Fast and Lossless Image Compression in Chaos-Based Encryption

Doi: 10.17932/ IAU.IJEMME.m.21460604.2015.5/3.955-962

***Sajad EINY*[1]**
***Solmaz EINI*[2]**

Abstract

The wide use of digital images leads to the necessity of securing them when they enter into an insecure channel. Image cryptography plays a vital role in the modern communication. For telecommunication systems through the internet, various compression and encryption techniques are proposed to satisfy a fast and secure transmission. However these two techniques have been studied separately. In this paper we propose new approach of fast image encryption algorithm with chaos-based encryption system using by cipher structure and in compression process by using a context matching method driven by the correlation between adjacent neighbor mask pixels. With this approach the size of transmission can be reduce and transmission can be secure.

Keywords: *Image Compression, Cyrptography, Chaos Based Encryption*

Introduction

In today's heterogeneous network environment, this requires more and more new techniques to meet the increasing needs of a modern society. In recent years, with the rapid development of computer science and network technology, people are obtaining, using and processing digital images more frequently. This situation brings us convenience, as well as potential threats. How to protect the information within the digital images from the attacks of intruders is becoming a more and more serious problem. Image compression is minimizing the size in bytes of a graphics file without degrading the quality of the image to an unacceptable level. The reduction in file size allows more images to be stored in a given amount of disk or memory space. It also reduces the time required for images to be sent over the Internet or downloaded from Web pages[1-5].

However, for any communication system, it is necessary to take into account two major requirements: a fast transmission to send the information from a transmitter to a receiver (that can be done using an efficient

compression technique) and a secure transmission of information which can be achieved using a powerful encoding algorithm. To satisfy these constraints, new compression and encryption methods allowing a fast and secure information transmission are proposed in the literature.

In case, these methods (compression and encoding) are often developed in an independent manner although they are strongly connected and one influences the other. Accordingly, we propose to combine compression with encryption and propose a new method of compression and encryption at same time[6-7].

It is supposed that we transmit important images to a receiver, preventing non-authorized people from intercepting the images. In order to encrypt the images we

[1] *Spatial Information Technology Jawaher Lal Nehro Hyderabad India, Istanbul Aydın University*
[2] *Spatial Information Technology Jawaher Lal Nehro Hyderabad India, Istanbul Aydın University*

cover the images with an insignificant image. In addition we would like to compress the transmitting data, to achieve a high speed Communications[8]. For this purpose we utilized a compression scheme which also uses multiple predictors. However the predictors are generated using local statistics and are used based on a switching algorithm which relies on the correlation between pixels. And in next step, chaos-based image encryption algorithm, in cipher architecture, is proposed. The flowchart of the algorithm is shown in following flowchart. An image is producing a binary data stream with masking data of image with a random key stream by a chaos-based random key stream generator then corresponding encrypted image is formed. The specific details of each component are to be discussed in the following sections[9].

Fast and lossless Image compression

Recently, Compression schemes have been greatly developed by various researchers [1]–[4].

This was introduced in order to solve the problems which consist of the separation of independent sources using observed mixed texture without a strong knowledge about sources and, in particular lossless compression schemes rely on statistical structure in the data. Lossless compression relay o statistical structure in the data and work on non-random data contain duplicated information that determine the probability of occurring and assigning the smallest part of the most common data.

This kind of algorithm is used in computing, for saving space and sending data through the web and viewing image online; The algorithm work in tow way; prediction and correction-based conditional average.

Prediction

Firstly, we perform prediction using a predictor selected from a fixed set of 9 simple linear predictors. Prediction errors are reordered to obtain probability distribution expected by the data model.

To predict the intensity of a specific pixel X, we use fast linear predictors up to 3 neighboring pixels: first left-hand neighbor, second upper neighbor , and third upper-left neighbor .

Lossless compression has eight linear predictive schemes named JPEG lossless algorithm.

