Key Independent Retrieval of Chaotic Encrypted Images

Ram Ratan

Defence Research and Development Organisation
Scientific Analysis Group, Metcalfe House Complex
Delhi-110054, India
ramratan_sag@hotmail.com

Abstract. A chaotic image encryption algorithm based on circular shift functions proposed for high security is analysed in this paper for retrieving encrypted images. Proposed retrieval scheme is key independent and based on divide and conquer attack where neighbourhood similarity characteristic of images is applied. The simulation results show that retrieved images have very good visual perception quality and are as similar as original images. The analysis indicates that above algorithm in present form is insecure and encrypted images can be retrieved efficiently.

Keywords: Image Secrecy, Chaotic Image Encryption, Circular Shift Function, Image Decryption, Divide and Conquer Attack, Neighbourhood Similarity.

1 Introduction

Security is an important issue in communication and storage of digital images because of rapid use of such media in the digital world nowadays and encryption is one of the ways to achieve security. Encryption is the process which tranforms the information with the help of encryption key into encrypted form which is unintelligible and looks like a random mesh. Image encryption has wide applications in strategic communication, telemedicine, medical imaging, multimedia systems, etc. Images are different from text and it is not a wise idea to use traditional encryption schemes to encrypt them because of much encryption time of large image size. Moreover, retrieved text must be same as original text but this is not necessary for images because of visual characteristics of human perception which tolerate small errors in retrieved images,i.e., small errors in retrieved images are acceptable. Decryption is the process by which original information is retrieved from encrypted infromation with the help of decryption key.

In order to achieve security, a variety of encryption schemes have been proposed which can be classified in three types: position permutation [1]-[5], value transformation [6]-[9] and visual transformation [5]. The present paper is concerned with position permutation where circular shift functions are used [1-2,8] to encrypt images. An image encryption algorithm given in [1] is based on bit circulation and called as Bit Recirculation Image Encryption (BRIE) and an

S. Chaudhury et al. (Eds.): PReMI 2009, LNCS 5909, pp. 483–488, 2009.

algorithm proposed in [2] is based on pixel circulation and called as Chaotic Image Encryption (CIE). Both the algorithms are also known as two dimentional circulation encryption algorithms (TDCEA) which consist of two dimentional circular shift functions.

The analysis of such methods for retrieval of information from encrypted images becomes important and necessary in some applications and is useful also in evaluation of such schemes for security. There are following attacks which can be applied in analysis of encryption techniques depending on various situations: (1) Known cipher image attack (2) Chosen cipher image attack (3) Known plain image attack and (4) Chosen plain image attack. The analysis of above methods is carried out for security [10-12] by applying known or chosen plain image and known cipher image attacks to obtain encryption key.

In this paper, a CIE algorithm based on pixel circulation using shift functions [1-2] is analyzed and an efficient retrieval scheme is proposed for retrieving chaotic encrypted images in which rows and columns shifts are applied. The retrieval scheme is independent of key and is applicable in a situation when only an encrypted image is known. The retrieval scheme is based on divide and conquer attack where neighbourhood similarity is considered as the correlation between adjacent columns and adjacent rows to correct the effect of circulation of pixels.

The paper is organized as follows. We firstly give a brief introduction of CIE in Section 2. Proposed image retrieval scheme is presented in Section 3. Simulation results and discussions on security issues of CIE are presented in Section 4. Finally, the paper is concluded in Section 5 followed by references.

2 CIE Algorithm

Idea of CIE is the pixel circulation of images which is controlled by chaotic pseudo random sequence. The algorithm has following four steps:

`Step-1` determines a chaotic system and its initial point $x(0)$, rowsize M and columnsize N of an image, iteration number $n0$, and constants α, β, and γ used to determine the rotation number.
`Step-2` generates the chaotic sequence from the chaotic system.
`Step-3` geterates the binary sequence.
`Step-4` includes special functions to rearrange image pixels.

