Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

ISBN: 978-981-07-6260-5

Implementation of Hybrid Algorithm for Secured Multimedia Messaging Service System Using Android

[Geetanjali R. Kshirsagar and Savita Kulkarni]

***Abstract* – Design and Implementation of Steganography along with secured message services in Mobile Phones is used to provide security to the data that flows across the mobiles. In this paper encryption and steganography algorithms are implemented using JAVA™ with android platform to provide the security for real time multimedia messaging service system. Establishing hidden communication for mobile has become an important subject of security. One of the methods to provide security is steganography. Steganography is used to hide secret information inside some carrier. Hiding information, especially in images has been an alternative solution for secret communication. To improve the security, encrypted secret data will be hidden inside MMS. The image is made to be hidden into image from MMS which provides more secured transmission than text information embedded into the MMS. The Least Significant Bit (LSB) embedding technique is used to hide the secret information (image). Different sizes of secret images are considered and later the calculations have been done for the MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) of image in MATLAB. Encryption and steganography algorithms are ported on HTC Desire mobile device with android version 2.2.3.**

***Keywords* – Android Platform, Encryption, LSB, MMS, MSE, PSNR, Security, Steganography.**

I. INTRODUCTION

After rapid growth of the Internet, establishing hidden communication is an important subject of security that has gained increasing importance. Telecommunication companies started to add additional features to their mobile phones such as MMS (Multimedia Messaging Service) in order to attract more customers. And users can securely communicate its secrets by means of sending and receiving MMS messages. One of the most popular uses of mobile phones has been the exchange of messages between users. The Short Messaging System (SMS) was introduced with GSM mobile phones and it very rapidly became popular among users. The Multimedia Messaging System (MMS) offers the ability to send and receive multimedia content using a mobile phone. Now a day, most of the mobile phones not only are capable of sending and receiving Multimedia Messages (MM), but also contain an embedded camera and can run customized applications (e.g. using Java 2 Platform Micro Edition, J2ME). MMS is a technology that allows a user of a properly enabled mobile phone to create, send, receive and store messages that include text, images, audio and video clips. One of the main and relatively new hidden communication methods is steganography. In steganography the data are hidden in a cover media so that other persons will not notice that such data is there. This is a major distinction of steganography method with the other methods of hidden exchange of information such as cryptography and can be mainly applied to media such as images, text, video clips, music and sounds. The combination of both may give the best results, as a message can be encrypted before it is hidden into another object. Steganography concerns itself with ways of embedding a secret message into a cover object. The encryption, transforming message (here used image) into cipher text (encoded form) and decryption, a reverse process, plays an important role in concealing the confidentiality of the message. The message is first encrypted with a key during an encryption process and then hiding it in available format (here used image). Thus sending an encrypted message increases the security level of the message. Once received, the message needs to be decrypted using same key which implies the concept of symmetric key steganography where the key is symmetric for both sender and receiver. In this approach data is first encoded, hidden in cover medium and is send to the intended recipient as a result the security of data is enhanced [3].

There is not such application have been developed for mobile phone to hide the data. In this paper mms technologies are used for sending message and data hiding technique for jpeg images is used as well as text hiding technique is used for steganography. Moreover, there are some constraints for the size of media text cannot exceed 30kB; an image must be below 100kB [2].

II. PROBLEM DEFINITION

The aim of the project is to hide the data as an image over an image from MMS using least significant steganographic algorithm and before hide, an image performs encryption on it. Send the stego file to the destination where the retrieving of the secret image is done on mobile device with Android.

A. Problem Solution

The proposed method should provide better security while transferring the data or message(s) from one end to the other end. The main objective of this project is to hide encrypted secret image into an image from MMS which acts as carrier file having secret data and to transmit to the destination securely without any modification. If any distortions occur in the image or on its resolution while inserting the secret message into the image, there may be a chance for an unauthorized person to modify the data. So, the data (image) encryption at sender and decryption at receiver and steganography plays an important role in this project.

