ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940
www.ijsem.org
Vol 14, Issuse.4 Nov 2023

FAST IMAGE ENCRYPTION BASED ON RANDOM IMAGE KEY

MR.LAXMIPURAM SUNEEL[1], ANKAM ARUNRAJ[2],BURSOO BRAHMA TEJA[3], KURVA PRAVEEN KUMAR[4] ,

Abstract—

Unsecured networks have recently become widely used for the transmission of confidential images. Consequently, cryptography is crucial for ensuring data cofidentiality. Developing a key that is resistant to statistical and differential attacks has always been a challenging objective. In this paper, a novel model is proposed to boost image encryption while maintaining key strength. The proposed model adapts MD5 and SHA-256 hash functions to produce a key. It generates four matrices, X, Y, Z, and W, by using a memristor hyperchaotic system. Arnold's transform was applied to the original image once the key was created. The images were then scrambled using five chaotic maps. The image is then DNA-encoded, diffused using three matrices, and finally DNA-decoded. The proposed model was assessed using twelve performance measures on nine popular images. Compared to previous studies, the results of the proposed model indicate a promising improvement in performance. It achieves a better performance by expanding the key space and increasing its sensitivity

1.INTRODUCTION

In recent years, image data has become increasingly significant. As a result, researchers have begun to search for techniques to handle such data. Cryptography is a scientific field in which they can be applied. Different approaches were applied to the images. Many cryptography systems have recently relied on chaotic systems, Arnold's transformations, and DNA encoding.Chaotic systems are used in many encryption systems owing to their main qualities, including sensitivity to the starting conditions and parameters, strong ergodicity, mixing capability, and highly intricate behavior. However, many chaotic encryption techniques are insecure and susceptible to cryptanalysis, preventing the use of purely chaotic systems in encryption [1]. Arnold's transformation function has several essential characteristics that lead to its use in cryptanalysis: it has a high degree of ergodicity and applies image cutting. However, they cannot be used in cryptography. The image histogram graph does not change because it changes the position of the pixels only, without changing their values. Because

[1] Asst.Professor in Department of Electronics and Communication Engineering,
[2.3.4]Student, Department of Electronics and Communication Engineering,
CMR Institute of Technology,
Hyderabad, Telangana, India.501401
[1] suneel.laxmipuram@cmritonline.ac.in , [2] arunrajankam@gmail.com , [3] brahmateja5351@gmail.com , [4]praveentej6521@gmail.com .

ISSN2454-9940
www.ijsem.org
Vol 14, Issuse.4 Nov 2023

of its advantages, DNA encoding is commonly employed in cryptanalysis. It has a great number of parallelisms, high information density, and it uses very little power. It does, however, have some limitations. DNA encryption rules can be predicted easily if they are combined with lowdimensional chaotic map. Another limitation is that the DNA rules should be related to the original image to improve the security of the encryption system [2]. These methods have recently been used in encryption. Some models have applied DNA encoding, phase-truncated fractional Fourier transform, Hyper-Chaos System, Arnold's transform, and SHA-256 hash function. The primary purpose of the encryption system is to generate the key. Extra encryption layers are required on the original image. Other models relied on chaotic maps only. Their main problem is to boost encryption levels. However, these models lacked a

strong key, which leads to the risk of being easily cracked. Two MD5 generated sequences were used in other models to generate the encryption key, which was then used to scramble chaotic maps with the DNA-encoded image. These models require additional encryption layers. To overcome these shortcomings, we propose a novel model which raises the levels of encryption while increasing the

security of the key. The proposed model starts by applying MD5 to the original image and its metadata in order to generate two keys. Both keys are then concatenated and run through SHA-256 to generate a final 256-bit hexadecimal integer, which is then fed into certain specific calculations

To generate the secret key

to generate the secret key. The Arnold's transform algorithm settings, the Hyper-Chaos System beginning values, and the encryption and decryption procedures constitute the key. The Hyper-Chaos System is then utilized to construct four matrices, which are subsequently diffused with the image. The third step is to apply the Arnold's transform algorithm to the original image, and the resulting image is then successively entered into the five chaotic maps. Finally, the result is encoded to DNA, diffused with the three matrices formed by the Hyper-Chaos System, and DNA-encoded, with the resulting image being DNA-decoded and the cipher image is obtained. To ensure that the model is efficient, it is evaluated on nine grayscale images using twelve evaluation measures. The key space and key sensitivity measure the key strength, while

Histogram analysis, Chi-square test, Correlation Coefficient Adjacent (CCA) analysis, Information Entropy, Irregular Deviation, NPCR, UACI, and MSE measure the efficiency of

the model. To measure the computational complexity of the model, computation analysis and time analysis are applied on the model. Compared to previous studies, the results of the proposed model show a promising improvement in performance. Regarding the key analysis, the model assumes a wide key space and is highly affected by minor changes. The cipher images' histograms are eventually distributed which is proven in chi-square results. The difference between information entropy of the cipher image from the original image indicates

great randomness, which is also visible in the correlation coefficient analysis of adjacent pixels of the cipher image and the irregular deviation analysis. The execution time of encryption and decryption processes vary since the key generation steps depend on the image size. It also appears in the computational complexity of the model. NPCR and UACI results show that even minor changes in the original image are causing great changes in the cipher image. MSE results

