StegoMMS for Smartphones

Harsha Punjabi¹, Deepi Agrawal², Supriya Kumari³, Ekta Bhagdev⁴
D.A. Chaudhari

Abstract—The rapid development of data transfer through internet has made it easier to send the data accurate and faster to the receiver end. Many transmission media are available in today’s world to transfer the data to destination like e-mails, social sites etc. Many approaches like cryptography are used to transfer the data securely to the destination without any modifications. It is focused on the implementation of symmetric and asymmetric cryptographic algorithms. The combination of both may give the best results, as before hiding the message into another object it can be encrypted. The concept of image cryptography concerns itself with ways of embedding a secret message into a cover object, without changing the properties of the cover object evidently. The embedding procedure is typically related with a key, usually called a stego-key. Without knowledge of this key it will be difficult for a third party to extract the message or even detect its presence. Once the data is been embedded into a cover object, it is called a stego object. It could also be used as a mean for hiding the exchange of one-time passwords between a corporate server and a mobile worker. We present many cryptographic algorithms that can be used in the MMS. These algorithms can be applied to image, audio or video files. Most research regarding security in mobile environments with limited resources in terms of processing power, memory capacity and energy autonomy. Users can benefit from covert channels in MMS in order to secretly exchange hidden messages and keys, without arousing suspicion of their existence.

Keywords—Information Hiding, Multimedia Messaging Service, Smart Phones, Steganalysis, Cryptography, Internet Security, Security Attacks, Elliptic Curve Cryptography.

I. INTRODUCTION

This software has been developed for implementing most of the cryptography techniques. This means that by using one of several different algorithms. The users can embed a message within an MMS. Images can be used as cover objects for implementing image steganography. Security is a major factor if the information is valuable and thus to protect the data during their transmission security is needed. The main goal of security is integrity, confidentiality and availability. The most important method used was hiding the data into image. This technique can be used in audio as well as video files to hide the information. The original message is called as plaintext.

The transformed message that is produced as output it is call as cipher text. One key is used that is known only to the sender and receiver. Encoder is the process of converting plaintext to cipher text using cipher and key. Decoder is the reverse process of encoder. Cryptography was created as a technique for securing the secrecy of communication and many other different methods have been developed to encrypt and decrypt data in order to keep the message secret into image.

Public key encryption is one of the techniques and other one is secret key encryption. Secret key encryption uses a single key for both encryption and decryption and public key encryption uses one key for encryption and another key for decryption. Public key encryption uses two types of keys that are private key and public key. The public key can be passed openly between the parties or published in a public repository, but the related private key remains private. Data encrypted with the public key can be decrypted only using the private key. Data encrypted with the private key can be decrypted only using the public key.

ECC is emerging as an attractive public key cryptosystem for mobile /wireless environments. Mobile devices have less memory and processing power. Methods of creating multiple threads for performing multiple ECC operations are used. The strengths and weaknesses of the chosen methods can be analyzed. To provide a common frame of reference all of the steganography methods implemented and analyzed used BMP images. 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. The name of such a technique derives from the Greek language, and it literally means “covered writing”. The basic idea is that no one can see that a document is hiding a secret, while the receiver can securely extract the secret from the carrier, or cover, message. The lightweight or feasible steganography is made by means of the exclusive use of a Smartphone. Because the actual Smartphone are equipped with a camera, they locally store the photos and they have some power of computation. The screens of such small devices are usually few hundred pixels per side, and can display, at the best, several thousand colors.
The CPU of Smartphone is rarely equipped with floating point co-processors, and operates at a frequency that is orders of magnitude smaller with respect to the PCs. Moreover, the RAM of the Smartphone is orders of magnitude smaller than the one into the PCs.

II. LITERATURE SURVEY

Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

The previously method used for sending the secret message written on wax covered tablet or tattooing the message on courier’s head. The initial algorithm used for encryption was Novel algorithm. It is a random distributed method. This method embeds one bit per pixel and one bit AES (advanced Encryption standard) was employed. But this method needs high CPU cost due to its complexity. Overcoming the disadvantage of navel algorithm, the improved novel comes into picture. This is based on standard symmetric key encryption algorithm (block cipher). To get more secure covert communication, the messages are encrypted before embedding.

The drawback of this method is that distortion of image occurs after secret data is embedded because pixel values are modified and even this method is time consuming compared to others.

III. PROPOSED WORK

This paper is developed for hiding information in any mms file. The scope of the project is implementation of cryptography tools in mobile devices for hiding information file into image files and the audio file and the path where the user wants to save Image/audio and extruded file.

The secret information which is getting hidden behind any type of mms file is known as encryption. And getting the secret information from mms file is known as decryption.

Covert communication is the main goal of steganography. Therefore, a fundamental requirement of this system is that the hidden message carried by stego-media should not be known to the third person.

The other goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application areas.

A. Image Cryptography Method

In this method, information is hidden in the least significant bits (LSB) of pixels colors. Each byte of information is hidden in two pixels. A byte is divided into eight bits for hiding the information. Using a password, we select two pixels in which a byte of information is hidden.

The algorithm for selecting the pixels for cryptography is as follow:

<table>
<thead>
<tr>
<th>Algorithm 1: Selecting Pixels</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The image is segmented into n blocks of m pixels. Then according to the password, a block is selected and the information is hidden in an empty pixel of this block.</td>
</tr>
<tr>
<td>2. If the selected block starts with the pixel number k and has m pixels then the number of the last pixel is k+m.</td>
</tr>
<tr>
<td>3. This algorithm uses an array of size m+1 for remembering empty pixels of current block. This array contains the number of pixels having no data. The last cell of the array is the total empty pixels in the current block.</td>
</tr>
<tr>
<td>4. According to the password, an empty pixel is selected and the last empty pixel number is copied to this array cell.</td>
</tr>
<tr>
<td>5. After this operation the total number of empty pixels on the block decreases by one. This method is also used for selecting a block to hide the information in it.</td>
</tr>
<tr>
<td>6. After selecting the pixels we hide a byte within them. Each pixel has three colors (RGB), and the information is stored in the LSB of these colors.</td>
</tr>
<tr>
<td>7. The changes of LSB may not be noticeable because of the imperfect sensitivity of the human eyes. It seems that the human eyes are less sensitive to blue colors, so more significant changes may be applied to blue colors, before the changes be recognized.</td>
</tr>
</tbody>
</table>

Therefore each byte of information is hidden into two pixels. - The number indicating the size of information is stored in the image as well. Knowing the size of the information is necessary for decoding correctly the information.
The decoding algorithm is the same as the coding algorithm. The PNG (Portable Network Graphics) format is used to represent images. This format is common for representing images on mobile phones and using in MMS and also the Java language supports this format. The PNG format is lossless. It uses compression therefore the size of the image is relatively small.

**Algorithm 2**

1. A few least significant bits (LSB) are substituted with in data to be hidden.
2. The pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image to minimize the errors.
3. Let n LSBs be substituted in each pixel.
4. Let $d =$ decimal value of the pixel after the substitution.
5. $d_1 =$ decimal value of last n bits of the pixel.
6. $d_2 =$ decimal value of n bits hidden in that pixel.
7. If $(d_1 - d_2) \leq (2^n)/2$
   
   Then no adjustment is made in that pixel.
8. Else
9. If $(d_1 < d_2)$
   
   $d = d - 2^n$.
10. If $(d_1 > d_2)$

   $d = d + 2^n$.

This ‘d’ is converted to binary and written back to pixel. This method of substitution is simple and easy to retrieve the data and the image quality better so that it provides good security.
The encoder algorithm is as given below:

Algorithm 3
1. for i = 1... Len (message) do
2. p = LSB (pixel of the image)
3. if p! = message bit then
4. pixel of the image = message bit
5. end if
6. end for

The encoding process shows that the entire algorithm can be implemented by writing just a few lines of code. The algorithm works by taking the first pixel of the image and obtaining its LSB value (as per line 2 of the Algorithm). This is typically achieved by calculating the modulus 2 of the pixel value. This will return a 0 if the number is even and a 1 if the number is odd, which effectively tells us the LSB value. We then compare this value with the message bit that we are trying to embed. If they are already the same, then we do nothing, but if they are different then we replace the pixel value with the message bit.

This process continues while there are still values in the message that need to be encoded.

The decoder algorithm is:

Algorithm 4
1. for i = 1... Len (image string) do
2. message string = LSB (pixel string of the image)
3. end for

The decoding phase is even simpler. As the encoder replaced the LSBs of the pixel values in c in sequence, we already know the order that should be used to retrieve the data. Therefore all we need to do is calculate the modulus 2 of all the pixel values in the stegogramme, and we are able to reconstruct m as m0 . The above Algorithm shows the pseudo code of the decoding process. Note that this time we run the loop for length of message instead of length of string. This is because the decoding process is completely separate from the encoding process and therefore has no means of knowing the length of the message. If a key were used, it would probably reveal this information, but instead we simply retrieve the LSB value of every pixel.

When we convert this to ASCII, the message will be readable up to the point that the message was encoded, and will then appear as gibberish when we are reading the LSBs of the image data.

B. Why Android?

Android is a software stack for mobile devices such as mobile telephones and tablet computers developed by Google Inc. and the Open Handset Alliance. Google released most of the Android code under the Apache License, a free software license. The Android Open Source Project (AOSP) is tasked with the maintenance and further development of Android. Android uses the Dalvik virtual machine (DVM) with just-in-time compilation to run compiled Java code. DVM is better than many standard VM’s for the following reasons:

- Designed to use less space.
- The constant pool is updated to use only 32-bit indexes in order to simplify the interpreter.
- DVM uses 16-bit instruction set which works directly on local variables.

Android has a large community of developers writing applications ("apps") that extend the functionality of the devices. There are currently more than 250,000 apps available for Android. Android Market is the online app store run by Google, though apps can also be downloaded from third-party sites. Developers write primarily in Java, controlling the device via Google-developed Java libraries.

V. CONCLUSION

The application creates a stego image in which the personal data is embedded and is encrypted with key which is highly secured. The message is protected from stego attacks. The image resolution is not affected much and is negligible when the message is embedded into the image and is secured with the personal key. So, the data is secured from unauthorized access. In the event of a non-compatible device trying to send a MMS, will receive an Internet link instead message can then be view on the Internet at a later stage.

REFERENCES