ANDROID BASED IMAGE STEGANOGRAPHY

PAWAN SHARMA, SRISHANTH SHETTY, OM KADAM,PROF.RITU SHARMA
STUDENT,STUDENT,STUDENT,PROFESSOR
ELECTRONICS AND TELECOMMUNICATION
ATHARVA COLLEGE OF ENGINEERING, MUMBAI, INDIA

Abstract : In this paper, we have proposed an application which is android based using a technique called least significant bit(LSB) algorithm. Steganography is a method of hiding data behind any cover object. Cover object can image, audio or video. Image is the best source to hide data as because image takes less space and its compression ratio is very less as compared to audio and video. Using image as cover object will make system run smoothly and it will remain undetected by the human eye. In this system, text is encoded behind image cover object and it can be decoded at the receiver point by using reverse LSB algorithm.

Keywords – Steganography,Least Significant bit(LSB),Android Application

I. INTRODUCTION

In today's time, as everything is turning into digital, sending data or private information is rapidly increasing. At the same time, threats of data hacking or leaking are also increasing. This threat has restricted people to share their data confidentially. So to overcome this problem, many techniques have been invented but they all could not solve this problem completely. To erase the threat of data, Steganography in the market to solve this problem. Steganography is the only technique which can erase this problem completely.

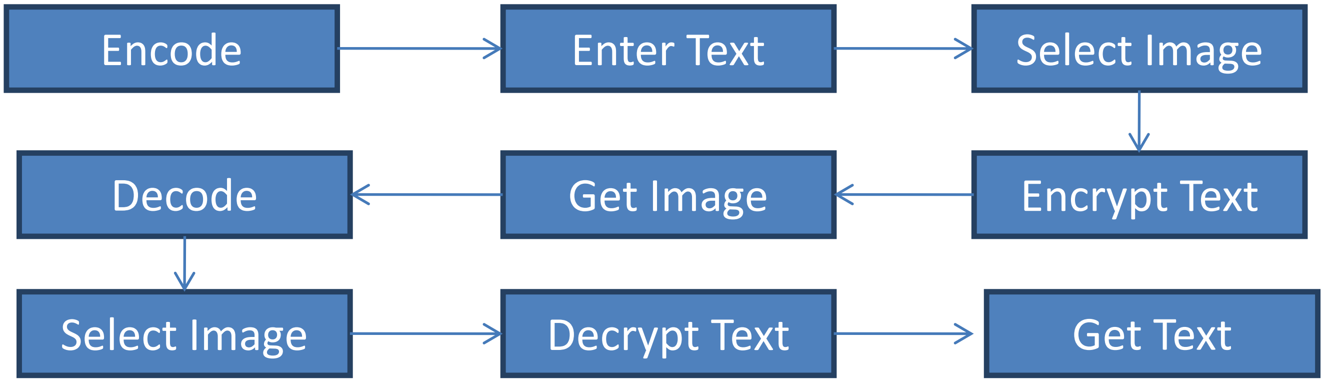
Well in steganography, there are various forms like image steganography, audio steganography video steganography, etc. Amongst this, all are best and gives good results but image is simple to handle and not very complex. As because Image Steganography does not take more space in a system and its compression is lossless. Loss in this format is negligible. On the contrary, audio and video are little lossy. In image steganography, image is used as a cover object to hide data behind it.

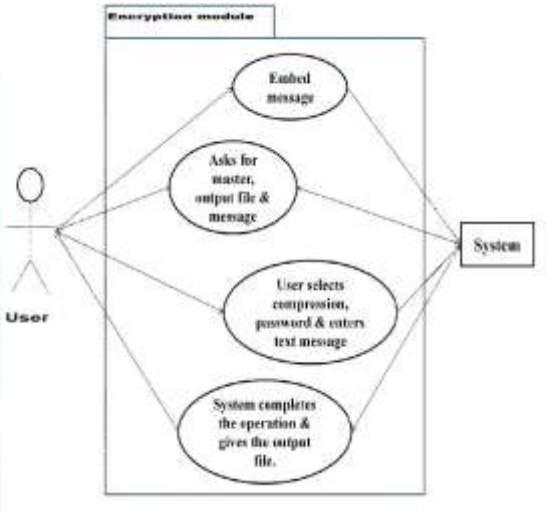
In image steganography, the message is hidden behind cover object by changing the bits. The bits are changed by using a very famous and most useful technique called Least Significant bit(LSB). In LSB, the redundant bits image are replaced by bits of data. In this way message is hidden behind image cover object and this image can be normally send from one point to another point using any sharing device. This system works better when the file is longer than the message file and image is gray scale.

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] whereas 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 detect ability of the resulting stego images [7].

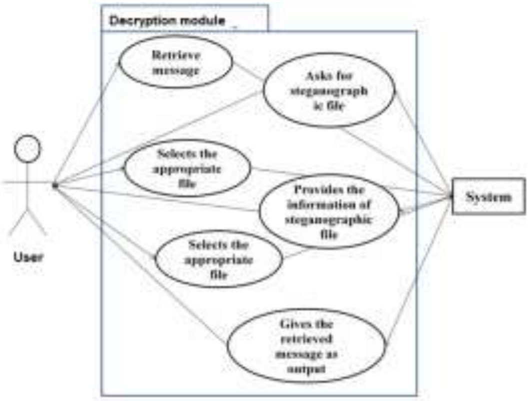
III. FLOW DIAGRAM




Encryption module
Embed message
Asks for master, output file & message
User
User selects compression, password & enters text message
System
System completes the operation & gives the output file.

Encryption module

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 &amp; 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 module
Retrieve message
Asks for steganograph ic file
Selects the appropriate file
User
Provides the information of steganographic file
System
Selects the appropriate file
Gives the retrieved message as output

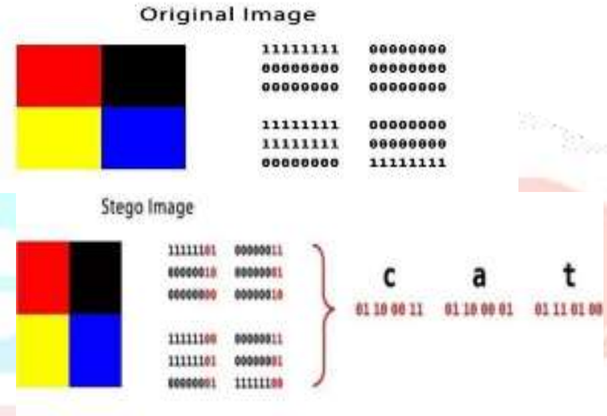
Decryption module

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

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.

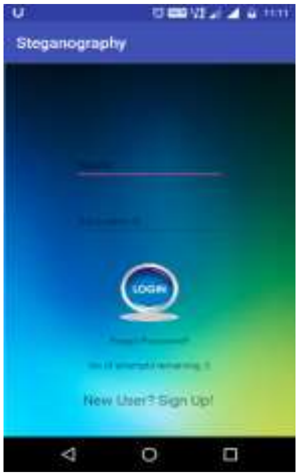


B. DATA EXTRACTION STEPS

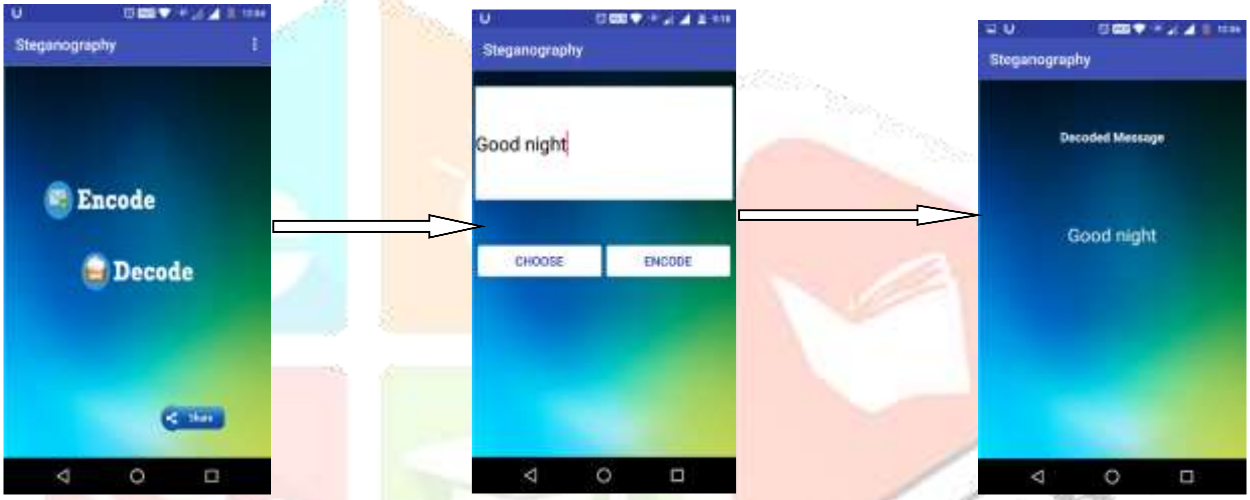
1. Extract the pixels of the stego image.
2. Now, start from first pixel and extract secret text characters from first component of the pixels. Follow up to terminating symbol
3. Then go to next pixels and extract secret message characters from first component of next pixels up to terminating symbol.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



When an user opens the app, user will get option to sign up or if already registered then directly sign in.



Once the user has signed in, user will get next interface in which will get options like encode, decode and a share button. After selecting the Encode option, image can be selected from the camera 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. After this user can send the stego image to its intended person. 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 easily decode the Secret message.

VI. ADVANTAGES

- Messages do not attract attention to themselves i.e. difficult to detect.
- It can only be detected by desirous 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.
- The compression of the 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 can also be used in steganography.

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.
- The security using least significant bit algorithm is good but in future it can be improved to a certain level by varying the carriers as well as 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, Springer-Verlag 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. Mc Kevitt, (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.