International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218147

Encryption Image using HiSea Algorithm Based on Android Operating System

Zainab Khyioon Abdalrdha
Department of Computer Science, College of Education, Mustansiriyah University, Bagdad-Iraq
zainabkhyioon83@uomustansiriyah.edu.iq

Article Info
Volume 8 Issue 1
Page Number: 222-228

Publication Issue :
January-February-2021

Article History
Accepted : 20 Feb 2021
Published : 28 Feb 2021

ABSTRACT

The mobile phone environment represents one of the important environments in encryption various multimedia (audio, image, and video) , and this depends on the type of algorithm used in the encryption process, as phones have limited memory and computational resources, Therefore the selection of the algorithm must be compatible with the mobile environment in terms of speed, safety and flexibility in addition to choosing an algorithm that The simplicity and safety of the image encryption process was investigated with lightweight and efficient computing. In this paper, Hybrid Cube Encryption (HiSec) was used. When implementing this algorithm in a smart phone environment, the results showed the ease of encrypting images and retrieving the original image, in addition to that it only requires small computational resources, and the algorithm was very effective in encrypting images on mobile phones. This suggested method has been implemented in the mobile environment with android OS. The proposed method has been programmed in JAVA, and the method has been tried on different types of mobile phones (such as Huawei Nova 2, Huawei Nova 7, HTC, NOT 8, Galaxy S 20, and HONOR).

Keywords: encryption image, hybrid cubes encryption algorithm, security of mobile, Android OS, and decryption image.

I. INTRODUCTION

The rapid development of Internet technology in digital world has become a point of great concern at the present time, especially in the digital age, especially information security issues, in general or in particular, whether it is text, pictures, or video, and other issues related to data confidentiality and integrity [1]. In the current era, the Internet has become a means that makes it easier for a person to communicate data, so the need for security has become necessary to protect information, whether text or images, so encryption is one of the technologies used in the mobile environment [2]. Because of the increased importance of encryption, many methods have been found in expanding the security circle, and these methods do not require difficult methods, only following simple mathematical methods. In an environment that is still limited, the proposed method aimed at obtaining an

encrypted image in a simple way that relied on Hi sec algorithm in a safe, high-speed and efficient way [3].

Due to the development in the digital world of internet speed, protection and security of digital images in mobile devices has become more important through the mobile. In recent times, as a result of the tremendous development in the digital world, the security of digital images has become more and more attractive in terms of attention, and image encryption technologies have come to convert one image to another. So that it is difficult to understand. On the other hand, following the reverse decoding method to retrieve the original image from encoded the image [4]. In the paper, the second part, the basic requirements for the security of mobile devices will be discussed, and the third part, an overview of the Hybrid Cube Encryption, (HiSea) algorithm used in image encryption. The general structure of the proposed approach will be in Part 4 and the general algorithm for the proposed approach will be in Part Five, implementation of the proposed system will be in Part 6, and the conclusions and future actions will be explained in Part 7.

II. The basic requirements for the security of mobile

Mobile applications are important applications as these applications are designed according to a program that is designed to be compatible with the Android environment. The most common applications are both iOS and Android [5], illustrated in Figure 1, which represents a bar chart between the different mobile apps for major application as of June 2016.

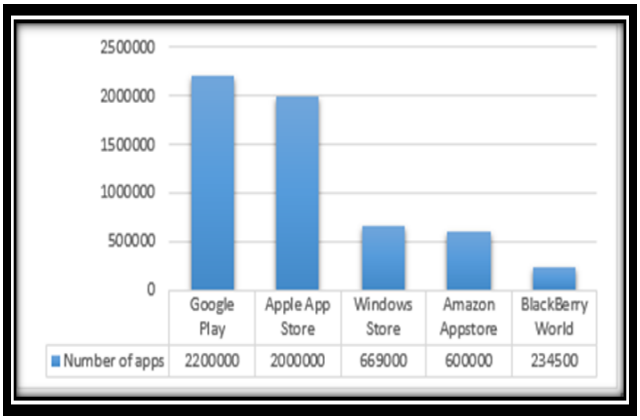

Figure 1. Ready Applications in various stores [6].

Applications used in Operating systems:

In this section, the mobile operating systems are described, which are both Android and IOS

A. Android operating systems

The Android operating system is considered one of the systems that depend on the Java language in writing the code in addition to it is an open source application and it was issued by Google by licensing Apache and the basic kernel is Linux, and the Android operating system can consist of five basic components Which is illustrated in Figure 2: a block diagram of the android OS [6-8].

