International Journal of Image Processing and Vision Science

Volume 1 | Issue 2 Article 15

October 2012

AN APPROACH TO IMAGE COMPRESSION AND ENCRYPTION

ABDUL RAZZAQUE
Department of Computer Science & Engineering, RCOEM, Nagpur INDIA, ab.razzaque@rediffmail.com

NILESHSINGH V. THAKUR
Department of Computer Science & Engineering, RCOEM, Nagpur INDIA, thakurnisvis@rediffmail.com

AN APPROACH TO IMAGE COMPRESSION AND ENCRYPTION

ABDUL RAZZAQUE & NILESHSINGH V. THAKUR

Department of Computer Science & Engineering, RCOEM, Nagpur INDIA
ab.razzaque@rediffmail.com, thakurnisvis@rediffmail.com

Abstract—Image compression scheme proposed by researchers have no consideration of security. Similarly image encryption scheme proposed by the authors have no consideration of image size. In this paper a simultaneous image compression and encryption scheme is discussed. The order of the two processes viz. compression and encryption is EC i.e. image encryption is performed first then the image compression is applied. For image encryption a symmetric key cryptography multiplicative cipher is used. Similarly for compression Discrete Cosine Transform is used. Image Compression is concerned with minimizing the number of bit required to represent an image. The compression can be lossless or lossy. Image Encryption is hiding image from unauthorized access with the help of secret key that key can be private or public.

Keywords*-image compression; image encryption*

I. INTRODUCTION

In image processing we have to deal with huge amount of data. Any image compression algorithm is used to reduce the amount of data required to represent a digital image and the basis of the reduction process is the removal of spatial and psychovisual redundancies. The compression can be lossless or lossy. If the reconstructed image from the compressed image is identical to the original image then it is a lossless compression otherwise it is a lossy compression.

However alone compression is not sufficient as it has an open access, anybody can access it. So if it is desired that it can be accessible only by authorized person it should be encrypted as well. The encryption can be performed either using Symmetric key cryptography or by using Asymmetric key cryptography. If same key is used for encryption and decryption then it is called as Symmetric key cryptography and if the different key is used for encryption and decryption then it is called as Asymmetric key cryptography.

The paper contains an approach to apply both image compression and image encryption. The general order followed by the researcher is CE i.e. compression followed by encryption. Very few authors first perform encryption. The order followed in this paper is EC i.e. encryption followed by compression. For encryption a private key cryptography using multiplicative inverse is applied. For compression Discrete Cosine Transform (DCT) is used.

The paper is organized as follows: Section 2 discusses the classification and description of image compression and encryption schemes used by researchers. Section 3 describes the proposed approach. Section 4 shows experimental setup and result. Finally in Section 5 the conclusion and future scope is described.

II. CLASSIFICATION AND DESCRIPTION OF RELATED WORK

The work on image compression and encryption performed by various researchers can be categorized in any of the following categories.

A. Compression followed by Encryption (CE)

In this sequence an intruder has less cleaves to access image but encryption may again increase the size.

B. Encryption followed by Compression (EC)

In this sequence size is not again increased but an intruder may have more cleaves to access the image.

C. Joint Compression and Encryption (JCE)

This approach is mostly used in recent days which may be fast as compared to previous two but procedure is complicated.

A. Research work on CE Approach

1. Howard Cheng and Xiaobo Li [1] performed compression using quad tree compression algorithm. And only partial encryption is applied. 13–27% of the output from quad tree compression algorithms and and less than 2% for 512X 512 images compressed by the SPIHT algorithm is encrypted**.** Limitation is that a different scheme has to be designed and analyzed for each compression algorithm.

2. A. Alfalou C. Brosseau *et al.* [2] performed compression based on the discrete cosine transform (DCT). Two levels of encryption are used. The first one is due to the grouping of the DCTs in the spectral domain and after a second transformation, i.e. to hide the target images, one of the input images is used as encryption key. The compression is better than JPEG in terms of PSNR. The proposed method achieves PSNR as 21.7186 as compared to that of JPEG as 20.6904 on applying on Lena image.

3. N.V.Thakur and O.G.Kakde [3] proposed the compression and encryption based on the fractal coding and spiral architecture but the compression method are lossy. Additionally to reduce time

complexity of fractal coding FFT based cross correlation is used. Any specific encryption method is not specified and any stream cipher algorithm can be used. Their experimental results are better than that of quadtree method w.r.t. PSNR ratio and encoding time.

