Jurnal Teknologi, 39(D) Dis. 2003: 1–12
© Universiti Teknologi Malaysia

IMAGE ENCRYPTION ALGORITHM BASED ON CHAOTIC MAPPING

MAZLEENA SALLEH[1], SUBARIAH IBRAHIM[2] & ISMAIL FAUZI ISNIN[3]

Abstract. Images are routinely used in diverse areas such as medical, military, science, engineering, art, entertainment, advertising, education as well as training. 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 discusses an alternative symmetric-key encryption algorithm for securing images, namely Secure Image Encryption (SIP) that is based on chaos. Unlike other popular encryption algorithms such as Triple-DES and IDEA, SIP manipulates pixels rather than bits. Generally, SIP comprises of three main components: (1) horizontal-vertical transformation function (HVT); (2) shift function (S), and (3) gray scale function (GS). HVT function is based on a two-dimensional chaotic map that utilized Baker's map algorithm. GS function extends the algorithm to three-dimension, whereby, the third dimension refers to the level of the gray-scale of a pixel. The algorithm supports two modes of operation namely Electronic Code Book (ECB) and Cipher Block Chaining (CBC). From the analysis done, SIP manage to encrypt images of various sizes even with the usage of weak keys that exist in Baker's map encryption algorithm.

Keywords: Confidentiality, chaos, cryptography, image encryption

Abstrak. Imej digunakan dalam pelbagai bidang seperti perubatan, ketenteraan, sains, kejuruteraan, kesenian, hiburan, pengiklanan, pendidikan dan latihan. Dengan bertambahnya penggunaan teknik digital bagi penghantaran dan penyimpanan imej, isu asas untuk melindungi kerahsiaan, keutuhan dan kesahihan imej perlu dititikberatkan. Kertas-kerja ini membincangkan algoritma alternatif penyulitan kekunci simetri, iaitu *Secure Image Encryption* (SIP), bagi melindungi keselamatan imej, Algoritma ini direka bentuk berdasarkan teknik *chaos*. SIP mengolah piksel, bukannya bit sebagaimana yang dilakukan oleh algoritma penyulitan yang popular seperti Triple-DES dan IDEA. Pada umumnya, SIP terdiri dari pada tiga komponen: (1) fungsi transformasi mendatar-menegak (HVT); (2) fungsi anjakan (S), dan (3) fungsi skala kelabu (GS). Fungsi HVT adalah berdasarkan pemetaan chaos yang digunakan dalam algoritma pemetaan Baker. Fungsi GS pula melanjutkan algoritma ini ke tiga-dimensi dengan dimensi ketiga merujuk kepada aras skala kelabu piksel. Algoritma ini menyokong dua mod operasi, iaitu *Electronic Code Book* (ECB) dan *Cipher Block Chaining* (CBC). Analisis yang dilakukan terhadap SIP menunjukkan aras keselamatan masih memuaskan walaupun kekunci yang digunakan terdiri daripada kekunci lemah jika digunakan dalam algoritma pemetaan Baker.

Kata kunci: Kerahsiaan, *chaos*, kriptografi, penyulitan imej

[1,2&3] Department of Communication and Computer System, Faculty of Computer Science and Information System, Universiti Teknologi Malaysia, Skudai 81300 Johor, Malaysia Tel: +60-07–557-6160 ext. 32369, Fax: +60-07–556-5044, {mazleena, subariah, ismail}@fsksm.utm.my

1.0 INTRODUCTION

The requirements of information security within an organization have undergone tremendous changes. Before the widespread use of data processing equipment, the security of sensitive documents depends on filing cabinets with a combination lock for storing paper-based files or documents. However the scenario has change with the introduction of computer in handling businesses in organizations. At the same time, advances in networking and communication technology bring the business organizations worldwide working together as one entity. Due to the impact of this globalization, vast amount of various digital documents such as texts, images, videos, or audio travels from one destination to another via the network line. However some of these documents might be sensitive and confidential and therefore need to be protected.

The common method of protecting the digital documents is to scramble the content so that the true message of the documents is unknown. There are various techniques to achieve this for example compression, digital watermarking, steganography and cryptography. In this paper we focuses on the security mechanism of digital image namely encryption with the usage of chaos mapping. Here we proposed an image encryption algorithm using chaos mapping and we showed that this algorithm could hide the original image through simple permutation of the pixels location as well as transformation of the gray scale value through Boolean XOR operation.

