Secured Compound Image Compression Using Encryption Techniques

V.Radha, *Member, IAENG*, D.Maheswari

***Abstract*—The amount of information transmitted using the Internet and a wireless network is continuously increasing, where predominant amount of information is image data. Sharing utilities, being easy, economical and technically sophisticated, are used abundantly by industries, businesses and individuals. However, this introduces serious concern on the protection issues which arise from the access concern. This paper deals with algorithms that provides solution to such concerns and discusses methods that can be combined with the compound image compression models**

***Index Terms*—Compound Image, Encryption, Decryption, Scrambling, Security.**

I. Introduction

In Finding effective ways to protect image data is challenging even with the most advanced technology and trained professionals. The increasing number of information-security-related incidents and organized crimes means that securing information is becoming a major issue in the current information-based economy. This has forced academicians, industrialists and researchers to focus on the protection of images during transmission.

To secure information, many research directions have been suggested in the past few decades. Several techniques have been introduced[1],[2],[3]most of which can be categorized into two techniques, namely, data hiding and encryption[4]. Data hiding technique hides a secret message into the image in a way that it is difficult to decipher by the hackers. Encryption, on the other hand, is the process of transforming the information to ensure security during transmission and storage. There are various image encryption systems to encrypt and decrypt data and there is no single encryption algorithm that satisfies all types of images [5].

Thus, in the present paper work, a chaotic-based image scrambling encryption method[6] that can be combined with JPEG compression technique is proposed.

Manuscript received July 26, 2011; revised August 12, 2011.

V. Radha is with the Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore, Tamilnadu, PIN 641043 India. (phone: +91422-2404983; e-mail:radhasrimail@gmail.com.)

D. Maheswari. is with the Dpartment of ComputerScience,R.V.SCollege ofArtsandScience,Coimbatore,Tamilnadu,India.(phone:+914222643682;email:mahileni@gmail.com).

II. Security Techniques

While considering compound images, three blocks need to be secured. They are Text region, Picture/image an Graphics regions. For protecting text region, a Block Transformation Coding(BTC) is used [7]. The picture/image and graphics region of the compound image is protected using an encryption algorithm proposed by Xiangdong [8]. This algorithm is based on chaos theory and sorting transformation and was proposed to encrypt gray scale images. The procedure uses an effective algorithm to scramble the image without the need for threshold quantization. To make the Xiangdong model compatible for segmented compound image region, it was modified in two manners. The first is to convert the encryption algorithm to work with color images. The second modification made is to combine the encryption and compression process. These changes will increase the overall efficiency of the compression system and make it adaptable for secure transmission.

III. Proposed Encryption Scheme

The process of proposed algorithm that combines encryption and compression is given in Figure 1. This process is divided into three steps,

(i) Color Space Conversion
(ii) Key Generator and Scrambling Algorithm
(iii) JPEG Compression

The color space of the image is first converted to YUV color space .The two most widely used color spaces for storing digital images are RGB color space and YUV color space.

A. Scrambling Algorithm

The proposed image encryption algorithm consists of two parts: scrambling of plain-image and mixing operation of scrambled image using discrete states variables of chaotic maps. The purpose of scrambling is to transform, a meaningful image into a meaningless, disordered and unsystematic image to obscure real meaning of image. A secret scrambling increases the computational complexity of potential chosen-plaintext attack, thereby making cryptanalysis of image encryption much more complicated. The result of scrambling algorithm is shown in Figure 2.

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

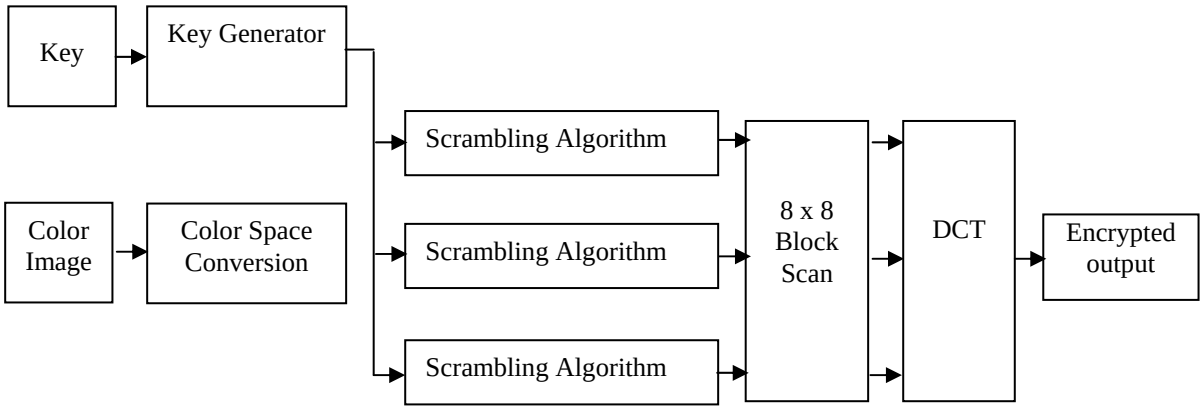

Figure 1 : Proposed Encryption Scheme for Picture and Graphics Block

Original Image Encrypted Image

Figure 2 Original and Scrambled Version of Lena and Airplane

IV EXPERIMENTAL RESULTS

The system was evaluated using various aspects like Compression Ratio, and Peak Signal to Noise Ratio (PSNR).

A. Performance Metrics

The performance of the proposed models was evaluated using different parameters like Average Moving Distance of Scrambling**,** Hamming Correlativity and Peak Signal to Noise Ratio. One of the objectives of the proposed compression models is to maintain the visual quality of the decompressed image. The quality of the decompressed image was ascertained by using the quality metric Peak Signal to Noise Ratio (PSNR).