Main algorithm of predictors:

1) First step make no scheme

2) 1-D predictors

$$x^{\eta}(i,j) = x(i-1,j)$$

$$x^{\eta}(i,j) = x(i,j-1)$$

$$x^{\eta}(i,j) = x(i-1,j-1)$$

3) 2-D predictors

$$x^{\eta}(i,j) = x(i-1,j) - x(i-1,j-1) + x(i,j-1)$$

$$x^{\eta}(i,j) = \{\frac{x(i-1,j) - x(i-1,j-1)}{2}\} + x(i,j-1)$$

$$x^{\eta}(i,j) = \{\frac{x(i,j-1) - x(i-1,j-1)}{2}\} + x(i-1,j)$$

$$x^{\eta}(i,j) = \{\frac{x(i,j-1) - x(i-1,j)}{2}\}$$

In this process $x(i,j)$ is the pixel of (i,j) and $x^{\eta}(i,j)$ the value of predictors.

If there is a subtraction operation in a calculation of the predictor, then its value may Be out of the nominal range of pixel intensities $[0;2^{n(i,j)}-1]$, where N denotes image bit.

Depth. In such a case, we take the closest value from the above range. We compress the Residuum symbol that is a difference between the actual $x(i,j)$ and the predicted $x^{\eta}(i,j)$
We reorder residual values to get the probability distribution close descriptive by simply picking symbols: first, last, second, last but one and so on:

$$x^{\eta}(i,j) = \begin{cases} 2n(i,j) & for\ n(i,j) < 2^n - 1 \\ 2\left(2^n - n(i,j)\right) & for\ n(i,j) > 2^n - 1 \end{cases}$$

Correction base

The conditional exception of x set of observation in y_i condition is:

$$E[X|Y_I] = \sum_X P[X = x|Y_I = Y_1, Y_2, Y_3, \dots, Y_N]$$

y_1	y_2	y_3
y_4		

The optimal value:

$$E\left[x_{i,j}\middle|(x_{i-l}, y_{j-m})_{l,m}^{i,j}\right] = 1$$

Prediction by particle matching is method is method to predict. The symbol depending on pervious. This method is called MARKOV model in [10-13].

Pixel $x_{i,j}$ we can define a set of pixels which are neighborhood of $x_{i,j}$ as it context. That are depending on the scanning and hence operational method. The pixels $x_1^{i,j}, x_2^{i,j}, x_3^{i,j}, \dots, x_k^{i,j}$ with set of value $\alpha = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_k)$ define: $\varsigma_k(\bar{\alpha}) = \{x_{l,m} : x_1^{l,m} = \alpha_1, x_2^{l,m} = \alpha_2, x_3^{l,m} = \alpha_3, \dots, x_k^{l,m} = \alpha_k\}$

ς_k Consist of all the pixels on the value of $(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_k)$ for sample mean:

$$\mu_{x|\alpha} = \frac{1}{\|\varsigma_k(\bar{\alpha})\|} \sum_{x \epsilon \alpha} x$$

Process algorithm

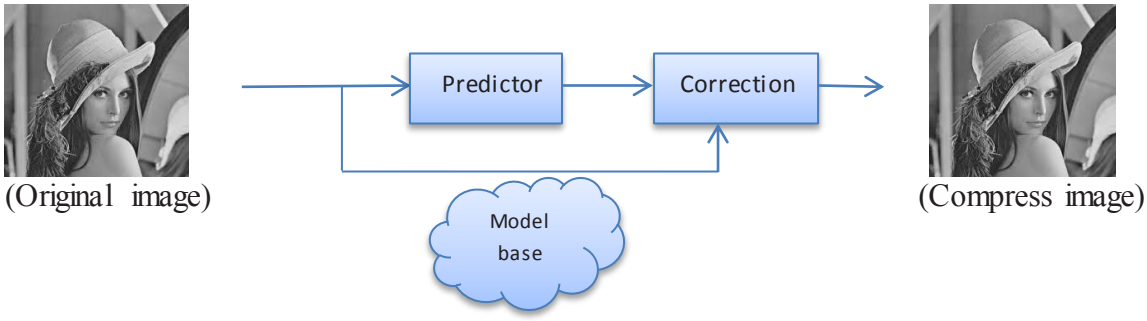
1) N set of x observation
2) For each x_i is in sequence of x on replace i: $y = [x_{i-n}, \dots, x_i]$
3) Let y target amount
4) Update all y amounts

x_1	x_2	x_3
x_4		

x_n y_m
(Content bass matching windows)

Pseudo-code:

While (not last value of α_n) do
Read neighbors
Shorten to 4 neighbors of content
While (context amount $(\varsigma_k(\bar{\alpha})) < 0$ do
Escape sequence of $(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_k)$
Calculate average sample mean $(\mu_{x|\alpha})$



(Original image) (Compress image)

Figure 1. *compression process*

Fast Encryption chaos-base

Chaos-base image encryption scheme: the main idea of chaos-based image encryption system is proposed in the diagram (2) that consist of two major parts, serving of initial key and mixing base upon two different chaotic maps.