Let f be an image of size $M \times N$ pixels, $f(x,y), 0 \leq x \leq M-1, 0 \leq y \leq N-1$, be the pixel value of pixel in f at position (x,y), the transformation image f' for given image f is obtained by following circular shift functions:

(i) $ROLR_l^{i,p}$: $f \rightarrow f'$ is defined to rotate each pixel in the i^{th} row in f, $0 \leq i \leq M-1$, in the left direction p pixels if l equals 0 or in the right direction p pixels if l equals 1.
(ii) $ROUD_l^{j,p}$: $f \rightarrow f'$ is defined to rotate each pixel in the j^{th} column in f, $0 \leq j \leq N-1$, in the up direction p pixels if l equals 0 or in the down direction p pixels if l equals 1.

(iii) $ROUR_l^{k,p}$: $f \rightarrow f'$ is defined to rotate each pixel at position (x, y) in the image such that $x + y = k$, $0 \leq k \leq M + N - 2$, in the upper right direction p pixels if l equals 1 or in the lower left direction p pixels if l equals 0.
(iv) $ROUL_l^{k,p}$: $f \rightarrow f'$ is defined to rotate each pixel at position (x, y) in the image such that $x - y = k$, $-(N-1) \leq k \leq M - 1$, in the upper left direction p pixels if l equals 0 or in the lower right direction p pixels if l equals 1.

BRIE consists of first two functions and CIE consists of all four functions. The solution to CIE is obtained for first two circular shift functions which are used in two dimentional circulation of pixels to get an encrypted image.

3 Image Retrieval Scheme

We see in the images that the value of pixels is normally varying smoothly in the neighbourhood regions which can help us in retrieval process. Divide and conquer attack can make the solution efficient to given complex problem by decomposing it into simple problems. We use these concepts in developing proposed image retrieval scheme. For retrieval of an encrypted image, we normally require decryption key but our proposed scheme is independent of keys and we do not require any information of such keys. As per divide and conquer attack we divide given image into columns and rows which make the retrieval of an encrypted image easy and efficient. The neighbourhood similarity is considered here as the correlation which is measured as the correlation between two adjacent rows (columns). These correlation values are used to get correct shift for each row and column and rearrange the pixels accordingly in obtaining retrieved image. The scheme is described as follows:

3.1 Removal of Columnwise Circulation Effect

It is achieved by computing correlation between all adjacent columns of given encrypted image f'. The correlation between two adjacent columns, j and $j+1$, with shift t is computed as

$$corr_t(j, j+1) = f'(i, j) \times f'((i+t) mod M, j+1), 0 \leq i \leq M - 1$$

This correlation is computed for all possible shifts, $0 \leq t \leq M - 1$ and the correct shift t for column $j + 1$ is obtained for which the value of correlation is maximum. In this manner the correct shift t_j is obtained for all the columns, $1 \leq j \leq N - 1$.

3.2 Removal of Rowwise Circulation Effect

It is achieved by computing correlation between all adjacent rows of given encrypted image f'. The correlation between two adjacent rows, i and $i + 1$, with shift t is computed as

$$corr_t(i, i+1) = f'(i, j) \times f'((i+1, (j+t) mod N), 0 \leq j \leq N-1$$

This correlation is computed for all possible shifts, $0 \leq t \leq N-1$ and the correct shift t for row $i+1$ is obtained for which the value of correlation is maximum. In this manner the correct shift t_i is obtained for all the rows, $1 \leq i \leq M-1$.

As per above procedures, the effect of columnwise and rowwise circulation of pixels is removed by rearranging pixels in columns and rows of f'. As the shifts for first column and first row are not taken into consideration while rearranging pixels in columns and rows, these leave shifting effects in the retrieved image.

