Kurdistan Journal of Applied Research (KJAR) | Print-ISSN: 2411-7684 – Electronic-ISSN: 2411-7706 | kjar.spu.edu.iq
Volume 2 | Issue 3 | August 2017 | DOI: 10.24017/science.2017.3.17

Data (Video) Encryption in Mobile Devices

Aya Khalid Naji
Computer Science Dept.
Mustansiriyah University
Baghdad, Iraq
ayaayak9@gmail.com

Saad Najim Alsaad
Computer Science Dept.
Mustansiriyah University
Baghdad, Iraq
dr.alsaadcs@uomustansiriyah.edu.iq

Abstract: In the development of 3G devices, all elements of multimedia (text, image, audio, and video) are becoming crucial choice for communication. The secured system in 3G devices has become an issue of importance, on which lot of research is going on. The traditional cryptosystem like DES, AES, and RSA do not able to meet with the properties of the new generation of digital mobile devices. This paper presents an implementation of video protection of fully encrypted using Elliptic Curve Cryptography (ECC) on a mobile device. The Android platform is used for this purpose. The results refer that the two important criteria of video mobile encryption: the short computation time required and high confidentially are provided.

Keywords: video encryption, Mobile Application, encryption, decryption, confidentiality, elliptic curve cryptography ECC, prime field, Android platform.

1. INTRODUCTION

Multimedia information like graphics, images, audio and video have been widely used in a smart phone device. Protection in video conference, video surveillance, pay-TV, etc., becomes a challenging work in video communication especially for wireless mobile device. An efficient multimedia encryption algorithms satisfying substitution and permutation and has brute force resistance will become growingly important [1] [2]. The efficiency of any mobile video encryption algorithm is concerned with two criteria: the first one is computational time required to process video data and the second one is memory usage according to the resources on the Smartphone [3].The secure storage of video data should be provided to protect confidentiality. Encryptions mostly consider as an efficient tool providing the confidentiality to protect information even with phone stolen.

Cryptography is a transformation of the plain message to make them secure and immune from intruders. Information security algorithms are widely used in the recent times to protect data [4], one of the promising cryptosystem is The Elliptic Curve Cryptography (ECC). It is introduced by Neal Koblitz and Victor Miller independently in 1985 [5] [6] and based on elliptic curve defined over a finite field to devise discrete logarithm cryptographic schemes [5]. ECC is based on the generalized discrete logarithm problem, ECC is often considered as the preferred public-key scheme. For example ECC implemented on 160 bit has the same level of security against attacks if we compare it with RSA 1024 bit.

2. LITERATURE REVIEW

This section is dedicated for some papers related to video encryption algorithms and focusing on Elliptic Curve Cryptography (ECC) and the improvement or modification on it.

- Rahouma, K.H. 2006 [7]. The idea of this paper is to use a number of curves with addition parameters to compute a new equation. The message is divided into blocks such that each block is of a length less than the smallest prime number P of the used ECC. The system uses a random sequence generator and modulus to determine the elliptic curve which is used to encrypt/decrypt a certain message block. The authors referred when disclosing some of the keys does not help an attacker to decrypt the message because the used EC and the keys are changed from a message block to another and does not know when and which EC they will be applied.

- D. Sravana Kumar, CH. Suneetha A., ChandrasekhAR 2012 [8], this paper adds another parameter called C point shared between (Alice and Bob) and each side selected his own point and used a special key for each message point. Each message should be converted to point and be encoded according to a table. The authors used two equations for encryption rather than one as in stander ECC and the method of encryption proposed here provides sufficient security against cryptanalysis.

- Rahul Singh, Ritu Chauhan , Vinit Kumar Gunjan, Pooja Singh 2014 [9] , this paper considers an elliptic curve cryptography over a finite field associated with prime number p >3, every value in the audio file is converted into an affine point (audio file into (Xm ,Ym) coordinate that is the point of elliptic curve and then encrypted). The authors converted a message to the point, according to Koblitz equation and encrypted audio by using the ECC algorithm. The authors claim their proposed algorithm is especially useful in applications where bandwidths, processing capacity, power availability or storage are constrained and can easily use in video applications.

