Chaotic Image Encryption Standard (CIES)

Akhil Kaushik
Assistant Professor
CSE Department
T.I.T&S Bhiwani

Satvika
Assistant Professor
IT Department
T.I.T&S Bhiwani

Manoj Barnela
Assistant Professor
Electronics Department
T.I.T&S Bhiwani

ABSTRACT

With the fast progression of data exchange in an electronic way, information security is becoming more important in data storage and transmission. Because of widely usage of images in industrial process, it is important to protect the confidential image data from unauthorized access. Security of these images while transferring over the internet happens to be more critical, when they are confidential weapon photographs, clandestine military data, furtive architectural designs of financial buildings and top-secret war plan designs, etc. In this paper, we have proposed a new partial symmetric-key based block cipher to meet the special requirements of secure image transfer. The performance of this algorithm is discussed against common attacks such as the brute-force attack, ciphertext attacks and plaintext attacks. The analysis and experimental results show that the proposed algorithms can fully encrypt all types of images. This makes them suitable for securing multimedia applications and shows they have the potential to be used to secure communications in a variety of wired/wireless scenarios and real-time application such as mobile phone services.

Keywords— Block cipher, Cryptography, Image encryption, Chaotic Image Encryption Standard (CIES).

1. INTRODUCTION

Network technologies and media services provide ubiquitous conveniences for individuals and organizations to collect, share, or distribute images/videos in multimedia networks and wireless or mobile public channels. Image security is a major challenge in storage and transmission applications. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security against eavesdropping. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Images are different from text as they are bigger in size and the decrypted image must be equal to the encrypted image. Another significant point to consider in transfer of digital images is their special attributes like bulk data capacity, high redundancy and high correlation between neighboring pixels[1][5]. Hence an inevitable and best solution to send images can be cryptography. Cryptography can be defined as the art of creating an unintelligible form from intelligent information[10]. It is done to ensure that if any eavesdropper comes in the scenario and tries to deduce the plaintext, then he is unable to discover this confidential data. It is one of the ancient technologies employed for secure transfer of messages to a remote area. Traditional usage of cryptography dealt only with textual data and not much focus was laid on the secure transmission of images or audio/visual data. But today, the situation has changed and now it is capable for handling any type of media or data. Encryption of textual data is relevant mostly to one-dimensional data, that's why these techniques are incompetent for two-dimensional digital images. Moreover, cryptography has walked gradually from early military and political fields up to more extensive civilian areas. It has played a crucial role in human lives, like Internet banking, e-commerce, e-finance, etc[12]. The established encryption algorithms like DES, AES, etc concentrate on changing two-dimensional data into one-dimensional data and then applying encryption on it[9]. But this technique is less efficient to encrypt and decrypt images and because of this reason, it is not preferred to use this primitive style of encryption on digital images.

The secure transfer mechanisms can be broadly classified into cryptography and steganography. Steganography is the art of hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message[14]. However, cryptography still stands out as the preferred way of image transfer. Image encryption can be accomplished by scrambling image pixel positions using different techniques in the spatial domain like recursive sequence based image scrambling approach[11]. Image encryption can also be accomplished by scrambling coefficient matrices/blocks in the transform domain. Nevertheless, these approaches have extremely low security levels due to the lack of security keys or the small key space[13]. Encryption in digital images mostly works at pixel level, which is the lowest level of information in the image. But due to strong correlation between neighboring pixels, data of one pixel can be decoded easily if one of neighboring pixel becomes known. However, an image can also be interpreted as an ordered arrangement of image blocks instead of pixels. An accurate orientation of these image blocks makes us able to infer information from the image, changing of which causes visual disruption[4]. Thus using block level encryption for images will help to overcome correlation between neighboring pixels, which is the chief nuisance in image encryption. The block size should be smaller for better transformation because only fewer pixels will keep their neighbor's data [6]. Due to these added advantages of blocks over pixels, block encryption is preferred over stream cipher. However, a considerable drawback of block cipher is that it produces same ciphertext for the same plaintext if encoded with the same key. The proposed encryption technique for image encryption is a partial symmetric-key algorithm i.e. it is not fully dependent over the secret key and hence achieving better computationally security against unauthorized attacks. It actually uses two keys for encoding; one at block level and other at pixel level encryption.

