A SURVEY ON SECURED IMAGE COMPRESSION

S. Shunmugan, Research Scholar, Manonmaniam Sundaranar University, Thirunelveli,
Email : shunsthc@gmail.com

Abstract - *In recent years, there is a rapid development in the multimedia and network technologies in computer era. Transmission of multimedia data over the network leads the major issues of security, privacy and data size. Security and privacy are not considered in the earlier Image compression techniques. To provide the privacy and security, the encryption is applied as well as compression reduces the data size. So that, to overcome the issues in multimedia and network technologies, compression is combined with encryption. Joint-Encryption-and-Compression (JEC) and Independent-Encryption-and-Compression (IEC) are the two types of secured compression algorithms. To provide secured and fast transmission of multimedia data, the encryption and compression processes are performed simultaneously in JEC. Various image encryption schemes are classified and reviewed in this paper, with respect to various parameters like Compression Ratio (CR), Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE), Time Consumption, Encryption Ratio, and Security techniques.*

Keywords – Encryption, Permutation, Randomization

1. Introduction

Nowadays, more and more sensitive images and videos are used in computer and transmitted over the internet and also people are offering web based learning through internet [1]. It needs to ensure information security and safety. Therefore, it is very important to protect the images with the information from unauthorized access.

Basically, Image Encryption is the process of converting an image into unreadable format (fig. 1) so that it can be transmitted over the network safely [2]. Its reverse process is image decryption, which is used to convert the unreadable format of an image to the original image and for this the receiver have to use the *key* for the encrypted data.

Original Image Encrypted Image

Fig. 1. Image Encryption

Image compression addresses the problem of reducing the amount of data required to represent a digital image. This process intended to yield a compact representation of an image by reducing the image storage size. Therefore the main aim of compression is to reduce the number of bits as much as possible while keeping the resolution and the visual quality of the reconstructed image as close to the original image as possible.

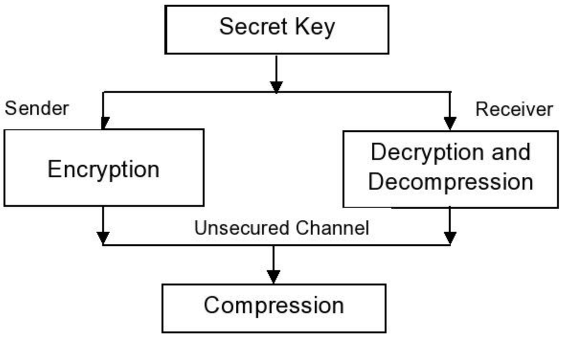

Fig. 2. Compression with encryption

When it is desired to transmit redundant data over an insecure and bandwidth-constrained channel, it is customary to first compress the data and then encrypt it and it is shown in fig. 2. In this paper, investigate the novelty of various secured compression schemes.

In this paper, the various types of secured compression techniques are narrated in section II and in section III a review of various types of Secured image compression techniques are discussed. Finally the general guidelines to be followed for secured image compression is concluded in section IV.

2. Types of Secured Compression

Secured compression scheme is divided into two types namely Independent-Encryption-and-Compression (IEC) [3] and Joint-Encryption-and-Compression (JEC). Further IEC is divided in to two types namely Compression before Encryption (CE) and Compression after Encryption (EC) and it is shown in fig 3.

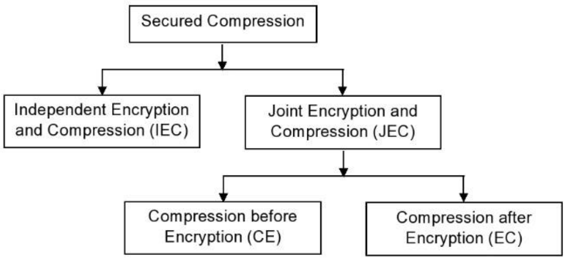
Secured Compression
Independent Encryption and Compression (IEC)
Joint Encryption and Compression (JEC)
Compression before Encryption (CE)
Compression after Encryption (EC)

Fig. 3. Secured Image Compression Technologies

In IEC, encryption and compression are taken place one after another. In CE compression, process is done first and then that data is encrypted subsequently. So the image size and the time consumption are reduced. Similarly in EC encryption, process is done first then that data is compressed subsequently. Here the consumption of time is more. In JEC, encryption and compression are taken place simultaneously. So the image size and the time consumption are reduced better than the earlier. It also provides better security.