The research work referred on CE approach is analyzed in table I.

TABLE I. ANALYSIS OF WORK ON CE APPROACH

Author	Compression	Encryption
[1]	Using Quadtree compression Algorithm	Set partitioning in hierarchical trees (SPIHT) algorithm.
[2]	based on the discrete cosine transform (DCT)	By grouping of the DCTs in the spectral domain and then hiding with an input image as encryption key.
[3]	Fractal coding is used. To reduce time complexity of fractal coding	Any stream cipher algorithm can be used. Regression can be used for

B. Research work on EC Approach

1. Mingyu Li *et al.* [4] used a RC5 stream cipher based scalable encryption scheme for low complexity transparent transcoding. CCSDS compression method is used which consist of two part DWT and Bit plane coding. Advantage is that Encryption is scalable.
2. V.Radha, D.Maheswari [5] proposed image encryption algorithm that consists of two parts: scrambling of plain-image and mixing operation of scrambled image using discrete states variables of chaotic maps. Discrete Cosine transform is used for compression. The proposed algorithm is strong in providing security and is also very fast. Since the key space is large therefore the attacker cannot decrypt an encrypted image without the correct key.

The research work referred on EC approach is analyzed in table II.

TABLE II. ANALYSIS OF WORK ON EC APPROACH

Author	Encryption	Compression
[4]	A RC5 stream cipher based scalable encryption scheme is used.	CCSDS compression method is used which consist of two part DWT and Bit plane coding.
[5]	By mixing operation of scrambled image using discrete states variables of chaotic maps.	Discrete Cosine transform is used.

C. JCE Approach

1. Alfalou et al. [6] used DCT to jointly compress and encrypt the image with a new system able to amalgamate spectral information. That spectral fusion, nondestructive, allows the compression and the encryption of information at the same time. Authors also showed that it is possible to use the DCT to jointly realize a compression and an encryption of the data by spectral fusion thus allowing a very important gain in transmission time.

D. Other Approach

1. Shiguo Lian *et al.* [7] proposed a totally different scheme. They carried out partial encryption before and after compression. JPEG is used for image compression. Using chaotic stream cipher encryption is carried out. Encryption consists of three parts: color plane Confusion, Sign encryption and DCT coefficient confusion space. They achieved the 75% compression ratio and 7.6%Encryption time ratio on Lena image of size 256×256.

III. PROPOSED APPROACH

In this paper simultaneous compression and encryption is applied on a gray level image. The order followed is EC i.e. Encryption is followed by Compression. For encryption and decryption the multiplicative cipher is used. And for compression and decompression DCT (Discrete Cosine Transform) is employed. The block schematic of the proposed approach is given in figure 1.

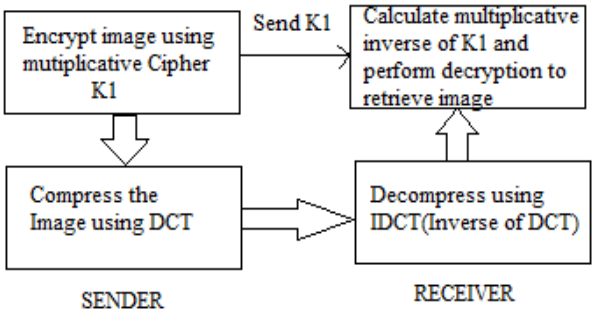


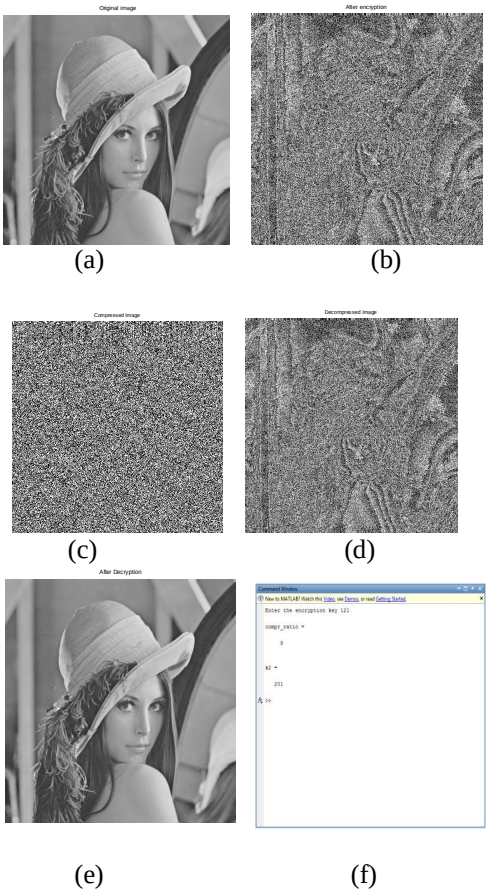
Figure 1. Block Schematic of the proposed approach

The steps followed are as follows.