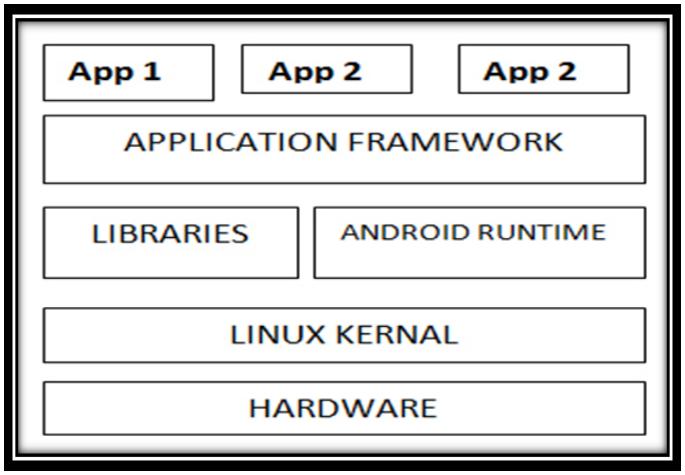

Figure 2. A block diagram of the android OS [8]

B. IOS

IOS is Objective-C written in Swift Xcode and issued by Apple. The operating system is a UNIX kernel. Apple products (iPhone and Apple) were used as the first release in June 2007 mainly [6] [9].

III. Overview of the HiSea

Hybrid Cubes Encryption Algorithm is considered as symmetric type because the encryption key and encrypted text are based on integers. The Hi Sea encryption algorithm was developed in 2011 by Sapiee Jame[10]-[11]. By combining and permeating integers this algorithm was created and to create an improved encryption method, the features of the public key are combined with the symmetric

algorithm component [12]. Although the encryption has been improved because there are disadvantages of Hybrid cipher algorithm, is a key transfer problem, as there must be a safe path in the process of transferring the key, and this algorithm has proven to be resistant to attacks, and this algorithm was considered useful. It is a safe option, and the public and private keys are kept secure despite the length of the resulting encrypted text.

Figure 3 illustrates the general design of HiSea where the plain text, the keys and the encrypted text in the encoding process are formatted in a 4-matrix arrangement. The following steps are used by the encryption algorithm:

1) step1: Plaintext can be encoded based on four arrays of Plaintext as P1-P4 where it is in the plain text format from 64 characters to 64 ASCII characters and output is used for p2 encryption process where it is used as an intermediate result (P1′) for P1 and continues in this way down to for P4. The process is performed to increase the complexity of the cipher text to ensure that any change made in P1 will be reflected in another cipher text , which is the main reason for incorporating this method.

2) step2: The temporary coded text named P1′ is generated by mixing P1 with the primary matrix (IM) down to p4. Then, P1′ is added with the session key (K1). To create diffusion in Ciphertext 1 (C1) the MixRow and MixCol functions are then used. Plain text with session key 2 (K2).

3) Step 2 is repeated with P3 and P4 to create ciphertext 3 (C3) and ciphertext 4 (C4).

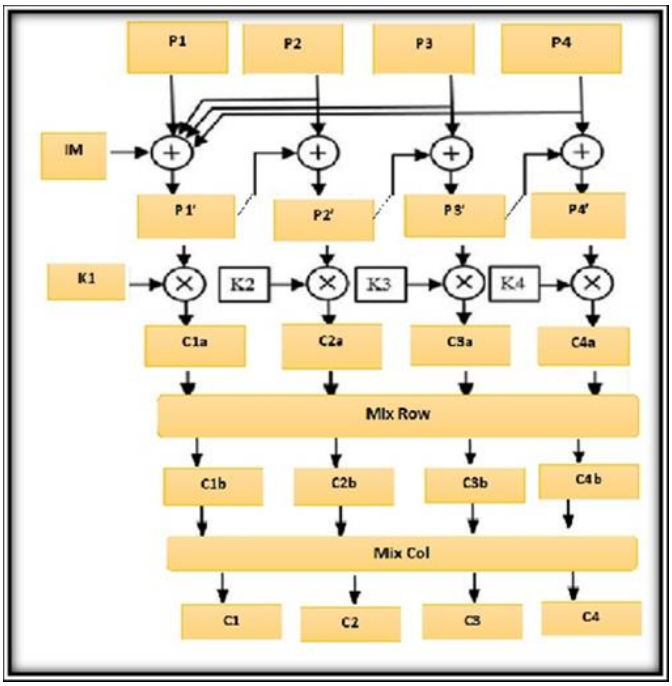

Figure 3. Hybrid Cubes Encryption Algorithm [11].

