Scientific Journal Impact Factor (SJIF): 5.278
International Journal of Modern Trends in Engineering and Research
IJMTER
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

IMAGE ENCRYPTION USING ECC AND CHAOTIC ALGORITHM BASED ON ANDROID OPERATING SYSTEM

Farah Neamah Abbas [1]
[1]*Al-Mustansiriyah University, College of Education Department of Computer Science*

Abstract-Image encryption is one of the most common and important method of image data encryption. Image encryption deals with applying image encryption algorithms to the sending image and convert it into cipher image and only authorized person can decrypt the cipher-image to gent the original image, this done using secret key(s). There are big numbers of encryption techniques including chaos-based schemes, some of them utilize one-dimensional chaotic maps for encryption, The aim of this work is to implement an acceptable image encryption approach to achieve high system performance. Image security using ECC and chaotic algorithms in Android application. However, Elliptic Curve Cryptography has been considered as a viable cryptographic technique due to its low computational overhead. In this research we will propose a new method in the android system using cryptographic algorithms that allow the user to encrypt messages before sending them to other people over the network. This application can be run on any device running on the Android operating system. This approach achieves a good encrypted image; in addition the retrieved image will be at high performance.

Keywords: Technique for Image Encryption, ECC and Chaotic Algorithms, Android Source Code, Components of Android Applications

I. INTRODUCTION

Recently with the growth of using smart phones, Internet and computer networks, there are vast amount of data, information, images, videos and multimedia daily transmitted via the Internet [1]. Digital images are types of images that are characterized by their attractiveness with a wide range of use and there are many users of great importance to apply methods to protect the content in their images to prevent unauthorized persons from manipulation and there are many applications such as databases of astrological images and conferences with confidential content and medical systems and others on the Internet This is why security is necessary for this type of application and there is the special application of industrial images that tend to refer to the resource and assets to protect these images and other unauthorized persons [2]. Android based smart phones have limited resources in terms of processing, power, and Memory. Android play a critical role in the popularity of smart phones applications also called apps. As these applications involve transmission of data over the network, there is a dreadful requirement to provide security primitives like validation, reliability and privacy. However, due to their resource restricted nature, predictable security protocols cannot be openly employed [3]. Public key cryptography (ECC algorithm) along with chaotic algorithm has been practical in giving security primitive for conventional networks.

II. TECHNIQUE FOR IMAGE ENCRYPTION USING ECC AND CHAOTIC TECHNIQUE

In this part of the schema paper a scheme with high security content to encrypt images using an algorithm elliptic curve and chaotic algorithms. In this part will show technique for image encryption.

Volume: 5, Issue: 07, [July– 2018] ISSN (Online):2349–9745 ; ISSN (Print):2393-8161

2.1. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a public key cryptographic encryption algorithm where two common keys are used and is available to everyone who is subscribed to communication and other private and is only available to the person who decrypts the encrypted message [3]. The public key encryption requires a set of constants that are previously defined to be recognized by each single device in communications. In this encryption we use the elliptical curved cryptography which is considered constants this type of encryption is considered much slower than the private key encryption as in Figure (1) which shows the elliptical curve [4].

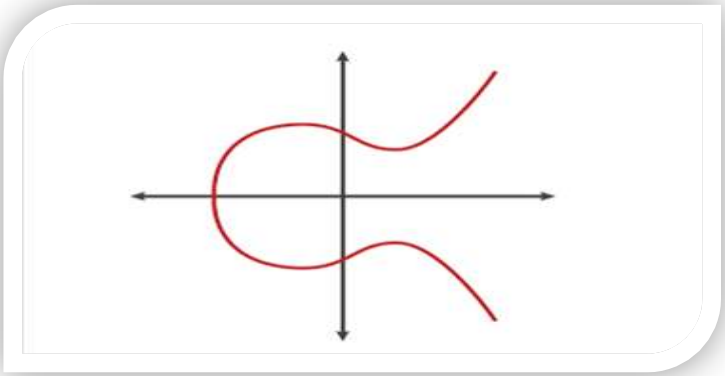


Figure 1:.Elliptic Curve [5].

