ISSN 2395-1621

Security For Message By Combining Steganography and Visual Cryptography

[#1]Prof. J.S.Kharat, [#2]Komal Shedge, [#3]Mamta Dharukar, [#4]Prajakata Sonwane, [#5]Karishma Shaikh

[1]kharat.jyo@gmail.com
[2]shedgekomal29@gmail.com
[3]prajaktasonawane978@gmail.com
[4]mamtadharurkar77@gmail.com
[5]shaikhkarishma77@gmail.com

[#12345]Department of Computer Engineering
JSPM NTC, Savitribai Phule Pune University
Pune-411030 India

ABSTRACT

Steganography is one of the art of hiding the fact that communication is taking place, by hiding information in other information such as images, videos, messages etc. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. In this paper we will discuss how digital images can be used as a carrier to hide messages. This paper also analyses the performance of some of the steganography tools. It is a useful tool that allows covert transmission of information over an over the communications channel. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This project intends to give an overview of image steganography, its uses and techniques. For a more secure approach, the project encrypts the message using secret key and then sends it to the receiver. The receiver then decrypts the message to get the original one.

Keywords: SI, DWT, PSNR, MSE.

ARTICLE INFO

Article History

Received: 24th May 2017

Received in revised form :

24th May 2017

Accepted: 27th May 2017

Published online :

27th May 2017

I. INTRODUCTION

Steganography is technique of hiding a file, message, image, or video within another file, message, image, or video. The difference between steganography and cryptography is that in cryptography, one can tell that a message has been encrypted, but he cannot decode the message without knowing the proper key. On the simplest level, steganography is private writing, whether it consists of hidden ink on paper or copyright information invisible in an image file. Where cryptography rush a message into a code to ambiguous its meaning, steganography hides the message entirely. These two secret communication technologies can be used differently or together for example, by first encrypting a message, then hiding it in another file for transmission. Internet users frequently need to store, send, or receive private information in the database. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. A major disadvantage to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually unencrypt the data. A solution to this problem is steganography. The obsolete art of hiding messages so that they are not detectable. No substitution or permutation was used. The hidden message is plain, but unsuspecting to the reader. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood. As the world becomes more anxious about the use of any secret communication, and as regulations are created by governments to limit uses of encryption, steganography's role is gaining prominence. The basic terminologies used in the steganography systems are: the cover message, secret

message, the secret key and embedding algorithm [5]. The cover message is the carrier of the message such as image, video, audio, text or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually used to embed the secret information in the cover message [8][9]. In steganography, before the hiding process, the sender must select an appropriate message carrier, an effective message to be hidden as well as a secret key used as a password. A robust steganography algorithm must be selected that should be able to encrypt the message more effectively. The sender then may send the hidden message to the receiver by using any of the modern communication techniques. The receiver after receiving the message decrypts the hidden message using the extraction algorithm and a secret key. This paper proposes a new algorithm to hide data inside an image using steganography technique. The algorithm that we have proposed is an enhanced version of LSB technique that is not very much robust. Also we have implemented a compression technique to increase the hiding capacity.

