption of data to all authorized users and its vice-versa to all unauthorized users. There are two common principles to design a cryptographic system: confusion and diffusion [4]. Confusion or substitution is the increasing of independency of the statistics of cipher on the statistics of the plain text, while the Diffusion or permutation is the shuffling of information from one into many, to hide the statistical structure of the message [2]. Since chaotic systems has characteristic like ergodicity, sensitive dependency on initial conditions and random like behaviors etc. These properties are of great importance in permutation and substitution process [10]. The rest of paper is organized is as follows. In Section 2, we describe the image encryption algorithm in detail. In Section 3 the experimental results and security analysis are presented and finally the Section 4 concludes the paper.

2. THE PROPOSED ALGORITHM
The presented image and video encryption algorithm includes following two stages:

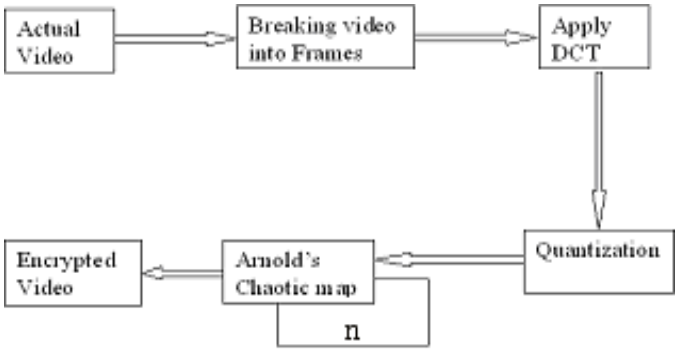

Fig 1: Encryption Process

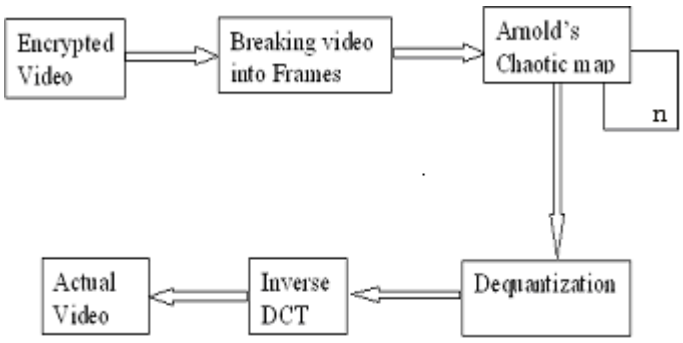

Fig 2: Decryption Process

Firstly the pixel value diffusion or substitution is done by computing the discrete cosine transform (DCT) of image in time domain. Then the confusion or permutation is done by changing the position of the pixels of the original image with the help of the Arnold's cat map.

2.1 Confusion

The first stage of the proposed encryption scheme is to compute the discrete cosine transform (DCT) of 8x8 pixel block of image. We can depict the procedure as the following steps.

Step1 The image is broken in to 8x8 blocks of pixels.

Step2 Working from left to right, top to bottom, the DCT is applied to each block.

Step3 Each block is compressed through quantization process by using JPEG default quantization matrix.

Step4 The array of compressed blocks that constitute the image is stored in a drastically reduced amount of space.

Step5 When desired, the image is reconstructed through decompression, a process that uses the Inverse Discrete Cosine Transform (IDCT).

2.2 Diffusion

The second stage is based on the truth that image data have strong correlations among adjacent pixels. Statistical analysis on large amount of images shows that averagely adjacent 8 to 16 pixels are correlative in horizontal, vertical and also in diagonal directions for both natural and computer graphical images. In order to disturb the high correlation among pixels, we adopt Arnold's cat map to permute the pixel positions of the plain-image. Assume that the dimension of the original image is NxN.

