Paradigms of Image Compression and Encryption: A Review

Pratistha Mathur
Manipal University Jaipur
pratistha.mathur@jaipur.manipal.edu

Anju Yadav
Manipal University Jaipur
anju.yadav@jaipur.manipal.edu

Viveak Kumar Verma
Manipal University Jaipur
vivek.verma@jaipur.manipal.edu

Renuka Purohit
Manipal University Jaipur
renukasatyakalp@gmail.com

***Abstract*-Image compression is a process of reducing size of an images at the time of transmission and at network level we also need some security mechanism for secure data transmission assurance. To provide data security we need a best encryption method for an image so that it does not affect image quality. The image compression schemes are of two types lossy and lossless or combination of both. The both (lossy and lossless) compression schemes can compress and decompress the image but some time compression made some loss of data so it is lossy otherwise lossless. To provide security as we know perform encryption and decryption process, there are two methods for key generation one is symmetric and other asymmetric. If we use same key for encryption and decryption i.e., known as symmetric system otherwise asymmetric cryptography system.**

In this paper, a detailed review of different Compression and Encryption schemes like CE, EC ,Joint compression and Encryption is given and we also analyzed their result on the basis of different parameter like compression ratio, PSNR, NPCR, UACI etc.

Keywords: CE, EC, Joint compression and Encryption lossless, lossy, encryption, symmetric, asymmetric.

I. Introduction

The growth of digital data and mainly image leads to need of large storage space, so reduction of size is required for limited band width in communication system. In addition to this data safety is highly concern during the transfer of data that may affect the high speed of data exchange.

Solutions of above problems are Image Compression and encryption technique, which is very important concept for exchanging images or data at network. The aim of this technique is to reduce size and provide fast transfer of data at the network in the secure manner.

In this section overview is given for different scheme i.e., CE, EC and JCE.

A. Image compression

Image compression is a method that reduces the image size, and to make their transmission faster in the limited bandwidth of the network and also consume less storage space. The compression is of two types lossy and lossless.

In lossy compression first we compress the file and then we decompress or restore that file at the decompression phase. If loss of some information is noticeable in image, it means comes in lossy compression. In this quality of image is degraded and we observed high compression ratio. Where as in lossless compression there is no loss of information at decompression process. The quality of image remains same as an original image and compression ratio is also low than the lossy compression. There are so many image compression algorithms like DCT, DWT, Huffman, Run Length Encoding, CS etc.

B. Image Encryption

When we transfer an image on a network the security is a major issue. Encryption is a process of encoding the image or message during exchanging or sharing it. It provides secure transmission of images on a network. There are two type of encryption method Symmetric and Asymmetric. Same key for the encryptions and decryption process is used in Symmetric key cryptography i.e., called public key. And two different keys for encryption and decryption process are used for an Asymmetric key cryptography i.e., public key and private key.

C. Image compression & Encryption schemes

To perform the Image compression and encryption there are three existing technique with different combination of compression and encryption i.e., CE, EC and JCE. The definitions of the above techniques are as follow:

D. Image compression followed by Encryption (CE):

In this process we fist compress the image and then encrypt. In this technique the image is secure but the size of compressed image is greater than EC.

E. Image Encryption followed by compression (EC):

In this process we first encrypt the image then compress. In this technique we get small size image but there are some security issues in this technique, so it is less secure than CE.

F. Joint Image compression & Encryption (JCE):

This is simultaneous process of compression & encryption for images. This process is more secure and faster than CE and EC.

II. Literature Review

This section gives a detailed review of image compression and encryption techniques i.e., CE, EC and JCE. And their results on the basis of performance metrics are included in the Table1, 2, and 3.