HiSea is considered secure as it is difficult for attackers or takes a long time due to the length of its key in addition to mathematically [12], [13].

IV. General Structure of Proposed Approach

In this part, the approach or method used to use the Hisea algorithm in order to encode and retrieve images in the environment of Android operating systems, which is mobile phones, which is considered this method is to improve the security of information in mobile phones in order to encrypt the images. The figure (6) shows the main of the proposed method according to algorithm. In addition, it appears that the proposed method for coding is based on Hi sea algorithm using a scheme shown in Figure (4). The proposed decoding method based on Hi sea algorithm is illustrated using a scheme shown in Figure (5).

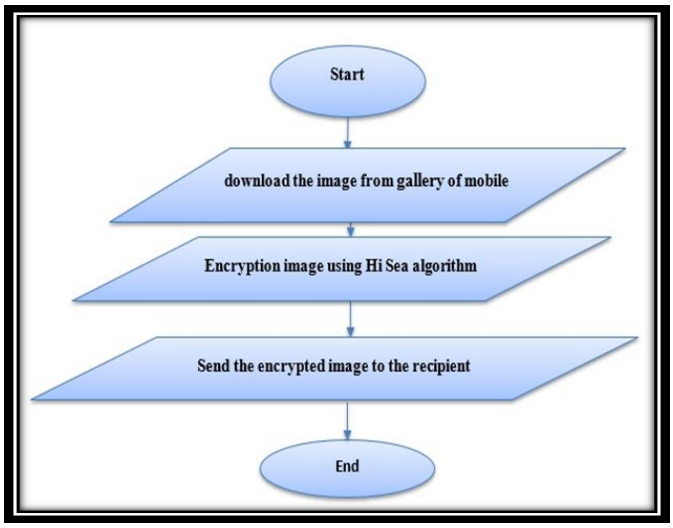

Figure (4). Scheme coding system suggested approach

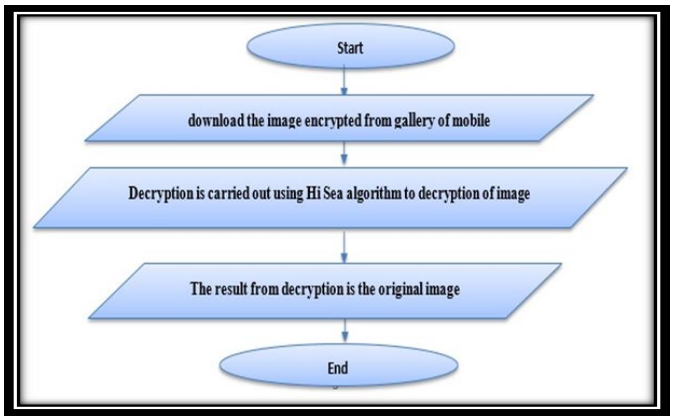

Figure (5) Scheme decoding system suggested approach

The algorithm used for the proposed method:

This section describes the proposed method based on Hisea proposed algorithm as it is shown in Figure 6.

Input: the original image
Output: image encryption

Step1: Choose the original image.
Step2: Image encryption using Hi Sea algorithm
Step3: Send the image encrypted to receiver.
Step4: The recipient of the encrypted image applies the process in a reverse manner, which is decryption, depending on the same application used to decryption the image and retrieve the original image.
Step5: The decoding process is performed based on Hi Sea algorithm to recover the original image.
Step 6: The original image is output
Step7: The end.

Figure (6). Suggested method algorithm

V. The executive side of the proposed method

The proposed method will be implemented according to the steps described in the algorithm (6), where upon implementation the application used to encrypt images in the mobile environment, depending on the Hisea algorithm, the main interface was composed of two parts (Hi sea encryption & Hi sea decryption), as shown in (7).

