ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 2, January 2018

Preserving Privacy of Personalized Data by Sobel Edge Detection in Hybrid Cloud

Mrs. V. Swetha[1], B. Sharon Deborah[2], T. Shruthi[3], M. Soundorya[4]
[1]Assistant Professor, Department of Computer Science and Engineering,[2,3,4]Students, Department of Computer Science and Engineering,Rajalakshmi Institute of Technology, Chennai, India.
Email: [1]swetha.v@ritchennai.edu.in, [2]sharondeborah.b.2014.cse@ritchennai.edu.in,
[3]shruthi.t.2014.cse@ritchennai.edu.in, [4]soundorya.m.2014.cse@ritchennai.edu.in

***Abstract*: Large scale image data sets are generated exponentially from Internet of Things (IoT). This is due to sophisticated cameras, many new editing software and also tremendous improvement in communication network. All the captured digital images are stored in the local storage. Due to insufficient in storage and renting the storage at free of cost, all the image data and other information are moved to public cloud storage. Data can also be stored in private cloud but it is pay per its usage. Though, cloud satisfies the user's needs by providing all types of services, it doesn't provide enough security. Data stored in cloud can be hacked easily by hackers over internet, because it's owned by third party cloud providers. For improving the security efficiency many different encryption and decryption methodologies are growing recently but still they are unsafe to the environment. This paper, describes how efficiently digital images are securely stored by encryption and compression methodology. It also highlights the current issues in security approaches and their comparative analysis.**

***Keywords*- Image segmentation, Encryption, Compression, reconstruction.**

I. INTRODUCTION

As image data are captured and collected massively from Internet of Things, the storage space for images is on demand. Capturing images especially human images becomes increasing, because of sophisticated cameras and technologies. All the images are collectively stored in local storage, since the demand in storage continues and to clear local storage & also to save local storage space, collection of images are stored in cloud. Cloud computing is a model of internet-based computing that provides shared processing resources that are available in a computer and provide data to computers and other devices on demand.It is the delivery of hosted services over the internet.The growing industry of cloud computing has provide a service paradigm of storage or computation outsourcing helps to reduce users burden of IT infrastructure maintenance, and reduce the cost for both the enterprises and individual users. The cloud is maintained and managed by third party service providers, when it comes under privacy concerns the third party can access the data at any time. And there is chance of deliberately alter the information or even delete it accidently. In order to avoid all these concerns, user can prevent them from unauthorized access by encrypting the data and processing it [22].

In cryptography, encryption is one of the techniques which are used to process the encoding information or messages in such a way that only authorized parties can access it. There are various different varieties of encryption techniques are available for providing security to messages or information, but still many researches are going in this encryption. The encryption scheme works as follows: the information or message is called the plaintext by applying any encryption technique to it, we arrive at cipher text, to decrypt the cipher text with the key for attaining plaintext, only the authorized user can access it [23]. The main purpose of image encryption is only for image protection [3]. To secure the information from service provider, the images are to be encrypted by the user before transmission [5]. In order to reduce the storage cost and transmission cost, compression technique is applied to the data. There may be

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 2, January 2018

lossy or lossless compression for compressing the data [24][5]. The way of transmission of image is, first the image is compressed for higher data transmission and then encryption is performed for security. The secret information is secure for both service providers and network intruders [5]. Reconstruction is nothing but reconstructing the original input data from different form. The reconstruction process may involve decryption or decompression with keys.

In this paper, different types of image segmentation, encryption and compression and image reconstructions are discussed below. This paper is organized as follows, section 1, general introduction about image protection, encryption, compression and image reconstruction, section 2, general classification of various scheme used in image segmentation, section 3, classifications of various schemes in encryption and image encryption, section 4,describes about varieties of compression and image compression schemes, section 5, various reconstruction process and conclusion is written in section 6.

II. IMAGE SEGMENTATION

Amir Masoud Ghalamzan Esfahani et al[1] proposes fast and unsupervised algorithm which can be all amount of key pixels for segmentation of SAR images. They proposed an algorithm called FKP_FCM which is very efficient and good for segmenting SAR images. In this, a small number of special pixels are considers as key pixels, by using fuzzy clustering based on nonlocal information are clustered and computed at low cost. The remaining non-key pixels are achieved by using both robust similarity metric and segmentation results of key pixels. Lijuan Cui et al [16] used stereo solar images for testing that are captured from twin satellites system of STEREO.