The concept of Arnold cat map [10] is given by Russian mathematician Vladimir I. Arnold, who discovered it using an image of a cat's face. The classical Arnold's cat map is a two-dimensional map [3,4] described by:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N \qquad (1)$$

where (x,y) is the pixel position in the NxN image so the coordinates of the pixels are:

$$S=\{ (x_n, y_n) : x_n, y_n = 0.1.2.....N-1\} \qquad (2)$$

and x_{n+1}, y_{n+1} is the transformed position after cat map. a and b are two positive integers control parameter. Arnold cat map is a chaotic map which has two typical factors, which bring chaotic movement: tension (multiply matrix to enlarge in x and y direction) and fold (taking mod in order to bring x, y in unit matrix).

Image pixel position is scrambled via the iteration of pixel positions of the cat map, consequently realizing the image encryption. The result of scrambling is different for various iteration times [1]. The cat map has the periodicity e.g. for a 256x256 image , it is hard to find out the trace of the original image after iterating just 30 time, reaching the effect of scrambling; the image after iterating 64 times is the same as the original image. With the difference of the parameter and the image's size, the periodicity is different. The Arnold's cat map only transforms the original image pixels position, however the pixels values is not changed in this permutation process.

The example of encryption and decryption process is shown in Figure 4 and Figure 5.

Fig 3: Original Image

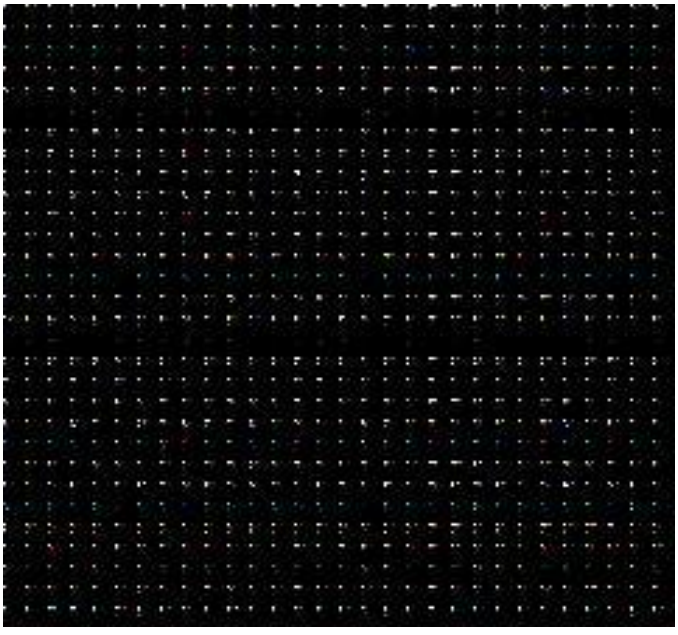

Fig 4: Encrypted Image

Fig 5: Decrypted Image

3. EXPERIMENTS RESULTS AND SECURITY ANALYSIS

A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute force attacks [5]. Here we discuss the security analysis of the proposed image and video encryption schemes based on statistical analysis such as color histogram, correlation and peak signal to noise ratio (PSNR) etc [6].

To prove that the proposed encryption scheme is secure against the most common attack, these statistical analysis test is performed on different images and similar results are obtained. It has been found that this scheme is suitable for images as well as for video data also.

3.1 Color Histogram Analysis

An image color histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculate and analyzed the histograms of the several encrypted as well as their original images that have widely different content.

The example of such histogram analysis are shown in Figure 6,7,8 and Figure 9,10,11.

It is clear from Encrypted Image Histogram figure that the histograms of the encrypted image are fairly uniform and significantly different from the respective histogram of the original image and hence it does not provide any clue to employ any statistical attack on the proposed image and video encryption procedure.