- Naik M., Sindkar A., Benali P., Moralwar C. 2014 [10], In this paper the authors described the technique to encrypt the data and messages in mobile devices transmitted over network .This technique is developed under android platform and used two algorithms for encryption data , the first used symmetric AES and the second used asymmetric ECC , in sender and receiver sides are used the appropriate keys for encryption and

decryption of the data .and he claims the system are achieving confidentiality ,authenticity ,and integrity of massage and data.

- Dhananjay M. Dumbere , Nitin J. Janwe 2014 [11] , this paper used Advanced Encryption Standard (AES) Algorithm for Video encryption. AES algorithm is also compared with a modified algorithm of the Data Encryption Standard (DES).The results referred that encryption and decryption time in AES is better.

- F. Hadi 2015 [12] . This thesis modified the AES to encrypt data mobile phone. He takes different cases to show result of system between classical AES and modified AES in terms of computational complexity and security. The platform used in mobile and programming language is the Android Studio. The author claims the adjust AES encryption algorithms have many advantages which are; robust encryption, fast encryption and decryption process, and easy implementation.

- A. Kareem 2015 [13], this thesis applied two types of modifications on AES (FMAES and SMAES) to encrypt video, he claims the experimental results indicate that the FMAES is more secure than the original AES and SMAES. The SMAES is secure a more than the original AES algorithm according to the results of the most security tests in addition it is faster than the original AES algorithm and FMAES algorithm. Both of the modified algorithms are supported through multithreading concept which is provided by the C# programming language. He extracts all video frames and divide these frames to four groups to divide them on four threads to speed the processing time that based on libraries provided by programming language.

- R. Samih 2015 [14], The proposed system used RC6 algorithm and XOR operation, in addition to the RC4 (that generate keys for all Blocks encryption).The platform used in the computer and the type of MPEG-4 used is (part 2).She uses a mechanism for access to frame of video for mp4 header by parts (stsz ,stsc and stco) , Elapsed time for encryption and decryption is long .

- Mankiran Kaur , Manish mahajan 2016 [15],This paper is used application in mobile devices to communicate between user and cloud computing using double algorithms are (AES , geometric host encryption algorithm (ghost)) and uploaded data on a server through registration by using a user name, password and email. This work is issued more security for data when the cloud computing be attacked, the user can download the data decrypted stored by the server and successfully stored in mobile devices.

3. SECURITY REQUREMENT FOR MOBILE DEVICE

A. Mobile Application

A mobile application is a computer program that its designed based on the operating system to be run on mobile devices.Until now, both iOS and Android are the most famous operating systems that can offer millions of applications. [16] .Figure 1 illustrates a bar chart among different applications in mobile devices for main applications stores as of June 2016.

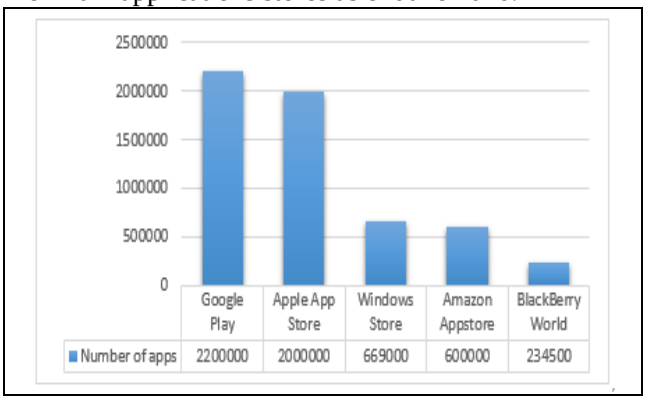

Figure1 Number of applications available in different stores [17].

1. Mobile Operating Systems

- **Android OS**

It is an open source released by Google under the Apache license. The kernel of an operating system is a Linux. Android apps are written in the Java language in android studio environment .The first Android phone is sold in October 2008 [18].

