International Journal of Multidisciplinary Research and Growth Evaluation.

A review of image processing through encryption and decryption

Sonia [1*], Mrinal [2]
[1] Research Scholar, Department of CSE, Meri College of Engineering, Sampla, Haryana, India
[2] Assistant Professor, Department of CSE, Meri College of Engineering, Sampla, Haryana, India

* Corresponding Author: **Sonia**

Article Info

ISSN (online): 2582-7138
Volume: 04
Issue: 01
January-February 2023
Received: 01-01-2023;
Accepted: 17-01-2023
Page No: 308-310

Keywords: Encryption, Decryption, data, image, review

Abstract
Security of images in multimedia software and applications is a major concern in the new Internet era. Encryption is the best way to ensure the safety of these images. When images are transmitted over unreliable networks using Image Encryption, it becomes difficult to analyze them. Additionally, it safeguards against unauthorized access. Data and personal information can be preserved in a variety of ways that have been investigated and developed. Image encryption is used to shield crucial data from unauthorized access. One of the most common methods for hiding data from unauthorised users is encryption.

Introduction

In recent years, the most pressing issue has been data integrity and security. Nowadays, nearly all data is transferred over computer networks, which has increased network attacks. In order to prevent multiple attacks, data must be encrypted and stored prior to transmission.

The use of computer algorithms to process digital images is known as digital image processing. A digital image is the system's input, which it processes using effective algorithms to produce an image as an output.

The process of hiding data through encryption involves changing the original text into cipher text. The data is encrypted using a variety of algorithms to produce various forms. For both encryption and decryption, the Cryptographic Algorithm makes use of a set of keys that are made up of various characters. The plain text is changed into the cipher text using the key, and the plain text is changed back into the cipher text for decryption. Data is transmitted and stored in a way that can only be accessed by authorized users in cryptography. Cryptography is a study of security of information by encoding it into indistinguishable structure. It is helpful approach to safeguarding the significant delicate data by involving numerical structure calculation for both encryption and unscrambling process. The key value determines the encryption and decryption procedures. The algorithm's strength is how difficult it is to get the original text and the key value. Depending on the keys, the algorithm is primarily divided into two types: symmetric and asymmetric. A symmetric algorithm is one in which the same keys are used for both the encryption and decryption processes. The stream and block ciphers of the symmetric algorithm are further subdivided. A block cipher is applied to a block of data, whereas a stream cipher is applied to a single byte of data. Two distinct keys are used in the asymmetric algorithm, one for encryption and the other for decryption. To prevent the message from being decrypted, the key should be kept secret. The reason for cryptography is to give Validation (demonstrating the one's personality), Non-renouncement (the recipient ought to realize the source ought not be faking), Respectability (information ought to be right, exactness, and reliability), and Security/privacy.

Review of literature

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.

In [3] the authors present a new Chaotic Key-Based Design for Image Encryption and Decryption. The VLSI architecture for image encryption and decryption algorithm is proposed. The XORed or XNORed bit-by-bit is used to predetermine keys for the chaotic binary sequence of the gray level of each pixel. There are the following features such as low computational complexity, no distortion, and high security. VLSI architecture has advantages such as low hardware cost, high computing speed, and hardware utilization efficiency. The architecture is also integrated with MPEG2 scheme and simulation results are also known.

In [4] the authors present a Modified AES Based Algorithm for Image Encryption. Most common technique to provide the security for image is encryption. There are wide applications of image and video such as internet communication, multimedia systems, medical imaging, tele medicine and military communication. There are different image protection techniques such as vector quantization. There are different methods for vector quantization where the image is decomposed into vectors where encoding and decoding is done by vector by vector. Or by dividing the image into desired form into large number of shadows that guarantee the undetectable to illegal users.

In [5] the authors present secure image encryption using AES. Security is the main and major issue in today's world. The transmission of image for communication has been increased and providing confidentiality from unauthorized access is the major task. It is difficult to provide an individual the security. There are various methods to protect the data from unauthorised user. AES is used for encryption and decryption of the image where the image using the key is converted into a form which cannot be recognised and later by authorised receiver it is converted back to original image.