1) Consider a standard gray level image for experiment.
2) Encrypt the image using multiplicative cipher at sender side.
3) Compress the output image got using DCT(Discrete Cosine Transform) at sender side.
4) Sender sends the image in both encrypted and compressed form to the Receiver.
5) Receiver first decompresses the image using IDCT(Inverse Discrete Cosine Transform).
6) Then receiver decrypts it using the multiplicative inverse of the key got from sender. Thus get the original image.

IV. EXPERIMENTAL SETUP AND RESULT

The proposed compression and encryption mechanism is implemented with MATLAB 2010 and windows 7 operating system with i5 processor and 4GB RAM. The experiments are carried out on 3 standard gray level images Lena.bmp Mandril.tif and Boat.gif of different formats. The compression ratio R is obtained as 8. Algorithm automatically generates the decryption key from the encryption key. The experimental results are shown through a to f in figure 3, 4 and 5 for Lena.bmp, Mandril.tif and Boat.gif respectively. The encryption keys used are 121, 127 and 135 respectively. The decryption keys given by the algorithm is 201, 127 and 55 respectively.

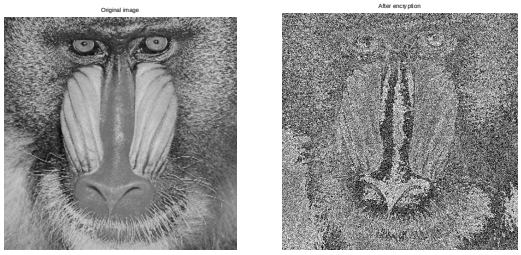


(a) (b)

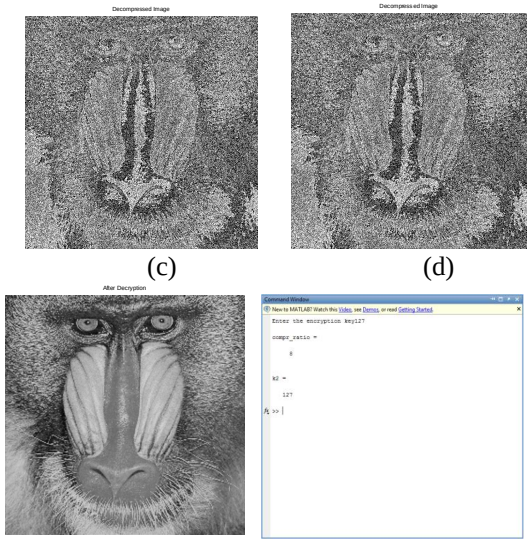
(c) (d)

(e) (f)

Figure 2 (a) Original Lena.bmp image (512×512) (b) After Encryption using key 121. (c) After Compression using DCT. (d) After Decompression using IDCT. (e) After Decryption using 201 as multiplicative cipher of the encrypted key. (f) Command window showing Decryption Key=201 and Compression Ratio=8.



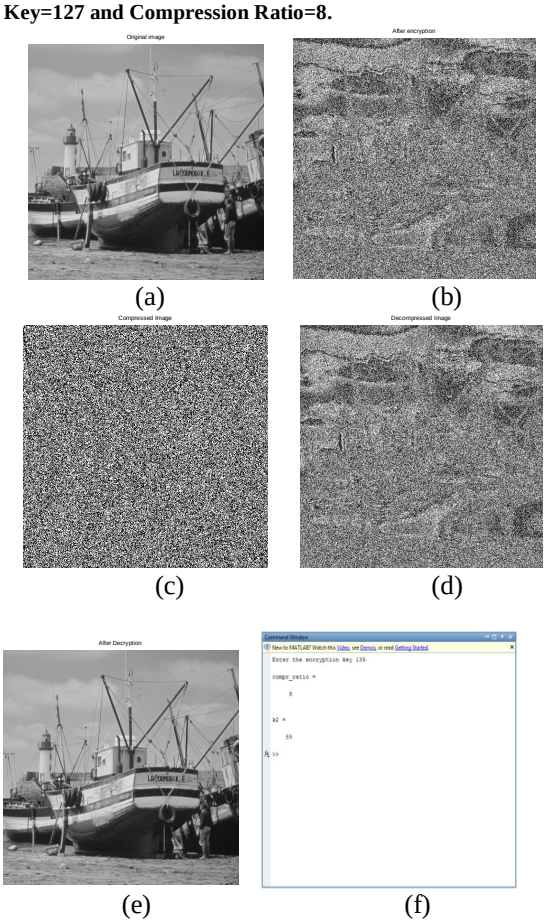
(a) (b)