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 [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 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 that may lead to various novel applications [2].

The paper presented here is organized as follows: Section 2 reviews several techniques that can be employed in securing images that include data compression, digital watermaking, steganography and cryptography. Section 3 illustrates the research methodology and introduce the proposed image encryption algorithm, Secure Image Encryption (SIP), that is based on a two-dimensional chaotic Baker's mapping. The analysis and discussions are covered in Section 4 while Section 5 concludes the paper.

2.0 MECHANISMS IN IMAGE PROTECTION

In the past several years there has been an explosive growth in the use of computer networks, whereby digital information such as text, images and other multimedia files are transmitted frequently via the networks. Digital information that is traveling across the networks can potentially be intercepted by someone other than the intended reci pient. Due to this digital information such as medical images requires confidentiality security service. Currently there are several approaches available for protecting digital images; a traditional method of hiding data is to scramble it so that the true message is unknown. This section reviews four approaches for protecting digital images: compression, digital watermarking, steganography and cryptography.

Basically, compression is a process of encoding data to another form by removing all the redundancy that occurs in the data. This encoding technique will change the data into unreadable form as well as reducing the size of the data file. Due to this characteristic, compression is usually employed when transmitting information over the network. For text file, retrieving back the data that is the process of decompression can be done successfully without any loss of information. However, this is not the case for digital images because most conventional image compression schemes such as Cosine Transforms, Wavelets, and Fractals inevitably produce image distortion or loss of resolution after decompression. These image distortions may include: blurring; visible tile boundaries, introduced image artifacts, and jagged or blurry motion. Further increase in compression will result in worse distortions and image quality can be unacceptable [3]. In security perspective this is not tolerable because the true message and its integrity is lost. Beside this, there are several issues that need to be concerned. Firstly, compression technique employs pattern library for encoding. This means for any group to compress or decompress the information, they must have the pattern library. This raises the issue of distribution. Providing that only authorized groups have the pattern library, then only it can be said that the secrecy of the information is maintained. Another issue is that almost all compression algorithms do not integrate password or key in the process of compression or decompression. This itself will reduce the security strength of the system.

Digital watermarking or also known as digital fingerprinting is another technique that is used for digital image protection. This technique inserts pattern of bits known as signature into a digital image, audio or video file. The signature identifies the image's copyright information such as profile information, or an identification number and it is integrated within digital files as noise, or random information that already exists in the file, thereby making the detection and removal of the watermark difficult. Even though digital watermarking technique is meant for copyright protection, it can be extended for hiding digital images instead of signature.

Steganography employs the same idea as digital watermarking. Classical steganography concerns with ways of embedding a secret message in a cover or host message such as a video, audio recording, or computer code. The embedding is typically parameterized by a key; whereby without knowledge of this key it is difficult for any third party to detect or remove the embedded material [4]. Both digital watermarking and steganography techniques do not randomize the information but instead it hides the digital image under a host image. The main drawback of these two techniques is that it requires another image whereby the size of the host image must be big enough to accommodate all the bits values of the protected digital image.

Another technique for securing digital data is cryptography. Unlike stagenography, cryptography does not hide the message but instead scrambles the message through an encryption process to produce an unreadable cipher text. The cipher text needs to undergo a process called decryption in order to retrieve back the original message. Likewise as in steganography, these two processes are done based on a specific key value. Traditional symmetric key encryption algorithms such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Rivest's Code 5 (RC5) are widely used today and they are considered to be computationally secure. These algorithms have been used in commercial networks since the last two decades. DES, a 56-bit key algorithm, is the first public standard for secret key encryption. It was developed at IBM in 1976. However, today it has been common practice to protect information with triple-DES instead of DES [5]. Triple-DES algorithm is basically a DES algorithm whereby the input data is encrypted three times with two or three different keys. On the other hand International Data Encryption Algorithm (IDEA) that was developed in 1990, uses 128-bit key and it is considered as one of the most secure encryption algorithm [6]. Table 1 compares the algorithm structure between DES, Triple-DES and IDEA in terms of key size, number of iteration, number of sub

Table 1 Comparison of DES, Triple-DES and IDEA

	DES	**Triple-DES**	**IDEA**
Key size (bits)	56	112 or 168	128
No. of rounds	16	48	8
No. of sub-keys	16	48	54
Key generation	Shift Permute	Shift Permute	Shifting
Block size (bits)	64	64	64
Mathematical operations	XOR, Fixed S-Boxes	XOR, Fixed S-Boxes	XOR, Addition, Multiplication
Attack	Broken: Brute Force, 1998	No known Attack	No known Attack

keys, block size and mathematical operations. Even though Triple-DES and IDEA can achieve high security, it may not be suitable for multimedia applications due to its large data sizes and real time constraint [7].