2. IMPLIED ENCRYPTION ALGORITHM

The proposed image encryption algorithm is a basically a block cipher which receives blocks of images as input and encrypts them concurrently using a single secret key. It is designed

primarily for secure transfer of two-dimensional digital images over unsecure communication channel. This algorithm has a special characteristic i.e. it operates at two levels of image data: block level and pixel level to add more chaos and confusion. Another crucial attribute of this algorithm is its partial dependence on the secret key for encryption; hence it is more rigid to break. It actually uses different keys at block level and pixel level; thus breaking one key will not be enough to decode whole image. Moreover, the primary key is changed for each block to annoy the eavesdropper. As primary key keeps on varying, customary attacks like brute-force attack[2] will be unable to interpret the plain image. Working at both block level and pixel level will also protect from high redundancy of color images.

3. ENCRYPTION PROCEDURE

In this algorithm, a variety of binary operations like Shift Left operation are performed on the message for protecting it[8]. In this operation, bits are shifted left to one place and the Most Significant Bit (MSB) is placed to Least Significant Bit (LSB) as shown in the diagram below.

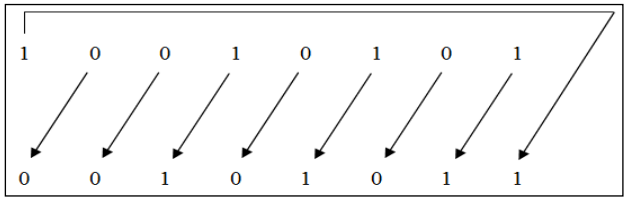

Figure 1: Binary shift-left operation

The steps of encryption process are as follow:

1) The given image is divided into number of blocks.
2) A block of pixels are selected and their red component's value out of RGB content is considered.
3) Binary shift-left operation is performed on this data random number of times.
4) A 24-bit primary key is randomly chosen from a database.
5) This primary key is applied on this Red, Green and Blue component of that block individually using a set of predefined binary operations and it is ensured that resultant data is of 24 bits.
6) The steps 2 to 5 are repeated till every block of image is encrypted.
7) After block level encryption is achieved, the next level of information i.e. each pixel is considered.
8) A random 8-bit minor key is chosen from a selected range of delimiters.
9) This 8-bit number is divided into 8 individual bits and then added in the 24-bit value of the pixel (RGB Component) at particular positions.
10) The resultant 32-bit data is converted into 24-bit data.
11) This 24-bit data is then converted back to RGB component of pixel and then a new pixel is formed, which is widely divergent from the plain image's pixel.
12) The steps 8 to 11 are repeated till every pixel of image is encoded to get the final cipher image.

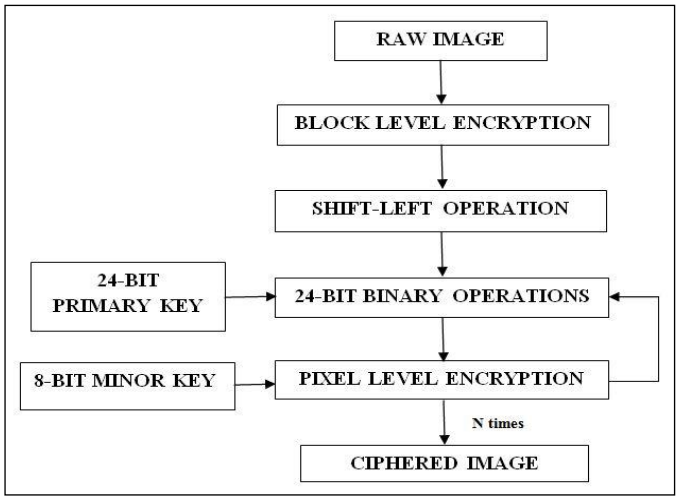

Figure 2: Encryption procedure of Proposed Algorithm

4. DECRYPTION PROCEDURE

Decryption procedure of suggested algorithm is exactly reverse of the encryption procedure, as the proposed algorithm is symmetric in nature. This symmetric nature of this algorithm keeps it simple and protects it against the man-in-the-middle attacks possible in the public key approach.

