Indonesian Journal of Electrical Engineering and Computer Science
Vol. 27, No. 3, September 2022, pp. 1698~1703
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v27.i3.pp1698-1703

Chaotic map technique for enhancement security for android mobile system based on image encryption

Kawther Thabt Saleh[1], Nisreen Abd Alhadi Jabr[2], Iman Hussein Al-Qinani[1]
[1]Department of Computer Science, College of Education, Mustansiriyah University, Baghdad, Iraq
[2]Branch of Teams Games, College of Physical Education and Sports Science, Mustansiriyah University, Baghdad, Iraq

Article Info

Article history:

Received Sep 18, 2021
Revised Jun 5, 2022
Accepted Jun 26, 2022

Keywords:

Android
Chaotic schemes
Image encryption
Mobile
Security

ABSTRACT

Network security continues to be the priority of many organizations. To ensure the protection of their data, they pay great attention to Encryption systems. Moreover, because of the enormous developments in networks of connection particularly the internet which has used by several people to share a variety of data kinds. The security of data has been a significant issue. As a result, there is a significant focus in using methods of decryption and encryption. Numerous encryption techniques have become advanced to preserve data protection, chaotic encryption systems are one of these methods widely used in recent years, where several techniques were proposed to use a chaotic map for encrypt images for the reason that of their characteristics e.g., random action unpredictability and initial conditions sensitivity. In this paper, proof authentication of sent information is used chaotic encryption algorithm to provide cipher text and hidden in image then send to another user. This approach is applied in cellular operating system environment (android). Thus, the sending and receiving of text will be safe and secure. The proposed approach is tested on different types of mobile. The proposed system gives good results.

Corresponding Author:

Nisreen Abd Alhadi Jabr
Branch of Teams Games, College of Physical Education and Sports Science, Mustansiriyah University
Baghdad, Iraq
Email: nisreen1987@uomustansiriyah.edu.iq

1. INTRODUCTION

Due to the requirement to interchange and keep certain kinds of information like aural, films, movie clips, images, and text through the network, which is the area where the information exchanged is easy to penetrate, encryption methods have been used to safeguard information from the unlawful arrival [1]-[5]. Image encryption is the generality helpful technique to protect private when save or transmitting photos over communications media. Military communications, multimedia schemes, medical research, online communications, and other applications for image encryption are possible. Images have certain physical characteristics, such as less sensitive, enormous storage power, data similarity and redundancy amid neighboring pixels that are different from text [6]-[10]. Many encryption techniques have arisen to get rid of these problems posed by image encryption. Several traditional encryption algorithms have been employed for many years for instance, data encryption standard triple (DES), Rivest-Shamir-Adleman (RSA), advanced encryption standard (AES), and DES [11], [12], but for image encryption these algorithms are not useful [13], [14], particularly when the size of the image is great [15]-[17]. More helpfulness has been paid recently to chaos-based techniques of image encryption [18]-[21]. We will illustrate the literature review in section 2, the preliminary concepts in section 3, the proposed system's general structure in section 4, experiment results and discussion in section 5. lastly, the conclusions are given in section 6.

2. LITERATURE REVIEW

There are several studies based on chaotic map that have been investigated in the last decade relevant to image encryption. Some of these studies will be discussed in this section. Liu and Wang [22] applied higher dimension and bit-level Chaotic method to encrypt a color image. They converted the color to gray image (Rx3C), then converted it to binary image and permuted it using a piecewise linear Chaotic method. Lastly, the chen framework was applied for disperse and confuse the 3-bands.

Maryoosh [23] presented the unprecedented image encryption framework depends on the Lorenz system, substitution-box, and polynomial map. The suggested mechanism encrypts 128-byte blocks then decrypts them. The plain image was initially perplexed, but the permutation algorithm made the result, after which the input block by block was replaced via the substitution-box variable and the key phases were added. The resulting exclusive-OR (XOR) image was generated by a logistic map with another encrypted key, and then the resulting image was confused again.

For image encryption, Wang *et al*. [24] uses period changes in bits of pixels and the Chaotic process. The random integer numbers of the like size such as the main image used for the cycle shift process. Thereafter, they used a Chaotic method to create a key that could be applied for encrypt the scrambled image.

