ENHANCED CHAOTIC IMAGE ENCRYPTION ALGORITHM BASED ON BAKER'S MAP

Mazleena Salleh **Subariah Ibrahim** **Ismail Fauzi Isnin**

Department of Communication and Computer System
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia, Skudai 81300, Johore, Malaysia

Tel: +60-07-557-6160 x 32369, Fax: +60-07-556-5044,

{mazleena, subariah, ismail}@fsksm.utm.my

ABSTRACT

Imaging has gained importance due to the improvements of performances in computer speed, media storage and network bandwidth. Along with this advancement, the fundamental issue of image security has become a major concern and because of this reason, research in image confidentiality has gained popularity amongst security experts.

This paper discusses an alternative chaotic image encryption based on Baker's map. This enhanced symmetric-key algorithm can support a variable-size image as opposed to the algorithm which is mainly based on Baker's map that requires only square image for encryption. In addition, the algorithm also includes other functions such as password binding and pixel shifting to further strengthen the security of the cipher image. The algorithm also supports two modes of operation namely EBC and CBC. The number of iterations to be performed can vary depending on the security level required by the user. The paper also includes an example of image encryption. From the analysis done, it shows that the security level is high even though keys that are found to be weak keys for Baker's map algorithm are being used in the algorithm.

Keyword:

Confidentiality, Image Encryption, Chaos Map.

1. INTRODUCTION

Nowadays, images are normally transmitted as well as stored in electronic form. The vulnerability of this form of information to be attacked such as modification and fabrication is higher as compared to paper-based image. One of the mechanisms that can be applied to guarantee the privacy, integrity and the authenticity in image transmission and archival applications is modern cryptography. Encryption algorithms such as Triple-DES, IDEA and RC5 that are computational complex are considered secure. On the other hand, chaotic encryption that requires a simple computational procedure offers an alternative for implementing a stream or block cryptosystem.

Chaos theory is a scientific discipline that focuses on the study of nonlinear systems. A non-technical definition of a chaotic system is one in which a tiny change can have a huge effect. The properties of chaotic systems are [1]:

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 a significant different outcome.
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.

Chaos encryption has been researched since the last decade. Several papers regarding this have been published, most of which discussed about application of chaos encryption in secure communication for text-based messages as well as optical data [2 - 8].

However, for the past five years there are several chaotic image encryption algorithms that have been proposed. These algorithms manipulate the pixels by scattering them according to some chaotic function. J. C. Yen and J. I. Guo proposed two chaotic image encryption algorithms [9–11] whereby the image's pixels are rearranged based on a random binary sequence generated by a chaotic system. Fridrich [12-13] proposed another chaotic image encryption algorithm that does not require a chaotic generator. Instead the permutation of the pixel's position is based on a two-dimensional Baker's map transformation. Conversely, these algorithms have one similarity, that is, the image to be encrypted is a square.

This paper is organized as follows: In Section 2 we discuss the proposed encryption algorithm and the analysis of the cipher image produced by the algorithm. In Section 3 we describe the future work that involves the realization of the algorithm with FPGA. Finally, we summarize the research work that has been done in Section 4.

0-7803-7761-3/03/$17.00 ©2003 IEEE

2. CHAOS IMAGE ENCRYPTION BASED ON BAKER'S MAP

This research has been inspired by the previous work done by Fridrich J. who adopts invertible two-dimensional chaotic maps on a torus or a square for the purpose of encryption [12 – 13]. A chaotic image encryption system based on the concept was developed and tested on several images of different sizes. It was discovered that there exists certain key values that resulted in weak encryption [14]. Therefore this research work intends to enhance the algorithm by introducing certain functions so as to eliminate all possible weak keys as well as to increase the encryption strength. These functions include changing the grayscale value of the pixels, transposing the pixels by shifting and binding a password to the image. Table 1 shows the comparison between the algorithm proposed by Fridrich and the researcher.

Table 1. Comparison of Image Encryption Systems

	Image Encryption System By Fridrich	Enhanced Image Encryption System
Image size	Square ($n \times n$)	Variable ($m \times n$)
Gray scale substitution	Addition and Subtraction	XOR
Additional Features	None	i. Password ii. Mode of Operation: ECB and CBC

The overall enhanced chaos image encryption block diagram is depicted in Figure 1. The encryption technique combines both position permutation and value substitution to randomize the scattering and to hide the original value of the pixels.