The steps of decryption are as follow:

1) The pixels of encrypted image are read from the received file and their corresponding RGB value is measured in binary form.
2) The respective minor key is read from the central database server.
3) Analogous binary operations are performed on the cipher text with help of the key.
4) Steps 2 to 3 are performed for all pixels till every pixel is reverted back to its prior condition.
5) Then the corresponding primary key is selected from the central server for first block.
6) Reverse binary operations are performed on the block's RGB component.
7) The steps 5 and 6 are repeated for every block till the end of image is reached.

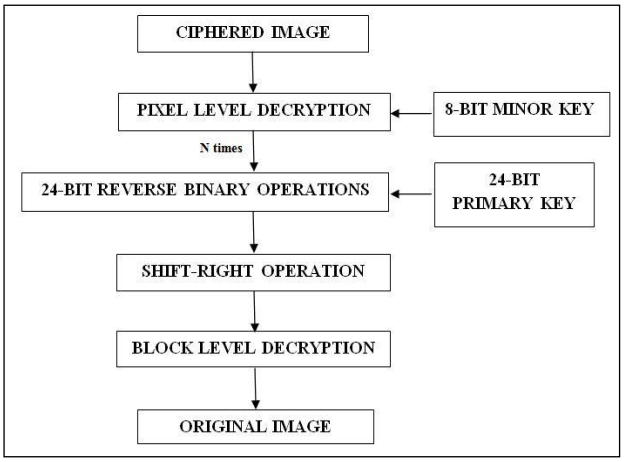

Figure 3: Decryption Procedure of Proposed Algorithm

5. SECURITY AND PERFORMANCE BENCHMARKING

Two most desired and significant features of any encryption are security and performance. The cryptosystem must strike a good balance between security and performance. The following section discusses security and performance analysis of proposed algorithm to figure out its impact.

5.1. Performance Evaluation

This algorithm is designed in such a way to achieve major aim i.e. the speed of encoding and decoding of digital image[7]. Some time-saving coding is done to achieve greater encryption speed. During the performance analysis, the following results of encryption and decryption are obtained for the proposed algorithm:-

Input Size (Pixels)	Encryption Time (sec)	Decryption Time (sec)	Total Execution Time (sec)
480 * 480	2.75	2.75	5.5
720 * 720	5.15	5.15	10.30
960 * 960	15	15	30

Table 1. Performance analysis of Proposed Algorithm

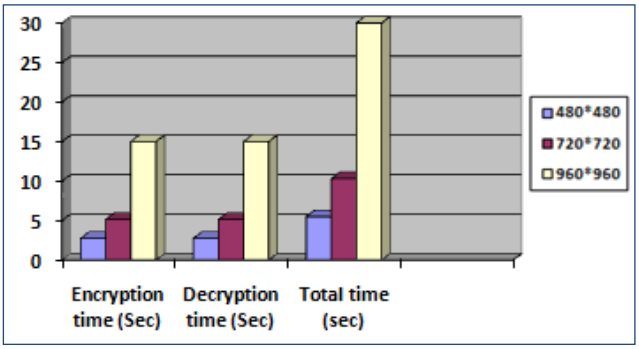

Figure 4: Input Size (pixels) vs Total Execution Time

The memory requisite of this algorithm is also lesser in comparison to other standard image cryptosystems due to small size of encryption keys. Hence it offers noteworthy performance which makes it a future solution to secure image transfer.

5.2. Security Analysis

Security is an important aspect for both, the encrypted objects and the encryption algorithms. Here some security issues of proposed algorithm are discussed from the cryptanalysis view:-

- The most promising feature of suggested algorithm is that it is not fully dependent on the secret key. A supplementary minor key is used to give an extra security features.
- Moreover, the proposed algorithm keeps changing the encryption key from a pre-decided range of delimiters; thus making it nearly impossible for a cracker to deduce the key, with help of replay attacks.
- A chief quandary in image encrypting algorithms is the strong relationship between neighbouring pixels [3]. The algorithm handles this issue pretty well and is designed to use dissimilar keys (at pixel level i.e. secondary key) to encrypt varied pixels and hence resolving the spatial challenging issue.
- Further, working at both block and pixel level of an image will also eradicate high redundancy i.e. same color of ciphered pixels that have same color in original image.
- Brute-force attacks also seem futile in breaking this cryptosystem as algorithm picks up a different key for every pixel and each block from a very vast key space.

