International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 3 Issue 11 ǁ November. 2015 ǁ PP.53-58

Photography Capture and Encryption on Smart Phones with Android Operating System

C. Cortés[1], D. Zamorano[2], C. Aguilar[3]
[1]Esime Culhuacan, National Polytechnic Institute.
[2]Esime Culhuacan, National Polytechnic Institute.
[3]Esime Culhuacan, National Polytechnic Institute.

ABSTRACT
This paper presents the development of an application for the encryption of photographs on Smartphones with the Android operating system, understanding how that image captured by the camerawithin the device , in order to ensure the privacy of this content to the user. The significance lies that the image data are encrypted before stored, improving the level of safety. The encryption algorithm used to encrypt the photographs is AES with a key of 256 bits. The results show that encryption time is imperceptible for the user and the decoded image is not at least changed from the original.
Keywords: *AES, Android, cryptography, Informatics security*

I. INTRODUCTION

Currently the technology in cell phones has evolved to such a degree that even they have been denominated as intelligentphones (smartphones) since besides fulfilling the basic functions of a conventional telephone, they give the opportunity to perform tasks that were previously possible only by using a computer. Including alsointegrated functionality from other devices such as a PGS browser, video game console, television, and digital camera, among others.

Within the market for Android smartphones is the (OS) operating system that has more presence. According to a study by the web monitoring company "Pingdom," during the period from October 2011 to October 2012, the number of smartphones in the world increased a 39%, and Android with an 88%, being found in the 70% of the devices (Pingdom, 2013). The information before mentioned can be seen in Figure 1.

On the other hand, the ability to take high-resolution photographs on these devices, notes how cameras are being replace by smartphones that mainly use the Android OS. Nevertheless since it is an article that is usually carried to all sorts of places, you may take the risk of being robbed or losing it.

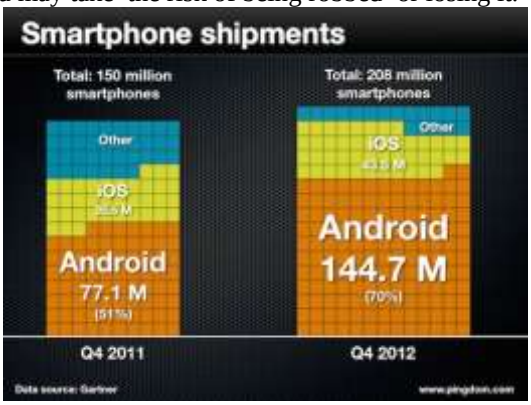

Figure 1. Growth of Smartphones with Android

According to the type of user, the loss of their Smartphone represents a level of danger; for example, there are activities such as the ones that perform agents, police or insurance companies, where the images captured by the camera in the device contain sensitive or careful information. Therefore it requires a mechanism that may allow maintaining the confidentiality of such images as they should not be exposed to people who might misuse them.

In the official Android store called "Play Store" many applications designed to protect the confidentiality of images or photographs may be found. Table I shows some examples according to the method of protection implemented.

Table 1. Applications for confidentiality of images

Applications	Method of protection
• KeepSafe • Smart Gallery Lock	By modifying the properties of the image, move the image to a hidden folder and change its extension .
• Super silent spy camera • Camopic	Using steganography, they hide the data of the secret a image in such a way that cannot be noticed the existence of the first.
• Photo Locker • SafeCamera	Using cryptography they generate an encrypted or secret image by applying a cryptographic algorithm and a secret key .

However these applications have some drawbacks, the first method, the device can be connected to a computer and check the folders to find the hidden image. The use of steganography is a better alternative because it is intended to not perceive the existence of a secret image, however, these applications retain the original file, in such a way that the image remains exposed to persons with bad intentions, on the other hand you can extract the hidden image by relatively simple means. In the case of cryptography it offers the best level of security because it is only possible to unprotect or check out the image only if you know if the key or password used for the encryption which does not occur in steganography as it is known.

The problem with most applications that use cryptography is that they only allow you to work with stored images in the permanent memory of the device. Therefore the action of taking a photograph and then encrypt it with some of these applications would have to be done with different applications and has certain vulnerabilities since:

- There is a lapse of time since the user captures a photography until he chooses to encrypt it, meanwhile the phone can be exposed to theft or lost.
- Although the original image is deleted or overwritten with the encrypted image, it is still possible to reconstruct it using data recovery techniques.
- They retain the original file, causing a vulnerability if this is not erased.

Based on the above, this paper shows the development of an application for smartphones with Android operating system to keep confidential those photographs with sensitive information. This is done at the moment of capturing, encrypting the image data that are returned by the camera through an array of bytes. The resulting arrangement, it may be said, the one containing the encrypted data, is the one stored in a file.