For correcting the effects due to first column and first row, we compute correlation between adjacent columns, $corr(j, (j+1) mod N), 0 \leq j \leq N-1$ and correlation between adjacent rows, $corr(i, (i+1) mod M), 0 \leq i \leq M-1$. The shifts t_c for column and t_r for row are obtained as $j+1$ and $i+1$ respectively for which correlation value is minimum. All the columns and rows of f' are rearranged according to t_c and t_r. Finally, the retrieved image f" is obtained.

4 Results and Discussions

CIE algorithm and image retrieval scheme given in this paper have been implemented on MATLAB Platform using MATLAB programming. The visual perception quality of retrieved images obtained with our scheme is very good and is same as that of original images. The error in retrieved images is measured as mean square error (MSE) which is computed as

$$MSE = \frac{1}{M \times N}[f(i,j) - f"(i,j)]^2, 0 \leq i \leq M-1 \text{ and } 0 \leq j \leq N-1.$$

The error in retrieved image f" is tolerable because it does not leave objectionable distortion in retrieved images. Simulation results for image encryption and image retrieval are respectively shown in *figure 1* and *figure 2*.

In *figure 1*, (a) and (e) are original images; (b) and (f) are encrypted images obtained by applying only rowwise circulations; (c) and (g) are encrypted images obtained by applying only columnwise circulations, and (d) and (h) are final encrypted images obtained by applying both rowwise and columnwise circulations. In *figure 2*, (a) and (b) are given encrypted images which have MSE as 7717 and 13312 and (c) and (d) are retrieved images which have MSE as 80 and 630. We see in *figure 1* and *figure 2* that retrieved images have very good visual perception quality with unnoticeable distortion and are as similar as original images.

The security of CIE is mentioned as $2^{(3M+3N-2)\times n(0)}$ and claimed it as very high [2]. In exhaustive approach there are $(M \times N)!$ trials for normal pixels permutation and $(M^N \times N^M)$ trials for circular shifts (ROLR and ROUD) used in encryption. In proposed retrieval scheme we require only $(M+N)$ trials to retrieve an image encrypted with above two circular shift functions. This shows that the CIE algorithm is insecure in present form and encrypted images of CIE can be retrieved efficiently. The CIE can be made secure against above attacks by incorporating masking or substitutions [6,13] in addition to circular shifts.