Hence from both performance evaluation and security analysis, it can be deduced that the proposed algorithm is an optimal solution for current and future needs of secure image transfer.

6. CASE STUDY

Here is an example showing the screen shots for the plaintext, cipher text and encryption process of proposed algorithm applied on a 2D digital image data.

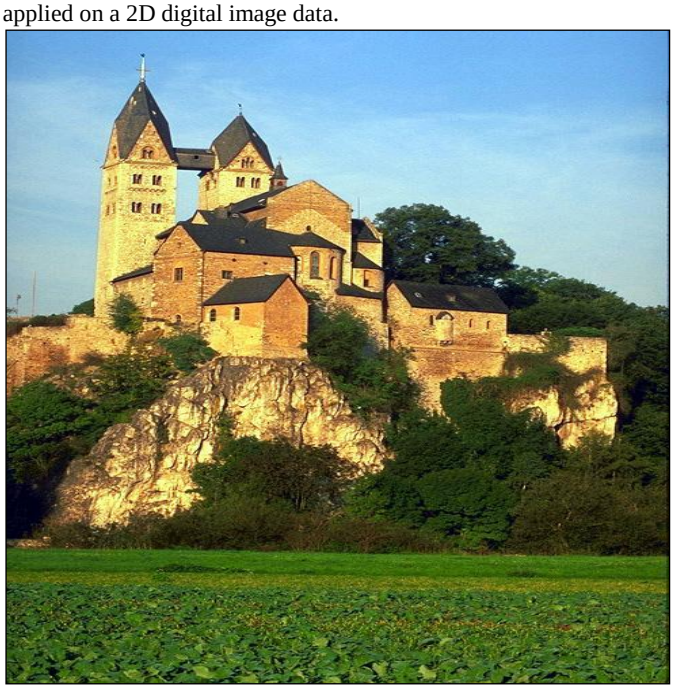

Figure 5: Plain Image for Proposed Algorithm

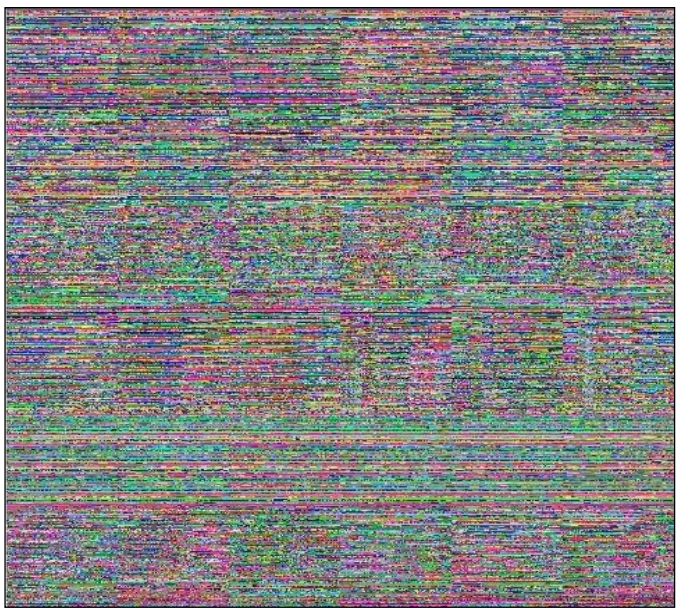

Figure 6: Cipher Image from Proposed Algorithm

7. CONCLUSION AND PROSPECT WORK

In this paper, a new approach to image encryption is discussed. This algorithm uses a partial symmetric-key technique i.e. no full-dependency on encryption key. It achieves this supplementary benefit by using an extra minor key in support to the primary key. The algorithm focuses on safety of transfer of digital images; hence, the encryption process involves two levels of encryption (block and pixel level) and thus making it tougher against unauthorized attacks. Experiments show that algorithm fully encrypts two-dimensional digital images and original images are also reconstructed without any kind of distortion. Security and Performance benchmarking show that this algorithm offers ultimate defence against illicit attacks with optimal memory requirements. Code optimization techniques are employed in this algorithm to enhance encryption and decryption speed. Finally it can be concluded that the proposed algorithm proves a competent technique for digital image encryption, and is a key for secure transfer of images.

