Image Encryption using n-Encryption Techniques

Madhvi Popli[1], Dr Gagandeep[2]
[1]PhD Scholar, Department of Computer Science, Punjabi University, Patiala
[2]Associate Professor, , Department of Computer Science, Punjabi University, Patiala
(E-mail: madhvi11mca@gmail.com)

Abstract—Today we are dependent on the internet for transferring and sharing images from one place to another. It is very easy to transfer information but very difficult for providing secured information and information security has become major challenge particularly in public sectors. To minimize these issues cryptography is used to change information into an unreadable form based on the key. For text and images, different cryptography techniques are applied. Text encryption methods are difficult to handle on images because of data redundancy and mass data capacity. A new approach for the colored images is proposed in this paper. We propose a method in which image is first partitioned into n multiple parts and n encryption algorithms are applied to encrypt and n decryption methods are applied to decrypt the n-images to obtain original image.

Keywords—*Cloud Computing; Cryptography; Image Encryption*

I. INTRODUCTION

Cloud computing becomes a promising technology by providing on-demand storage and computing services at affordable rates. The modern cloud technologies have changed every one perception regarding infrastructure architecture, development and delivery models. The user needs to pay for the services as they used and the user can have access data and service anywhere/anytime. Today in the information system, security and ethical issues become the most important concern for most of the organizations.

Cryptography is an art of achieving security to protect data from unauthorized access by making it to non-readable by applying encryption at sender side and transform into readable form by decrypting it at the receiver side. To ensure the confidentiality of the data encryption is necessary. Cryptography becomes more complex and used advanced mathematical procedures during encryption and decryption processes. Symmetric and Asymmetric are two main algorithms. The basic difference between the two encryption technique is the use of secret keys.

Symmetric key algorithm required secured exchange of secret keys and uses the same key for encryption and decryption process. These methods are computationally low cost and require fewer resources whereas , these methods are computationally high cost and require more resources. With the evolution of information technology, network security issues become acute. When massive amount of data is transferred from one place to another then in that case field of security and encryption become very important.

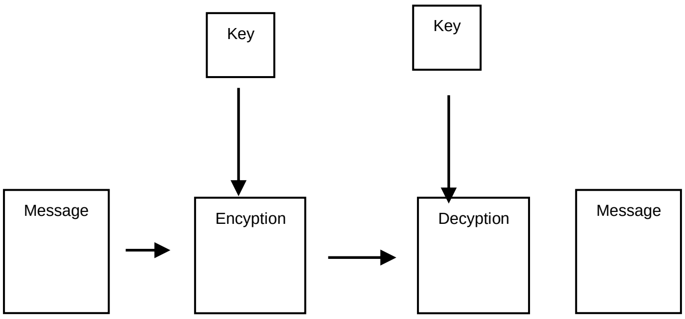

Fig I(a). Symmetric Key

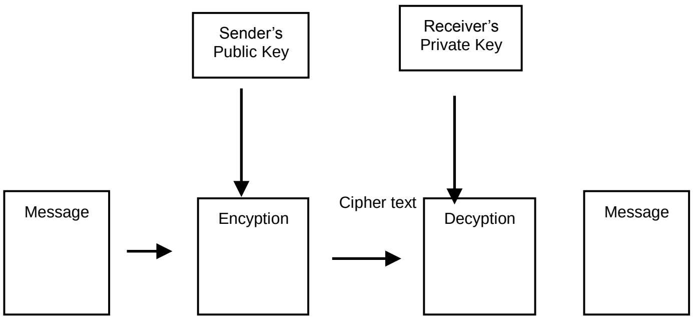

Fig I(b). Asymmetric Key

Encryption is an art of representing any data into unreadable form so as to prevent it from disclosure of important information. Text encryption methods are difficult to be applicable on image for encryption purpose due to image features such as data redundancy and capacity. Traditional methods are not meet the actual requirement for securing image. More than 80% of the information can be obtained visually by representing in the form of an image. Security of the image is necessary that aim to get a new image which is hard to recognize. Image encryption is main important part of privacy. The main challenge is to encrypt data when it is connected to the image privacy.

There are various image encryption methods and these methods are categorize into three major groups. Position

Permutation based Algorithms, Value Transformed based Algorithms and Position Substitution based Algorithms.

A. Position Permutation based Algorithms

Rearrangement of elements either done by bit, pixels or block wise in the plain image is known as Transposition. Bit permutation decreases actual value of information where as Blocks and pixels permutation increases security level.