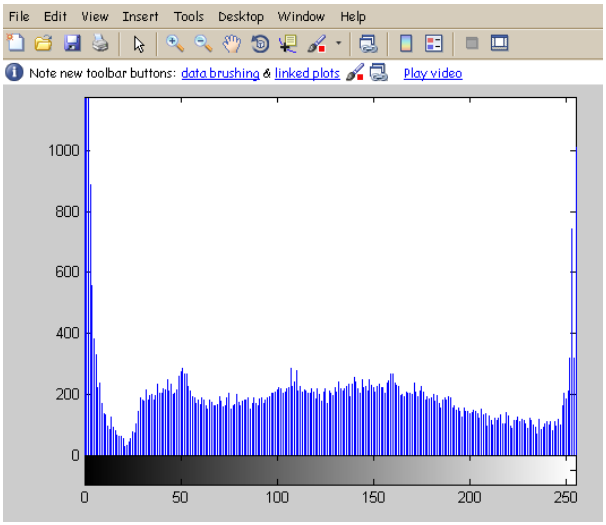

Fig 6: Original Image Histogram(Red)

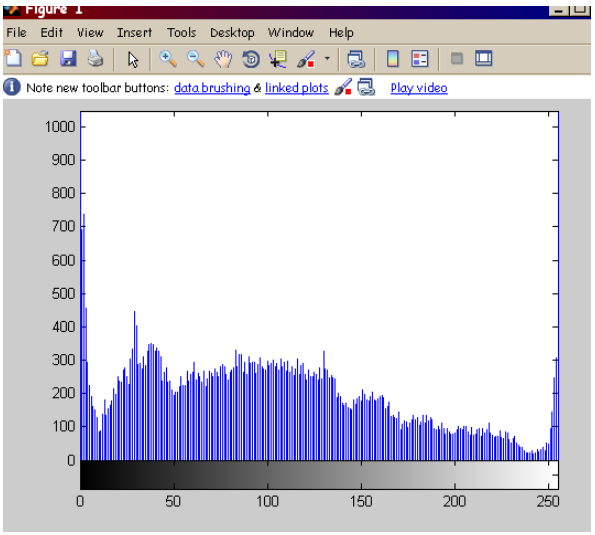

Fig 7: Original Image Histogram (Green)

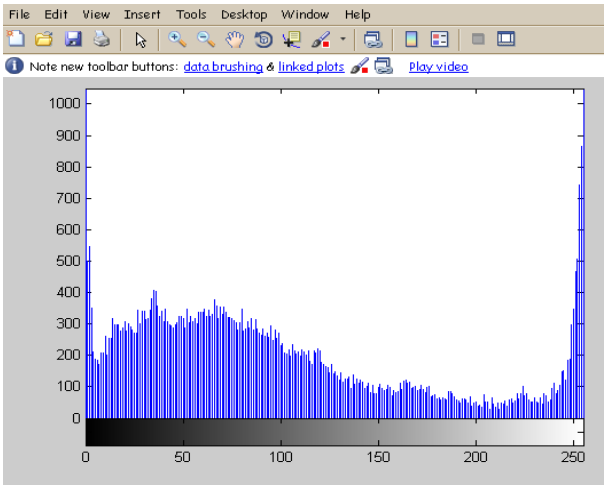

Fig 8: Original Image Histogram (Blue)

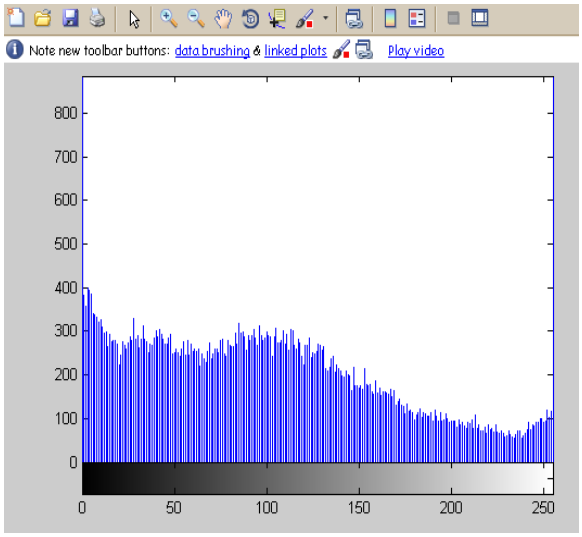

Fig 9: Encrypted Image Histogram (Red)