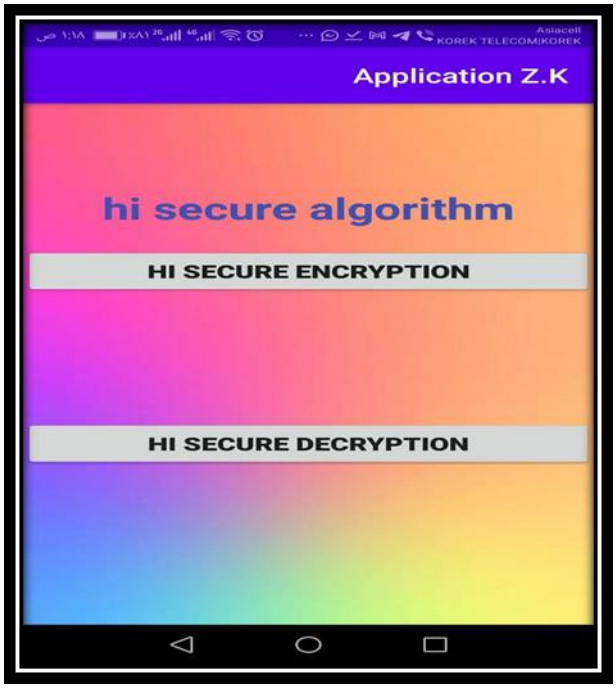

Figure (7) The main interface for encryption images

Step1: Click on Hi sea algorithm to encryption image as shown in Figure (8).

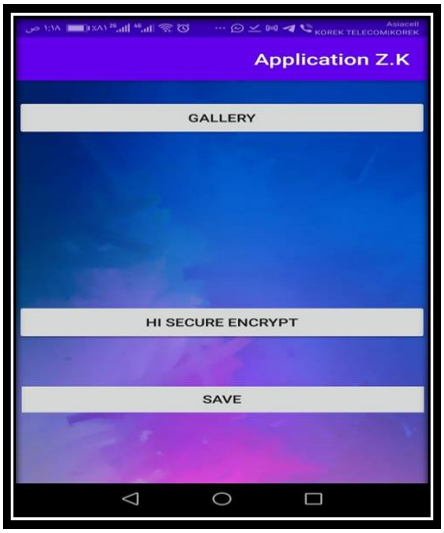

Figure (8) Hi sea encryption for operation encryption

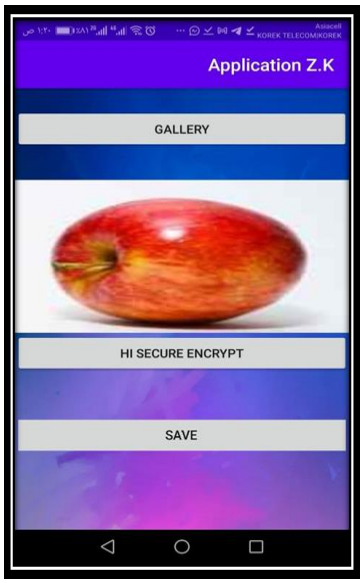

Figure (9) Download the original image.

Step3: the image is encryption using Hi sec algorithm, the result is the image encrypted as Illustrated in Figure (10).

Figure (10) image of encryption.

Step 4: The recipient of the encrypted image applies the process in a reverse manner, which is decryption, depending on the same application used to decryption the image and retrieve the original image as illustrated in Figure (11).

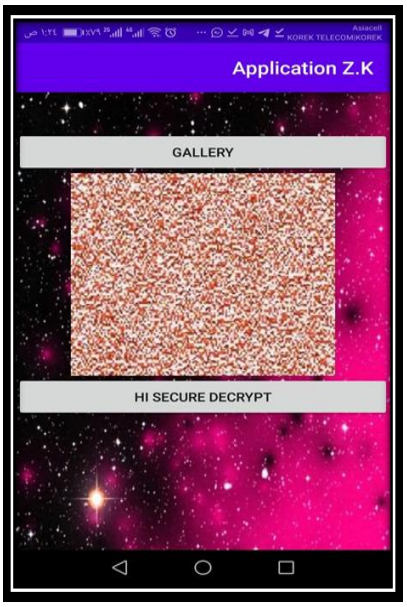

Figure (11) Download the image Encryption

Step 5 : Choose Hi secure decrypt, to decrypt the image, the decryption result is the original image, as illustrated in Figure (12).

Figure (12) Decryption of the image.

Step 6 : End.