3. PRELIMINARY CONCEPTS

3.1. Chaotic systems

The near association between Chaotic systems and cryptography contributes to the best option for data encryption using chaos-based algorithms. It is advantageous to have an encryption scheme that takes less time to execute for real-time applications, but without sacrificing the desired security. A strong mixture of protection, high speed and less power consumption is the chaos-based encryption technique. Chaotic device properties, for example sensitivity to primary parameters and conditions. randomness has attracted researchers' attention, as these characteristics actually fulfill the essential principles of the design of cryptographic algorithms. Chaos-based algorithms have revealed superior features in complexity and security using these favorable characteristics [25].

3.2. Android

Android is a mobile touchscreen Operating system depending on a make- over of the Linux kernel and additional open-source programmers that is specifically advancement for smartphones and tablets. android auto for vehicles, android tv for televisions, Google has continued to create android wear for wristwatches, each it has graphical user interface (GUI) [26], [27]. Android is also used in personal computer (PCs), digital cameras, game consoles, and other mobile devices. It was created from the ground up for the aim of becoming the first full, accessible, and free platform created exclusively for mobile devices. Android is a free and open interface that anyone can use [28].

4. PROPOSED SYSTEM'S GENERAL STRUCTURE

The proposed structure aims to improve the security of mobile image-embedded content. This approach is carried out depending on the source of the Android operating system in order to develop presentation. First, Algorithm 1 depicts the system's proposed general algorithm. The flowchart in Figure 1 display the general nature for encryption mechanism and the hidden of the proposed scheme. Following that, the flowchart in Figure 2 depicts the general nature of the decryption mechanism and extraction of the suggested scheme.

4.1. Execution of the proposed system

In this work, the implementation of the offered framework is according to algorithm 1. The proposed framework is intended to boost the hiding text output in mobile's images. The platform which used in this work is java. The proposed approach is tested on different types of mobile the Android operating system is the source of mobile's images. As shown in:

a. Steps in sender side:

- Step1: Write the plain text “secret text that must be hidden” to platform mobile (Home Window) as shown in Figure 3.
- Step2: Click on the button "encryption" for encryption operation is done on the plain text using Chaotic algorithm, the result of this step is cipher text” y0JX_&uaoM~`=|\tD_'5hO.=|N[M<” as illustrated in Figure 4.
- Step3: Click on the button "hidden info" will move to Hidden Info Interface as shown in Figure 5 in order to embedding important information inside image for security purpose by using XOR operation.

- First, click on the button "open picture gallery" for the image is loaded from the gallery which may be found in mobile's memory, as shown Figure 6. Then click on the button "hidden by XOR Method" to embed the cipher text in the image, as shown in Figure 7.
- Step 4: Click on the button "save picture" to save picture after end embedding operation as shown in Figure 7.

Algorithm 1. General algorithm of proposed system

Side of sender
Input: Plain text
Output: Cipher text hidden in image
Step1: Enter the plain text.
Step2: Chaotic algorithm is used to encrypt text; the output of the encryption operation is a cipher text.
Step3: Load image, and then using the XOR operation performs on bits stored in pixels at part alpha position.
Step4: Save the image.
Step5: End.

Side of receiver
Input: Image with hidden cipher text
Output: Plain text
Step1: Load the image with hidden text (image saved in sender side).
Step2: Extract the cipher text from the image by the XOR embedding operation.
Step3: After extraction of cipher text from image, decryption is carried out using Chaotic algorithm.
Step4: The result from decryption operation is plain text after using Chaotic algorithm.
Step5: End.

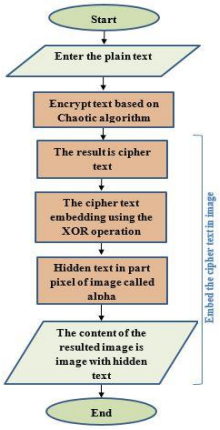

Figure 1. Flowchart of the suggested system for encryption and hidden information (side of sender)

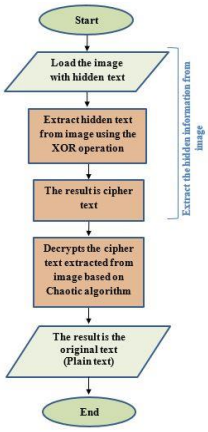

Figure 2. Flowchart of the suggested system for extraction process and decryption information (side of receiver)

Figure 3. Input plain text in home window application homepage (sender side)

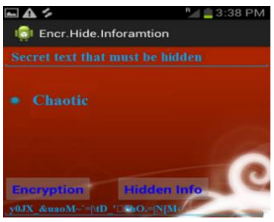

Figure 4. The cipher text is resulted by chaotic algorithm (sender side)

