Arrasikhun International Journal, Volume 4, Issue 1, June 2018
ISSN: 2462-2508

Selective Image Encryption and Compression Technique: Review

Shadi M S Hilles[1], Mahmood Abdullah Salem[2]
[1,2]Computer Science department, Faculty of Computer & IT,
[1, 2] Al Madinah International University,
Kuala lumpur, Malaysia
[1]shadihilless@gmal.com, [2]mahmodalattas0@gmail.com

Abstract

In line with a growing need for data and information transmission in a safe and quick manner, The security becomes an important issue of communication and storage of image due to the growth of multimedia application. Encryption is one of the ways to ensure high security. Images are used in many fields such as military and medical science. researches on image protection and security through a combination of cryptographic and compression techniques begin to take form. The combination of these two methods may include into three categories based on their process sequences. The first category, cryptographic technique followed by compression method. The second combination, compression technique followed by the cryptographic method, has an advantage where the compression technique can be lossy, lossless, or combination of both. The third category, i.e. compression and cryptographic technologies in a single process either partially or in the form of compressive sensing .
Keyword: compression, Image, encryption

1. Introduction

In recent years, encrypted signal processing has attracted many research interests .based on the homomorphism properties of a cryptosystem, the discrete Fourier transform and adaptive filtering can be implemented in the encrypted domain and to reduce the complexity of a composite signal representation the method can be used. A part of significant data of a plain the signal is encrypted for the purpose of the content protection and the remaining data are used to carry them additional message for copyright protection, in joint encryption and data hiding.

A number of works on encrypted compressing have been also presented. When an the original image is encrypted by a sender for privacy protection, a channel provider without the knowledge of a cryptographic key and the original information may reduce the information amount due to the less number of channel resource. In the compression of encrypted data is analyzed with the theory of source coding and decoder. So it represents the performance of compressing encrypted data may be good when compare with the compressing non-encrypted data.

Image compression by using reversible integer wavelet transforms has several advantages. The most important one is through the use of suitable techniques, a full bit stream can be generated. And also, the decoder can extract a loss version of the image, continue to decode at higher rates until the image is perfectly reconstructed. But this technique contains the major disadvantage that, if resolution scalability is not desired instead, the decoder can't extract a low resolution version of image and continue to decode the bit stream.

In an encrypted image is decomposed in a progressive manner by using rate-compatible punctured turbo codes, the data in most significant planes are compressed, based on local statistics of a low-resolution the version of the image. Furthermore, loss compressive encrypted images have been developed, by using several methods. in with the help of pixel permutation, the original grayscale image is encrypted then the encrypted data are compressed by removing rough and fine information of coefficients generated from orthogonal transform.

However, encryption rate-distortion performance is low and which has the leakage of statistical information. In binary images are converted into binary phase encoded pixels and which are encrypted by binary random phase XOR operation. But the security of this technique is very less when compared with the encryption in the compressed domain.

So to overcome the above disadvantages a new scalable coding algorithm is used for image compression and encryption. This paper proposes a novel scheme of scalable coding for encrypted gray images. The pixel values are completely concealed in the encryption phase of the proposed scheme. So that an attacker cannot obtain any statistical information from its original image. Then, the encrypted data are decomposed into several parts; bit stream is achieved by combining each part.

At the receiver side with the help of the cryptographic key, if the more bit streams are received the original content will be reconstructed with a higher resolution.

The rest of this paper is ordered as follows.

In Section II a brief review of encryption for an uncompressed image is given. In Section III the proposed scalable coding algorithm is introduced and discussed by calculating its performance factors.

Finally, some conclusions and future avenues for research are represented in Section IV.

2. Encryption technique

Selective chaos-based image-encryption and compression algorithm. The block diagram of this algorithm is shown in Figure 1. The encryption and compression operations is shown in Figure 1(a). First, we have set the chaotic map parameters (the initial values) as well as to select the external encryption keys.

The chaos-based encryption algorithm is as follows: after wavelet transformation, an amount of 25% (in case of one-level decomposition) or 6.25% (in case of two-level decomposition) of the original image, which corresponds to the important part, is transformed into one-dimensional vector with a dimension equal to the important part size, let us call it .

The chaotic map will be run for iterations and generate a vector of ones and zeros of dimension equal to

Too, it will be called a threshold vector, then the pixels of the image vector will be encrypted with one two, or three external encryption keys according to that threshold vector.