The elliptical curve parameters include six cases: T = (N, e, f, G, n, h(The ellipsoid curve above the field is p can be defined according to the following equation x^3 + ex + f Where e, f Є P and $4e^3$ + $27f^2$ $\neq 0$.

1. Problem for Discrete Logarithm

The use of the ECC algorithm, which depends on the Elliptic Curve Discrete Logarithm Problem, and this use led to the difficulty in detection by the attacker, which led to increased security. Here we will use two points N,Q on the elliptical curve such that p N = Q which k is a scalar and for the points cannot be calculated to obtain a large number Enough k is the logarithm separated by the two points.

2. Public Key Cryptosystem for ECC

In the public key algorithm here in the elliptic curve key algorithm we assume that someone (T) wants to send a message secure 'm' it to someone else (S) you can know the point on the curve which are defined as n value such as, n P = P+P+..+P…. n times = O (infinity).

3. Generation of ECC keys (Public and Private)

All the object in the cryptosystem conform to the parameters (a, b, p, G, n). Generator point is called G and the order of G is called n. Generate a random number for A (n A < n) which represents a private key and we calculate the public key PA = G .n A, Generate a random number for B (n B < n) which represents a private key and we calculate the public key PB = G n B.

4. Common key Generation

Entity computes the Common key after the public key exchange between the parties is complete and the key calculation process is performed (entity A computes his Common Key by K= nA.PB, Entity B computes his Common Key by K= nB.PA. The keys (A,B) have the same value due to:: nA.PB = nA. (nB.G) = nB (nA.G) = nB. PA.

5. Encryption Operation

To send a image we force the image after symbolize the image in the form of RGB matrix (Depends on the pixel size of image) 'PmI=aPm // a: pixel value of the image from image grid //

Volume: 5, Issue: 07, [July– 2018] ISSN (Online):2349–9745 ; ISSN (Print):2393-8161

Pm: random point on EC, 'PmI' sent from the sender A to the recipient B. The sender A will choose a positive integer 'k' that represents this number as a private key 'nA', generates the public key PA = nA × G and then produces the encrypted text Cm' which contains a pair of points Cm = {kG, PmI + kPB}, where G it represents a selected base point on the elliptical curve. The recipient's B calculated public key is PB= n B.G with private key 'nB'.

6. Decryption Operation

In the process of decryption the decryption image where the recipient of the message to hit the first point in a pair by B's the private key and subtract the output from the second point PmI + kPB - nB(kG) = PmI + k(nB G) - nB(kG) = PmI.

2.2. Chaotic Algorithm

Chaos theory is a branch of nonlinear dynamic systems. These dynamic systems with low dimensions have the potential for complex and unpredictable behavior. Here the complexity of determining equations from the source is not a prerequisite for generating random sequences. The short chaotic system is an overlap between rigid order and unpredictability Probability as described in Figure (2) Chaos iterative function [6].

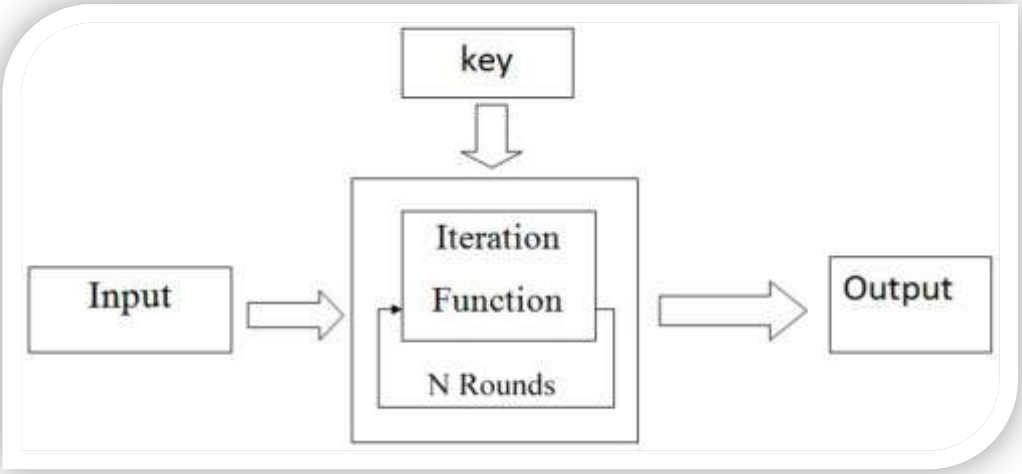


Figure 2: Chaos iterative function[6].

