International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2021.3715

E-ISSN : 2454-6135

Volume.7, No. 6
June -2021

Subject Review: Encryption of Image in the Android Environment in Various Algorithms

Ahmed Kareem Ridha[1], Raghda Sattar Jabar,[2] and Iman Hussein AL Qinani[3]

Assistant Teacher [1-] and Teacher [3]

[1,3]Department of Computer Science, Collage of Education

[2] Department of Quality Assurance

University of Mustansiriyah, Iraq

ABSTRACT

In the vast and still evolving the world of digital transfer, data/image security is one of the most important considerations. One method is to encrypt files. One of the well-known mechanisms for maintaining privacy of pictures to a trustworthy, unrestricted public, the media as a result, this medium is vulnerable to attacks, Encryption algorithms that are effective are a must for data transfer that is stable a variety of techniques. This paper is a study of research authors in the field of image encryption for the Android Environment for different algorithms, with a research review for the period (2010-2021) to see how the field of image encryption has progressed and the best algorithms in their performance.

Keywords: Image Encryption, ECC and Chaotic Algorithms, Handheld devices, Android Applications, Image decryption.

1. INTRODUCTION

With the advancement of digital communication technologies, new issues arise to protect digital media from unauthorized access. To meet the demand for secure encryption techniques, substantial research in the cryptography sector is required. To deal with the unique characteristics of digital photographs as a representative information resource, special encryption techniques are required [1]. Mobile phones have become the most significant and habitual item for every human being today. Security of the image and digital information has become the most critical concern in our society as a result of the rising usage of smart phones, tablets, computers, the rise of the internet, and multimedia technology. A criminal or thief is someone who reads and modifies information while it is being transmitted. As a result, to safeguard such sensitive information. There are two types of encryption algorithms: public and private. Asymmetric and symmetric keys encryption are two different types of encryption. Only one key is needed to encrypt and decrypt data with symmetric keys encryption, also known as secret key encryption. Before sending data between entities, the key should be distributed. The importance of keys cannot be overstated [2]. DES, 3DES, AES, and Blowfish are examples of symmetric key encryption methods. This work is divided into multiple sections, the second of which discusses the advantages of image encoding. Part 3 reviews the literature survey for encoding pictures in various methods inside the Android environment, Part 4 presents the performance literature study for the charts presented, and lastly, Part 5 presents the conclusions.

2. IMAGE ENCRYPTION BENEFITS

Pixels are the basic building blocks of images. The process of transforming an image into an unreadable format is referred to as "image encryption.". Many digital services necessitate secure digital picture storage and transfer. Because of the rapid growth of the internet in today's digital world, digital image security has grown increasingly significant and garnered a lot of attention, The frequency of multiple personalities [3]. Images have an important role in our lives. It has become commonplace to photograph special occasions. CT scans and MRI images are used to diagnose abnormal symptoms. Patients who seek a second opinion frequently confront the challenge of safeguarding their privacy while yet transmitting their CT or MRI pictures securely. With the advancement of technology and the creation of picture encryption methods, however, transmitting and receiving photos has gotten easier. However, an open platform such as the internet may not always be safe for transmission. Military and medical photographs are sensitive and must be kept out of the hands of unauthorized individuals. As a result, a secure image sharing

technique that ensures the safe image transfer is required. Cryptography is crucial to reaching this goal, because image encryption is becoming more common and necessary [4].

3. SURVEY OF LITERATURE

Many studies and research have been conducted in the last decade due to the importance of picture encryption methods in the process of enhancing security, and the urgent need for them has arisen since the growth of the Android environment; therefore, in this section, we will examine some research in the field of encryption. In this paper, authors [5], Presented a method for encoding images using "elliptic curve coding" methodology. The applied technique uses an effective approach to address image coding issues, with the original image represented as a collection of pieces that produced a two-dimensional image on the coordinates where the ECC system was employed. Because pixel coordinates were employed to speed up the process and it was used to encode the photos, the proposed method's encryption strength was decided by the algorithm's keys, and so there was no impact on the runtime's strength and performance. To ensure SSL security, improved performance and security were sought in the search.

