INTERNATIONAL JOURNAL OF DATA SCIENCE RESEARCH

IJDSR, Volume 1, Issue 2 March 2018,
Al-Madinah International University
Malaysia

Image Compression and Encryption Technique: Review Paper

Shadi M.S. Hilles[1], *Mohd Shaifulnizam Shafii*[2]

[1] *Faculty of Computer and Information Technology, Al-Madinah International University (MEDIU), Malaysia, shadihilless@gmail.com*

[2]*Faculty of Computer and Information Technology, Al-Madinah International University (MEDIU), Malaysia, fibonac32@gmail.com*

Abstract

Compression is reducing size of data for storage and transmission bandwidth. Image compression technique is lossless and lossy, the technique is to keep or reduce output of decompress format compare to original source. The lossless and lossy compression technique will have their process and algorithm to completed their objective compression and decompression. Encryption is about securing image exchanging via internet, thus prevent to be accessed by unauthorized users. Basic encryption method is symmetric and asymmetric.

Keywords: *Image, Compression, lossless, lossy, encryption, symmetric, asymmetric*

1. INTRODUCTION

Compression is the process or reduction data file size. Compression give benefit in term of less storage, faster transmission and faster to read or write file. Huge data file size is compressed to smaller one for the compressed data file transfer over minimum or limited network bandwidth. Thus real-time application, huge data size is possible to transfer over the internet around the world. Data compression is performed on several types of media source from text, speech, audio, image and video.

Image exchanging in public internet platform became practice now as it is fast and easy to share. However, the transfer of image via internet has security concern, which someone not in recipient of image transferring activity may intercept to get the image without permission. Thus, image encryption is necessary and needed in exchanging image via internet or sharing application medium. Encryption method can be categorised Symmetric and Asymmetric. Symmetric key encryption is encryption use single key for both the encryption and decryption process while Asymmetric key encryption use two keys which is private key and public key.

Compression and encryption are interconnected with each other. Their objective to reduce image file size, retain quality in reconstruction image from compression, manageable in available transmission bandwidth and secured during transferring.

2. LITERATURE REVIEW

2.1 Image Compression

Compression has two methods which are lossless and lossy. Lossless compression is where compressed data retain its original format without loss of information, while lossy compressed data will lose some original information but the loss is small to noticeable by human sense of eye and ear. Lossless compression is used for critical mission application such financial document and lossy is for application can be tolerated in slightly loss of information such as pictures. Compression required algorithm and several prominent compression algorithm techniques such as the Huffman, Run Length Encoding, arithmetic, and entropy. Image compression is data compression to reduce size of digital image. The format of compression image is GIF, PNG, JPEG and more on.

Table 1: Lossy and Lossless comparison

Features	**Lossy**	**Lossless**
Image reconstruction	Quality degraded compare to original image source	Quality remain the same with original image
Compression size rate	High compression up to 50% of original data file size	2:1 , the most is 3:1 ratio

2.2 Image Encryption

Symmetric key encryption is encryption use single key for both the encryption and decryption process. Example encryption using symmetric key are AES and DES. For example to transfer file from sender PC to receiver PC, one of the PC should first generate key and then share the key copy to another PC. Thus both PC sender and PC receiver have the same key copy. The PC sender will use the key for encrypting the file, while the receiver will use the key to decrypting the file.

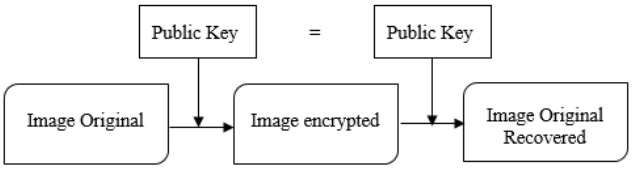

Figure 1: Symmetric encryption

While Asymmetric key encryption use two keys which is private key and public key. The public key use for encrypting while the private key use for decrypting. Example encryption using asymmetric key algorithms are RSA and DSA. For example to transfer file, PC server need to generate the key pair once another PC wants to encrypt file first before uploading to the PC server, the PC server will send the public key to another PC and private key will stay on the PC server. Thus, another PC sender will have public key and PC server receiver will have private key.