III. ENCRYPTION

Paul M. Chau and Philip P. Dang [20] proposed a novel scheme where compression and encryption process are joined together for internet multimedia applications in which image encryption is performed by Data Encryption Standard (DES). The simulation result of their proposed systems is enhanced transmission rate and provides security when data transmitted over the internet. Guangtao Zhai et al [9][18] proposed a novelty scalable compression scheme for stream cipher encrypted image. Xinpeng Zhang[21][2] designed a practical scheme for image encryption. A pseudorandom permutation technique is used for encrypting the original image by which confidentiality and access control are achieved. He then shuffled the pixel position and masked the pixel values in encryption phase. The security of encryption is comparatively weaker than standard stream cipher.

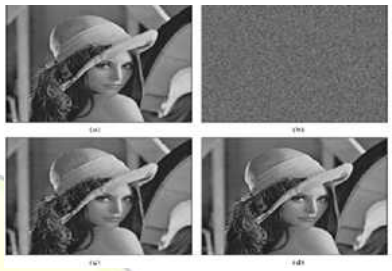

Fig.1 represents(a) Original image, (b) its encrypted image, (c) the medium reconstructed image from compressed data with less PSNR value, and (d) the final reconstructed image with more PSNR value.

Guorui Feng et al [11] proposed a novel scheme for scalable coding of encrypted images. In their encryption phase, the original pixel values are masked by modulo-256 addition with pseudorandom numbers which are derived from secret key. The encoded bit streams are made up of quantized remainders of Hadamard coefficient and encrypted subimage.

Fig.2. represents (a) original image and (b)encrypted image.

Atef Masmoudi and William Puech[3] proposed a technique called chaos-based pseudorandom bit generator for encrypting the original image. He provided a scheme that uses the advantages of chaos theory in data encryption which is also useful for many applications mainly, image protection. Their image encryption is satisfactory without any arithmetic coding (AC) compression efficiency loss after the numerical simulation analysis.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 2, January 2018

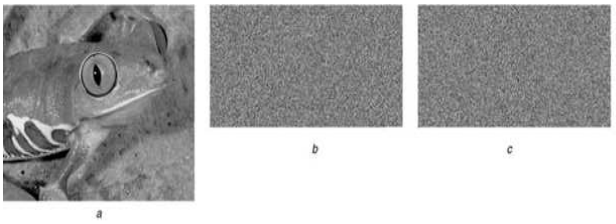

Fig.3 represents (a)Original image of Frog and its corresponding compressed-encrypted images using the key both on (b)SAC (c) AAC-0.

Guorui Feng et al [10] proposed a novel scheme for compressing encrypted data with auxiliary information. In which, they encrypt the uncompressed original content and generate some auxiliary information. Hui Liu [12] described a novel scheme for encryption called Advanced Encryption Standard (AES) which produce dynamic key generator such as 2D chebyshev and 2D Henon map. To make this algorithm more efficient, secure and practical they used chaotic key generator from the simulation results of several attacks. [6] discussed about Submerge Detection of Sensor Nodes. Underwater networking sensor nodes provide the oceanographic collection of data and monitoring of unmanned or autonomous underwater vehicle to explore sea recourses and gathering of scientific data. The sensor network contains the statistical data about the sensor nodes. High Speed Optical communication is provided between the nodes in a point to point fashion. The design emphasis on the modulation and demodulation of the signals and thereby providing the synchronization between the nodes. The challenges include waterproofing, casing, calibration. Furthermore the research issues are outlined.

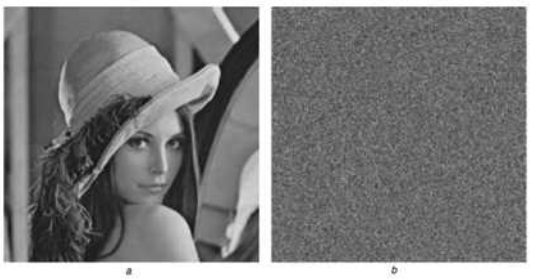

Fig.4 represents (a)original and decrypted image and (b)encrypted image which is decrypted using the key.