There are a number of definitions of chaos that have some special characteristics to it [7].

• **Nonlinearity**: The change in the first element does not affect the change in the first element and also the representation can be in a different element or the same.

• **Determinism**: Here means the possibility of being governed by correct and accurate rules with any element.

• **Sensibility to initial condition**: means that the resulting final state is completely different because the changes were not mentioned in their initial state

• **Irregularity:** means that there is chaos in the system.

• **Long term prediction**: Because of the initial conditions, the disorder will produce an indefinite long-term forecast.

• **The logistic map**: The map is a single dimension that gives the parameters of the encryption process and is considered a logistics map Xn + 1 = A Xn (Xn − 1).

III. SOURCE CODE FOR ANDROID

Android is open source software that has been established for a wide range of equipment's and various factors. The goal of Android is to create open platform software for transport and original equipment manufacturers, and the Android developers worked on innovations where they

produced a successful production work in the real world that improves mobile and users. It is necessary to emphasize that there is no possible central point of failure where a particular plant can restrict or control the innovations of another country. The coded has an open source project where the codes are located, which are imported by the exporter and which are specialized for production, Although the Android consists of several sub-projects, but the management of this process by project management technology and here we looked at this product as a single software product and not just a specification or a set of pieces can be replaced and the main objective is the construction of the port of the Android [8], in figure (3) shown Android Stack.

Figure3: Android Stack [8].

IV. COMPONENTS OF ANDROID APPLICATIONS

4.1. Applications

The android environment is highly flexible to allow any application to take advantage of features already created by other applications. The Figure3: Block diagram of android operating systems architecture showed four basic applications (App 1, App 2, App 3 and App 4), these four applications will give an idea only to many site-specific applications that are ground-breaking and can be installed directly without the need to integrate with an operating system [9].

4.2. Framework of Application

The advantage of the component is that any application can take these possibilities and publish, where each application is characterized by its content on the basic components and also includes the interfaces of different forms of buttons and menus and the abundance and ability of applications to review alerts and alerts for each application from the status bar of each application, The resource manager : Access to non-software resources, format files and other content. Content Providers: allows all applications to share data and access other data applications [10].

4.3. Runtime of Android Runtime

In this section all the features of the android applications are implemented from the time of the android operation. This device is considered as Dalvik Virtual Machine means to implement the android application in addition to the virtual machine. This consists of Java libraries, which are available for all Android devices [11].

4.4. Kernel Android

The basis of the operating system of the Android is the Linux 2.6 kernel, which is basically the source of Linux, which was compiled from mobile devices and is a kernel or bridge between the

hardware and software and the preparation of the cache is protected and scheduling and load the triggers to other commands [9, 11].