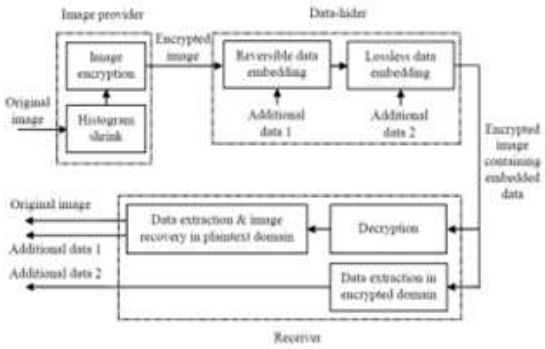
reveal that different features in encryption layers expand the space between the original and encrypted images. The contributions of this work consist of:

- Proposing a novel gray-scale image encryption model using DNA operations.
- Proposed model raises the encryption levels while enhancing the key security.
- Proposed model is comprehensively assessed using twelve performance measures on nine images.

3.BLOCK DIAGRAM

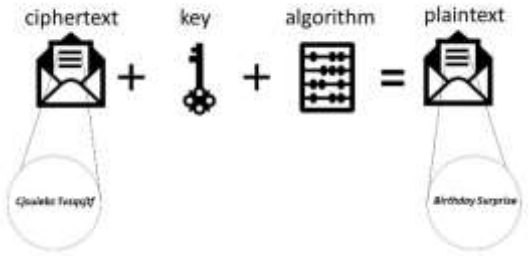
INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940
www.ijsem.org
Vol 14, Issuse.4 Nov 2023



4 PROPOSED SYSTEM

This paper proposes a lossless, a reversible, and a combined data hiding schemes for public-key-encrypted images by exploiting the probabilistic and homomorphic properties of cryptosystems. With these schemes, the pixel division/reorganization is avoided and the encryption/decryption is performed on the cover pixels directly, so that the amount of encrypted data and the computational complexity are lowered. In the lossless scheme, due to the probabilistic property, although the data of encrypted image are modified for data embedding, a direct decryption can still result in the original plaintext image while the embedded data can be extracted in the encrypted domain. In the reversible scheme, a histogram shrink is realized before encryption so that the modification on encrypted image for data embedding does not cause any pixel oversaturation in plaintext domain. Although the data embedding on encrypted domain may result in a slight distortion in plaintext domain due to the homomorphic property, the embedded data can be extracted and the original content can be recovered from the directly decrypted image. Furthermore, the data embedding operations of the lossless and the reversible schemes can be simultaneously performed in an encrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption.



5 LOSSLESS DATA HIDING SCHEME

In this section, a lossless data hiding scheme for public-key-encrypted images is proposed. There are three parties in the scheme: an image provider, a data-hider, and a receiver. With a cryptosystem possessing probabilistic property, the image provider encrypts each pixel of the original plaintext image using the public key of the receiver, and a data-hider who does not know the original image can modify the ciphertext pixel-values to embed some additional data into the encrypted image by multi-layer wet paper coding under a condition that the decrypted values of new and original cipher-text pixel values must be same. When having the encrypted image containing the additional data, a receiver knowing the data hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image. In other words, the embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption since the decrypted image would be same as the original plaintext image due to the probabilistic property. That also means the data embedding does not affect the decryption of the plaintext image. The sketch of lossless data hiding scheme is shown in Figure 1.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

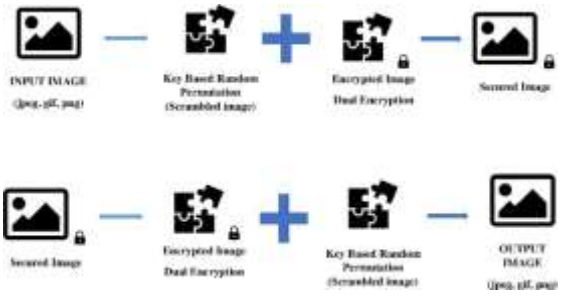
ISSN2454-9940
www.ijsem.org
Vol 14, Issuse.4 Nov 2023

Lossless Data Hiding Scheme

- A lossless data hiding scheme for public-key-encryptedimages is proposed. There are three parties in the scheme: an image provider, a data-hider, and a receiver.
- With a cryptosystem possessing probabilistic property, the image provider encrypts each pixel of the original plaintext image using the public key of the receiver, and a data-hider who does not know the original image can modify the ciphertext pixel-values to embed some additional data into the encrypted image by multi-layer wet paper coding under a condition that the decrypted values of new and original cipher-text pixel values must be same.
- When having the encrypted image containing the additional data, a receiver knowing the data hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image.
- The embedded data can be extracted in the encrypteddomain, and cannot be extracted after decryption since the decrypted image would be same as the original plaintext image due to the probabilistic property.

Reversible Data Hiding Scheme.

