Real Time Image Security For Mobile Communication Using Image Steganography

Mrs. Richa Raja Gautam
M.E. Scholar
Raipur Institute of Technology, Mandir Hasod
Raipur, India

Prof. Rakesh Kumar Khare
Head of Department (I.T)
Raipur Institute of Technology, Mandir Hasod
Raipur, India

Abstract

The fascinating rise in Mobile communication in the last few decades, leads the requirement of the secure communication of data between mobile receivers. Especially security matters a lot during transmission of images and videos. This is a new technique for secured image transmission, in this method a dummy image will be used as a carrier of main image and main image will be hidden inside the dummy image using the most efficient LSB modification algorithm. In addition to this to hide main image inside the dummy image a random key will be used, the key and the main image both simultaneously embedded on the dummy image. . The same key will be then used by the receiver to extract the hidden image inside the dummy image.

1. Introduction

A. Overview-

The presence of mobile networks has prompted new problems with security and privacy. Having a secure and reliable means for communicating with images and video is becoming a necessity and its related issues must be carefully considered.

Hence, image security and image encryption have become important. The images can be considered nowadays, one of the most usable forms of information. Image and video encryption have applications in various fields including Mobile Communication, Internet communication, multimedia systems, medical imaging, telemedicine and military communication [1-3].In case of mobile communication the images or videos are transferred in real time hence the most important obstacle is speed of operation.[4-5].In the digital world nowadays, the security of digital image has become more and more important because of the advances in communication technology and multimedia technology. We can realize that more and more researches have been developed for security issues to protect the data from possible unauthorized instructions [6].

B. Research Objectives-

The objective of this project work is to develop and implement a real time image security system for mobile communication, which can resolve the above mentioned problems. The proposed algorithm is based on the private key image stenography based on LSB modification technique. In this project work a dummy image will be used to hide the main image with the help of LSB modification technique with a user defend key or randomly generated key. To ensure the high security efficiency this algorithm facilitate that the key generated for image recovery at the receiver mobile also embedded with the main image inside the dummy

image so that the intended mobile receiver can only recover the private or main image.

2. Overview of Steganography

A. Stenography concepts-

Although Steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem proposed by Simmons [7], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication [08]. The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information [9].

B. Different kinds of Steganography-

Almost all digital file formats can be used for Steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [10]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [11]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 1 shows the four main categories of file formats that can be used for Steganography.

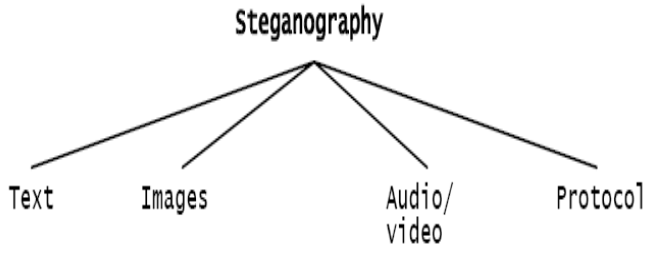


Figure 1: Categories of Steganography

Hiding information in text is historically the most important method of Steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message. It is only since the beginning of the Internet and all the different digital file formats that is has decreased in importance [1].

C. Image Steganography-

As images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist.

3. Proposed Approach

A. Methodology-

This is a new technique for secured image transmission, in this method a dummy image will be used as a carrier of main image and main image will be hidden inside the dummy image using the most efficient LSB modification algorithm. In addition to this to hide main image inside the dummy image a random key will be used, the key and the main image both simultaneously embedded on the dummy image. The same key will be then used by the receiver to extract the hidden image inside the dummy image. The most important feature of this algorithm is that during the communication if a hacker hacked the transmitted image can not able to extract main image without having the key.

Since Mobile communication belongs to very low power circuits hence during the development of this algorithm the most important obstacle is that, we have

to ensure low power consumption during the communication , for that we have to avoid complex and large time taking algorithms. That's why we have used the LSB modification technique for this project.

The methodology is explained below with the help of flow chart

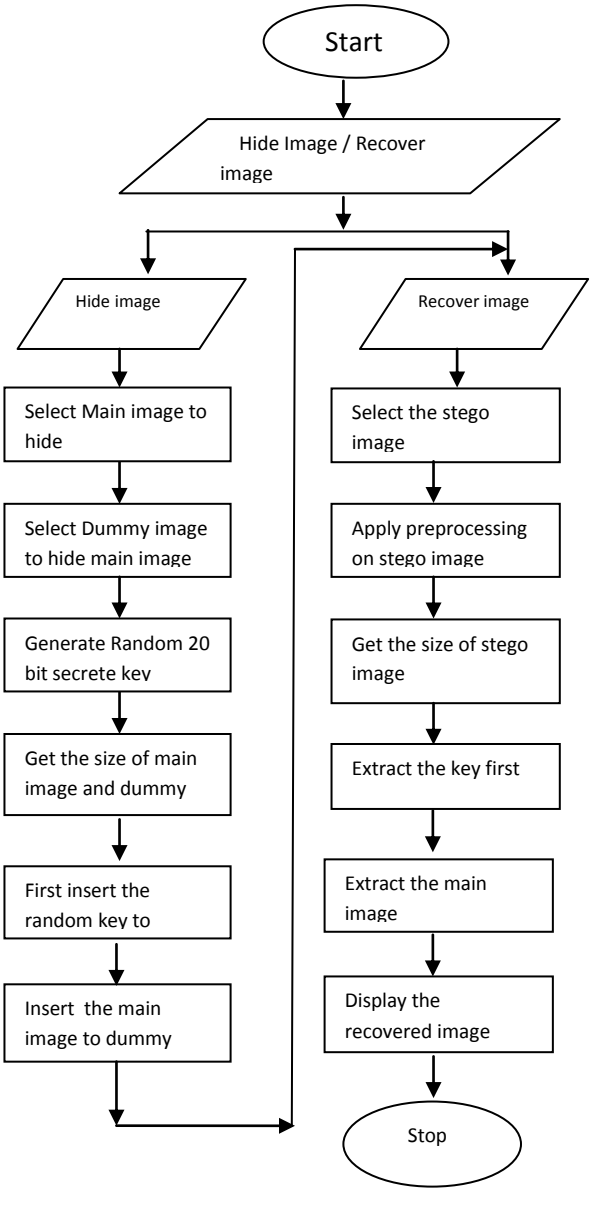
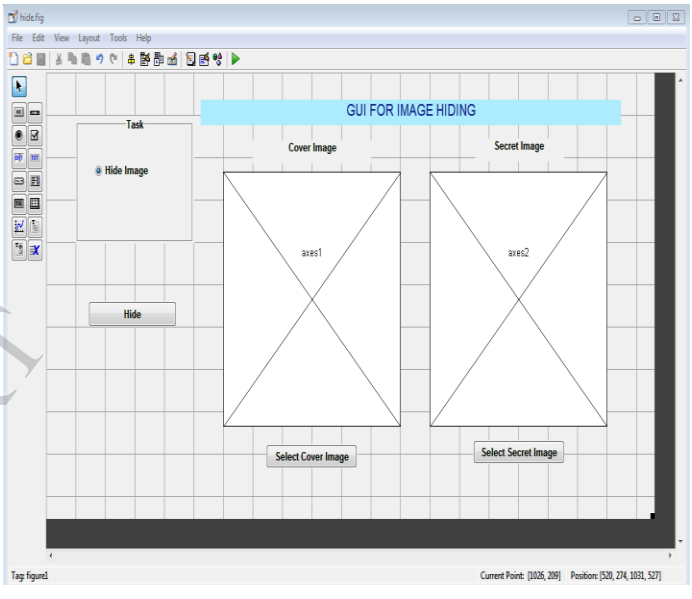


Fig 2. Flow chart of the Project Algorithm

B. Graphical User interface development for encryption-

The graphical user interface is the strongest tool to provide the complete facilities and complete visualization of the developed works. In this project work a GUI has been developed for the image hiding based on the concept of the algorithm developed in this project. The screen shot of developed GUI for image hiding is show in figure (3).



Fig(3) developed GUI for image hiding

4. Conclusion

In this Modern era, image Transmission and processing plays a major role, and during the transmission and reception the image security plays an important role so that no one can receive or hack the private images. In this project work a simple as well efficient algorithm has been successfully developed and implemented on MATLAB for real time image security for mobile communication. In addition to this the low power implementation has also been successfully achieved for mobile communication.

In spite of this the developed algorithm contains an efficient preprocessing frame work which was not

available earlier, and during the preprocessing it has been found that the preprocessing frame work can able to remove up to 60% of noise attacks successfully. I.e. by using the developed project user can recover the secrete image even though the stego image is corrupted by noises.

5. References

[1] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science,

www.liacs.nl/home/ tmoerl/privtech.pdf.

[2] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001

[3] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

[4] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998

[6] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[7] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002

[8] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001

[9] Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983

[10] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[11] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996