B. Value Transformed based Algorithms

The algorithm is based on the technique in which pixel value is changed to some other value. The new pixel value is computed by applying some mathematical algorithm on the pixel and with some formulas new pixel value is produced for that pixel.

C. Position Substitution based Algorithms

This technique is obtained by combining both algorithms position permutation and value transformation. Pixels are first reordered and key generator is used to substitute the pixel values. [1]

Some basic parameters are used to measured the performance of the encryption techniques. These parameters are Visual Degradation, Compression Friendliness, Format Compliance, Encryption Ratio, Speed, and Cryptographic Security. There are much related works that relates to image encryption techniques and methods used by various authors. This paper has following structure : section II Related Works, III Proposed Work and IV Conclusion of the paper.

II. RELATED WORKS

Kester et al. [2] proposed a hybrid approach for image encryption using AES and RGB cryptographic technique. Shared secret keys are generated using Advanced Encryption Standards which is used for RGB pixel displacement and shuffling. Lu et al. [3] provides quantitative comparison between homomorphic encryption-based and feature/index randomization-based techniques, for confidentiality-preserving image search in terms of search accuracy, security strength, and computational efficiency. Among two techniques homomorphic technique is considered to be more secure but computational complexity is very high where as the index randomization technique offer high efficiency. Both techniques have good search accuracy but they do not provide privacy protection.

Amalarethinam et al. [4] proposed Magic Rectangle (MR) a new encryption algorithm on images. Author introduced magic rectangle to provide additional level of image security. Image is converted in to blocks of bytes and theses bytes are replaced with the MR values and image is encrypted with public key cryptography. Magic rectangle is an arrangement of integer of mxn order where sum of all elements in every rows and columns are equal. Any order with even integers such as 4x6, 8x12, 16x24 etc are used in this method. Magic rectangle can be constructed using several parameters such as seed value, row sum, column sum, Min start and Max start values.

Xiang et al. [5] proposed a scheme with the help of steganography for the client who are resource-limited and does not want to reveal original image to the cloud. Chaotic selective encryption is outsourced by the client for the images. Client first select important data and selectively encrypt and embeds into cover image then, sends stego image to the cloud. In first phase, the coordinates of pixels are permutated by multidimensional chaotic map and in second phase pixel values are masked using a bitwise exclusive by another one-dimensional chaotic map. The author used chaotic map to encrypt image with the help steganography to the cloud.

Yassin et al. [6] has proposed two-factor authentication scheme with partial image encryption to overcome authentication issues and drawbacks. First factor includes one-time password and second factor is partial encryption using edge detection. The edge detection method is used to detect edges that changes intensity rapidly and the places of edge pixels. The edge detection method output is binary image having edges refereed as ‘1’ and black pixels referred as ‘0’. Canny’s edge detection scheme is used for partial encryption of images along with the symmetric encryption.

TABLE I: COMPARISON OF EXISTING TECHNIQUES

S.NO.	YEAR	NAME OF RESEARCHER	METHOD
1	2014	Quist-Aphetsi Kester, Laurent Nana and Anca Christine Pascu	Hybrid approach for image encryption using AES and RGB cryptographic technique
2	2014	Wenjun Lu, Avinash L. Varna and Min Wu	Homomorphic encryption-based and Feature/index randomization-based techniques
3	2015	D.I. George Amalarethinam and J. Sai Geetha	Magic Rectangle (MR)
4	2015	Tao Xiang, Jia Hu and Jianglin Sun	Chaotic image encryption
5	2015	Ali A.Yassin, Abdullah A. Hussain and Keyan Abdul-Aziz Mutlaq	Two-factor authentication scheme with partial image encryption
6	2016	Purvee Raghuwanshi, Jijo. S. Nair and Saurabh Jain	Logistic function along with XOR
7	2017	Nidhal K. El Abbadi, EnasYahya and Ahmed Aladilee	Cat Map concept and Shadow Process algorithm
8	2017	Fang Han, Xiaofeng Liao, Huiwei Wang, Bo Yang, and Yushu Zhang	Self-adaptive DFrRT and random phase encoding
9	2017	Kapil Mishra and Ravi Saharan	Length Encoding Scheme and Henon Chaotic Map Encryption
10	2017	S. Sowmiya, I. Monica Tresa and A. Prabhu Chakkaravarthy	Pan Magic Square encryption

Raghuwanshi et al. [7] Proposed a new cryptographic approach for colored images. A logistic module one of the method of chaotic map is applied on the image which is selected for encryption that shuffles the image pixel results in to mapped image. XOR function is applied on mapped and the original image results in to distorted image. Logistic function is used for encryption and decryption along with XOR function.