3. Literature Review

Many secured data compression algorithms have been developed and used. Each and every algorithm has specific use to compress files of different types like text files, image files, video files, etc.

3.1. IEC Algorithms

A compression method with encryption, using the words (patterns or orders) by the SCAN language is presented by Nikolaos G. Bourbakis [4]. The SCAN is a formal language-based two-dimensional spatial-accessing methodology. A wide range of scanning paths or space filling curves can be generated efficiently in the SCAN language. Both binary and grey level images are compressed and encrypted in their methodology. Using fractal based language G-SCAN, the compression is done by Genetic Algorithm. Encryption is done by using transposition cipher based on SCAN. This method achieved 2.8:1 Compression Ratio.

A new lossless compression with encryption of binary and gray-scale images is presented by S.S.Maniccam and N.G. Bourbakis [5]. SCAN methodology is used for the compression and encryption schemes. For 512 x 512 gray scale Lena Image 50 seconds is consumed for compress-encrypt and 10 seconds is consumed for decompress-decrypt. This method achieved 1.6353 Compression Ratio.

A method combined compression and encryption based on Independent Component Analysis (ICA) and Discrete Cosine Transform (DCT) is proposed by Masanori Ito *et al*. [6]. This method covered target images with an insignificant image to hide them and their mixtures to be transmitted are obtained in encryption. The original images are reconstructed by applying some Independent Component Analysis (ICA) algorithm to the mixed images. DCT and simple low pass filter is used in Compression. In this method the quality of the original image is reduced by removing the higher frequency components.

A fault tolerant compression method with encryption using DWT (Discrete Wavelet Transform) and AES is proposed by Younggap You and Hanbyeori Kim [7]. It is suitable only for Medical image and videos. It is highly suitable to improve error avalanche effect for the erroneous bits in encrypted image data.

A secured compression based on the discrete cosine transform (DCT) is performed by Alfalou *et al.* [8]. Encryption is done in two levels. Grouping of the DCTs in the spectral domain is done in first level. In second level for transformation, one of the input images is used as encryption key. This method provides better PSNR than the standard JPEG for the Lena image. It achieved PSNR as 21.7186 and for JPEG it is 20.6904

A fast and secured compression method is proposed by Goh Han Keat *et al.* [9]. It is used to overcome the speed and the security of the existing conventional compression and encryption methods for real time images. For compression they applied Embedded Zerotree Wavelet (EZW) encoder and for encryption they used Stream ciphers RC4. They obtained better security level, and minimal space consumption. And the security feature is integrated with arithmetic encoding.

3.2. CE Algorithms

A compression after encryption is proposed by A. Kingston *et al.* [10] with the advantage of the Mojette transform properties. A cascade of Radon projection helps fast encryption of a large amount of digital data. They used AES, DES, 3DES and IDEA algorithms to encrypt very small percentages of high resolution images with the encrypted data. Entropy coding is used for lossless compression. The public key encryption algorithms, like RSA is used to reduce the percentage of encrypted data.

Distributed source coding is proposed on compression of encrypted data by Anil Kumar and Anamitra Makur [11]. They applied this method for both gray scale and color images for lossless compression on encrypted data. For compressing the cipher texts, they also applied encryption on the prediction errors instead of directly applying on the images and use distributed source coding. Decompression and decryption are combined as a single process. They obtained compression ratios varying from 1.5 to 2.5. For lena image this method obtained 5.39 BPP.

An orthonormal basis vectors encryption scheme with JPEG is proposed by Fawad Ahmed *et al.* [12]. The cipher-image data is compressed using JPEG lossy compression to recover the plaintext-image. By adjusting the values of the encryption method, various levels of secured image can be generated.

A RC5 stream cipher based scalable encryption scheme with CCSDS compression method is proposed by Mingyu Li *et al.* [13]. It is used for low complexity transparent transcoding. The DWT and Bit plane coding are done in CCSDS. The Scalability of Encryption is the specialty of this method.

Slepian-Wolf coding encryption with progressive lossless compression is proposed by Wei Liu *et al.* [14]. In progressive compression, the decoder can observe a low-resolution image. This method saved 70% to 90% compression rate of the optimal conventional intra-frame coder in spite of inefficient channel codes. It has a better coding performance

An image encryption algorithm followed by compression algorithm is proposed by Radha and Maheswari [15]. Encryption process is divided into two parts. In the first stage the plain image is scrambled and in the second stage the scrambled image is combined using discrete states variables of chaotic maps. By using DCT the compression is done. Since the key space is large, the attacker cannot decrypt an encrypted image without the correct key, so this method is highly secured with greater speed.

3.3. EC Algorithms

A simultaneous compression and encryption method is proposed by Vikram Jagannathan, *et al.* [16]. In this method a new Congruence theory and Chinese Remainder Theorem are used. It achieved 1.85 better compression ratio on Lena image than Huffman and LWZ. The proposed method has better security despite the performance.

A jointly compression and encryption using DCT is proposed by Alfalou *et al.* [17] to amalgamate spectral information. Simultaneously a nondestructive compression and the encryption of information are obtained by the spectral fusion. This method shown the amalgamation of spectral fusion that is more important in gaining transmission time.

An OMHT (Optimized Multiple Huffman Tables) technique used multiple Huffman tables which is generated for grayscale and color image is proposed by Shaimaa *et al.* [18]. In this method, a highly secured performance with better compression ratio especially at low bit rate is obtained than MHT and JPEG. The encryption cost of OMHT is lesser than COS cryptographic cipher.

A simultaneous compression and encryption by using Alpha rooting method is proposed by Eric Wharton *et al.* [19]. Despite computational complexity and compression ratio, it achieves a better compression. The magnitudes of the coefficients are reduced in Alpha rooting functions. For Lena image, compression ratio 6.0845:1 is obtained.

Simultaneous Vector Quantization and Selective Encryption is proposed by Yassin *et al.* [20]. For compression a nonstandard asymmetric lossy image compression technique is applied. And for Encryption, a simple encryption algorithm to pseudo randomly shuffle the indices of the codebook before performing VQ technique is applied. SE scheme selectively encrypts ~8% to ~13% of the compressed bit stream by either full indices or both full indices using prediction tables respectively.

Both compressing and encrypting the image using the set partitioning in hierarchical trees (SPIHT) & Encryption is based on feed forward-feedback nonlinear dynamic filter (FFNDF) is proposed by Li Hengjian *et al.* [22] . For encryption RAC is applied to generate key. The combined methods obtained modern functionalities, such as selective encryption, total encryption and conditional access.

4. Conclusion

Various independent-encryption-and-compression and joint-encryption–and-compression techniques are reviewed and the results obtained are discussed in this paper. And also, it gives a clear idea about the need of security and privacy in compression techniques. Every technique is having its own pros and cons. It is evident from the reviewed papers that the joint-encryption-and-compression technique provides a better performance in privacy and security, speed and compression. It is concluded that the quality of the privacy and security is measured by the encryption ratio which is a security technique and the quality of image can be measured by PSNR, MSE and CR. A new compression technique with more privacy and security is needed to improve the performance to cope with the current changes.

References

[1] Afolabi, A.O. and Adagunodo, “Implementation of an improved data encryption algorithm in a web based learning system”, Phys. Int., 2: 31-35. DOI: 10.3844 / pisp. 2011.31.35, 2011.

[2] Yuan Yan Tang, *Fellow, IEEE ”* Designing an Efficient Image Encryption-Then Compression System via Prediction”, IEEE, *2011,*

[3] Lier P., Moury, G., Latry C., and Cabot F., “Selection of the SPOT-5 image compression algorithm” in Earth Observing Systems III” (W.L.Barnes, ed.), vol. 3439-70, pp. 541, San Diego, CA, SPIE, Oct 1998.