- **iOS**

It is close source released by the Apple Company. The kernel of an operating system is UNIX. iOS apps are written in Objective-C in Swift or Xcode environment. The first iPhone release in June 2007 mainly uses for the apple product such as the iPhone and iPad [18] [19].

B. Video Encryption

The technique to protect video is by encrypting the video itself, which is the main concern in mobile device applications and issues. The unauthorized users cannot read that data, and hackers or thieves will not be able to read encrypted data on mobile devices. This paper presents an implementation for using ECC in mobile device for video encryption file. The propose ECC algorithm focuses on increasing the security of the algorithm the video for mobile phone.

C. Mathematics of Cryptography

Groups: A group , denoted as G=<{..},•> is set of elements with one binary operation(•) satisfying the following four properties: Closure , Associative law ,Identity law , Invers law , If a group G also satisfies the commutative then G is called Abelian group [20] . Elliptic curve satisfies Abelian group.

Field: denoted by **F** (consist of a set) with two operations, addition (denoted by +) and multiplication (denoted by •), that accomplish the usual arithmetic properties.

- Prime field F_P where P is a prime.
- Binary field F_{2^m} where m is a positive integer.

Group Operation on Elliptic Curves In this section we consider the Group operation is addition "+". Addition means that to add two given points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, the result $R = (x_3, y_3)$. Two cases we have to present:

Case (1): when $P \neq Q$

The construction works as follows draw a line through *P* and *Q* and obtain a third point of intersection between the elliptic curve and the line. Mirror this third intersection point along the *x*-axis. This mirrored point is, by definition, the point *R* [21].

Case (2): when P=Q

This is the case where that is computed *P+Q but P=Q* = 2P, draw the tangent line through *P* and obtain a second point of intersection between this line and the elliptic curve, and mirror the point of the second intersection along the *x*-axis. This mirrored point is the result *R* of the doubling [21].

Table 1 illustrates the more details between case1 and case2

	Name	Slope	Figure	New value calculation
Case1 $P \neq Q$	**Adding**	$Slope = \frac{y2-y1}{x2-x1} \ mod\ p$ **(1)**	**Figure 2.a**	$x3 = Slope^2 - x_1 - x_2 \ mod\ p$ **(3)** $y_3 = Slope(x_1 - x_3) - y1 \ mod\ p$ **(4)** [21]
Case2 **P=Q**	**Doubling**	$Slope\ \frac{3x_1^3+a}{2y1} \ mod\ p$ **(2)**	**Figure 2.b**	

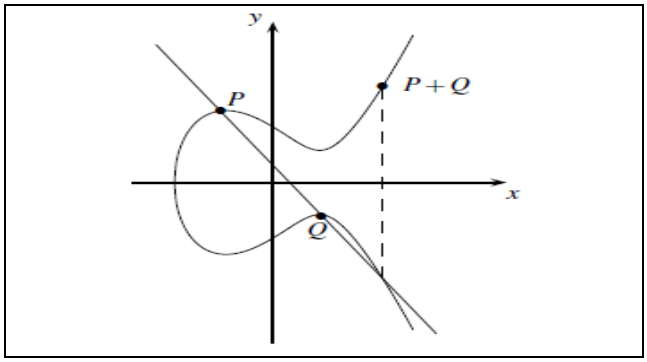

Figure 2.a Adding on an elliptic curve.

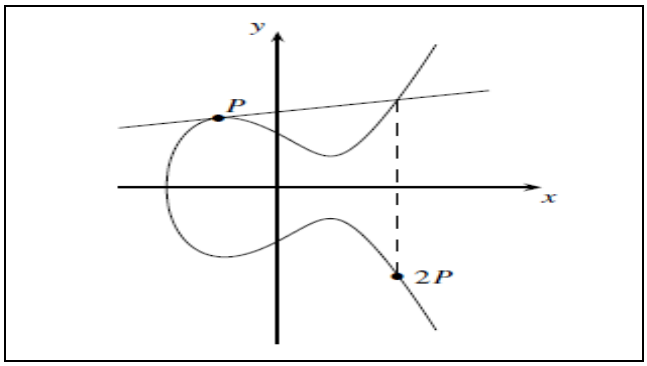

Figure 2.b Doubling on an elliptic curve.