Chandrashekhar Kanargaonkar and Ravi Prakash Dewangan[5] mainly focus on compression of encrypted image. Their encryption process is based on permutation technique, that is, they combined the pixels and permutation technique for image encryption. If available number of keys is very large, then it makes encryption stronger. Chandrashekhar Kanargaonkar and Ravi Prakash Dewangan proved that random permutation technique for image encryption is fast and provides high degree of security.

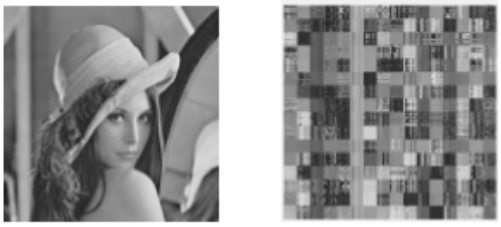

Fig.5 represents the (a) original image and (b) encrypted image using combination of pixels and block permuted image.

IV. COMPRESSION

Edward J. Delp and O. Robert Mitchell [8] proposed a new technique called Block Truncation Coding (BTC) for compression and it is compared with transform and other techniques.

Fig.6 represents the original image (top) and coded image (bottom) of data rate with 2 bits/pixels.

Jidong Shen [14] for the first time, he proposed a DPCM based on modular algorithm for compression technique. The length of code words required by the entropy coding is necessarily limited to some positive integer by using this technique. The advantage of using this predictive image compression system due to its simplicity, shorter length of codeword and information preserving. Paul M. Chau and Philip P. Dang [20] proposed a technique called joint compression and encryption where Discrete Wavelet Transform (DWT) for image compression process. Their algorithm compresses the data with high compression ratio and provides enhanced security for transmission process.Fig.7 represents the compressing of images using DWT.Daniel Schonberg et al presented a scheme in which the order of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 2, January 2018

steps is reversed, i.e. first encryption and then compression, such that the compressor does not have any knowledge of encryption key. Their encrypted data has been compressed to its original rate. Guangtao Zhai et al [9][18]

Fig.7

proposed a novelty scalable compression scheme for stream cipher encrypted image. They used a base layer for compressing the uniform non-overlapping patches of encrypted image with down-sampled version. Dilshad Rashed V A and Remya S [7][18] proposes a method for encrypted gray scale image called Resolution Progressive Compression (RPC) based on DWT. Their main focus of using this image compression algorithm is to reduce transmission time and memory space. In this algorithm, they compress the image into resolution progressively by which the decoder can access the image partially. It also provides less computational complexity and better coding efficiency. In order to provide more security to the data they combined the compression algorithm with cryptography technique. This algorithm performs good for color images and gray scale images.

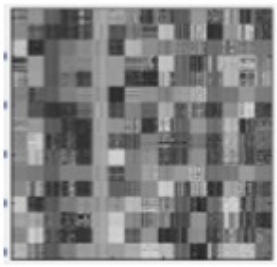

Fig.8

Fig.8 represents the haar wavelet compressed image.

Xinpeng Zhang[21][2] designed a practical scheme for lossy compression. He compressed the encrypted data using orthogonal transform by discarding the excessively rough and generated fine information coefficients which leads to reduce in data amount. Lijuan Cui et al [16] described that the adaptive distributed compression solution by using particle filtering which tracks the correlation and also performs disparity estimation at the decoder side.

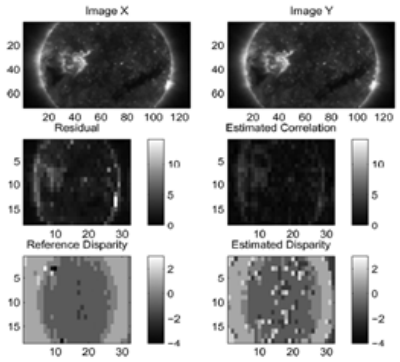

Fig.9 represents final calculation of disparity and correlation for solar image.