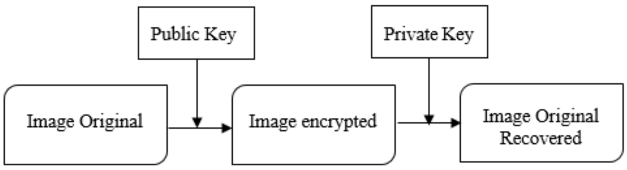

Figure 2: Asymmetric encryption

Concluded based on the above key operation, symmetric key encryption required less CPU computation compare to asymmetric key encryption, thus symmetric key encryption is faster. In term securing file transfer, symmetric key encryption has major disadvantage because it use same key to encryption and decryption, thus the same key caused difficulty to distributed the key safely.

2.3 Image Compression and Encryption Categories

Combination of image compression and encryption can be categorised to compression followed by encryption (CE), encryption followed by compression (EC) and joint Compression and encryption (JCE). Details as follow:

2.3.1 Compression followed by Encryption (CE)

The approach an invader have less cleave to access the image but due to compression followed by encryption the size of the image may be increased. Some research work on CE method:

Table 2: Compression followed by Encryption (CE) summary

No.	Author, Year	Compression	Encryption	Compression Method	Encryption Method
1	Kumar and Vaish [8], 2017	Lossy, Lossless	Symmetric	DWT, SVD, Huffman	Stream Cipher
2	Tong et al.[9], 2016	Lossy, Lossless	Symmetric	LWT, SPIHT	Stream Cipher
3	Chal.la et al.[10], 2015	Lossless	Asymmetric	CNA	LWE and Public Key

2.3.2 Encryption followed by Compression (EC)

The approach size is not been increased but due to encryption followed by compression an invader can access the image due to more clues. The research work:

Table 3: Encryption followed by Compression (EC) summary

No.	Author, Year	Compression	Encryption	Compression Method	Encryption Method
1	Mariselvi and Kumar[14], 2014	Lossless	Symmetric	RPC (Huffman or Arithmetic Coding	DES
2	Kale et al. [15], 2014	Lossless	Symmetric, Asymmetric	Shanon Fano	RSA, 3D-AES
3	Aujla and Sharma[16], 2014	Lossy	Symmetric	DWT (Haar and Daubechies)	Random Permutation

2.3.3 Joint Compression and Encryption (JCE)
The procedure of this approach is complicated and is recently used but it is faster as compared to previous two approaches CE and EC.

Table 4: Joint Compression and Encryption (JCE) summary

No.	Author, Year	Compression	Encryption	Compression Method	Encryption Method
1	Hamdi et al.[13], 2017	Lossy, Lossless	Symmetric	DWT, SPIHT	Confusion and Diffusion Technique Which is Integrated and Connected to Compression Chains
2	Xiaoyong et al.[12], 2016	Lossy, Lossless	Symmetric	DCT, Quantization, Ziqzaq Scan, Entropy Coding	Selective Encryption , NGKT
3	Wang et al. [11], 2015	Lossy, Lossless	Symmetric	LS DCT, DWT, Quantization and Adaptive Arithmetic Coding	Selective Encryption (Stream and Permutation Ciphers)

3. DISCUSSION

3.1 Compression followed by Encryption (CE)

1) Kumar and Vaish [8] proposed a compression-encryption image method to transmit image quickly and securely through the network. The core idea of the proposed method is to select significant and non-significant coefficient in the wavelet domain. These two coefficients will be encrypted using pseudo-random number sequence and permutation on their each coefficient. The proposed method is first to perform a DWT transformation process. Furthermore, do the pseudo random encryption process (PRNG) and then the compression process using the quantization and entropy coding, whereas wavelet sub-bands detail (LH, HL, HH) substitution process is carried out using the k2 key and is subsequently encrypted using coefficients permutation. The next process of image encryption result is compressed using Singular Value Decomposition (SVD) and Huffman code. Seeing that performance of image compression is mostly based on the selected wavelet transformation filter, then the use of different filters like biorthogonal wavelet, Haar, Symlets, Daubechies, Coiflets, etc., is also tested. The test results demonstrate that the use of biorthogonal wavelet filter produces better compression performance. For example, when image Lena is compressed using wavelet biorthogonal on singular values (SVs) =256 and η = 1, the CR value is 0.2883 and PSNR value is 45.66 dB. By

contrast, CR values for other wavelets like Symlets, Daubechies, Coiflets, Haar and Discrete Meyer wavelet are 0.2970, 0.2967, 0.2979, 0.3014 and 0.3092 each respectively, while appropriate PSNR values are 45.75 dB, 45.95 dB, 45.04 dB, 42.64 dB, 47.89 dB. Also, the proposed method has an advantage of making use of SVD to obtain a better compression performance while maintaining the desired features of the reconstructed image. The proposed scheme is immune to brute force attacks and proved to be more efficient than that of Zhang and to be better than that of JPEG standard