II. CRYPTOGRAPHY

Cryptography is the science that deals with the study of techniques to transform the information in such a way that it may not be understood at a simple glance. Usually to encrypt a file it is necessary to establish a clue or a key, also known as password. The key should only be known by the person or persons who wish to have an access to the encrypted information (Aguillon, 2012).

When it is required to keep certain information secret so that only the person who knows the correct password may be able to have access to it, the symmetric key cryptography that consists in performing the encryption and decryption of a message using the same secret clue or key is used (Stallings, 2011: 33), as shown in Figure 2.

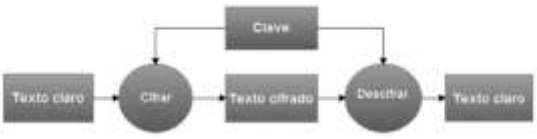

Figure2. Symmetric scheme of the cryptographic key

Among the symmetric key algorithms are:

- DES (Data Encryption Standard)
- TripleDES o TDES
- AES (Advanced Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish
- Twofish
- RC4

For this project AES was used that works with blocks of 256 bits in length, this algorithm was published in 2001 by the National Institute of Standards and Technology (NIST) as FIPS PUB 197, It was later adopted as standard encryption by the government of the United States. Its main features are:

- Key of 128, 192 and 256 bits. This meets the security needs of the user.
- It is of common knowledge that it has been studied and tested by cryptanalysts worldwide, positioning itself as a highly reliable algorithm.

In the PKCS#5 (standard password-based encryption) a standardized symmetric key encryption is described called PBES2 (Password-Based Cryptography Standard 2) which can involve selection of parameters such as an initialization vector and a refilledmethod. A bypass function based key password is combined which should be PBKDF2 (Password-Based Key Derivation Function 2) . (Kaliski, 2000: 9).

It is a fact that the length of the information needed to encrypt not always will be a multiple of 256 bits (16 bytes) for that, padding or filling methods are employed in order to achieve the required length. The method specified in PBES2 known as padding and consists of adding N number of bytes as needed, where the value of each byte is equal to N (Kaliski, 2000: 11), this can be viewed in Figure 3.

As already mentioned AES works 256-bit blocks, thus to encrypt greater length information it is necessary to use what is known as the operating mode. The most widely used is the CBC (Cipher Block Chaining) that consists of applying the XOR operation on the plaintext and cipher text of the previous block.

As in the first block, cipher text is not available from a previous cipher text block, an initialization vector containing random values is introduced. Thus it is achieved that two identical messages will not generate the same ciphertext (Stallings, 2011: 199),. The operation is described in Figure 3.

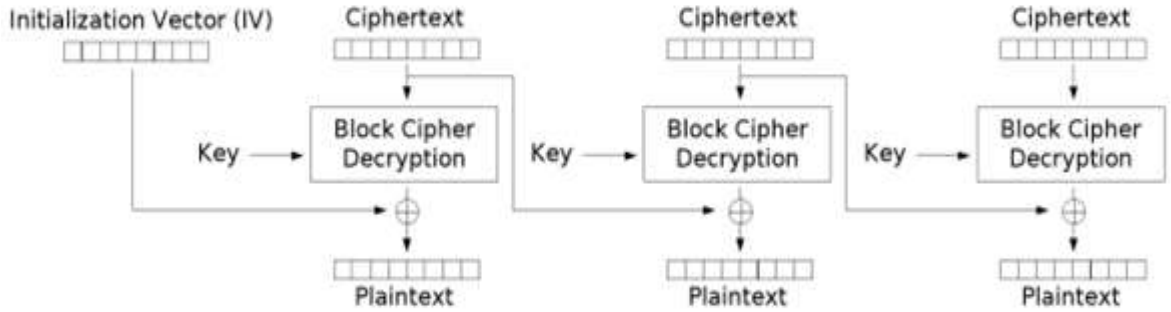

Figure 3. Encryption in CBC mode

To generate the 128, 192 or 256 bits that form the encryption key used with AES, key derivation functions are used. These receive as input besides the user's password, a number of iterations and a string of randomly generated bytes, this helps mitigate dictionary attacks and rainbow tables. The function used is PBKDF2 (Password-Based Key Derivation Function 2) (Kaliski, 2000: 11), which is described as follows:

DK = PBKDF2(PRF, P, S, c, dkLen) (1)

Where:

PRF: pseudorandom function used
P: User password
S: Sal, generated randomly
c: Number of iterations
dKLen: Length of the derived key
DK: Derivative key

III. MATERIALS AND METHODS

The software used for the design and programming was Eclipse v4.2 along Android SDK was integrated, the programming languages used were Java and XML. We worked with the spiral software development model in such a way that in the first stage will have the basic operation of encrypting a photograph, and in later stages the interaction would improve and perfection its interaction with the user.