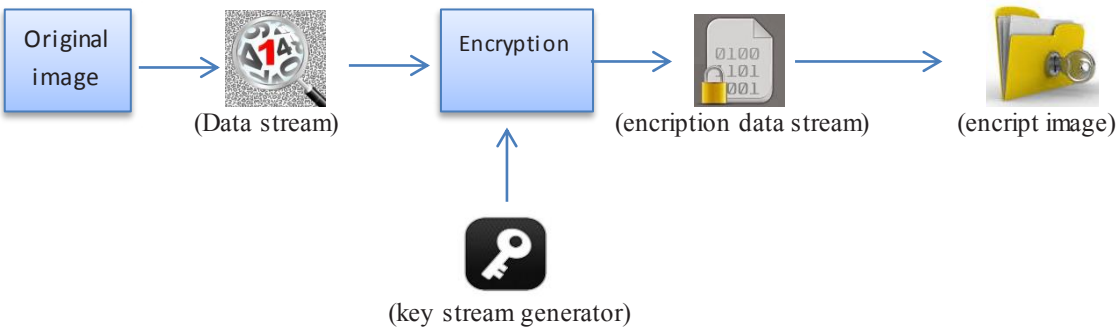


Figure 2. *encription procces*

To generating the random key stream , the first should be created. For first key the following mathematice formolas describe:

$$x_{n=1} = f(x_n)$$
$$= \begin{cases} g\left(\frac{x_n}{p}\right) & if 0 < \frac{x_n}{2^l + 1} < p \\ g\left(\frac{2^l + 1 - x_n}{1 - p}\right) & otherwise \end{cases}$$

In this formolus pϵ[0,1] , $x_n \epsilon\{1,2,\ldots., 2^l\}$ and x_0 the first value of g(0) function.
Which can be flooring. This this randome algorithm is so weak and not good enough due to its randome process therefore, we are using

high dimentional map to mixing up the sequence generator. This theory in[4]
Is serving the porpose
Cat map is formed by:
h_c: y=Ax mod 2^l
Where x=$[x_1, x_2, x_3, x_4, \ldots, x_m]^t$ and y=$[y_1, y_2, y_3, y_4, \ldots, y_n]^t$
x_i *and* $y_j \epsilon$ [0, 2^{l-1}]

A=
$A_{1\,1} A_{1\,2} A_{13} A_{14} A_{15} \ldots A_{1\,M} A_{2\,3} A_{2\,4} \ldots A_{(M-1),M}$

Is an matrixM*M with each $A_{i\,j}$ mixing I th and j th dimention in details:

$$A=\begin{bmatrix}1 & a_{12} & \cdots & 0\\ b_{12} & 1+a_{12}b_{12} & 0 & 0\\ 0 & 0\ldots & \ddots & \vdots\\ \vdots & \vdots & 1 & 0\\ 0 & 0\ldots & & 1\end{bmatrix}\ldots\begin{bmatrix}1 & 0 & \cdots & a_N\\ 0 & 0 & 0 & 0\\ 0 & 1\ldots & \ddots & \vdots\\ \vdots & \vdots & 1 & 0\\ b_M & 0\ldots & 1+a_Nb_M & \end{bmatrix}$$

$$\times\begin{bmatrix}1 & 0 & \cdots & 0\\ O & 1 & a_{23} & 0\\ 0 & b_{32}\ldots & \ddots & \vdots\\ \vdots & \vdots & 1 & 0\\ 0 & 0\ldots & & 1\end{bmatrix}\ldots\begin{bmatrix}1 & 0 & \cdots & a_N\\ 0 & 0 & 1 & 0\\ 0 & 1\ldots & \ddots & \vdots\\ \vdots & \vdots & 1 & 0\\ 0 & 0\ldots & 1+a_{N-1}b_{M-1} & \end{bmatrix}$$

Where a_N, b_M are integer in $[0, 2^{l-1}]$ .This high-dimensional Cat map, h_c, is used as our post-processing unit for mixing up the initial key stream.

key stream generator

the useful way for sending secret data without data integrity is bite sequence as key. Therefore, adds this to plain text to form of the cryptogram like bellow chart.