2) Tong et al.[9] also conducted a study to combine lossy compression technique using lifting wavelet transform(LWT) and lossless compression technique using SPIHT coder, followed by cryptosystem symmetric using Chaotic sequence generation. Testing of the proposed method is done using five grayscale image data with a size of 512 x 512 pixels. The measurement result of the change rate of cipher text is about 50% (the change rate is the ratio of the position of the original cipher text and cipher text in which the plaintext is modified). The testing result of changing one bit of bitmap image, on the modification level of cipher stream, ranges between 40-44%, indicating a high sensitivity to plain text. Based on the testing of the key sensitivity of five images, an average value of key sensitivity is more than 49.9%, indicating that algorithm has an excellent key sensitivity. Its compression ratio is about 50% of the original file size. The test results histogram also looks flat; it shows that the frequency of appearance of colour in the cipher image looks evenly, so is secure against statistical attack. The entropy value is relatively high as well, i.e., 7.99 in average which is close to 8, meaning that this method is secure from cryptanalytic entropy attack.

3) Chal.la et al.[10] proposed a Learning with Errors (LWE) and public-key based compression which is implemented using CNA to reduce a key size. CNA is a new lossless compression algorithm which is practical and has a higher adaptive capability.

3.2 Encryption followed by Compression (EC)

1) Mariselvi and Kumar [14] has also proposed the compression of encrypted images through RPC. The symmetric cryptographic employed is DES algorithm followed by lossless compression technique using Huffman coding or arithmetic coding. The coloured images of encryption using DES algorithm are subsequently down sampled to generate sub-images. Each sub-image is then encoded using Huffman or arithmetic coder for performance comparison. Testing of the proposed method is done at four grayscale images to measure Peak Signal Noise Ratio (PSNR) and Compression Ratio (CR) when using arithmetic coding and Huffman coding. The testing result of PSNR values and their compression ratios indicates that Huffman Coding generates higher scores than those of arithmetic coder.

2) Kale et al. [15] combine symmetric cryptographic techniques 3D-Advanced Encryption Standard (3D-AES) and asymmetric cryptography using the RSA method, with lossless compression technique using Shanon fano. The method of 3D-AES is used to generate symmetric keys by randomizing first key arrays three times which generates a better key in each randomization. As a result, the final key will be stronger than standard AES keys. This technique is capable of providing a high level of informational protection of message confidentiality, and originality exchanged between two parties as well as reducing the length of words. This application works on smartphones and does not require other encryption tools.

3) Aujla and Sharma [16] proposed a combination method of the symmetric cryptographic technique using random permutation method and lossy compression technique using Haar and Daubechies wavelet transformation method to enhance the efficiency of compression process of already encrypted images. The application of this approach results in a positional change for the similar pixel values after their encryption. The resultant images are almost identical to the original as the correlative values among neighbouring pixels are relatively high. The result of the encrypted image compression, using orthogonal wavelet transform, is that the majority of the pixels is converted into a series of coefficients. There will be a reduction of data if you remove redundant information contained in the coefficient. This application of compression approach to encrypted images proved to be more efficient according to a testing on CR, Mean Square Error (MSE), and PSNR.