B. Proposed System Architecture

The data hiding patterns using the steganographic technique in this project can be explained using this simple block diagram shown in Fig. 1 and 2.

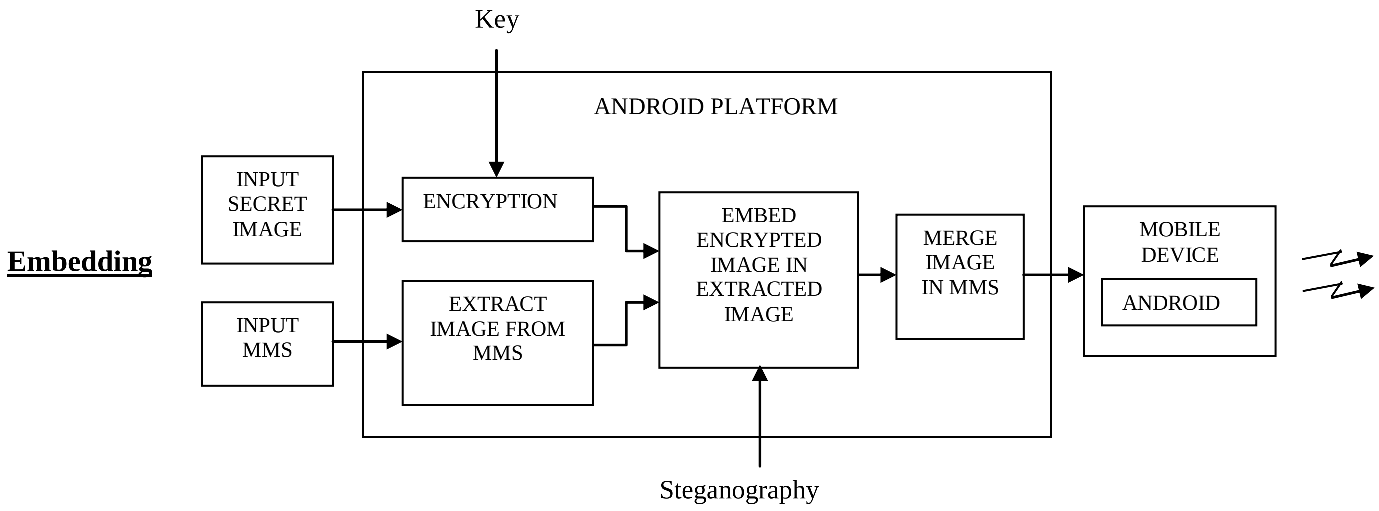


Figure 1: Block Diagram of Embedding Process in Binary Image

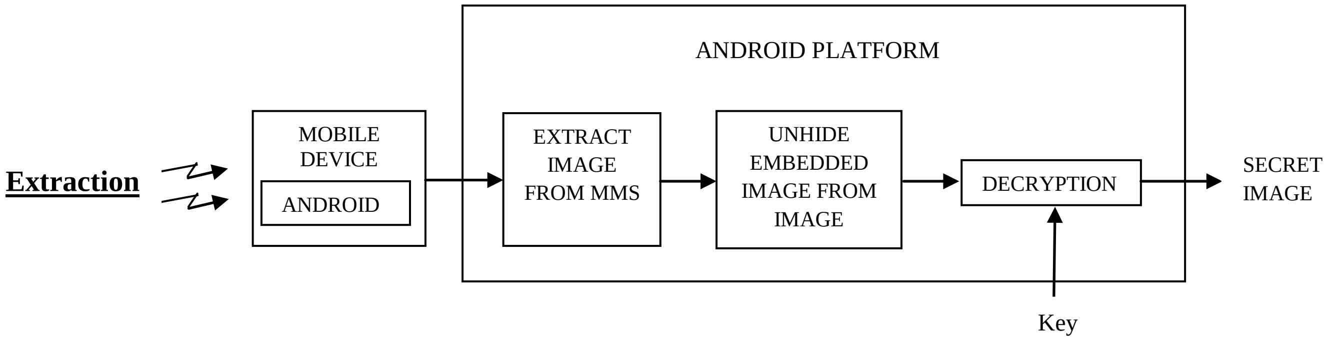


Figure 2: Block Diagram of Extracting Process from Binary Image

III. IMAGE STEGANOGRAPHY ALGORITHM

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colours of each component like RGB (red, green and blue) are changed [5]. LSB is effective in using BMP images since the compression in BMP is lossless. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a large image which is used as a cover. For JPEG, the direct substitution of stenographic techniques is not possible since it will use lossy compression. So it uses LSB substitution for embedding the data into images [1].

Each of these pixels in an image is made up of a string of bits. The 4-least significant bits of 24-bit true color image holds 4-bit of desired secret message (image) by simply overwriting the data. By experimental, we note that: The impact of changing the 4-least significant bits will be minimal and indiscernible to the human eye [4].

A. 4-LSB Embedding Algorithm

1. Start
2. Read Multimedia Message from MicroSD card of an Android mobile device.
3. Extract an image from Multimedia Message
   Cover image = Extracted image
4. Convert the cover image into stream of binary bit.
5. Make 4 LSB of each byte zero.
6. Read a Secret image from Android mobile's MicroSD card.
7. Encrypt Secret image using key, PRNG and encryption algorithm with Android platform.
8. Convert Encrypted Secret image into stream of binary bit.
9. Read the lower nibble of Encrypted Secret image byte.
10. Hide lower nibble of Encrypted Secret image byte into the lower nibble of blue channel pixel byte of Cover image.
11. Read the upper nibble of Encrypted Secret image byte.
12. Hide upper nibble of Encrypted Secret image byte into next blue channel byte of the Cover image.
13. Go to step 9 till to hide complete encrypted secret image
14. Merge an image with hidden encrypted image (stego image) into MMS.
15. Send MMS.

As given in algorithm secret image byte is divided into two nibble. Hide each nibble into the blue channel byte of cover image.

The minimum size of Cover image = 10* Size of Secret image + n (where n is size of cover image header)

n pixels are added because secret data is not be added in the header of cover image; therefore start setting secret data after the header of cover image. We just presented the used algorithm to hide a JPEG image file in a BMP image. In the next section, we present the extracting algorithm [7].

B. 4-LSB Extracting Algorithm

Extracting the secret image data is performed by reversing the process used to insert the secret message in the cover image. The following steps describe the details of extraction process.

1. Read Multimedia message.
2. Extract the image from Multimedia message i.e. stego image
3. Read lower nibble from first pixel of blue channel from stego image which is the lower nibble of secret image.
4. Read lower nibble from second pixel of blue channel from stego image which is the upper nibble of the secret image.
5. Now this is the byte of secret image.
6. Repeat the step 3 and step 4 to read all byte of secret image.
7. Decrypt secret image using same key.
8. Display retrieved secret image.

For measuring the quality of reconstructed image as compared to the original image, the metric needs to be define. There are three common error metrics used for estimating noise on images: MSE, PSNR, and SSIM.

IV. IMPLEMENTATION

The cover images and secret images to send/transfer are stored in the MicroSD card of Android mobile device with android version 2.2.3. Cover image along with text message is Multimedia Message. Access both the images (cover and

Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6260-5

secret) from sdcard using android and follow the steps below on android platform to perform steganography.

A. The first part is encryption / decryption process which is implemented in JAVA™ on android platform and the output of encryption is saved in a file which will be needed at a time of hiding the content in an image from MMS.

B. In the next phase, the encrypted file and cover image is taken as an input file. The file is hiding in the image and this implementation is done in JAVA™ with android platform.

C. At the receiver side, follow exactly opposite steps. First unhide the encrypted image and then decrypt it.

D. The last phase is MSE and PSNR calculation and analysis which is implemented in MATLAB version 11. The function code is written in Editor Window for PSNR calculation which is executed and the PSNR for the two images – original secret image at sender and retrieved secret image at receiver.

V. RESULT

Evaluation parameters are used Peak Signal to noise ratio (PSNR), Mean Square Error (MSE) as performance parameters to measure the quality of image.

Signal-to-noise ratio can be defined in a different manner in image processing where the numerator is the square of the peak value of the signal and the denominator equals the noise variance. Two of the error metrics used to compare the various image de-noising techniques is the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR).

Mean Square Error (MSE):

Mean Square Error is the measurement of average of the square of errors and is the cumulative squared error between the stego and the original image. The error indicates the distortion in an image. MSE can be calculated by using 2-D mathematically equation described as follows:

$$\mathrm{MSE} = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - \bar{X}_{ij})^2. \qquad (1)$$

where, Xij = The value of pixel in cover image
Xij = The value of pixel in stego image
N = Size of image

Peak Signal to Noise Ratio (PSNR):

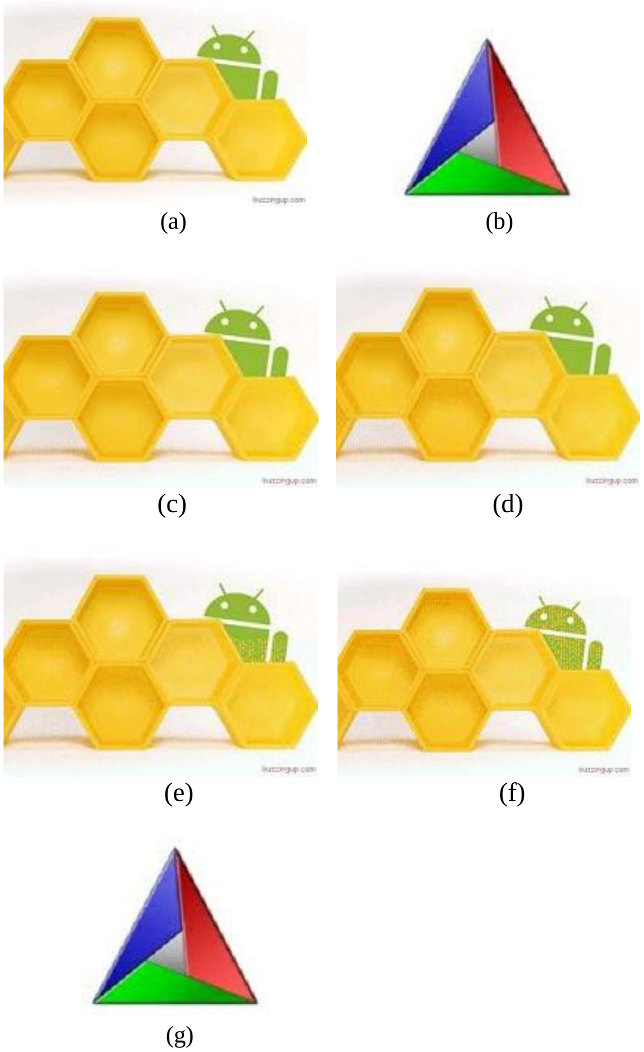
PSNR is a measure of the peak error. Peak Signal to Noise Ratio is the ratio of the square of the peak value the signal could have to the noise variance as shown in (2).

$$\mathrm{PSNR} = 10 \text{ X } \log \frac{255^2}{\mathrm{MSE}} \ \mathrm{dB} \qquad (2)$$

A higher value of PSNR is good because of the superiority of the signal to that of the noise. MSE and PSNR values of an image are between original image and stego image. Fig. 4 and 6 shows the comparison of MSE and PSNR calculated for given example 1 and 2.

The proposed algorithms are implemented to hide a secret image into cover image. Results of developed algorithms for encryption and steganography are shown in Table I and Table II.

EXAMPLE 1:



(a) (b)

(c) (d)

(e) (f)

(g)

Figure 3: (a) Cover Image (b) Secret Image (c) Stego Image (Secret Image Size = 75 X 75) (d) Stego Image (Secret Image Size = 150 X 150) (e) Stego Image (Secret Image Size = 200 X 200) (f) Stego Image (Secret Image Size = 250 X250) (g) Retrieved Secret Image

TABLE I. PSNR CALCULATION OF VARIOUS SIZES OF SECRET IMAGE: EXAMPLE 1(Android Logo)

Cover Image Size	Secret Image Size	MSE	PSNR
200 X 142	100 X 100	3.3104	42.9320
200 X 142	150 X 150	5.1030	41.0526
200 X 142	200 X 200	6.2098	40.2001
200 X 142	250 X 250	8.2693	38.9561

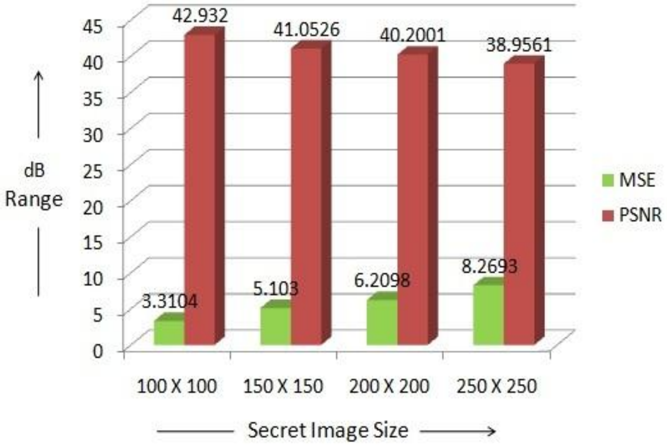
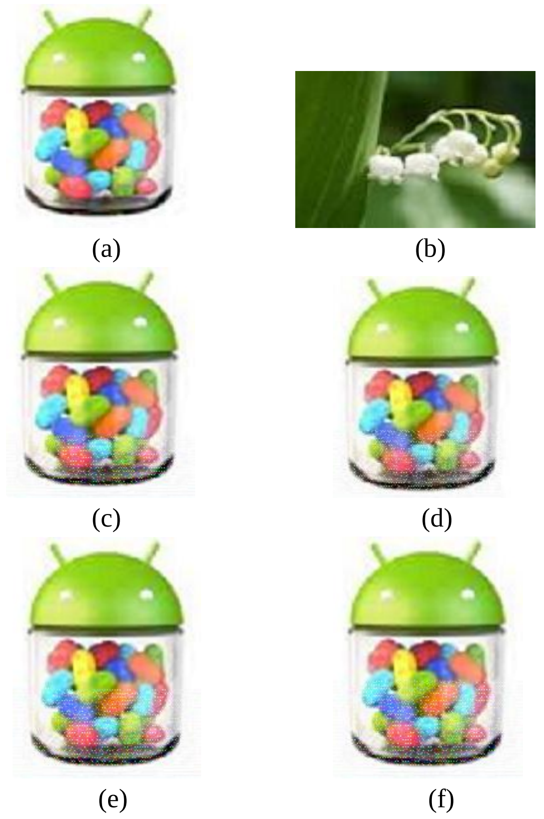
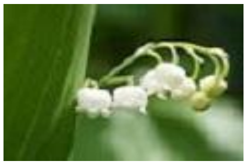


Figure 4: MSE and PSNR Comparison

EXAMPLE 2:





(g)

Figure 5: (a) Cover Image (b) Secret Image (c) Stego Image (Secret Image Size = 100 X 75) (d) Stego Image (Secret Image Size = 140 X 105) (e) Stego Image (Secret Image Size = 150 X 112) (f) Stego Image (Secret Image Size = 160 X120) (g) Retrieved Secret Image

Table II: PSNR CALCULATION OF VARIOUS SIZES OF SECRET IMAGES: EXAMPLE 2(Jellybean)

Cover Image Size	Secret Image Size	MSE	PSNR
150 X 203	100 X 75	3.7269	42.4173
150 X 203	140 X 105	4.0179	42.0908
150 X 203	150 X 112	4.5364	41.5636
150 X 203	160 X 120	4.9885	41.1511

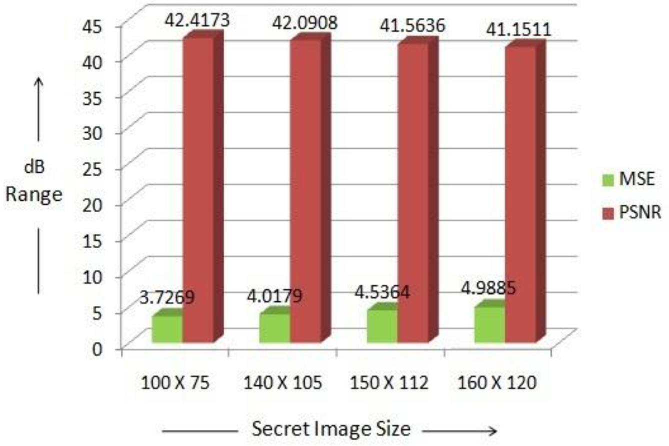


Figure 6: MSE and PSNR Comparison

VI. CONCLUSION

4-LSB substitution is successfully implemented to hide secret image into an image from MMS which provides the security during transmission of MMS. Algorithm is developed on android platform and tested by porting same on actual android mobile device HTC Desire with android version 2.2.3. PSNR changes as varying size of secret image. From the results it is observed that noise in stego image increases as size of secret image increases and PSNR should be greater than 38dB to transfer image successfully. In this way encryption and steganography security algorithms are successfully implemented using Android platform with high potential of security.

ACKNOWLEDGMENT

Authors would like to thank Electronics and Telecommunication Department and the faculty of Maharashtra Institute of Technology, Pune, for their co-operation and the help in completion of this project. Also, I thank all my friends and family members for their appraisal and criticism, which helped me to make my project success.

REFERENCES

[1] Mr. Vikas Tyagi " Data Hiding in Image using least significant bit with cryptography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012

[2] Rosziati Ibrahim, Law Chia Kee "MoBiSiS: An Android-based Application for Sending Stego Image through MMS" ICCGI 2012 : The Seventh International Multi-Conference on Computing in the Global Information Technology June 24-29, 2012 - Venice, Italy

[3] S.Mohanapriya "Design and Implementation of Steganography Along with Secured Message Services in Mobile Phones" International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 5, May 2012

[4] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav "Steganography Using Least Signicant Bit Algorithm" Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, pp. 338-341

[5] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy " Implementation of LSB Steganography and its Evaluation for Various File Formats" Int. J. Advanced Networking and Applications Volume: 02, Issue: 05, Pages: 868-872 (2011)

[6] B.V.Rama Devi, P.Prapoorna Roja, D.Lalitha Bhaskari and P.S.Avadhani , "A New Encryption Method for Secure Transmission of Images" International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 2801-2804

[7] B.N.Jagadale, R.K.Bedi,Sharmishtha Desai," Securing MMS with High Performance Elliptic Curve Cryptography" International Journal of Computer Applications (0975 – 8887)Volume 8– No.7, October 2010

[8] http://www.developers.android.com

[9] http://www.intechopen.com

[10] http://www.mathworks.com

AUTHORS

Geetanjali R. Kshirsagar - B.E. (Electronics and Telecommunica - tion),M.E. (Electronics - Digital System) (Appeared) Maharashtra Institute of Technology, Pune.

Savita Kulkarni – B.E. (Electronics), M.E. (Computer Engineering),Associate Professor, Department of Electronics and Telecommunication, Maharashtra Institute of Technology, Pune.