II. PROPOSED SYSTEM

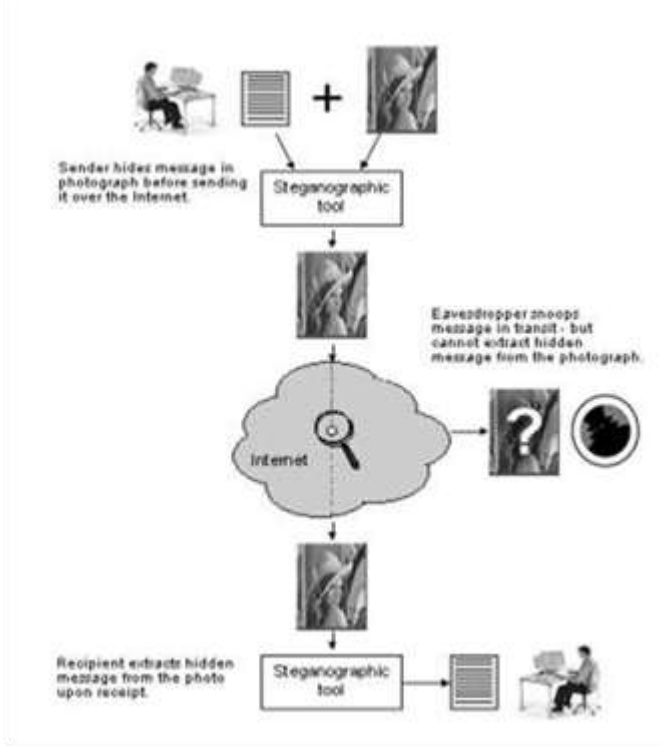

Fig no 1 : System Architecture

This system is able to send and receive encrypted messages embedded inside images. The user is able to choose the image he wants and the program must tell if this image will suit the text or not. No pixel deformation or size distortion is allowed. TIF image**s** may suffer slight size increments or decrements, but we will get to that later. The user can set a different password for every message he sends, which will enable the manager to transmit the same image to two groups, but with two different passwords and two different messages. Encrypting data has been the most popular approach for protecting information but this protection can be broken with enough computational power. An alternate approach to encrypting data would be to hide it by making this information look like something else. In this way only concern receiver would realize its true content. In particular, if the data is hidden inside of an image then everyone would view it as a picture. At the same time receiver could still retrieve the true information. This technique is often called data hiding or steganography. For implementing steganography the images which are collection of pixels should be in a proper format. For this purpose image processing is done to convert the required image in proper format. Image processing usually refers to digital image processing. Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame.

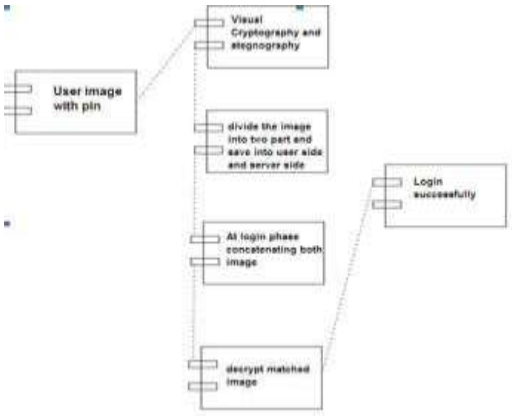

Fig No 2 Component Diagram

A Component diagram depicts how components are wired together to form larger components or software system**.**
In this diagram the user image in combined with visual Cryptography and steganography then images id divided into two part and save into two side one is user slide and another is server side. When user login into system the divided images is concatenating after that it decrypt the images and loin is successful.

III. ALGORITHMS

Algorithm to embed text message:

Step 1: Read the cover image and text message which is to be hidden in the cover image.

Step 2: Convert text message in binary.

Step 3: Calculate LSB of each pixels of cover image.

Step 4: Replace LSB of cover image with each bit of secret message one by one.