In [6] the authors present an image encryption and decryption using AES algorithm. The design of effectively security for the communication of the image is done by using AES algorithm for encryption and decryption. AES has replaced Data Encryption Standard (DES) by providing more security. AES key expansion uses the 128 bit key for encryption process by using bit wise exclusive or operation of image set pixels.

In [7] the authors present an Image Encryption Based n AES Key Expansion. There are specific characteristics of image such has high rate of transmission with limited bandwidth, redundancy, bulk capacity and correlation among the pixels. These are characteristics has to be notice will encrypting the image. So, AES algorithm is used with the key expansion where encryption process is done by using bit wise exclusive or operation of image pixels set along with 128 bit key. The key is generated at the sender and receiver side based on the AES Key Expansion.

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

Table 1

Paper	Technique Used	Merits	Demerits
Digital RGB Image Encryption Based on 2D Cat Map and Shadow Numbers [8]	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 [9]	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 [10]	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 [11]	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 [12]	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 [13]	ACM and modified Camellia	Large key space and short encryption time	
Image Encryption using Chaos Theory [14]	Chirikov Map	Resitance to cryptanalysis	Only 1 map for both diffusion and confusion
Arnold's Cat Map algorithm in Digital Image Encryption [15]	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 [16]	AES	AES better than blowfish, DES, 3DES	Due to close relation in adjacent pixels the AES is not much secure.

Conclusion

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 CE. The mathematical theory of communication. The Bell System Technical Journal. 1948;27:379-423.
2. Shannon CE. Communication theory of secrecy systems. The Bell System Technical Journal. 1949;28:656-715.

3. Jui-Cheng Yen, Jim-In Guo. A New Chaotic Key-Based Design for Image Encryption and Decryption; c2000.
4. M Zeghid, M Machhout, L Khriji, A Baganne, R Tourki. A Modified AES Based Algorithm for Image Encryption; c2007.
5. P Radhadevi, P Kalpana. Secure Image Encryption Using Aes; c2012.
6. Roshni Padate, Aamna Patel. Image Encryption and Decryption Using Aes Algorithm; c2014.
7. Jose´ J. Amador, Robert W. Green, Symmetric-Key Block Cipher for Image and Text Cryptography; c2005.
8. Nidhai K, El Abbadi, Enas Yahiya, Ahmeda Aladilee. Digital RGB Image Encryption Based on 2D Cat Map and Shadow Numbers, Institute of Electrical and Electronics Engineers; c2017.
9. Chong Fu, Zhou-feng Chen, Wei Zhao, Hui-yan Jiang. A New Fast Color Image Encryption Scheme using Chen Chaotic System, Institute of Electrical and Electronics Engineers; c2017.
10. 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; c2014.
11. Nidaa Abdul Mohsin Abbas. Image encryption based on Independent Component Analysis & Arnold's Cat Map, Egyptioan Informatics Journal, Science Direct. 2016;17(1):139-146.
12. Hikmat N. Abdullah, Hamsa A. Abdullah. Image Encryption using Hybrid Chaotic map, IEEE; c2017;121-125.
13. Marwa S, Elpeltagy, Moataz M. Abdelwahab, Mohammed S. Sayed. Image encryption using Camellia and Chaotic maps, Institute of Electrical and Electronics Engineers; c2015;209-214.
14. Minal Govind Avasare, Vishakha Vivek Kelkar. Image Encryption using chaos theory, Institute of Electrical and Electronics Engineers; c2015.
15. Eko Hariyanto, Robbi Rahim. Arnold's Cat Map Algorithm in digital Image Encryption, International Journal of Science and Research; c2013;1363-1365.
16. Yogita Verma, Neerja Dharmale. A Survey paper based on image encryption and decryption using modified advanced encryption standard, International Journal of Science and Research; c2013;352-355.