As an alternative technique for multimedia data especially image, it has been suggested by several researchers to use chaos encryption [8 -13]. In most of the system, the encryption algorithm mani pulates the pixels of an image instead of mani pulating the bits of the image. Chaotic maps and cryptographic algorithms have some similarities: sensitivity to a change in initial conditions and parameters, random-like behavior and unstable periodic orbits with long periods. The desired diffusion and confusion properties required in a cryptography algorithm are achieved through the repeated processing. On the contrary, iterations of a chaotic map spread the initial region over the entire phase space. The parameters of the chaotic map may represent the key of the encryption algorithm. An important difference between chaos and cryptography is that encryption transformations are defined on finite sets, while chaos has meaning only on real numbers [14].

2.1 Related Works

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 as well as in optical data [15–23]. 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. Yen, and Guo [8-10] proposed two chaotic image encryption algorithms whereby the image's pixels are rearranged based on a random binary sequence generated by a chaotic system. Li *et al.,* [13] and Cai, Y. improved the chaotic encryption scheme of Alvarez *et al*., [13] because the original scheme is so vulnerable to attacks. Conversely, Fridrich [11-12] 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. The algorithms proposed by Fridrich, and Yen and Guo have one similarity that is; the image to be encrypted is a square.

3.0 RESEARCH METHODOLOGY

This research has been inspired by the work done by Fridrich [11-12]. who adopts invertible two-dimensional chaotic maps on a torus or a square for the purpose of encryption. However, earlier findings of the research work discover that there exist certain key values that resulted in weak encryption [1]. The main challenge of the research is to overcome the weak key problem, to extend the algorithm to support variable size images and to introduce electronic codebook (ECB) and cipher block chaining (CBC) mode of operations.

In this research work we proposed Secure Image Protection (SIP) algorithm that was designed based on Baker's chaotic map. The main objective of SIP was to overcome the weak key problem as well as to enhance the security strength of the algorithm. The design is discussed in Section 3.1. Several testing was done on SIP algorithm that includes the usage of weak keys, variable size images as well as the two operation modes of ECB and CBC. The output cipher images were then compared with the cipher outputs of other conventional symmetric encryption algorithms, namely DES, Triple-DES and IDEA.

3.1 Secure Image Encryption (SIP)

Generally, SIP comprises of three main components: (1) horizontal-vertical transformation function (HVT); (2) shift function (S), and (3) gray scale function (GS). HVT function is based on a two-dimensional chaotic map that utilized Baker's map algorithm. GS function extends the algorithm to three-dimension, whereby, the third dimension refers to the level of the gray-scale of a pixel. The algorithm supports two modes of operation namely Electronic Code Book (ECB) and Cipher Block Chaining (CBC). Table 2 shows the comparison between the algorithm proposed by Fridrich and the SIP.

3.1.1 System Input

The inputs to the system are the image to be encrypted and the key value. In this paper we use f to denote an image of size $m \times n$ where m and n represent row and column of the image respectively. $f(x, y)$ is the gray scale value of a pixel at position x and y