In this paper, the authors Emy Setyaningsih et. al., [6] employed algorithms that integrated Playfair's cipher with the Vigenere cipher in this manner. Experimental results for encoding the images were displayed as a result of this high-speed scanning, as it was seen that the histogram had a variable distribution and a substantial difference in side the graph of the normal image, and the intensity value in the graph of the encoded image was uneven and skewed. The experimental results also revealed that following coding, there was a linkage between the pieces of the image. The rate of pixel change in the image is rapid enough that encoding it is challenging, as evidenced by the average quality, and when employing this approach and applying it to a mobile phone, it only requires a modest amount of CPU resources. Because the entropy number is extremely close to 8, with an average of 7.9984, the tests demonstrate that the suggested encryption scheme is secure. The average correlation value between the plain and encrypted pictures is 0.000254. The average quality of encryption is 655.7976, indicating that the rate of pixel change is sufficient for this system to be regarded effective and safe. The application was also successfully built on mobile phone devices of a reasonable size using the JAR file format (88 Kb). The image encryption method takes 3.76 seconds on average to finish. Decryption takes about 0.97 seconds on average. It states that the proposed method works well for encoding color image data and that it may be utilized on mobile phones because it uses less CPU resources.

Suchita Tayde et al., **[7]** employed the AES algorithm to alleviate problems created by late operations with other approaches, such as the 3DES algorithm. This is due to the fact that it contains more than one key, and the second issue is the security aspect in other algorithms, where encryption is used to secure information in terms of storing and sending data. These problems were solved with the help of the AES algorithm. Sharing daily data, whether it was a file, text, image, or any other type of formatting, and transferring it for a variety of purposes including banking services and others, increased security. As a result, the information security aspect is an important aspect and depending on the basic android environment and the AES encryption and decryption method this research was done. When the file and the image encryption method was adopted the encryption and decryption processes were faster, and the android phone worked faster while ensuring great protection against unauthorized access.

In this paper JEAN DE DIEU NKAPKOP1 et al., [8] The authors presented an Android application development method for image confidentiality security of the developed algorithm. The proposed application was designed based on the Java programming language and Android Software Development Kit, to transmit and receive any type of image in a confidential manner before transferring it over the network to

DOI : 10.31695/IJERAT.2021.3715

another user via smart mobile phones. or transferred via Android-based tablets. The TCP/IP protocol is utilized for communication as well as image file transfer between devices. The suggested mobile picture encryption application allows for efficient picture file sharing between two mobile devices while maintaining a high level of security to prevent the users' private images from being leaked to an unauthorized end-user. This makes it ideal for sharing private photographs encrypted in real time between at least two Android mobile devices.

The authors Mohamed Boussif1 et al., [9] provide a secure medical picture transfer technique via a smartphone in this work, which is based on a suggested image encryption technique that uses the matrix product and exclusive addition. This study is unique in that it presents a low-complexity encryption method that can run on an embedded system in real time. Experiments indicate that the proposed encryption method may provide excellent security while still being fast. On this study, a CCS (Code Compiler Studio) tool was used to correct the C / C ++ code in the card, which was implemented on the DSK C6416 through the proposed system, and then we worked on preparing the DSP / BIOS for real-time data exchange (RTDX), which consists of configuring Off-ship memory for transferring image data between a PC and the C6416 DSK. the function is then encrypted when the argument is set, allowing encoding and decoding. The crypto analysis shows that the proposed encryption approach is resistant to a variety of assaults. The encryption technique is shown to run in real time on embedded devices (DSK C6416 and Android smartphone).

To achieve high system performance, the author of this work [10], will implement an acceptable image encryption technique. In an Android application, image security is achieved through the use of ECC and chaotic algorithms. Due to its minimal computing overhead, Elliptic Curve Cryptography has been considered a potential cryptographic approach and present a novel approach in the Android system that uses cryptographic methods to allow users to encrypt images before sending them over the network in this study. This method produces a good encrypted image, as well as a high-performance recovered image. The ECC technique was used to encrypt the images, which is tough to decipher for use in appropriate mathematical operations. Because a chaotic system would not generate the same results if the input keys are not the required keys, it is difficult to attack the plain text without knowing the secret keys, the author employed the chaotic algorithm in this work and this program can be used on any Android-powered device.

The authors of this paper Noveline Aziz Fauziah et al., [11] provided a new way for encrypting multimedia from photos, text, or other files, based on the Android environment, using the AES algorithm and the SHA-256 algorithm to offer data security when transported via the network due to the strength, speed, and safety of both methods. Encryption and decryption are both faster and better using AES. In this study, keys were produced using the SHA-256 algorithm in a custom Android application in order to communicate encrypted data via the chat application, Multimedia assets such as images, audio, and video are among the data to be protected. The user then inputs a key when the file is loaded into the application. The encoded files are kept in UUencoding format to minimize compression when delivering files using a file Chat program as well as to secure the contents of the file because the message cannot be seen directly. As a result, the file is more secure. The results of experiments for various applications of encoding multimedia files have been successful, despite the fact that the process of encoding and decoding increases the original file size slightly.