D. Proposed System Using Elliptic Curve Cryptography Encryption and Decryption

The proposed encryption / decryption system contains five stages: Getting the Base point, Calculating private/public keys for sender and receiver, Encryption side and Decryption side. These stages are illustrated with example in sections E1, E2, E3, E4 and E5 respectively and as shown in Figure3 flowchart of block diagram system:

- **E1 Open Video** User select video from storage we treated the video with full encryption without entering into the video of header structure and open as byte.

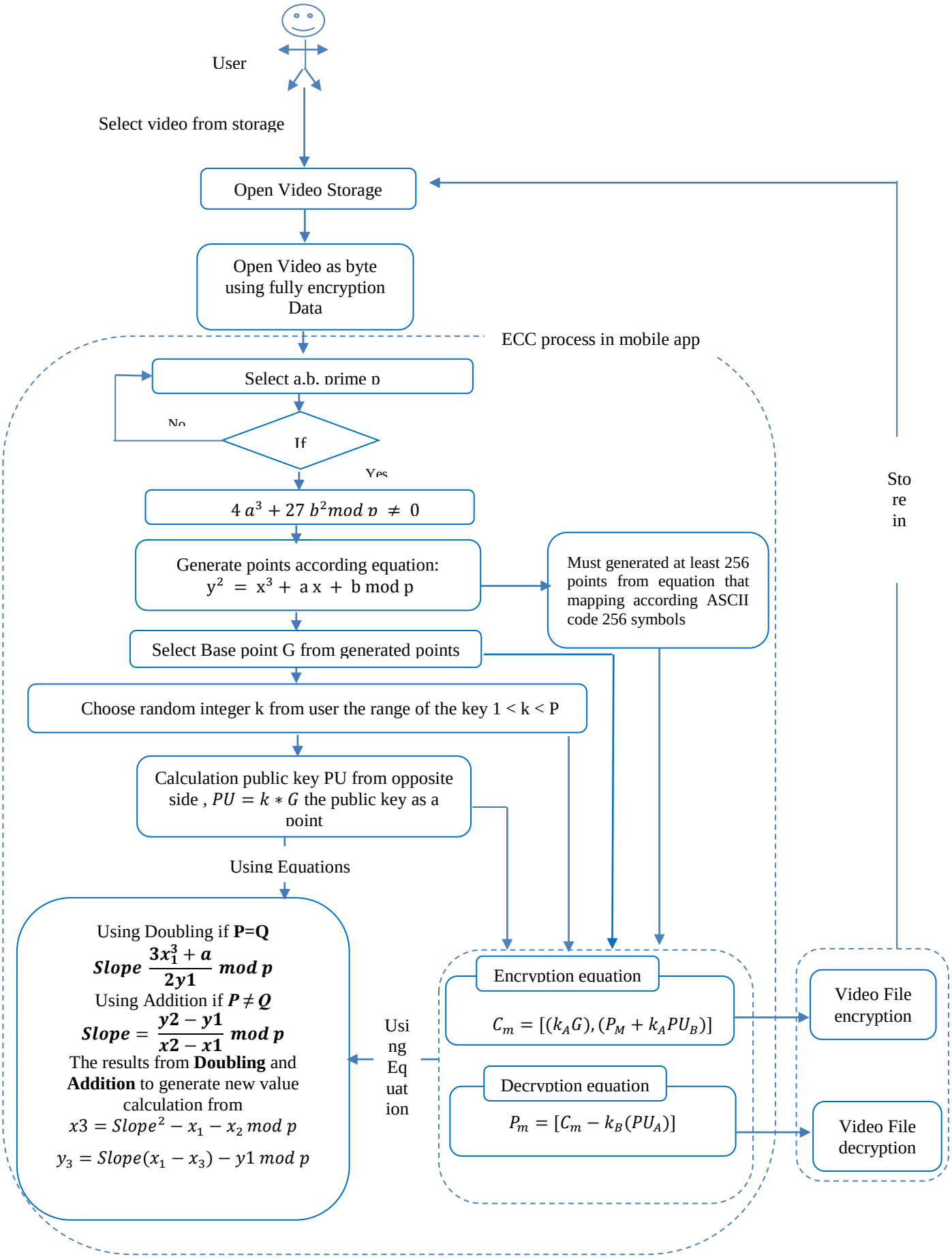

Figure 3 flowchart of block diagram system

- **E2 Algorithm 1. Find Base Point**

Input: *Select prime number p*
S is set of point // s is empty
Output: Base Point G
Step 1: choose a and b such that:
$4\,a^3 + 27\,b^2 mod\ p\ \neq\ 0$
Step 2: for x = 0 to p-1
for y = 0 to p-1
if $y^2\ =\ x^3 +$ a x + b mod p add point (x,y) to s
End for
End for
Step 3: select point G from s

Illustration example:
Prime number: 251

Step1: (a,b)= (4,4)

Step2: Number of points generated in step 2 is 257 points are below:
{(0,2),(0,249),(1,3),(2,32),(,2,219),…,(245,212),(246,19),(246,232),(247,41),(247,210)}.

The points generated from step2 are depicted in figure 4.
Output: Base point G: (0,2).

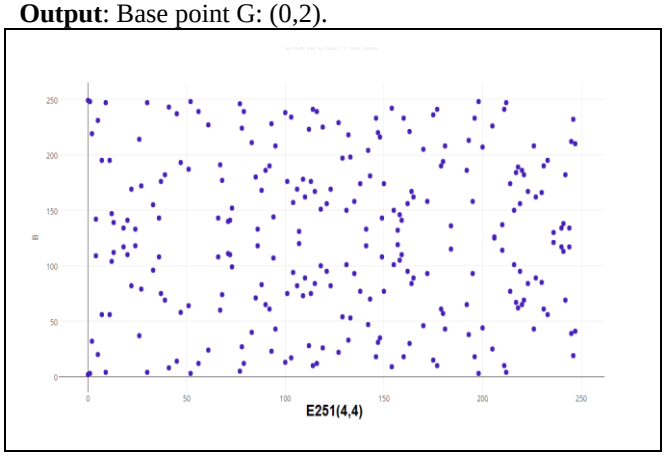

