Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 9, September 2019

IMAGE ENCRYPTION BY APPLYING SECURE HASH SHA-256: A REVIEW PAPER

Dr. Dinesh H.A
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: ha.dinesh@jainuniversity.ac.in

Abstract

A new image encryption algorithm based on chaos and SHA-256 is proposed in this paper in order to resolve the complexity of key management in "one-time pad" encryption systems and also resist the assault of selected plaintext. It adopts the structure of uncertainty and diffusion. First, to ensure that each encrypted result is different, the environment of a plaintext image is surrounded by a sequence created from the SHA-256 hash value of the plaintext. Secondly, by adding the disruption term associated with the plaintext to the chaotic sequence, the image is scrambled according to the random sequence obtained. Third, in the diffusion stage, the cypher text (plaintext) feedback mechanism of the dynamic index is adopted, i.e., the cypher text (plaintext) position index used for feedback is dynamic. In the "one time pad" encryption scheme, the above steps can ensure that the algorithm can avoid selected plaintext attacks and can resolve the complexity of key management.

Keywords: *Image Encryption, Image Data, Medical Areas, Security, Robots, Data protection.*

I. INTRODUCTION

Digital image processing technology has also rapidly evolved and penetrated into all areas of life in recent years with the rapid growth of computer technology, such as remote sensing, industrial detection, medicine, meteorology, connectivity, investigation, intelligent robots, etc. Image data has, thus, drawn widespread interest [1]. Security of image data is very important, especially in special military, commercial and medical areas [2]. Image encryption has become one of the ways to protect digital image transmission. Image data, however, has the characteristics of large volumes of data, strong correlation and high redundancy, leading to low encryption efficiency and low security, so conventional encryption algorithms such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) do not satisfy image encryption needs [3].

Fig. 1: Illustrates the Real Images and Encrypted Images.

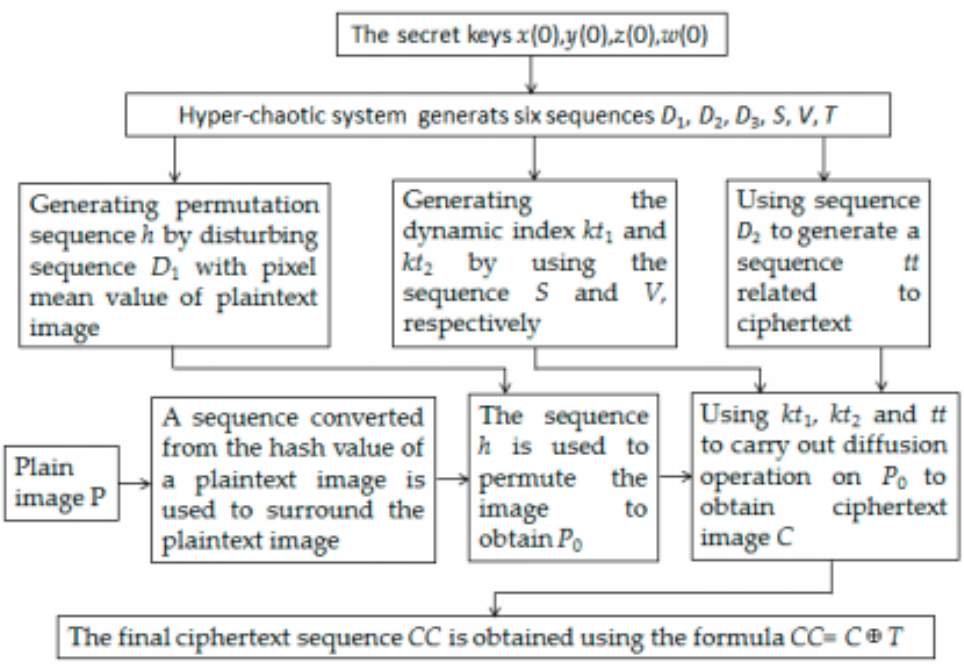

Fig. 2: Illustrates The Flow Chart of The Encryption Scheme Procedure.

A hash function is a function which may be utilized in order to map the data of arbitrary size to data of a fixed size. Here, we utilize the SHA-256 to originate the 256-bit hash value V, that can be segregated into 32 blocks with the same size of 8-bit, the i-th block vi ∈ [0, 255], i = 1, 2, . . . , 32, so it can be expressed as V = v1, v2, . . . , v32. Suppose the size of the plain-image P is m × n, obtain an integer k as:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

$$cov\,(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\;(y_i - E(y))$$

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\sqrt{D(x)}\; \neq 0, \sqrt{D(y)} \neq 0$$

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\ \%$$

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C1(i,j) - C2(i,j)|}{255}\right] \times \frac{100\%}{M \times N}$$

Another critical constraint is the correlation coefficient to ensure that the encryption algorithm is very accurate. The expression is given below [4].

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Where $C(x,y), D(x)$ and $D(y)$ may be evaluated by utilizing the following equations [5].

$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))^2$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(y))^2$$

II. LITERATURE REVIEW

Zhou et al. conducted a review on image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transformation. Most of the current image encryption

techniques bring security risks for linear transformation or are extended by encryption data for direct adoption of nonlinear transformation. A novel image compression-encryption scheme is proposed to solve these difficulties by integrating 2D compressive sensing with nonlinear fractional Mellin transformation. In this scheme, the original image is measured in two directions by measurement matrices to simultaneously achieve compression and encryption, and then the nonlinear fractional Mellin transform re-encrypts the resulting image. The measuring matrices are managed by a map of chaos. To obtain the decryption image, the Newton Smoothed l0 Standard (NSL0) algorithm is applied. The results of the simulation verify the validity and reliability of this regime [6].

III. DISCUSSION AND CONCLUSION

A new image encryption method that includes three key components is proposed: inserting image pixels, pixel scrambling, and pixel diffusion. First, the plaintext image hash value is transformed into a pseudo-random sequence, then pseudo-random sequences are applied to the plaintext image field surrounding it. In the permutation and diffusion method, the pseudo-random sequences used are connected to the plaintext image, which can resist the selected plaintext attack. Our algorithm converts the hash value of the plaintext image, unlike previous algorithms, into a pseudo-random sequence, which takes the pseudo-random sequence as part of the encrypted image, whereas the previous algorithm takes the plaintext image's hash value as part of the key. The key of the encryption scheme is just the initial value of the chaotic system in our encryption algorithm, minimizing the complexity of key management.

IV. REFERENCES

[1] E. N. Kumar and E. S. Kumar, “A Simple and Robust EVH Algorithm for Modern Mobile Heterogeneous Networks- A MATLAB Approach,” 2013.

[2] S. K. Sabnis and R. N. Awale, “Statistical Steganalysis of High Capacity Image Steganography with Cryptography,” 2016, doi: 10.1016/j.procs.2016.03.042.

[3] M. Kumari, S. Gupta, and P. Sardana, “A Survey of Image Encryption Algorithms,” *3D Res.*, 2017, doi: 10.1007/s13319-017-0148-5.

[4] S. Kumar, A. Gupta, and A. Arya, *Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio*. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)/ISSN(Online): 2320-9801, 2016.

[5] M. Khan and T. Shah, “A Literature Review on Image Encryption Techniques,” *Autoimmunity Highlights*. 2014, doi: 10.1007/s13319-014-0029-0.

[6] N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, “Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform,” *Opt. Commun.*, 2015,

doi: 10.1016/j.optcom.2014.12.084.