Compressive and Progressive Multi Key Chaotic Encryption

P. Sankaranarayanan¹, R. Tamijetchelvy²

¹Assistant Professor, Dept. of ECE
Bharathiyar College of Engg. & Technology, Karaikal, India

²Assistant Professor, Dept. of ECE
Perunthalaivar Kamarajar Inst. of Engg. & Technology, Karaikal, India

ABSTRACT
The rapid development of wireless technologies has become major solution for next generation wireless communication networks. The demand for secure communication is an important research issue. And also with the development of Internet and multimedia applications, the processing of information, storage and transmission become most important crucial factor. A combined encryption and compression process are needed to satisfy the mentioned issues. Chaotic cryptographic scheme is a new dimensional encryption algorithm for both real time and non real time communications. Chaos signals are random in behaviour, continuous in nature and sensitive dependence on initial conditions. Image Compression is the solution linked with transmission and storage of large amount of information. In this paper an optimized combined fast chaos based multikey encryption followed by DCT compression methods are proposed for grayscale images. Simulation results show that the proposed combined scheme outperforms the existing scheme in terms of considerable reduction in encryption decryption time as well as the storage and transmission capacity. The security of the proposed scheme is also analyzed by various cryptanalysis attacks.

Keywords: Monochrome, Compression, Iteration, Key-size, Pretreatment.

1. INTRODUCTION
In recent years of plethora of wireless technologies, information security becomes essential in various environments such as internet communication, multimedia applications, medical imaging field, tele-medicine and military communication. So there is a need to increasing interest in the area of cryptography, steganography, etc [1, 2]. Most of the cryptographic schemes have proposed for network security, some of them are novel and efficient methods to develop secure image encryption [3]. Image encryption schemes have been widely intentional to meet the requirement for real-time secure image transmission application over the wireless internetwork environment [4, 5]. Traditional image encryption techniques such as data encryption standard (DES), advanced encryption standard etc. has the limitation of low-level effectiveness when the image size is large enough [6]. The chaos-based image encryption scheme is a new dimensional approach and efficient way to deal with the inflexible problem. The chaos-based encryption schemes are quite popular and provide a complex cipher image, fast and highly secure [7]. Chaotic encryption scheme composed of two steps, pixel confusion and pixel diffusion. In the first stage of chaotic confusion, a permutation of the chaotic maps is used to confuse the pixel position with the primary keystream. In second stage of pixel diffusion, the values of each pixel changes one by one with the help of chaotic confusion process. One dimensional chaotic scheme has the advantages of high level competence and difficulty in nature such as Logistic map [8], which is widely used now. But their weakness includes small key space, less security is still a problem.

The Lorenz system is a classical high-dimension chaotic system and its chaotic state is unquestionable. The encrypting sequences produced by Lorenz system have three advantages. First the structure of this system is more complex than the low-dimension chaotic systems [9] and is more difficult to forecast such chaotic sequences. Secondly the real value sequences of three system variables can be used separately or put them collectively to use. Lastly the three initial conditions and three control parameters of this system complete the secret-key. A new chaotic key-based algorithm (CKBA) for image encryption was mentioned in provides that CKBA is very weak to the known-plaintext attack and its security to brute-force ciphertext only. In [10], a chaotic key-based algorithm for secured image encryption was proposed, which is a value substitution cipher. So CKBA is not secure from the robustly cryptographic perspective. Known-plaintext and chosen-plaintext attacks will be very meaningful if a same key is used to encrypt more than one plaintexts, particular in the case that larger number of [11] plaintexts are all encrypted with a same key. JPEG image compression standard use DCT is a fast transform and widely used robust method for image compression. It provides excellent energy compaction
for highly correlated images. DCT has fixed beginning images and gives superior conciliation between information packing ability and computational difficulty. Image compression is very important for efficient transmission and storage capacity of images. Command for communication of multimedia data through the telecommunications network and accessing the multimedia data through Internet is growing increasingly [12]. With the use of digital multimedia applications, requirements for storage, management, and transmission of digital images has grown explosively and occupies large memory.

The changing of the image data is completed based on the arrangement of color image blocks to edge blocks and non-edge blocks approaches, then the edge block of the image is compressed with low compression and the non edge blocks is compressed with high compression [13]. Mohamed et al. [14] proposed a hybrid image compression method in which the image is compressed using lossy compression techniques and the rest of the image is compressed using lossless compression methods. In hybrid compression of color images with larger insignificant conditions by histogram segmentation method, input color image is subjected to level of binary segmentation using histogram to detect the background items. The rest of this paper is organized as follows. Section II provides the overview of chaotic systems, Section III describes the need for image compression, Section IV describes the proposed combined encryption and compression algorithm mechanism. Section V demonstrates the simulation results and discussions of proposed techniques and finally section VI conclude the results of the proposed work and scope for future research.

2. AN OVERVIEW OF CHAOTIC SCHEMES

The chaos based image encryption has recommended a new and optimized way to deal with the difficult problem of quick and highly secure image encryption schemes. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, nonperiodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications. One-dimensional chaotic system with the advantages of high level optimized efficiency and simplicity [15], such as Logistic map, has been widely used now. But their weakness, such as small key space and weak security, is also disturbing [16, 17]. Chaos is an different field of nonlinear dynamics and has been widely analyzed in recent years.

2.1 Rossler System

Rossler motivated by the geometry of continuation in dimension three in particular, by the reinjection principle, which is based on the attribute of recreation type systems, and always present a Z-shaped time-consuming manifold in their phase space. This manifold, the suggestion is slow awaiting an edge is reached at which the trajectory jumps to the other branch of the manifold, not allowing for periodic relaxation oscillations in dimension two but also for higher types of relaxation behavior [18].

\[ \begin{align*}
\frac{dx}{dt} &= (-y - z) \\
\frac{dy}{dt} &= (x + ay) \\
\frac{dz}{dt} &= (bx - cz + xz)
\end{align*} \]  

(1)

2.2 Lorentz System

The Lorenz system of ordinary differential equations having chaotic solutions for certain parameter values and initial conditions. Lorenz chaotic systems have a classical high dimensional chaotic state is indubitable. The number of sequence made on either side varies unpredictably from one to the next sequence.

\[ \begin{align*}
\frac{dx}{dt} &= \sigma (y - x) \\
\frac{dy}{dt} &= x (p-z) - y \\
\frac{dz}{dt} &= (xy - bz)
\end{align*} \]  

(2)

2.3 Hénon System

The Hénon chaotic map is a discrete time dynamical system that exhibit chaotic behaviour. The map is a simplified model of the Poincaré section of the Lorenz model. The map depends on two important parameters a and b. For the classical values the Hénon map is chaotic. For other values of a and b the map may be chaotic, intermittent, or converge to a periodic orbit. An overview of the type of behavior of the map at different parameter values may be obtained from its orbit diagram. The Hénon map does not have a strange attractor for all values of the parameters a and b. The Hénon map is a discrete-time dynamical system. Two fundamental characteristics of chaotic systems can be illustrated very well at the Hénon system.

\[ \frac{dx}{dt} = a - (y^2 - bx) \]
The first one is the sensitive dependence on the initial conditions. This causes systems having the same values of control parameters but slightly differing initial conditions to diverge exponentially during their evolution in time. The second characteristic is called ergodicity. Ergodicity is the large set of identical systems which only differ in their initial conditions will be distributed after a sufficient long time on the attractor exactly the same way as the series of iterations of one single system.

3. NEED FOR IMAGE COMPRESSION

Concerning the image quality, the most important significant step in moving from analog to the digital is the digitization of the signals. There are two basic requirement of maintaining the image quality. Primarily the data rate of digital image and secondly the total amount of digital storage capacity required. In case of real time applications, the total amount of data capacity required is even more worrisome. The key solution to this approach provides flexible principles for dealing out large amounts of information is image data reduction or image compression. The main approach in image compression is the reduction of redundant bits in an image while preserving information. Compressing an image is considerably different than compressing raw data bits.

Generally the common purpose compression techniques can be used to compress images results in less optimization. This is because images have definite statistical properties which can be oppressed by encoders exclusively designed for them. And also some of the improved particulars in the image can be sacrificed for the sake of saving more bandwidth or storage capacity is reduced. But due to compression, the image quality will be degraded. There are two types of compression lossy and lossless compression. A loss of information perfectly avoided in lossless compression in which image data are reduced while the image information is completely preserved. The first step of lossless compression is the predictive encoding. Its effect is to change the statistics of the image pixel significantly. Statistical encoding is another important advance to lossless data reduction. Statistical encoding is mainly booming if the gray level statistics of the images has already been changed by predictive coding. Lossless compression involves with compressing image which reverse process when decompressed will be an exact reproduction of the original image. This type of lossless compression is applicable for some applications includes executables, documents etc.

Another approach is the lossy compression, in some other applications, images need not be reproduced exactly as the original one. An approximation of the original image is enough for most purposes, as long as the error between the original and the compressed image is tolerable. A lot of image compression techniques is employed DCT, DWT, SPHIT etc. Some properties of the DCT which are of particular value to image processing applications such as it exhibits excellent decorrelation properties, excellent energy compaction for highly correlated images, separability, symmetric transformation and orthogonality. The original input image is divided into blocks of size (8×8), then each block is pre processed with level shifting by 2^n−1 as shown in fig. 1. Then each block is processed separately with 2D Discrete Cosine Transform. Transform eliminates correlations its advantage of working in the frequency domain is that our visual system is less sensitive to distortion around edges, the transition associated with the edge masks our ability to perceive the noise. The transformed image is quantized with the help of quantization table. Quantizer saves a lot of bits but no longer have an exact reproduction of original image block. The AC and DC coefficients are separated and provide zigzag scanning. Finally the quantized values are encoded to produce the compressed image. The reconstructed image is obtained by reversible process as shown in fig. 2.
4. PROPOSED COMPRESSIVE AND PROGRESSIVE MULTIKEY CHAOTIC ENCRYPTION

The proposed combined encryption and compression process provides an optimized and efficient way for image security. Many chaotic based image encryption schemes have been proposed for both single key and multi key techniques. The stages mainly consist of confusion (permutation) process and diffusion process. The confusion process is obtained by permuting the pixel position, while the diffusion process is merely found in the pixel value diffusion stage. However in most of the encryption schemes, the required numbers of confusion and diffusion iterations are unnecessarily larger to achieve a high level of security. Therefore the efficiency of the encryption process is thus downgraded. The first stage of the proposed work focuses on chaotic encryption based on multikey concept. Multikey uses three important chaotic systems Lorentz, Lu and Chen in the direction X, Y and Z. The encryption stage for grayscale images is illustrated in fig. 3. The input grayscale image is confused with three chaotic systems with the 128 bit external key stream. Hence the pixel position are confused and the corresponding system equation is given in equation (4), (5) and (6). Finally the confused image is diffused with another chaotic sequence with another 128 bit external keystream.

![Figure 3 Combined Encryption and Compression stages](image)

The first chaotic sequence is Lorentz system equation and its control parameters is given below

\[
\begin{align*}
\frac{dx}{dt} &= \sigma (y - x) \\
\frac{dy}{dt} &= x (\rho - z) - y \\
\frac{dz}{dt} &= xy - \beta z
\end{align*}
\]

where the initial conditions are \(x(1) = 1.1840, y(1) = 1.3627, z(1) = 1.2519\), \(\sigma = 10, \beta = 8 = 3, \rho = 28\).

The second chaotic sequence is Chen system and its control parameters are \(x(1) = 1, y(1) = 1, z(1) = 40, a = 35, b = 3, c = 28\).

\[
\begin{align*}
\frac{dx}{dt} &= a(y - x) \\
\frac{dy}{dt} &= (c - a)x - xz + cy \\
\frac{dz}{dt} &= xy - bz
\end{align*}
\]

The third chaotic sequence is Lu system and its control parameters are \(x(1) = 1.1, y(1) = 1.1, z(1) = 40, a = 36, b = 3, c = 20\).

\[
\begin{align*}
\frac{dx}{dt} &= a(y - x) + yz \\
\frac{dy}{dt} &= -xz + cy \\
\frac{dz}{dt} &= xy - bz
\end{align*}
\]

The encrypted image provides high complex cipher image with chaotic sequence. The encrypted image is then compressed with DCT method. JPEG image compression standard use DCT is a fast transform and widely used robust method for image compression. It provides excellent energy compaction for highly correlated images. The stage in DCT compression is the block processing where the input image is divided in to blocks. Then apply 2D DCT for each block which converts time domain to frequency domain. The transformed image is then quantized with the quantization table. Run length encoding is applied for the quantized image which is then ready for transmission in wireless environment.
The second stage of the work is the reverse process, first the compressed image is decompressed by decoder, dequantizer and IDCT stages. Then the decompressed image is decrypted by multikey chaotic system. The combined techniques increase the security as well the reduced storage capacity for transmission. Here the compression process is employed after encryption process. Because in this work lossy compression technique is employed. The reconstructed image is similar to original image. If the compression process is employed before the encryption process then it is quite difficult to reconstruct the original image. But the important advantage is the greatly reduced encryption time which is more applicable for real time applications. Based on the applications the encryption and compression process can be interchanged.

