GLOBAL JOURNAL OF ENGINEERING, DESIGN & TECHNOLOGY
(Published By: Global Institute for Research & Education)
www.gifre.org

DIGITAL IMAGE ENCRYPTION USING SCRAMBLING ALGORITHM AND CHAOTIC SEQUENCE

Ms.Anusha M.S. & Mrs Madhurageetha M.S.
M.Tech, Dept of CSE, PESCE, Mandya, Assistant Professor, Dept of CSE, PESCE, Mandya

ABSTRACT

With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Because of widely using images in industrial process, it is important to protect the confidential image data from unauthorized access. In this paper chaos based image encryption algorithm utilizes the good features of chaotic sequence related to cryptographic properties, such as pseudo-random, sensitivity to initial conditions and aperiodicity. The logistic mapping is used to generate chaotic matrix which is used to scramble the location of pixels in a digital image.

Keywords- digital image; Image scrambling; chaotic sequence; logistic mapping.

1. INTRODUCTION

Security of multimedia data is receiving more and more attention due to the widespread transmission over various communication networks. It has been noticed that the traditional text encryption schemes fail to safely protect multimedia data due to some special properties of these data and some specific requirements of multimedia processing systems, such as bulky size and strong redundancy of uncompressed data. Therefore, designing good image encryption scheme has become a focal research topic since the early 1990s. Inspired by the subtle similarity between chaos and cryptography, a large number of chaos-based image encryption schemes have been proposed [1–6]. Unfortunately, many of these schemes have been found insecure, especially against known and/or chosen-plaintext attacks.

Chaos signals are considered good for practical use because they have important characteristics such as they are highly sensitive to initial conditions and system parameters, they have pseudo-random property and non-periodicity as the chaotic signals usually noise-like, etc. Consequently, the combination of chaotic theory and cryptography forms an important field of information security. The characteristics of chaotic signals make chaos system an excellent and robust cryptosystem against any statistical attacks. The chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques to meet the demand for real-time image transmission over the communication channels. Therefore, chaos based image encryption is given much attention in research of information security and a lot of image encryption algorithms based on chaotic systems have been proposed. There have been many image encryption algorithms based on chaotic maps like the Logistic map, the Standard map, the Baker map, the Cat map, the Chen map[7], etc. In order to improve the security performance of the image encryption algorithm, the concept of shuffling the positions of pixels in the plain-image and then changing the gray values of the shuffled image pixels is used. But, there are two disadvantages in the above algorithms, one is high computational complexity, the other is lower key space. This paper presents a new digital image scrambling encryption algorithm based on logistic mapping.

2. RELATED WORK

2.1 Study of Existing Encryption Algorithm:

Image Encryption using Digital signature algorithm encrypts the image and embeds the digital signature into the image prior to transmission. This encryption technique provides three layers of security. In the first step, an error control code is used which is determined in real-time, based on the size of the input image. Without the knowledge of the specific error control code, it is very difficult to obtain the original image. The dimension of the image also changes due to the added redundancy. This poses an additional difficulty to decrypt the image. Also, the digital signature is added to the encoded image in a specific manner. At the receiver end, the digital signature can be used to verify the authenticity of the transmitted image.

The algorithm which uses SCAN language has lossless image compression and encryption abilities. The distinct advantage of simultaneous lossless compression and strong encryption makes the methodology very useful in applications such as medical imaging, multimedia applications, and military applications. The drawback of the methodology is that compression-encryption takes longer time.

Image scrambling is a widely applied in digital image watermark technology. Therefore, Arnold transform is often used, but its security is not enough. We can choose different transform coefficient and times in image scrambling, it is difficult to restore the original image after the transform because the transform coefficient is not the only, which can improve the efficiency of scrambling algorithm and watermarking security

2.2 Study of Chaos theory:

Chaos theory is a field of study in mathematics, with applications in several disciplines including physics, engineering, economics, biology, and philosophy. Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions. Small differences in initial conditions (such as those due to rounding errors in numerical computation) yield widely diverging outcomes for chaotic systems, rendering long-term prediction impossible in general this happens even though these systems are deterministic, meaning that their future behavior is fully determined by their

initial conditions, with no random elements involved. In other words, the deterministic nature of these systems does not make them predictable. This behavior is known as deterministic chaos, or simply chaos.

Chaos theory is a scientific discipline that focuses on the study of nonlinear systems that are highly sensitive to initial conditions that is similar to random behavior, and continuous system. The properties of chaotic systems are : (i) Deterministic, this means that they have some determining mathematical equations ruling their behavior. (ii) Unpredictable and non-linear, this means they are sensitive to initial conditions. Even a very slight change in the starting point can lead to significant different outcomes. (iii) Appear to be random and disorderly but in actual fact they are not. Beneath the random behavior there is a sense of order and pattern. The highly unpredictable and random–look nature of chaotic output is the most attractive feature of deterministic chaotic system.

Logistic Mapping

The **logistic map** is a polynomial mapping of degree 2, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations.

Mathematically, the logistic map is written

$X_{k+1} = \mu X_k (1 - X_k)$

where:

X_k is a number between zero and one, and represents the ratio of existing population to the maximum possible population at year n, and hence x0 represents the initial ratio of population to max. population (at year 0)

· μ is a positive number, and represents a combined rate for reproduction and starvation.

