User-Level Security for Image Transferring in Mobile Devices

A.N.J.A De Silva[1], T. Arudchelvam[2]

[1] *Department of Computing and Information Systems, Wayamba University of Sri Lanka*
[2]*Department of Computing and Information Systems, Wayamba University of Sri Lanka*
[1] Corresponding author <silva142134@wyb.ac.lk >

Abstract— *At present mobile phone is an essential thing in our day to day life. People use mobile phones to send messages, to take photos and share them, etc. Now smart phones are highly used for several purposes such as taking photo, sending photo as message, sending voice message, etc. there are several mobile applications which are providing facilities for image sharing/transferring. Most of these applications provide end to end encryption/decryption. Some images contain very sensitive information. Therefore, security is very important in image transferring. This paper presents a method to maintain user-level security in image transferring. In mobile applications, different kinds of encryption methods are used to implement user-level security. But in this application, text-based image encryption is proposed. RGBA values and ASCII values of the text are used. Also, the Random seed matrix is used to improve encryption and the seed number will be depending on the text we used to encrypt. We used bitwise operators in this work. By using this application users can transfer images safely and decide encryption method and key themselves.*

Keywords— ASCII, bitwise operators, encryption, RGBA color space, user-level security

I. INTRODUCTION

Nowadays mobile phones are a very essential thing for our day to day life. Mobile phones are used to send text messages, photo messages, voice messages, etc... Most importantly most of the manufacturers now considering better camera facility for their devices. Some people used to capture their important documents as images rather than travel with those documents. Some people capture their important life events and they want to share them safely. Therefore, it is necessary to securely save and transfer images because they can contain very sensitive information. Most of the mobile applications don't let the user to decide their security level of the images. When we implemented the user-level security method, the user can maintain their security on their images. User level security in text messages is reported in (Arudchelvam, 2016). There, a user can select the encryption method and the key for the encryption. The notable point in (Arudchelvam, 2016) is that time to time user can select suitable encryption method and the key. This gives an extra security to those messages. Further, some sensitive message can be encrypted and saved in the mobile phones rather than storing the bare message itself.

II. IMAGE ENCRYPTION

Image encryption methods work on altering an image into another image that is unable to recognize by an intruder. In order to keep an image secured, that image can be encrypted and stored. It is important that no one is able to recognize the image without using a decryption key (Alsafasfeh, 2011), (Patidar, 2009) when user-level security is properly maintained. Lots of image encryption methods have been suggested to fulfil this need, but some of them were proven insecure or not adequate (Shujun.Li, 2002). That's why continuous development of further methods of image encryption is needed. Further, it should be noted that user should be able to choose the encryption method and the key as they wish. Then, as it is not a common method, an intruder cannot guess the encryption method and the key for it.

A. Encryption and Decryption of Images Using Chaotic Mapping

In, (Ahmad, 2010), the new image encryption algorithm based on three chaotic maps is explained. In the proposed algorithm, the plain-image is first decomposed into 8x8 size blocks and then the block-based shuffling of the image is carried out using 2D Cat map (Ahmad, 2010),. Furthermore, the control parameters of shuffling are randomly produced using a 2D coupled Logistic map to enforce the secrecy of the image. Next, the shuffled image is encrypted using a chaotic sequence created by one-dimensional Logistic map. The simulation and experimental results show that the proposed algorithm can encrypt and decrypt the images successfully using same secret keys, and the algorithm had good encryption effect, large key space and high sensitivity to small change in secret keys. But this algorithm is based on the concept of shuffling the positions of the pixels and changing the gray values of the image pixels. So we can't predict the outcome for color images. Since we are talking about mobile devices, these calculations and operations can take considerable time. Ismail Amr Ismail (Ismail, 2010), proposed a new chaotic image cipher in which they applied an external secret key with 104 -bits size and two

chaotic logistic maps. They produced control parameters from the external secret key for both chaotic logistic maps. In order to make the system more secure; they used a feedback mechanism in their image cipher.

B. Encryption-Decryption RGB Color Image Using Matrix Multiplication

A method of image encryption-decryption technique has been suggested in (Al-Laham, 2015) which uses matrix multiplication and inverse matrices. According to the results of our experiments, the proposed method rapidly increases the image transmission security and improves the encryption-decryption process by eliminating the mean square error and increasing the speed of the encryption-decryption process. This method propose because of the disadvantages of the work carried out in the (Ahmad Sharadqa, 2015) such as,

1. The red and green components obtained in direct conversion phase must be saved because they are applied to create the color image in the inverse conversion state.
2. The saved components in the previous disadvantage need an extra memory space.
3. The saved components in 1 need extra time for data transmission.
4. The red and green components obtained in direct conversion state must be sent and they are not secure.

C. Encryption-Decryption RGB Color Image Using Matrix Multiplication

By, Khalaf, Abdulrahman (Khalaf, 2016) proposed a method to color image encryption and decryption algorithm and implemented depends on fast image key. Image key can be produced from the same image or any image must be the same size of the original color image. The sender and receiver must share the same image key which has the same characteristics of the hash function, therefore, the unauthorized people cannot discover the plain image from key notably, even if a one-pixel value is changed, the key they generated will be different. The results show the suggested algorithm gives a good result.

