iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.43626

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Android Application for Image Steganography using Android Studio

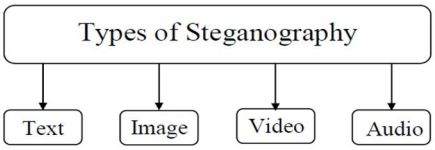
Dr. K. Jayasakthi Velmurugan[1], Ganesh S[2], Daniel Alfred Visuvasam W[3], Akash K R[4]
[1]*Associate Professor, Department of Computer Science and Engineering, Jeppiaar Engineering College, Chennai-600119*
[2, 3, 4] *Student of Jeppiaar Engineering College, Department of Computer Science and Engineering*

Abstract: ***Image Steganography is mainly used for hiding an image or secret message in a cover image. For data hiding, this technique is being widely used for so many years. Image steganography is being used now by government, individual sender and receiver, in business and in so many fields. Now-a-days, this process has become very popular worldwide. People are doing research on image steganography and inventing new even stronger algorithms for image steganography. Hiding data in cover image by modifying bits of that is now optimized by so many new algorithms. Enthusiastic people are increasing demand of researching on image steganography and developing PC software and mobile application using different developing tools, programming languages and their own invention, algorithms etc. Steganography is the process of hiding a secret message within a larger one, in such a way that someone cannot know the presence or contents of the hidden message. Although related, steganography is not to be confused with Encryption, which is the process of making a message unintelligible. Whereas, steganography attempts to hide the existence of communication. The main advantage of steganography algorithm is because of its simple security mechanism. Because the steganographic message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing the existence and the appropriate encoding scheme.***
Keywords: steganography, hiding, algorithms

I. INTRODUCTION

Data hiding is a popularly used technique for secure communication. Data hiding is the technique of embedding information into digital content without causing perceptual degradation. Watermarking, cryptography and steganography are three famous techniques used in data hiding. Steganography is an ancient science for hiding the information in the communication. Steganography is defined as a technique for concealing information and it is applied in the area of the computers and networks widely.

There are different types of steganography processes like steganography for hiding data in a text, steganography for hiding data in an image, steganography for hiding images in an audio, steganography for hiding images in a video, steganography for hiding images in a protocol etc. Among them, image steganography is the mostly used technique now-a-days. Image Steganography is defined as a hiding process of a secret message within an image in such a way that others cannot understand the presence of contents of the hidden message.



II. LITERATURE SURVEY

A literature survey is a summary of a set of related research. It selects information from papers, and organizes and integrates it into a logical justification. This section aims to report a study of researchers' preferences in selecting information from cited papers to include review, and the kinds of transformations and editing applied to the selected information**.**

G. Prashanti and K. Sandhyarani have done survey on recent achievements of LSB based image steganography. In this survey, authors discuss the improvements that enhance the steganographic results such as high robustness, high embedding capacity and un-detectability of hidden information. Along with this survey two new techniques are also proposed. First technique is used to embed data or secret messages into the cover image and in the second technique a secret gray scale image is embedded into another gray scale image. These techniques use four state table that produce pseudo random numbers. This is used for embedding the secret information. These two methods have greater security because secret information is hidden on random selected locations of LSBs of the image with the help of pseudo random numbers generated by the table.

Bingwen Feng, Wei Lu, and Wei Sun in their paper "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", purposed a state of-the-art approach of binary image steganography. This technique is proposed to minimize the distortion on the texture. In this method of steganography, firstly the rotation, complement and mirroring invariant texture patterns are extracted from the binary image. They also proposed a measurement and based on this proposed measurement this approach is practically implemented. Practical results show that proposed steganographic approach has high statistical security with high stego image quality and high embedding capacity.

III. SYSTEM REQUIREMENTS

A. Hardware Requirements

1) Minimum i5 or above Processor
2) Minimum 4 GB or above RAM
3) Windows OS

B. Software Requirements

1) Java
2) XML
3) Android Studio

IV. ARCHITECTURE DIAGRAM

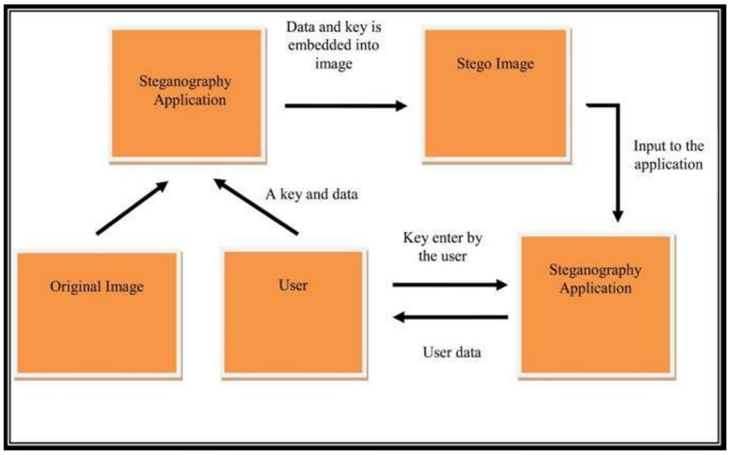


Fig. 1: The General Steganography System

V. EXISTING SYSTEM

There have been many techniques for hiding messages in images in such a manner that the alterations made to the image are perceptually indiscernible. However, the question whether they result in images that are statistically indistinguishable from unhampered images has not been adequately explored. There are various algorithms used to hide a message in an image. But, mostly in all the places the old algorithms are used. Which is not a huge problem, but as the technology develops, the latest algorithm must be used to not question the privacy of users.