- This section proposes a reversible data hiding scheme for public-key-encrypted images. In the reversible scheme, a preprocessing is employed to shrink the image histogram, and then each pixel is encrypted with additive homomorphic cryptosystem by the image provider.
- When having the encrypted image, the data-hider modifies the ciphertext pixel values to embed a bit-sequence generated from the additional data and error-correction Due to the homomorphic property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values, implying that a decryption can be implemented to obtain an image similar to the original plaintext image on receiver side.
- Because of the histogram shrink before encryption, the data embedding operation does not cause any overflow/underflow in the directly decrypted image. Then, the original plaintext image can be recovered and the embedded additional data can be extracted from the directly decrypted image.
-



Combined Data Hiding Scheme

- A lossless and a reversible data hiding schemes for public-key-encrypted images are proposed. In both of the two schemes, the data embedding operations are performed in encrypted domain.
- On the other hand, the data extraction procedures of the two schemes are very different. With the lossless scheme, data embedding does not affect the plaintext content and data extraction is also performed in encrypted domain.

6. CONCLUSIONS

This work proposes a lossless, a reversible, and a combined data hiding schemes for cipher-text images encrypted by public key cryptography with probabilistic and homomorphic properties. In the lossless scheme, the ciphertext pixel values are replaced with new values for embedding the additional data into the LSB-planes of ciphertext pixels. This way, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, a preprocessing of histogram shrink is

made before encryption, and a half of ciphertext pixel values are modified for data embedding. On receiver side, the additional data can be extracted from the plaintext domain, and, although a slight distortion is introduced in decrypted image, the original plaintext image can be recovered without any error. Due to the compatibility of the two schemes, the data embedding operations of the lossless and the reversible schemes can be simultaneously performed in an encrypted image. So, the receiver may extract a part of embedded data in the encrypted domain, and extract another part of embedded data and recover the original plaintext image in the plaintext domain.

ACKNOWLEDGMENT

We are extremely grateful to Dr.M.JangaReddy, Director, Dr.B.Satyanarayana, Principal and Dr.K.Niranjan Reddy, Head of Department Electronics and Communication Engineering, CMR Institute of Technology for their inspiration and valuable guidance during the entire duration.

We are extremely thankful to our guide Mr.L.Suneel, Assistant Professor in Department of ECE , CMR Institute of Technology for his constant guidance, encouragement and moral support throughout the project.

REFERENCES

[1] N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, "High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," *Digital Signal Processing*, 20, pp. 1629−1636, 2010.

[2] J. Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE Trans. on Circuits and Systems for Video Technology*, 13(8), pp. 890−896, 2003.

[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," *IEEE Trans. on Circuits and Systems for Video Technology*, 16(3), pp. 354−362, 2006.

[4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless Generalized-LSB Data Embedding," *IEEE Trans. on Image Processing*, 14(2), pp. 253–266, 2005.

[5] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding," *IEEE Trans. on Information Forensics and Security*, 10(3), pp. 653-664, 2015.

[6] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," *IEEE Trans. on Multimedia*, 15(2), 316−325, 2013.

[7] W. Zhang, X. Hu, X. Li, and N. Yu, "Optimal Transition Probability of Reversible Data Hiding for General Distortion Metrics and Its Applications," *IEEE Trans. on Image Processing*, 24(1), pp. 294-304, 2015.

[8] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative Encryption and Watermarking in Video Compression," *IEEE Trans. on Circuits and Systems for Video Technology*, 17(6), pp. 774−778, 2007.

[9] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A Commutative Digital Image Watermarking and Encryption Method in the Tree Structured Haar Transform Domain," *Signal Processing: Image Communication*, 26(1), pp. 1−12, 2011.

[10] X. Zhang, "Commutative Reversible Data Hiding and Encryption," *Security and Communication Networks*, 6, pp. 1396−1403, 2013.

[11] X. Zhang, "Reversible Data Hiding in Encrypted Image," *IEEE Signal Processing Letters*, 18(4), pp. 255−258, 2011.

[12] W. Hong, T.-S. Chen, and H.-Y. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," *IEEE Signal Processing Letters*, 19(4), pp. 199−202, 2012.

[13] J. Yu, G. Zhu, X. Li, and J. Yang, "An Improved Algorithm for Reversible Data Hiding in Encrypted Image," *Proceeding of the 11th International Workshop on Digital-Forensics Watermark (IWDW 2012)*, Shanghai, China, Oct. 31-Nov. 02, 2012, Lecture Notes in Computer Science, 7809, pp. 358-367, 2013. [14] W. Puech, M. Chaumont, and O. Strauss, "A Reversible Data Hiding Method for Encrypted Images," *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, *Proc. SPIE*, 6819, 2008.

[15] X. Zhang, "Separable Reversible Data Hiding in Encrypted Image," *IEEE Trans. Information Forensics & Security*, 7(2), pp. 526−532, 2012.

[16] Z. Qian, X. Zhang, and S. Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream," *IEEE Trans. on Multimedia*, 16(5), pp. 1486−1491, 2014