International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Android Based Image Steganography

Ragul M[1], Dr. Lakshmi J. V. N[2]

[1]Master of Computer Application, [2]Assistant Professor,
[1,2]Department of MCA, Jain Deemand-to-be University, Bangalore, Karnataka, India

ABSTRACT

In this paper, text information is encoded behind the Image cover object at the sender and decoded at the receiver, provided by additional security features in the application. In this paper, we propose an In this paper, we propose an In this paper, we propose an object by changing the least significant bits of the image pixels because the image acts as the best source to hide the message that is invisible to the human eye. In this application, the text message is encrypted on the back of the sender's image card object and decoded on the receiver, which is provided with additional security features in the application.

KEYWORDS: *Steganography, Least Significant Bit (LSB), Android Application*

How to cite this paper*:* Ragul M | Dr. Lakshmi J. V. N "Android Based Image Steganography" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.1645-1647, URL: www.ijtsrd.com/papers/ijtsrd35733.pdf

IJTSRD35733

INTRODUCTION

Nowadays smart phones have become the most important part for every person in this world because they serve man in different ways. They provide reliable and efficient operation like desktop or laptop computers. As technology grows, size becomes smaller and performance enriches smartphones. Technology makes it easy and inexpensive to access, process and store and transfer information from one place to another. Due to this unreliable and constantly evolving environment, the need to protect data, information and communication is an important topic of research and research for researchers.

So far, several methods have been proposed to encrypt the message to prevent unauthorized access to the message from the earpiece. Cryptography is one such method in which confidential information is encrypted with a file or object and encrypted within the target. But the drawback of the cryptography method is that the presence of the secret message can be detected in the encrypted message because it alters the whole structure of the object Steganography is such a method in which the intruder cannot detect the presence of the message. In steganography, the message is hidden behind a cover object, also known as an envelope. The cover object can be an image, audio, text or other file format.

In image steganography, the message is encrypted with an image by changing the pixel bits. The most common and popular method of modern steganography is to use the LSP technique. This technique works best if the file is longer than the message file and the image is gray. Less important bit (LSP) is a technique in which less significant bits of image are replaced by secret message bits.

Proposed System

The Android application in this project was created using Android Studio software. In this Android application, options like data encryption and decoding are provided. This can be done by hiding the Information back of the Image. Images in use can be used with the dual options of mobile gallery or mobile camera. Besides, we are going to add an additional feature of login ID and password for both sender and recipient. In this Android application, the user interface will have a registration option in which the user has to enter the login ID or name and password. The application UI has encryption and decode option to select the basic image that the application can access from the mobile phone gallery. After selecting the Encode option, the image is selected from the photo gallery of the mobile phone, and then the user is provided with a text box to write the encrypted text message that needs to be encrypted with the image to be converted to stego-image using the LSP method.

LSB (lowest significant bit)

LSB is the lowest significant bit byte value of the image pixel. LSB-based image steganography embodies the secret of the most significant bits of pixel values of the cover image . The concept of LSB embedding is simple. It takes advantage of the fact that the level of accuracy in many image formats is much higher than can be perceived by the average human eye. Therefore, since the altered image has slight variations in its colours, a human being cannot distinguish it from the original by looking at it. In the standard LSB technique, eight bytes of pixels are required to store 1 byte of confidential data, but in the proposed LSB technique, only four bytes of pixels are sufficient to hold a message byte. The remaining bits in the pixels remain the same.

ENCRYPTION

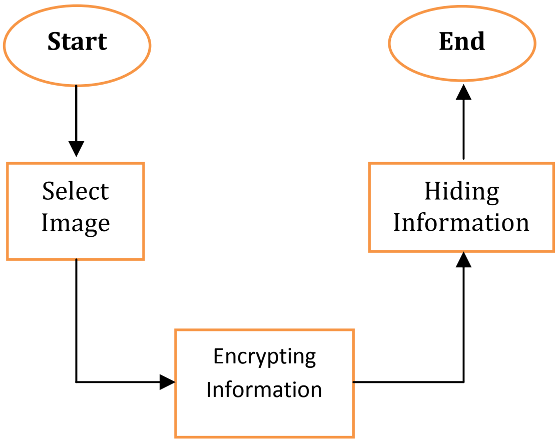
To hide a data behind the cover image, the first user log in to the System. The embedded message feature embeds a message in the main file. The system asks for the primary file & amp Release file. After the user specifies the files, the system prompts you to embed the message in the file. The system prompts you to compress the output file. The password must be encrypted in the Release File. After completing the above steps the message is embedded in the release file .Then using the LSB method, the secret message is hidden behind the cover image. The most common and simplest way to embed information in a cover image is with an LSB. The LSB of an image is replaced by a bit of secret message. Using the 24 bit image, each of the red, green and blue colors can be used to hide a secret message. Now, the message is encrypted as soon as it is hidden. This is called a stego film and you can send it anywhere you want.

Decryption

On target, the receiver receives the stego image and encrypts the message behind the stego file using the reverse LSB algorithm. The Recover Message feature retrieves a message from a primary file. The system asks for the primary file. After the user specifies the primary files, the system returns the primary file information. If the primary file is encrypted with a password, the system prompts for the password, and if the user specifies the correct password, the system returns the recovery message.

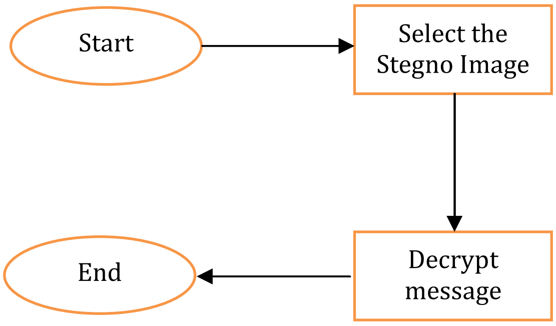
Encoding Algorithm

1. the extracted secret message is compressed because the contents of the compressed string are difficult to detect and read, and this reduces the size of the string.
2. the compressed string is encrypted with a secret key. Finally, encrypts the message encrypted in the image. It uses LSB steganography embedding to encrypt data into an image.
3. The process will stop when the message is encrypted.



Decoding Algorithm

1. First, Decode the Information from the encrypted image using LSB decoding.
2. Second, decrypt the compressed Information from the decoded Information using the secret key.
3. Finally, Minimize the Information to get the original compressed Information.



Advantage

1. Execution time is fast.
2. The information hidden on the cover card cannot be detected from the steganization attack.
3. Hide large-scale text on the cover image. Image Hide small image as large cover image.
4. The sender can protect the confidential information in the image by setting the password on the cover image.
5. Works on all versions of the Android operating system.

Future Scope

1. Improves the compression ratio of images.
2. It can be extended to a level which can be used for different types of image formats like bmp, jpeg.
3. So other image formats will also be used for steganography.
4. The less significant bit algorithm can be upgraded to several levels by using different keys for significant encryption and encryption.

Conclusion

Image steganography allows two people to communicate privately. We have created an Android application using this technique to hide the secret image and text message in the image and securely without worrying about human medium attack by password protecting the image. It provides protection from attackers. We use the LSB algorithm, an efficient algorithm for stego application.JPEG, BMP and PNG type image can be used as cover image and input secret image in our application. This application does not change the secret information of the original image after hiding it.

References

[1] R. Chandramouli, M. Kharrazi, and N. Memon, "Image Steganography and Steganalysis: Concepts and Practice", T. Kalker et al. (Eds.): IWDW 2003, LNCS 2939, SpringerVerlag Berlin Heidelberg, 2004, pp. 35–49.

[2] F. A.P. Petitcolas, R. J. Anderson, "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 98, Special Issue on Copyright & Privacy Protection. ISSN 0733-8716, pp 474- 482.

[3] P. Salee, "Model–based Steganography", In: Proceeding of the 2nd International workshop on digital water marking, Seoul, Korea, October 20-22 2003 , LNCS , vol.2939, pp. 254- 260.

[4] https://www.clear.rice.edu/elec301/Projects01/steganosaurus/background.html.

[5] Data Security Using Image Steganography and Weighing Its Techniques.

[6] International Journal of Mobile & Adhoc Network|Vol2|issue 2|May 2012 150 Steganography on Android Based Smart Phones.

[7] https://www.theverge.com/2017/2/16/14634656/android-ios-market-share-blackberry-2016.

[8] https://developer.android.com/reference/android/media/Image.html.

[9] T. F. M. White, J. E. Martina, Mobile Steganography Embedder, 11 SBSeg Simposio Brasileiro Em Seguranca Da Informacao E De Sistemas Computacionais, Bsalia-DF, 6 a 11de Novembro de 2011.

[10] MobiStego:http://play.google.com/store/apps/details? Id=it.mobistego, visited on 04.06.2018.