VI. PROPOSED SYSTEM

We look at some specific image-based steganography techniques and show that an observer can indeed distinguish between images carrying a hidden message and images which do not carry a message. We derive a closed form expression of the probability of detection and false alarm in terms of the number of bits that are hidden. This leads us to the notion of steganographic capacity, that is, how many bits can we hide in a message without causing statistically significant modifications? Our results are able to provide an upper bound on the capacity. Our ongoing work relates to adaptive steganographic techniques that take explicit steps to foil the detection mechanisms. And a much stronger algorithm is used to ensure the safety of the encrypted text in the image.

VII. ADVANTAGES OF STEGANOGRAPHY

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

This method featured security, capacity, and robustness, the three needed aspects of steganography that makes it useful in hidden exchange of information through text documents and establishing secret communication.

Important files carrying confidential information can be in the server in and encrypted form No intruder can get any useful information from the original file during transmit.

With the use of Steganography, Corporation Government and law enforcement agencies can communicate secretly.

VIII. PROJECT SCOPE

This application would enable defense personnels to send confidential data of high priority to others. Because the human eye cannot decipher that there is any encrypted text, it can be put to great use while remaining easy to understand and use. The major limitation of the application is designed for images cover files. It accepts only images as a carrier file. The future work on this project is to improve the compression ratio of the image to the text. This project can be extended to a level such that it can be used for the different types of multimedia files.

IX. FUTURE SCOPE

In today's world, we often listen a popular term "Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography, this problem is often taken as Steganalysis. Steganalysis is a process in which a steganalyzer cracks the cover object to get the hidden data. So, whatever be the technique will be developed in future, degree of security related with that has to be kept in mind. It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future solution for this above-mentioned problem.

We hope to add support to hide all file formats. This allows for a much broader spectrum of uses: one would be able to encode .gif, .png, .pdf, .mp3, etc. The program would be more versatile because often hiding text just isn't enough. We also would like to implement batch image processing and statistical analysis so that we can run the program through a dataset of images and detect Steganography and perhaps crawl through Google Image Search to see how prevalent Steganography is. We eventually plan to port the program to use C/C++ so that we may take advantage of bit-fields in C and learn to code GUI's as well. I have a plug-in handler developed for C++ that I would like to use in this project so that third-party developers may contribute to the project.

X. CONCLUSION

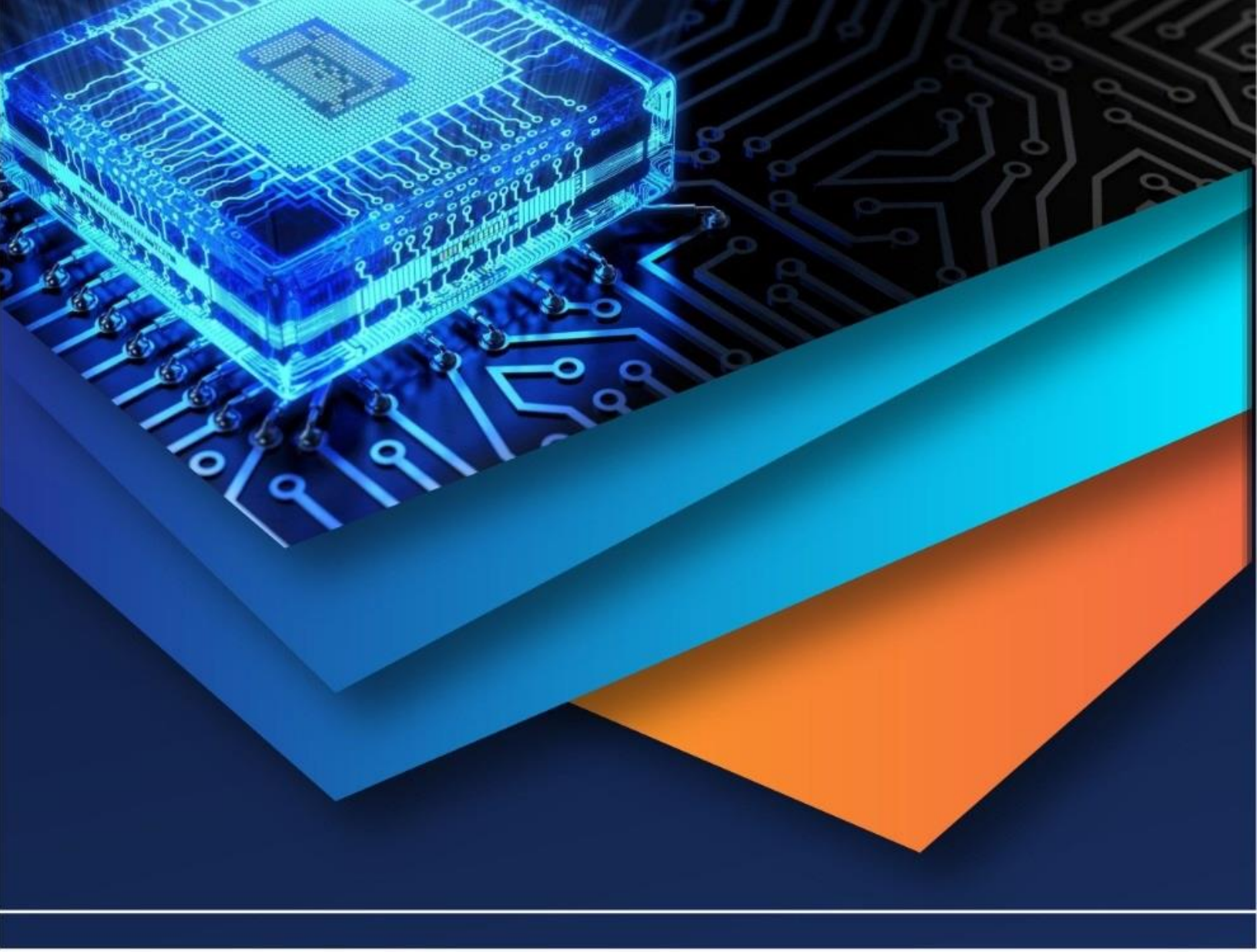
As steganography becomes more widely used in computing, there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. Many currently used techniques are not robust enough to prevent detection and removal of embedded data. The use of benchmarking to evaluate techniques should become more common and a more standard definition of robustness is required to help overcome this. For a system to be considered robust it should have the following properties:

1) The quality of the media should not noticeably degrade upon addition of a secret data.
2) Secret data should be undetectable without secret knowledge, typically the key.
3) If multiple data are present, they should not interfere with each other.
4) The secret data should survive attacks that don't degrade the perceived quality of the work.

This work presents a scheme that can transmit large quantities of secret information and provide secure communication between two communication parties. Both steganography and cryptography can be woven into this scheme to make the detection more complicated. Any kind of text data can be employed as secret msg. The secret message employing the concept of steganography is sent over the network. In addition, the proposed procedure is simple and easy to implement. Also, the developed system has many practical, personal and militaristic applications for both point-to-point and point-to multi- point communications.

REFERENCES

[1] Feng, J.B., Lin, I.C., Tsai, C.S., Chu, Y.P., 2006. Reversible watermarking: current status and key issues. International Journal of Network Security 2 (May), 161–170.
[2] C. K. Chan, L. M. Cheng, “Hiding data in image by simple LSB substitution”, pattern recognition, Vol. 37, No. 3, 2004, pp. 469-474.
[3] R. Chandramouli, N. Memon, “Analysis of LSB Based Image Steganography Tech-niques”, IEEE pp. 1019-1022,2001.
[4] Jhukkj F. Hartung and M. Kutte "Information hiding-a survey, " Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Content, Volume: 87 Issue:7, pp. I062-I078, July. 1999.
[5] Nidhi Sharma, Manu Devi, “Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images,” Proceedings of 2014 RAECS UIET Panjab University Chandigarh,06-08, March 2014.
[6] Padmini.K, Champakamala.B.S, Radhika.D. K Asst Professors, Department of TCE, Don Bosco Institute of Technology, Bangalore, “Least Significant Bit algorithm for image steganography “India International Journal of Advanced Computer Technology(IJACT), Volume 3,Number 4.
[7] Kaur Jaspreet and Singh Sandeep “Odd-Even Mes-sage Bit Sequence Based Image Steganography”, (IJC SIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3930-3932.
[8] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM, 47:10, October 2004.
[9] Morkel T., Eloff J. H. P., and Olivier M. S., “An Overview of Image Steganography”, Information and Computer Security Architecture (ICSA) Research Group, University of Pretoria, South Africa, 2005.
[10] E. L. Hall. Computer Image Processing and Recognition. New York: Academic Press, 1979.
[11] J. Burns. Developing Secure Mobile Application. ISEC Partners, October 2008. https://www.isecpartners.com/files/iSEC_Securing_Android_Apps.pdf, accessed November 2010.
[12] Wikipedia. Android.Wikipedia, 2010.http://en.wikipedia.org/wiki/ Android (Operating System), accessed October 2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY