IMAGE STEGANOGRAPHY

S. Venesh
Student/ Department of CSE, ACGCET, KKD, Tamil Nadu, India

Dr. C. Uma Rani
Faculty/ Department of CSE, ACGCET, KKD, Tamil Nadu, India

Abstract

Steganography is the art and science of writing hidden messages in such a way that no one apart from sender and intended recipient even realizes there is a hidden message. There are often cases when it is not possible to send messages openly or in encrypted form. Steganography is intended to provide secrecy. The main aim of steganography is to hide the secret messages and also for communication transferring of data. Steganography authorized sender and receiver will be aware of existence of secret data. This paper intends to give the an overview of image steganography and its use hiding the data or files like text, audio etc, Steganography use LSB and AES algorithm where AES used for password protecting system and LSB use for hiding the data, this password hiding system can be in the several forms. Audio, thumb impression, iris based etc,… which all can be initiated, but the proposed work hides password in multiple occurrences in an image where no one can detect their presence.

Keywords: *Least significant algorithm, AES algorithm, Process, Hiding information.*

Introduction

In the modern world communication is important to us, so the steganography is important way of communication to pass the secret things one person to another one. The word Steganography literally means “covered writing”. It is a combination of the Ancient Greek word “STEGOS” meaning cover and “GRAFIA” means writing. Steganography is art of the and science of invisible communication. This is the hiding information, thus hiding the existence of the communicated information. It hides the existence of the data. It is one of the methods to protect the sensitive data from malicious attack.

It replaces unneeded or unused bits in the regular computer files. It is used send or receive the invisible information. Steganography techniques can be applied to Images, video file, audio file, and etc,. At the technology compare with steganography it protects the information from pirating copyrighted materials as well as aiding in unauthorized viewing. There are five types of steganography they are

- TEXT steganography
- IMAGE steganography
- AUDIO steganography
- PROTOCOL steganography
- VIDEO steganography

Steganography popularly used some programming languages they are

- C#,
- JAVA,
- PYTHON
- MATLAB

Steganography Process

Image as a Carrier

It is an efficient technique for steganography, an image is uses as cover for hiding the actual data. Digital image are preferred media for hiding information due to their high capacity and low impact in visibility**.**

Pixels Representation in RGB

Basic RGB colour model, every pixels are represented by off bytes namely as ALPHA (degree formation of transparency& Alpha bit is used to carry the data as it has no much importance in image representation), RED (Intensity of red colour), GREEN (Intensity of green colour), BLIUE (Intensity of blue colour),.

Bandwidth Reduced File Transfer

If an image data takes 6- min to transfer the data, between two system and text files takes 3-min.One can use steganography technique embedding the text in the image and the total content will be transferred in 6-min.Basic algorithm used for the main purpose in the image steganography they are Text on Image algorithm.

Literature Survey

We referred to a few previously published papers that had relatively to similar objective as most of the publishers are used the different languages .some of the codings from the differ language not apt for now a days. So we new technique to achieve the goal with time efficient manner. Most of the paper focused on same thing with different substitution of algorithms.

OPAP reduces the distortion caused by the LSB substitution method. The pixel value is adjusted after the embedding of the secret information is done, to get better quality of the stego image without disturbing the data embedded [1]. This is very Simple methodology and Easy to retrieve.

This IP LSB substitution approach uses pre processing of the secret information. In this method for each section of secret images it is determined whether it is to be inverted or not before it is embedded. In addition, the bits which are used to record the transformation are treated as secret keys or additional bits to be re-embedded [2].

The number of insertion bits is dependent on whether the pixel is in an edge area or smooth area. In edge area, the difference between the adjacent pixels is more, whereas in the smooth area it is less as human perception is less sensitive to subtle changes in edge areas of a pixel [3].

Proposed Work

Images are the most popular form to hide the data. Steganography is writing hidden messages in such away that no one apart from sender and intended recipient even realizes there is a hidden message. In this process an image is taken and secret messages is set in that image and is passed to the sender. The sender can then extract the information from the image using the key provided by the sender. The work proposed is to encrypt and decrypt the data with the password protected for encryption and decryption. But if the third party get stegano image it will never decrypt because it is password protected and data still is in the form of audio file can also be embedding to a image is increased due to the present in the image but that will be negligible. But the important thing is that if the size of data is greater than the size of image, it will never be hide in image.

In order to understand the process by which information is hidden within a image, Stegno analysis, one must understand the various terms to describe the different components. Different sources use various terminologies to refer to the same components and these are most commonly used. The fig 1 shows that the block diagram for proposed system.