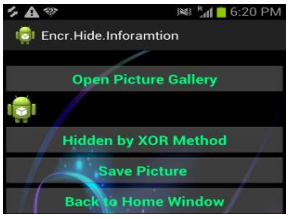

Figure 5. Hidden info interface (sender side)

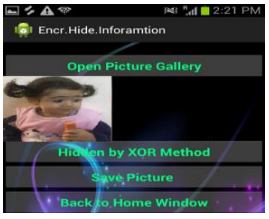

Figure 6. Load the image (sender side)

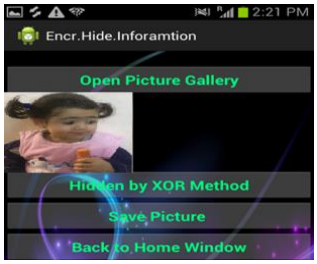

Figure 7. Embedding operation and save image (sender side)

b. Steps in receiver side:

- Step1: (Extract Information Interface) in side of receiver presented in Figure 8. The receiver can extract hidden information from image, via the click on the button "Open Picture Gallery" to load image from mobile as shown in Figure 9.
- Step2: Extract the cipher text from the image by the XOR embedding operation by click on the button "Extract Info from Picture" show in Figure 10.
- Step3: Decryption operation for extracted information is done by using Chaotic algorithm. The cipher text" y0JX_&uaoM~`=|\tD_'5hO.=|N[M<" decrypted by using Chaotic algorithm.
- Step4: The result of decryption operation is original text" Secret text that must be hidden" as shown in Figure 11.

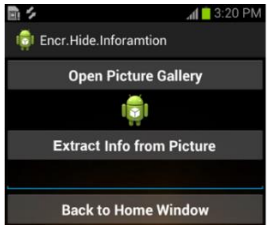

Figure 8. Extract information interface (receiver side)

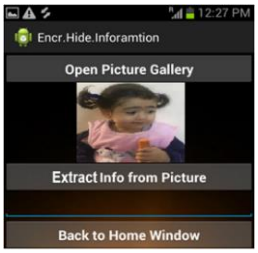

Figure 9. Load the image with hidden text (receiver side)

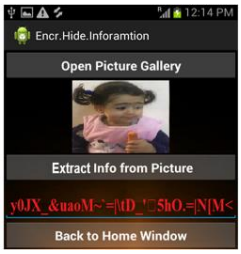

Figure 10. Extract information from picture (receiver side)

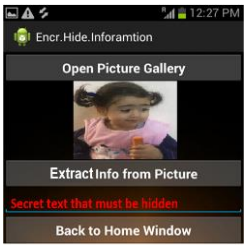

Figure 11. Decryption by using chaotic algorithm (receiver side)

5. EXPERIMENT RESULTS AND PROPOSED SYSTEM DISCUSSION

This part displays the outputs of performing the suggested method and the outputs of testing it with the Chaotic algorithm. Different color image formats (Joint photographic experts group (JEPG), portable network graphics (PNG) and bitmap (BMP)) were used in the experiments. Figure 12 and Table 1 shows several images before text embedding and images after text embedding. The experiment results are satisfactory after the implementation of Chaotic algorithm for encryption and decryption text, and using the exclusive-OR (XOR) operation to embed the cipher text in image (mobile's camera images). The JPEG image format is the batter than PNG but the BMP image format is the best. The recovered image after extraction process is the same as the original image before embedding process.

Figure 12. Images before embedding cipher text

Table 1. Images after embedding text

Images after embedding cipher text				
Plain text=”Be Ready for Next Mission”				
Cipher text=”H0 X_31l*Aez0e\tDC'|eD”				
				
Run time for decryption cipher text				
41.5286	2.8482	11.8547	3.5874	33.1858

6. CONCLUSION

This paper presents methods for encryption and decryption and embedding text in/from mobile’s image, that method is especially designed for Android operating system environment. Therefore, this method is compatible with any Android-based tablet computer and cell phone. The use of the chaotic algorithm speeds up the execution of this scheme on a cell phone and adds another layer of security. Using the XOR operation with the chaotic algorithm to hide the text in the picture gives the system more protection and complexity. The proposed method is clearly effective based on the experimental results, as there is no difference between the original and the steganography image.

ACKNOWLEDGEMENTS

The authors would like to thank Mustansiriyah University (www. uomustansiriyah.edu.iq) Baghdad, Iraq for its support in the present work.