978-1-7281-1711-9/19/$31.00 ©2019 IEEE

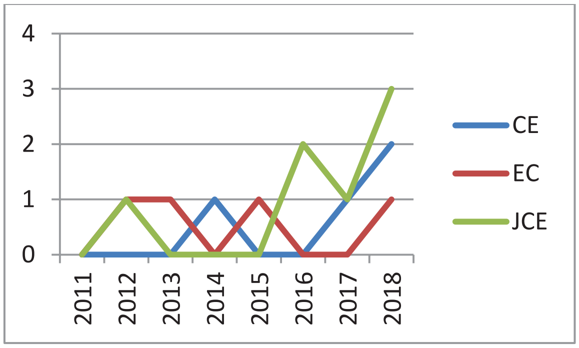

Fig. 1. Year wise classification of research

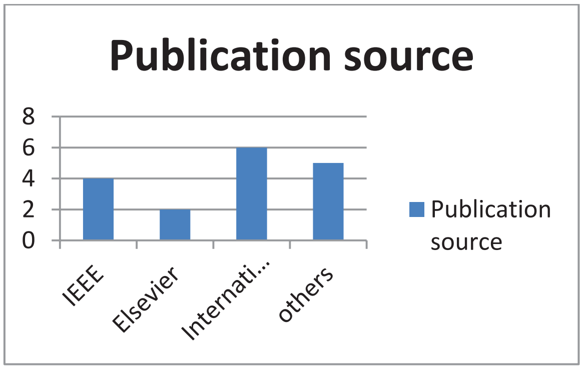

Fig. 2. Publication source of Compression and Encryption schemes.

The Fig.1 defines Year wise classification of research on CE, EC and JCE techniques. It shows that JCE approach is increasing year by year than the CE and EC. Figure 2 shows the different publication source of compression & encryption concept.

A. *Image compression followed by Encryption (CE):*

Sun et. al. [1] have proposed a novel approach of image compression and encryption based on fractal dictionary and Julia set. This approach gives good image quality and also minimizes the time. **Karim et. al. [2]**used crypto-compression technique. In this technique encryption is done within compressed image, for compression and encryption they used DCT and RLE encoding methods respectively. This approach mainly used for medical images. **Setyaningsih et. al. [3]** proposed a novel compression encryption approach i.e. Chaos-Based Dynamic Session Key (CEA-CBDSK), is used encrypt image data and DWT for compression. CEA-CBDSK technique provides better secure transmission against cipher text-only attack, statistical attack, and differential attack. This method is used for gray scale images and in future it may be implemented for color images, with some better key distribution method. **Chandana et. al. [4]** proposed a novel approach for an image compression and encryption for satellite images. In this JPEG-lossless compression technique is used and for encryption one-dimensional chaotic image encryption techniques are used to solve key issues. They also analyzed the result on parameters like USCI and Compression ratio etc. see in table 1. **W. Puech et. al. [5]** proposed the novel compression and encryption approach, for compression they used DCT and for encryption cipher generation AES cipher is used. This technique gives good PSNR value. **Hamdi et al. [6]** proposed the partial compression and encryption. They used the DWT and set partitioning in hierarchical trees (SPIHT). They also used the concept of chaotic sequence. These approaches increased its speed and security. They also used large key space which provides safety against attacks.

TABLE I. COMPRESSION AND ENCRYPTION

S. No.	Author, Year	Compression Scheme	Cryptographic Scheme	Compression Method	Cryptographic Method	PSNR	CR	TIME (sec)	Type of image
1	Yuanyuan Sun, Rudan Xu, Lina Chen, Xiaopeng Hu,2014	Lossy	Symmetric	Fractal dictionary	Julia set as stream cipher	32.483		CT./DcT-0.234/0.015	Normal
2	Med Karim Abdmouleh and Med Salim Bouhlel 2017	Lossless	Symmetric	JPEG DCT	Triple-DES RLE				Medical images
3	Emy Setyaningsih,Retantyo Wardoyo,Anny Kartika sari,2018	lossy	Symmetric	DWT	Chaos-Based Dynamic Session Key (CEA-CBDSK) and DWT	38.8435	37.3047	CT./DcT ET/DeT-12.8361s 18.1816s	normal
4	Chandana U K, Dr. Megha P Arakeri,2018	Lossless	Symmetric	jpeg	One-dimensional chaotic	55.3629 dB	76%		satellite images
5	W. Puech et J. M. Rodrigues.	lossy	Symmetric	DCT	AES	16.31dB.	1.23		medical images