This nonlinear difference equation is intended to capture two effects.

1> Reproduction where the population will increase at a rate proportional to the current population when the population size is small.

2> Starvation (density-dependent mortality) where the growth rate will decrease at a rate proportional to the value obtained by taking the theoretical "carrying capacity" of the environment less the current population

3. PROPOSED IMAGE ENCRYPTION ALGORITHM

3.1. Definition of logistic mapping:

The classical chaos system in one-dimension is a logistic mapping, which can be defined as above mentioned formula Where 0 ≤≤ μ≤≤≤4 is branch parameter and xk (0,1) Research on Chaos dynamic system show that when 3.5699456 ≤≤ μ ≤≤4, logistic mapping will be in chaos condition. That is, with the initial state x0, the state sequence { xk ; k=0,1,2,3……}generated by logistic mapping is an a periodic, nonconvergent course, which sensitively depends on the initial state.

3.2. Algorithm Description:

The encryption process for a gray image using the new digital image scrambling encryption algorithm is performed according to the following steps:

Step 1. Input a gray image and expressing it with a matrix $I_{M \times N}$, transform $I_{M \times N}$ to a sequence of numbers V . $I_{M \times N}$ is a scrambling matrix, $T_{M \times N}$ is a nature variable matrix. Set $T_{M \times N} = 0$, i = 0 , goto (Step 2);

Step 2. Select a fixed point (i0, j0) as an initial point from M × N , 1 ≤ i0, j0 ≤ M, Mi = i0, Ni = j0, save components of V to , I' (Mi Ni)and set T (Mi , Ni) =1, goto (Step 3);

Step3. i = i +1,Mi = φ (Mi − 1),

Ni = φ (Ni −1) , φ (Mi − 1), φ (Ni − 1) are chaotic sequence control functions, goto (Step 4);

Step 4. If T= 0 , goto (Step 6), else T=1 , select a variable f =1, goto (Step 5);

Step 5. If f < M ,Mi =θ (Mi), Ni = ρ (Ni), θ (Mi),ρ (Ni) are location select function, set Mi = Mi +1,

Ni = Ni , if Mi <1, then Mi = Mi +M ,if

$T_{(Mi , Ni)} = 0$, goto(Step 6);

if $T_{(Mi , Ni)} = 1$, set f = f +1; If f > M , Mi = Mi, Ni = Ni +1 , set f =1 ,

if $T_{(Mi , Ni)} = 0$, goto(Step 6), if $T_{(Mi , Ni)} = 1$, set f = f +1, goto (Step 5);

Step 6. Save the components of V to $I'_{(Mi,Ni)}$ and set $T_{(Mi , Ni)} = 1$, if i < MxN, goto(Step 3), else scrambling end, get the scrambling matrix

I' (M xN) and then an encryption image is generated. The decryption process is similar to that of the encryption process except that some steps are in a reversed order.

4. ADVANTAGES

Key space refers to the total number of different keys that can be used in an algorithm.

In proposed algorithm, the key include

μ=(3.5699456,4), *x*0=(0,1) are all real number in the interval. So the key space should be sufficiently to make brute-force attack infeasible.

5. RESULT AND CONCLUSION

We have shown image in Fig. 1. The fig.1 (a) shows the original image, Fig. 1(b)shows the encrypted image, The algorithm is simple with low computation cost and can be easily implemented in hardware. Digital design of the proposed algorithm using chaos has been developed and thus makes it suitable for real time authentication as well as secured communication.

FIG 1.a

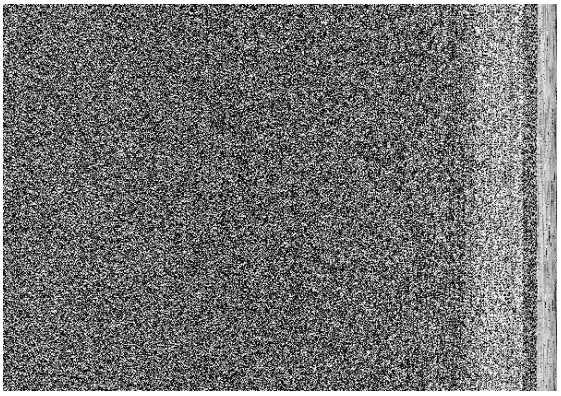

FIG 1.b

6. FUTURE WORK

In future, it can be implement for video encryption and decryption.

REFERENCES

1) J.-C. Yen, J.-I. (2000) Guo, A new chaotic key-based design for image encryption and decryption, in: Proc. IEEE Int. Conf. Circuits and Systems.
2) H.C. Chen, J.C. Yen, (2003) A new cryptography system and its VLSI realization, J. Systems Architecture
3) H.C. Chen, J.I. Guo, L.C. Huang, and J.C. Yen, (2003), Design and realization of a new signal security system for multimedia data transmission, EURASIP Journal on Applied Signal Processing.
4) G. Chen, Y. Mao and C. K. Chui, (2004) A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solutions & Fractals.
5) Musheer Ahmad et al (2009) , A New Algorithm of Encryption and Decryption of Images Using Chaotic Sequence.