2.1 Image Setup

f denotes an image of the size $m \times n$ where m and n represent row and column of the image. $f(x, y)$ is the gray scale value of a pixel at position x and y where $0 < x \leq m-1$ and $0 < y \leq n-1$. Before proceeding to the encryption process, the image will undergo an initial setup. Padding pixels are appended to the image so that the image can be partitioned into blocks of smaller sizes whereby every block of the image is a square of the same size, $b \times b$. The blocking and padding conditions are as follows:

If $m = n$, image can be divided into a^2 blocks of where $m = ab$.

If $m < n$, image is divided into a blocks where $a = (n + \text{padding pixels})/m$ and b = m.

If $m > n$, image is divided into a blocks where $a = (m + \text{padding pixels})/n$ and $b = n$.

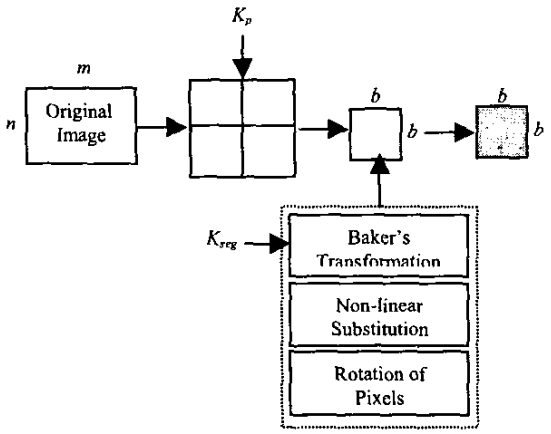

Figure 1. Block Diagram of Enhanced Chaotic Image Encryption Based on Baker's Map

2.2 Encryption Key

The algorithm requires parameters that will act as a key to the system and they are:

i. Key of 128 bits (16 characters), K_p.

ii. Size of segments in the block i.e $K_{seg} = \{s_1, s_2, \ldots, s_m\}$ where $s_1 + s_2 + \ldots + s_m = b$.

iii. Number of iterations, K_r.

The K_p acts as a salt to K_{seg} and it is calculated by hashing an input password. With the binding of the key, brute force attack will require extra computational work. The number of iterations basically determines the level of security. Obviously a higher number of iterations increases the computational time but it increases the security of the cipher image.

2.3 Encryption Process

The encryption process comprises of four main functions.

Function 1: Binding of password to image.

Each of the pixel will be XOR with the subset bits of the passwords. After every bit of the password is used, the password will be rotated to the left by one bit before reusing for the next pixel.

Function 2: Stretching and stacking.

This is the actual Baker's transformation that does the transformation as follows: (i) stretching operation transforms the unit square $[0,1]^2$ to $[0,2] \times [0, \frac{1}{2}]$, and (ii) stacking and contracting operation transforms on $[0,2] \times [0, \frac{1}{2}]$ as follows; rectangle $[0, 1] \times [0, \frac{1}{2}]$ to $[0,1] \times [0, \frac{1}{2}]$ and $[1,2] \times [0, \frac{1}{2}]$ to $[0,1] \times [\frac{1}{2},1]$ [12].

Function 3: Nonlinear feedback substitution.

This function changes the gray scale level of the pixels by performing a simple bit-wise nonlinear feedback operation, that

is $f'(x_{l+1}, y_k) = f(x_l, y_k)$ XOR $f(x_{l+1}, y_k)$. The algorithm is as follows:

FOR $k = 0$ to $b - 1$ DO
    FOR $l = 0$ to $b - 1$ DO
        $f'(x_{l+1}, y_k) = f(x_l, y_k)$ XOR $f(x_{l+1}, y_k)$;
    END
END

Function 4: Shifting pixels in the rows.

To further randomize the transposition of the pixels, the pixels in each row will be rotated to the left with 0, 1, 2, 3 or 5 shifts. The algorithm is as follows:

FOR $l = 0$ to b-1 DO
    shift_no = l mod 5;
    FOR $k = 0$ to b-1 DO
        Rotate_left row(l) for shift_no of times;
    END
END

Function 2, 3 and 4 are repeated for K_r number of rounds. For decryption process, the algorithm works in the reverse mode.

2.4 Encryption Operational Mode

There are two possible modes of encryption, Electronic Code Book (ECB) and Cipher Feedback Chaining (CBC) that is supported by the algorithm. ECB encrypts each partitioned block independently of each other. On the other hand, CBC can increase the security strength whereby all the blocks can be bonded together. To achieve this binding, the ciphered block of the previous block is XORed to the next current block.

2.5 Output Analysis

Function 1 that is the binding of the password to the image is excluded from the output analysis. This is because the research work are concerned mainly with the elimination of the possible weak keys, K_{seg}, in the system and this is done through Function 2, 3 and 4. For testing purpose, we have chosen the image of Figure 2(a) with the size of 220 × 80, the use of one of the weak keys that is K_{seg} = {8, 8, 8, 8, 8, 8, 8, 8, 8, 8} and the block size of 80 × 80. The testing is done for both operational modes ECB and CBC. The cipher image size is 240 × 80 (padded with 20 × 80 pixels of white gray scale). Figure 2(b) - 2(e) is the cipher images with a single and four iterations respectively. Comparing these images with original images from visual perception, the pixels of the cipher images are scattered and chaotic. With a higher number of iterations, pixels are more randomly scattered.

Figure 2(a). Original Image of the size 220 × 80

Fig 2(b). 1 Iteration, ECB Mode

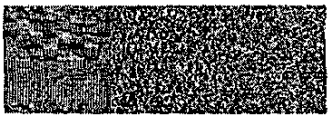

Fig 2(c). 1 Iteration, CBC Mode

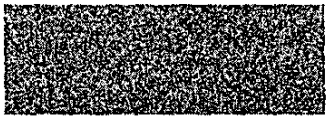

Fig 2(d). 4 Iterations, ECB Mode

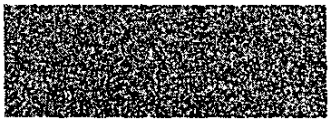

Fig 2(e). 4 Iterations, CBC Mode

Figure 2. The Cipher Analysis

Due to additional functions in the encryption algorithm, the execution time increases compares to Fridrich's algorithm. The number of iterations also affects the time performance but based on the experimental analysis, four to eight iterations is enough to randomized the pixels of the image.

3. FUTURE WORKS

3.1 Hardware Implementation

Image processing involves vast amounts of data and the cryptosystem that manages image must have the capability of a high processing rate. To support this requirement, an apposite solution would be the employment of an adaptive processor that can provide software-like flexibility with hardware-like performance. Field-Programmable Gate Arrays (FPGA) technology is a growing area of research that has the potential to provide the performance benefits of ASICs and the flexibility of processors.

The implementation of an encryption system on an FPGA is attractive because implementing a system in hardware is, by nature, more physically secure and potentially faster [15]. In addition to this fact, there are other advantages of implementing with FPGA, among which are: (i) algorithm upload whereby updating algorithm requires no change of hardware, (ii) architecture efficiency due to parameterized optimization and (iii) cost efficiency [16].

From the hardware perspective, FPGAs offer the benefits of both PLD and MPGA. The basic components of FPGA which are re-programmable matrix of logic IC, registers, RAM and routing resources can be used for: (i) performing logical and arithmetical operations, (ii) variable storage and, (iii) transferring data between different parts of the system. Furthermore, since CPU does not govern the entire chip and none sequential instructions to be processed, typically thousands of operations can be performed in parallel on an FPGA during every clock cycle [17]. Furthermore, FPGAs can be reconfigured very quickly, allowing their configuration to be altered according to the requirements of a computation.

Figure 3 depicted the overview of a proposed system implementation of the encryption algorithm. A domain-specific approach will be used in the design whereby the domain is

defined by the algorithm as well as the targeted FPGA architecture. There are two specific domains i.e the encryption modes, ECB and CBC; and based upon the request of the user, the chosen domain will be downloaded to the FPGA for reconfiguration. However there are other important requirements that need to be considered during the design which are the requirement of large I/O and high register density for data. To further increase the performance, pipelining will be also considered during the design.

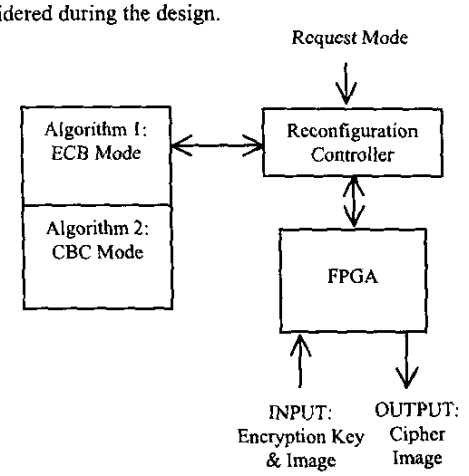

Figure 3. Proposed Overview Block Diagram

With the implementation of the system, trade-offs between speed, cost, power consumption, and security will be investigated.

4. SUMMARY

The goal of the research succeeded in improving Fridrich's work in chaotic image encryption using Baker's map. The algorithm proposed is tested by experimenting with grayscale value of the pixels and transposing of the pixels, in two different operational modes. The analysis of the resulted image in the experiment shows that the enhancement algorithm can effectively eliminate the weak keys and increase the encryption strength.

Realizing it with FPGA can significantly augmented the performance of the algorithm. This will be done in our future research whereby the feasibility, flexibility and performance of the proposed algorithm will be tested besides further enhancing the encryption algorithm example combining the input key values with Function 4 of the algorithm.

5. ACKNOWLEDGEMENT

The authors would like to acknowledge the contribution of Mohd Rozi Katmin for developing the system. This software is the result of a research supported by a seed grant from the Research Management Center of Universiti Teknologi Malaysia.

6. REFERENCES

[1] Chaos Mathematics. December 2001. Citing Internet sources URL: http://library.thinkquest.org/3120/text/math.htm

[2] Habutsu T., Nishio Y., Sasase I., and Mori S. *A Secret Key Cryptosystem by Iterating a Chaotic Map*, Proceedings of Eurocrypt '9: 127-140, 1991.

[3] Kotulski Z. and Szczepański J. *Discrete Chaotic Cryptography (DCC)*. Technical Report, Institute of Fundamental Technological Research, Polish Academy of Sciences, 1997.

[4] Fraser B., Yu P. and Lookman T. *Secure Communications Using Chaos Synchronization*. Physics in Canada, Special Issue on Nonlinear Dynamics Vol. 57(2): 155-161, 2001.

[5] Scharinger, J. *Secure And Fast Encryption Using Chaotic Kolmogorov Flows*. Technical report, Department of System Theory, Johannes Kepler University, 1998.

[6] Svensson M. and Malmquist J.E. *A Simple Secure Communications System Utilizing Chaos Functions To Control the Encryption and Decryption of Messages*. Project Report, Dept. of Physics, Lund Institute of Technology, 1996.

[7] Shore K.L. *Infrastructure for Chaotic Optical Data Encryption*, EPSRC Project GR/K78799, School of Electronic Engineering & Computer, University of Wales, Bangor, 2000.

[8] Focus Systems. *JAVA-Compatible Chaos Encryption A new Standard for IT Security*. Financial Times 2001. Citing Internet Sources URL http://www.focus-s.com/pdf/news/news010531.pdf.

[9] Yen J.C and Guo J. I., *A New Chaotic Image Encryption Algorithm*, Proc. 1998 National Symposium on Telecommunications, pp.358-362, Dec., 1998.

[10] Yen J. C. and Guo J. I. *A New Chaotic Mirror-Like Image Encryption Algorithm and Its VLSI Architecture*. Pattern Recognition and Image Analysis, Vol. 10, No. 2, pp. 236-247, 2000.

[11] Yen J. C. and Guo J. I. *Efficient Hierarchical Chaotic Image Encryption Algorithm and Its VLSI Realization*. IEE Proceeding Vis. Image Signal Process, Vol 147, No.2, April, 2000.

[12] Fridrich J. *Symmetric Ciphers Based on Two-Dimensional Chaotic Maps*, Int. J. Bifurcation and Chaos, 8(6), 1998.

[13] Fridrich J. *Image Encryption Based on Chaotic Maps*, Proc. IEEE Conf. on Systems, Man, and Cybernetics, pp. 1105-1110, 1997.

[14] Salleh, M., Ibrahim, S. Isnin, I.F. *Ciphering Key Of Chaos Image Encryption*.International Conference on Artificial Intelligent in Engineering and Technology, June 2002.

[15] Cappelletti L. *An FPGA Implementation Of A Chaotic Encryption Algorithm*, TESI DI LAUREA, Università Degli Studi Di Padova Facoltà Di Ingegneria. 2000. Citing Internet sources URL: http://www.ir3ip.net/~iw3axl/Didattica/thesis.pdf

[16] AJ Elbirt, W. Yip, B. Chetwynd, C. Paar, *Review of:An FPGA-Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists*. 3rd AES Candidate Conference, April 2000.

[17] Prasanna, V.K. and Dandalis, A. *FPGA-based Cryptography for Internet Security*,Technical Paper, MAARCII Project. Department of EE-Systems, University of Southern California. Citing Internet sources URL: http://maarcii.usc.edu/Publications/andreas_osee00.pdf