Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 8, August 2019

HYBRID METHODS OF PICTURE ENCRYPTION AND DECRYPTION: AN ANALYTICAL STUDY

Hari Krishna Moorthy
Faculty of Engineering and Technology
Jain (Deemed-to-be University), Ramnagar District, Karnataka - 562112
Email Id- hari.moorthy@jainuniversity.ac.in

Abstract:

To encrypt digital media, the majority of imaging techniques use symmetrical and asymmetric cryptography algorithms. In the literature, most of the academic papers concentrate mainly on the Advanced Encryption Standard (AES) encryption and decryption algorithm. This paper proposes an analysis of Elliptic Curve Cryptography (ECC) with Hill Cipher (HC), ECC with Advanced Encryption Standard (AES) and ElGamal with Double Playfair Cipher hybridization for image encryption and decryption by hybridization (DPC). This study is based on the following parameters: I time of encryption and decryption, (ii) encrypted image entropy, (iii) decrypted image intensity loss, (iv) PSNR (Peak Signal to Noise Ratio), (v) Number of Pixels Changing Rate (NPCR), and (vi) Unified Average Changing Intensity (UACI). The hybrid method involves the speed and ease of symmetric algorithm implementation, as well as enhanced asymmetric algorithm security. Asymmetric key cryptography is supported by ECC and ElGamal cryptosystems, while symmetric key algorithms include HC, AES, and DPC.

Keywords: *Encryption and Decryption; Peak Signal to Noise Ratio; Number of Pixels Change Rate (NPCR); Unified Average Changing Intensity (UACI); Lossy Compression.*

I. INTRODUCTION

Color image encryption techniques are highly demanded to ensure the secrecy of the image data during transmission over insecure networks around the globe. Due to the growth of multimedia applications worldwide, various studies on pragmatic image encryption techniques have been investigated from the confidentiality perspective of color photos [1]. The techniques of color image encryption plays a key role in maintaining the privacy of the strikers' sensitive image data globally over the internet. In order to preserve the quality of the colored images, there are many ways that are used to ensure the quality of the images during decryption. Privacy is one of the tough components that require more attention to safe worldwide image data [2]. In contrast to the grey images, the color images provide enormous data to be used extensively in the communication arena [3].

A. **Correlation examination of the colored images: -**

The similarity analysis of color pictures is performed using the following formulas. In order to determine the similarity between the two adjacent pixels of the plain image as well as the cypher image, correlation plays a critical role. By utilizing the following formulas, one can calculate the correlation coefficient of the image [4].

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

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

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

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

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

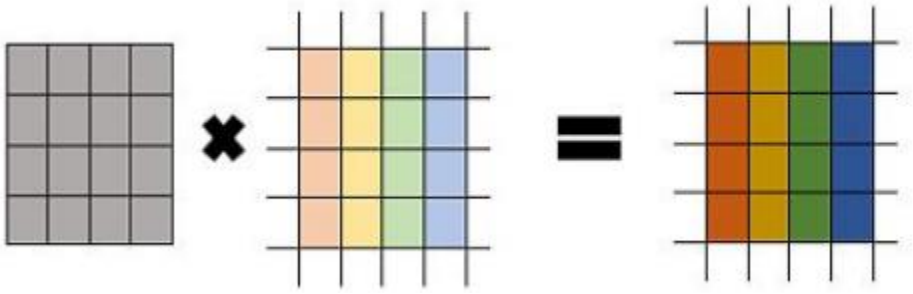

Fig. 1 Illustrates elliptic curve cryptography (ECC) with hill cipher.

B. **Differential examination of the colored images: -**

In order to lose the picture data through the communication channel during the transmission, there are some parameters that ensure the vulnerability of the various color image formats against the different attacks from the strikers. The Amount of Pixel Change Rate (NPCR) and the Strength Shifting Unified Average (UACI). The formulas for the NPCR and UACI calculation for a colored picture are given in below [5].