Abbadi et al. [8] Proposed concept of for image encryption based on the scrambling position of pixel and by changing intensity of pixel. In first step two dimension Cat map concept is used to scramble image with uniform distribution and in second step Shadow process algorithm for encryption process. Shadow process depends on two keys which can be any positive values when multiplied together obtained base product value minus one. One key is used for encryption process and other for decryption process.

Han et al. [9] proposed a self-adaptive scheme for double color-image encryption to prevent security risks for the generation of complex image due to the adoption of linear transform, and data redundancy. In this scheme, each RGB color component is compressed by 2D compressive sensing (CS) and then complex image is re-encrypted by self-adaptive DFrRT and random phase encoding. For decryption process, Inverse operations of self-adaptive random phase encoding and DfrRT are applied to the encrypted image. The projection neural network algorithm is adopted for the reconstruction operation and for decryption process.

Mishra et al. [10] presented technique using an integrated image compression by run length encoding scheme and encryption technique using henon chaotic map. This scheme uses run length encoding for lossy image compression that generates (value,count) pairs. In this approach, pixel values are made to be odd and count values to be even and then embedded in to the image. To enhance the security of digital image, image size and resolution are changed and encryption is performed using henon chaotic map.

Sowmiya et al. [11] Proposed Pan Magic Square encryption algorithm for image. Using PMS, image is first partitioned into pixels by changing RGB values of pixels and then by user's key 64 magic squares are generated and based on square values image is encrypted and transmitted to the receiver. Reverse process is done to decrypt the image. In this method, the original image is computed only after 64 squares.

III. PROPOSED WORK

When a massive amount of information is transferred over internet in this twenty first century, encryption and information security becomes very important. We propose a model in which image is first partitioned in to n parts. Each part will go under encryption process using n different encryption algorithms and send to cloud for storage. In image encryption process , the given image is first partitioned in to n parts. Different encryption techniques are applied to different parts of image using any cryptography algorithm. The obtained cipher text images are send to cloud for storage purpose. The entire process is reversed for the decryption process. The n-decryption techniques are applied to decrypt the cipher-text image and original image is obtained.

In Encryption process, original image is partitioned into n parts image 1, Image 2, Image 3… Image n-1, Image n. Each part of image is encrypted using different cryptographic techniques. Suppose Image 1 is encrypted by shuffling RGB values, Image 2 is encrypted using Blowfish technique and so on. Different encrypted images E_Img 1, E_Img 2,.. E_Img n-1, E_img n are send to cloud for storage. The whole process is reversed to obtained original image from the n encrypted images by applying n decryption techniques.