B. Image Encryption and Compression (EC):

Zhu et. al. [7]: performed compression on cipher image based on Gauss random matrix, random scrambling matrix and the scrambling sequence T techniques. They performed joint decompression and decryption to restore an original image. This technique provides robustness against noise and efficient encryption method. **Jing-Yu et. al. [8]** proposed a novel encryption and compression method for color images. They used hyper-chaotic system for encryption, which is utilized to make palette with fruit colors and uniformly distributed color. In this technique similarity near about 95% and compression ratio 75% is achieved. **Dewangan et. al. [9]** proposed compressed and encrypted technique based on wavelet and random permutation. They used different types of wavelet and the haar wavelet gave high compression ratio and better PSNR value for reconstructed image. **Wang et. al. [10]** proposed encryption and compression is based on ETC algorithm using rate-distortion optimization. And for decomposition may used ILWT. This method gives high level of security.

C. Joint Image Compression and Encryption (JCE):

Nasrullah et. al. [11] proposed a secure and efficient network utilization using the combination of compression and encryption technique. In this paper Joint image compression and encryption approach used in which lossless compression by IWT and encryption by SPIHT, Kd-tree and multiple chaotic maps is achieved. This technique provide high compression ratio and also secure at network level. **Al-Maadeed et. al [12]** proposed technique which provide high compression of an image with good quality and effective cipher method for security use at network. In this technique the cipher image have good diffusion and confusion properties. **Peiya Li et al. [13]** has implemented encryption and compression scheme based on loosy JPEG standard. They used image-content-adaptive scheme to generate secrete key. **Jiaojiao Xie et. al. [14]** performed joint compression and encryption using concept of chaos map, sparse decomposition and Chinese remainder theorem. These techniques give better compression ratio and security. They used hash function BLAKE2 to produce the 256-bit encryption key which makes this technique more secure. **Peiya Li et. al. [15]** gave a novel joint image compression and encryption approach using 8×8 block discrete cosine transform (DCT), with some transformation. These techniques provide security against different cryptography attack. **Longyuan Guo et. al. [16]** used combined approach of crossover operator and SPIHT encoding for joint image compression and encryption. This approach gives strong protection against attacks on the network. **Wang et. al. [17]** used JCE approach for medical images and also uses the tensor-based algorithm. In the paper the reconstruction process results does not gave good reconstructed image, and also have a poor quality.

III. Result analysis parameter

A. Peak Signal to Noise Ratio (PSNR)

It is the quality measurement factor for an image, after reconstruct an image the PSNR is calculated for image quality analysis [1].

$$\text{PSNR}=10 \log \max^2 /\text{MSE}$$

MSE-mean square error

B. Compression Ratio (CR)

It can be defined as pixel ratio between compressed and uncompressed image. The bpp is bits per pixel. [11]

$$\text{CR}=\frac{Number\ of\ bits\ in\ Plain\ Text}{Number\ of\ bits\ in\ Cipher\ Text}$$

$$\text{bpp}=\frac{Total\ bit\ in\ compressed\ image}{Total\ number\ of\ image\ Pixels}$$

TABLE II. Encryption And compression

S. No.	Author, Year	Compression Scheme	Cryptographic Scheme	Compression Method	Cryptographic Method	PSNR	CR	Type of image
1	Shuqin Zhu , Congxu Zhu , And Wenhong Wang 2018	lossy	Symmetric	scrambling sequence T,	SHA 256 using Gaussian measurement matrix, random scrambling matrix and the scrambling sequence	25.6457	0.55	Normal Image
2	Abdul Razzaque & Nileshsingh V. Thakur 2012	lossy	Symmetric	DCT and IDCT	multiplicative cipher	7.1862	8	Normal Image
3	PENG Jing-yu, GONG Sheng-rong 2013	lossless	Symmetric	hyperchaotic system	hyperchaotic system	33.3927	75%	Normal Image
4	Ravi Prakash Dewangan, Chandrashekhar Kamargaonkar 2015	lossy	asymmetric	DWT	random permutation	32.75	1.0634 bpp	Normal Image