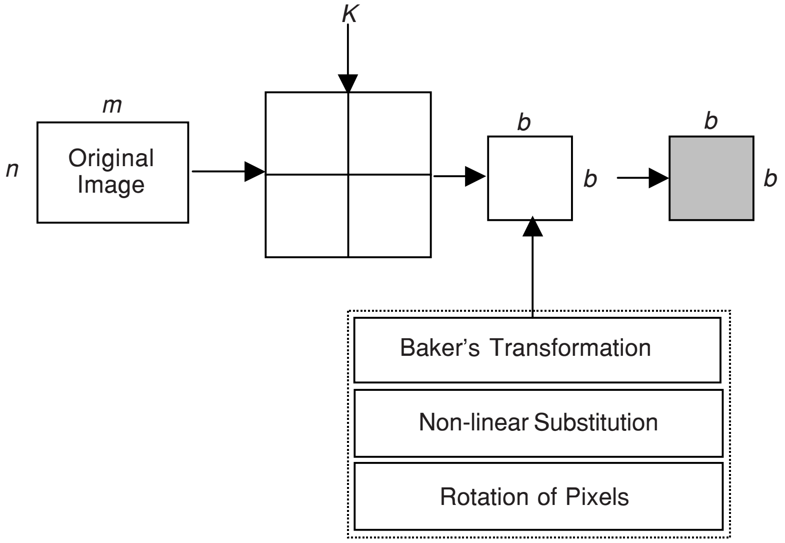


Figure 1 Block diagram SIP

Table 2 Comparison of image encryption systems

	Image encryption system by Fridrich	**Secure image encryption**
Image size	Square $(n \times n)$	Square or any rectangle sizes $(m \times n)$ where $m = n$ or $m \neq n$
Gray scale substitution	Addition and subtraction	XOR
Additional features	-	Mode of operation: ECB and CBC

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 square blocks of size, $b \times b$.

The encryption key $K(K_{seg}, K_r)$ comprises of two parameters and they are:

(i) Size of segments in the block denoted by $K_{seg} = \{s_1, s_2, \ldots, s_m\}$ where $s_1 + s_2 + \ldots + s_m = b$.

(ii) Number of iterations denoted by K_r.

The number of iterations basically determines the level of security. Obviously a higher number of iterations increase the computational time but it enhances the security of the cipher image, as this will increase the work for brute force attack. Figure 2 shows the overall SIP system.

3.1.2 Evcryption Process

The encryption process comprises of three main functions.

Function 1: Stretching and stacking.
This is the actual Baker's transformation that does the transformation as follows:

(i) the stretch operation transforms the unit square $[0,1]^2$ to $[0,2] \times [0, ½]$,

(ii) the stack operation transforms $[0, ½] \times [0,1]$ to $[0,1] \times [0, ½]$ and $[½,1] \times [0,1]$ to $[0,1] \times [½,1]$.

Function 2: 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 $f(x_{l+1}, y_k)$ for $k = 0 - (b\text{-}1)$ and $l = 0 \text{ - } (b\text{-}1)$.

Function 3: Shifting pixels in the rows.
To further randomize the transposition of the pixels, pixels in each row will be rotated to the left with 0, 1, 2, 3 or 5 shifts depending on the value of modulus (row number).

All of the above functions are repeated for K_r number of rounds. For decryption process, the same algorithm works in the reverse mode. Figure 1 depicted the SIP algorithm.

4.0 RESULTS AND DISCUSSION

DES, Triple-DES and IDEA algorithm has been tested on digital image A (100 × 100 pixels) as depicted in Figure 2 for two different operational modes, ECB and CBC. The results of these processes are as shown in Table 3 and Table 4. Here we can conclude that the cipher images resulted from all the three algorithms under ECB operation of mode display a vivid figure of the original image. This is due to the following reasons:

i. Block size of the algorithm is small, that is only 64 bits (approximately less than three pixels); and
ii. Each block is encrypted individually.

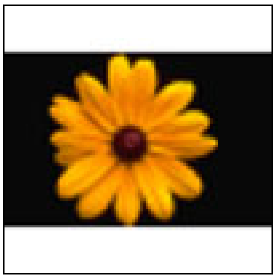


Figure 2 Original image A

Table 3 Cipher image aunder ECB Mode

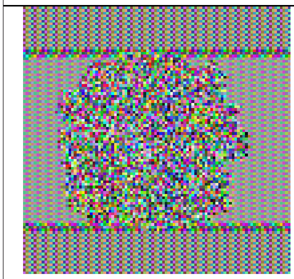
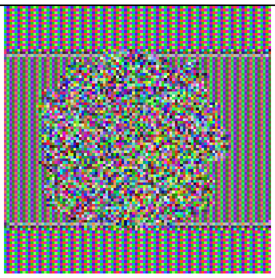
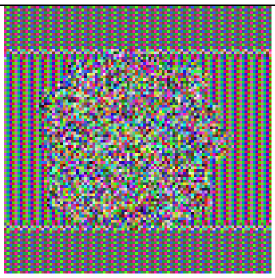
DES	Triple-DES	IDEA
		

