International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

An Efficient Method of Compressing Encrypted Images

Sathyalakshmi .L[1], Mohanarathinam .A[2]

[1]PG Scholar, ECE Department, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu 641032, India

[2]Assistant Professor, ECE Department, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu 641032, India

Abstract: ***In this paper proposes a novel scheme of compressing AES encrypted images. The content owner encrypts the original uncompressed images by double encryption methods. Then, the channel provider who cannot access the original content may compress the encrypted images by a quantization method with optimal parameters. At the receiver side, the principle image content can be reconstructed using the compressed encrypted image and the secret key. Experimental result shows the ratio-distortion performance of the proposed scheme is better than that of previous techniques.***

Keywords: Data Compression, Advanced Encryption Standard, Security, Compression-Ratio

1. Introduction

Compressing encrypted multimedia is an emerging technology aimed at reducing the data amount of cipher-text signals without revealing the plain-text context [1], [2], [3], [4]. In some scenarios that a content owner encrypts the uncompressed plain signals for privacy protection [4], the task of compression may be left to a channel or storage-device provider who has limited available resources but not the encryption key. After receiving the compressed encrypted data, an authorized user with secret key can reconstruct the plaintext content.

For the encrypted multimedia compression, the cipher-text signals can be viewed as the source, and the secret key. The goal is to efficiently compress the cipher-texts and to retrieve the plaintexts from compressed data by exploiting the side information. A number of practical schemes using Slepian-Wolf coding have been proposed. For example, the original binary image may be encrypted by adding a pseudorandom string, and the encrypted data compressed as the syndromes of low-density parity-check (LDPC) channel codes [2]. Compression of encrypted data for memoryless and hidden Markov sources using LDPC codes [5], and lossless compression for encrypted gray and color images using LDPC codes in various bit-planes [6] can be realized. In [7], encryption is performed on prediction errors rather than the image pixels, and LDPC codes are used to compress the cipher-texts. In [8], the encrypted image is decomposed in a progressive manner, and the data in most significant planes compressed using rate-compatible punctured turbo codes. The plaintext content can be perfectly decoded using some local Statistics obtained from a low-resolution version. In [9], a lossless compression method for cipher-texts encrypted by AES and cipher-block chaining mode is developed. In [10], after producing the cipher-text images by pixel-permutation, the encrypted data are compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. At the receiver side, the discarded rough information of coefficients is retrieved by an iterative procedure with the aid of spatial correlation in natural images so that the principle plaintext content is reconstructed. In another method of scalable coding for encrypted images, the original pixel values are masked by a modulo-256 addition to avoid leakage of statistical information, leading to better security. The more the available bit streams at receiver side, the higher the resolution of principle plaintext contents can be reconstructed. Although the performance of encrypted data compression may be as good as that of non-encrypted data compression in theory [1], the practical compression ratio-distortion performance is not up to that of the conventional compression methods.

This paper proposes a novel scheme of compressing encrypted images with comparison of AES and Chaotic Baker Map. In encryption phase, the original uncompressed images are encrypted by the content owner. In compression phase, the encrypted data in various DCT sub-bands are effectively compressed by using a quantization mechanism without revealing the original content, and an optimization method with ratio-distortion criteria is employed. At a receiver side with secret key, the principle plaintext content can be reconstructed. The experimental result shows the ratio-distortion performance of the double encryption methods.

2. Proposed Scheme

In the proposed system, a series of pseudorandom numbers derived from a secret key are used to encrypt the original pixel values [1]. After encryption, the image is compressed using DCT quantization method. When having the encoded bit streams and the secret key, a decoder can first obtain an approximate image by decrypting the quantized image and then reconstructing the detailed content using the quantized coefficients with the aid of spatial correlation in natural images.

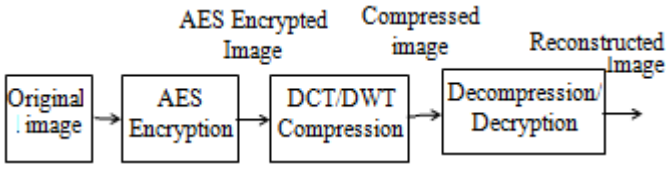

Figure 1: Block Diagram for AES Encryption Method

Licensed Under Creative Commons Attribution CC BY

A. AES Enccryption

AES is a symmetric block cipher with a block size of 128 bits. AES is based on a design principle known as a substitution-permutation network, combination of both software and hardware [1]. AES allows three different key lengths of 128, 192 or 256 bits. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher-text. Encryption consists of 10 rounds of processing for 128 bit keys, 12 rounds for 192 bit keys and 14 rounds for 256 bit keys. Except for the last round in each case, all other rounds are identical. Fig. 1 sketches the block diagram for double encryption methods.