The author of this paper Zainab Khyioon Abdalrdha, [12], presented a new approach for encrypting photos on a mobile phone based on the Hybrid Cube Encryption (HiSec) algorithm. The technique worked well for encrypting photos on mobile phones. Depending on the Android environment, this suggested solution has been implemented. The proposed approach was written in JAVA and tested on a variety of mobile telephone (including the Huawei Nova 2, and others), with the results demonstrating the ease with which photographs may be encoded and retrieved, as well as the fact that it only uses a tiny amount of processing resources. This approach gave a reliable image of decryption operations at the receiver end, and the execution process was fast and secure thanks to the Hisea algorithm. This is in contrast to the standard

DOI : 10.31695/IJERAT.2021.3715

encryption methods, which are not dependent on the Android environment.

5. CONCLUSION

During the period covered in review this study (2010-2021), we looked at a new method for encoding images that was dependent on the Android environment, we talked about security, image encryption, different types of encrypted image transfer software for mobile phones, and reviewed the work of some of the authors. The methods can be used on any Android phone. Our next review will be to compare and paper-based literature scanning for video coding on Android with the traditional encoder method. We noted the usefulness and security of algorithms that have been used in many JAVA-enabled mobile devices and Android tablets when analyzing the proposed research on image encryption in different ways. Our goal with this brief review is to provide a succinct and easy-to-understand overview of the contents of the above-mentioned articles so that readers can choose the methodology that best meets their needs. Each strategy is explored briefly.

ACKNOWLEDGMENT

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

REFERENCES

[1] Ali M. Meligy , Hossam Diab ,and Marwa S. El-Danaf ," Chaos Encryption Algorithm using Key Generation from Biometric Images", International Journal of Computer Applications (0975 – 8887) Volume 149 – No.11, September 2016.

[2] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882.

[3] RAVI SHANKER YADAV1, MHD. RIZWAN BEG2 & MANISH MADHAVA TRIPATHI3, "IMAGE ENCRYPTION TECHNIQUES: A CRITICAL COMPARISON", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN 2249-6831 Vol. 3, Issue 1, Mar 2013, 67-74.

[4] Manish Kumar1 , Rachid Ait Maalem Lahcen3 ,R. N. Mohapatra3 , Chandan Alwala2 , and Surya Vamsi Krishna Kurella2," Review of Image Encryption Techniques", IOSR Journal of Computer Engineering (IOSR-JCE) -ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 1, Ser. I (Jan - Feb 2020), PP 31-37.

[5] T. N.Shankar, Dr.G.Sahoo and Dr.S.Niranjan, "IMAGE ENCRYPTION FOR MOBILE DEVICES", 978-1-4244-7770-8/10/$26.00 ©2010 IEEE.

[6] Emy Setyaningsih[1], Catur Iswahyudi[2], and Naniek Widyastuti3 , "Image Encryption on Mobile Phone using Super Encryption Algorithm", TELKOMNIKA, Vol.10, No.4, August 2012, pp. 835~843.

[7] Suchita Tayde*, Asst. Prof. Seema Siledar ," File Encryption, Decryption Using AES Algorithm in Android Phone, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015.

[8] JEAN DE DIEU NKAPKOP1 , GEORGE-NICOLAE MATEI ," ANDROID APPLICATION FOR CONFIDENTIAL IMAGE COMMUNICATION USING CHAOTIC ENCRYPTION", MTA REVIEW • Vol. XXVI, No. 2, Jun. 2016.

DOI : 10.31695/IJERAT.2021.3715

[9] Mohamed Boussif1 , Noureddine Aloui2, Adnane Cherif1 ," Smartphone application for medical images secured exchange based on encryption using the matrix product and the exclusive addition", Accepted on 9th July 2017 E-First on 14th September 2017 doi: 10.1049/iet-ipr.2017.0229 www.ietdl.org.

[10] Farah Neamah Abbas ," IMAGE ENCRYPTION USING ECC AND CHAOTIC ALGORITHM BASED ON ANDROID OPERATING SYSTEM", International Journal of modern Trends in Engineering and Research, volume-5/issue7/2018 DOI:10.21884/IJMTER.2018.5174.ZJHHS.

[11] Noveline Aziz Fauziah, Eko Hari Rachmawanto, and De Rosal Ignatius Moses Setiadi ,"Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application", International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Date of Conference: 21-22 Nov. 2018, Date Added to IEEE Xplore: 14 October 2019,DOI: 10.1109/ISRITI.2018.8864485
Publisher: IEEE ,Conference Location: Yogyakarta, Indonesia.

[12] Zainab Khyioon Abdalrdha, "Encryption Image using HiSea Algorithm Based on Android Operating System", 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.

DOI : 10.31695/IJERAT.2021.3715