An Image Encryption and Decryption Techniques Using Two Chaotic Schemes

Dr. Vivek Sharma, Hariom C. Agnihotri, Chetan H. Patil
Head , Deptt of CSE,, Research Scholar , Assistant Professor
VNS Institute of Technology, S.G.D.C.O.E Jalgaon
sharma.vivek95@yahoo.in, hagnihotri2011@gmail.com , chetanhpatil@gmail.com

Abstract: A chaotic system for an image encryption and decryption is the basic theme of this paper. Presentably many image encryption algorithms have been proposed, based on one chaotic system. An image encryption and decryption scheme based on two chaotic systems is being proposed. The scheme combines the spatial – domain encryption of digital images and the traditional stream cipher technology. The very wide encrypting space is the main advantage of using two chaotic systems. In addition to chaotic sequences are easy to control and easy to generate. The encryption phase makes use of two chaotic sequences to encrypt an image. The reverse operation is carried out to recover original image in decryption phase.

Keywords:Cryptography,ChaoticSequence,Chaoticsystem,Image Encryption

1. INTRODUCTION

The need of reliable method of encryption has persisted throughout history. There are numerous encryption applications range from defense and intelligences use daily commercial activities. A technology has improved to allow for easier and better encryption and transmission, so has it also allowed improvement in interception and cryptanalysis. Codes have been becomes more advanced, progressing from simple character-replacement ciphers to today's algorithm of large pseudo-primes, exponents, and modular congruence. But the concept has remained simple; it is desirable to be able to send information from one point to another without any one being able to understand it in the middle. The advent of the internet has made security of data and protection of privacy a major cause concern for anyone. The highly unpredictable and random-look nature of chaotic signals is the most attractive feature of deterministic chaotic system that may lead to novel applications. With the fast development of the computer technology and information processing technology, the problem of information security is being more and more important. Information hiding is usually used to protect the important information from disclosing when it is transmitting over an insecure channel. Digital image encryption is one of the most important methods of image information. The image encryption techniques mainly include compression methodology, cryptography mechanism, chaos techniques, and DNAtechniques and so on. Chaos and cryptography have some common features, which is discuss in subsequent section. With the advancement of mobile communication technologies, the utilization of audio-visual information in addition to textual information becomes more prevalent than the past. Cryptography approaches are therefore necessary for secured multimedia content storage and distribution over open networks such as the internet. A traditional way to resist statically and differential cryptanalysis is to employ permutation and diffusion alternatively. Recently, research on image encryption using chaos theory has been emerged. Some chaotic image encryption schemes use a multi dimensional chaotic map for pixel permutation in the spatial domain while taking another one dimensional (1D) chaotic map for key stream generation in the diffusion function. Various image encryption schemes under this architecture have been proposed.[1-11]

2. IMAGE ENCRYPTION TECHNIQUES

In this section ,few proposed techniques for Image encryption based on chaotic schemes are presented.

2.1In Spatial Domain the techniques are as follows

1. A New Mirror-Like Image Encryption Algorithm and Its VLSI Architecture
2. A New Block Image Encryption Algorithm by Fridrich
3. A New Chaotic-Like Image Encryption Algorithm and Its VLSI Architecture
4. A New Chaotic Image Encryption Algorithm by Sobhy
5. A Technique for Image Encryption using Digital Signatures
6. A Technique for Image Encryption using multi level and image dividing technique
7. A Technique for Image Encryption using 1D chaotic map
8. A Technique for Image Encryption using chaos technique
9. A Technique for Image Encryption using chaos technique.
10. A Technique for Image Encryption using chaotic neural system

2.2 For Frequency domain the encryption techniques are as follows.

1. Partial Encryption Algorithms by Cheng and Li
2. Selective Encryption Methods for Raster and JPEG Images by Droogenbroeck and Benedett
3. Selective Bitplane Encryption Algorithm by Podesser, Schmidt and Uhl

3. RELATIONSHIP BETWEEN CRYPTOSYSTEM AND CHAOTIC SYSTEMS:

The advantage of chaos lies in its random behavior and sensitivity to initial conditions and parameter.chaos-based encryption algorithm have shown some exceptionally good properties in security , complexity, speed, computing power, computational overhead etc. there exit a close relationship between traditional cryptosystemand chaotic systems in many aspects. The chaotic systems experiences many superior dynamical properties which can analogously correspond to those required in cryptosystem. the common relationship which promotes chaos theory in to practical cryptographic design is summarized in Fig 1 in particular, the notion of confusion in traditional cryptosystems causes plain image transforming to random cipher image such that there should be no repeated pattern in cipher image. by the same token, the trajectories of chaotic system pass through all points of the phase space generally with uniform distribution. In other words, it is very difficult to predict the final position of one point from its initial position. it is indeed the concept of ergodicity which can beassociated with confusion in cryptosystems.