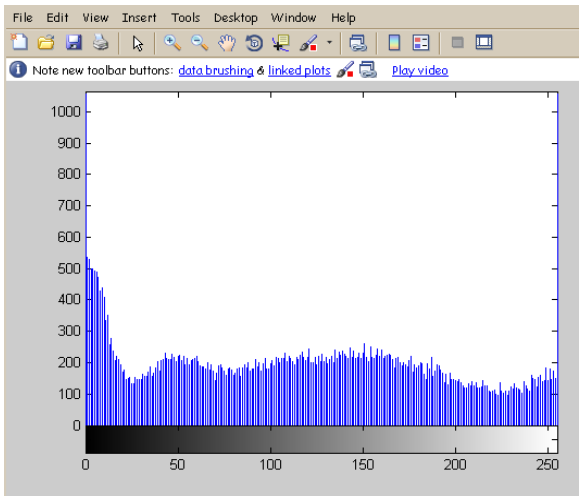

Fig 10: Encrypted Image Histogram (Green)

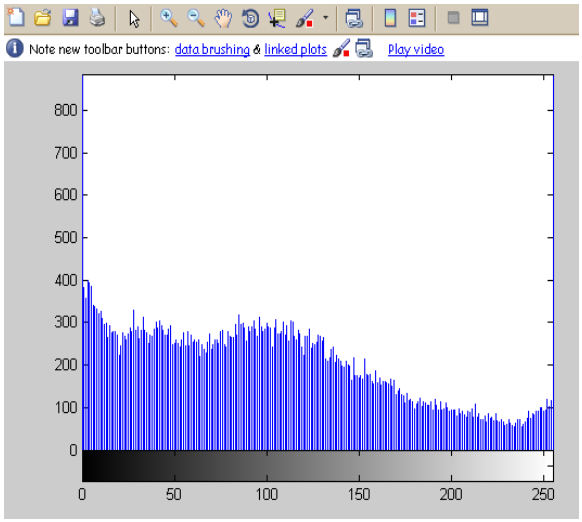

Fig 11: Encrypted Image Histogram (Blue)

3.2 Correlation Coefficient Analysis

In addition to the histogram analysis, we have also analyzed the correlation between original and encrypted image. For an ordinary image, pixels are usually highly correlated with its adjacent pixels either in horizontal, vertical or diagonal directions. These high-correlation properties can be quantified as the correlation coefficient for comparison. This correlation coefficient is computed with the help of matlab 2D correlation coefficient function which is based on following equation (3). This equation computes the correlation between original and encrypted images of same dimension.

$$r = \frac{\sum_m \sum_n \left(A_{mn} - \overline{A}\right)\left(B_{mn} - \overline{B}\right)}{\sqrt{\left(\sum_m \sum_n \left(A_{mn} - \overline{A}\right)^2\right)\left(\sum_m \sum_n \left(B_{mn} - \overline{B}\right)^2\right)}} \quad (3)$$

Where A and B are the matrices of same size

and $\overline{A}$ = mean2(A), and $\overline{B}$ = mean2(B)

The following table represents the comparison of correlation coefficient between some randomly chosen original image frame and encrypted image frame.

TABLE 1. **CORRELATION COEFFICIENT OF ORIGINAL AND ENCRYPTED IMAGE**

Frame Number	R	G	B	Average Value
MissAmerica50	0.0089	0.0085	0.0046	0.00733
MissAmerica100	0.0124	0.0099	0.0052	0.00917
MissAmerica150	0.0129	0.014	0.0045	0.01047
MissAmerica200	0.0064	0.008	0.0047	0.00637
MissAmerica250	0.0086	0.0107	0.0087	0.00933
MissAmerica300	0.0051	0.0057	0.0023	0.00437

We have calculated the correlation coefficient between original and encrypted image matrix by (3). The results obtained, which are shown in Table1. These correlation analysis prove that the proposed encryption technique satisfies tending towards zero co-correlation. The correlation coefficient near zero indicates the very little correlation among the pixels. However, the pixels in the original image were highly correlated.