Atef Masmoudi and William Puech[3] proposed a technique for compression called arithmetic coding (AC). He shuffled the cumulative frequency of vector input symbols to make AC secure and completely key dependent for decoding process to incorporate the chaos theory into AC. They presented a scheme in which lossless image compression is exploiting the efficiency of AC. Bingsheng Zhang et al[4] proposed an outsourced recovery framework architecture called Outsourced Image Recovery Services (OIRS). They choose OIRS design for compressing framework, which is simple for traditional sampling and image acquisition compression. For reducing the storage overhead in cloud, the data owners use compression image samples. Their main focus of designing OIRS is sparse data, for compressed sensing it's an typical application scenario. Guorui Feng et al [10] proposed a novel scheme for compressing encrypted data with auxiliary information. The original content cannot be accessed by channel provider so; they may compress the encrypted data content by quantization method with optimal parameters which are derived from the part of auxiliary information. Their compression technique is only compatible with modulo – 256 additions and not for other encryption approaches. They compared their model with others and found that the compression performance is improved and computational complexity is also reduced. Lina Dong et al[17] proposed a novel scheme for compression and encryption operations by using fractal dictionary and Julia set. They used fractal dictionary encoding scheme for compression process which not only reduces the time consumption but also gives better quality image. Jiantao Zhou et al[13][15] designed a highly efficient image Encryption-Then-Compression (ETC) system where lossless and lossy compression are used. They used an arithmetic-coding based approach for exploiting the compression of encrypted image more efficiently. Jiantao Zhou et al described that comparing state-of-the- art lossless/lossy image coders which considers the unencrypted image as inputs with their compression efficiency, it is slightly

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 2, January 2018

worse, when their compression technique is applied to encrypted images. Chandrashekhar Kanargaonkar and Ravi Prakash Dewangan[5] mainly focus on compression of encrypted image because compression of encrypted image is quite complex when compared with traditional image. So, they used wavelet transform technique to do their compression operation. Five types of wavelets are used by Chandrashekhar Kanargaonkar and Ravi Prakash Dewangan such as Symlet, debuncies, Biorthogonal, coifelet, haar. They proved that haar wavelet has higher compression ratio with better reconstructed image. Nan Liu and Wei Kang[19] proposed an optimal rate-distortion code a novel scheme for compression of encrypted data. Their proposed approach achieves compression rate and secret key value. They also showed that this system attains strong security and information leakage vanishes exponentially.

V. IMAGE RECONSTRUCTION

Edward J. Delp and O. Robert Mitchell[8] reconstructed the outsourced image which has artifacts that are quite different and comparable from other techniques. In the presence of channel errors, they produced a coded image which is more robust and also requires very little error protection overhead. Their recovered outsourced image produced good quality of image further; it can be enhanced at the data rate of 1.5 bits/pictures element. Jidong Shen [14] distortionlessly reconstructs the original input image from predictive decoding with the help of smaller codebook. Paul M. Chau and Philip P. Dang [20] reconstructed the input image with acceptable quality.

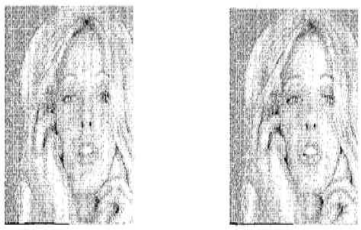

Fig. 10represents that, first image is the original image and next image is the reconstructed image.

Daniel Schonberg et al presented the numerical results, that the original source image is recovered when the compressed data is encrypted. Xinpeng Zhang[21][2] designed a practical scheme for image reconstruction. He reconstructs the original image by iteratively updating the coefficient values of orthogonal transform by exploiting the spatial correlations in natural image, when having the compressed data and permutation way. When higher the compression ratio and smoother the original image he yields a reconstructed image of better quality. Guorui Feng et al [11] reconstructs the approximate image at the receiver side by decrypting the subimage. The quantized data provide more elaborate information for image reconstruction by hadamard coefficient In their approach the bitstreams are generated with multiple-resolution construction, when more bitstreams are received, the principle content with high resolution are gained. Lijuan Cui et al [16] compares non-adaptive scheme with their proposed adaptive scheme by which the decoding performance is gained. Guorui Feng et al [10] reconstructed the original image with the help of secret key and compressed encrypted data. The iterative reconstruction procedure of original content is needless at receiver side.

