International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 11 | Nov -2016 www.irjet.net p-ISSN: 2395-0072

Multimedia Content Securing By Using Steganography Technology for Android Application

Akshay Andhale[1], Vaibhav Dhas[2], Abhilash Tekale[3],Shubham Awate[4]

STES Sinhgad Institute of Technology and Science, Narhe, Pune-411041
Department of Computer Engineering

Abstract – *Data is associate very important quality for any individual or organization and must be protected from intruders or hackers. The need to hide data from hackers has existed since precedent days ancient times, and nowadays, there are developments in digital media, such as audio, video, images, and so on. To secure secret information, different media strategies are used and steganography is one. Steganography hides the data underneath other data without any differentiable changes. Many individual steganography tools can be used to transfer data securely and, in this paper, a new tool is proposed that decreases time and energy. Using this tool, we hide the text in audio, video, or images in one place, so there was no need to have access to multiple tools. This proposed tool developed using the Least Significant Bit (LSB) approach.*

Keywords: Steganography, Least Significant Bit, Android, RGB

1.INTRODUCTION

Steganography provides secrecy of text or images to prevent them from attackers. Steganography engraft the message image duringa cover image and changes its properties. Steganography provides secret communication in order that intended hacker or attacker unable to detect the presence of message. To prevent the detection of secret messages is the major art of steganography. It includes a vast array of secret communications strategies that conceal the message's terribly existence. These strategies include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum [1].

The development of data communications enabling the Exchange of information via mobile devices more easily. Security within the exchange of information on mobile devices is extremelyimportant. One of the weaknesses in steganography is the capacity of data that can be inserted. With compression, the size of the data will be reduced[2].

In this paper, designed a system application on the Android platform with implementation of LSB steganography and cryptography using TEA to the protectionof a text message. The size of this text message may be reduced by performing lossless compression technique with help of LZW method. The benefits of this technique is will give double security and more messages to be inserted, so it is expected be a good way to exchange information data.

1.1. Problem Statement

In gift technique, user sends data from one system to the desired system in native space Network. Because of the security issues not only authorized persons but also unauthorized persons can access data.

2.LITERATURE SURVEY

This work is concerned with implementing Steganography for images, with associate improvement in each security and image quality. The one that is implemented here is a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality is improved by bit-inversion technique. In this technique, least significant bits of canopy image are inverted after LSB steganography that co-occur with some pattern of other bits and that reduces the number of changed LSBs.

In paper [1], associate improvement within the plain LSB based image steganography is proposed and implemented. The paper proposes the use of bit inversion technique to improve the stego image quality. Two schemes of bit inversion techniques are given and implemented. In these techniques, LSBs of some pixels of canopy image are inverted if they occur with a particular pattern of some bits of the pixels. In this way, less variety of pixels is changed in comparison to plain LSB method. So PSNR of stego image is improved. For accurate de-steganography, bit patterns for which LSBs has inverted must be hold on at intervals the stego image somewhere. The proposed bit inversion technique provides good improvement to LSB steganography.

In paper [2], steganography technique using Daubechies Discrete Wavelet Transform (DWT) is enforced. First the cover image is reworked with the help of DWT and secret information is embedded in coefficients of Daubechies

DWT which gives stego image. Reverse process is applied to obtain secret information from stego image.

In paper [3], introduces a best approach for Least Significant Bit (LSB) based on image steganography that improvestheexisting LSB substitution techniques to boost the protection level of hidden information.It is a new approach to substitute LSB of RGB true colour image. The new security conception hides secret information at intervals the LSB of image where a secret key encrypts the hidden information to protect it from unauthorized users.

3. PROPOSED SYSTEM

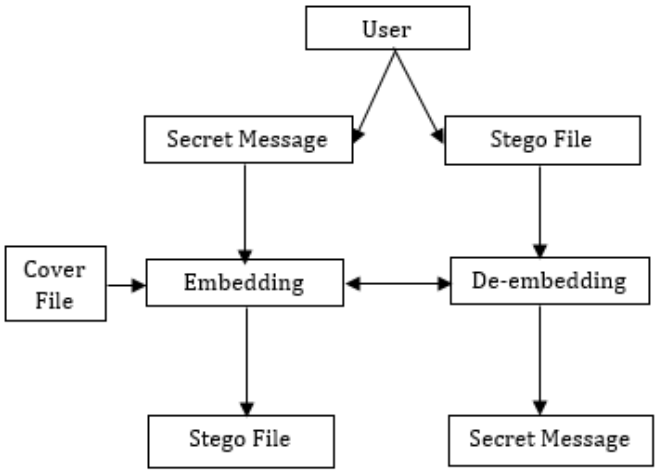

Fig-1: Architecture of Steganography

The basic concept is that it has a cover object that is used tocover the original message image, a host object that is themessage which is to be transmitted, a stego-key which is used to hide the message image into cover image, and the steganography algorithm to carry out the specified object. The output is an image called stego-image which has the Message image inside it, hidden. This stego image is then sent to the receiver where the receiver retrieves the message image by applying the de-steganography.

4. OBJECTIVE

The objective of this project is to hide the existence of secret text in digital files from everybody, except the sender and receiver. The objective of this project can be achieved by using the least significant bit (LSB) algorithm for hiding text in digital files. Then the sender and receiver will use this tool to hide and extract the secret text in digital files.

5. FUTURE SCOPE

Future work includes experimentation with a wider range of images with high quality and more optimised one. Also to sustain the message even after the alteration createdwithin the cover image like cropping, resizing etc. The future work on this project is to improve compression ratio of image to the text. This project can be extended to a level such that it can be used for the different types of image formats like .bmp, .jpeg, .tif etc., within the future. The protection using Least Significant Bit Algorithm is good but we can improve the level to a certain extent by varying the carriers as well as using different keys for coding and secret writing. Future implementations will improve the research related works which may be exhausted relevance all on top of referred approaches like DCT. This will include implementation of DCT which is more suitable for formats like jpeg and mpeg. DCT implementation will provide working with wider range of images with less calculation. It involves fewer calculations owing to FFT algorithmic program employed in it.

6.CONCLUSION

This research introduces a new tool. This recently developed steganography tool is used for embedding and de-embedding digital files. For this project, confidential data was secured by using the least significant bit (LSB) algorithm. LSB coding is one of the simplest ways to embed information in digital files because it replaces LSB with the message to be encoded. The secret message is embedded into a digital file with a key file that generates a stego-file. The digital file can be image, audio, or video, and a stego-file combines the secret message and digital file. The key file is common for hiding and extracting the secret message. At the time of extraction, we gave the stego file and key file, each of which de-embedded and displayed the secret message. In general, this tool allows users to hide secret text in digital files and extract the same secret text from those digital files. The tool can be used to hide a secret message from hackers while transferring the message among users. A user with some basic information will use this tool either as a sender or as a receiver. Some test cases are performed for each hiding and extracting the secret message in image, audio, and video. This demonstrates that mistreatmentthis tool can do the confidentiality of secret data.

7.REFERENCES

[1] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, "Enhancing the Security and Quality of LSB based Image Steganography".
[2] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, "An Improved Inverted LSB Image Steganography".

[3] Ajaya Shrestha, Dr. Arun Timalsina, "Color Image Steganography Technique Using Daubechies Discrete Wavelet Transform".
[4] "A steganography implementation" by Mehboob, Faruqui.
[5] S.M Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography Using Secret Key".
[6] Dalila Boughaci, Abdelhafid Kemouche and Hocine Lachibi LRIA-USTHB,"Stochastic Local Search Combined with LSB Technique for Image Steganography".