A Multimedia Chaos-Based Encryption Algorithm

Brahim Boulebtateche
Mohammed Mourad Lafifi
Salah Bensaoula
A MULTI MEDIA CHAOS-BASED ENCRYPTION ALGORITHM

Brahim BOULEBTATECHI(1), Mohamed Mourad LAIFI(2), and Salah BENSAOULA(3),

Department of Electronics, Faculty of Eng. Sciences, University Badji Mokhtar of Annaba, 23000 Annaba, Algeria
(1) bbouleb@yahoo.fr, (2) radlafmou@yahoo.fr, (3) bensaoula_salah@yahoo.fr.

ABSTRACT

In digitally modern world, the fundamental issue of multimedia data security (such as digital audio signals, images, and videos) is becoming a major concern due to the rapid development of digital communications and networking technologies. Traditional encryption schemes such as DES (Data Encryption Standard) and its equivalent perform poorly for multimedia data because of the large data size and high redundancy. Chaotic systems are extremely sensitive to control parameters and initial conditions. This feature has been found very effective in the field of cryptography. In this paper, a computer based system of encryption using chaotic time series is described. The system is used for encrypting audio and image files for the purpose of providing secure data bases and/or sending sensitive multimedia data over open networks (such as Internet). It uses data sorting and circular shifting processes in 2-D direction according to some secret computer-generated sequence of chaotic ordered numbers. Several experimental results on audio and image data encryption and decryption, key sensitivity tests, and statistical analysis show that the proposed approach for multimedia cryptosystems performs efficiently and can be applied for secure real time encryption and safe transmission of confidential data.

Keywords: Multimedia Cryptosystems, Audio Data, Image Encryption, Chaos-Based Encryption.

1. INTRODUCTION

Multimedia data are becoming strongly related to our daily life and used in diverse areas such as medical, military, science, engineering, art, entertainment, and advertising. With the increasing use of digital techniques for transmitting and storing images, the fundamental issue of protecting the confidentiality, integrity as well as the authenticity of images has become a major concern. Traditional encryption schemes do not work for multimedia data because of their large size and high redundancy. Therefore new encryption schemes have been proposed for multimedia data that are composed of two basic components: permutation of the pixel values and diffusion of the pixel values (XORing with a key) with ciphertext feedback (XORing with a previous iteration of the image) [1,2,3]. These two components use pseudo random number sequences generated using a chaotic dynamic system. The two components are also performed alternately for several rounds. Such schemes have been broken using chosen-images attack where several plain-image – cipher-image pairs are known to the cryptanalyst [4,5]. This weakness in the scheme is due to a weak diffusion function, and insensitivity to changes in plain-images and key streams. One can reproduce the mask used in the diffusion effect by XORing a plain-image to a cipher-image. This mask can, then, be used to recover the plain-image from a new cipher-image.

This paper discusses an alternative chaos-based symmetric-key encryption algorithm for securing images and audio signals. We propose an encryption method for multimedia signals that do not allow masks to be of any use in the cryptanalysis. Unlike other popular encryption algorithms, this algorithm manipulates pixels rather than bits. The proposed approach consists of two main components: (1) scrambling data in a pseudo-random manner obtained through chaotic functions and (2) many horizontal/vertical cyclic shift of scrambled data to render encryption more complex to decipher.

The organization of this paper is as follows. Section 2 describes the relation between chaos theory and cryptography. In section 3, proposed encryption algorithm is described in detail; from initial set up to finalizing the cipher-data. Section 4 describes experimental work, and discusses the corresponding results. The last section concludes the paper.
2. CHAOS THEORY AND CRYPTOGRAPHY

Cryptography is the science of protecting privacy and authenticity of information under hostile conditions. Modern cryptography is now routinely employed for large scale information exchange using networking schemes. A cryptosystem is a computer program transforming information in a key-dependent and apparently unpredictable manner. The structure of an encryption session is shown in Figure 1. A cipher is another name for a cryptographic algorithm. The purpose of a cipher is to take unencrypted data, called the plaintext, and produce an encrypted version of it, called the cipher text. There are two classes of ciphers: block ciphers and stream ciphers. A stream cipher encrypts one bit of the plaintext at a time, whereas block ciphers operate on blocks of plaintext that are larger than one bit. The difference is, however, largely artificial since a stream cipher can be regarded as a block cipher with a size of one bit.

One of the fundamental principles of chaotic functions is sensitive dependence, or sensitivity to initial conditions and highly complex random-like nonlinear behaviors. Due to the deterministic yet unpredictable complex patterns generated by chaotic nonlinear dynamic system, when embedded onto a data stream, in addition to the intrinsic feature strong sensitivity to initial conditions, transfers in some way these properties to the data to be encrypted. The result is an output stream that is highly unpredictable and unreadable. For this reason, a great deal of effort has been devoted to apply chaos theory to cryptography.

For image encryption, two-dimensional (2D) or higher-dimensional chaotic maps are naturally used as the image can be considered as a 2D array of pixels. First application of discrete chaotic dynamic systems in cryptography was proposed in 1989 by Matthews [7]. In [11], CKBA (chaotic key based algorithm) is proposed in which a time series based on chaotic map is generated, and used as a key. According to this sequence, image pixels are rearranged and then XOR or XNOR is applied with the secret key. Fridrich [3] suggested that a chaos-based image encryption scheme should be composed of two processes: chaotic confusion and pixel diffusion. The former permutes the pixels of a plain image with a 2D chaotic map while the latter alternates the value (grey-level) of each pixel in a sequential manner. This architecture formed the basis of a number of chaos-based image ciphers proposed subsequently [1,3,4,9,10,11].

Most of these algorithms are prone to fail under incessant cipher attack as a result of the smallness of their key space as pointed out by Li et al. in [6], and also they demand a huge amount of computation time due to repeating process of shuffling and quantization of real valued sequence of chaotic numbers into binary representation.

3. DESCRIPTION OF THE ENCRYPTION ALGORITHM

The proposed encryption process consists of two major steps. In the first step, the algorithm takes an audio signal of length N or an image I of any size M ×N and shuffles them by sorting audio data or image pixels using one or two independent 1-D Logistic maps, respectively. (grey scale or colour images are treated in the same manner). The correlation among audio and image data is, thus, completely disturbed since such signals present strong correlation among their values. To improve further the encryption security, the second part of the algorithm apply a cyclic shift along both directions (row- and column-wise) to the output of the first step by amounts computed from the chaotic sequences.
3.1. LOGISTIC MAP

The one-dimensional Logistic map, one of the simplest nonlinear dynamic discrete systems that exhibit chaotic behaviour for a selective set of its parameter, is defined by:

\[ x_{n+1} = \mu \cdot x_n \left(1 - x_n\right) \]  \hspace{1cm} (1)

where \( x_0 \) is the initial condition, \( \mu \) the system parameter and \( n \) the number of iterations. Nonlinear analysis shows that the map is chaotic for 3.569945672 < \( \mu \) < 4.0 and \( x_{n+1} \) belong to the interval \[ 0, 1 \] for all \( n \) integer. The sequence of real numbers generated from eqn.(1) present a noise-like pattern. This sequence does not require any type of pre-processing for our algorithm. It is employed as such to embody the unencrypted data with this random-like pattern. Therefore the need for a quantization process is avoided which makes encryption faster compared to other algorithms that use binary-valued chaotic sequences.

3.2. ENCRYPTION ALGORITHM

In this section, we describe the encryption algorithm in detail. The secret keys of the algorithm are the parameter \( \mu \) of 1-D logistic map and the initial condition \( x_0 \) for audio data encryption, the pair of parameters \((\mu_x, \mu_y)\) of two independent 1-D logistic maps and the initial values \(x_0, y_0\) to generate two independent chaotic sequences of \( x \) and \( y \) values for greyscale image encryption, and finally three pairs of parameters \((\mu_x, \mu_y)\) of two independent 1-D logistic maps and the corresponding initial values \(x_0, y_0\), where each pair is used to encrypt only one component (i.e., the Red, Green and Blue components) of a colour image.

According to each type of data, the encryption steps are as follows:

1. Get the total number \( N \) of audio signal samples, or get the size \( M \times N \) of an image where \( M \) represents the total number rows and \( N \) the total number of columns of whatever image.
2. Iterate each logistic map for \((1000 + N)\) times for audio signals, or, \((1000 + M)\) times to generate \( x \)-value sequence and \((1000 + N)\) times to produce \( y \)-value sequence independently for grey scale image encryption. This process of chaotic sequence is also used for each component of an RGB colour image.
3. Sort in ascending order (descending order can be also used) the rest of generated sequences after discarding the first 1000 values and put the index position of the sorted values in vector form.
4. Obtain the cipher data by mapping position in original data to its corresponding index position in the sorted sequence. This will produce randomly scrambled data.
5. Apply a circular shift to the scrambled data by an offset of \( P_x \) steps along row direction and \( P_y \) steps along column direction. This produces the encrypted data (audio or images).

The decryption process has the same structure of the encryption. The circular shift offset values are negated and the encryption procedure is reversed.

4. EXPERIMENTAL ANALYSIS

Experimental analysis of the new algorithm presented in this paper has been done with audio signals and images as well. Fig. 2 shows the experimental results with an audio sound. Fig. 4(a) is the original sound. Fig.2 (b) is its encrypted signal with the encryption key \( K = (\mu, x_0) = (4.0, 0.1) \). As we can see, the encrypted image is noise-like and unintelligible. Fig. 2(c) is the decrypted signal by use of the decryption algorithm with the same key. It can be seen that the decrypted sound is clear and exactly the same as the original one. But if we use the wrong key, we will get an unexpected noisy sound. For example, Fig. 2(d) shows the decrypted image using the wrong key \( K = (\mu, x_0) = (3.999999, 0.0999993) \). Fig. 3(a)-(d) shows results obtained with grey-scale images of size 256×256.