The future work will include:

- Hardware realization of the algorithm.
- Use of scrambling technique for additional security.
- Extending algorithm for audio and video files.
- Improvement of execution time of the algorithm.
- Make it more adjustable for larger file size.
- Use of compression methodology along with encryption procedure.

8. REFERENCES

[1] Zhang S. and M. A. Karim, pp. 318-322, Vol. 21, No. 5, June 5 1999, Color image encryption using double random phase encoding, Microwave and optical technology letters.

[2] Li C. et. al., pp. 1371–1381, 2009, On the security defects of an image encryption scheme, Image and Vision Computing.

[3] Lukac R., Plantaniotis N.K., pp. 454-464, 2005, A cost-effective encryption scheme for color images, Science Direct real time imaging.

[4] Shujun L. and Zheng X., pp. 708-711, Vol. 2, 2002, Cryptanalysis of a chaotic image encryption method, Inst. of Image Process. Xi'an Jiaotong Univ. Shaanxi, IEEE International Symposium.

[5] Maniccam S.S and Bourbakis N.G., pp. 1229-1245, 2001, Lossless image compression and encryption using SCAN, Pattern Recognition.

[6] Pareek N., Patidar V. and Sud K., pp. 926–934, 2006, Image encryption using chaotic logistic map, Image and Vision Computing 24 (9).

[7] Guo J.I. and Yen J.C., 2008, A new mirror-like image encryption algorithm and its VLSI architecture, Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.

[8] Schneier B., 1994, Applied Cryptography : Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., New York, USA.

[9] Dang P.P. and Chau P.M., pp. 395~403, 2000, Image encryption for secure Internet multimedia applications, IEEE Transactions on Consumer Electronics, 46(8).

[10] Menezes A. J., Oorschot P. C. V., and Vanstone S. A., 1997, Handbook of Applied Cryptography. New York: CRC Press, Inc.

[11] Ashtiyani M., Birgani P.M. and Hosseini H.M., pp. 1-5, 2008, Chaos-based medical image encryption using symmetric cryptography, 3rd International conference on Information and Communication Technologies: From theory to applications ICTTA 2008.

[12] Stallings W., Nov 2005, Cryptography and Network Security: Principles and Practice, Prentice Hall (4th edn.), Inc., New York, USA.

[13] Cheng L. K., Dec 2003, Computer Cryptography – Data Privacy and Security in Computer Network. Tsinghua University Press (3rd edn.), Inc., Beijing China.

[14] Gary K., An Overview of Cryptography, an article available at www.garykessler.net/library/crypto.html.

9. AUTHOR'S PROFILE

Mr. Akhil Kaushik has received the Master degree in Information Technology from Central Queensland University, Melbourne, Australia. Currently he is working as an Assistant Professor in CSE Department of the Technological Institute of Textile & Sciences, Bhiwani, Haryana, India. He has his research contribution ten at International level in various proceeding like IEEE, IJCEE, ICFN, ICNIT and six at National level. His research interest includes network security, cryptography and Artificial Intelligence.

Ms. Satvika has received her Master degree in Computers Science and Enginnering from Chaudhary Devilal University Sirsa, Haryana, India. Currently she is working as an Assistant Professor in IT Department of the Technological Institute of Textile & Sciences, Bhiwani, Haryana, India. She has published many international research papers in IEEE and other reputed journals. Her research interest includes Artificial Intelligence and network security.

Mr. Manoj Barnela has received Master degree in VLSI designing and Embedded systems from Guru Jambheshwar University Hisar, Haryana, India. Currently he is working as an Assistant Professor in Electronics Department of the Technological Institute of Textile & Sciences, Bhiwani, Haryana, India. He has published three international research papers in IEEE, ICNIT, IJARCS and three at national level. His research interest includes VLSI designing, CMOS digital integrated circuits and cryptography.