B. Average Moving Distance of Scrambling

The average moving distance of scrambling is defined as Equation (1).

$$\|D\|_2 = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\sqrt{(w-i)^2+(v-j)^2} \qquad (1)$$

where M and N is the dimension of the image, i, j are coordinates of original and w and v are coordinates of encrypted image. The larger the Average distance ratio the less is the relation between the original and encrypted image.

Table I shows the average moving distance of scrambling obtained by the proposed algorithm while given with 256 x 256 images.

TABLE I
AVERAGE MOVING DISTANCE OF SCRAMBLING

Image Used	Maximum (ADR)	Minimum (ADR)	Average
Lena	84.7127	84.0298	84.37
Airplane	87.0943	86.8912	86.99

From the results projected, it can be seen that both images produce a high average moving distance, which indicates that the system is highly secure.

C. Hamming Correlativity

Since proposed image scrambling algorithm belongs to row scrambling algorithm that scrambles image row by row. Hamming correlativity H depicts similarity between two rows' permuting address codes. This value will be low if the system is more secure. Hamming correlativity is calculated as below.

Let $\{t_1, t_2, \ldots, t_N\}$ and $\{s_1, s_2, \ldots, s_N\}$ be two row's permuting address codes of length N, the Hamming correlativity H is defined using Equation 2

$$H = \sum_{i=1}^{N}\delta(t_i, s_i) \quad \text{where} \delta(a,b) = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$$

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The results obtained during experimentation with respect to Hamming correlativity is shown in Table II.

TABLE II
HAMMING CORRELATIVITY

Image Used	Hamming Correlativity
Lena	0.91
Sail Boat	0.96

From the results, it is evident that the encryption algorithm is highly secured as indicated by the low hamming correlativity (less than 1).

D. Peak Signal to Noise Ratio

In the present paper work, the encryption algorithm is combined with JPEG compression technique, so that it will provide an efficiency way for transmitting images. Several experiments were conducted to verify the quality of the image after decryption. The quality of the image was ascertained using the PSNR metric and is tabulated in Table III for the two selected images.

TABLE III
PSNR AFTER DECRYPTION

Image Used	PSNR
Lena	44.2
Sail Boat	45.6

The high value obtained proves that the quality of the image after decryption and decompression is good and can be considered by many transmission applications.

E. Speed of Encryption and Compression

For this experimentation, the selected two images were resized to different sizes and the ratios between encryption / decryption process and encoding / decoding process were calculated. Table IV presents this result. All the experiments were conducted in Pentium IV machine with 512 MB RAM.

As seen from the table, the speed of the algorithm is directly proportional to the size of the image. Further, it can be seen that the time taken is between 9.8 seconds and 11.2 seconds, which means that both encryption and compression process are very fast.

TABLE IV
SPEED OF ENCRYPTION AND COMPRESSION

Image	Size	Time (Seconds)
Lena	128 x 128	11.36
	256 x 256	9.80
Airplane	128 x 128	12.01
	256 x 256	11.20

V. CONCLUSION

This paper introduced the encryption algorithm that is to be used to secure the picture/image and graphics regions of a compound image. Experiments conducted with natural images show that the proposed algorithm is strong in providing security and is also very fast. Further, simulations showed that the key space is large and the attacker cannot decrypt an encrypted image without the correct key. All these advantages motivated the researcher to use this algorithm to encrypt the picture/image and graphics regions during compression.

REFERENCES

[1] Scharinger, J. (1998) Fast encryption of image data using chaotic Kolmogorov flow, J. Electronic Imaging, Vol.7, No.2, Pp. 318-325.
[2] Wu, C.P. and Kuo, C.C. (2005) Design of integrated multimedia compression and encryption systems, IEEE Transactions on Multimedia, Vol. 7, No. 5, Pp. 829-839.
[3] Wu, J., Xia, B., Liu, J. And Tian, J, (2004) A Secure Image Transmission Scheme Based On Digital Watermark And Cryptography, Proceedings Of International Symposium On Intelligent Multimedia, Video And Speech Processing, Pp. 278-281
[4] Xiang, T., Wong, K.W. and Liao, X. (2007) Selective image encryption using spatiotemporal chaotic system, Chaos, Vol. 17, No. 2, Pp. 023115-023115-12.
[5] P.V. Reddy, K.V .Sharma, P.Mallesham,. and P.Radhadevi, (2010) Secure Image Transmission Through Unreliable Channels, International Journal on Computer Science and Engineering, Vol. 02, No. 06, Pp. 2053-2058.
[6] Yu, X.Y., Zhang, J., Ren, H.E., Xu, G.S. and Luo, X.Y. (2006) Chaotic Image Scrambling Algorithm Based ob S-DES, Journal of Physics : Conference Series, Vol. 48, Pp. 349-353
[7] D.Maheswari, and V.Radha (2010) Secure Layer Based Compound Image Compression using XML Compression, 2010 IEEE International Conference on Computational Intelligence and Computing Research, ISBN:978-1-4244-5966-7,Pp.494-498.
[8] Xiangdong, L., Junxing, Z., Jinhai, Z. and Xiqin, H. (2008) Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation, International Journal of Computer Science and Network Security, Vol. 8 No. 1 pp. 64-68.
[9] Battiato, S., Gallo, G., Impoco, G. and Stanco, F. (2004) An Efficient Re-Indexing Algorithm for Color-Mapped Images, IEEE Transaction on Image Processing, Vol.13, No.11, Pp.1419-1423.
[10] Benabdellah, M., Himmi, M.M. and Zahid, N. (2007) Encryption-compression of images based on FMT and AES Algorithm, Applied Mathematical sciences, Vol. 1, No.25, Pp. 2203-2219.

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)