3.3 Joint Compression and Encryption (JCE)

1) Hamdi et al. [13] proposed a method using a more efficient compression technique to generate a high-quality image and little computational complexities. The cryptographic method is confusion and diffusion technique which is integrated and connected to compression chains. The first step is to generate three keys for encryption process using Chirikov Standard Map algorithm. The next step is to perform DWT transformation and is followed by a bit encryption on wavelet coefficient (LL Subband) using the first key, whereas other subbands are undergoing encryption process using the list of LIP and second key. The third step is permutation after SPIHT coding. This stage is to increase the diffusion of the encrypted image. It is to ensure an efficient informational diffusion according to bitwise permutation process. The testing result of the image of a house using level-3 decomposition shows that PSNR value is 39.674, while the image of an airplane using level-2 decomposition shows that PSNR value is 38.013. The average key sensitivity of MAD value for ten tested data images with three different keys is 85.13, which is closer to its ideal value, 85.33 (256/3). By contrast, the average number of pixels change rate (NPCR) of 10 tested images for all stages is 99.55% bigger than the required value of 99%, and the value of Unified average changing intensity (UACI) of 33.59% is larger than the required value of 33%. Thus, the result of differential analysis indicates that the proposed encryption algorithm is very sensitive to small changes in the original images and very resistant to differential attacks.

2) Xiaoyong et al. [12] combined a compression technique using an algorithm of generalized knight's tour, DCT, Quantization and zigzag scan coder and symmetric cryptosystem technique using non-linear chaotic maps method. In contrast, the encoding procedure uses a nested generalized knight's tour (NGKT) matrix generated scrambling by Semi Ham algorithm on the bright image. Furthermore, this is to produce a high image compression ratios by utilizing DCT and quantization coding[18], moreover, the image encryption technique has varieties of methiod [20, 21]. The diffusion process is subsequently done using encryption parts of DCT coefficient obtained from Chen chaotic map. The evaluation of the proposed scheme is carried out by a series of tests using five grayscale images, and the results show that the proposed scheme has a compression performance and good security. Evaluation is also done using compression Degree (CD) used to reflect the compression performance. After the testing result of 5 data, it turns out that the compression performance of the proposed method is better than that of Zang, Yuen, and Zhou, to which this paper refers. However, it is closer to JPEG algorithm. Analysis of key space shows that computational accuracy of 64-bit double precision numbers is about 10-14. The key space of each chaotic map is 1014, and chaotic key space is 1014 × 1014 × 1014 = 1042 which are bigger than 2100[43] that the proposed scheme is relatively resistant to brute force attacks. The testing of key sensitivity provides a value of > 99%, meaning that the key sensitivity is excellent. The testing of differential attacks shows that NPCR value is over 99% and UACI value is over 33%. It means that the proposed scheme is sensitive to plain image and is capable of blocking differential attacks due to its high NPCR and UACI values. The Robustness analysis shows that an image obtained from a decryption process is still recognizable even though it is not as good as the original. The last test is a Structural Similarity Index Measurement (SSIM) comparing images regarding lighting, contrast, and structure, replacing the application of PSNR method in evaluating the similarity among pictures. The testing result of SSIM of 5 data shows a result that is closer to 0, meaning that the proposed scheme is secured.

3) Wang et al. [11] technique the difference on the Schema Lifting (LS) DCT that is performed on the input image before processing the transformation DWT. Having finished performing the separation of subband approximation (LL) and subband details (LH, HL, HH) through DWT transformation process, encryption and compression are done using a different method. After getting subband LL proceed with the encryption method process using a stream cipher, other subbands are encrypted using a permutation method. By contrast, compression is performed by a third party. Regarding subband LL, the result of encryption is then compressed using lossless compression process (encoding is carried out on each coefficient bit). With subbands LH, HL, and HH, encryption results are then compressed using rate-distortion optimized quantization and is followed by a coding process using an arithmetic coding method. The test results of the proposed method are equivalent to the value of the smallest compression ratio (CR = 4.461) when using filters Bior2.2. By contrast, the best-suited subband level for the proposed scheme is on level 3. Also, the proposed scheme provides a small computation time.

4. CONCLUSION

In this paper, several of the current important image compression and encryption techniques have been analysed. The compression technique is lossy or lossless. Lossless compression is preferred for same image quality however if the image quality is tolerable, lossy compression can be considered due high compression up to 50% of original data file size which give storage and transmission advantages.

Encryption method either symmetric or asymmetric. Combination of compression and encryption has the research works performed by researcher around the worlds has been categorized such as CE, EC and JCE.

References

[1]. Walaa Z. Wahba, Ashraf Y. A. Maghari(2016). Lossless Image Compression Techniques Comparative Study. International Research Journal of Engineering and Technology (IRJET) Volume 03 Issue 02, Feb 2016.