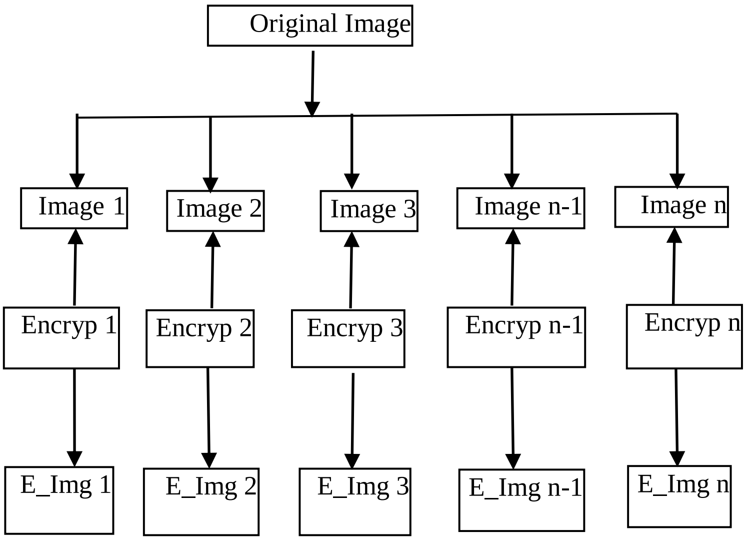

Fig II(a). Encryption Process

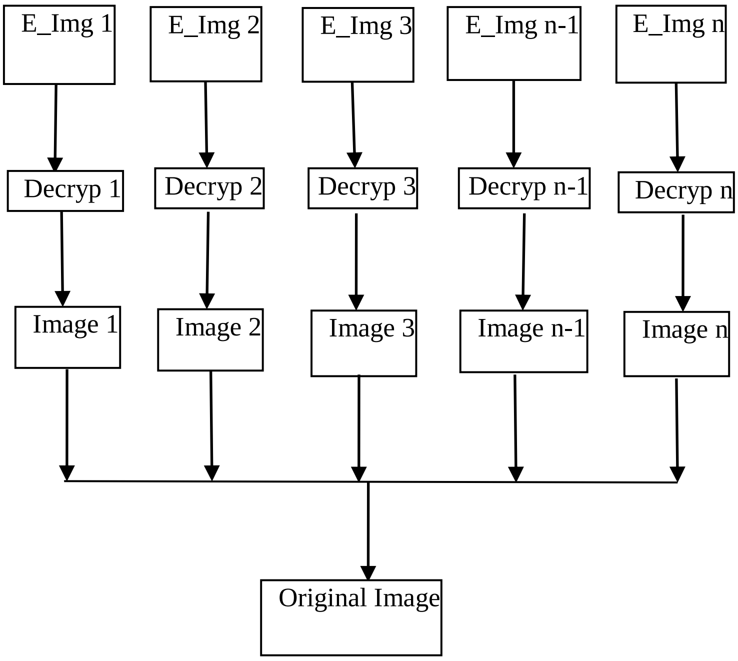

Fig II(b). Decryption Process

The proposed method is most efficient and it is hard to detect which encryption technique is actually applied to image as unauthorized user always try to access original image stored in cloud but encryption techniques are applied to parts of image which are stored in cloud not on original image. So it will become difficult which technique is applied for encryption process.

IV. CONCLUSION

Cloud computing becomes a promising technology by providing on-demand storage and computing services at affordable rates. Traditional methods are not meet the actual requirement for securing image. The different methods has been discussed by various authors in order to sending image in secured manner by using various cryptography techniques. This paper introduces new techniques by partitioned image into multiple parts before encryption and then multiple encryption methods are applied to encrypt different parts of image and reverse process is applied for decryption process to obtain original image. It makes algorithm efficient and hard to detect which encryption technique is actually applied to image.

REFERENCES

[1] Gajendra Singh Chandel, Vinod Sharma, and Uday Pratap Singh, "Different Image Encryption Techniques-Survey and Overview",International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, pp 264-268, 2016

[2] Quist-Aphetsi Kester, Laurent Nana and Anca Christine Pascu, "A Novel Cryptographic Encryption Technique for Securing Digital Images in the Cloud Using AES and RGB Pixel Displacement", IEEE European Modelling Symposium (EMS), pp 293-298, 2014

[3] Wenjun Lu, Avinash L. Varna and Min Wu, "Confidentiality-Preserving Image Search: A Comparative Study Between Homomorphic Encryption and Distance-Preserving Randomization", IEEE Access, vol. 2, pp 125-141, 2014

[4] D.I. George Amalarethinam and J. Sai Geetha, "Image encryption and decryption in public key cryptography based on MR", IEEE International Conference on Computing and Communications Technologies (ICCCT), pp 133-138, 2015

[5] Tao Xiang, Jia Hu and Jianglin Sun, "Outsourcing chaotic selective image encryption to the cloud with steganography", Digital Signal Processing, Elsevier, vol. 43, pp 28-37, 2015

[6] Ali A.Yassin, Abdullah A. Hussain and Keyan Abdul-Aziz Mutlaq, "Cloud authentication based on encryption of digital image using edge detection", IEEE International Symposium on Artificial Intelligence and Signal Processing (AISP), pp 1-6, 2015

[7] Purvee Raghuwanshi, Jijo. S. Nair and Saurabh Jain, "A secure transmission of 2D image using randomized chaotic mapping", IEEE Symposium on Colossal Data Analysis and Networking (CDAN), DOI 10.1109/CDAN.2016.7570870, 2016

[8] Nidhal K. El Abbadi, EnasYahya and Ahmed Aladilee, " Digital RGB Image Encryption Based On 2D Cat Map and Shadow Numbers, IEEE Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), pp 162-167, 2017

[9] Fang Han, Xiaofeng Liao, Huiwei Wang, Bo Yang and Yushu Zhang, “A Self-adaptive Scheme for Double Color-image Encryption”, IEEE Ninth International Conference on Advanced Computational Intelligence (ICACI), Doha, Qatar, pp 121-128, February 2017

[10] Kapil Mishra and Ravi Saharan, “Image Encryption Utilizing Lossy Image compression”, IEEE International Conference on Computer Communications and Electronics (Comptelix), Jaipur, India, pp 494-500, July 2017

[11] S. Sowmiya, I. Monica Tresa and A. Prabhu Chakkaravarthy, "Pixel based image encryption using magic square", IEEE International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), DOI 10.1109/ICAMMAET.2017.8186634, 2017