Data Hiding in encrypted Image by DWT

Dr. Vivek Sharma[1], Hariom C. Agnihotri[2]
Head , Deptt of CSE[1], Research Scholar[2]
VNS Institute of Technology sharma.vivek95@yahoo.in[1],
hagnihotri2011@gmail.com[2]

Abstract:

Steganography is the skill of hiding the existence of data in other transmission medium to attain secret communication. It does not restore cryptography but quite boost the security using its obscurity features.

We have proposed a Steganography technique in this paper.

Biometric characteristic used to apply steganography in images. Here important data is implanted within image which will give an outstanding secure location for data hiding.

Different steps of data hiding can be applied by cropping an image interactively. With the help of cropping an improved security than hiding data without cropping the whole image, so cropped region works as a key at decoding region. So with this object oriented steganography we track area of given images with the higher security and satisfactory PSNR.

Modern steganography goal is to keep its mere presence undetectable.

Encoding and decoding process for the conversion of original image to stego image and vice versa can be implemented using BASE 64 algorithmic strategies.

Keywords: DWT, classifier, data hiding, steganography, digital watermarking, BASE 64

I. INTRODUCTION

1.1 Steganography

Steganography is the skill and science of writing hidden messages in such a way that no one, apart fro the sender and receiver, suspects the survival of the message, a form of security through obscurity.

Fig 1.1 Steganography

The advantage of steganography as compared to cryptography is that messages do not draw awareness to themselves. Whereas cryptography protects the contents of a message, steganography can protect both messages and communicating parties.

1.2 Data Hiding

In computer field , information hiding is the standard of separation of the *design decisions* in a computer program that are most likely to change, thus shielding other parts of the program from extensive alteration if the design decision is changed. The shields involve providing a steady interface which secures the rest of the program from the implementation. Data hiding is a software development technique specifically used in object-oriented programming to hide internal object details. Data hiding ensure limited data access to class members and secures object's integrity by preventing accidental or planned changes.

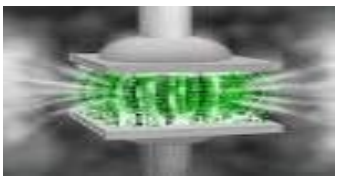

Fig1.2 Data Hiding

II. INTORDUCTION TO STEGANOGRAPHY

2.1 Introduction

In Steganography secret message is the data that the sender needs to remain confidential.

The host is the medium in which the message is implanted and serves to hide the presence of the message.

A **digital watermark** is a type of indicator secretly implanted in a noise-tolerant signal such as audio or image data. It is classically used to recognize ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal.

2.2 Digital Water marking

Both steganography and digital watermarking use steganographic techniques to implant data secretly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority.

Fig 2.1 Digital Watermarking

2.3 DWT technique

Digital Data is available in World Wide Web in the form of Images, Audio and video in large amount. It is very easy to copy, distribute, modify, manipulate and destroy by the intruders, So there is a great need to protect the integrity of the digital data, The technique that is useful to avoid unauthorized copying or tempering of digital data is Watermarking. Digital watermarking is used for protection of digital images. Secret data can be hidden in one of the high frequency sub-band of DWT by tracing pixels present in the given image. Different steps of data hiding can be applied by cropping an image interactively. Cropping results into an enhanced security than hiding data without cropping i.e. in whole image, so cropped region works as a key at decoding side.

This is another frequency domain in which steganography can be implemented. DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifacts. This drawback of DCT is eliminated using DWT.DWT applies on whole image. DWT offers better energy compaction than DCT without any blocking artifact. DWT splits component into numerous frequency bands called sub bands known as

- LL – Horizontally and vertically low pass
- LH – Horizontally low pass and vertically high pass
- HL - Horizontally high pass and vertically low pass
- HH - Horizontally and vertically high pass

An image can be decomposed into a pyramid structure with various band information.

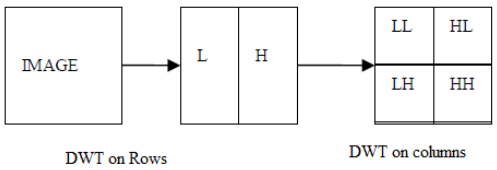

Fig 2.2 DWT Decomposition

DWT coefficients, the original signal can be reconstructed. This process is called the inverse DWT (IDWT).