REFERENCES

[1] S. Jahangir and T. Shah, “A novel multiple color image encryption scheme based on algebra M(2, F2[u]/ ⟨u8⟩) and chaotic map,” *Journal of Information Security and Applications*, vol. 59, p. 102831, Jun. 2021, doi: 10.1016/j.jisa.2021.102831.

[2] H. Li *et al.*, “A novel image encryption scheme based on non-adjacent parallelable permutation and dynamic DNA-level two-way diffusion,” *Journal of Information Security and Applications*, vol. 61, p. 102844, Sep. 2021, doi: 10.1016/j.jisa.2021.102844.

[3] T. Janani and M. Brindha, “A secure medical image transmission scheme aided by quantum representation,” *Journal of Information Security and Applications*, vol. 59, p. 102832, Jun. 2021, doi: 10.1016/j.jisa.2021.102832.

[4] S. Mukherjee, S. Sarkar, and S. Mukhopadhyay, “Pencil shell matrix based image steganography with elevated embedding capacity,” *Journal of Information Security and Applications*, vol. 62, p. 102955, Nov. 2021, doi: 10.1016/j.jisa.2021.102955.

[5] J. Zhang, T. Cui, and C. Jin, “A generic framework for decomposing block cipher structure with secret components,” *Journal of Information Security and Applications*, vol. 60, p. 102855, Aug. 2021, doi: 10.1016/j.jisa.2021.102855.

[6] J. S. Khan and S. K. Kayhan, “Chaos and compressive sensing based novel image encryption scheme,” *Journal of Information Security and Applications*, vol. 58, p. 102711, May 2021, doi: 10.1016/j.jisa.2020.102711.

[7] S. K. Nayak and S. Tripathy, “SEPS: Efficient public-key based secure search over outsourced data,” *Journal of Information Security and Applications*, vol. 61, p. 102932, Sep. 2021, doi: 10.1016/j.jisa.2021.102932.

[8] S. Ajish and K. S. AnilKumar, “Secure mobile internet voting system using biometric authentication and wavelet based AES,” *Journal of Information Security and Applications*, vol. 61, p. 102908, Sep. 2021, doi: 10.1016/j.jisa.2021.102908.

[9] S. Roy, M. Shrivastava, U. Rawat, C. V. Pandey, and S. K. Nayak, “IESCA: An efficient image encryption scheme using 2-D cellular automata,” *Journal of Information Security and Applications*, vol. 61, p. 102919, Sep. 2021, doi: 10.1016/j.jisa.2021.102919.

[10] S. Kumar, “Image data security using Quasigroup combined with Fibonacci Q-transformation,” *Journal of Information Security and Applications*, vol. 61, p. 102941, Sep. 2021, doi: 10.1016/j.jisa.2021.102941.

[11] J. I. M. Bezerra, V. V. D. A. Camargo, and A. Molter, “A new efficient permutation-diffusion encryption algorithm based on a chaotic map,” *Chaos, Solitons and Fractals*, vol. 151, p. 111235, Oct. 2021, doi: 10.1016/j.chaos.2021.111235.

[12] X. Wang and N. Guan, “Chaotic image encryption algorithm based on block theory and reversible mixed cellular automata,” *Optics and Laser Technology*, vol. 132, p. 106501, Dec. 2020, doi: 10.1016/j.optlastec.2020.106501.

[13] A. A. Abbasi, M. Mazinani, and R. Hosseini, “Evolutionary-based image encryption using biomolecules and non-coupled map lattice,” *Optics and Laser Technology*, vol. 140, p. 106974, Aug. 2021, doi: 10.1016/j.optlastec.2021.106974.

[14] X. Wang and N. Guan, “A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation,” *Optics and Laser Technology*, vol. 131, p. 106366, Nov. 2020, doi: 10.1016/j.optlastec.2020.106366.