D. Encryption-Decryption RGB Color Image Using Matrix Multiplication

Madhu, Shrija & Ali Hussain, Mohammed (Madhu, 2014) has proposed two simple methods for encrypting an image which is less complicated than RSA and DES algorithms and has given good results on being implemented in MATLAB. In both the methods, encryption is done using a key image. The method uses XOR operation for encryption while in the second method bit plane concept and shuffling is done along with XOR operation. Both the techniques were applied on separate images and the results obtained were commendable. The level of encryption will be depending upon the choice of the key image.

One of the major drawbacks in (Khalaf, 2016), (Madhu, 2014) is users have to share an image. It requires lots of space and takes time. Next drawback is the selected image must be the same size as the original image. To overcome these drawbacks we are proposing text base image encryption/decryption method.

III. IMPLEMENTATION

The first phase is an encryption part which contains the following sequence of steps:

1. Get the pixel values of the original image to a matrix.
2. Get the secret key and applying it to a matrix same size as the original image.

Ex-

If original image is 3x3, then secret key matrix should be 3x3

Secret key="test"

$$T=\begin{matrix} t & e & s \\ t & t & e \\ s & t & t \end{matrix}$$

3. Generate Pseudo Random Number matrix same size as the original image size within range [0,255].

Ex-

$$Rn=\begin{matrix} 145 & 120 & 70 \\ 243 & 10 & 21 \\ 123 & 165 & 98 \end{matrix}$$

Seed number is generated using placement values of secret key

```
for(int cnt=1;cnt<=value.length();cnt++){

    seedno= seedno +(cnt*(int)value.charAt(cnt-1));

}
```

(int)value.charAt(cnt-1)➔ ASCII value of the character

4. Separate the pixel values in to red, green, blue and alpha matrices.

Ex-

$$R=\begin{matrix} 123 & 244 & 55 \\ 10 & 173 & 210 \\ 36 & 67 & 138 \end{matrix} \quad G=\begin{matrix} 88 & 145 & 26 \\ 42 & 125 & 172 \\ 45 & 188 & 102 \end{matrix}$$

$$B=\begin{matrix} 78 & 149 & 120 \\ 49 & 6 & 218 \\ 109 & 195 & 159 \end{matrix} \quad A=\begin{matrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{matrix}$$

5. Convert the matrix T in to ASCII value array.

Ex-

$$T = \begin{matrix} t & e & s \\ t & t & e \\ s & t & t \end{matrix} \rightarrow T = \begin{matrix} 116 & 101 & 115 \\ 116 & 116 & 101 \\ 115 & 116 & 116 \end{matrix}$$

6. Perform XOR operation , save the answer to a matrix

Ex-

Re(0,0)=R(0,0)^T(0,0)^Rn(0,0)
Ge(0,0)=G(0,0)^T(0,0)^Rn(0,0)
Be(0,0)=B(0,0)^T(0,0)^Rn(0,0)
Ae(0,0)=A(0,0)^T(0,0)^Rn(0,0)

.

.

.

.

Re(3,3)=R(3,3)^T(3,3)^Rn(3,3)
Ge(3,3)=G(3,3)^T(3,3)^Rn(3,3)
Be(3,3)=B(3,3)^T(3,3)^Rn(3,3)
Ae(3,3)=A(3,3)^T(3,3)^Rn(3,3)

7. Create a pixel array using encrypted red, green, blue and alpha values.
8. Resultant image is encrypted image.

The second phase is decryption part which follows the above steps again.

IV. RESULTS

A sample picture is encrypted with secret key “test” as an example. Then it is decrypted with same secret key. The original picture is given in Fig. 1; encrypted image in given in Fig. 2; Decrypted image is given in Fig. 3.

