

# A New Android Based Steganography Application for Smartphone's

Jibi G Thanikkal<sup>1</sup>, Mohammad Danish<sup>2</sup>, Saoud Sarwar<sup>3</sup>

<sup>1, 2, 3</sup>Department of Computer Science & Engineering, Al-Falah University, Dhauj, Faridabad

---

**Abstract:** Recent development in communication technology has led to wider use of smart phones like android, iPhones etc. Smart phones are widely utilized with many applications like social networking, enterprise and a fast way of sharing files like photos, videos etc also happens. People share their information in Social networks, groups, forums etc. The main design goals of these types of data exchange are the authentication and copy right protection. Many a times, crackers are in news for revealing the personal data/files. Hence it was important to secure the data from being stolen or illegally altered or to keep secrecy while transferring/sharing.

The secrecy of data can be achieved through cryptography and steganography. Sender can hide some data in cover medium and at the receiver side, the same can be completely extracted. In this fast moving world the main design issues on the mobile phone applications are the performance of the algorithm. The present study proposes a novel method for the secure transfer of data in smartphones. This proposed scheme deals with a high performance reversible data hiding algorithm utilizing simple XOR operation in the spatial domain. In this method the data is hiding in a cover file like image, video or audio etc. which will provide high security to the data content along with the high bandwidth.

**Keywords:** XOR algorithm, Secret data, Smart phones, Steganography.

## 1. INTRODUCTION

Smart phones became an important part of the people living in this century. It has the functionality similar to computers and hence become all-in-one portable devices providing interconnectivity and device-to-device communication. The improvement in capabilities will be further happened with the addition of 4G technologies and will cause the popularity of smart phones to continually rise.

Smartphones are made by every major phone manufacturer viz. Apple, Samsung, LG, HTC, Nokia, Sony Ericsson, Motorola, RIM, Palm and others. Android, Apple iOS and Windows operating system are used in these kinds of modern phones. Google Android is the most popular operating system on mobile phones, and there are hundreds of phone models from dozens of manufacturers that use it.

Android is an open source and Linux-based operating system for mobile devices such as smartphones and tablet computers[1]. Android was developed by the Open Handset Alliance, led by Google, and other companies. Android offers a unified approach to application development for mobile devices which means developers need only develop for Android, and their applications should be able to run on different devices powered by Android. Android applications are usually developed in the Java language using the Android Software Development Kit. Once developed, Android applications can be packaged easily and sold out either through a store such as Google Play or the Amazon Appstore.

Unfortunately, today's smartphone users are in a situation strikingly similar to that faced by computer users few decade ago. Security resources for smartphones are very limited and not fully developed[2]. As a result, most smartphones lack the level of security you find on your computer. Meanwhile, the complexity of smartphones continues to grow along with the number and types of network-borne threats. This makes smartphones both an easy target for crackers and malware and a more inviting one than well-protected desktop systems.

The secrecy of data can be achieved through cryptography and steganography. Using steganography the sensitive data can be masked in any cover media. Steganography together with cryptography is found to provide high security in data transfer [3, 4]. Data hiding is an embedding method that conceals messages into digital media to convey the message secretly [5]. Data hiding methods can be classified into non-reversible [6-7] and reversible [8-9]. Non-reversible methods generally provide higher payload and better image quality than those of reversible methods, and therefore, have many applications, such as image authentication [11] and tamper detection [12].

Smart phones are becoming popular for sharing data these days due to their popularity and ease of availability. Sharing secret data through smart phones may require a secured way of communication. This can be achieved by use of steganography. The data can be embedded using a steganographic algorithm at sender's end. When the data travels through the communication channel, there is very less

probability that the attacker can guess that there is hidden information present in the data. After reaching the receiver's end, the hidden message can be retrieved by applying the extraction algorithm.

In this paper, we propose an innovative high performance reversible data hiding method that can embed high capacity of message bits and recover image after data extraction. This new method is based on XOR algorithm. It can embed more data than many of the existing reversible data hiding algorithms. With the reversibility nature of XOR operation the original message data was restored. Location map was used in this scheme to store the location information of all selected cover image pixels.

This XOR Reversible Data hiding algorithm works on Android smart phones. The application is designed on eclipse using Java Programming language. The Reversibility nature of XOR operation is utilized here for achieving security in Spatial Domain. The first part of the algorithm use to embed the secret data in to the cover image and the second part extracts the secret data from the given embedded image.