[15] X. Wang, S. Chen, and Y. Zhang, "A chaotic image encryption algorithm based on random dynamic mixing," *Optics and Laser Technology*, vol. 138, p. 106837, Jun. 2021, doi: 10.1016/j.optlastec.2020.106837.
[16] M. Z. Talhaoui and X. Wang, "A new fractional one dimensional chaotic map and its application in high-speed image encryption," *Information Sciences*, vol. 550, pp. 13–26, Mar. 2021, doi: 10.1016/j.ins.2020.10.048.
[17] X. Zhang and Y. Hu, "Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding," *Optics and Laser Technology*, vol. 141, p. 107073, Sep. 2021, doi: 10.1016/j.optlastec.2021.107073.
[18] X. Wang, W. Xue, and J. An, "Image encryption algorithm based on Tent-Dynamics coupled map lattices and diffusion of Household," *Chaos, Solitons and Fractals*, vol. 141, p. 110309, Dec. 2020, doi: 10.1016/j.chaos.2020.110309.
[19] A. A. Abbasi, M. Mazinani, and R. Hosseini, "Chaotic evolutionary-based image encryption using RNA codons and amino acid truth table," *Optics and Laser Technology*, vol. 132, p. 106465, Dec. 2020, doi: 10.1016/j.optlastec.2020.106465.
[20] Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, "Image Encryption Based on Chaotic Sub-Block Scrambling and Chaotic Digit Selection Diffusion," *Optics and Lasers in Engineering*, vol. 134, p. 106202, Nov. 2020, doi: 10.1016/j.optlaseng.2020.106202.
[21] M. Wang, X. Wang, Y. Zhang, S. Zhou, T. Zhao, and N. Yao, "A novel chaotic system and its application in a color image cryptosystem," *Optics and Lasers in Engineering*, vol. 121, pp. 479–494, Oct. 2019, doi: 10.1016/j.optlaseng.2019.05.013.
[22] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, no. 16–17, pp. 3895–3903, Aug. 2011, doi: 10.1016/j.optcom.2011.04.001.
[23] A. A. B. Maryoosh, "A new block cipher algorithm for image encryption based on chaotic system and S-Box," *International Journal of Civil Engineering and Technology*, vol. 9, no. 13, pp. 318–327, 2018.
[24] X. Y. Wang, S. X. Gu, and Y. Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Optics and Lasers in Engineering*, vol. 68, pp. 126–134, May 2015, doi: 10.1016/j.optlaseng.2014.12.025.
[25] Z. S. Dhaief, R. A. Mustafa, and A. A. Maryoosh, "Hiding Encrypted Text in Image using Least Significant Bit image Steganography Technique," *International Journal of Engineering Research and Advanced Technology*, vol. 06, no. 08, pp. 63–75, 2020, doi: 10.31695/ijerat.2020.3642.
[26] L. Zhang, Y. Guo, X. Guo, and X. Shao, "Does the layout of the Android unlock pattern affect the security and usability of the password?," *Journal of Information Security and Applications*, vol. 62, p. 103011, Nov. 2021, doi: 10.1016/j.jisa.2021.103011.
[27] M. Hussain *et al*., "Conceptual framework for the security of mobile health applications on Android platform," *Telematics and Informatics*, vol. 35, no. 5, pp. 1335–1354, Aug. 2018, doi: 10.1016/j.tele.2018.03.005.
[28] H. Altuwaijri and S. Ghouzali, "Android data storage security: A review," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 5, pp. 543–552, Jun. 2020, doi: 10.1016/j.jksuci.2018.07.004.

BIOGRAPHIES OF AUTHORS

Kawther Thabt Saleh received the B.Sc. in Computer Science from Mustansiriyah University-Iraq (2005), and M.Sc. in Computer Science from Al-Balqa' Applied University-Jordan (2011). She has nearly 16 years of experience in teaching in Computer Science department, College of Education, Mustansiriyah University. She has published over many papers in international and national journals and conferences. Her fields of interests include image processing, pattern recognition, Artificial Intelligence. She can be contacted at email: kawtherthabt@uomustansiriyah.edu.iq.

Nisreen Abd Alhadi Jabr received the B.Sc. in Computer Science from Mustansiriyah University-Iraq (2009), and M.Sc. in Computer Science from Mustansiriyah University-Iraq (2016). She has nearly 10 years of experience in teaching in Computer science department. She's currently a lecturer with the Branch of Teams Games, College of Physical Education and Sports Science, Mustansiriyah University. She has many published papers in the Computer Science field. Her research interests are in Artificial Intelligence, pattern recognition, and image processing. She can be contacted at email: nisreen1987@uomustansiriyah.edu.iq.

Iman Hussein AL-Qinani received B.Sc. in Computer Science from Mustansiriyah University-Iraq (2004), and M.Sc. in Computer Science from Al-Balqa' Applied University-Jordan (2011). She has nearly 15 years of experience in teaching in Computer Science department. She's currently a lecturer with the Department of Computer Science, College of Education, Mustansiriyah University. She has many published papers in the Computer Science field. Her research interests are in image processing, biomedical, and Artificial Intelligence. She can be contacted at email: iman.alqinani@uomustansiriyah.edu.iq.