The application is divided into five activity's or windows:

- Menu
- Request of the password for encryption
- Camera Interface
- File Browser
- Request of the password for decryption

The overall operation and the flow of information is illustrated in Fig. 4.

The menu is what is first shown when the application starts, it is made up of two buttons, the first one calls the activity "Password request." The idea is to work with a password by session of photography, this means that the

photographs taken at one point or at the same time should be encrypted with the same password, this provides a balance of security and productivity. The second button calls for the "File Explorer" so that the user may choose the picture he needs to decipher. In Figure 5 this section is observed.

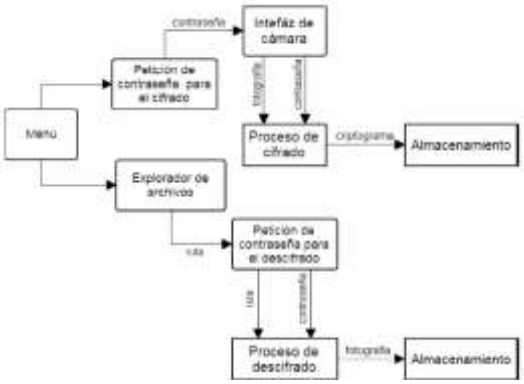

Figura 4. Application scheme

Figure 5. Screen where the menu is displayed

Next the user is asked to enter a password for the photography session. It requires that the word entered has a minimum length of 8 characters according to letters and numbers. When the word entered meets these characteristics the activity is called "Camera interface" sending as a parameter the password entered.
Figure 6 The design is shown

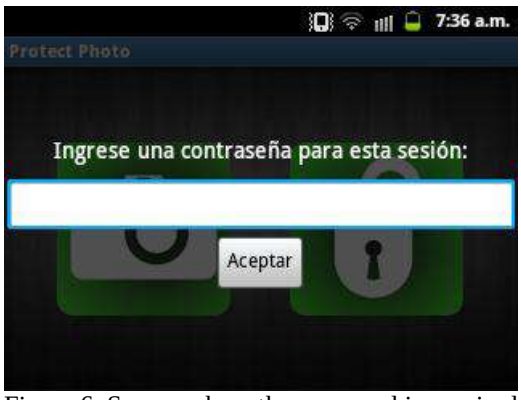

Figure 6. Screen where the password is required

Subsequently, the interface lets you view what the camera sensor captures. It has a button that activates capture processes and encryption as shown in Figure 7. Once the user presses this button, is generated in the RAM of the phone, a vector of bytes with the photo information in format JPEG. The vector and the user's password enter the encryption process comprising the following phases:

Key derivation:. Added to the PBKDF2 function is the password, a number of 1000 iterations and the salt consisting of MD5 hash of the photography that yield an output a 256-bit key length.

Encryption: It is performed with the AES-256 algorithm in CBC mode and PKCS5Padding, for this, the key is introduced, the vector containing the photograph information and an initialization vector that just as the salt consists in the MD5 hash of the picture.

After the contents of the vector encryption with the MD5 hash of the unencrypted image is stored in the multimedia default directory /mnt/sdcard/ DCIM with the extension .jpg. After this process is ended we may have the possibility for more captures. When you want to encrypt with another password you only have to return to the start menu and start a new photo session.

Figure 7. Camera's interface.

Once you have encrypted photographs and the user wants to view its contents, you can access the file browser, it allows you to navigate through folders and select a file with the extension .jpg, when this is done you call the activity "Petition password for decryption "sending the path of the selected file. Figure 8.