Fig.11 (a)Image reconstruction with PSNR 35.5 dB and compression ratio 0.172 and (b) Image reconstruction with PSNR 32.8 dB and compression ratio 0.114.

Bingsheng Zhang et al[4] proposed an outsourced recovery framework architecture called Outsourced Image Recovery Services (OIRS). Outsourced Image Recovery Service makes use of techniques from varies domains, and also aims to take design complexity, security, and efficiency into consideration from the very beginning of the service recovery flow. They have proved that besides the simplicity and efficiency of OIRS, both the sparse data and non-sparse data can able to handle image reconstruction to achieve effectiveness and robustness.

Fig.12 represents the comparison of recovered images using different number of measurements m in OIRS. (a) m=128, (b) m=192, (c) m=256.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)

Aspects	Performance	Related Work	Advantages	Disadvantages
Image Segmentation	Better[1]	FKP_FCM algorithm[1]	Efficient segmentation[1]	Lower potential[1]
Encryption	Faster[5][12] [20]	Pseudorandom permutation[2][21], chaos-based pseudorandom bit generator[3], permutation technique[5], prediction error and random permutation[13][15][19], Modulo-256 addition encryption[11], Advanced Encryption Standard[12], Julia set[17], Data Encryption Standard[20]	Useful for many applications[3], High security[5][13][15] [19][12],efficient [12][20],high plaintext sensitivity[17], fast transmission[20]	Weaker security[2]
Compression	Better performance[3] [7][18][10], worst[13][15]	Auxiliary information[10], scalable compression scheme[9][18], fractal dictionary[17], Orthogonal transformation[2][21], Arithmetic Coding[3][13][15], wavelet transform[5], Resolution Progressive Compression[7][18], Block Truncation Coding[8], DPCM algorithm[14], particle filtering[16], rate-distortion code[19]	Higher compression ratio[5][20], , less computational complexity[7][18] [10], simplicity[14],reduces time[17], better image quality[17], no information leakage[19], security[19][20]	Slightly worst compression [13][15]
Image reconstruction	Good[21][2]	Orthogonal transform[21][2], PSNR technique[5], Outsourced Image Recovery Services[4], iterative and multi scale technique[9], quantized data[11], predictive decoding[14]	Smooth and better image[21][2][5] [17],acceptable image quality[20]	Error protection overhead [8]

Table-1 represents the comparisons of various techniques and their performances used in image segmentation, encryption, compression and reconstruction.

Lina Dong et al[17] proposed a novel scheme for compression and encryption operations by using fractal dictionary and Julia set. They used fractal dictionary encoding scheme for compression process which also helps to give better quality image for reconstruction.

Fig.16 the left side image is the original image and the one that is on the right side is the reconstructed image.

Guangtao Zhai et al [9] used the decoder to reconstruct the image that are applied with iterative and multi scale technique from all available samples. Chandrashekhar Kanargaonkar and Ravi Prakash Dewangan[5] has reconstructed the compressed image to original image by using PSNR. They referenced that PSNR of reconstructed image is better at lower bpp.

VI. CONCLUSION

Due to rapid progress growth in communication network technology is increasing widely; it is insecure when various data are exchanged over the internet. So, the data should be secured from unauthorized users and other vulnerable cases. Various interesting research topics in image encryption process are filed; need to design a way, how to protect the data from unauthorised users and other vulnerable cases. Varieties of encryption techniques are currently available and also illustrated in this framework to provide high security for image data. These encryption processes are not still perfect to gain the high accuracy in encryption process and also requires further modifications.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 2, January 2018

ACKNOWLEDGMENT

We are grateful to extend our sincere gratitude to our organization and to Mrs.V.Swetha for sharing the pearls of wisdom to complete this project.

REFERENCES

[1] Amir Masoud Ghalamzan Esfahani, Biao Hou, Licheng Jiao, Ronghua Shang, Rustam Stolakin, Yijing Yuan, "A fast algorithm for SAR image segmentation based on key pixels" in IEEE Journal of selected topics in applied earth observations and remote sensing.

[2] Asha P.Ghodake, Sujata Mendgudle , "Security and Privacy of Image by Encryption, Lossy Compression and Iterative Reconstruction" in International Journal of computer Applications (0975-8887), vol. 62, no. 1, Jan. 2013.