[2]. Karpakam, Amutha (2016).Image Encryption and Compression Using Scalable Coding Techniques. Scholars Journal of Engineering and Technology (SJET) Sch. J. Eng. Tech., 2016; 4(1):1-5.

[3]. Riyaz Sikandar Kazi, Navnath Pokale and Prafull Sureshchandra Kamble (2015).Survey on image encryption and compression techniques. International Journal of Advanced Research in Computer Science Engineering and Information Technology Volume: 4 Issue: 3 20-Apr-2015,ISSN_NO: 2321-3337.

[4]. X.-J. Tong, P. Chen, and M. Zhang (2016). A Joint Image Lossless Compression and Encryption Method Based on Chaotic Map. Multimedia Tools and Applications, Jul. 2016.

[5]. A.Poorani, B.Manju (2016).Secure image transformation using Encryption and Compression techniques. International Journal of AdvancedResearch in Science,Engineering and Technology Vol. 3, Issue 5 , May 2016.

[6]. Ranjan Kumar H. S, Fathimath Safeeriya S. P., Ganesh Aithal and Surendra Shetty (2017). A Survey on Key(s) and Keyless Image Encryption Techniques. Cybernetics and Information Technologies Volume 17, No 4 Sofia 2017.

[7]. Kolpe Swapnali R (2016). Implementation of efficient Image Encryption then compression (ETC) System. IJARIIE-ISSN(O)-2395-4396 Vol-2 Issue-3 2016.

[8]. M. Kumar and A. Vaish (2017). An Efficient Encryption-Then-Compression Technique for Encrypted Images using SVD. Digital Signal Processing, vol. 60, pp. 81–89, Jan. 2017.

[9]. X.-J. Tong, P. Chen, and M. Zhang(2016). A Joint Image Lossless Compression and Encryption Method Based on Chaotic Map. Multimedia Tools and Applications, Jul. 2016.

[10]. R. Challa, G. Vijaya Kumari, and P. S. Sruthi(2015).Proficient LWE-Based Encryption using CAN Compression Algorithm. Conference on Power, Control, Communication and Computational Technologies for Sustainable Growth (PCCCTSG). IEEE, 2015, pp. 304–307.

[11]. C. Wang, J. Ni, and Q. Huang (2015). A New Encryption Then Compression Algorithm using The Rate Distortion Optimization. Signal Processing: Image Communication, vol. 39, pp. 141–150, Nov. 2015.

[12]. J. Xiaoyong, B. Sen, Z. Guibin, and Y. Bing (2016). Image encryption and compression based on the generalized knight's tour, discrete cosine transform and chaotic maps. Multimedia Tools and Applications, Jul. 2016.

[13]. M. Hamdi, R. Rhouma, and S. Belghith (2017). A Selective Compression-Encryption of Images Based on SPIHT Coding and Chirikov Standard Map. Signal Processing, vol. 131, pp. 514–526, Feb. 2017.

[14]. C. MariSelvi and A. Kumar (2014).A Modified Encryption Algorithm for Compression of Color Image. International Journal of Recent Development in Engineering and Technology, vol. 2, no. 3, pp. 94–98, 2014.

[15]. N. A. Kale and S. B. Natikar (2014). Secured Mobile Messaging for Android Application. International Journal of Advance Research in Computer Science and Management Studies, vol. 2, no. 11, pp. 304–311, 2014.

[16]. H. K. Aujla and R. Sharma (2014). Designing an Efficient Image Encryption Then Compression System with Haar and Daubechies Wavelet. International Journal of Computer Science and Information Technologies (IJCSIT), vol. 5, no. 6, pp. 7784–7788, 2014.

[17]. 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.

[18]. Hilles, S. M., & Hossain, M. A. (2017). English Steganography Techniques: A Review Paper. International Journal on Contemporary Computer Research (IJCCR), 1(3), 22-28.

[19]. 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.

[20]. Hilles, S. M., & Hossain, M. A. (2018). Classification on Image Compression Methods. International Journal of Data Science Research, 1(1), 1-7.

[21]. Hilles, S. M., & Salem, M. A. (2018). Selective Image Encryption and Compression Technique. Arrasikhun Journal, 4(1), 39-42.