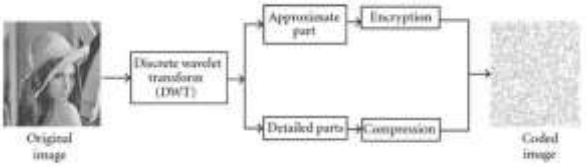

Fig 1: (a) The process flow of the encryption and compression operations

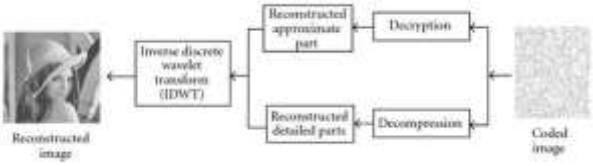

Fig 1: (b) The steps of decryption and decompression taken to reconstruct the image

From Figure 1(b), the secret image of size (128×128) pixels is decomposed using discrete wavelet transform (DWT). In practice, this process of decomposition usually repeated n times, and it is repeated just on the LL-sub band as mentioned for octave-band decomposition. Here in this work, the decomposition will be for one-level or two-level decomposition in order to compare different amounts of encrypted data and examine their effect on security. The image is decomposed into four sub images:

The approximation component (LL) and three detail components (horizontal, vertical, and diagonal). The most important component, the LL component, is then encrypted using a chaos-based image-encryption algorithm, and the other three components are subsequently compressed using wavelet analysis. The implementation of the algorithm achieves high

Encryption rates, as discussed in Section 5. The steps of decryption and decompression taken to reconstruct the image are described at Figure 1(b).

2.1. Encryption for uncompressed images technique

A secure computing environment is completed only by considering encryption technology.

The term encryption refers the original information can only be decoded, read and understood by people for whom the information is intended. It is the process of encoding data to prevent unauthorized parties from viewing or modifying it. Encryption is used to provide highest levels of security to network communication, email, files stored on hard drives or floppy disks, and other information that requires protection.

By generating key we can provide the higher security. Only an authorized person can use the key value to encode or decode the original content. Keys are denoted in different forms such as passwords, numbers which are generated by an algorithm. By using key value sender and recipient of message can understand how the message can be encrypted. By using the key value recipient can properly decode the message.

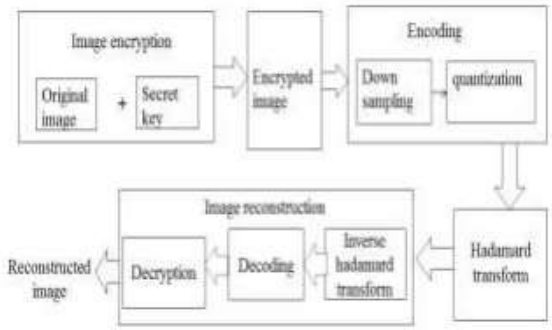

Fig.2: Block Diagram Of Scalable Coding Algorithm

Initially original image pixel values are added with the pseudo random numbers. Here XOR operation is done to add the every pixel values of original image with the pseudo random bit sequence. After that encrypted image is given to the encoding operation. In this phase down sampling is done to reduce the sampling rate of encrypted image. Then quantization is done to round off the encrypted pixel values into its nearest integer pixel values.

Then Hadamard transform is applied to compress the encoded bit streams. Transform is basically a mathematical tool, which allows us to move from one domain to another domain to perform the task at hand in easier manner. The transformation may place the image data in a more compact form so that they can be stored and transmitted efficiently.

Transforms play a major role in various image processing applications such as image analysis, image enhancement, and image filtering and image compression. After that inverse Hadamard transform

is applied at the receiver side to get back the uncompressed encrypted image. Then decoding is done covert data into its original format after that by using secrete key in decryption phase original image is reconstructed.

2.2. The procedure of sorting out literature

In line with a growing need for data and information transmission in a safe and quick manner, researches on image protection through a combination of cryptographic and compression techniques begin to take form. Combination of these two methods may be classified into three categories based on their processual sequences: a cryptographic technique followed by a compression technique [encryption compression], a compression technique followed by a cryptographic method [compression-encryption], and both techniques employed in a single process [hybrid compression encryption].

The procedure type of literary works is done by seeking out articles in journals and conference proceedings, published from 2004 up to 2016. This searching uses ontology of hybrid image compression encryption mapped and taken from several sources: IEEEXplore Digital Library(IEEEXplore), Science Direct(Direct), Springer, Scholar and other journals and proceedings outside IEEEXplore, Direct, Springer, Scholar, and others. This procedure results in 64 articles with the following details: IEEEXplore (10 articles), Direct (11articles), Springer (17 articles), Scholar (20 articles), and others (6 articles). Step two: 64 articles is classified into 3 (three) based on their techniques: compression-encryption, encryption-compression, and hybrid compression encryption. Classification of those articles results in 47 (73.44%) relevant articles as shown in Fig 3.

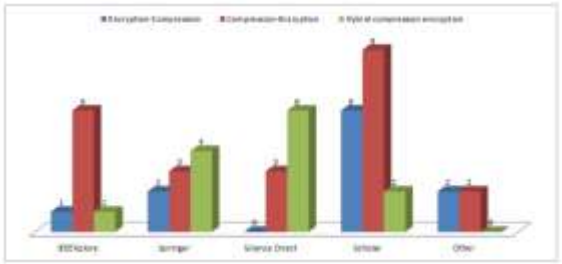

Fig. 3. Articles sorted by classification

Analytical result of 47 articles can be classified into three groups as shown in Fig 2. There are 11 articles (23.40%) in the First group discussing the development of cryptographic techniques followed by compression techniques.

The second group of 23 articles (48.94%) discusses the development of compression techniques followed by cryptographic techniques. The third group of 13 articles (27.66%) presents the combination of both techniques.

Conclusion

The most combination of Encryption-Compression the technique discussed above uses symmetric cryptographic and lossless compression method. In fact, it shows that the process focuses more on image security than on data size reduction.

The application of the lossless compression technique is to ensure that all data is reversible and can be reverted to the original while maintaining the high quality of reconstructed images and compression ratio. As such, this concept is most applicable when data accuracy is of paramount importance, such as textual information, biomedical image, and legal data. The majority of the measurement of the quality of the decompression image against the original image, the compression ratio, as well as the processing time, are used to measure the success of the proposed method, while the measurement results cipher visual image is used to analyze the level of security of some of the proposed method. The combination of Compression-Encryption technique has some advantages because compression method can be lossy, lossless, or combination of both. In contrast, most cryptographic techniques use symmetric cryptography by developing a chaotic method to generate a symmetric key.

As such, this approach applies to data image, either audio or video. Conversely, the proposal to use various chaotic methods aimed at generating a symmetric key to enhancing its security.

The hybrid compression-encryption technique is capable of providing real data security assurance with such a low the computational complexity that it is eligible for increasing the efficiency and security of data/information transmission.

So the concept qualifies for and could improve transmission efficiency and data security by improving the performance of each compression and cryptographic technique through hybrid concept.

This concept is expected to be able to combine excellent properties of lossy and lossless compression techniques and to offset the downside of symmetric and asymmetric cryptographic techniques, particularly about cipher key management, to obtain the much smaller size of data, still good quality of data during reconstruction and security assurance

References

[1]. P Refregier, B Javidi - Optics Letters, 1995, “Optical image encryption based on input plane and Fourier plane random encoding , https://scholar.google.com

[2]. J Zhou, X Liu, OC Au, YY Tang - IEEE Trans. information, 2014, “Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation., https://scholar.google.com

[3]. H. Hossam El-din, H. M. Kalash, and O. S. Farag Allah, “An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption, https://scholar.google.com

[4]. Advances in Optics and Photonics, 2009, “Optical image compression and encryption methods , https://scholar.google.com

[5]. L. Qiao and K. Nahrstedt, "Comparison of mpeg encryption algorithms, https://scholar.google.com
[6]. B. Bhargava, C. Shi, and S. Y. Wang, "MPEG video encryption algorithms," Multimedia Tools and Applications. https://scholar.google.com
[7]. J. But, "Limitations of existing MPEG-1 ciphers for streaming video," Tech. Rep. Swinburne University, Melbourne, Australia, April 2004. https://scholar.google.com
[8]. Hilles, S., & Maidanuk, V. P. (2014). Self-organization feature map based on VQ components to solve image coding problem. ARPN Journal of Engineering and Applied Sciences. Vol. 9,№ 9: 1469-1475.
[9]. Hilles, S. M., & Hossain, M. A. (2017). English Steganography Techniques: A Review Paper. International Journal on Contemporary Computer Research (IJCCR), 1(3), 22-28.
[10]. Hilles, S. M., & Hossain, M. A. (2018). Classification on Image Compression Methods. International Journal of Data Science Research, 1(1), 1-7.
[11]. Mady, H. H., & Hilles, S. M. (2017). Efficient Real Time Attendance System Based on Face Detection Case Study "MEDIU Staff". International Journal on Contemporary Computer Research (IJCCR), 1(2), 21-25.
[12]. Майданюк, В. П., Мазін-Хіллес, Ш., & Мельник, С. В. (2004). Кодування зображень з використанням SOFM. Інформаційні технології та комп'ютерна інженерія, 1(1), 49-52.
[13]. Hassan, S. S. M., & Hilles, S. M. (2014). Enhancing Security Concerns in Cloud Computing Virtual Machines:(Case Study on Central Bank of Sudan).