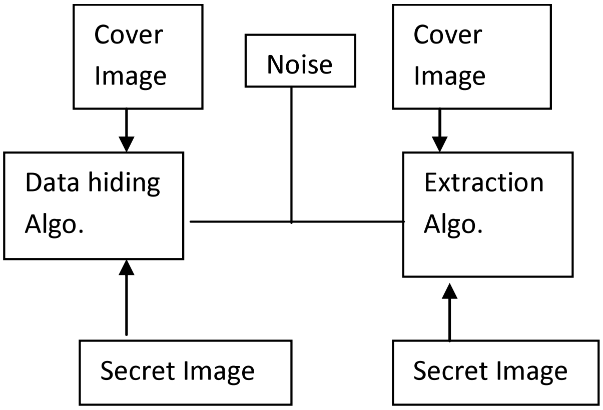


Fig 1: Proposed System

Experiments and Results

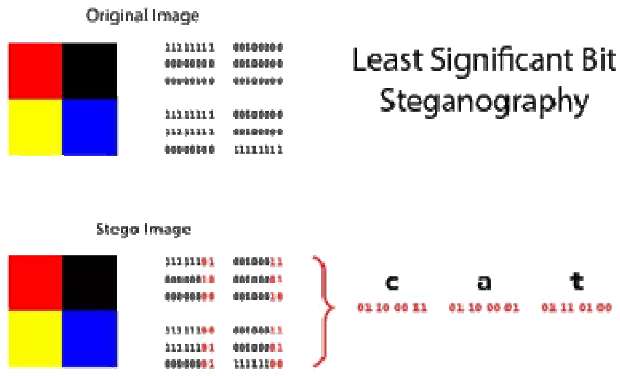
There are several different techniques for concealing data inside of normal files. One of the most widely used and perhaps simplest to understand is the lab technique, known commonly as LSB. This technique changes the last few bits in a byte to encodea message, which is especially useful in something like an image, where the red, green, and blue values of each pixel are represented by eight bits (one byte) ranging from 0 to 255 in decimal or 00000000 to 11111111111 in binary. The Main component is called the MESSAGE Changing the last two bits.

Least Significant Bit (LSB)

LSB is technique or method in encrypting and decrypting the secret information. LSB method is based on altering the redundant bits that are least important with the bits of the secret information. The aim of the LSB is to transmit the secret information to the receiver without knowing to the intruder that the message is being passed. The least significant bit (in other words, the 8th bit) of the bytes inside an image is changed to a bit of the secret message. Digital images are of two types (i) 24 bit images and (ii) 8 bit images.

In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden.

A stego-image is obtained by applying LSB algorithm on both the cover and hidden images. The hidden image is extracted from the stego-image by applying the reverse process then have 16 bits. If the LSB of the pixel value of cover image C (i, j) is equal to the message bit m of secret massage to be embedded,

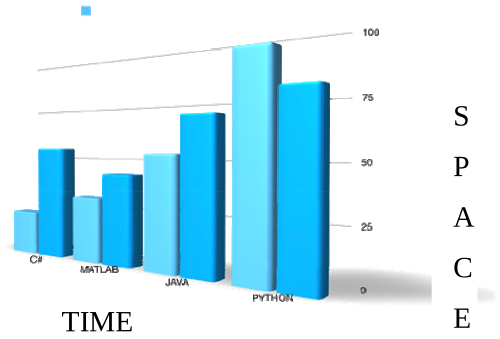


C(i, j) remain unchanged; if not, set the LSB of C(i, j) to m.

S(i, j) = C(i, j) - 1, if LSB(C(i, j)) = 1 and m = 0 S(i, j) = C(i, j), if LSB(C(i, j)) = m S(i, j) = C(i, j) + 1, if LSB(C(i, j)) = 0 and m = 1

where LSB(C(i, j)) stands for the LSB of cover image C(i, j) and m is the next message bit to be embedded. S(i, j) is the stegano image already know each pixel is made up of three bytes consisting of either a 1 or a 0.

This statistics represents time and space complexity year by year because of their efficient algorithm with efficient coding from programming language. This based upon the improvement of the technology in day by day.



Conclusion & Future Scope

Implementation of Image Steganography is very useful to our NATION for some security reason to transfer the data without seeing of third party. In this paper LSB method is used for Image Steganography with implementation of efficient programming language PYTHON.

Future enhancement to improve the password techniques with sensors like thumb impression, voice control, iris scanner it's better thing to save time complexity and protect from the hackers in technique of steganography.

Acknowledgement

We hereby show our gratitude to our college. "Alagappa Chettiar Govt. College of Engineering and Technology". We are using this opportunity to prove and improve ourself. We should like to extend our gratitude to the TEQIP-Ⅲ (a world bank assisted project through NPIU, New Delhi) which provided us with great financial support for us through the endeavor through this work.

References

1. Chan, Chi-Kwong, and Lee-Ming Cheng. "Hiding data in images by simple LSB substitution." Pattern recognition 37, no. 3 (2004): 469-474.
2. Yang, Cheng-Hsing. "Inverted pattern approach to improve image quality of information hiding by LSB substitution Pattern Recognition 41, no. 8 (2008): 2674-2683.
3. Sancheti, Ankita. "Pixel Value Differencing Image Steganography Using Secret Key." International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN (2012): 2278-2284.
4. Simmons, Gustavus J. "The prisoners' problem and the subliminal channel." In Advances in Cryptology, pp. 51-67. Springer US, 1984.
5. Mohammeda, Arifullah, Kin-Ying Wonga, Paritala Vikrama, Kishore K. Chiruvellab, and Arifullah Mohammed. "Phytochemical Screening and Antimicrobial Potentials of Borreria sps (Rubiaceae)." (2014).
6. Hussain, Mehdi, and Mureed Hussain. "A survey of image steganography techniques." (2013).
7. Dhand, Geetika. "Information Hiding Techniques." In proceeding of the national conference: INDIAcom-2008.
8. Swanson, Mitchell D., Bin Zhu, and Ahmed H. Tewfik. "Robust data hiding for images." In Digital Signal Processing Workshop Proceedings, 1996., IEEE, pp. 37-40. IEEE, 1996
9. Robinson, Jonathan, and Vojislav Kecman. "Combining support vector machine learning with the discrete cosine transform in image compression." IEEE Transactions on Neural Networks 14, no. 4 (2003): 950-958.