Table 4 Cipher image a under CBC mode

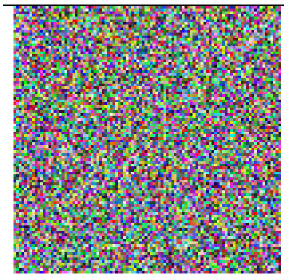
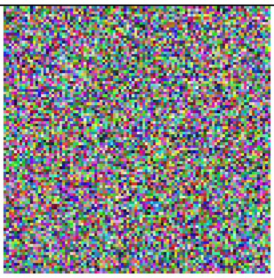
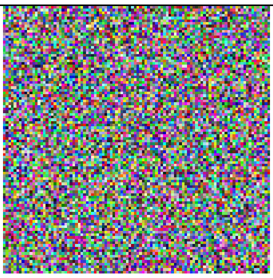
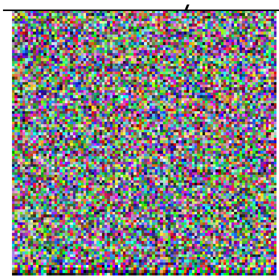
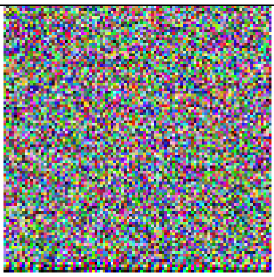
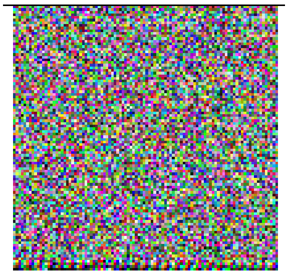
DES	Triple-DES	IDEA
		

Table 5 Cipher image a encrypted with SIP algorithm

Encryption with Weak keys	Encryption under ECB	Encryption under CBC
		

However the gray level of the image has changed due to the permutation and the substitution operations of the algorithm on the bits of the image. On the other hand, encrypting under CBC operational modes gives a better cipher. The encrypted images do not show any clue of the original image because CBC mode of operation binds the previous output data block with the current input data block. As a result, the cipher image is more chaotic and random. It should be noted here that the processing time increases due to extra calculation for binding operations.

For SIP algorithm two images were tested, image of Figure 2 and Figure 3(a). For the first image, we tested with weak key value of {(10, 10, 10, 10, 10, 10, 10, 10, 10, 10), 4} with no division of blocks and secondly with a key value of {(25,25), 4} and the size block of 50 × 50 under both mode of operations. The cipher image is as shown in Table 5. The image of Figure 3(a) is of size 220 × 80 and here we tested with a weak key of value {(8, 8, 8, 8, 8, 8, 8, 8, 8, 8), 4}. The block size of the image is set to 80 × 80 and due to this, the cipher image size will be of the size 240 × 80 (padded with 20 × 80 pixels of white gray scale). Figures in 3(b) - 3(e) are the resulted cipher images with a single and four iterations for each mode.

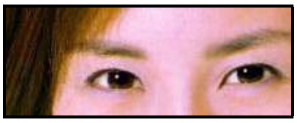


Figure 3(a) Original image of the size 220 × 80

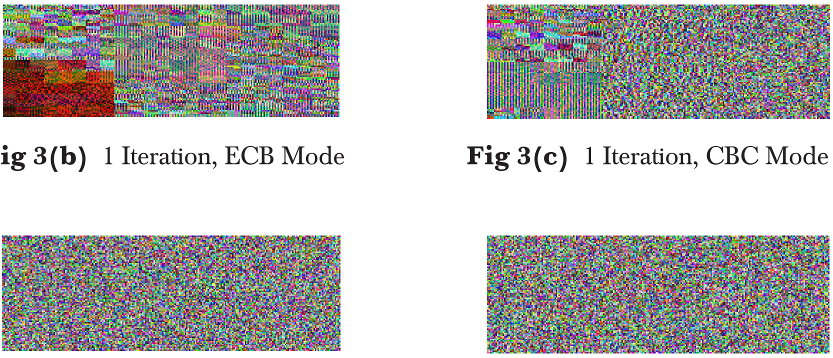


Fig 3(b) 1 Iteration, ECB Mode

Fig 3(c) 1 Iteration, CBC Mode

Fig 3(d) 4 Iterations, ECB Mode

Fig 3(e) 4 Iterations, CBC Mode

Figure 3 The cipher analysis of SIP

Comparing all the images encrypted with SIP we can conclude that we successfully deleted all possible weak keys that previously exist. In fact even under the usage of a simple key value, SIP managed to produce a good cipher image. The pixels of the cipher images are scattered and chaotic as well as changed the gray scale value of each pixel. With a higher number of iterations, pixels will be more randomly scattered.

5.0 CONCLUSION

Advances in information communication technology have contributed to the strong interest in digital storage and transmission. However, hand in hand with the full development in communication equipment nowadays, illegal data access has become easier and more prevalent in communication network. Due to this there is an increase in awareness of securing the confidentiality of data. Encryption is one of alternative techniques that can be applied to any system for safeguarding sensitive data.

SIP is implemented to protect images, making them safe from all avenues of illegal access and tampering. The main objective of SIP that is to eliminate any weak keys is successfully overcome. In addition to this, SIP has the capability to encrypt any size images, square or rectangle as well as incorporate ECB and CBC mode of operation.

This research work will be extended to include the integration of user password into the image during the encryption process. This will give a higher security level. In addition we will also complement the work with a thorough cryptanalysis of the algorithm and to compare the execution time of brute attack with other symmetric encryption algorithms.

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.

REFERENCES

[1] Salleh, M., S. Ibrahim, and I. F. Isnin. 2002. "Ciphering Key Of Chaos Image Encryption". Proceeding of International Conference on AI and Engineering Technology. UNIMAS, Sabah, Malaysia.

[2] Jakimoski, G. and L. Kocarev. 2001. "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps". *IEEE Transactions On Circuits And Systems–I: Fundamental Theory And Applications*. 48(2): 163-169.

[3] Holtz, K., 1998. "Advanced Data Compression promises the next big Leap in Network Performance". Proceedings of IS&T/SPIE EUROPTO Conference, Zurich Switzerland.

[4] Anderson, R. J., and F.A.P. Petitcolas. 1998. "On The Limits of Steganography". *IEEE Journal of Selected Areas in Communications*. 16(4): 474-481.

[5] RSA Security. http://www.rsasecurity.com/rsalabs/faq/3-2-6.html

[6] S'ergio, L. C., Salom'ao and Jo'ao M. S. de Alcantara. 2000. Improved IDEA www.cos.ufrj.br/~felipe/recentpapers/sbcci2000.pdf

[7] Chik, X. Y et al. 2001. "Fast Encryption for Multimedia". *Consumer Electronics, IEEE Transactions.* 101-107.

[8] Yen, J.C and J. I. Guo. 1998. "A New Chaotic Image Encryption Algorithm". Proceedings of National Symposium on Telecommunications. 358-362.

[9] Yen, J. C. and J. I Guo. 2000. "A New Chaotic Mirror-Like Image Encryption Algorithm and Its VLSI Architecture". *Pattern Recognition and Image Analysis*. 10(2): 236-247.

[10] Yen, J. C. and J. I. Guo. 2000. "Efficient Hierarchical Chaotic Image Encryption Algorithm and Its VLSI Realization". IEEE Proceeding Vis. Image Signal Process. 147(2).

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

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

[13] Li, S., X. Mou, and Y. Cai. 2001. "Improving Security of a Chaotic Encryption Approach". *Physics Letters A.* 290(3-4): 127-133.

[14] Jiang, Z. P. 2002. "A Note on Chaotic Secure Communication Systems". *IEEE Transactions On Circuits And Systems–I: Fundamental Theory And Applications.* Vol. 49.

[15] Habutsu, T., et al. 1991. "A Secret Key Cryptosystem by Iterating a Chaotic Map". Proceedings of Eurocrypt '9: 127-140.

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

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

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

[19] Svensson, M. and J. E. Malmquist. 1996. "*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.

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

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

[22] Sobhy, M. I. and A. R Shehata. 2001. “Chaotic Algorithms for Data Encryption”. *IEEE, 0-7803-7041-4.*

[23] Li, S. et. al. 2002. “Chaotic encryption scheme for real-time digital video”. Proc.of SPI,E Vol. 4666: 149-160, Real-Time Imaging VI, Nasser Kehtarnavaz; Ed.