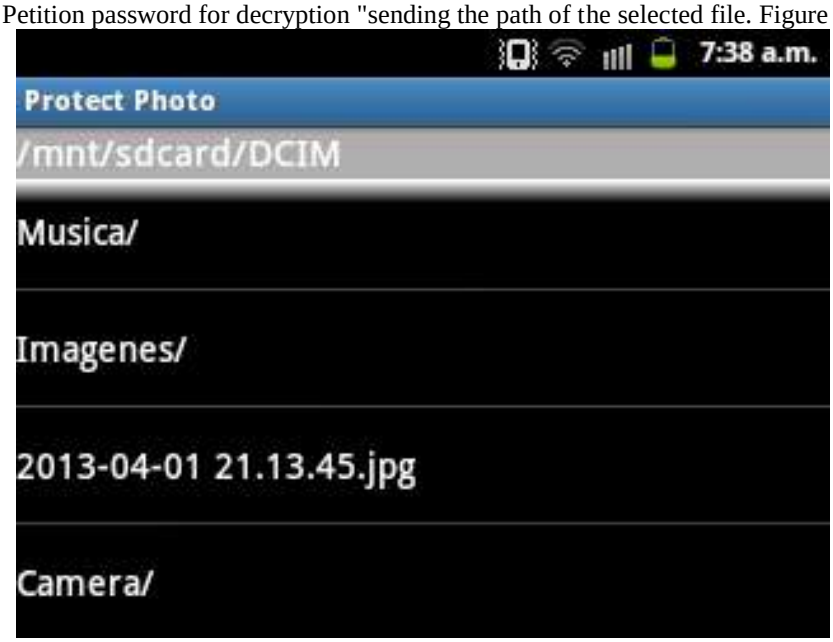

Figure 8. File Browser.

Once the file is selected a password is requested, validating the user to enter at least one character. Once the password is entered the data file is read and inserted into a vector, the vector and password are sent to the decryption process. If the password is correct, the vector will contain the photo data which are stored in the same directory as the encrypted file.

IV. RESULTS

Two types of tests were conducted, the first of which was to estimate the time of encryption and decryption in the second the integrity of photography that means that the image data unencrypted (original) were the same data of the decoded image.

V. TIME OF ENCRYPTION AND DECRYPTION

By the "LogCat" tool integrated in Eclipse, the times that take the application to perform the encryption and decryption of a photograph measured in milliseconds, they were measured.The results are shown in Table II.

TableII. Measuring time encryption and decryption

Num.	Encryption	Decryption
1	586	586
2	742	742
3	710	625
4	687	548
5	734	656

The average time duration of the encryption process is 692 milliseconds, and the average time for the decryption process is 632. This covers the time occupied by the PBKDF2 function and AES. The tests were conducted in 2-megapixel images captured with a Samsung Galaxy Y phone, which is one of the phones with the lowest processing power.

VI. INTEGRIDAD DE LA FOTOGRAFÍA

This test was to verify that the data of the unencrypted image and that of the decoded image are exactly the same, in order to do, this application was modified in such a way that photography was stored unencrypted and also its cryptogram. The test consisted in realizing several shots and after deciphering the cryptograms generated, the images obtained were analyzed with the "MD5 & SHA-1 Checksum Utility" and "ExifTool" programs. The results showed that no bit was modified in the decoded image, since the hash of the original image and the encrypted one were identical and there was no change in their metadata of creation.

VII. CONCLUSIONS

The developed application is very useful for those who require confidential use of photographs, having the confidence that these images are protected by reliable mechanisms, plus the time needed for the encryption process is virtually imperceptible, the user can also be sure that the photograph did not suffer any alterations.

REFERENCES

[1] Royal Pingdom. (2013). El aplastante dominio de Android, en cinco gráficos. 14-05-2015, Website of The Economist: http://www.eleconomista.es/CanalPDA/2013/42591/el-aplastante-dominio-de-android-en-cinco-graficos/

[2] William Stallings. (2011). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE FIFTH EDITION. United States of America: Prentice Hall.

[3] Erika Aguillón Martínez. (2012). Servicios de Seguridad de OSI. 14-04-2015, de UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO Sitio web: http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/11-concepto-de-criptografia.

[4] B. Kaliski. (2000). PKCS #5: Password-Based Cryptography Specification Version 2.0. RSA Laboratories: Network Working Group.

[5] H. Maiorano. (2009). Criptografía: técnicas de desarrollo para profesionales. Buenos Aires: Alfaomega.

AUTHOR PROFILE:

Carlos Cortés Bazán, Computer Systems Engineer from Tecnologico de Estudios Superiores del Oriente Mexico State in 2006 with honors. From 2006-2009 he worked in the development of various relevant software projects for the National Polytechnic Institute. He is an academic member of the International Network for Engineering Education since 2011. In 2013 he receives the Master degree in Engineering and Safety Information Technology. He is currently a full-time research professor in the Department of Computer Engineering in ESIME Culhuacan I.P.N. His research interests include the development of systems, databases, computer forensics, cryptography and analysis of algorithms.

Dolores Zamorano Saavedra. She is a methodological research and hasmaster's degree in Educational Sciences. Now a days it is a research professor at the School of Mechanical and Electrical Engineering (ESIME) in Mexico. Her areas of development are assessment and project development, scientific writing and methodology of science

Celedonio Enrique Aguilar Meza wasborn in Mexico on march 3, 1959andholds a degree in communications and electronicsfrom theNationalPolytechnic Institute IPN, is currentlyre search professoranddevelopment areas are the processing and handling, coding and compression, safety and efficient transmission.