Figure 4 Generator points from main equation.

- **E3 Select Key**

k_A and k_B are the private key of the sender (Alice) and the private key of the receiver (Bob) respectively . Choose random integer k such that 1 < k < P.
Calculate public key Alice (PU_A) and Bob (PU_B) from k integer value for each side with G where G the Base Point on elliptic curve $PU = k * G$.

Example:

Alice selects for example: 17
Bob selects for example: 18

Public key for Alice $PU_A\ = k_A * G$
$=17\ (0,2)$
$= (121,95)$

Public key for Bob $PU_B\ = k_B * G$
$= 18\ (0,2)$
$= (83,40)$

- **E4 Encryption Side Equation**

Using addition and doubling operation for use the encryption equation:

$$C_m = [(k_A G), (P_M + k_A PU_B)]$$

P_m : (x,y) Represent the plaintext as the point on a curve, for example : (72,141) .
$C_m = [\ (17(0,2))\ ,\ \ ((72,141) + 17(83\ ,40))\ ]$
$= [\ (121,95)\ ,\ \ ((72,141) + (79,12))\ ]$
$= [\ (121,95)\ ,\ \ (163,30)\ ]$
Public key cipher message (Cm)

- **E5 Decryption Side Equation**

Using addition and doubling operation for use the decryption equation:

$$P_m = [C_m - k_B(PU_A)]$$

$= [(163\ ,30) - 18(121,95)]$
$= [(163\ ,30) - (79,12)]$
$= [(163\ ,30) + (79,-12)]$
Where -12 is eliminating 251-12 =239
$= [(163\ ,30) + (79,239)]$
$= (72,141)$

Note: These parameters are illustrative.