TABLE III. JOINT IMAGE COMPRESSION AND ENCRYPTION

S. No	Author, Year	Compression Scheme	Cryptographic Scheme	Compression Method	Cryptographic Method	PSNR	CR	TIME (sec)	Type of image
1	Nasrullah ,et al. 2018	lossless	Symmetric	IWT ,Kd-tree	set partitioning in hierarchical trees (SPIHT),optimized Kd-tree and multiple chaotic maps	39.85	8.19/0.97	CT-19.2 s ET-19.2 s	Normal image
2	Somaya Al-Maadeed et.al. 2012	lossy	Symmetric	DWT	1d chaotic map	-	-	ET-.5s	Normal image
3	Peiya Li and Kwok-Tung Lo2018	lossy	Symmetric	JPEG	BLAKE2 hash	33.3429	0.917bpp	CT-0.63s	Normal image
4	Jiaojiao Xie,XiaojunTong,Yimao Zhao 2016	lossy	Symmetric	DCT Dictionary, Chinese remainder theorem	chaos map i	33.27	15		Normal image
5	Peiya Li , Kwok-Tung Lo 2018	lossy	Symmetric	jpeg,dct	RC4	13.9444			Normal image
6	Longyuan guo, jianping , qingtao xue 2017	lossy	Symmetric	crossover operator and SPIHT e	chaotic sequence ,SHA2		7.3635		Normal image
7	Qingzhu Wang et al 2016	lossy	Symmetric	tensor compressive sensing (TCS)	3D Lorenz.	37.76	0.9122		medical imag.es

C. *Number of Pixel Change Rate (NPCR):*

It is standard to test sensitivity of plane image, calculating number of pixel change rate of an image. [1]

$$\text{NPCR}=\frac{1}{W\times H}\sum_{i=1,j=1}^{W,H} D(i,j)\times 100\%$$

D. *Unified average of changing intensity (UACI):*

It is used to measure change between original and *e*ncrypted image. High value of UACI provide more secure image and it is also resistant to attack. [1]

$$\text{UACI}=\frac{1}{W \times H}\sum_{i=1,j=1}^{W,H}\frac{C1(i,j)-C2(i,j)}{255}\times 100\%$$

IV. DISCUSSION

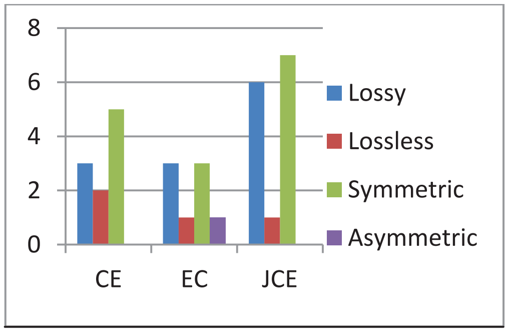

Fig. 3. Classification of Compression and Cryptographic schemes.

These papers gave the novel approaches for of CE, EC and JEC. The results are analyzed on the basis of different parameters compression ratio and PSNR. Maximum approaches gave good PSNR value and compression ratio (See in Table 1, 2 and 3). Some paper also calculated sensitivity of image by changing the pixel value by different metric parameter like NCPR and UACI. Figure 3 shows the classification of compression and encryption schemes, in which we have observed that now a day's maximum papers works on lossy compression and symmetric cryptography.

V. CONCLUSION

In compression and encryption schemes have advantage that the compression can be lossy and lossless and according to our analysis they gave better PSNR and compression ratio. Most of time they used symmetric key cryptography scheme, as it gives good NPCR and UACI values for test of image sensitivity.

For image encryption and compression schemes compression give good image quality but compression ratio is effected some time and for encryption most of time symmetric key cryptography scheme is used. By using EC scheme it provide more secure image transmission.

And joint image compression and Encryption is the hybrid approach for reducing the size of image and encrypting image simultaneously. It gives more secure and compressed image then CE and EC approach. It gives better compression ratio and PSNR value, also give better NPCR and UACI values then the CE and EC approach.