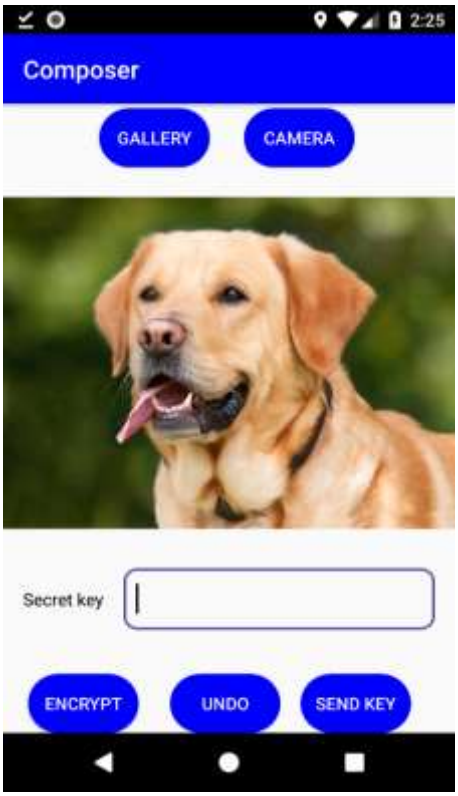

Figure 1. Original Image

Figure 2. Encrypted Image

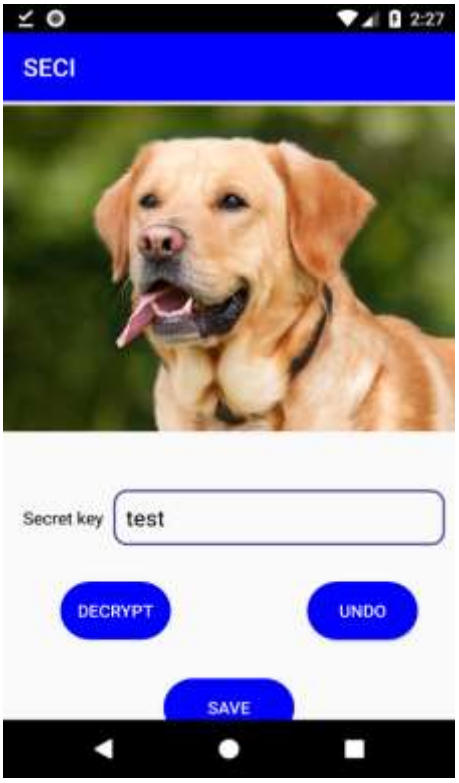

Figure 3. Decrypted Image

The time taken for the proposed method is also a crucial aspect for a good image encryption/decryption. Time taken by the proposed method to encrypt/decrypt various different resolution images has been measured.

Table 1. Encryption / Decryption rates

Image Size	Encryption Time (ms)	Decryption Time (ms)
272*170	51	61
400*250	61	122
800*500	235	264
912*513	267	585
1920*1080	1159	2933
1800*1350	1372	2954
3984*1538	3475	7078

Encryption/Decryption time can be varying depending on the device performance and condition. When the device have good memory and processing speed, calculation time will reduce. Large size images produce large matrix, so it will take time to do the calculations if the device have low processing speed. The above encryption/decryption is done in Google pixel 1 device.(4 GB ram, Quad-core (2x2.15 GHz Kryo & 2x1.6 GHz Kryo) CPU)

V. CONCLUSION

In this work, an Android application is developed for implementing image encryption. The users are able to choose the desired secret key. The sender and the receiver should exchange the secret key separately. If the secret key is longer than image, additional characters will be neglect. As it is user-level security, this is essential. For the high-resolution images, encryption and decryption time is high. Therefore, inside the application, we are providing camera application that can control the resolution. This application is useful for exchanging images and storing private documents as images and also a user may keep the secured information in an image and store only the encrypted image in the device. Though the phone or the mobile device is lost, those data which are stored using these methods, cannot be handled by unauthorized people. Hence, the proposed technique is very reliable and accurate.

ACKNOWLEDGEMENT

Authors thank the Wayamba University of Sri Lanka for the support given for this work.

REFERENCES

Ahmad, Musheer. & Shamsher Alam, M., 2010, *"A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping"*, International Journal on Computer Science and Engineering. 2.

Al-Laham, Mohammad., 2015, "*Encryption-Decryption RGB Color Image Using Matrix Multiplication*", International Journal of Computer Science and Information Technology. 7. 109-119. 10.5121/ijcsit.2015.7508.

Alsafasfeh,Q., and Alshabatat, A., 2011, "*Image Encryption Based on Synchronized Communication Chaotic Circuit*" Journal of Applied Sciences Research, Vol. 7, No. 4.

Arudchelvam,T., and Fernando, W. W. E. N., 2016, "*User Level Security in Short Message Service*", Int. Journal of Information and Communication Engineering, Vol:10, No:6.

Ismail, I., Amin M., and Diab H., 2010, *"A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps"*, International Journal of Network Security, Vol.11, No.1, PP.1–10, July 2010.

Khalaf, Abdulrahman., 2016, "*Fast Image Encryption based on Random Image Key*", 10.13140/RG.2.1.3107.4327.

Madhu, Shrija., & Ali Hussain, Mohammed, 2014, "*Securing Medical Images by Image Encryption using Key Image*", International Journal of Computer Applications. 104. 30-34. 10.5120/18184-9079.

Mitra A, Subba Rao A & V, Mahadeva Prasanna Y & R, S. (2006). A new image encryption approach using combinational permutation techniques. 1.

Patidar, V., Pareek, N. K., and Sud, K. K., 2009 , *"A New Substitution-Diffusion Based Image Encrypete Using Chaotic Standard and Logistic Maps"*, Communications in Non-Linear Science and Numerical Simulation, Vol. 14, No. 7.

Sharadqh ,Ahmad., 2015 "*RGB Color Image Encryption-Decryption Using Gray Image*", IJCSI International Journal of Computer Science Issues, Volume 12, Issue 3, ISSN (Print): 16940814 | ISSN (Online): 1694-0784 www.IJCSI.org 137

Shujun.Li., and Zheng, X., 2002, "*Cryptanalysis of a chaotic image encryption technique*", Inst. of Image Process, Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. IEEE International Symposium on Publication Date: 2002, Vol. 2.