4. RESULTS

Eight video files have been tested on smart phones using fully encryption. 256 points must be generated on a curve and each input character is converted to byte code according to the standard ASCII code table for video representation. Android platform with version Jelly Bean (4.1) is used for ECC implementation. Table 2 presents the video files and the time required for encryption and decryption and with charts as show in Figure 5 , Figure 6 respectively . The measurements in the table refer that the implementation of ECC in smart phones contributed positively in solving the limitations of video phones security.

Table 2: Video encryption and decryption results for different sizes.

Video	Type Of Video	Size	Duration MM:SS	Resolution	Encryption Time MM:SS	Decryption Time MM:SS
Va	MP4	932 KB	00:15	400*400	00:30	00:55
Vb	MP4	1.1 MB	00:42	360*360	00:35	01:10
Vc	MP4	1.92	00:28	480*480	01:20	02:20
Vd	MP4	2.5 MB	00:09	1280*720	01:20	02:20
Ve	MP4	2.3 MB	00:53	470*360	01:20	02:20
Vf	MP4	2.54 MB	01:44	400*400	01:30	02:22
Vg	MP4	2.6 MB	00:34	270*480	01:25	02:30
Vh	MP4	5.2 MB	01:34	368*368	02:40	05:55

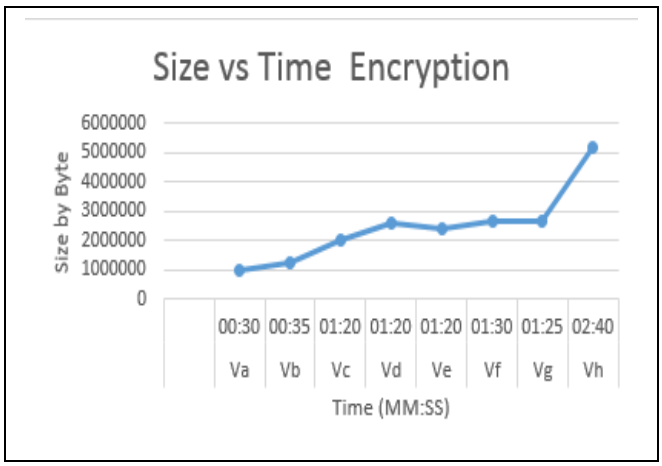

Figure 5 Time encryption

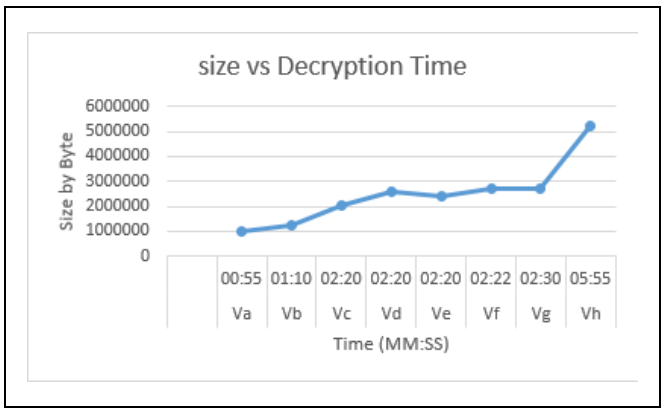

Figure 6 Time Decryption

After we use the side encryption algorithm ECC of operation to access program and get the video file from the video store, we will notice the video as shown in the figure 7.

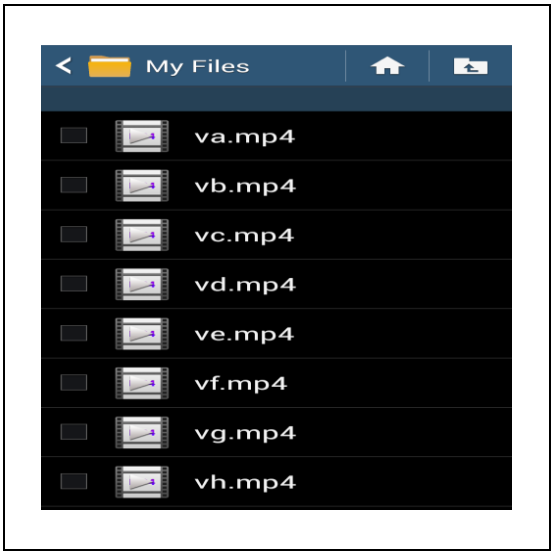

Figure 7 Video encryption

When we click on any video encryption does not display video and show message as shown in the figure 8.