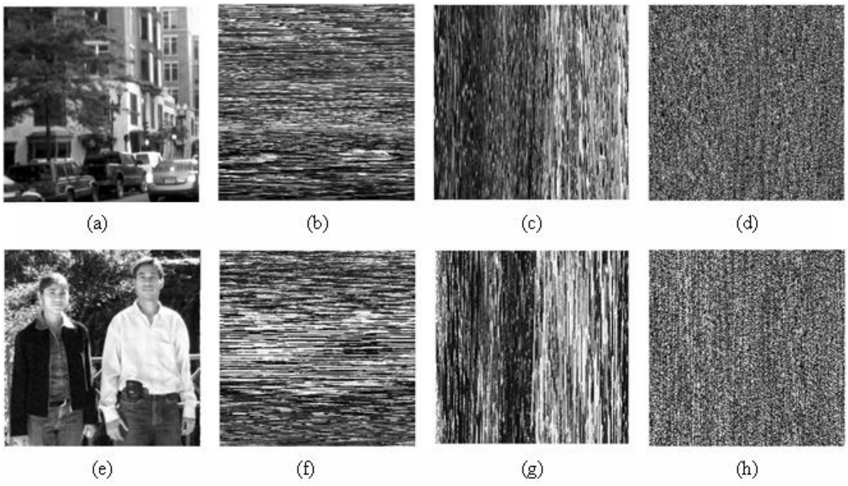

Fig. 1. Original and Encrypted Images

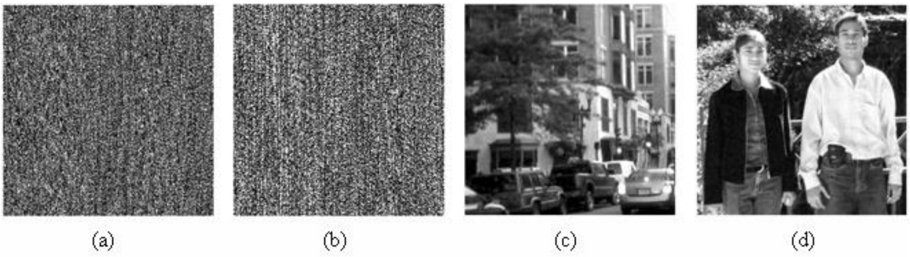

Fig. 2. Encrypted and Retrieved Images

Above retrieval scheme is developed for gray level images but can also be considered for binary images to retrieve chaotic encrypted images. For binary images, the correlation between two adjacent columns (rows) with shift t required in image retrieval is to be computed as given below:

$corr_t(j, j+1) = \frac{1}{N}[$ no. of matches $(f'(i,j) = f'((i+t)modM, (j+1)modN))-$ no. of mismatches $(f'(i,j) \neq f'((i+t)modM, j+1)), 0 \leq i \leq M-1]$.

The pixels in f' are rearranged as per above retrieval scheme to retrieve binary encrypted images.

5 Conclusion

An image retrieval scheme has been presented in this paper for retrieving encrypted images of chaotic image encryption algorithm in which circular shift functions are applied for columnwise as well as rowwise circulation of pixels.

Image retrieval is automatic, efficient and independent of keys. Image retrieval scheme is based on divide and conquer attack in which neighbourhood similarity characteristic between adjacent columns and rows is used in image retrieval. It has been shown in simulation results that the chaotic image encryption algorithm which consists of circular shift functions is insecure and the encrypted images can be retrieved with very good visual perception quality as similar to original images.

References

1. Yen, J.-C., Guo, J.-I.: A new chaotic image encryption algorithm and its VLSI architecture. In: Proc. IEEE Workshop Signal Processing Systems, pp. 430–437 (1999)
2. Yen, J.-C., Guo, J.-I.: A new chaotic image encryption algorithm. Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China, E-mail: jcyen@mail.lctc.edu.tw
3. Yen, J.-C., Guo, J.-I.: Design of a new signal security system. In: Proc. IEEE Intl. Symposium on Circuits and Systems (ISCAS 2002), vol. 4, pp. 121–124 (2002)
4. Furht, B., Kirovski, D.: Multimedia Security Handbook. CRC Press, Boca Raton (2004)
5. Guo, J.-I., Yen, J.-C.: A new mirror-like image encryption algorithm and its VLSI architecture. In: Proc. 10th VLSI Design/CAD Symposium, Taiwan, pp. 319–322 (1999)
6. Maniccam, S.S., Bourbakis, N.G.: Lossless image compression and encryption using SCAN. Pattern Recognition 34, 1229–1245 (2001)
7. Maniccam, S.S., Bourbakis, N.G.: Image and video encryption using SCAN patterns. Pattern Recognition 37, 725–737 (2004)
8. Ozturk, I., Sogukpinar, I.: Analysis and comparision of image encryption algorithms. Proc. of World Academy of Science, Engineering and Technology 3 (2005)
9. Chang, C.-C., Hwang, M.-S., Chen, T.-S.: A new encription algorithm for image cryptosystems. Journal of Systems and Software 58, 83–91 (2001)
10. Li, S., Zheng, X.: On the security of an image encryption method. In: Proc. IEEE Intl. Conf. on Image Processing (ICIP 2002), vol. 2, pp. 925–928 (2002)
11. Li, C., Li, S., Chen, G., Chen, G., Hu, L.: Cryptanalysis of new signal security system for multimedia data transmission. EURASIP Journal on Applied Signal Processing 8, 1277–1288 (2005)
12. Li, C.: Cryptanalysis of some multimedia encryption schemes. M.S. Thesis (2005)
13. Menezes, A., Van Oorschot, P., Vanstone, S.: Handbook of applied cryptography. CRC Press, Boca Raton (1996)