3.3 PSNR Analysis

The matlab PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR value, the better the quality of the compressed or reconstructed image. 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. The lower the value of MSE, the lower will be the error. To compute the PSNR, the block first calculates the mean-squared error (MSE) using the following equation:

$$\text{MSE} = \frac{\sum_{M,N}\left[I_1(m,n) - I_2(m,n)\right]^2}{M * N} \qquad (4)$$

Where I1 and I2 are encrypted and original image matrix. M and N are the number of rows and columns in the input images. Then the block computes the PSNR using the following equation:

$$\text{PSNR}=10\ \log_{10}\left(\frac{R^2}{MSE}\right) \qquad (5)$$

Where R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, then R is 255.

The following table represents the comparison of PSNR between some randomly chosen original image frames and encrypted image frames.

TABLE 2. **PSNR VALUE OF ORIGINAL IMAGE**

Frames	**R**	**G**	**B**	**Average Value**
MissAmerica50,100	17.06	17.16	17.67	17.29667
MissAmerica100,150	14.02	13.86	15.01	14.29667
MissAmerica150,200	11.54	11.59	9.366	10.832
MissAmerica200,250	13.53	14.08	14.82	14.14333
MissAmerica250,300	12.71	12.52	13.79	13.00667

TABLE 3. **PSNR VALUE OF ENCRYPTED IMAGE**

Frames	**R**	**G**	**B**	**Average Value**
MissAmerica50,100	24.62	24.1	24.76	24.49333
MissAmerica100,150	22.36	21.94	22.72	22.34
MissAmerica150,200	21.4	21.15	21.28	21.27667
MissAmerica200,250	22.55	22.69	22.62	22.62
MissAmerica250,300	22.26	22.31	22.68	22.41667

4. CONCLUSIONS

In this paper, a feasible chaos based encryption and decryption algorithm is proposed for image and video in time domain and frequency domain. Which uses discrete cosine transform (DCT) function and Arnold's cat map. The DCT function is used for calculating discrete cosine transform in time domain which substitute the actual pixel value with the quantized pixel values. So the independency of the statistics of cipher on the statistics of the plain text increases and also compression is achieved. The Arnold's cat map introduces the diffusion or permutation. This process is the shuffling of information from one into many, to hide the statistical structure of the image data.

5. REFERENCES

[1] C.Dongming, "A feasible chaotic encryption scheme for image", International workshop on chaos-fractals theories and applications, IWCFTA-2009. IEEE2009

[2] Juan Li, Yong Feng, Xuqiang Yang, "Discrete chaotic based 3 D image encryption scheme", National natural science foundation of china, IEEE2009

[3] T.J. Chuang, J.C. Lin, "New approach to image encryption, J. Electronic Imaging", 1998, 7(2) pp..350-356.

[4] J.Fridrich. " Symmetric ciphered based on two dimensional chaotic maps", Int. J. Bifurcat Chaos, 1998, 8(6): pp. 318-325.

[5] G.Chen, Y. Mao, and C.K. Chui, " A symmetric image encryption based on 3 D chaotic maos", Chaos, Solutions and Fractals, 2004 21(3): pp.749-761.

[6] Pareek, N.K., V. Patidar, and K.K. Sud, "Image Encryption Using Chaotic Logistic Map", Image and Vision Computing, 2006 24(9): pp. 926-934.

[7] H. Cheng, X.B. Li, "Partial encryption of compressed image and videos", IEEE Trans. Signal Process. 2008 48(8): pp. 2439-2451.

[8] Chong Fu, Zhen-chuan Zhang , Ying-yu Cao. " An improved image encryption algorithm based on chaotic maps" Third International Conference on Natural Computation. 2007, Vol. 13, pp.189-193.

[9] Di Xiao, X.F. Liao. "An analysis and improvement of a chaos based image encryption algorithm". Chaos Solutionsand Fractals. 2009 vol.40, pp. 2191-2199.

[10] Z. Mingming, T. Xiaojun, " A multiple chaotic encryption scheme for image" , 6 International Conference on Wireless and Communication (WICOM) 2010. 978-1-4244-3708-5.