Each round of processing includes one single byte based substitution step, row wise permutation step, a column wise mixing step and addition of round key. The order in which these four steps are executed is different for encryption and decryption. AES operates on a 4× 4 column-major order matrix of bytes. The 4×4 matrix of byte is referred to as state array. Each column or row of state array is a word.

Prior to the round based processing for encryption, the input state array is XORed with the first four words of the key schedule. The same process happens during decryption, except that the cipher text state array is XORed with the last four words of the key schedule.

For encryption, each round consists of the following four steps

1. Substitute Bytes
2. Shift rows
3. Mix columns
4. Add round key

The last step consists of XORing the output of the previous three steps with four words from the key schedule. The first three functions of an AES round are designed to thwart cryptanalysis via the methods of "confusion" and "diffusion." The fourth function actually encrypts the data. Diffusion means patterns in the plaintext are dispersed in the cipher text. Confusion means the relationship between the plaintext and the cipher text is obscured.

B. DCT Compression

The discrete cosine transform (DCT) helps separate the image into parts of differing importance. The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain.

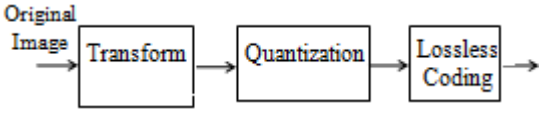

Figure 2: DCT Compression

A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio and, to spectral for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient, whereas for differential equations the cosines express a particular choice of boundary conditions.

C. DWT Compression

The wavelet transform (WT) has gained widespread acceptance in signal processing and image compression. Because of their inherent multi-resolution nature, wavelet-coding schemes are especially suitable for applications where scalability and tolerable degradation are important. Recently the JPEG committee has released its new image coding standard, JPEG-2000, which has been based upon DWT. Wavelet transform decomposes a signal into a set of basis functions. These basis functions are called wavelets. Wavelets are obtained from a single prototype wavelet y(t) called mother wavelet by dilations and shifting:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right) \quad \text{.....(1)}$$

where a is the scaling parameter and b is the shifting parameter.

The wavelet transform is computed separately for different segments of the time-domain signal at different frequencies. Multi-resolution analysis analyzes the signal at different frequencies giving different resolutions. MRA is designed to give good time resolution and poor frequency resolution at high frequencies and good frequency resolution and poor time resolution at low frequencies. It is good for signals having high frequency components for short durations and low frequency components for long duration like images and video frames.

3. Compression of Encrypted Image

When having the encrypted image, if the channel resource is sufficiently abundant so that any compression is needless, the channel provider may transmit the encrypted image directly. In this case, clearly, an authorized user with the secret key can decrypt the received data to retrieve the original image without any distortion. If the channel resource is limited, then perform a data-compression using a quantization method before transmission. The compression procedure is as follows. Actually, the compression will be performed in 64 DCT sub-bands with different quantization parameters. The channel provider firstly implements 2D DCT in the encrypted image with a block-by-block manner. Then, he reorganizes the coefficients in each sub-band as a vector, which is denoted as $[C^{(u,v)}(1),C^{(u,v)}(2),\ldots..,C^{(u,v)}(N_1N_2/64)]^T$ $(1\leq u,v\leq 8)$.

After that, perform orthogonal transform for the vectors. By using the orthogonal transform, the reconstruction error will be uniformly scattered over all the DCT coefficients in a same sub-band, leading to a reconstruction result with better visual quality. For each sub-band, the channel provider selects a positive real number $\Delta^{(u,v)}$ and a positive integer $M^{(u,v)}$, and calculates

$$Q^{(u,v)}(t) = \mathrm{mod}\left\{round\left[\frac{D^{(u,v)}(t)}{\Delta^{(u,v)}}\right], M^{(u,v)}\right\},$$

$1\leq u,v\leq 8,\ 1\leq t\leq N_1N_2/64$ .....(2)

Licensed Under Creative Commons Attribution CC BY

where the round operation returns the nearest integer and the mod operation gets a remainder.

4. Image Reconstruction

With the compressed data and the secret key, a receiver can perform the following steps to reconstruct the principal image content.

- Decompose the compressed data to get the encrypted image $c_D(i,j)$, the values of $[Q^{(u,v)}(1), Q^{(u,v)}(2),\ldots,Q^{(u,v)}(N_1N_2/64)]^T$, $\Delta^{(u,v)}$ and $M^{(u,v)}$, using inverse DCT.
- Decrypt the image $c_D(i,j)$ to retrieve the original image by AES decryption and Reversible Chaotic-Bakered Map.
- Calculate PSNR, MSE, BPP, Correlation Coefficients and Compression-Ratio for both AES Encrypted and Chaotic-Bakered image.
- Finally, compare the results.

5. Experimental Results

The test image Lena sized 512×512 was used as the original in the experiment. Certain parameters are used for the evaluation of AES and Chaotic-Bakered Map such as entropy, standard deviation, mean, correlation-coefficients, histogram, PSNR, compression-ratio and MSE.

A.Entropy

Entropy of a source gives idea about self-information i.e., statistical measure of randomness that can be used to characterize the texture of the input image. Encryption and Decryption produces the same result that means no loss of information. Information entropy is calculated by

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times log_2 \frac{1}{p(m_i)} \quad \ldots\ldots\ldots\ldots\ldots(3)$$

where p(mi) represent the probability of occurrence of the symbol mi.

***B.*Correlation Coefficient**

Correlation determines the relationship between two variables. In other words, correlation is a measure that computes degree of similarity between two variables. Correlation coefficient is calculated by

c.c = corr2(x, y) ……(4)

C. Compression-Ratio

Compression reduce storage space and transmission bandwidth. Some image encryption algorithms impact data compressibility or introduce additional data that is necessary for decryption process. DWT produces better compression ratio. Compression-ratio is given by

$$C.R = \frac{\text{Encrypted image}}{\text{input image}} \quad \ldots\ldots\ldots\ldots(5)$$

D. PSNR

Peak signal-to-noise ratio can be used to evaluate an encryption scheme, which indicates the changes in pixel values between the plaintext image and the ciphertext image. PSNR is calculated by

$$PSNR = 10 \log_{10}\left(\frac{255^2}{MSE}\right) \quad \ldots\ldots\ldots\ldots\ldots(6)$$

Table.1 shows the evaluated parameters difference between the AES Encrypted Image and Chaotic-Bakered Image. Fig. 3 shows the original image. Fig. 4 shows the AES Encrypted Image. Fig. 5 shows the compressed image. Fig. 6 shows the reconstructed image. Fig. 7 shows the histogram of original, AES Encrypted image and Reconstructed Image.

Table 1: Comparison of encrypted images

Encryption Technique/image	C.R	PSNR	C.C	Entropy
Modulo-256 Addition with DCT Compression	0.1955	30.13	0.0015	7.334
AES with DCT Compression	0.5012	30.06	-0.0019	7.334
AES with DWT Compression	0.8300	30.01	-0.0019	7.334

