**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 3, Issue. 4, April 2014, pg.433 – 439***

**RESEARCH ARTICLE**

# Enhancing Security in Mobile Communication using a Unique Approach in Steganography

**Prof. Sharmishta Desai**
Dept. of Computer Engineering, MIT College of Engineering, Pune, India
desai.sharmishta@gmail.com

**Sanaa Amreliwala**
Dept. of Computer Engineering, MIT College of Engineering, Pune, India
sanaa.amreliwala@gmail.com

**Vineet Kumar**
Dept. of Computer Engineering, MIT College of Engineering, Pune, India
vineet.z91@gmail.com

## Abstract

***Mobile phones are the most commonly used devices in today's scenario. The need for secured communication has become more imperative. Steganography is the most reliable technique for communicating critical information through publicly available communication channels. There are various techniques available for transfer of critical data such as cryptography and steganography. A proposed model of communicating hidden data through public portals has been discussed in this paper, where in text steganography and Image steganography are used.***

## 1. Introduction

Steganography is a kind of data hiding technique that provides way of security protection for digital image data. [1] Unlike utilizing a particular cipher algorithm to protect secret data from illicit access, the purpose of steganography is to embed secret data in preselected meaningful data or information, called camouflage data, without creating visually perceptible changes to keep an attacker unaware of the existence of the secret. Steganography can be done on image, text, audio, video, etc.

In recent years, the fast growth of internet has made digital media very popular. Digital media have many advantages in communication field but it also has increased the digital duplication, tampering and hacking. So, information security is an inseparable part of data communication.

 

In this paper we discuss the approach we have used for implementation of LSB algorithm, for encoding and decoding the secret information by means of double layer data privacy, one being the steganographic algorithm and other being password enabled encoding and decoding. A unique way of data hiding is implemented by dividing the plain text and hiding it in image cover file as well as text cover file.

## 2. Literature Survey

### 2.1 Information privacy

Information privacy is the privacy of personal information and usually relates to personal data stored on computer systems. The need to maintain information privacy is applicable to collected personal information, such as medical records, financial data, criminal records, political records, business related information or website data.

Information privacy is considered an important aspect of information sharing. With the advancement of the digital age, personal information vulnerabilities have increased.

Information privacy may be applied in numerous ways, including encryption, authentication and data masking - each attempting to ensure that information is available only to those with authorized access. These protective measures are geared towards preventing data mining and the unauthorized use of personal information, which are illegal in many parts of the world.

### 2.2 Steganography

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means "covered writing." It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures covert channels, and spread spectrum communications. [1]

It is the art and science of hiding communication [3]. Steganography involves hiding information so it appears that no information is hidden at all. It attempts to prevent an unintended recipient from suspecting that the data is there. [4] The goal of steganography is to avoid drawing suspicion to the transmission of the secret message. On other hand, steganalysis is a way of detecting possible secret communication using against steganography. That is, steganalysis attempts to defeat steganography techniques. It relies on the fact that hiding information in digital media alters the carriers and introduces unusual signatures or some form of degradation that could be exploited. Thus, it is crucial that a steganography system to ascertain that the hidden messages are not detectable. [5]

### 2.3 Secret text within image sharing

A secret text is first processed and is then hidden in 1 or more user-selected cover images. It is suggested to select these cover images to contain well-known contents, like famous character images, well-known scene pictures, etc., to increase the steganographic effect for the security protection purpose. [6]

In this method we hide information in the least significant bits (LSB) of pixels colors. In this method each byte of information is hidden in two pixels. For hiding the information a byte is divided into eight bits. By using a password, two pixels are selected in which a byte of information is hidden. [2]

### 2.4 Secret text within text sharing:

A secret text is first processed and is then hidden in 1 or more user-selected cover images. It is suggested to select these cover images to contain well-known contents, like famous character images, well-known scene pictures, etc., to increase the steganographic effect for the security protection purpose. [6]

Generally sharing secret text using text steganography is not preferred as it has limitations like capability of holding lesser amount of data without making it evident that there is some hidden message present.

### 2.5 Smartphones for sharing secret data:

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 encoded 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 decoding algorithm.

## 3. Research Methodology

### LSB Technique and Algorithm

The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colours will be indistinguishable from the original by a human being, just by looking at it. By using the least significant bits of the pixels' colour data to store the hidden message, the image itself is seemed unaltered. [7]

In LSB steganography, the least significant bits of the cover image digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a grayscale value. Suppose the first eight pixels of the original image have the following grayscale values. [6]

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

To hide the letter A whose binary value is 01000001, we would replace the LSBs of these pixels to have the following new grayscale values:

11010010
01001011
10010110
10001100
00010100
01010110
00100110
01000011

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego-image will be hardly noticeable to the human eye. However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats are difficult to detect contrary to 8 bit format.

Another technique which is used for LSB steganography is LSB grid technique.

**Algorithm**

**Embedding the message: -**

1: Read the cover image and text message which is to be hidden in the cover image.
2: Convert text message to binary.
3: Calculate LSB of each pixel of the cover image.
4: Replace LSB of the cover image with each bit of secret message one by one.
5: Write stego-image

 

**Retrieving the message: -**

1: Read the stego-image.
2: Calculate LSB of each pixels of stego-image.
3: Retrieve bits
4: convert each 8 bit into character.

## 4. Implementation Details of Proposed Method

### 4.1. Image Steganography

In this type of steganography, Text Data is hidden inside Cover Image by using the well-known LSB method.

#### Encoding Method

1: Represent the pixels of the image in an array form pixel by pixel.
2: Read the message to be hidden.
3: Convert it into byte form.
4: Read the message bit by bit from the character bytes (Each character byte has 8 bit representation).
5: Put indicator characters into the LSB bits of the initial pixels of the image array using bitwise operators (This is to indicate that the image contains embedded message).
6: Put message bits into the LSB bits of the colour representations of each pixel in image array using bitwise operators.
7: Iterate till entire message is encoded into the Image.
8: Create an image pixel by pixel by using this new image array which has been modified to contain secret message (by using image bitmap and file operations).
9: Finally store this image at a particular destination with appropriate extension.

#### Decoding Method

1: Represent the pixels of the image in an array form pixel by pixel.
2: First check if the initial pixels of the image contain characters which indicate that there is some message hidden inside the image.
3: If no, then give error.
4: If yes, that is, if there are indicator characters (characters that indicate image contains embedded message), then start decoding process.
5: Consider first pixel after indicator characters.
6: Extract the LSB of the pixel in image array and store in a binary variable (byte form).
7: Iterate this process till we extract all the set of characters.
8: Convert final byte form message into string form and make it human readable and present it to the user as hidden message.

### 4.2. Image + Text Steganography

When user selects this option, his/her message is hidden in two different parts. One part inside an Image, and other inside a cover set of Text.

Comparing Image and Text Steganography, Text steganography has a large number of drawbacks.
Two main drawbacks are:
a) Capacity
b) Security concerns.

Text can store very limited set of characters and Image can store a large number of characters without problem.

#### Encoding Algorithm

Before main encoding process, the entire message is divided into two parts. One part is hidden in Cover Image and other is hidden inside Cover Text.

 

We use the ratio 1:5
That is, for every 5 bits to be encoded using image steganography, 1 bit is encoded using text steganography.

1: The characters which are supposed to be embedded inside a text are put in a string.
2: The string is read one by one, character by character and compared with set of alphabets and also its case is checked (upper or lower).
3: The appropriate word is selected according to the given character and put in a sentence to generate a cover text sentence.
4: Example, if two characters read from String "abcde" are "a" and "b"
A sentence is constructed having initial string "I like to eat" and concatenated with character substitutions "a" and "b" in their word form.
That is generated cover text would be "I like to eat apple, banana."
5: This process is iterated till all cover characters are read and the final cover text is generated.
6: This sentence is given to user as cover text.
7: The rest of the characters are given as input to Image Steganography and normal Image Steganography is done.

### Decoding Algorithm

Before main decoding starts, a large number of checks are performed to check whether user has entered correct image, correct set of text, and also the entered text is in appropriate order or not.
1: The given set of sentence is separated to generate words, and from the given words the first character is extracted and concatenated to a string which is initially "".
2: This process continues till all characters are in the string.
3: Now decoding process of the Image is done to retrieve the characters embedded inside the image.
4: This set of characters is stored inside another string.
5: After all embedded characters are extracted using Image Steganography decoding process, the final image string and text string are concatenated together to form final user message.
6: This final user message is then displayed to the user as hidden message.
7: However note that, if one of the check returns false, entire process is stopped, and decoding is aborted.

## 5. Comparison

Here, we compare the time required for encoding the message "hi HOW ARE YOU? 1213" with different sizes of cover images.

### 5.1. Device: Android Emulator AVD

Specifications:
1] Operating System: Android 4.4.2 (API 19)
2] RAM: 512MB
3] Resolution of Display: 720x1280

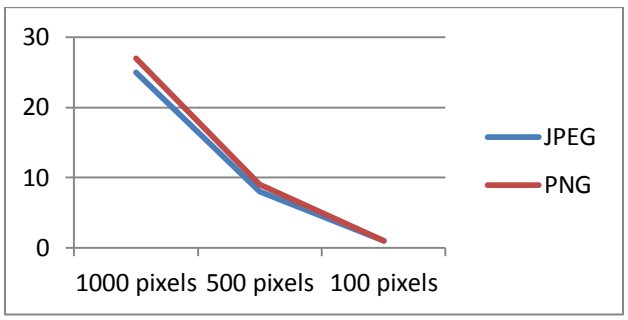


Chart 1: Comparison for time in seconds taken by Android Emulator AVD for different resolution images.

 

### 5.2. Device: BlackBerry Z10

Specifications:
1] Operating System: BlackBerry 10 OS 10.2.1
2] RAM: 2GB
3] PROCESSOR SPEED: 1.5GHz
4] Resolution of Display: 768x1280

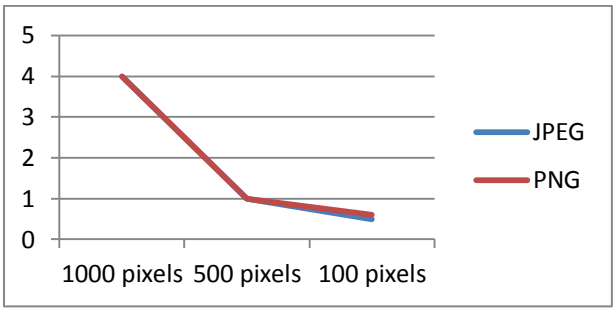


Chart 2: Comparison for time in seconds taken by blackberry Z10 for different resolution images.

### 5.3. Device: Sony Ericsson ARC S

Specifications:
1] Operating System: Android 4.0.4 (Cyanogen Mod ICS)
2] RAM: 512MB
3] PROCESSOR SPEED: 1.4GHz
4] Resolution of Display: 480x854

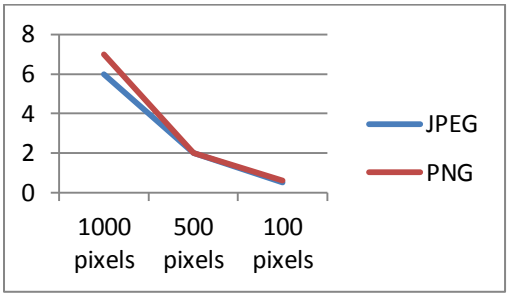


Chart 3: Comparison for time in seconds taken by Sony Ericsson ARC S (Android v4.0.4) for different resolution images.

## 6. Conclusion

As explained above, the approach used for hiding crucial information is one which is unique as the data is divided and hidden into image and text cover files if text + image option is chosen. Also, if only image cover file is chosen, the entire secret message can be hidden in the image itself. The comparison shows various devices taking the amount of time that they use in encoding a particular message in a cover image file. Thus, this approach is unique and secure for communicating secret data through smartphones.

## References

[1] Neil F. Johnson, Sushil Jajodia, Computing Practices. Exploring Steganography, “Seeing the Unseen” , George Mason University.

[2] Mohammad Shirali-Shahreza , Computer Science Department Sharif University of Technology Tehran, IRAN, ”Steganography in MMS”, Multitopic Conference, 2007. INMIC 2007, IEEE International.

[3]N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security and Privacy Mag.”, 2003, vol. 1, no. 3, pp. 32–44,.

 

[4] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science, Springer, 1998. Pp. 32-47.

[5] Ankita Agarwal, "Security Enhancement scheme for image steganography using S-DES Technique", International Journal Of Advanced Research in Computer Science and Software Engineering, April 2012,vol. 2 issue 4.

[6] The paper by C.-C. Lin, W.-H. Tsai (" Secret image sharing with steganography and authentication", 2004)

[7] M. S. Sutaone, M.V. Khandare," Image Based Steganography Using LSB Insertion Technique", Wireless, Mobile and Multimedia Networks, 2008, IET International Conference.

 