International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.03, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Lossy Compression Approach of Compressing Encrypted Images

S.V.V.D.Jagadeesh[1], K. Raja Sravan Kumar[2]

[1,2]Dept. of IT, Aditya Engineering college., Surampalem, E.G.dt,AP, (India)

ABSTRACT

In this paper proposing a novel scheme of compressing encrypted images. In the encryption phase, the original pixel values are masked by a modulo-256 addition with nonrandom numbers that are derived from a secret key. After decomposing the encrypted data into a down sampled subimage and several data sets with a multiple-resolution construction, an encoder calculates the subimage and the Hadamard coefficients of each data set to reduce the data amount. Then, the data calculates subimage and coefficients are regarded as a set of bitstreams. Because of the hierarchical coding mechanism, the principal original content with higher resolution can be reconstructed when more bitstreams are received.

Keywords:Hadamardtransform, image compression, image encryption, scalable coding.

I.INRODUCTION

In recent years, encrypted signal processing has motivated to considerable research interests [1]. The discrete Fourier transform and adaptive filtering can be implemented in the encrypted domain based on the homomorphic properties of a cryptosystem [2], [3], and a composite signal representation method can be used to reduced the size of encrypted data and computation complexity [4]. In joint encryption and data hiding, a part of significant data of a plain signal is encrypted for content protection, and the remaining data are used to carry the additional message for copyright protection [5], [6]. With some buyer–seller protocols [7], [8], the fingerprint data are embedded into an encrypted version of digital multimedia to ensure that the seller cannot know the buyer's watermarked version while the buyer cannot obtain the original product on template base process. A number of works on compression encrypted images have been also presented. When a sender encrypts an original image for privacy protection, a channel provider without the knowledge of a cryptographic key and original content may be given to reduce the data amount due to the limited channel resource. In [9], the compression of encrypted data is looked into with the theory of source coding with side information at the decoder, and it is pointed out that the performance of compressing encrypted data may be as good as that of compressing non-encrypted data in theory. Two practical approaches are also given in [9]. In the first one, the original binary image is encrypted by adding a pseudorandom string, and the encrypted data are compressed by finding the syndromes of *low-density parity-check* (LDPC) channel code. In the second one, the original Gaussian sequence is encrypted by adding an independent identically distributed Gaussian sequence, and the encrypted data are quantized and compressed as the syndromes of trellis code. While Schonberg *et al.* [10] study the compression of encrypted data for memoryless and hidden Markov sources using LDPC codes, Lazzeretti and Barni [11] present several lossless compression methods for encrypted gray and color images

by employing LDPC codes into various bit planes. In [12], the encrypted image is decomposed in a progressive manner, and the data in most important planes are compressed using rate-compatible punctured turbo codes.

II.PROPOSED SYSTEM

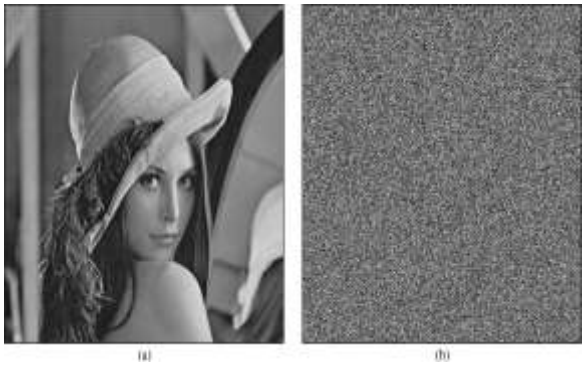
In the proposed system, a series of pseudorandom numbers derived from a secret key are used to encrypt the original pixel values. After decomposing the encrypted data into a subimage and several data sets with a multiple-resolution construction, an encoder quantizes the subimage and the Hadamard coefficients of each data set to effectively reduce the data amount. Then, the quantized subimage and coefficients are regarded as a set of bitstreams. When having the encoded bitstreams and the secret key, a decoder can first obtain an approximate image by decrypting the quantized subimage and then reconstructing the detailed content using the quantized coefficients with the aid of spatial correlation in natural images.

2.1 IMAGE ENCRYPTION

The original image is in an uncompressed
format and that the pixel values are within [0, 255], and denote the numbers of rows and columns as N1 and N2 and the pixel number as (N=N1 X N2). Therefore, the bit amount of the original image is 8N. The content owner generates a pseudorandom bit sequence with a length of 8N. Here, we assume the content owner and the decoder has the same pseudorandom number generator (PRNG) and a shared secret key used as the seed of the PRNG. Then, the content owner divides the pseudorandom bit sequence into N pieces, each of which containing 8 bits, and converts each piece as an integer number.

2.2 ENCRYPTED IMAGE ENCODING

Although an encoder does not know the secret key and the original content, he can still compress the encrypted data as a set of bitstreams. First, the encoder decomposes the encrypted image into a series of subimages and data sets with a multiple-resolution construction. The encoder transmits the bitstreams with an order. If the channel bandwidth is limited, the latter bitstreams may be abandoned.
A higher resolution image can be reconstructed when more bitstreams are obtained at the receiver side.

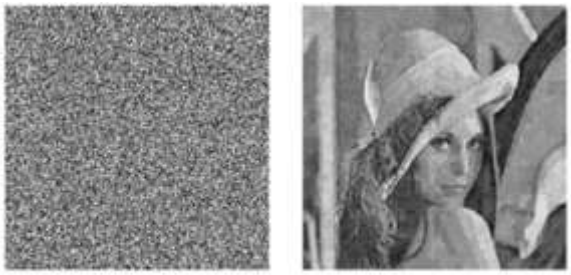


2.3 IMAGE DECRYPTION

This module is the opposite as such as Encryption module where the Key file should be also specified same as that of encryption part. Then the user should select the encrypted image and then should select the extract button so that the hidden message is displayed in the text area specified in the application or else it is extracted to the place where the user specifies it.

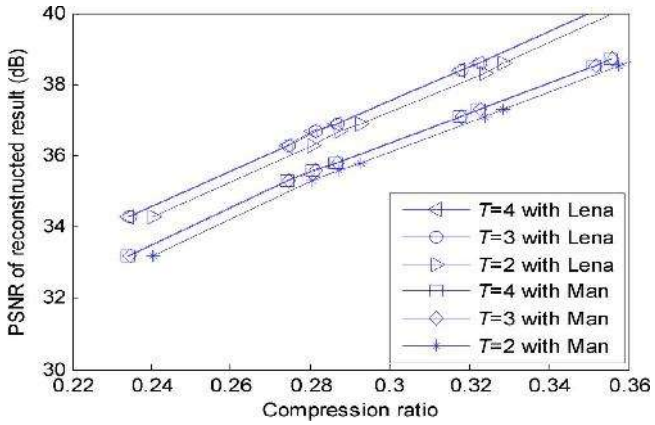
2.4 IMAGE RECONSTRUCTION

With the bitstreams and the secret key, a receiver can reconstruct the principal content of the original image, and the resolution of the reconstructed image is dependent on the number of received bitstreams. While BG provides the rough information of the original content, BS can be used to reconstruct the detailed content with an iteratively updating procedure.



(a) (b)

III.EXPERIMENTAL RESULTS



We also compare the proposed scheme with theprevious methods and unencrypted JPEG compression. Because it is difficult to completely remove the spatial data redundancy by the operations in the encrypted domain, the rate–distortion performance of the proposing scheme is significantly lower than that of JPEG compression. In this introducing scheme, the original values of all pixels are encrypted by a modulo-256 addition with pseudorandom numbers, leading to semantic security. That explains theproposing scheme is more suitable for real-time decompression and some scenarios without feedback channel.

ADVANTAGES

1. The subimage is decrypted to produce an approximate image; the quantized data of Hadamard coefficients can provide more detailed information for image reconstruction.

2. Bitstreams are generated with a multiple- resolution construction, the principal content with higher resolution can be obtained when more bitstreams are received.

IV. CONCLUSION

This paper has proposing a novel scheme for compressing encrypted images. The original image is encrypted by a modulo-256 addition with pseudorandom numbers, and the encoded bitstreams are made up of a quantized encrypted subimage and the quantized remainders of Hadamard coefficients. At the receiver side, while the subimage is decrypted to produce an approximate image, the quantized data of Hadamard coefficients can provide more detailed information for image reconstruction. Since the bitstreams are generated with a multiple-resolution construction, the principal content with higher resolution can be obtained when more bitstreams are received.

V.ENHANCEMENT

Proposing a lossy compression scheme for images having their pixel value encrypted with a standard stream cipher. Suppose the size of an original 8-bit grayscale image is $N1 \times N2$, its encrypted version is E. We downsample the encrypted image by a factor of two in both dimensions and generate four sub-images, denoted as $E00$, $E01$, $E10$ and $E11$. Here, the first digit "1"(or "0") denotes that the horizontal offset for downsampling is 1 (or 0) pixel, the second digit "1"(or "0") denotes that the vertical offset is 1 (or 0) pixel. The uncompressed $E00$ sub-image will be transmitted to the decoder. To compress, assume only $N = 2$ bit-planes of subimage $E11$ are transmitted. We denote the decimal value of $N = 2$ bits b7b6 as $w \in [0, 2N - 1] = [0, M - 1]$. Let Δ be the stepsize corresponding to the most significant bit-plane of the two bits, so $\Delta = 27$ when $N < 8$. The bit rate per information source bit (corresponding to compression rate) is $R = 0.25 + 0.25N / 8$. We predict every pixel of $E11$ using its four neighbor pixels with the context adaptive interpolation (CAI) scheme first. Then we match the bit-plane values (b7b6) of every CAI prediction pixel ($pred0$) with the received b7b6. If they match with each other, we accept $pred0$ as r, otherwise searching for the best-matching prediction among the interpolation values between every two pixels of its four neighbors.

REFERENCES

[1.] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2001.

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

[4.] 4. R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and color images," in *Proc. 16th EUSIPCO*, Lausanne, Switzerland, Aug. 2008 [Online]. Available:http://www.eurasip.org/Proceedings/Eusipco/Eusipco2008/papers/1569105134.pdf

[5.] 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.

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

[7.] A. Bilgin, P. J. Sementilli, F. Sheng, and M. W. Marcellin, "Scalable image coding using reversible integerwavelet transforms," *IEEE Trans. Image Process.*, vol. 9, no. 11, pp. 1972–1977, Nov. 2000.

AUTHOR'S PROFILES

Mr.S.V.V.D.Jagadeesh, is an Assistant Professor of Aditya Engineering College, IT Department Surampalem. He pursued his M.Tech [Computer Science & Engineering] from Aditya Engineering college in the year 2013 and he received his B.Tech from Godavari Institute of Engineering and Technology, affiliated to JNT University, Kakinada in the year 2009. His area of interest includes Image processing, Information Security and, all current trends and techniques in Computer Science.

Mr.K.Raja Sravan Kumar, well known Author and excellent teacher Received B.TECH and M.Tech (SE) from JNTUK university is working as Assistant Professor and, Department of IT, M.Tech Software engineering , Godavari Institute of Engineering and Technology, He is an active member of CSI,ISTE. .He has 6 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals . His area of Interest includes Image processing, flavors of Cloud Computing and Web technology and other advances in computer Applications.