TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 3, ISSUE 3
ISSN: 2054 - 7420

Android Application Development for Secure Data Transmission using Steganography

[1]Vineet Jeswani, [2]Savita Kulkarni and [3]Manisha Ingle
Department of Electronics and Telecommunication, Maharashtra Institute of Technology, Pune, India
[1]vineetjeswani26@gmail.com; [2]savita.kulkarni@mitpune.edu.in; [3]manisha.ingle@mitpune.edu

ABSTRACT

Real time implementation of Steganographic algorithm along with encryption is used to achieve secure data flow across Android mobiles. In this paper, pixel value differencing (PVD) technique one of the steganographic algorithm with AES encryption are implemented using JAVATM on android platform to achieve high level security for real time multimedia messaging service (MMS) system. One of the important concerns in any communication system is the security of the data transmission from eavesdropper. To overcome this security problem, the most effective technique is the steganography. Steganography is used to hide secret information onside some carrier. Image is taken as a carrier file to hide secret information (text, image, audio). To add more security, encryption is also done on the secret file which will be hidden inside MMS. The Pixel Value Differencing (PVD) technique is used to hide secret information (text, image, audio). Different sizes of secret images are considered keeping the fixed size of cover image and the calculations have been done for MSE and PSNR of image in MATLAB. Later, the results of the PVD are compared with the LSB technique. Encryption and Steganographic algorithms are ported on Sony Xperia M mobile device with Android version 4.3.

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

1 Introduction

The basic purpose of mobile is communication. Over the last few decades mobile phones have evolved very rapidly. Earlier, mobiles where used to communicate via voice call only. Later, came the era of the GSM mobile phones in which communication was possible through short messaging service (SMS) which used the text format to communicate and it became very popular among users. With more evolution, communication became possible through multimedia messaging service (MMS) in which communication became possible via text, audio, image and video. MMS is a technology that allows a user of an enabled mobile phone to create, send, receive and store messages that include text, images, audio and video clips properly. Today is the era of smart phones where various operating systems are available such as Android, Windows, Blackberry, IOs and many more with various features. With this ever growing technology, security has become an important subject and has gained increasing importance. The security with Android is least as compared with other OS currently available in the market. Moreover, android is an open source and free platform where a developer can create its own application and share it on play store with users. Users can explore the play store and can get the required applications very easily and most of the applications are freely available. Adding to many advantages of Android, more than 80% of the smart phone users prefer Android over others. Due to all this reasons, we have selected Android to achieve MMS security. To achieve the security various techniques are available such as encryption, cryptography, steganography. The best suitable and the

DOI: 10.14738/tnc.33.1292
Publication Date: 27th June 2015
URL: http://dx.doi.org/10.14738/tnc.33.1292

most secured technique is the steganography. Steganography is the art of hiding the secret data over the cover medium. There are many advantages of steganography over other techniques. Even in the steganography techniques, there are various algorithms such as Least Significant bit (LSB) algorithm, Pixel value differencing scheme (PVD) algorithm and many more. The LSB-based technique, directly embed the secret data into the spatial domain in an unreasonable way without taking into consideration the difference in hiding capacity between edge and smooth areas. In general, the alteration tolerance of an edge area is higher than that of a smooth area, this meaning that, an edge area can conceal more secret data than a smooth area. While human perception is less sensitive to subtle changes in edge areas of a pixel, it is more sensitive to change in the smooth areas. While in case of the PVD technique, the correlation between neighboring pixels to determine whether a pixel is located in an edge area or a smooth area, the PVD method does not utilize the smooth area to hide large amount of secret data, the capacity is still low. In order to achieve higher capacity, a combination of PVD and LSB can be used. These techniques are based on the idea of using PVD when the difference between a pair of pixels is large (edge area), and using LSB method when the difference is small (smooth area). To add further more security, along with these steganographic techniques, encryption is also done on the secret file in which a hiding data will be encrypted with a secret key which will be available to both sender and receiver so that it can be used while retrieving the secret data at the receiver's end.

2 Problem Definition

The aim of the project is to hide the data as an image or text over an image from MMS using pixel value differencing steganographic algorithm and before hiding, an image performs encryption on it. Send the stego file to the destination where the retrieving of the hidden data is done on mobile device with Android.

2.1 Problem Solution

Hiding an image over an image has already been achieved using 4-LSB steganography algorithm. But the drawback with this technique is that the cover image should be of .bmp format and the secret image should be of .jpg format. Moreover the efficiency of this technique is low.

To overcome these drawbacks, PVD algorithm is used. 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 increase the data hiding capacity and the data transfer efficiency as compared to that of the 4-LSB algorithm hide encrypted secret image into an image from MMS which acts as base 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, text) encryption at sender and decryption at receiver and steganography plays an important role in this project.

2.2 System Architecture

The data hiding patterns using the PVD stegano-graphic technique in this project can be explained using this simple block diagram which is similar to that used in the previous work where Steganography was achieved using 4-LSB algorithm. The block diagram is kept same because only the steganography is changed i.e. from 4-LSB to PVD as shown in figure 1 and 2. [1]

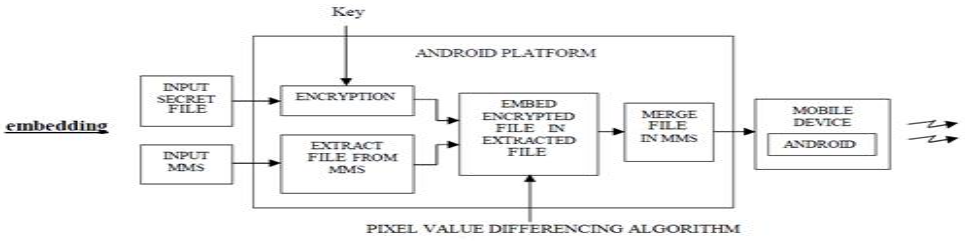


Figure 1 Embedding at Transmitter

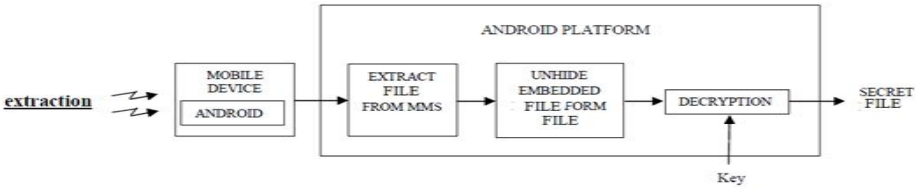


Figure 2 Extraction at Receiver

3 Steganography

In steganography the data are hidden in a cover media so that other persons will not notice that such data is there.

Or Steganography is a technology of hiding messages inside some harmless carriers to shelter the communication so that the outsiders may not discover the existence of information in the carrier. Steganography is mainly applied to media such as images, text, video clips, music and sound.

The different types of steganography techniques that are available are:

1. Pure steganography
2. Secret key steganography
3. Public key steganography

3.1 Pure Steganography

Pure Steganography is the process of embedding the data into the object without using any private keys as shown in Figure. This type of Steganography entirely depends upon the secrecy. This type of Steganography uses a cover image in which data is to be embedded, personal information to be transmitted, and encryption decryption algorithms to embed the message into image. These types of steganography can't provide the better security because it is easy for extracting the message if the unauthorized person knows the embedding method. It has one advantage that it reduces the difficulty in key sharing.

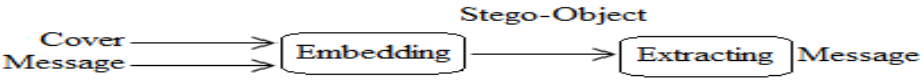


Figure 3 Pure Steganography

3.2 Secret key Steganography

Secret key Steganography is another process of Steganography which uses the same procedure other than using secure keys shown in Figure. It uses the individual key for embedding the data into the object that is similar to symmetric key. For decryption it uses the same key which is used for encryption. This type of Steganography provides better security compared to pure Steganography. The main problem of using this type of steganographic system is sharing the secret key. If the attacker knows the key it will be easier to decrypt and access original information.

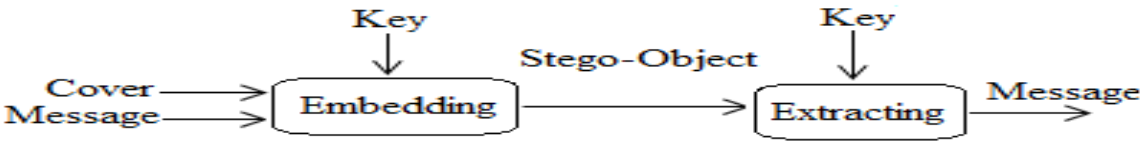


Figure 4 Secret key Steganography

3.3 Public key Steganography

Public key Steganography uses two types of keys shown in Figure. One for encryption and another for decryption. The key used for encryption is a private key and for decryption, it is a 'public key' and is stored in a public database.

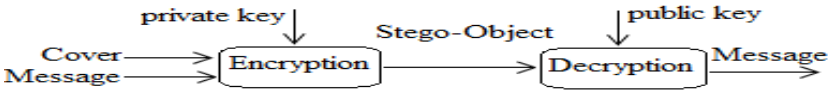


Figure 5 Public key Steganography

4 Image Steganography

Images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For this different image file formats, different steganographic algorithms exist.

4.1 Lsb technique

The most basic and important image Stegano-graphic Technique is Least Significant Bit embedding tech-nique. In this technique, data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. In this technique, least significant bit of each pixel is replaced with secret message bit until message end. When using a 24-bit image one can store 3 bit in each pixel by changing a bit of each if the red, green and blue color components. An 800 x 600 pixel image can store 1,4400,00 bits or 180,000 bytes of embedded data. For example a 24 bit can be as follows:

(10110101 01101100 10101101)
(10110110 11001101 00111110)
(10110101 01100011 10001110)

The number 150 which binary representation is 10010110 is embedded into the least significant bits of this part of the image, the resulting grid as follows:

(10110101 01101100 10101100)
(10110111 11001100 00111111)

(10110101 01100010 10001110)

Although the number is embedded into the first 8 bytes of the grid, only the 3 underlined bits need to be changed according to the embedded message. On an average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. There are 256 possible intensities of each primary color, so, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye, thus the message is successfully hidden. If the message is hidden even in the second to least significant as well as in least significant bit then too no difference is seen in the image. In LSB Technique, consecutive bytes of the image data from the first byte to the end of the message are used to embed the information. But this approach is very easy to detect. A more secure system can be in which the sender and receiver share a secret key that specifies only certain pixels to be changed. Even if the intruder suspects that LSB steganography has been used, there is no way of knowing which pixels to target without the secret key. In its simplest form, LSB makes use of BMP images, since they use lossless compression. To hide a secret message inside a BMP file, one would require a very large cover image. For this reason, LSB method has also been developed for use with other image file formats. This type of information hiding algorithm could be a major risk because eavesdropper can apply sequential scanning based technique to recover the secret message [1-5].

4.2 Pixel Value Differencing Scheme

Wu & Tsai discuss Pixel Value Differencing (PVD) scheme. This technique takes advantage of the characteristics of human visual system. In this technique, the original cover image is divided into non overlapping blocks of two pixels. A range table with a number of contiguous ranges is fabricated. The width of each range in the table is in power of 2. Now, difference is calculated between two consecutive pixels of a block. The block with large difference value is considered in edge area and with small difference value is considered in smooth area where the small or large values are taken depending upon some pre-specified threshold value. The human eyes are more sensitive to noise in smooth area than in the edge area. This method embeds more bits in edge areas in contrast to smooth areas. This technique doesn't have sufficient embedding capacity. Another technique discussed by Wu, Tsai and Hwang that also exploits the characteristics of the human visual system. In this method, the image is also divided into non-overlapping blocks of two consecutive pixels and then the difference value is calculated for each block in similar way as in. On the basis of the difference value, each block is identified either as a part of smooth region or edge region. This method embeds the secret data bits into the smooth regions by simple LSB substitution method and for edge area the Wu & Tsai's scheme is used. Thus, it increases the data hiding capacity to a great extent without disturbing the image quality much. The methods discussed in identify the horizontal edges only [6-7].

Table 1. Range Table

Range (R)	Lower Bound (LB)	Upper Bound (UB)
R1	0	15
R2	16	31
R3	32	63
R4	64	127
R5	128	255

5 Implementation

The cover images and secret images to send/transfer are stored in the MicroSD card of Android mobile device with android version 4.3 whereas text has to be directly given as a secret file which we want to hide and send. Cover image along with text message is Multimedia Message.

5.1 Embedding Algorithm

1. Start
2. Pick base image as a carrier file from Micro SDcard of Android mobile device.
3. Pick the data to be hidden either text or image or audio.
4. If the data to hide is in text format input it manually.
5. If the data to hide is image search in Micro SDcard.
6. Encrypt the hiding data with AES encryption algorithm.
7. Perform Steganography using Pixel Value Differencing (PVD) algorithm.
8. PVD differentiates smooth area and the edge area and accordingly hides more data in the edge area.
9. Generate an MMS using this Stego image.
10. Send it over Android platform.

The secret file is hidden in the blue channel of the base 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.

5.2 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
3. image.
4. Separate out the data of the hidden file from the base
5. image by performing stegnalysis.
6. Once the data is completely separated perform decryption on the secret file with the same key used for encryption.
7. Display the hidden file (text or image or audio) from Micro SDcard.

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.

6 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).

6.1 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:

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

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

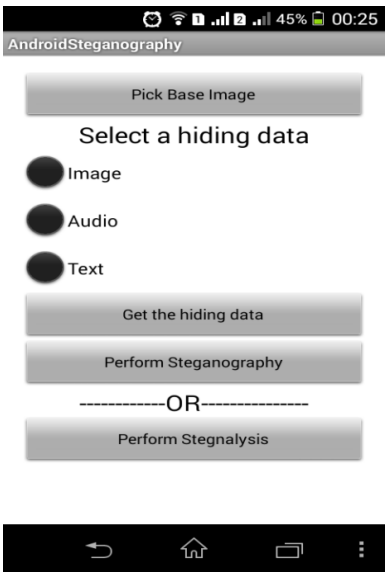
6.2 Peak Signal to Noise Ratio (PSNR):

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).

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

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.

6.3 Graphical User Interface (GUI):



Example 1: Hiding image within an image

Base Image

Secret Image

Table 2. Comparison of MSE for Various Sizes of Secret Image: Example 1(Jelly Bean)

Base Image Size	Secret Image Size	MSE using 4-LSB	MSE using PVD
150X203	100X75	3.7269	2.5025
150X203	140X105	4.1079	3.7599
150X203	150X112	4.5364	3.9336
150X203	160X120	4.9885	4.2094

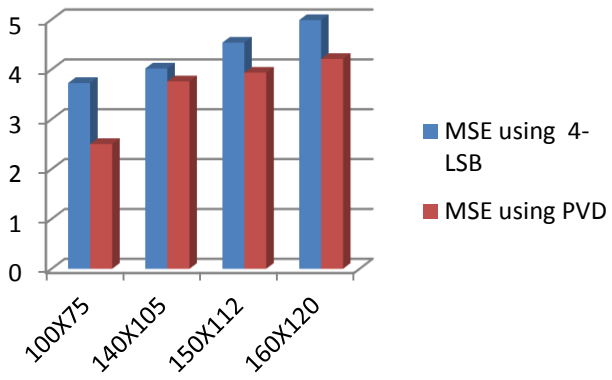
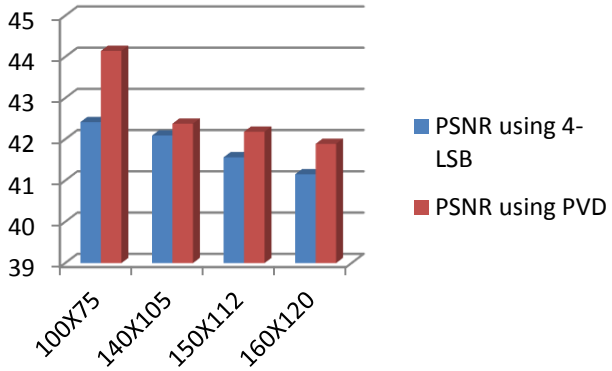


Table 3. Comparison of PSNR for Various Sizes of Secret Image: Example 1(Jelly Bean)

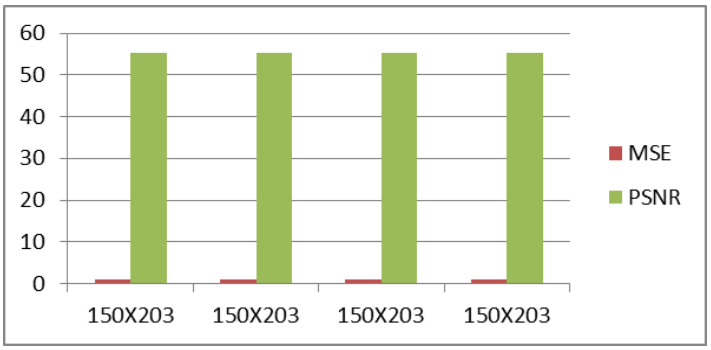
Base Image Size	Secret Image Size	PSNR using 4-LSB	PSNR using PVD
150X203	100X75	42.4173	44.147
150X203	140X105	42.0908	42.3791
150X203	150X112	41.5636	42.1829
150X203	160X120	41.1511	41.8886



Example 2: Hiding text within an image

Table 3. Calculation of MSE And PSNR For Hiding Text

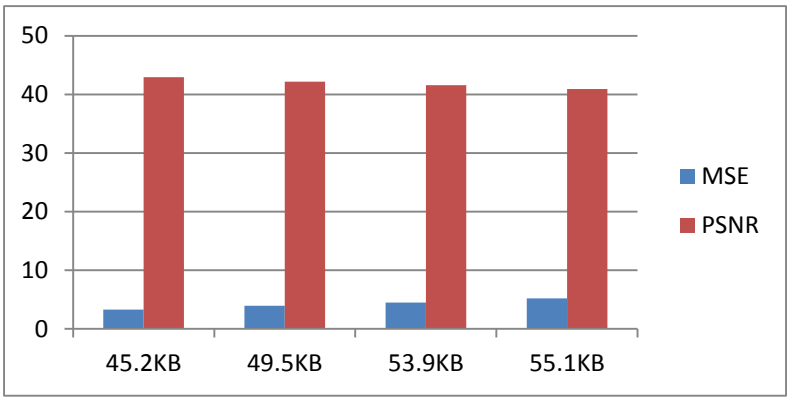
Base Image Size	No of text characters	MSE	PSNR
150X203	20	1.0019	55.3901
150X203	30	1.002	55.3844
150X203	40	1.0023	55.3809
150X203	50	1.0025	55.3744



Example 3: Hiding audio within an image

Table 3. Calculation Of MSE And PSNR For Hiding Audio

Base Image Size	Audio Size	MSE	PSNR
150X203	45.2KB	3.3084	42.9346
150X203	49.5KB	3.9411	42.1746
150X203	53.9KB	4.5217	41.5777
150X203	55.1KB	5.2304	40.9545



7 Conclusion

PVD steganographic algorithm is successfully implemented to hide secret data (image, text) into an image from MMS which provides the security during transmission of MMS. Comparison between PVD and LSB algorithm is done by calculating MSE and PSNR of the Stego images. And the results of PVD are more effective as compared to that of LSB. Moreover, hiding text and audio is also achieved in this project which was not done using LSB algorithm. Algorithm is developed on android platform and testing is done on the actual android mobile device Sony Xperia M with android version 4.3. In this way, AES encryptions along with PVD Steganography algorithm 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] Geetanjali R. Kshirsagar, Savita Kulkarni “Implementation of Hybrid Algorithm for Secured Multimedia Messaging Service System Using Android” Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

[2] 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

[3] 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

[4] 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

[5] Mukesh Garg, A.P. Gurudev Jangra "An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques" International Journal of Advanced Research in Computer Science and Software Engineering. Volume 4, Issue 1, January 2014

[6] Wu D. C and Tsai W. H. (2003), "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613-1626.

[7] Wu H.C., et al. (2005), "Image Steganographic scheme based on pixel-value differencing and LSB replacement methods", VISP(152). [8]Marghny H. Mohamed, Naziha M. Al-Aidroos and Mohamed A. Bamatraf "Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference" International Journal in Foundations of Computer Science & Technology (IJFCST), Vol. 2, No.6, November 2012.