Fig. 3(a) is the original ‘Cameraman’ grey-scale image. Fig. 4(b) is its encrypted image with the encryption key \( K = (\mu_x, x_0, \mu_y, y_0) = (4.0, 0.0) \). As we can see, the encrypted image is completely different from the plain image and does not provide any information for breaking the encryption. Fig. 3(c) is the decrypted image by use of the decryption algorithm with the same key. It can be seen that the decrypted image is clear and the plain image is well recovered without any distortion. But if we use the wrong key, we will get an unrecognizable image. Fig. 3(d) shows the decrypted image using the wrong key \( K = (\mu_x, x_0, \mu_y, y_0) = (4.0, 0.10001, 4.0, 0.0999991) \). Fig. 4(a)-(d) shows results obtained with RGB colour image of size 306×648.

Fig. 4(a) is the original ‘Circuit Board’ colour image. Fig. 4(b) is its encrypted image with the encryption key \( K_R = (\mu_x, x_0, \mu_y, y_0) = (4.0, 0.1, 4.0, 0.1) \) for the Red component, \( K_G = (\mu_x, x_0, \mu_y, y_0) = (3.88, 0.1, 3.97, 0.1) \) for the Green component and \( K_B = (\mu_x, x_0, \mu_y, y_0) = (3.99, 0.1, 3.78, 0.1) \) for the Blue component. As we can see, the encrypted image is noise-like and unintelligible. Fig. 3(c) is the decrypted image by use of the decryption
algorithm with the same key. We can clearly see
that the plain image is well reconstituted. But if we
use the wrong key, we will get an unrecognizable
image. Fig. 4(d) shows the decrypted image using
the wrong keys $K_R = (\mu_x, x_0, \mu_y, y_0) = (4.0,
0.10000031, 4.0, 0.0999991)$, $K_G = (\mu_x, x_0, \mu_y, y_0) =
(3.87889, 0.1000011, 3.989996, 0.099998)$ and $K_B$
$ = (\mu_x, x_0, \mu_y, y_0) = (3.98996, 0.10001, 3.77999,
0.099996)$ for the RGB components, respectively.
So it can be concluded that the chaotic encryption
algorithm is sensitive to the key, a small change of
the key will generate a completely different
decryption result and can not get the correct plain-
data ( audio or images, for instance).
To test the correlation between corresponding
pixels in plain-image on one side and ciphered
image and deciphered images on the other side, the
following formulas have used to calculate the
correlation coefficient of each pair:

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

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

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

$$\tau_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)D(y)}},$$

where $x$ and $y$ are grey-scale values of
the corresponding images.

![Fig. 2 Audio Signal Encryption and Decryption Experiment Results](image)

Fig. 2 Audio Signal Encryption and Decryption Experiment Results: (a) Plain Signal, (b) Encrypted Signal, (c) Decrypted Signal by Correct Key ($\mu=4.0$, $x_0=0.1$), (d) Decrypted Signal by Wrong Key ($\mu=3.99999$, $x_0=0.0999993$).

The correlation coefficients are shown in Table 1 and Table 2. These correlation analysis prove that
the chaotic encryption algorithm have succeeded
to de-correlate the encrypted images and, using the
right key, to reconstruct the decrypted image
exactly similar to the plain image. Yet, a small
change in the key produces a totally dissimilar
decrypted image from the original one.

<table>
<thead>
<tr>
<th>Table 1. Correlation Coefficients of Pairs of Grey Scale Images</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Grey Scale Images</strong></td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

![Fig. 3 Gray Scale Image Encryption and Decryption Experiment Result](image)

Fig. 3 Gray Scale Image Encryption and Decryption Experiment Result: (a) Plain Image, (b) Encrypted Image, (c) Decrypted Image by Right Key ($\mu=4.0$, $x_0=0.1$), (d) Decrypted Signal by Wrong Key ($\mu=3.99999$, $x_0=0.0999993$).

![Fig. 3 RGB Colour Image Encryption and Decryption Experiment Result](image)

Fig. 3 RGB Colour Image Encryption and Decryption Experiment Result: (a) Plain Image, (b) Encrypted Image, (c) Decrypted Image by Right Key, (d) Decrypted Signal by Wrong Key, See Text.
Table 2
Correlation Coefficients of Pairs of RGB Colour Images

<table>
<thead>
<tr>
<th>RGB Images</th>
<th>Encrypted Image</th>
<th>Decrypted Image with Correct Key</th>
<th>Decrypted Image with Wrong Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain Image</td>
<td>0.0038</td>
<td>1</td>
<td>-0.0014</td>
</tr>
</tbody>
</table>

5. CONCLUSION

In this paper, a multimedia data encryption algorithm based solely on index manipulation of independent 1-D logistic maps is presented. The same encrypting scheme was applied to various types of data (audio sound, grey scale and colour images) of different sizes. It operates directly on real numbers without a need for a quantization process which could cause a severe drawback for this algorithm when used for real time encryption. Experimental results show that the proposed approach is really effective and performs with higher security the encryption task. Therefore, this algorithm can be very useful for critical data transmission over unsecured open networks.

ACKNOWLEDGEMENT

This project was funded by the Laboratory of Signals and Automation (LASA) at the Badi Mokhtar University of Annaba, Algeria.

REFERENCES: