International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 18 (2015) pp 39217-39222

A New Chaotic Algorithm For Image Encryption And Decryption Of Digital Color Images

M. Surya Bhupal Rao
Research Scholar, Department of Computer Science and Engineering,
St.Peter's University, Avadi, Chennai suryabhupal@gmail.com

Dr V.S. Giridhar Akula,
Professor & Principal Department of Computer Science and Engineering
Methodist College of Engg& Technology, Abids Hyderabad akulagiri2002@gmail.com

Abstract
This work proposes a new algorithm on Image Encryption and Decryption methods. Chaotic maps are used to preserve the properties of chaos and also to preserve complex non linearity. Repeated permutations are avoided but pixel values are changed by the diffusion function. By incorporating all these features, the proposed cryptosystem avoids all the crypto graphical weaknesses of earlier chaos-based encryption systems. Number of security analysis were carried out on the new algorithm and simulation results show that encryption and decryption are good and the proposed chaotic algorithm is proven to be the good procedure in terms of robustness.

Keywords: Data Hiding, Chaotic Maps, Secret Image Holder, Pixel, Visual Cryptography, diffusion function.

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. For example, video surveillance systems for homeland security purposes are used to monitor many strategic places such as public transportation, commercial and financial centers. Large amounts of videos and images with private information are generated, transmitted, or restored every day.

In addition, medical images with a patient's records may be shared among the doctors in different branches of a health service organization over networks for different clinical purposes. These images and videos may contain private information. Providing security for these images and videos becomes an important issue for individuals, business and governments as well. Moreover, applications in the automobile, medical, construction and fashion industry require designs, scanned data, and blue-prints to be protected against espionage. Considering the long lifetime of image in the afore-mentioned domains, it is imperative to develop and employ techniques which protect the content throughout their lifetime. Image encryption is an effective approach to protect images or videos by transforming them into completely different formats Several interesting approaches for image encryption have been developed. One method based on the cryptography concept considers images as data blocks or streams. It encrypts images block by block or stream by stream using different techniques. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are two examples of this approach. However, such encryption methods incur large computational costs and show poor error resilience.

Image encryption can be accomplished by scrambling image pixel positions using different techniques in the spatial domain.One example is the recursive sequence based image scrambling approach. It scrambles images using different recursive sequences such as the Fibonacci sequence, Cellular automata and chaotic maps.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. Furthermore, the permutation-only based encryption schemes are known to be vulnerable for plaintext attacks. Another approach for image encryption is to change image pixel values based on the combination of image bit plane decomposition and logic operations. The security level of this method is much lower because the results of its decomposition process and logic operations are predictable. It is not immune to plaintext attacks.

To achieve higher levels of security, one solution is to change image pixel values while scrambling the positions of image pixels or blocks using different techniques. In this paper, we introduce two new lossless image encryption algorithms using a new concept "key-image" which is a binary image with the same size as the original image to be encrypted. One algorithm, called the BitplaneCrypt, generates the key-image by extracting a binary bit plane from another new or existing image. The key image of the other algorithm, called EdgemapCrypt, is an edge map obtained from a new or existing image using a specific edge detector with a specified threshold. The algorithms decompose the original image into its binary bit planes. The bit planes are encrypted by performing an XOR operation with the key-image one by one. And then the order of all the bit planes is inverted. The resulting encrypted image can be obtained by applying a scrambling algorithm to the image from a combination of all bit planes.

In the present era of computers and fast communication, one needs to protect communicated information (message or plain text) from unauthorized user, while sending it through any electronic media. So, security of visual data is an important issue in the design of communication systems. Data hiding techniques and visual cryptography are used to introduce

confidentiality and security when visual data are transmitted through unsecured communication channels. Data hiding techniques try to embed data in digital media and transmit it in an imperceptible way.

The private-key and the public-key are the two well-known cryptosystems, using these we enable to keep the secret data securely in such a way that that invader cannot able to understand what the secret data means. The data encryption standard (DES) and Rivest, Shamir, Adleman (RSA) and Advanced Encryption Standard (AES) are three representative methods. Apart from cryptography, steganography provides another way to keep the data secure. The Steganography consists of techniques to allow the communication between two persons. It hides not only the contents but also the existence of the communication in the eyes of any observer. These techniques use a second perceptible message, with meaning disjoined by the secret message. This second message works as a "Trojan horse", and is a container of the first one. The new technologies and, in special way, the information networks require more and more sophisticated strategies in order to prevent the message privacy. In this context, digital images and audio is excellent candidate to turn into containers of the messages, since the bits of a secret text message can be superimposed, as slight noise, to the bits employed for coding a digital image.

There are two methods of performing steganography, one in spatial domain, and the other in frequency domain. Each technique has its own advantage and disadvantage. In the spatial domain, we can simply insert data into host image by changing the gray levels of some pixels in the host image, but the inserted information may be easily detected using computer analysis. In the frequency domain, we can insert data into the coefficients of a transformed image, for example using discrete Fourier transform (DFT), discrete cosine transform (DCT) and discrete Wavelet transform (DWT). But we cannot embed too much data in the frequency domain because the quality of the host image will be distorted significantly.

The mechanism is desirable in which the secret depends not on one person but on a group of people which is known as the secret sharing. The real life application of this scheme is when it's necessary in a company that the managers to share the digital documents. This concept gives a good solution for data security because all members are required to break the secret and this the main advantage of the secret sharing.

Related Work

In 1994, Naor and Shamir described a new (k, n) visual cryptographic scheme using black and white images, where the dealer encodes a secret into n participants. The secret is visible only if k or more participants stack in their shares together. The concept of arcs to construct colored visual cryptography scheme has been proposed by Verheul and Van Tilborg where colored secret images could be shared. The number of colors and number of sub pixels determined the resolution of the revealed image and thus if the number of colors was large, then coloring the sub pixels and stacking the shares precisely becomes a difficult task. In, a new visual cryptographic scheme to improve the visual effect of the shares was proposed by Hwang. This scheme was useful when the number of shares was large and could be implemented only for black and white images. Subsequently Chang, Tsai and Chen modified and extended this scheme to color images using Color Index Tables. In, Chang proposed a scheme wherein the size of the shares is fixed and independent of the number of colors appearing in the secret image. Further, the pixel expansion was only 9, which was the least amongst the previously proposed methods. But this algorithm is only applicable for (n, n) schemes.

Steganography is one of the data hiding technique in which Secret communications take place that conceal the very existence of the message. Cryptography in another type of data hiding technique in which message to be hidden is encoded using encryption or coding techniques. Here we know that a message is there but cannot understand it. Watermarking is another technique in which information that is hided is directly related to the item in which it is embedded.

On the other hand, in visual cryptography or visual secret sharing (vss), the original input image is shared between a set of participants P by a dealer (secret image holder). Based on the sharing policy, only qualified subsets of participants can recover the original input image.

Two important factor s that used to determine the efficiency of any visual cryptography scheme, namely:

1) The quality of the reconstructed image and
2) The pixel expansion (m).

Any loss of information during the reconstruction phase leads to reduction in the quality of the recovered image. On the other hand pixel expansion refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. For bandwidth constrained communication channels it is desirable to keep m as small as possible. For color images, reducing pixel expansion is of paramount importance since they occupy more space and consume more bandwidth compared to grayscale and binary images. Most of the previous works in this area try to optimize pixel expansion or obtain perfect reconstruction.

In Visual Cryptography schemes (VCS) the traditional stacking operation of sub pixels and rows interrelations is modified. This new technique does not require transparencies stacking and hence, it is more convenient to use in real applications. However, it requires the use and storage of a Color Index Table (CIT) in order to losselessly recover the secret image. CIT requires space for storage and time to lookup the table.

Also, if number of colors c increases in the secret image, CIT becomes bigger and the pixel expansion factor becomes significant which results in severe loss of resolution in the camouflage images. Ours is an advanced scheme for hiding a colored image into multiple images that does not require a CIT. This technique achieves a lossless recovery of the secret image but the generated shares (camouflage images) contain excessive noise.

Visual cryptography is a new cryptographic scheme where the cipher text is decoded by the human visual system. Hence, there is no need to any complex cryptographic computation for decryption. The idea is to hide a secret message (text, handwriting, picture, etc…) in different images called shares

or cover images. When the shares (transparencies) are stacked together in order to align the sub pixels, the secret message can be recovered. The simplest case is the 2 out of 2 scheme where the secret message is hidden in 2 shares, both needed for a successful decryption. This can be further extended to the k out of n scheme where a secret message is encrypted into n shares but only k shares are needed for decryption where k≤ n. If k-1 shares are presented, this will give no information about the secret message. The inconvenience with the previous schemes was that they used meaningless shares to hide the secret and the quality of the recovered plain text is bad. More advanced schemes based on visual cryptography where a colored image is hidden into multiple meaningful cover images is a new colored secret sharing and hiding scheme.

Cryptography (from Greek krypto's, "hidden", and gr'aphein, "to write") is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge the art of encryption. In the past, cryptography helped ensure secrecy in important communications, such as those of spies, military leaders, and diplomats. In recent decades, the field of cryptography has expanded its remit in two ways. Firstly, it provides mechanisms for more than just keeping secrets: schemes like digital signatures and digital cash, for example. Secondly, cryptography has come to be in widespread use by many civilians who do not have extraordinary needs for secrecy, although typically it is transparently built into the infrastructure for computing and telecommunications, and users are not aware of it.

Cryptography has had a long and colorful history. Generally speaking the earliest forms of secret writing required only pen and paper, and are now collectively termed classical cryptography. The two main categories are transposition ciphers, which rearrange the order of letters in a message, and substitution ciphers, which systematically replace groups of letters with others. Classical ciphers tend to leak varying amounts of information about the statistics of the plaintext, and because of this they are easily broken, for example by frequency analysis. Classical ciphers still enjoy popularity today, though mostly as puzzles.

Various devices and aids have been used for encryption. Early in the 20th century, several mechanical devices were invented for performing encryption, including rotor machines - most famously the Enigma cipher used in World War II. The ciphers implemented by these machines brought about a significant increase in the complexity of cryptanalysis. The various attacks on Enigma, for example, succeeded only after considerable effort. Occasionally, these devices have featured in films, such as in the James Bond adventure From Russia with Love.

With the advent of digital computers and electronics, very complex ciphers could be implemented. A characteristic of computer ciphers is that they operate on binary strings unlike classical and mechanical schemes, which use an alphabet of around 26 letters, depending on the language. Computer ciphers are also much more resistant to cryptanalysis; few are susceptible to a cipher text-only attack.

Extensive academic research into modern cryptography is relatively begun in the open community during the 1970s with the specification of DES and the invention of RSA. It is well that much progress has been made in a short time; popular applications such as the Internet and mobile phones have repositioned cryptography, historically the sole province of a few groups with exceptional needs for secrecy, into a mainstream technology on which millions rely.

As well as noting lessons from its history, cryptographers are also careful to consider the future. Moore's law is routinely taken into account when specifying key-lengths and the potential effects of quantum computing have already been considered. Note also quantum cryptography.

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers).

The first visual cryptographic technique was pioneered by Moni Naor and Ad Shamir in1994. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Practically this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares revealed no information about the original image.

Visual Cryptography is a graphical form of information concealing. It can be seen as a cryptographic primitive, since it offers methods and technologies for building more complex information security systems.

The techniques of visual cryptography are inspired from the general secret sharing schemes as presented by Adi Shamir and G.R. Blakley. The main difference between the visual and the general secret sharing schemes is that for the first ones the secret will be visually reconstructed in the decryption phase.

In its simplest scenario, a visual cryptography scheme involves a dealer and two participants to the scheme. The dealer chooses a secret message that can be written text, a picture, a scheme, a spreadsheet calculation etc. and splits it in two "shadow images" called shares. Every participant to the scheme will receive a separate share printed onto a transparency. In the decryption process, the participants only have to carefully superimpose their shares and the secret will be visually revealed. Such a scheme will be called a two–out–of–two visual cryptography scheme.

Novelty contributions are provided in implementing general k–out–of–n visual cryptography schemes. In such schemes the secret information can be reconstructed if and only if a minimum of k participants in a set of n participants will superimpose the shares they own. An adversary analyzing less then k shares can obtain no information (from the theory of information point of view) considering the secret message, no matter her computing power and analysis method used. Hierarchical visual cryptography schemes based on access structures and graph theory are also considered. In this type of visual cryptography schemes, some definite sets of qualified participants from a general set P of participants can be chosen. The qualified subsets are the only ones that can reconstruct the secret information.

On special interest are the extended visual cryptography schemes for "natural images" – continuous tone gay images.

In a two–out–of–two extended visual cryptography scheme, the two shares the secret image is split into are "innocent" images hiding the very intention of sending a secret message.
Further contributions are made considering the applications of visual cryptography in e-commerce, especially for scenarios that involve the presence of a corrupt Post of Sale (POS).
Being one-time-pad method, visual cryptography is information-theoretically secure. That means, its security derives purely from the information theory. This aspect makes visual cryptography interesting since the security of the most actual cryptographic primitives is based on the difficulty of solving hard mathematical problems.
Steganography is the art and science of hiding the fact that communication is taking place. Using steganography, you can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message.
Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an"invisible" message will not do so. Both sciences can be combined to produce better protection of the message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.
The chaos-based image cryptosystem mainly consists of two stages [2]. The plain image is given at its input. There are two stages in the chaos- based image cryptosystem. The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable. The pixel permutation is carried out by a chaotic system [1,2]. The chaotic behavior is controlled by the initial conditions and control parameters which are derived from the 16-character key. To improve the security, the second stage of the encryption process aims at changing the value of each pixel in the whole image an important tool to protect image from attackers. The basic idea of encryption[5,6] is to modify the message in In the diffusion stage, the pixel values are modified sequentially by the sequence generated from one of the three chaotic systems selected by external key. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The randomness property inherent in chaotic maps makes it more suitable for image encryption.

Proposed System

1. First input original image s taken and then to get the cipher image we used chaotic algorithm in which should pixels positions are change for high security
2. In the decryption we use reverse process of the encryption means input is cipher image and result image is plain image

The EdgemapCrypt algorithm:

The edge map is frequently used in image enhancement, compression, segmentation and recognition. The application of edge maps can also be extended to image encryption. In this section, we introduce a new image encryption algorithm using an edge map which is called the EdgemapCrypt algorithm. An edge map is considered as the key-image in this algorithm. Such edge map is generated from another different image with the same size as the original image using a specific edge detector with a selected threshold value.
The EdgemapCrypt algorithm first decomposes the original image into its binary bit planes. Each of them is encrypted by performing an XOR operation with the key-image, which is an edge map created from another image. Next, the algorithm inverts the order of all XORed bit planes and combines them together. The resulting image is scrambled by using a selected scrambling algorithm to generate the final resulting encrypted image. The EdgemapCrypt algorithm is illustrated in Fig. 1. Similar to the BitplaneCrypt algorithm, a 3D image can be encrypted by applying the EdgemapCrypt algorithm to all its 2D components individually. Any new or existing image with the same size of the original image can be used to generate the edge map, the keyimage.
It could be an image in the public online database or a new image generate by the users. The edge map can be obtained by using any existing edge detector such as Canny, Sobel, Prewitt, or any other edge detector. The users have flexibility to choose any existing image or any existing edge detector or any threshold value to generate the edge map used as a key-image. They also have flexibility to use any existing image scrambling method for the EdgemapCrypt algorithm. Therefore, the security keys for this algorithm consist of the image or its location which is used to generate the edge map, the type of the edge detector, the edge detector's threshold, and the security keys of the scrambling algorithm. To reconstruct the original image, the users should be provided the security keys which help them to obtain the correct edge map. The decryption process first generates the edge map from the selected image using the security keys. It then unscrambles the encrypted image using the selected scrambling algorithm. Next, it decomposes the unscrambled image into its binary bit planes and performs XOR operation between the edge map and each bit plane. The order of all bit planes is restored to the original order. The reconstructed 2D image/component can be obtained by combining all bit planes.

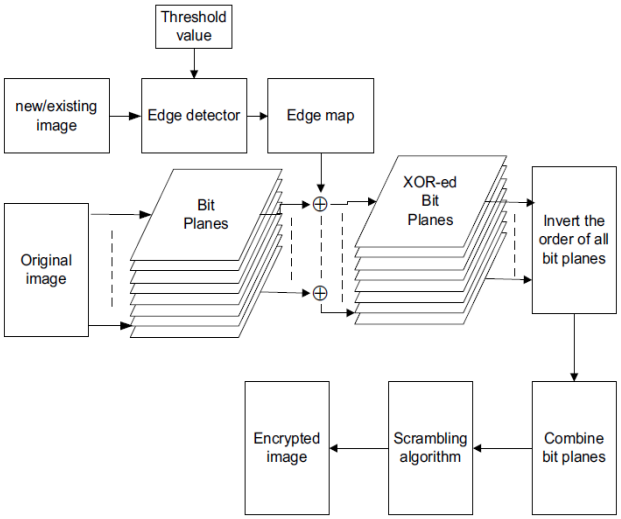

Figure 1. The EdgemapCrypt algorithm

Results

The proposed image encryption system uses any one of the chaotic system for pixel position permutation and one of the same chaotic system for pixel value modification. Several simulation results are provided to show the performance of the algorithms for 2D and 3D image encryption. In all experimental results of this paper, both algorithms utilize the image scrambling algorithm based on the Generalized P-Gray Code in with the security keys: $n=2=2$, $p = 0$.

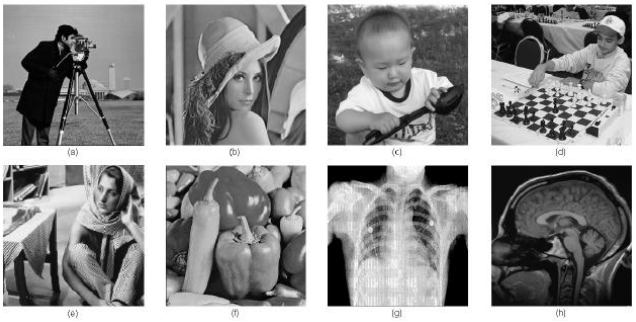

Figure 2. Test images. (a) 256×256 Cameraman; (b) 256×256 Lena; (c) 256×256 Baby; (d) 256×256 Chessplayer; (e) 512×512 Barbara; (f) 512×512 Peppers; (g) 512×512 CT ribs image; (h) 512×512 MRI brain image

2D IMAGE ENCRYPTION:

There are several types of 2D images such as grayscale images, medical images and biometrics. The 2D image can be decomposed into several binary bit planes and encrypted one by one. Figure 3 and Figure 4 shows the Grayscale image encryption using the EdgemapCrypt algorithm, Color image encryption using the EdgemapCrypt algorithm.

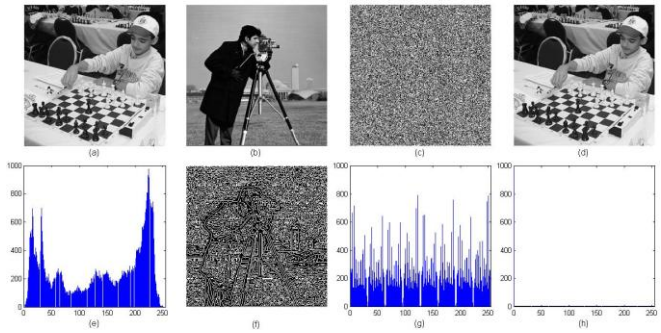

Figure 3. Grayscale image encryption using the EdgemapCrypt algorithm. (a) The original 256×256 grayscale image; (b) A 256×256 Cameraman image; (c) The encrypted image; (d) The reconstructed image; (e) Histogram of the original image in (a); (f) The edge map of the Cameraman image in (b), Sobel, 0.3; (g) Histogram of the encrypted image in (c); (h) Histogram of the difference between (d) and (a).

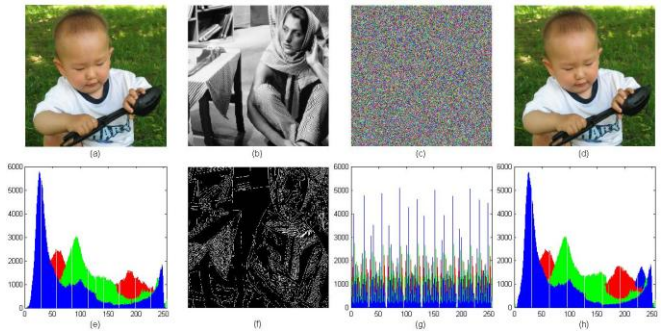

Figure 4. Color image encryption using the EdgemapCrypt algorithm. (a) The original 512×512 color image; (b) A 512×512 grayscale Barbara image; (c) The encrypted color image; (d) The reconstructed color image;(e) Histogram of the original image in (a); (f) The

Conclusion

Based on the design rules discussed earlier, the new image encryption scheme was designed. A suitable chaotic map preserving the properties of chaos after discretization was chosen. By choosing a high dimensional chaotic system, the key space is increased. Complex non-linearity was preserved by choosing suitable chaotic maps. Repeated permutations are avoided but pixel values are changed by the diffusion function. By incorporating all these features, the proposed cryptosystem avoids all the crypto graphical weaknesses of earlier chaos-based encryption systems. Number of security analysis were carried out on the new algorithm and simulation results show that encryption and decryption are good and the algorithm has good security and robustness.

References

[1] Xiping He Qionghua Zhang, "Image Encryption Based on Chaotic Modulation of Wavelet Coefficients", Congress on IEEE Image and Signal

Processing (CISP'08), Sanya, Hainan, Vol.1, pp.622-626, 27- 30 May 2008.

[2] Xin Zhang, Weibin Chen, "A New Chaotic Algorithm For Image Encryption", pp 889-892 IEEE ICALIP2008

[3] Dong enxeng, Chen Zengqiang, Yuan zhuzhi, Chen zaiping, "A Chaotic Images Encryption Algorithm with The Key Mixing Proportion Factor",pp 169-174 Computer Society IEEE 2008.

[4] Chong Fu, Zhen-chuan Zhang, Ying-yu Cao, "An Improved Image Encryption Algorithm Based on Chaotic Maps", Computer Society, IEEE 2007

[5] Huang Yuanshi, Xu Rongcong, Lin Weiqiang, "An Algorithm for JPEG Compressing with Chaotic Encrypting", Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation (CGIV'06), 2006

[6] Peng Fei, Shui-Sheng Qui, Long Min, "An Image Encryption Algorithm based on Mixed Chaotic Dynamic Systems and External Keys", Proceedings of 2005 International Conference on Communications, Circuits and Systems,,Vol. 2, pp.1139, 27-30 May 2005.

[7] Guang ZH, Huang FJ, Guan WJ, "Chaos-based Image Encryption Algorithm", Physics Letters A, Vol.346, pp.153 – 157, 2005.

[8] Wang Ying, Zheng DeLing, Ju Lei, Wei Yaoguang, "The spatial Domain Encryption of Digital Images Based on High-Dimension Chaotic System", Proceedings of the IEEE Conference on

[9] Zhang Han, Wang Xiu Feng, Li Zhao Hui, Liu Da Hai, Lin You Chou, "A New Image Encryption Algorithm Based on Chaos System", Proceedings of the 2003 IEEE International Conference on Robotics, Intelligent Systems and Signal Processing, Changsha, China, pp.778- 782, October 2003.

[10] Kristina Kelber, Wolfgang Schwarz, "General Design Rules for Chaos-Based Encryption systems", Proceedings of 2005 International Symposium on Nonlinear Theory and its Applications(NOLTA2005) Bruges, Belgium, October 18-21, pp.465-468, 2005.

[11] Yong-Hong Zhang, Bao-Sheng Kang, Xue-Feng Zhang, "Image Encryption Algorithm Based On Chaotic Sequence", Proceedings of the 16th International Conference on Artificial Reality and Telexistence - Workshops (ICAT'06),Hang Zhou, Zheijang, China, pp. 221-223, Nov.2006.

[12] Chengqing Li, "On the security of a class of Image Encryption Scheme", IACR's Crytology ePrint Archive: Report 2007/339, August 2007.

[13] Junan Lu, Xiaoqun Wu, Xiuping Han, Jinhu Lü, "Adaptive feedback synchronization of a unified chaotic system", Physics Letters A, Vol.329, pp. 327-333, 2004.

[14] Borko Furht and Darko Kirovski," Multimedia Security Handbook", CRC Press, December 2004.