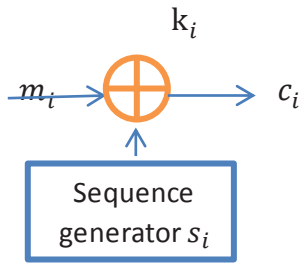


Figure 3. *key generator key generator*

The key can be parameter in f and first state is $s_0.s_i = f(k, s_{i-1})$, $k_i = g(s_i)$, $c_i = m_i \oplus k_i$ Byte-based stream cipher with initial $s[k]$=k for I in 0,…, 255 and 0,…,255 equal to

$s[k] + k[i] \leftrightarrow s[j] + k[i]$

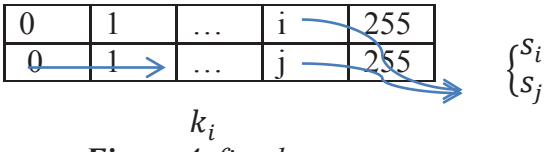


Figure 4. *first key stream*

Pseudo algorithm

(1) With a user key, construct the parameters needed for the key generator. The computational procedures are to be discussed in above.

(2) The image is firstly transformed into a standard data stream (Fig. 1). Taking an image in true color with

(N*M) pixels as an example, if each pixel consists of RGB format, a stream of total c_i data can be formed by partitioning the bits obtained from pixels.

3) For each data m_i, it will be masked by the key stream with the following function: $c_i = (d_i + k_i + c_{i-1}) mod 2^l$

4) The encrypted data stream is converted back into RGB format for storage or transmission. Decryption is similar to encryption, except that the following decryptions function:$\widehat{D}_i = (c_i - k_i - d_{i-1}) mod 2^l$ $\widehat{D}_i$ Is decrypting sequence[13-15].

Experimental results

In order to validate our approach several simulations are conducted. "Lena" compressed image are encrypted and decrypted by the proposed method. 512×512 color JPEG format files are used as the original images. An example of the simulations is shown in Fig. 8. The first row of Fig.4 shows the original source images (a),

the images in the second row were obtained by applying optimize chaotic to the compressed image in (b), and the last row corresponds the reconstructed images which the receiver can obtain (c). After execution of cat map and applying chaotic algorithm to the compressed components with the random key generator, we can get the source images.

The quality of the reconstructed images, however, is not as same as the original ones, because compression cut off higher frequency components. Moreover, the order of the outputs is not always same as that of the original images.

Figure 4a. *Orginalimage*

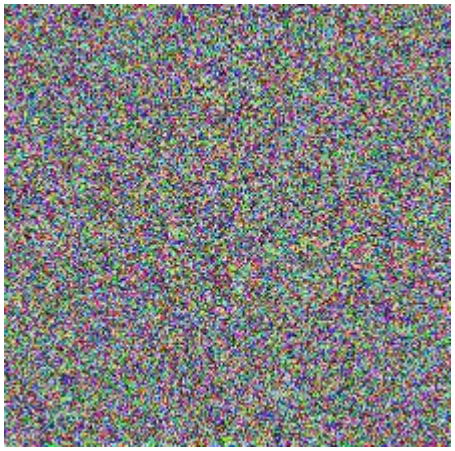


Figure 4b. *encripted and copressed*

Figure 4c. *recovered image*

In this test the below table shows ability of this algorithm:

Items	value
PSNR	78.04
MCSE	0.002
ENTROPY	7.62

The picture of histogram shows no different between original image and recovered image.