Chaotic system	Traditional cryptosystems
ergodicity	Confusion
Sensitivity to initial condition and system parameters	Diffusion
Parameters	Encryption key
Iterations	cipher

Fig 1.comparison of some features characterized by chaotic system and cryptosystems.

to develop a good cryptosystems, another essential design principal is the property of diffusion. By doing so, a totally different cipher image is resulted no matter how one bit of key or plain image is changed.This implies that the system is sensitive to plain image and its encryption key.

On the other hand, chaotic systems highly depend on initial conditions and parameters or initial point leads to the trajectory diverged significantly. In this regard, chaotic systems and cryptosystems can naturally consideration, cryptosystems confuse and diffuse plain image by members of cipher rounds. Similarly, for chaotic system the initial region is ultimately scattered over the entire phase space via iterations. it is therefore expected that chaos theory can be exploited in the field of cryptography by taking such system parameters and initial condition as secret key s while considering the iteration of chaotic map equivalent to round of the encryption function.

4. CHAOTIC ENCRYPTION SCHEMES FOR DIGITAL IMAGES

In practice, large – scale data encryption seems to be rather difficult and slow to obtain a real data permutations and diffusion by conventional means such as DES, IDEA and AES. An example is a digital image characteristic with bulk data capacity and strong correlation among pixels. In this sense, a direct extension from document encryption to digital image may not be efficient without special modifications. Worse still, it would pose a problem if convention block cipher is applied unwisely. Because of high redundancy for the area with the same or similar color it leads to the identical repeated patterns, when a block cipher is used in the ECB mode. Hence, it is clear that image encryption has its own requirements in contrast to textual one. Alternatively, the well established chaos theory and the simplicity of discredited chaotic maps make chaos-based techniques even more suitable for image encryption than many traditional encryption schemes. the plain image can be swiftly shuffled and diffused by the application of chaotic maps usually derived from simple equations. thus, it can provide a relatively fast and secure means for real-time data transmission over high speed networks.

5. ENCRYPTION AND DECRYPTION OF IMAGE

Themain aim of this paper is to discuss an image encryption and decryption scheme based on two chaotic systems. By combining the spatial-domain encryption of digital images and traditional stream ciphers technology, the security of the encryption scheme can be enhanced effectively.

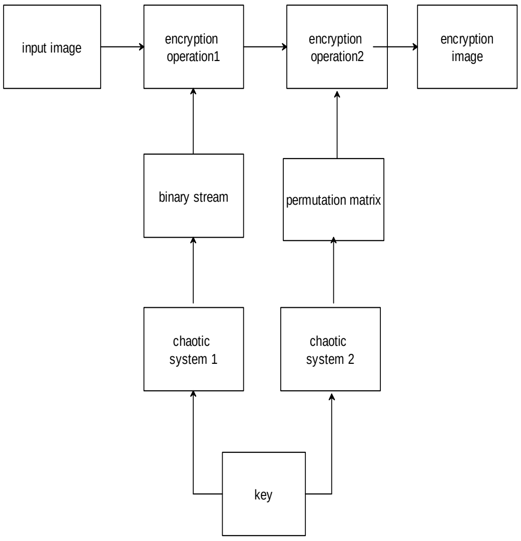

Fig. 2 Encryption Process

Fig. 2 pictorially depicts the proposed methodology of image Encryption. One of the chaotic systems is used to generate a chaotic sequence. Instead of Encryption an image in a chaotic signal directly, the proposed scheme uses two chaotic system based on thethought of higher secrecy of multi system.Then this chaotic sequence is transformed into a binary stream by a threshold function. The other chaotic system is used to construct a permutation matrix. Firstly plain n image is encrypted by using the binary stream as a key stream. Secondly, this Encrypted image is again encrypted bypermutation matrix. Decryption process works vice-versa to the Encryption process, to recover original image. The proposed technique is thoroughly analyzed and some details are discussed in coming section.

6. THE SECURITY ANALYSIS

A good Encryption scheme should resist all kind of known attacks. at present, the main attacks aimed at the chaotic Encryption systems include key space analysis, statistical analysis, known –plain-text attack, cipher-text only attack and so on. The proposed technique extracts all known security measures. Some security analyses performed on the proposed image Encryption scheme as follows. Theseanalysis show the satisfactory security of the proposed scheme.

6.1 key space analysis

In the proposed scheme, every chaotic system, even low-dimensional system, has at least a two double data as the initial value and the parameter of the system. This means the key space is at least 2^{256}. Because of more parameters and initial value, the higher dimension chaotic system will have larger key space.

7. BRUTE FORCE

The most important aspects of attacking an Encryption algorithm are the identification of the key and the computational effort required to determine it. in the proposed scheme, at least 2^{256} mathematical steps are required for brute force cryptanalysis. Sobhy [12] developed second method of chaotic Encryption algorithm. At the same timesome counter measures are introduced in this paper, such as using a multi-system algorithm consisting of different individual algorithm. in this paper, the Encryption scheme consists of two chaotic systems, and by combining the spatial-domain Encryption and the traditional stream ciphers technology, the security of the Encryption scheme is enhanced effectively.

6. CONCLUSION

In this paper we have discussed how effectively us chaos theory can be used for Digital image encryption. With larger key space and sensitive to the key, the technique can withstand against most known attacks. Hence the proposed technique can be used as effective tool for secured digital image Encryption.

References

1. Li Chang-Gang, Han Zheng-Zhi, and Zhang Haoran, “Image Encryption Techniques : A Survey”, Journal of Computer Research And Development, Vol 39, no. 10, pp 1317-1324,oct.2002
2. Wei Ding, Wei-Qi Yan, And Dong-Xu Qi, “A Novel Digital Hiding Technology Based On Tangram And Conways Game”, Processing Of 2000
3. Zhao Xue-Feng, “Digital Image Scrambling Based On The Baker’s Transformation”, Journal Of Northwest Normal University(Natural Science), Vol 39 , No. 2, pp. 26-29, Feb.2003
4. Bao Guan-Jun, Ji Shi-Ming, And ShenJian Bin, “Magic Cube Transformation And Its Application In Digital Image Encryption”, Computer Application, Vol22 ,No. 11. pp. 23-25, Nov.2002.
5. Zhu Guibin, Cao Changxiu, Hu Zhongyu, Et Al., “An Image Scrambling And Encryption Algorithm Based On Affine Transformation”, Journal Of Computer Aided Design And Computer Graphics, Vol 15 , No.6, pp. 711-715 , June .2003
6. Jui-Cheng Yen, And Jiun-In Guo, “A New Chaotic Key- Based Design For Image Encryption And Decryption”, IEEE Symposium on ISCAS 2000, Geneva, pp. IV- 49-IV-52, May. 2000.
7. M.I. Sobhy, and a.r.shehata, “chaotic algorithm for data encryption”, IEEE Proceeding of ICASSP 2001,Vol 2, pp. 997-1000, May.2001
8. MazleenaSallen, Subariah Ibrahim, and Ismail FauziIsnin, “enhanced chaotic image encryption algorithm based on vaker’s map”, IEEE Proceeding of ISCAS 2003, Vol 2 , pp. II-508-II-511 , May .2003
9. shaojiangdeng, linhuazhang, and di xiao, “image encryption scheme based on chaotic neural system”,j.wang, X.Liao, and z. yi(eds.):ISNN 2005, LNCS 3497,pp.868-872,2005.
10. Wangying, zhengdeling, ju lei, et al., “ the spatial- domain encryption of digital image based ondimension chaotic system”, proceeding of 2004 IEEE conference on cybernetics and intelligent systems, Singapore, pp. 1172-1176, December. 2004.
11. m.i. sobhy, and a.r.shehata, “methods of attacking chaotic encryption and countermeasures”, IEEE proceeding of ICASSP 2001, vol 2, pp. 1001-1004, May. 2001.
12. jianchengzou, changzhenxiong, dongxu qi, et al., “ the application of chaotic maps in image encryption”, IEEE Proceeding of on NEWCAS 2005, pp. 331-334, June. 2005.