5. Simulation Results and Discussion

This section provides an experimental results and analysis to show how the performance of the proposed combined encryption and compression is greatly improved using multi key concept. The proposed image encryption scheme uses Lorenz, Chen and Lu chaotic system for encryption process in X, Y and Z direction. The grayscale image is taken for encryption of size 256x256 and its corresponding histogram analysis is show in fig. 5.

![Figure 4 Combined Decryption and Decompression stages](image_url)

![Figure 5 Original Image and its Histogram analysis](image_url)

![Figure 6 Original Image after Confusion Process and its Histogram analysis](image_url)
The grayscale image is encrypted using chaotic sequence generated by Lorentz, Chen and Lu systems with external 128 bit keystream. Based on the generated chaotic sequence the pixel positions are confused. So that the statistical nature of the image is completely changed but its histogram analysis is similar to original image. Therefore confusion process only changes the nature of the image and it is highly correlated with original image as in fig. 6. Hence another stage is required to confusion process to uncorrelated with the original image. Diffusion process is carried out for highly uncorrelated image as in fig. 7.

The basic requirement of improving the image quality is the data rate of digital image and the total amount of digital storage capacity. In case of real time applications, the total amount of data storage capacity required is even more difficult. The key solution to this problem is the image data reduction or image compression. DCT lossy compression technique is employed. The diffused encrypted image of size 256x256 is divided into blocks and 2D forward DCT is applied to each block. The transformed image is then quantized, encoded and finally the compressed image is transmitted over wireless medium as depicted in fig. 8.
At the receiver side the compressed image is decompressed first and decrypted. Decompression process is exactly the reverse process of compression. Finally the decompressed image is decrypted using another chaotic sequence with another 128 bit external key. The decrypted image is not exactly as same as the original image, lossy compression is employed hence there will be an loss in the reconstructed image and this is advisable for some of the applications as in fig. 9 and fig. 10. Hence the proposed system proves to be more efficient and secure for both real time and non real applications.

The robustness of the proposed multikey chaotic encryption and compression scheme is analyzed with various security tests. Key space analysis and encryption time analysis were carried out to exhibit the reasonable security of the proposed scheme. For a high secure image encryption, the key stream should be large enough to make impossible for brute force attack. A 16 byte key is used to produce a long key stream with combined Chen, Lorentz and Lu methods for confusion and diffusion of image pixel. The long and different key distribution scheme proposes to encrypt grayscale image with multi-keys, which increase the security level. It has been stated that the encryption time is greatly affected by pixel by pixel approach and it is greatly reduced for block-by-block approach.

6. CONCLUSION AND FUTURE SCOPE
An efficient and optimized combined chaotic encryption and DCT compression for grayscale image schemes have been demonstrated. The proposed work is achieved by combining some existing chaotic cryptographic schemes with mutlikey concept and compression. From the simulation results, it is observed that the original grayscale image is compared with and without compression. The reconstructed image is exactly same as the original image for without compression. It is concluded that the proposed cryptosystem is very much suitable for real-time transmission. The future work aims towards lossless compression since for medical application exact original information is needed. A few points with recommended, a large number of iterations rounds guarantee to achieve sufficient security and thus result in disappointing encryption speed.

References


AUTHOR

P. Sankaranarayanan received the B. Tech and MBA Degree in Pondicherry University, M.Tech degree (Communication Systems) in PRIST University. Currently working as an Assistant Professor in Bharathiyar College of Engineering and Technology, Karaikal. Research interest includes Image Processing, Wireless networks and Cryptography.

R. Tamijetchelvy received the B. Tech Degree in Pondicherry Engineering College (2004) and obtained Master degree affiliated to Anna University (2007). Currently as a Part time Ph. D Research Scholar in Pondicherry Engineering College and also working as an Assistant Professor in PKIET, Karaikal. Research interest includes Image Processing, Mobility management in wireless networks and Cryptography.