[3] Atef Masmoudi, William Puech, "Lossless chaos-based crypto-compression scheme for image protection" in IET image processing, vol. 8, Iss. 12, pp. 671-686, 2013.

[4] Bingsheng Zhang, Cong Wang, Janet M. Roveda, Kui Ren, "Privacy assured outsourcing of image reconstruction service in cloud" in IEEE transactions on emerging topics in computing, July 2013.

[5] Chandrashekhar Kanargaonkar, Ravi Prakash Dewangan, "Compression of encrypted image using wavelet transform" in International Journal of advanced research in computer and communication engg., vol. 4, Iss. 11, Nov. 2015.

[6] Christo Ananth, S.Surya, Berlin Mary, "Submerge Detection of Sensor Nodes", International Journal Of Advanced Research Trends In Engineering And Technology (IJARTET), Volume II, Special Issue XXV, April 2015

[7] Dilshad Rashed V A, Remya S, "Resolution progressive compression of encrypted images" in International Journal of signal processing systems, vol. 1, no. 1, Jun. 2013.

[8] Edward J. Delp, O. Robert Mitchell, "Image compression using block truncation coding" in IEEE transactions on communications, vol. 27, no. 9, Sept. 1979.

[9] Guangtao Zhai, Jiantao Zhou, Oscar C. Au, Xianming Liu, Yuan Yan Tang, "Scalable compression of stream cipher encrypted images through context-adaptive sampling" in IEEE transactions on information forensics and security, vol. 9, no. 11, Nov. 2014.

[10] Guorui Feng, Liquan Shen, Xinpeng Zhang, Yanli Ren, Zhen Xing Qian,"Compressing encrypted images with auxiliary information" in IEEE transcations on multimedia.

[11] Guorui Feng, Xinpeng Zhang, Yanli Ren, Zhen Xing Qian,"Scalable coding of encrypted images" in IEEE transactions on image processing, vol. 21, no. 6, Jun. 2012.

[12] Hui Liu, Jianhua Li, "Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map" in IET information security, vol. 7, Iss. 4, pp. 265-270, Feb 2013.

[13] Jiantao Zhou, Oscar C. Au, Xianming Liu, Yuan Yan Tang, "Designing an efficient image Encryption-Then-Compression system via prediction error clustering and random permutation" in IEEE transactions on information forensics and security, vol. 9, no. 1, Jan. 2014.

[14] Jidong Shen, "A novel image-compression technique using the modular algorithm" in SMPTE Journal, May 1993.

[15] Kalyani G. Nimbokar, Mangesh M. Ghonge, Milind V. Sarode, "A Survey based on designing an Efficient Image Encryption-then-Compression System" in International Journal of computer Applications (0975-8887), National level Technical conference, X-PLORE 14.

[16] Lijuan Cui, Lina Stankovic, Samuel Cheng, Shuang Wang, Vladimir Stankovic, "Onboard low complexity compression of solar stereo images" in IEEE transactions on image processing, vol. 21, no. 6, Jun. 2012.

[17] Lina Chen, Rudan Xu, Xiaopeng Hu, Yuanyuan Sun, "Image compression and encryption scheme using fractal dictionary and Julia set" in IET image processing, July 2014.

[18] Lina Dong,Qiuming Yao, Wei Liu, Wenjun Zeng, "Efficient compression of encrypted grayscale images" in IEEE transcations on image processing, vol. 19, no. 4, April. 2010.

[19] Nan Liu, Wei Kang, "Compressing encrypted data: achieving optimality and strong secrecy via permutations" in IEEE transactions on information theory.

[20] Paul M. Chau, Philip P. Dang, "Image encryption for secure internet multimedia applications" in IEEE transcations on consumer electronics, vol. 46, no. 3, Aug. 2000.

[21] Xinpeng Zhang, "Lossy compression and iterative reconstruction for encrypted image" in IEEE transactions on information forensics and security, vol. 6, no. 1, March 2011.

[22] https://en.m.wikipedia.org/wiki/Cloud_computing.

[23] https://en.m.wikipedia.org/wiki/Encryption.

[24] https://en.m.wikipedia.org/wiki/Image_compression.