ISSN: 2454-1907
DOI: https://doi.org/10.29121/ijetmr.v5.i1.2018.49

IJETMR
International Journal of Engineering Technologies and Management Research
A Knowledge Repository

REVIEW OF IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES FOR 2D IMAGES

Jalpa Shah [*1], J S Dhobi [2]
[*1, 2] Department of Computer Engineering, Government Engineering College, Gandhinagar, Gujarat, India

Abstract:
In the emerging era of Internet, multimedia software and application security of images is of major concern. To offer security to these images encryption is the way for robust security. With Image Encryption it becomes difficult to analyze the image that is communicated over untrusted network. Also it provides security for any unauthorized access. The paper provides an introduction to cryptography and various image encryption techniques are reviewed for 2D images.

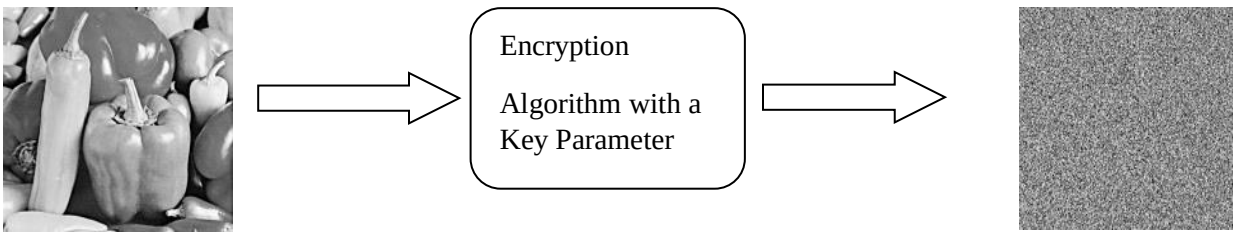
Keywords: *Internet; Security; Image Encryption; Cryptography; 2D Image; Access.*

Cite This Article: Jalpa Shah, and J S Dhobi. (2018). "REVIEW OF IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES FOR 2D IMAGES." *International Journal of Engineering Technologies and Management Research*, 5(1), 81-84. DOI: 10.29121/ijetmr.v5.i1.2018.49.

1. Introduction

Digital image processing is the use of computer algorithms to perform image processing on digital images. The input of that system is a digital image and the system process that image using efficient algorithms, and gives an image as an output.

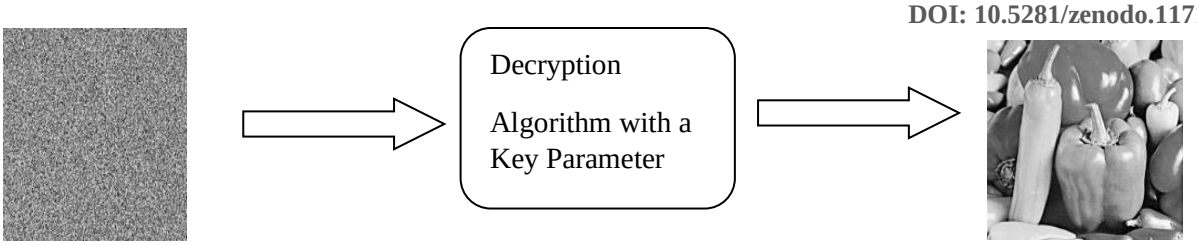
Image Encryption is the conversion of image to unknown format using some cryptography algorithm and a key. Similarly Image Decryption is the conversion of unknown format of image to original image using the decryption algorithm. The model of Image Encryption & Image Decryption is shown in Fig 1 and Fig 2 respectively.



Original Image Encrypted Image

Figure 1: Model of Image Encryption (Grayscale Image)

ISSN: 2454-1907
DOI: 10.5281/zenodo.1171480



Encrypted Image Original Image

Figure 2: Model of Image Decryption (Grayscale Image)

Based on the number of keys there are 2 types of Cryptography algorithms: Secret Key Algorithm in which only 1 key parameter is used to encrypt and decrypt the data(text, video, images, etc) and Private Key Algorithm in which 2 keys are used for encryption and decryption purpose. The former is known as Symmetric Key Algorithm and latter is known as Asymmetric algorithm.

The digital images have high correlation between adjacent pixels; hence traditional cryptography algorithms cannot be used.

2. Terminology in Image Encryption and Image Decryption

Various terms that are used in Image Encryption & Image Decryption Algorithms are described as under:

Plain image: A source or an original image is known as plain image.
Cipher image: encrypted or coded image is called cipher image.
Encryption or Enciphering: the process from transforming the plain image to cipher image is called Encryption or Enciphering.
Decryption or Deciphering: Restoring the plain image from cipher image is called Decryption or Deciphering.
Cryptography: The many schemes used for enciphering constitute the area of encryption that is known as cryptography.

