IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 4, PP 55-59

Android Based Secret Information Sharing Using Steganography

Srishanth Shetty[1], Pawan Sharma[2], Om Kadam[3], Ritu Sharma[4]
[1,2,3,4](Department of Electronics and Telecommunication, Atharva College Of Engineering, India)

Abstract: *In this paper, we have proposed an Android Application based on Image Steganography using Least Significant Bits (LSB) algorithm. Steganography technique helps to share secret information behind an image cover object by changing the least significant bits of the Image pixels as Image acts as a best source for hiding message which cannot be detected by Human Eye. In this application, text information is encoded behind Image cover object at the sender and decoded at the receiver, provided by additional security features in the application.*

Keywords: *Steganogaphy, Least Significant Bit (LSB), Android Application.*

I Introduction

In today's digital world of communication, information sharing is at its peak. Due to this, there is a large scope for the hackers, intruders to illegally access information causing threat to the privacy of genuine sender and receiver. So privacy of data sharing is a top concern. One of the techniques to ensure privacy of the message is by hiding the data or message from the intruder. This can be achieved by the technique known as Steganography. Steganography is a method in which the data or message is hidden behind another cover object. In this paper, we develop an Android application based on Image Steganography where data is hidden behind an image cover object by using LSB algorithm.

So far, many methods have been proposed to encrypt message to avoid illegal access of message from eavesdropper. Cryptography is one such method in which the secret information is encrypted with a file or object and decrypted at the destination. But drawback in cryptography method is that the presence of secret message can be detected in the encrypted message, as it modifies the whole structure of the of the object Steganography is one such method in which the presence of message is not detectable to intruders. In Steganography, the message is hidden behind a cover object also called as an envelope. The cover object can be an image, audio, text or other file formats.

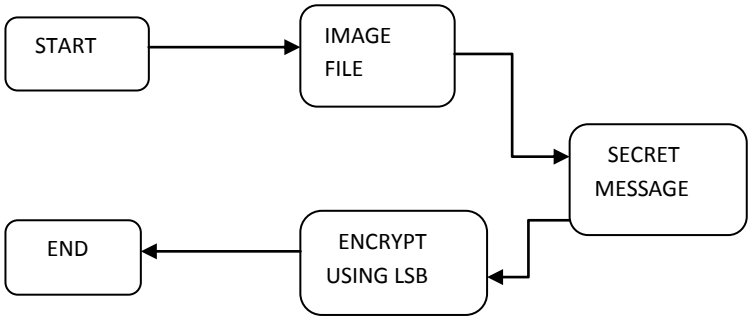
In Image Steganography, the message is encrypted with an image by changing the pixel bits. The most common and popular method of modern day Steganography is to make use of LSB technique. This technique works best when the file is longer than the message file and if image is gray scale. Least Significant Bit (LSB) is a technique in which the least significant bits of the image is replaced by the secret message bits.

II Literature Survey

There are various other data hiding techniques for different purposes and applications. These techniques are collectively known as 'information hiding' techniques [1]. Some of these are namely Steganography, cryptography; watermarking and fingerprinting are inter-linked to each other as well. Steganography also called 'Covered Writing' [3] conceals very existence of hidden secret data in cover object [4] where as cryptography scrambles the data to prevent the attacker from understanding the contents [5]. Steganography also used where cryptography is either not allowed or not to be used. Steganography and cryptography are complementary and orthogonal to each other and both can be used in combined form provide higher level of security. Watermarking is the process of embedding watermark signal into multimedia data to

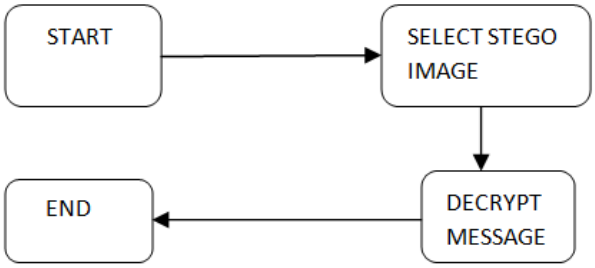
generate watermarked object to protect authenticity of owner on that digital object and mainly focuses on the robustness of embedded message rather than capacity or concealment. Since increasing capacity and robustness at the same time is not possible [6] therefore watermarking can be used for copyright protection and tracking legitimate use of a particular software or media. In fingerprinting, on the other hand, separate marks are embedded in the copies of the object that are supplied to different customers such as hidden serial numbers which enables the intellectual property owner to identify individuals who break their license agreement and supply the property to third parties [2].Steganography provides an ultimate guarantee of authentication that no other security tool can ensure. The primary goal of Steganography techniques is to maximize embedding rate and minimizing the detectability of the resulting Stego images [7].

III Overall Flow Diagram



ENCRYPTION

For hiding a data behind cover image, first user has to login into the system. The embed message feature, embeds a message into a master file. The system asks for the master file & output file. After the user specifies the files, the system asks for the message to embed into the file. The system also asks to compress the output file; password to be encrypted into output file. After the completion of above steps the message is embedded into the output file .Then using LSB algorithm, secret message is hidden behind the cover image. LSB is a common and simple way to embed information in a cover image. The LSB of an image is replaced by bit of the secret message. Using image of 24 bit, a bit of each of the red, green and blue colour can be used to hide secret message. Now, once the message is hidden i.e. it is encrypted. It is called as Stego image and can be sent to the intended destination.



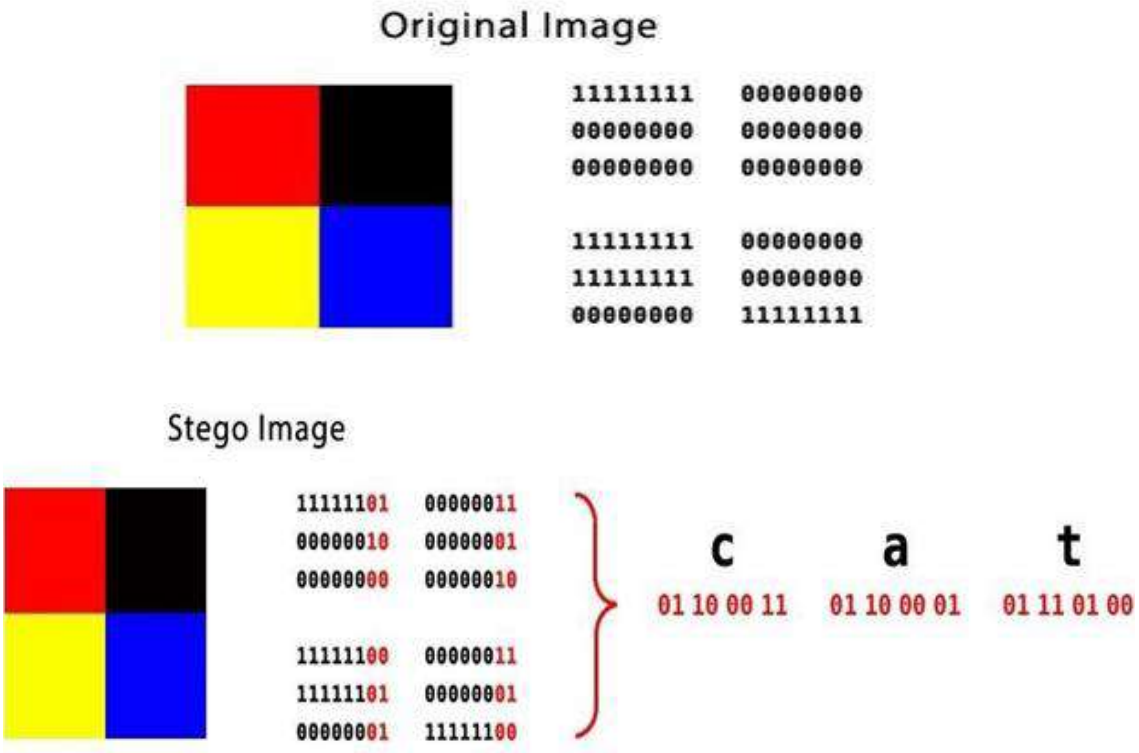
DECRYPTION

At the destination, receiver receives the stego image and using inverse LSB algorithm decrypts message behind the stego file. The retrieve message feature retrieves a message from a master file. The system asks for the master file. After the user specifies the master files, the system gives the information of master file. If the master file is encrypted with password, the system asks for the password, if the user specifies correct password, the system gives the retrieved message.

IV. Lsb Algorithm

A. EMBEDDING DATA STEPS

1. Extract the pixels of the cover image
2. Extract the character
3. Insert characters of text file in each first component of next pixels by replacing it.
4. Repeat till all the characters has been embedded.
5. Place some terminating symbol to indicate end of data.
6. Obtained stego image.



B. DATA EXTRACTION STEPS

1. Extract the pixels of the stego image.
2. Now, start from first pixel and extract secret text characters from first component of the pixels. Follow up to terminating symbol
3. Then go to next pixels and extract secret message characters from first component of next pixels up to terminating symbol.
4. Extract secret message

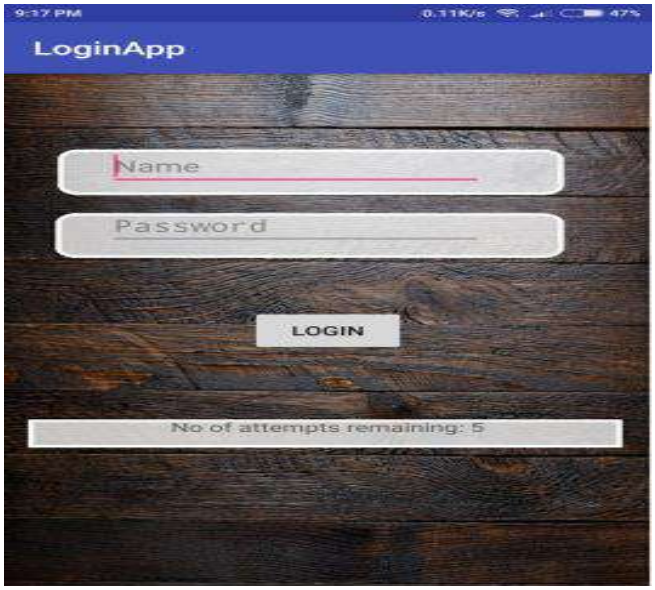
V. Proposed Work

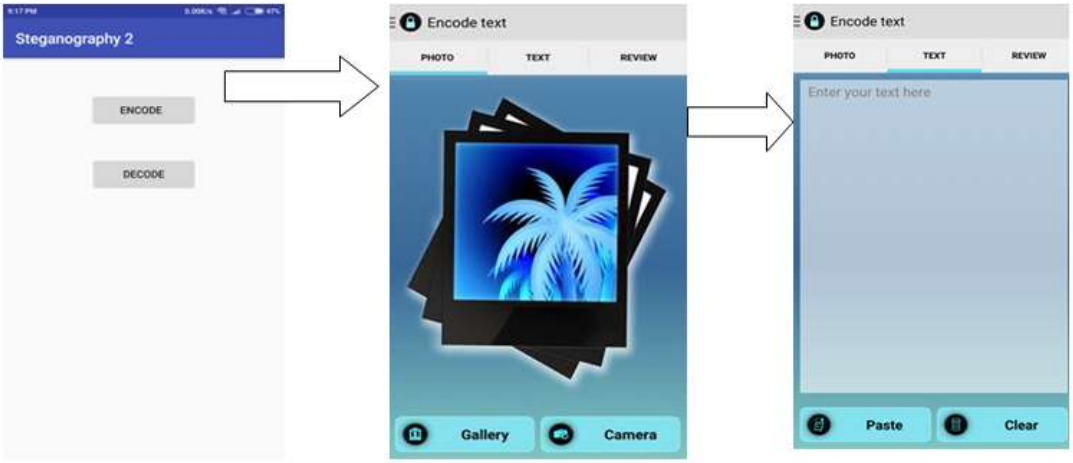
In this paper, an android application is developed using Android Studio Software. In this android app, options like encoding and decoding the data is provided. This can be done by hiding the data behind an image. Images in the application can be used by dual options either by mobile gallery or by mobile camera. Besides, we are also going to add extra feature which is login id and password to both the sender and the receiver.

In this android app, the User interface (UI) will have a Register option in which the User has to enter the Login Id OR Name and Password.

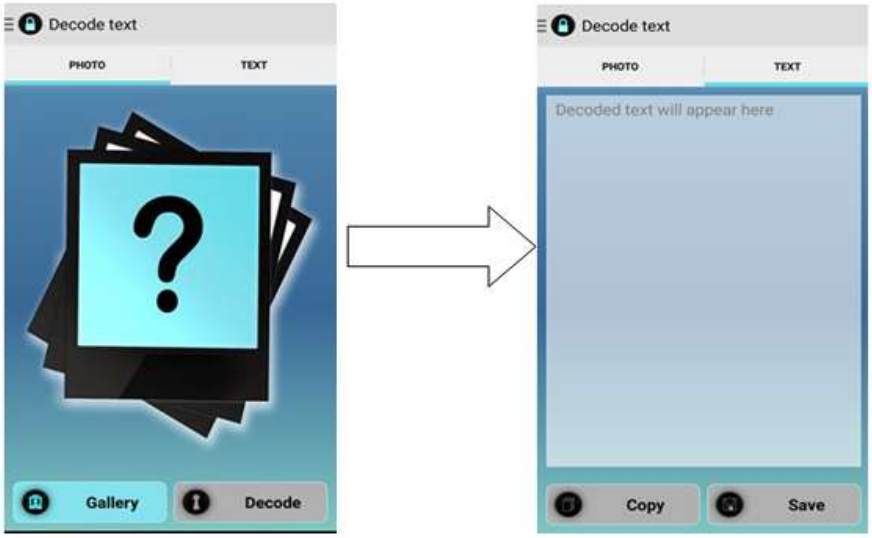
The app UI will have encode and decode option where the app can access and select the base image from the mobile phone gallery.

After selecting the Encode option, image is selected from photo gallery of Mobile phone and then, the user is provided a Text Box for writing the secret text message to be encoded with the image using LSB algorithm converting into Stego-image.





At the Receiver side, by selecting the Decode option in the UI, it can select the Stego-image file and then the by using Inverse LSB algorithm can decode the Secret message and then display it to the Receiver.



VI. Advantages

• Messages do not attract attention to themselves i.e. difficult to detect.
• It can only be detected by desired receiver.
• Provides better security for sharing data in LAN,MAN & WAN.
• The proposed technique uses LSB to hide data from a pre -defined position agreed between two parties. Same position is used only once to enhance security.
• Network surveillance and monitoring systems will not flag messages or files that contain Steganography data.
• Along with hiding secret information, Steganography also conceal the communicating parties.

VII. Applications

• Fields of application
1. Defense and intelligence
2. Medical
3. Online banking
4. Online transaction
• Confidential communication and secret data storing.
• Protection of data alteration.
• The health care, and especially medical imaging systems, may very much benefit from information hiding techniques.
• In military applications.
•Transport highly private documents between international Governments.

VIII. Conclusion

• Smart Steganography application software provided for the purpose , how to use embed message into image The master work of this application is in supporting the facility of compressing of output file, even encrypt the output file .
• Steganography can be the best security tool.
• Hiding a message with steganography method decreases the chance of a message getting detected.
• Using this method, encryption routines can become much stronger.

IX. Future Scope

• The compression ratio of images can be improved.
• It can be extended to a level such that it can be used for the different types of image formats like bmp, jpeg, .tif etc.
• So other image formats also will come in use for Steganography.
•Least significant bit algorithm can be improved to a several level by using the different keys for encryption and decryption.

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]. J. Silman, "Steganography and Steganalysis: An Overview", SANS Institute, 2001.
[5]. W. Huaiqing and W. Shouzhong, "Cyber Warfare: Steganography vs. Steganalysis", October 2004, Vol. 47, No. 10 communication of ACM, pp. 76-82.
[6]. A. Cheddad, J. Condell, K. Curran, & P. McKevitt, (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, Vol 90, Issue 3, March 2010, pp. 727-752.
[7]. M. Kharrazi, H.T. Sencar and N. Memon, "Cover Selection for Steganographic Embedding", IEEE International Conference on Image processing, 8-11 oct 2006, Atlanta USA, pp. 117-120.