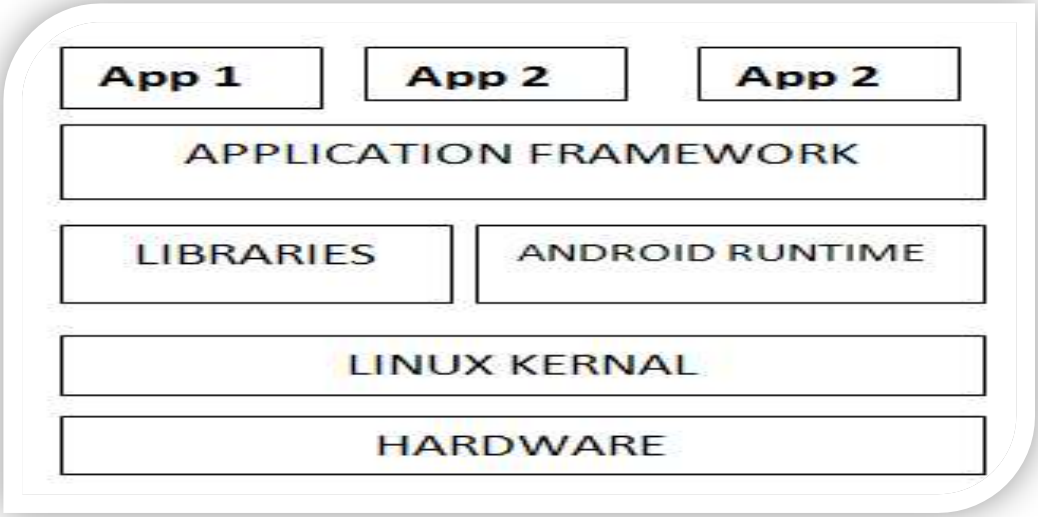


Figure4: Components of Android Applications[12] .

V. THE METHOD APPROACH

This section explains the general algorithm method for this search. Shown in the algorithm (1)

Input: Image
Output: Image encrypted

Process:
Step1: Enter the Image
Step2: The image is encoded as a three-dimensional matrix of colors(RGB) and this depends on the size of the pixel.
Step3: Divide the three-dimensional matrix of colors (RGB) into individual elements R,G and B to make transfers of these colors.
Step4: Plot the chosen Elliptic curve.
Step5: Encrypt the image using an algorithm ECC.
Step6: Encrypt the result from ECC algorithm with chaotic technique.
Step7: send image encrypted over Means of communication e.g. (telephone call , viber, yahoo mail or web site).
Step8: The recipient of the encrypted image is applying operation decryption of the image.
Step9: Using chaotic algorithm to retrieve the image encrypted then we use an ECC algorithm to retrieve image.
Step10: The result is a plaintext.
Step11: End.

Algorithm 1: The Proposed Method Algorithm to encryption and decryption operation.

VI. EXPERIMENTAL WORK

In this part will execution example according to steps in algorithm (1), the interface of the proposed system includes two parts that will encrypt the images and decode the images as shown in the figure (5).

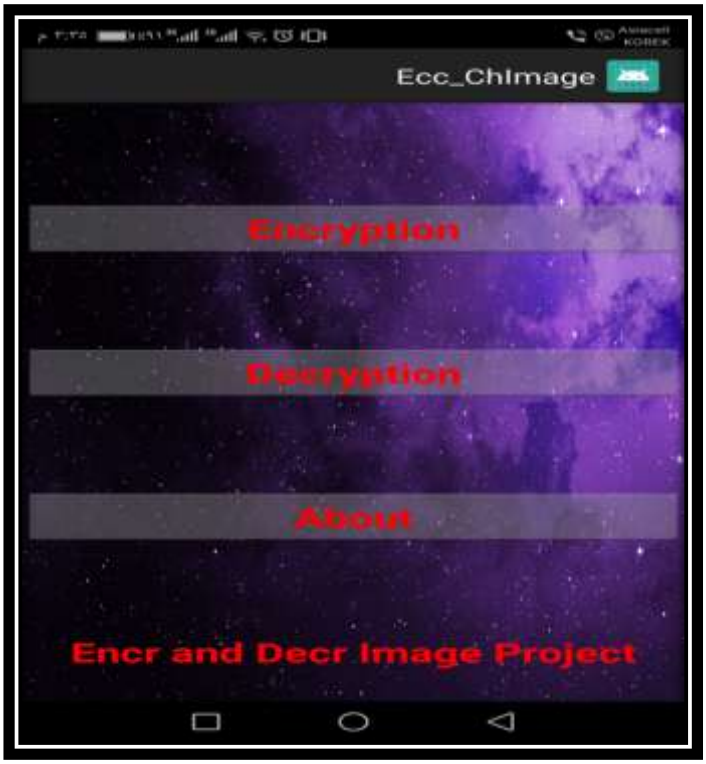
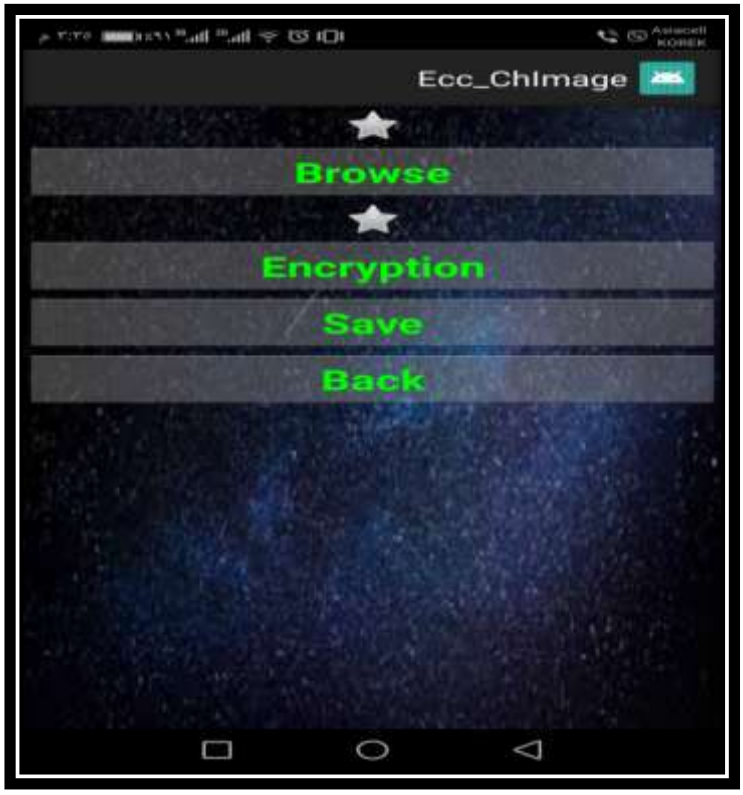


Figure 5: The Interface of the Proposed System

Step2: By pressing the Select Browse to select the image to be encrypted as shown in the figure (6).



Step3: By choosing a picture Gallery then encryption image by using ECC and chaotic technique. Then save, as shown in Figure (7).

Figure 7: Browse the Image

Step4: After browse the image select encryption image as shown in Figure (8).

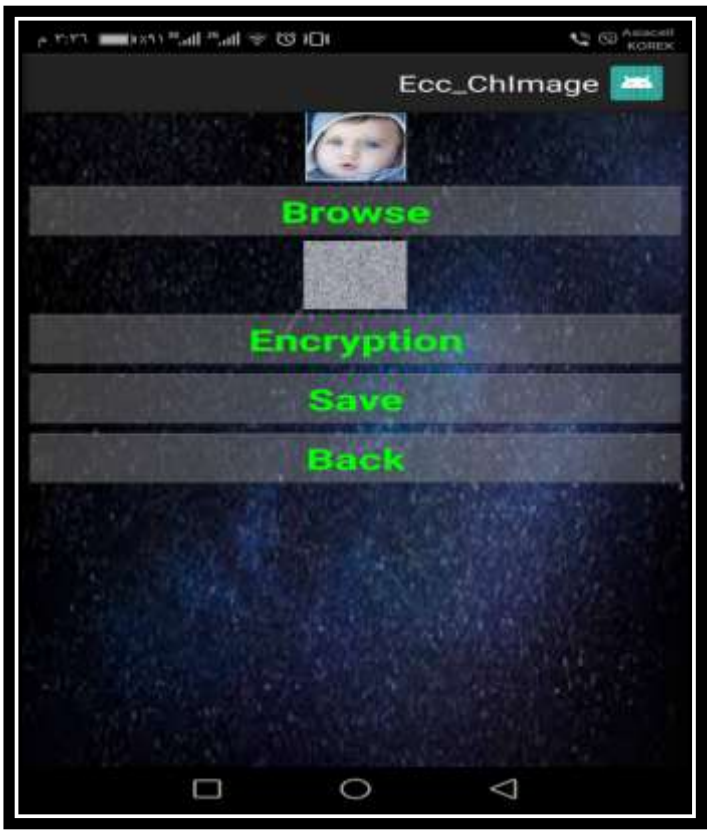


Figure 8: Image encryption by using ECC & Chaotic

Step5: Decryption on the image by clicking on "decryption", then click on browse to load image encrypted to extract original image", the result of Extract is illustrated in Figure (9) & (10).