Shannon, in one of the fundamental papers on the theoretical foundations of cryptography [1, 2], gave two properties that a good cryptosystem should have to hinder statistical analysis: diffusion and confusion. Diffusion means that if we change a pixel of the plain image, then several pixels of the cipher image should change, and similarly, if we change a pixel of the cipher image, then several pixels of the plain image should change. This means that frequency statistics of pixels in the plain image are diffused over several pixels in the cipher image, which means that much more cipher image is needed to do a meaningful statistical attack. Confusion means that the key does not relate in a simple way to the cipher image. In particular, each character of the cipher image should depend on several parts of the key.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1171480

3. Literature Review

The comparison of various image encryption algorithms is given in following table:

Paper	Technique Used	Merits	Demerits
Digital RGB Image Encryption Based on 2D Cat Map and Shadow Numbers[3]	2D Cat Map and Shadow method[RGB]	Shadow number uses 2 keys :1 as image another is derived using the equation	Key Sensitivity analysis not done. O/p of ACM and with shadow numbers does have much difference.
A New Fast Color Image Encryption Scheme using Chen Chaotic System[4]	Chen Chaotic System[RGB]	Less no of cipher rounds. Good security & Speed performance	Permutation and Diffusion are done by Chen System only.
A Chaotic Cryptosystem for Images based on Henon and Arnold Cat Map[5]	ACM and Henon Map	Various formats of images used	Other maps can be used
Image encryption based on Independent Component Analysis & Arnold's Cat Map[6]	ACM & ICA	Resistance to crypanalysis due to ICA.	2 images are used for Encryption purpose.. For Decryption JADE algorithm is used.
Image Encryption using Hybrid Chaotic map[7]	ACM with Henon& Logistic Map. [Grayscale]	Entropy and NPCR close to ideal values	Key sensitivity tests not done.
Image encryption using Camellia and Chaotic maps[8]	ACM and modified Camellia	Large key space and short encryption time	
Image Encryption using Chaos Theory [9]	Chirikov Map	Resitance to cryptanalysis	Only 1 map for both diffusion and confusion
Arnold's Cat Map algorithm in Digital Image Encryption[10]	ACM	Image pixel shuffled in RGB image	After fixed number of iteration ACM produces original image.
A Survey paper based on Image Encryption and Decryption using modified advanced encryption[11]	AES	AES better than blowfish, DES, 3DES	Due to close relation in adjacent pixels the AES is not much secure.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1171480

4. Conclusions and Recommendations

Thus the image encryption and decryption with the help of chaos system is better than the existing traditional algorithms. The paper gives only theoretical comparison of various methods.

References

[1] Shannon, C. E. (1948). The mathematical theory of communication. The Bell System Technical Journal, 27,379–423.
[2] Shannon, C. E. (1949). Communication theory of secrecy systems. The Bell System Technical Journal, 28, 656–715.
[3] Nidhai K. El Abbadi, Enas Yahiya, Ahmeda Aladilee. Digital RGB Image Encryption Based on 2D Cat Map and Shadow Numbers, IEEE, 2017.
[4] Chong Fu, Zhou-feng Chen, Wei Zhao, Hui-yan Jiang. A New Fast Color Image Encryption Scheme using Chen Chaotic System, IEEE, 2017.
[5] Ali Soleymani, Md Jan Nordin, and Elankovan Sundararajan. A Chaotic Cryptosystem for Images based on Henon and Arnold Cat Map, The Scientific World Journal, Hindawi, 2014.
[6] Nidaa Abdul Mohsin Abbas. Image encryption based on Independent Component Analysis & Arnold's Cat Map, Egyptioan Informatics Journal, ScienceDirect, 2016, Vol 17, Issue 1, pp. 139-146.
[7] Hikmat N. Abdullah, Hamsa A. Abdullah. Image Encryption using Hybrid Chaotic map, IEEE, 2017, pp. 121-125.
[8] Marwa S. Elpeltagy, Moataz M. Abdelwahab, Mohammed S. Sayed. Image encryption using Camellia and Chaotic maps, IEEE, 2015, pp. 209-214.
[9] Minal Govind Avasare, Vishakha Vivek Kelkar. Image Encryption using chaos theory, IEEE, 2015.
[10] Eko Hariyanto, Robbi Rahim. Arnold's Cat Map Algorithm in digital Image Encryption, IJSR, 2013, pp. 1363-1365.
[11] Yogita Verma, Neerja Dharmale. A Survey paper based on image encryption and decryption using modified advanced encryption standard, IJSR, 2013, pp. 352-355.

*Corresponding author.
E-mail address: jalpa08ce91@ gmail.com