VI.CONCLUSION

In this paper, a new method for encrypting images was used, which is the Hi sea algorithm for image security and image encryption. The proposed work was carried out in mobile phones that depend on the environment of the android operating system, although the algorithm was subjected to several attacks by brute force, but due to the length of the key it is difficult to predict The key was either faster and provided stronger security than other traditional systems. This method provided a reliable picture at the recipient's end regarding decryption operations, the proposed method was compatible with all Android environments, meaning different types of mobile phones, and the implementation process was fast and safe depending on the Hisea algorithm. Which differs from the encryption methods used in the traditional encryption methods that do not depend on the Android environment In the future is the implementation of Hisea algorithm and NTRU encoding algorithm in our proposed model. This paper represents a brief description and a brief description of Hisea algorithm to improve the coding systems used in operating systems, especially the Android environment.

VII. ACKNOWLEDGMENT

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

VIII. REFERENCES

[1]. Mahmud H, A., Angga W, B., Tommy, Marwan E, A., & Siregar, R. (2018)," Performance analysis of AES-Blowfish hybrid algorithm for security of patient medical record data", Journal of Physics: Conference Series, 1007, 01 2018. doi:10.1088/1742-6596/1007/1/012018

[2]. Rani R, Sharma G, 2017, "Review Paper on Data Hiding In 3D Barcode Image Using Steganography", International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May-June 2017, 2271—2276, ISSN No. 0976-5697, DOI: 10.26483/ijarcs.v8i5.4056

[3]. Emy Setyaningsih* 1, Catur Iswahyudi2, Naniek Widyastuti3," Image Encryption on Mobile Phone using Super Encryption Algorithm", TELKOMNIKA, Vol.10, No.4, December 2012, pp. 837~845 ISSN: 1693-6930, DOI: 10.12928/telkomnika. v10i4.23

[4]. Shankar, T. N., Sahoo, G., & Niranjan, S. (17 December 2010),"Image Encryption for mobile devices", IEEE Xplore:. doi:10.1109/icccct.2010.5670766 .

[5]. H. Zimeng, "Security of Mobile Devices and Wi-Fi Networks,"(2015) , Bachelor's Thesis MAMK Unviversity of applied sciences, https://www.theseus.fi/

[6]. Aya Khalid Naji and Saad Najim Alsaad (August 2017) , "Data (Video) Encryption in Mobile Devices", Kurdistan Journal for Applied Research kjar.spu.edu.iq,Volume 2, Issue 3, , P-ISSN: 2411-7684 – E-ISSN: 2411-7706, DOI: 10.24017/science.2017.3.17

[7]. A.MohdShahdi, M.NurEmyra, N.Rathidevi, H.Rosilah and H.Nor Effendy, (2013) " Comparison Between Android and iOS Operating System in terms of Security," In Proceedings of the IEEE International Conference on Information Technology in Asia (CITA), DOI: 10.1109/CITA.2013.6637558

[8]. A.Jeremy,H. Alexander V. and A.Naser,(2014), "Cider: Native Execution of iOS Apps on Android, " in Proceedings of the International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS),pp.367-381, , https://doi.org/10.1145/2654822.2541972

[9]. Vaibhav Kumar Sarkania,(2013), " Android Internals" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN 2277 128X, Volume 3, Issue6,

pp 143-147, https://www.coursehero.com/file/21330755/V3I6-0134/

[10].J. Thakur, Nagesh Kumar ,(2011), "DES, AES, and Blowfish: Symmetric key cryptography," International Journal of Emerging Technology and Advanced Engineering, vol. 1, no. 2, pp. 6-12, https://www.academia.edu/3345271.

[11].Muhammad, Sapiee Jamel, Abdulkadir, Zahraddeen A. Pindar, Nur Shakir, Mustafa Mat Deris,(2017), "A Survey on the Cryptographic Encryption Algorithms," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 8, no. 11, p. 7978, https://thesai.org/Downloads/Volume8No11.

[12].Jamel, S., Deris, M. M., Yanto, I. T. R., & Herawan, T. (2011). The Hybrid Cubes Encryption Algorithm (HiSea). Communications in Computer and Information Science, 191–200,,Springer-Verlag , doi:10.1007/978-3-642-21153-9_18

[13].M. F. Mushtaq, S. Jamel, K. M. Mohamad, S. A. A. Khalid, and M. M. Deris,(2017), “Key generation technique based on triangular coordinate extraction for hybrid cubes,” Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 9, no. 3-4, pp. 195-200, https://www.semanticscholar.org

Cite this article as :

Zainab Khyioon Abdalrdha, "Encryption Image using HiSea Algorithm Based on Android Operating System", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 1, pp. 222-228, January-February 2021. Available at

doi : https://doi.org/10.32628/IJSRSET218147

Journal URL : https://ijsrset.com/IJSRSET218147