A Secure Image Cipher Scheme for Real Time Applications

[#1]R.Ramya, M.E Computer Science and Engineering,Hindustan College of Engineering and Technology,Coimbatore. ramya.05cse@gmail.com

#2 Besnet George,M.E *Computer Science and Engineering,Hindustan College of Engineering and Technology,Coimbatore.* besnetg@gmail.com

Abstract—

Due to the unlimited growth of Internet and communication technologies, the extensive use of images in diverse areas such as medical, military, science, engineering, art, entertainment, advertising, education has become unavoidable. 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. This paper proposes a new encryption algorithm for providing confidentiality of images based on chaos theory. The experimental results of the proposed algorithm have been analyzed with benchmark images and are compared with various image encryption algorithms proposed in the literature.

Keywords— Image encryption, One time pads, Chaos theory, Information security, Image Confidentiality

INTRODUCTION

Many applications like military image databases, confidential video conferencing, personal online photograph albums, medical imaging system, Cable TV requires a fast and efficient way of encrypting images for storage as well as in transmission. Many encryption methods have been proposed in literature, and the most common way to protect large multimedia files is by using conventional encryption techniques. Implementations of popular public key encryption methods, such as RSA or El-Gamal cannot provide suitable encryption rates, while security of these algorithms relies on the difficulty of quickly factorizing large numbers or solving the discrete logarithm problem, topics that are seriously challenged by recent advances in number theory and distributed computing. On the other hand, private key bulk encryption algorithms

Triple DES or Blowfish [2], are more suitable for transmission of large amounts of data. However, due to the complexity of their internal structure, they are not particularly fast in terms of execution speed and cannot be concisely and clearly explained, so that to enable detection of cryptanalytic vulnerabilities. Chaotic maps present many desired cryptographic qualities such as simplicity of implementation that leads to high encryption rates, and excellent security

II. RELATED WORK

A wide variety of cryptographic algorithms for images have been proposed in the literature. Kuo et al [1] proposed an image encryption method known as image distortion which obtains the encrypted image by adding the phase spectra of the plain image with those of the key image. This method is safe but no image compression is considered. N.G. Bourbakis et al [2] have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based two-dimensional spatial- accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves. Chin – Chen Chang et al [3] have used the popular image compression technique, vector quantization to design an efficient cryptosystem. The images are first decomposed into vectors and the sequentially encoded vector by vector. Fridri [4] demonstrated the construction of a symmetric block encryption technique based on two dimensional standard chaotic map. Scharinger et al [5] designed a kolmogorov flow based image encryption technique in which the whole image is taken as a block and permuted through a key controlled chaotic system. A shift register pseudo random generator is also used to provide confusion in data. Yen and Guo [6] proposed an image encryption scheme called BRIE based on chaotic logistic map. The basic principle is bit circulation of pixels, which is controlled by a chaotic pseudo random sequence. Recently Li et al [7] have proposed a video encryption technique based on multiple digital chaotic system CVES in which pseudo random pixels are generated to make the video and perform pseudo random permutation of the compressed video. Chen et al [8] have proposed a system in which a 2D chaotic map is generalized to three dimensions which employs 3D catmap to shuffle the image pixels.

III. PROPOSED ALGORITHM

A.Chaos Functions

Chaotic functions which were first studied in the 1960's show numerous interesting properties. The iterative values generated from such functions are completely random in nature although limited between bounds. The iterative values are never seen to converge after any value of iterations. However the most fascinating aspect of these functions is their extreme sensitiveness to initial conditions. For example even if the initial start value of iterations is subjected to a disturbance as small as 10^{-100}, iterative values generated after some number of iterations are completely different from each other. It is this extreme sensitivity to the initial conditions that make chaotic functions very important for applications in cryptography. One of the simplest chaos functions that has been studied in recent times is the function

$$f(x)=p*x*(1-x)$$

which is bounded for the limits $0<p<4$. This function can be written in iterative form as

$$x(n+1)=p*x_n(1-x_n)-$$

with x_0 as the starting value. A thorough treatment and analysis of this function can be found

B. Generation Of Multiple Keys And One Time Pads

For application of the above function for generating multiple keys for symmetric cryptography, it is proposed that the values yielded by the chaos function be converted to appropriate key representations. For this, the following three factors have to be decided:

i) The starting value for the iterations (x_0),

ii)The number for decimal places of the mantissa that are to be supported by the calculating machine

iii) The number of iterations after which the first value can be picked for generating keys.

iv)The number of iterations to be maintained between two picked values thereafter.

C. Encryption Methodology

The idea used in the proposed work is called as one-time pad, in which the key has the same length as the plain text and is completely in random. A one time pad is a perfect cipher, but is almost impossible to implement commercially. If the key must be newly generated each time the sender cannot intimate the receiver about the new key every time. The proposed algorithm generates new keys to be used for every pixel encryption based on the logistic equation used and its initial condition. A modified version of one time pad where in the encryption and decryption is performed by XOR operation of pixels (usually represented by 8 bits) with the independently generated key at the sender and receiver is used.

Step1: Global Parameters

An indexed key table consisting of all possible keys for a desired key length is published. For example if a key of length 8 is required, all possibilities of the Keys are generated, tabulated and indexed. The index identifies the key to be selected at any instant of time.

TABLE 1 LOOK UP TABLE FOR ENCRYPTION KEYS

Index	**Key**
1	0 0 0 0 0 0 0 0
2	0 0 0 0 0 0 0 1
….	
256	1 1 1 1 1 1 1 1

2) Step2: Secret Parameters

Alice(Sender) and Bob(Receiver) agrees upon the chaotic equation, its initial values, The number for decimal places of the mantissa that are to be supported by the calculating machine ,the number of iterations after which the first value can be picked for generating keys and the number of iterations to be maintained between two picked values thereafter. These parameters are very short which could be sent using the public key possessed by the receiver. Any public key encryption algorithms such as RSA or Key exchange algorithms like Diffie Hellmann can be used.

3) Step 3:

Using the above mentioned secret parameters, Both the sender and receiver runs the chaotic equation

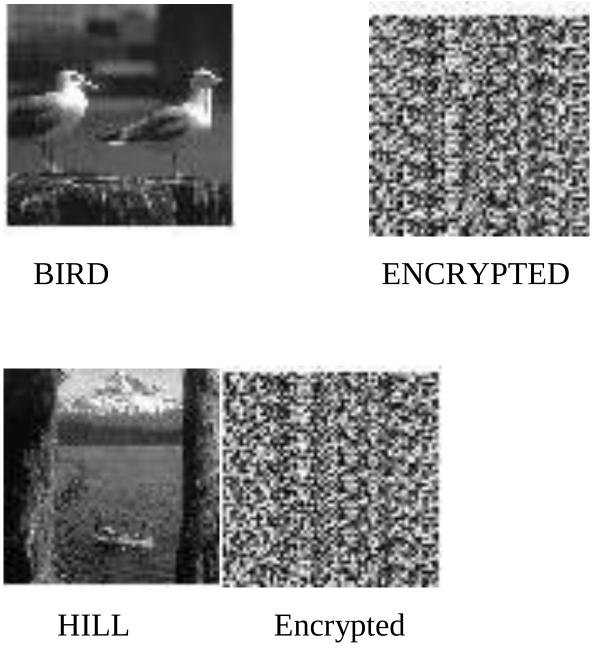
$f(x+1) = 4*x*(1-x)$.

4) Step 4:

Every pixel in the image is encrypted sequentially using the XOR scheme of bit pattern of the pixel with the key. The key is changed for every pixel encryption. The key to be used for every pixel encryption is decided by the value generated during the corresponding iteration of the chaotic equation.

IV. EXPERIMENTAL RESULTS

The proposed algorithm is implemented in MatLab 6.0 in windows environment and tested for various test images in color and grayscale format for many of the image file formats like JPEG,GIF,BMP and a few of them have been presented here. A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute force attacks



BIRD

ENCRYPTED

HILL

Encrypted

Fig 2. Original and Encrypted Image samples

A. Key Space Analysis

The strength of any cryptographic algorithm depends upon the key space which should be sufficiently large enough to make the brute force attack infeasible. The proposed algorithm utilizes almost all the keys in the key space. if an 8 bit key is used there are 2^8 possible keys and all of these keys are used in random order based on the chaos value generated depending upon the initial conditions and the skip value of iterations. If an opponent tries for brute force attack, he would have to try all combinations for all keys for every pixel which

is computationally infeasible.

B. *Statistical Analysis*

The robustness of any algorithm is proved by analysing its strength against statistical attacks. The strength of the proposed algorithm is measured by the histogram analysis of the plain and encrypted images and by the correlation coefficient between the adjacent pixels in both plain and encrypted images

c. *Execution Time*

Another important tool to evaluate the efficiency of algorithms is measuring the amount of time required to encrypt an image. In this investigation, actual time in CPU cycles will be used as a measure of execution time.

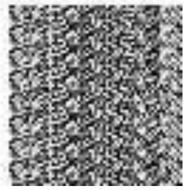
TABLE IV

COMPUTATIONAL TIME COMPLEXITY ANALYSIS

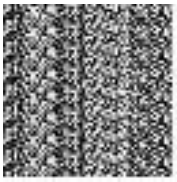
Algorithm	**Lena**	**Gold Hill**
Yen, Guo et al	0.33	0.98
Socek *et al.*	1.05	2.27
Bourbakis et al	2.54	4.77
Mitra *et al.*	1.82	2.96
Proposed	1.07	0.659

d) *Key Sensitivity Analysis*

High key sensitivity is required by secure image cryptosystems, which means that the cipher image cannot be decrypted correctly although there is only a slight difference between encryption or decryption keys. The proposed algorithm is experimented for various initial values whose difference is negligibly small. This is similar to avalanche effect in text encryption where a small bit difference in the key could produce a significant difference in the cipher text produced. An original image in Fig. 1(a) is encrypted by using various initial values such as k=0.3, 0.29995, 0.2990, 0.3005, 0.3010 and the results



0.3000



0.3010

V. CONCLUSIONS

The work proposed in this paper makes use of chaos theory in order to introduce nonlinearity in selecting the key for transposition of image pixels. Experimental Results have shown that the proposed algorithm significantly resists against statistical attacks. Also, by the principle of working the algorithm is significantly strong against brute force attack and key sensitivity tests. The time taken for encryption is relatively less in comparison with the algorithms proposed in the literature. The above mentioned features make the algorithm suitable for image encryption in real time applications.

REFERENCES

[1] C.J.Kuo, Novel image Encryption Technique and its application in progressive transmission. Journal of Electron imaging 24 1993 pp 345-351.

[2] N.J.Bourbakis , C.Alexopoulos, Picture data encryption using SCA patterns. Pattern Recognition 256 1992 pp567 -581.

[3] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, “A new encryption algorithm for image cryptosystems”, The Journal of Systems and Soft ware 58 (2001), 83-91.

[4] Fridrich Jiri, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos 8 (1998) (6), pp. 1259–1284.

[5] [5] J. Scharinger, Fast encryption of image data using Kol mogrov flow, J. Electronic Eng 7 (1998) (2), pp. 318–325.

[6] J.C Yen, J.I Guo, A new image encryption algorithm and its VLSI architecture in proceedings of IEEE workshop signal processing ystems, 1999 pp 430-437.

[7] Shujun Li, Guanrong Chen and Xuan Zheng,"Chaos-based encryption for digital images and videos," chapter 4 in Multimedia Security Handbook, February 2004.