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

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

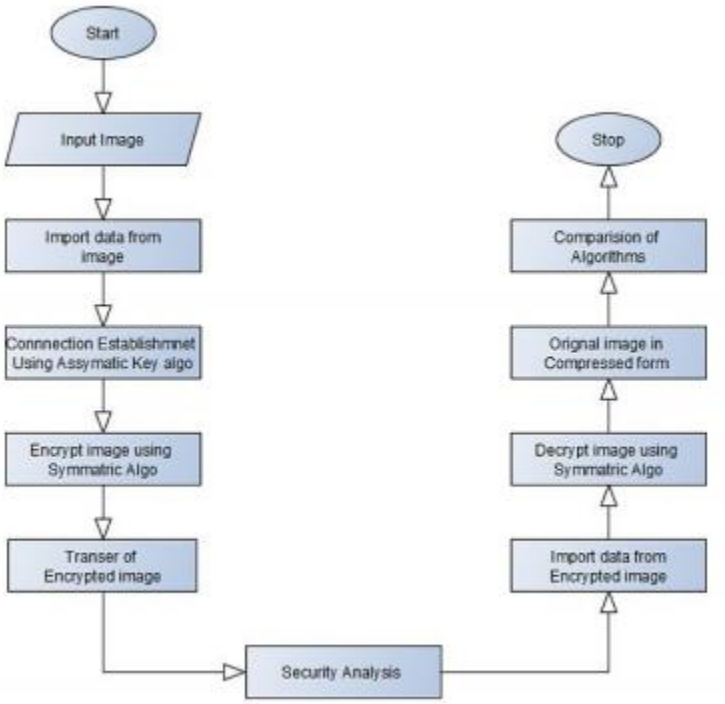

Fig. 2 Illustrates the flow chart for image encryption and decryption.

II. LITERATURE REVIEW

Zhou et al. investigated another novel image encryption algorithm based on chaos and Line map. Data security boundaries have become increasingly blurred in the era of big data. Our defense of privacy is undergoing a new round of testing. In particular, multimedia big data photos also hold several secrets or data regarding privacy. In the processing and transmission of image content, how to ensure protection and authorize access to sensitive data becomes a hot issue of urgency. In this post, we propose a new algorithm for symmetrical image encryption based on the skew tent map. The proposed algorithm is ideal for encryption of any image size using a new chaos-based line map [6].

Chai et al. investigated a color image cryptosystem based on dynamic DNA encryption and chaos. This paper introduces a cryptosystem of color images based on complex DNA encryption and chaos. First, the plain color image is decomposed into red, green and blue elements, and then a plain-text-dependent simultaneous intra-inter-component permutation mechanism (SCPMDP) is introduced to shuffle them. Secondly, a DNA encoding rule transforms the recombined permutable components into a DNA matrix.

III. DISCUSSION

Figures 2 display the flow diagram for the proposed hybrid encryption and decryption algorithm. The key created by the Elliptical Curve Sensors 2020, 20, 5162 9 of 18 Cryptography (ECC) asymmetric key algorithm is used to create a relation [2]. The picture encryption is achieved using the Elliptic Curve Cryptography (ECC) symmetric hybrid algorithm with Hill Cipher, Advanced Encryption Standard (AES) ECC, and Double Playfair Cipher ElGamal [7].

Correlation coefficient:

Another critical constraint is the correlation coefficient to ensure that the encryption algorithm is very accurate. The expression is given below [8].

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

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

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

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

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

IV. CONCLUSION

Digital images are critical images that, by network channel transmission, must be protected against intruders. Different imaging methods are used to encrypt images using symmetrical algorithms of asymmetry and encryption. Only either symmetrical encryption and decryption or asymmetric encryption and decryption are supported by many picture algorithms. Three separate hybrid approaches, such as Hill Cipher ECC, Sensors 2020, 20, 5162 16 of 18 Advanced Encryption Standard ECC and Double Playfair Cipher ElGamal, have been studied for the implementation of image encryption. Test cases are evaluated using a set of grayscale and colored images, as well as

performance metrics. We can deduce the algorithm is better suited to the user's needs when calculating all the parameters such as Encryption Time, Decryption Time, Entropy, and Squared Error in Decrypted Image, PSNR, NPCR, and UACI. With lower values of encryption and decryption time, the result indicates effectiveness. Entropy Value, the proposed hybrid algorithm, has closed to 8, which is better than current algorithms. In the Decrypted image, we obtain the lower value of Squared Error that has proven better than other algorithms. The PSNR value, however, is greater by the metric scales and the greater the NPCR value, the better the algorithm is, and the higher the UACI value means that it is safer from attacks.

v. REFERENCES

[1] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, 2015, doi: 10.1016/j.sigpro.2014.10.033.

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

[3] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Processing*, 2017, doi: 10.1016/j.sigpro.2017.04.006.

[4] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, 2018, doi: 10.1016/j.optlastec.2017.10.024.

[5] X. Zhang and W. Chen, "A new chaotic algorithm for image encryption," 2008, doi: 10.1109/ICALIP.2008.4590187.

[6] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing*, 2015, doi: 10.1016/j.neucom.2014.11.095.

[7] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: A survey," 2014, doi: 10.1109/ICSIP.2014.80.

[8] Sanjeev Kumar, "Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 4, no. 8, 2016.

Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 8, August 2019