## 2. PROPOSED SCHEME AND ALGORITHM

XOR is a logical operation, pronounced *Exclusive OR*. It yields true if exactly one (but not both) of two conditions is true. For multiple arguments, XOR is defined to be true if an odd number of its arguments are true, and false otherwise. The proposed method can be explained in a simpler manner. Let, P (pixel) and M (message) are two binary numbers, then XOR (P, M) is the exclusive-or operation of the two binary numbers, i.e., if P=1 and M=1, then L (location map) = XOR (P, M) = 0. In this method, we utilize the reversibility nature of XOR operation. Let us apply this peculiarity in the above analysis, i.e. if L= XOR (P, M) = 0, then M=XOR (P, L) =1 and P=XOR (L, M) =1. This property of XOR is utilized in the proposed scheme. If we apply this in experimental set up, inserting one bit message M into least significant bit (LSB) of pixel P, location map L is marked as 1 if the LSB of P and M are different, otherwise L is marked as 0.

The above operation will provide the result of the location map, and based on XOR, result on LSB of P and M, decision for the embedding at LSB of image pixel will be taken. If the location map is 0, it indicate that the LSB bit of P and M are same and the pixel remains without getting edited, else otherwise. Image name, secret message, result image name are the inputs to the embedding algorithm.

The following example explains it in simpler manner.

### Embedding Process:

Pixel = 170 =10101010

Bit =1

Location Map = XOR (LSB of P, B) =1

Embedded Pixel =set LSB of P as B=171=10101011

### Extraction Process:

Pixel = 171 =10101011

Location Map =1

So Bit = LSB of P= 1

Extracted Pixel =XOR(LSB of P, Bit)=170=10101010

### The Embedding Algorithm

- Read the cover image and text message which is to be hidden in the cover image( $P_i$ )
- Convert text message to binary ( $B_i$ )
- Calculate the Location Map  $L_i$  as XOR (LSB of  $P_i$ ,  $B_i$ )
- Replace LSB of the cover image with each bit of secret message one by one.
- Create Embedded Image

### The Extraction Algorithm

- Read the Embedded image.
- Retrieve  $B_i$  bits as the LSB of Embedded image
- Convert each 8 bit into character.
- Calculate the LSB of Extracted image as XOR (LSB of  $P_i$ ,  $B_i$ )
- Create Extracted Image

In the present study, all the experiments are performed in actual bit stream. At the sender side, gray scale image is converted to 8 bit pixel array. Location map array is generated to store the location information of editable position of pixel values. In the receiver side, to retrieve message data, LSB of image pixels are extracted. And to retrieve the original image back, the XOR operation is performed between each of the LSB of image pixels with location map bit.

The application is designed in Android 4.4.2 (Kitkat) using Java programming language. Both the embedding and extraction part of the application will read the image from Android Gallery and save back to android sdcard memory. The message data is provided through soft keyboard via user interface. The extracted secret data will display in the text view provided in user interface.

## 3. RESULT AND DISCUSSION

In this application four 8-bit gray images are used to verify the strength and payload of the algorithm. The pure payload and location map length are used to calculate amount of payload after improvement. Peak Signal to Noise Ratios (PSNR) are calculated to verify the efficiency of the proposed scheme. The PSNR measure the difference between cover image and

embedded image. PSNR is calculated as per the following equation (1).

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \dots\dots\dots (1)$$

Table provides the embedded pay load size and the PSNR of embedded image. The present study using XOR algorithm attained a PSNR of 49 dB. Tian [8] could achieve PSNR of 44 dB. Guiet *al.* [13] achieved average PSNR of 40.53 dB. Tian [8] used difference expansion algorithm and the redundancy in the digital content to achieve reversibility. Whereas, Guiet *al.* [13] used generalization predictions-error expansion and adaptive embedding strategy and attained high capacity RDH with limited distortion. The trade-off between PSNR and payload for the proposed method using various images in the spatial domain is drawn in Fig. 1. Figure 1 indicates that the average PSNR is about 46.5 dB under a payload of 36000. On the other hand, the average of 48.5 PSNR is achieved at payload 18000.

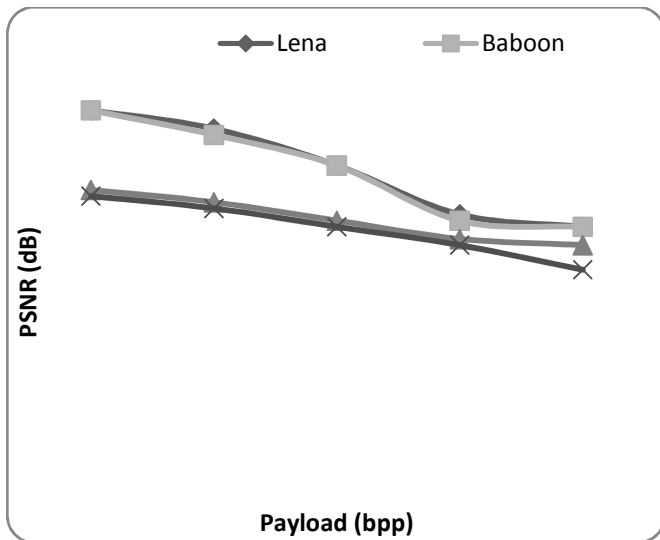






Fig. 1. The PSNR and payload performance generated by the proposed method in the spatial domain

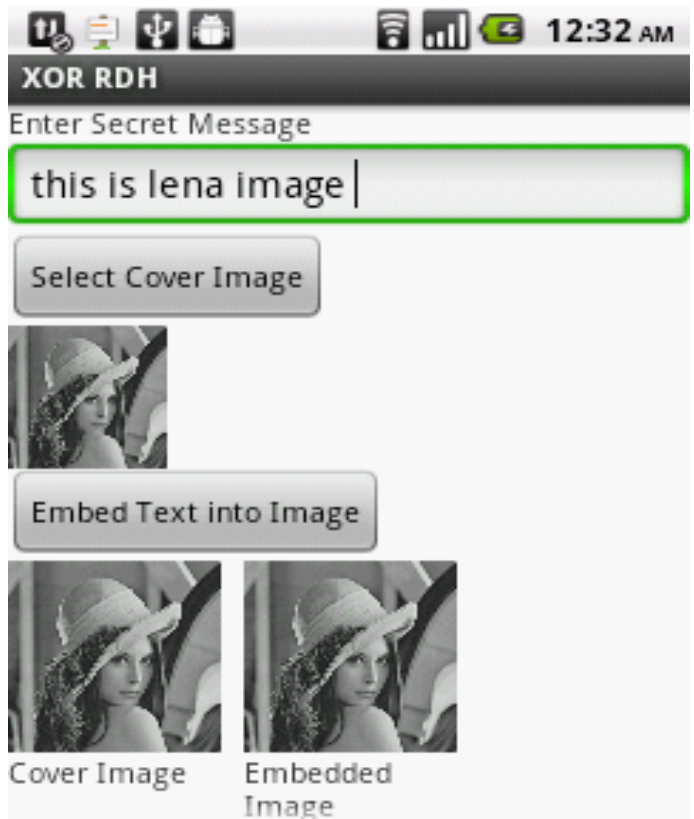
Our algorithm can embed 1/8 bit of the cover image (width x height). Multilayer embedding is also possible by extending the algorithm. The proposed system employ location map similar to the message bits array, and this schemes is also simpler compared to the other reversible data hiding algorithms in spatial domain [8, 14]. The working application in the android smartphone is given in Fig 2.

Very recently few studies have come out with LSB algorithm for securing data transfer in smart phones [15]. The least significant bits of the cover image digital data are used to conceal the message. Bucerzan et al. [16] developed a SmartSteg application that works on Android platform and the

same could hide and fast encrypt files using digital images of MB dimension as cover. In this method also LSB steganography is combined with a random function and symmetric key cryptography to transfer digital information. Whereas the present study could achieve a higher performance using the XOR algorithm.

Table 3. Embedded payload size vs PSNR of embedded image.

Image and Size		PSNR at Payloads				
		36000	18000	10000	5000	1000
	Lena (512x512)	49	51	59	65	68
	Baboon (512x512)	49	50	59	64	68
	Camera man (256x256)	46	47	50	53	55
	Suzie (240x351)	42	46	49	52	54



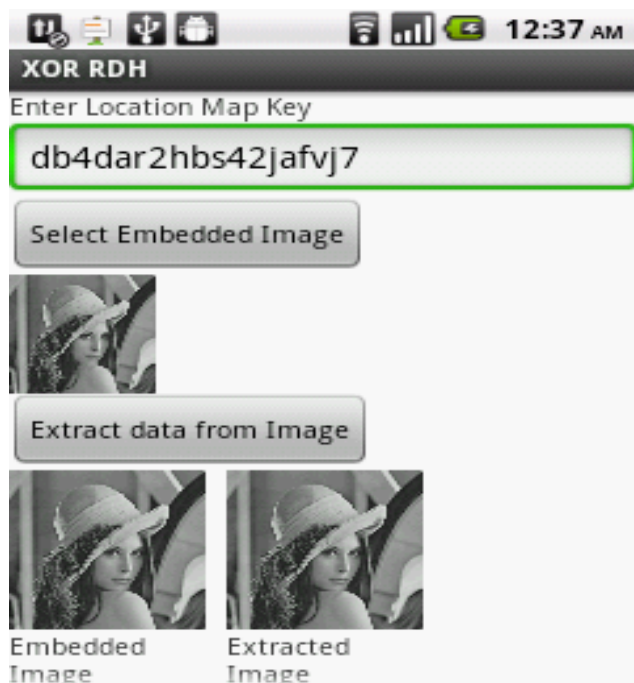


Fig. 2. The working model in Android domain

#### 4. CONCLUSION

The present study attempted to explore novel algorithms which could allow data transfer in high technology mobile phones with utmost security. The basic idea behind the proposed work was to delineate the applicability of XOR algorithm and its reverse nature in Android platform. The secrecy of data here is achieved through XOR reversible steganography. The data hidden by sender in an image is completely extracted at the receiver end. This method can be applied in all types of Android platform irrespective of any versions of Android Operating System. This method can also be used to hide the data in image, video or audio etc. which will provide high security to the data content along with the high bandwidth.

#### 5. ACKNOWLEDGEMENT

The first author would like to thank the Head of the Department and other faculties of Department of Computer Science and Engineering and authorities of Al-Falah University for providing necessary facilities to complete the research work.

#### REFERENCES

- [1] <http://tutorialspoint.com/android>
- [2] Jeon, W., J. Kim, Y. Lee, and D. Won, 2011. A Practical Analysis of Smartphone Security, In M.J. Smith, G. Salvendy (Eds.): Human Interface, Springer-Verlag Berlin Heidelberg, 311-320.
- [3] Stallings, W., 2003. Cryptography and Network Security-principles and practices. Pearson Education, Inc.
- [4] Singh, A., S.Malik, 2013. Securing Data by Using Cryptography with Steganography. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5): 404-409.
- [5] Provos, N., P.Honeyman, 2003. Hide and seek: an introduction to steganography. IEEE Security and Privacy, 1(3): 32-44.
- [6] Mielikainen, J., 2006. LSB matching revisited. IEEE Signal Process. Lett. 13(5): 285-287.
- [7] Zhang, X., S.Wang, 2006. Efficient steganographic embedding by exploiting modification direction. IEEE Communications Letters, 10(11): 781-783.
- [8] Tian, J., 2003. Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology, 13(8): 890-896.
- [9] Yanga, C. Y., W.C.Hua, C.H.Linb, 2010. Reversible Data Hiding by Coefficient-bias Algorithm. Journal of Information Hiding and Multimedia. Signal Processing, 1(2):91-100.
- [10] Zhang, X., Z.Qian, G. Feng, Y. Ren, 2014. Efficient reversible data hiding in encrypted images. Journal of Visual Communication and Image Representation, 25(2): 322-328.
- [11] Chen, Y.S., R.Z.Wang, 2011. Reversible authentication and cross-recovery of images using  $(t, n)$ -threshold and modified-RCM watermarking. Optics Communications, 284(12):2711-2719.
- [12] Hsu, S.F., Tu, 2010. Probability-based tampering detection scheme for digital images. Optical Communications, 283(9): 1737-1743.
- [13] Gui, X., X.Li, B.Yang, 2014. A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding. Signal Processing, 98: 370-380.
- [14] Yang, C.Y., W.C.Hu, 2010. Reversible Data Hiding in the Spatial and Frequency Domains. International Journal of Image Processing, 3(6): 373-382.
- [15] Desai, S., Amreliwala, S, and V. Kumar, 2014. Enhancing Security in Mobile Communication using a Unique Approach in Steganography. International Journal of Computer Science and Mobile Computing, 3(4): 433-439.
- [16] Bucerzan, D., Ratiu, C. and M.J. Manolescu, 2013. SmartSteg: A New Android Based Steganography Application. International Journal of Computers, Communication and Control, 8(5):681-688.