Figure 9: Load the Image Encrypted

Figure 10: Decryption Image

VII. CONCLUSIONS

1. The ECC algorithm is used for image encryption and is characterized by speed in the key generation process compared to cryptographic algorithms such as RSA and Diffie-Hellman.
2. In this research, RGB color images were used, which were encrypted using the algorithms of (chaotic and ECC algorithms), which were characterized by their ability to retrieve images without any change in the parameters of the images.
3. In this research, an elliptical curve encoding was discussed to address the requirements and safety of Android users. The image encryption was based on the ECC algorithm which is difficult to break down for adoption in action on appropriate mathematical processes.
4. In this work, we used the chaotic algorithm because chaotic system will not produce the same results if the inputs keys are not the specified keys so it is difficult to attack to have the plain text without knowing the secret keys, in this paper to increase the security we use many algorithms to cipher the image as a public key cryptography (ECC algorithm) with chaotic algorithm.
5. The Android is designed to enable the developer to write innovative applications as it is an open source software where developers can enjoy many benefits. The Android is a new platform for mobile development, avoiding past failures and using and building new.
6. This research gave a brief overview of the behavior of Android and his abilities and solved the security problem by increasing the use of cascading encryption.
7. In the future, this work is carried out in the research with the addition of other types of algorithms in an environment other than an android, such as e-mail and other environments.

VIII. ACKNOWLEDGMENT

The author would like to thank AL_Mustansiriyah University (www.uomusiriyah.edu.iq) Baghdad-Iraq for its support in the present work.

REFERENCES

[1] [1]Reynaldo E. Castillo,[2] Gerald T. Cayabyab, [3]Bartolome T. Tanguilig II , SECURITY ASSURANCE FRAMEWORK FOR SMS USING CASCADED ENCRYPTION ALGORITHM, ISSN (Online):2278-5299, Volume 4, Issue 1: Page No.47-55, January-February 2015.
[2] Ali Soleymani, Md Jan Nordin, and Zulkarnain Md Ali, "A Novel Public Key Image Encryption Based on Elliptic Curves over Prime Group Field",Journal of Image and Graphics, Volume 1, No.1, March, 2013.
[3] A. Kataria, T. Anjali and R. Venkat, "Quantifying the smartphone vulnerabilities", Signal Processing & Integrated Networks (SPIN), International Conference on, 2014doi: 10.1109/SPIN.2014, (2014), pp.645, 649.
[4] B. Dan, "Dalvik VM Internals", http://sites.google.com/site/io/dalvik-vm-internals, **(2008)**.
[5] Muneer Ahmad Dar[1] and Javed Parvez[2,"] Security Enhancement in Android using Ellipic Curve Cryptography", International Journal of Security and Its Applications,Vol. 11, No. 6 (2017).
[6] Masmoudi, A.; Puech, W.; Bouhlel, M.S. A new joint lossless compression and encryption scheme combining a binary arithmetic coding with a pseudo random bit generator. Int. J. Comput. Sci. Inf. Secur. 2010, 8, 170–175.
[7] Piyush Kumar Shukla[1],*, Ankur Khare[2], Murtaza Abbas Rizvi[3], Shalini Stalin [4] and Sanjay Kumar[5], Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing, ISSN 1099-4300, Entropy 17.2015.
[8] "The Android Source Code". Source.android.com. Retrieved February 2, 2017.
[9] Jianye Liu, " Research on Development of Android Applications" Fourth International Conference on Intelligent Networks and Intelligent Systems , IEEE 978-0-7695-4543-1,Volume 3,pp 69-72,2011
[10] Chao Wang, Wei Duan, Jianzhang Ma and Chenhuri Wang, " The research of Android System architecture and application programming" Computer Science and Network Technology International Conference (ICCSNT),Volume 2 , pp 785 – 790,2011.
[11] Kirandeep, "Implementing Security on Android Application" The International Journal of Engineering and Science (IJES), ISSN: 2319 – 1813, ISBN: 2319 – 1805,Volume 2, Issue 3,pp 56-59 ,2013.
[12] Er.Amanpreet Kaur1, Er. Navpreet Singh2,"SMS Encryption using NTRU Algorithm",ISSN : 2347 - 8446 (Online), Vol. 3, Issue 2 ,Apr. - Jun. 2015.

