IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 27-28

A review on Security Issues in image Steganography

A.Aarthi Devi
MSC Computer Science, PG Department of Computer Science, Tamil Nadu

Abstract: *Using image stitching and image steganography security can be provided to any image which has to be sent over the network or transferred using any electronic mode. There is a message and a secret image that has to be sent. The secret image is divided into parts.The first phase is the Encrypting Phase, which deals with the process of converting the actual secret message into cipher text using the AES algorithm. In the second phase which is the Embedding Phase, the cipher text is embedded into any part of the secret image that is to be sent. Third phase is the Hiding Phase, where steganography is performed on the output image*
Of Embedding Phase and other parts of the image where the parts are camouflaged by another image using least significant bit replacement. These individual parts are sent to the concerned receiver. At the receivers end decryption of Hiding phase and Embedding Phase takes place respectively. The parts obtained are stitched together using k nearest method. Using SIFT features the quality of the image is Improved.
Keywords: *Cryptography, image steganography, image stitching.*

I. Introduction

In present time security is major concern while transmitting any message over a network. Network security is not sufficient as cyber crime is increasing therefore other method is used for providing security. Security provided to image using image steganography and stitching is beneficial.AES algorithm is used to encrypt text message and embedded in a part of the image the text message is difficult to find. Image is divided into parts and then sent to the receiver. This Makes it difficult to get access to all the parts of the image at once therefore it become highly difficult for the invader to decode the document. There is no limitation on the image format that can be used. The image can be gray scale or colored but the size of the message needs to be of only 140 characters.

Steganography

Steganography is a Greek word which means concealed writing. The word "steganos" means "covered " and "grapy " means "writing" . Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, and stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia objects like audio, video, images are used as a cover sources to hide the data.

Text steganography

It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are
o Format Based Method
o Random and Statistical Method
o Linguistics Method

Image steganography

Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

II. Network or protocol steganography

It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc. as cover object. In the OSI layer network model there exist covert channels where steganography can be used.

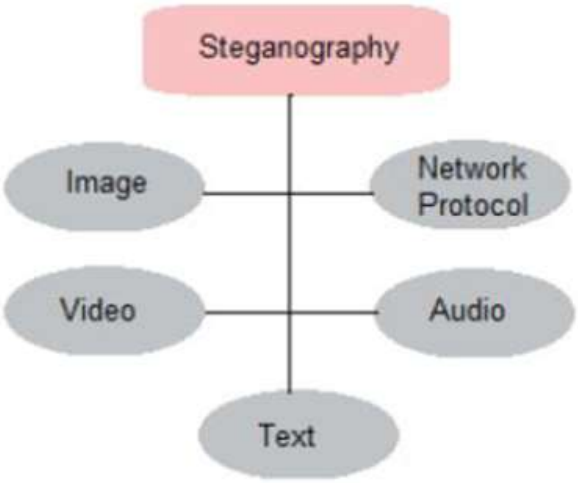

Fig. 1 Steganography types

III. Existing system

Various systems are available for information hiding in an image, but they have some drawbacks i.e., they either do not encrypt the message or use a very weak algorithm in order to perform cryptography. They use the same key for encryption and decryption making it easy for the invader to get access of the information. In some other cases the technique used may not be very efficient that is, the original image and the resulting image will be easily distinguishable by naked human eyes. For example DES algorithm, an encryption algorithm, and used keys of smaller sizes (64 bit key) hence it was easy to decode it using computations. Algorithms using keys of these sizes are easily cracked by any intruder. So it is better if one goes for algorithms using keys of larger size which are difficult to decrypt and provide better security. Where stitching is concerned, multiband blending, gain compensation, automatic straightening makes the image smooth and more realistic

IV. Conclusions

This paper has presented a novel system for data and image encryption using AES algorithm for cryptography, image steganography and image stitching which can be used by banking, consultancies and detective agencies. It has put forth a new system which combines text cryptography and image Steganography which could be proven a highly secured method for data transactions in the near of the image to be sent is broken down into parts and encrypted individually and sent over the network it becomes difficult of the invader to get access of all the parts. Additionally since every part is camouflaged by a cover image, the encrypted image looks like just another regular image. Thus fooling the invader with the help of invariant local features and a probabilistic model for image matching purpose in image stitching, allows us to recognize multiple panoramas in unordered image sets, and stitch them fully automatically without user input. With the help of SIFT features and RANSAC algorithm the output of the image is rectified and we get a smooth image. This image can also be used as a password to open a document of a file.

References

[1]. ”Automatic Panoramic Image Stitching using Invariant Features”, Matthew Brown and David G.Lowe of Computer Science, University of British Columbia, Vancouver, Canada.

[2]. ”High payload using mixed codebooks of Vector Quantization”, H. B. Kekre, Tanuja K. Sarode,ArchanaAthawale, KalpanaSagvekar

[3]. ”H.B.Kekre,ArchanaAthawale and Pallavi N.Halarnkar,”Performance Evaluation of Pixel Value Differencing and Kekre’s Modified Algorithm for Image Hiding in Images”,ACM International Conference on Advances in Computing,Communication and Control(ICAC3)2009.