(c) (d)

(e) (f)

Figure 3 (a) Original Mandril.tif image (512×512) (b) After Encryption using key 127. (c) After Compression using DCT. (d) After Decompression using IDCT. (e) After Decryption using 127 as multiplicative cipher of the encrypted key. (f) Command window showing Decryption Key=127 and Compression Ratio=8.



(a) (b)

(c) (d)

(e) (f)

Figure 4 (a) Original Boat.gif image (512×512) (b) After Encryption using key 135 (c) After Compression using DCT (d) After Decompression using IDCT. (e) After Decryption using 55 as multiplicative cipher of the encrypted key. (f) Command window showing Decryption Key=55 and Compression Ratio=8.

V. CONCLUSION AND FUTURE SCOPE

In this paper, many of the current important image compression and encryption techniques have been presented and analyzed. The best way of fast and secure transmission is by using compression and encryption of multimedia data like images.

The research works have been categorized in the following three categories based on the order of the two process viz. CE, EC or JCE.

The compression technique observed is either lossy or lossless. Always lossless compression is preferred but to achieve secrecy some image quality degradation is accepted.

Encryption applied by different researchers by means of encrypting algorithm which encrypt the entire or partial multimedia bit sequence using a fast conventional cryptosystem . Much of the past and current research targets encrypting only a carefully selected part of the image bitstream in order to reduce the computational load, and yet keep the security level high [8].

In the proposed approach the key is required to send separately. This is a different issue of securely transmitting the secret key. Future scope of the proposed work is that we can design the mechanism to securely transmit the key so that unauthorized person should have no access to it.

The performance evaluation factors are PSNR ratio and coding decoding time for compression and encryption respectively. But the balancing parameter for the combined process is not yet been defined.

It is important to note here that irrespective of the format of the input image the compression ratio given by the proposed approach using DCT is constantly 8. Since DCT consider the block of 8 × 8 pixels to accomplish compression.

REFERENCES

[1] Howard Cheng and Xiaobo Li, "Partial Encryption of Compressed Images and Videos" IEEE Transactions On Signal Processing, Vol. 48, No. 8, pp. 2439-2451, August 2000

[2] A. Alfalou C. Brosseau, N. Abdallah, and M. Jridi, "Simultaneous fusion, compression, and encryption of multiple images", OPTICS EXPRESS 24024Vol. 19, No. 24 OSA, 2011

[3] N.V.Thakur, and O.G.Kakde, "Compression Mechanism for Multimedia System in consideration of Information Security" Proceeding of International workshop on Machine intelligence Research MIR Day GHRCE-Nagpur, India, pp. 87-97, 2009

[4] Mingyu Li, Xiaowei Yi and Hengtai Ma, "A Scalable Encryption Scheme for CCSDS Image Data Compression Standard" 978-1-4244-6943-7/ IEEE pp. 646-649, 2010

[5] V.Radha, D.Maheswari, "Secured Compound Image Compression Using Encryption Techniques", 978-1-4244-5967-4/ IEEE 2010

[6] A. Alfalou, A. Loussert, A. Alkholidi, R. El Sawda, "System for image compression and encryption by spectrum fusion in order to optimize image transmission", ISEN-BREST Laboratory L@BISEN, France, IEEE, 2007

[7] Shiguo Lian, Jinsheng Sun, Zhiquan Wang, "A Novel Image Encryption Scheme Based-on JPEG Encoding", Proceedings of the Eighth International Conference on Information Visualisation (IV'04) 1093-9547/IEEE, 2004

[8] Monisha Sharma and Manoj Kumar Kowar, "Image Encryption Techniques Using Chaotic Schemes: A Review" International Journal of Engineering Science and Technology Vol. 2(6), ISSN: 0975-5462, pp. 2359- 2363, 2010