Step 5: Write stego image

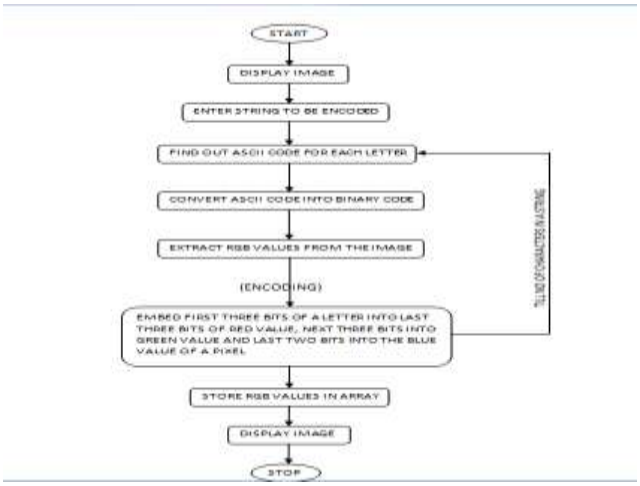

Figure No 3: FLOWCHART

IV. RESULTS

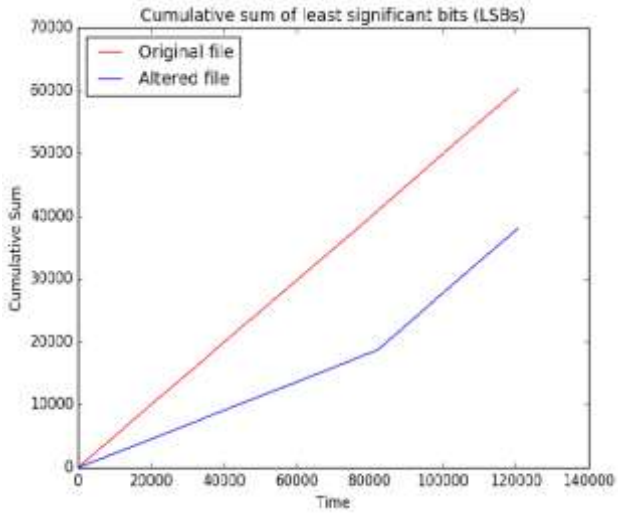

Fig no 4: Result

This result defined as two respective dimentions that is Time and Cumulative Sum , Time indicates as a flow of execution (as a original file) from 0-140000 and Cumulative sum (as a altered file) of least significant bit (LSB) and its defined range from 0-70000 . The basic terminologies used in the steganography systems are: the cover message, secret message, the secret key and embedding algorithm. In this Paper Original file consist of name of the person or his/her personal information and altered file is consist of the modified image. In the previous paper used a Blowfish Algorithm with JPEG image format but in this paper used Blowfish as well as LSB algorithm with PNG image format, with the help of this we can achieve the better result for security purpose.

V. CONCLUSION

In this project, the system contains Steganography technique for JPEG images. Firstly the system consist basic LSB technique that allows hiding information in JPEG images by using the least significant bits of pixels. This systems found that with LSB steganography method is not effective to hide information in the JPEG image because the size of the image increases greatly after inserting information which facilitates the discovery of the hidden information.

FUTURE SCOPE

This can be further extended to have support for the Video files. Currently, for encoding, the system use this software and for transmission This system use some other medium. So the current software can itself be used to transmit the files also. Currently, the length of the message file has some limitations for the Audio Steganography, so for the same, we can have support for a wider size of files. Can be implemented as a plugin to a web browser.

ACKNOWLEDGEMENT

We would like to thanks S. Arjun, and A. Joseph and T. Narasimmalou, referees for their very useful comments and suggestions on earlier versions of the manuscript. Their We would like to thanks S. Arjun, and A. Joseph and T. Narasimmalou, referees for their very useful comments and suggestions on earlier versions of the manuscript. Their input has led to an improved version of the paper. The satisfaction that accompanies the successful completion of any task would be incomplete without mentioning the people who made it possible. We are grateful to a number of individuals whose professional guidance along with encouragement have made it very pleasantendeavor to undertake this project. . We have a great pleasure in working project Security for Message by Combining Steganography and Visual Cryptography in Steganography under the guidance of Prof.J.S.Kharat. We are truly thankful and grateful to all people for their valuable guidance and also encouragement. We take an opportunity to thank all the staff members of our department.

REFRENCES

[1] S. Arjun, (2007), An approach to adaptive steganography based on matrix embedding ; Univ. Coll. of Eng. (A), Hyderabad ;Negi, A. ; Kranthi, C.; DivyaKeerthi TENCON 2007 - 2007 IEEE Region 10 Conference.

[2] D. Boughaci, B. Benhamou, H. Drias , (2010): ”Local Search Methods for the optimal winner determination problem”, in Journal of Mathematical modelling and Algorithms (Springer), volume 9, Issue 2 (2010), pp:165-180, June 2010.

[3] B. G. Banik and S. K. Bandyopadhyay, “A DWT Method for Image Steganography”, International Journal of Advanced Research in Computer Science and Software Engineering, 2013

[4] A. Joseph and T. Narasimmalou, “Optimized Discrete Wavelet Transform based Steganography”, IEEE Interational Conference on Advanced Communication Control and Computing Technologies, 2012 Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (UERA), Vol. 2, Issue 3, pp. 338-34 1,2012.

[5] Kevin Curran, Karen Bailey, "An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence, Vol. 2, Issue 2, pp. 1-40,2005.

[6] K.B. Raja, C.R. Chowdary, Venugopal K R, L.M. Patnaik, "A Secure Image Steganography using LSB, OCT and Compression Techniques on Raw Images", IEEE International Conference on Intelligent Sensing and Information Processing (ICISP), pp. 170-17 6, December 2005.