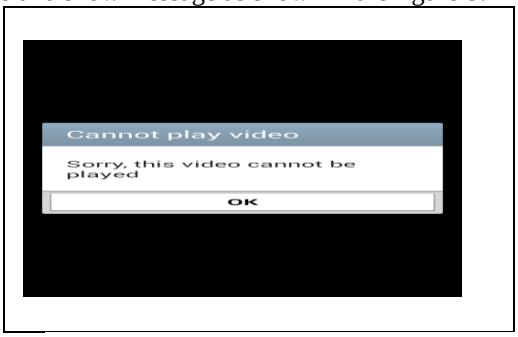

Figure 8 Video message

When we use the side decryption algorithm ECC of operation to access program and get the video decryption file from the video store, we will notice the video as shown in the figure 9.

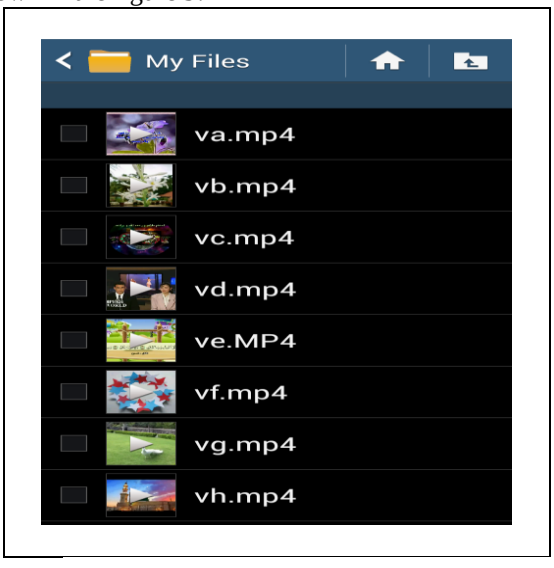

Figure 9 Video Decryption

5. DISCUSSION

The paper basically aims to develop a system for video encryption on mobile device using ECC algorithm. We aim to prove in high reliability and reasonable time.

4. CONCLUSION

The implementation of ECC on video data that applied under mobile platform using android studio, a similar technique for implementation ECC can be used for encrypting data and decryption data like text, image, sound, and real time in mobile communication with dynamic exchange key. It is noted that the decryptions take more time relatively with the encryption time required and this is acceptable because of the nature of the algorithm besides that the algorithm is implemented in limited resources memory in the mobile platform compared with the computer platform.

The advantage of this system is achieving the protection for video of data in mobile devices such as confidentiality for the secure end to end user and the user interface (IU) it is easy for interacting and not difficult for using by any person when needed encryption video file.

5. REFERENCE

[1] P. Saranya.,M.LVaralakshmi "H.264 based Selective Video Encryption for Mobile Application," International Journal of Computer Applications, vol. 17, pp. 21-25, 2011.

[2] A.Saad Najim, H.Eman, "A Speech Encryption based on Chaotic Maps," International Journal of Computer Applications, vol. 93, pp. 19-28, 2014.

[3] M.Danang Tri, Dr. Ir. Rinaldi Munir, M.T., "Secured Video Streaming Development On Smartphones With Android Platform, " In Proceedings of the IEEE International Conference on Telecommunication Systems, Services, and Applications (TSSA), pp. 340-344, 2012.

[4] S.Laiphrakpam Dolendro, S. Khumanthem Manglem, "Implementation of Text Encryption using Elliptic Curve Cryptography, " In Proceedings of the Elsevier International Multi-Conference on Information Processing(IMCIP), pp.73-82, 2015.