REFERENCES

[1] Yuanyuan Sun, Rudan Xu, Lina Chen, Xiaopeng "Image Compression And Encryption Scheme Using Fractal Dictonary And Julia Set", Hu,IET image processing ,2015,vol.9.lss3,pp. 173-183.

[2] Med Karim Abdmouleh and Med Salim Bouhlel, "Effective Crypto-compression Scheme for Medical Images" International Journal Of Computers And Communications Volume 11, 2017, ISSN: 2074-1294.

[3] Emy Setyaningsih,Retantyo Wardoyo,Anny Kartika sari, "New Compression Encryption Algorithm Using Chaos-Based Dynamic Session Key", International Journal On Smart Sensing And Intelligent Systems, Issue 1 | Vol. 11 (2018).

[4] Chandana U K, Dr. Megha P Arakeri, "A Novel Approach to Compression and Encryption of Large Color Images", Volume: 05 Issue: 09 Sep 2018 www.irjet.net e-ISSN: 2395-0056 p-ISSN: 2395-0072

[5] W. Puech et J. M. Rodrigues "Crypto-Compression Of Medical Images By Selective Encryption Of Dct" .

[6] M. Hamdi, R. Rhouma, and S. Belghith "A Selective Compression Encryption of Images Based on SPIHT Coding and Chirikov Standard Map,", http://dx.doi.org/10.1016/j.sigpro.2016.09.011 0165-1684/& 2016 Elsevier B.V. All rights reserved.

[7] Shuqin Zhu, Congxu Zhu, And Wenhong Wang, "A Novel Image Compression-Encryption Scheme Based on Chaos and Compression Sensing", 2169-3536 ,2018 IEEE.

[8] Jing-yu, GONG Sheng-rong, "Encryption and Compression Scheme of Color Image Based on a Hyperchaotic System", PENG iJOE – Volume 9, Special Issue 6: "AIAIP2012", July 2013.

[9] Ravi PrakashDewangan, Chandrashekhar Kamargaonkar, "Compression of Encrypted Image using Wavelet Transform" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 11, November 2015.

[10] Chuntao Wang,Jiangqun Ni,Qiong Huang, "A New Encryption Then Compression Algorithm using The Rate Distortion Optimization,", 0923-5965/& 2015 Elsevier B.V. All rights reserved.

[11] Nasrullah, Jun Sang , Muhammad Azeem Akbar ,Bin Cai , Hong Xiang and Haibo Hu , "Joint Image Compression and Encryption Using IWT with SPIHT, Kd-Tree and Chaotic Maps", Appl. Sci. 2018, 8, 1963; doi:10.3390/app8101963.

[12] Somaya Al-Maadeed, Afnan Al-Ali, and Turki Abdalla, "A New Chaos-Based Image-Encryption and Compression Algorithm", Hindawi Publishing Corporation Journal of Electrical and Computer Engineering Volume 2012, Article ID 179693, 11 pages doi:10.1155/2012/179693.

[13] Peiya Li and Kwok-Tung Lo, "A Content-Adaptive Joint Image Compression and Encryption Scheme", IEEE Transactions On Multimedia, Vol. 20, No. 8, August 2018.

[14] Jiaojiao Xie,XiaojunTong1,Yimao Zhao, "Joint image compression and encryption method", 2nd Information Technology and Mechatronics Engineering Conference (ITOEC 2016).

[15] Peiya Li , Kwok-Tung Lo, "Joint Image Compression and Encryption Based on Alternating Transforms with Quality Control", 978-1-4673-7314-2/15 ©2015 , IEEE VCIP 2015.

[16] Longyuan Guo, Jianping Li, Qingtao Xue, "Joint Image Compression And Encryption Algorithm Based On Spiht And Crossover Operator", 978-1-5386-1010-7/17/$31.00 ©2017 IEEE.

[17] Qingzhu Wang, Xiaoming Chen, Mengying Wei1 and Zhuang Miao, Wang et al "Simultaneous encryption and compression of medical images based on optimized tensor compressed sensing with 3D Lorenz",. BioMed Eng OnLine (2016) 15:118 DOI 10.1186/s12938-016-0239-1.