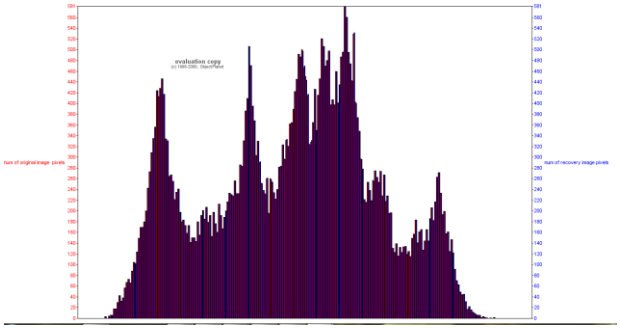


Figure 5. histogram diagram

Conclusion:

In this paper, we presented a novel image encryption technique for compressed domain. Our proposed technique can work efficiently and independently regardless of the image size, quality and dimension. The experimental results shown in this paper proved that the encryption of the proposed method is extremely high if the relative compression ratio is compromised. Double layer of security

for the embedding text ensures the protection of data against any intruder attack. In addition, the user has been given the freedom of choosing the key and using it by anyway s/he likes. Further research over the proposed method has also been discussed so that studies on this Stream can be continued smoothly.

REFERENCES

[1] "HDCP specification rev 1.3," Dec. 2006.

[2] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," in IEEE Trans. Signal Processing, Oct. 2004, vol. 52, pp. 2992–3006.

[3] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," IEEE Trans. Inform. Theory, vol. 19, pp. 471–480, Jul. 1973.

[4] C. Shannon, "Communication theory of secrecy systems," in Bell System Technical Journal , 1949, vol. 28, pp. 656–715.

[5] F. Kschischang, B. Frey, and H. Loeliger, "Factor graphs and the sum product algorithm," in IEEE Trans. Inform. Theory, Feb. 2001, vol. 47, pp. 498–519.

[6] R. G. Gallager, Low Density Parity Check Codes, Ph.D. thesis, MIT, Cambridge, MA, 1963.

[7] D. Schonberg, K. Ramchandran, and S. S. Pradhan, "LDPC codes can approach the Slepian Wolf bound for general binary sources," in 40th Annual Allerton Conf., Oct. 2002, pp. 576–585.

[8] T. J. Richardson and R. L. Urbanke, "The capacity of low-density paritycheck codes under message-passing decoding," IEEE Trans. Inform. Theory, vol. 47, pp. 599–618, Feb. 2001.

[9] W. Hong, T. Chen, and C. Shiu, "Lossless Steganography for AMBTC-Compressed Images", IEEE Congress on Image and Signal Processing, Vol. 2, pp. 13-17, July 2008, DOI: 10.1109/CISP.2008.638.

[10] A.M. Fard, M.-R. Akbarzadeh-T, and F. Varasteh-A, "A New Genetic Algorithm Approach for Secure JPEG Steganography", IEEE International Conference on Engineering of Intelligent Systems, pp. 1-6, September 2006, DOI: 10.1109/ICEIS.2006.1703168.

[11] M. Ishaque, and S.A. Sattar, "Quality Based JPEG Steganography Using Balanced Embedding Technique", IEEE International Conference on Emerging Trends in Engineering and Technology, pp. 215-221, January 2010, DOI: 10.1109/ICETET.2009.188.

[12] M. Hasan and K. M. Nur, "A Lossless Image Compression Technique using Location Based Approach ", International Journal of Scientific and Technology Research (IJSTR), vol. 1, issue. 2, March 2012.

[13] M. D. Lema and O. R. Mitchel, "Absolute Moment Block Truncation Coding and its Application to Color

Images", IEEE Transactions on communications, Vol. 32, Number.10, pp. 1148-1157, 1984, DOI: 10.1109/TCOM.1984.1095973.

[14] Z. Zhao and L. Tang , "High Capacity Reversible Data Hiding in AMBTC-Compressed Images ", International Journal of Digital Content Technology and its Applications, Vol. 6, Number 2, February 2012.

[15] C. Velasco, M. Nakano, H. Perez, R. Martinez, and K. Yamaguchi, "Adaptive JPEG Steganography using Convolutional Codes and Synchronization Bits in DCT Domain", IEEE International Midwest Symposium on Circuits and Systems, pp. 842-847, September 2009, DOI: 10.1109/MWSCAS.2009.5235899.