[4] Nikolaos G. Bourbakis, “Image Data Compression-Encryption Using G-Scan Patterns”, *IEEE 0-7803-4053-1/97*, pp. 117-1120, 1997.

[5] S. S. Maniccam, and N. G. Bourbakis, “SCAN Based Lossless Image Compression and Encryption”, *IEEE 0-7695-0446-9/99*, pp. 490-499, 1999.

[6] Masanori Ito, Noboru Ohnishi, Ayman Alfalou and Ali Mansour, “New Image Encryption And Compression Method Based On Independent Component Analysis”, *IEEE*, 2007

[7] Younggap You, Hanbyeori Kim, “Endoscopy Image Compression and Encryption under Fault Tolerant Ubiquitous Environment”, 978-1-4244-4918-7 *IEEE*, pp. 165-168, 2009

[8]. 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

[9] Goh Han Keat, Azman Samsudin and Zurinahni Zainol, “Enhanced performance of secure image

using Wavelet compression", Universiti Sains Malaysia (USM), pp. 71-74, 2005

[10] A. Kingston, S. Colosimo, P. Campisi, F. Autrusseau, "Lossless Image Compression And Selective Encryption Using A Discrete Radon Transform", *IEEE-1-4244-1437-7/07*, ICIP, pp.IV 465-468, 2007

[11] Anil Kumar A and Anamitra Makur, "Distributed Source Coding based Encryption and Lossless Compression of Gray Scale and Color Images" ,*IEEE978-1-4244-2295-1*, 760 MMSP Singapore, pp. 760-764, 2008

[12] Fawad Ahmed, M Y Siyal and Vali Uddin Abbas, "A Perceptually Scalable and JPEG Compression Tolerant Image Encryption Scheme", Fourth Pacific-Rim Symposium on Image and Video Technology *978-0-7695-4285-0/ IEEE* pp. 232-238, 2010

[13] 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

[14] Wei Liu, Wenjun Zeng, Lina Dong and Qiuming Yao," Resolution-progressive Compression of Encrypted Grayscale Images", University of Missouri, Columbia MO 65211, USA, 2007

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

[16] Vikram Jagannathan, Aparna Mahadevan, R. Hariharan and E. Srinivasan, "Number Theory Based Image Compression Encryption and Application to Image Multiplexing" ‖ *IEEE - ICSCN 2007*, pp.59-64, 2007.

[17] 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

[18] Shaimaa A. El-said Khalid F. A. Hussein Mohamed M. Fouad, "Securing Image Transmission Using In- Compression Encryption Technique" *International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (5)* pp. 466-481, 2010

[19] Eric Wharton, Karen Panetta, and Sos Agaian, "Simultaneous Encryption / Compression of Images Using Alpha Rooting", Data Compression Conference 1068-0314/*IEEE* pp 551, 2008.

[20] Yassin M. Y. Hasan, Mohammed F. A. Ahmed, and Tarik K. Abdelhamid, "Image adaptive selective encryption of vector quantization Index compression" *978-1-4244-5654-3/09IEEE* pp. 1277-1280 ICIP 2009.

[21] Li Hengjian, Wang Jizhi, Wang Yinglong and Tian Min Xu Shujiang, "A flexible and secure image compression coding algorithm", *International Conference on Future Information Technology and Management Engineering* 978-1-4244-9088-211 0/ IEEE pp. 376-379, 2010.

S. Shunmugan received the M.C.A degree from Manonmaniam Sundaranar University, Tirunelveli in 1999, M.Phil (Computer Science) degree from Manonmaniam Sundaranar University, Tirunelveli in 2004 and M.E (Computer Science & Engineering) degree from Manonmaniam Sundaranar University, Tirunelveli in 2013. He is working as Assistant Professor of Computer Science, at S.T.Hindu College, Nagercoil since 2001. His current research interest include signal or image processing, medical imaging, and biometric imaging.