[5] H.Darrel ,M.Alfred and V.Scott , Guide to Elliptic Curve Cryptography, Springer, 2004.

[6] Y. Salem, "Implementation of Elliptic Curve Cryptography using biometric features to enhance security services," Msc, University Malaya, 2009.

[7] K. Rahouma, "A Modified Menezes-Vanstone Elliptic Curve Multi-Keys Cryptosystem," semanticscholar.org 2006. [Online].Available: https://pdfs.semanticscholar.org/d13c/05f9256790d9af7637009168b3018fdaf06b.pdf.

[8] D. Sravana Kumar, CH. Suneetha A., ChandrasekhAR, "Encryption of Data Using Elliptic Curve Over Finite Fields," International Journal of Distributed and Parallel Systems ,vol.3,pp.301-309, 2012.

[9] S. Rahul, C. Ritu, G.Vinit Kumar , and S.Pooja, "Implementation of Elliptic Curve Cryptography for Audio Based Application," International Journal of Engineering Research & Technology , vol. 3, pp. 2210-2214, 2014.

[10] N.Mayur, S.Avinash, B.Pratik,and M. Chetan, " Secure and Reliable Data Transfer on Android Mobiles Using AES and ECC Algorithm, " International Journal of Innovative Technology & Adaptive Management (IJITAM) www.ijitam.org 2014[Online].Available:http://www.ijitam.org/doc/v11c4.pdf.

[11] M. Dhananjay, J. Nitin , " Video Encryption Using AES Algorithm," In Proceedings of the IEEE International Conference on Current Trends in Engineering and Technology (ICCTET), pp.332-337, 2014.

[12] F. Hadi, "A Modified AES for Mobile Devices," MSc thesis in Computer Sciences University of Technology, 2015.

[13] A. Kareem, "An Efficient Block Encryption Cipher Based on Chaotic Maps for SecureVideo Applications, " MSc thesis in Computer Sciences , Al-Mustansiriyah University, 2015.

[14] R. Samih, "MPEG-4 Encryption based on RC6 and RC4," MSc thesis in Computer Sciences , Al-Mustansiriyah University, 2015.

[15] K.Mankiran, M.Manish, "Enhancing Security in Mobile cloud computing using double-encryption model, " International Journal of Modern Computer Science , vol. 4, pp. 69-73 , 2016.

[16] H. Zimeng, "Security of Mobile Devices and Wi-Fi Networks," Bachelor's Thesis MAMK Unviversity of applied sciences , 2015.

[17] The Statistics Portal https://www.statista.com/statistics/266211/distribution-of-free-and-paid-android-apps/ (2017).

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

[19] A.Jeremy,H. Alexander Van't,and A.Naser, "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 UT, USA, 2014.

[20] I. Jabbar, "Secure E-Voting System Using Homonrphic Encryption, " Msc , University of Mustansiryriah, 2016.

[21] C. Paar , J. Pelzl , Understanding Cryptography A Textbook for Students and Practitioners, Springer, 2010.

[22] E.D.Ziad,Y.N Shahrul , and R B O Rozmie r" A New Modification for Menezes-Vanstone Elliptic Curve Cryptosystem, " Journal of Theoretical and

Applied Information Technology, vol. 85, pp. 290-297,2016.
[23] K. Rabah, “Theory and implementation of elliptic curve cryptography,” Journal of Applied Sciences, pp. 604-633, 2005.

ACKNOWLEDGMENTS

I would like to thank the Mustansiriyh University to its study . I also would like to thank Pro. Saad and Mr. Faisal and my family and my friends .

Biography

Dr. Saad Najim Alsaad is Professor in Computer Science at College of Science/ Mustansiriyah University Baghdad / Iraq. He is working as senior in Computer Science Department. He is working as teaching staff member more than 20 years.

Aya Khalid Naji is a computer science graduate at 2011-2012 and currently a master's student in the research stage at College of Science/ Mustansiriyah University Baghdad / Iraq.