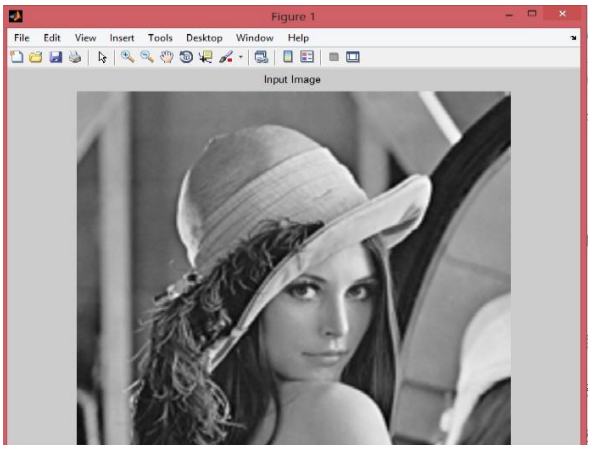

Figure 3: Original Image

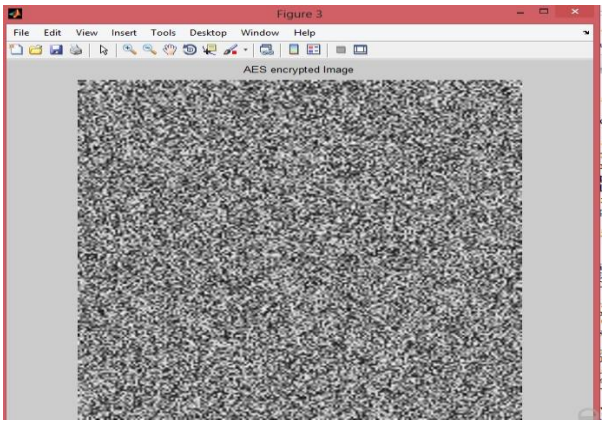

Figure 4: AES Encryption

Figure 5: Compressed image

Licensed Under Creative Commons Attribution CC BY

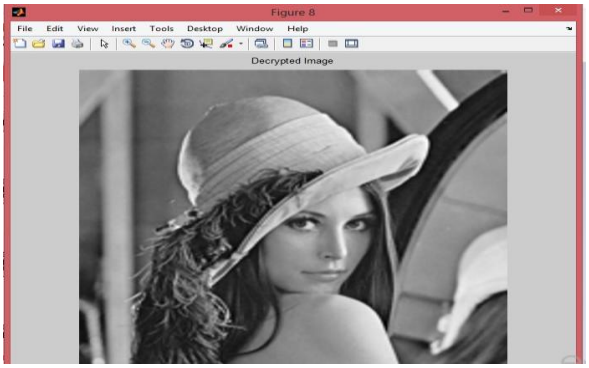

Figure 6: Reconstructed Image

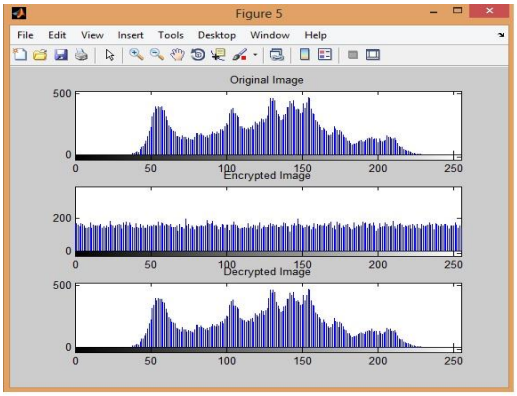

Figure 7: Histogram Analysis

6. Conclusion

This work proposes a scheme of compressing AES Encrypted Image. At receiver side, the principle image content can be reconstructed using the compressed encrypted data and the secret key. Compared with previous methods, the compression performance is therefore improved and the computational complexity is significantly reduced. Finally, we conclude with the remark that it is useful for real time image encryption and transmission applications.

References

[1] Xinpeng Zhang, Yanli Ren, Liquan Shen, Zhenxing Qian, and Guorui Feng,"Compressing Encrypted Images with Auxiliary Information," IEEEIEEE TRANSACTIONS ON MULTIMEDIA, VOL. 16, NO. 5, AUGUST 2014

[2] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[3] Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," EURASIP J. Inf. Security, pp. 1–20, 2007.

[4] N. S. Kulkarni, B. Raman, and I. Gupta, "Multimedia encryption: A brief overview," Recent Adv. Multimedia Signal Process. Commun., vol. SCI 231, pp. 417–449, 2009.

[5] D. Schonberg, S.C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in Proc. 43rd Annu. Allerton Conf., Allerton, IL, USA, 2005.

[6] R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and color images," in Proc. 16th Eur. Signal Processing Conf. (EUSIPCO 2008), Lausanne, Switzerland, Aug. 2008.

[7] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in Proc. IEEE 10th Workshop Multimedia Signal Processing, 2008, pp. 760–764.

[8] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Signal Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[9] D. Klinc, C. Hazayy, A. Jagmohan, H. Krawczyk, and T. Rabinz, "On compression of data encrypted with block ciphers," in Proc. IEEE Data Compression Conf. (DCC '09), 2009, pp. 213–222.

[10] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 53–58, 2011.

Licensed Under Creative Commons Attribution CC BY