The DWT and IDWT for two dimensional images z[m,n]can be defined by:

DWTn [DWTm[x [m, n]]]

2.4 BASE 64 Encryption Scheme

In cryptography, **encryption** is

the procedure of encoding messages in such a way that unauthorized user cannot read it, but only authorized parties can.

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

Fig 2.3
Encryption

Base64 is an encoding algorithm used to change text and binary streams into printable and easy-to-process form to be consumed by various programs as well as transmitted over the network.

Base64 encoding is generally achieved by splitting a stream or block of data into 6-bit fragments and interpreting each fragment as the position in the following series of characters.

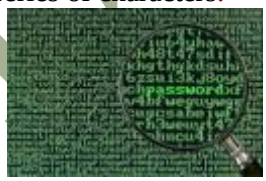

Fig 2.4 Encryption on series of characters

After the Base64 encoded block is obtained it is ready to be processed, or transmitted, for example for MIME content transfer encoding used in email transmission.

Base64 decoding employs a reverse algorithm to yield the original content. While Base64 encoding alters the original content, it is not suitable as an encryption mechanism as it can be easily decoded to reveal the original content. For that there are various encryption algorithms and products to be used. PGP is one of the better known encryption products.

IV.RESULT AND ANALYSIS

After we have derived the descriptive results, the next job is to deliver the results of any statistical analysis that have been performed on the data. There are separate resolutions about how our analysis should be labeled. The simple design is as follows: firstly the data being analyzed is outlined, and then the statistical analysis is performed. After this the actual results in every figure of the analysis are given:

Following is the home page of our application which is specifying various options like compression, encryption, and vice versa. We are specifying compressed matrix for the image and also for the original image. “Browse” option is provided to select the image, and then the same selected image will get loaded into the application. Where we wish to perform the various operations like encryption and compression.

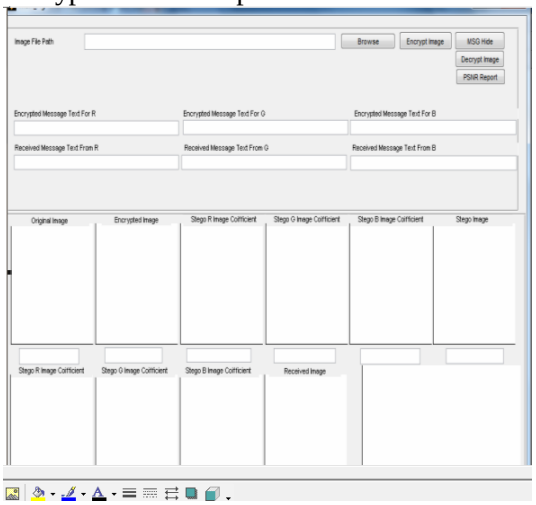

Fig 4.1 Home page of an application

For the purpose of encryption we are providing the key value by using which image will be encrypted. Also we are providing the message to be hidden into the image.

As soon as image is loaded into the application, after providing the key value we are encrypting the image. Then this encrypted image will be used for compression purpose.

Snapshot depicts the same as we are selecting an image for further operations.

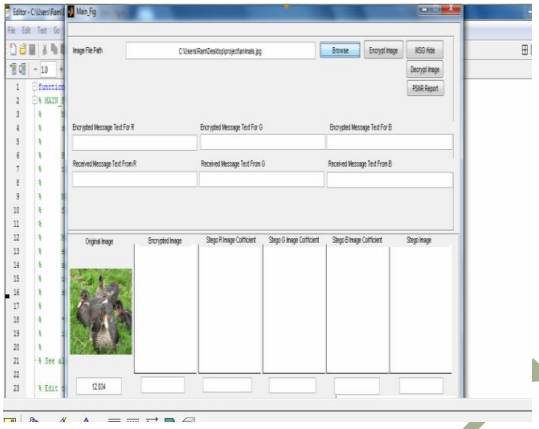

Fig 4.2 Browsing for selection of an Image

Any opponent that can see the cipher text should not be able to control anything about the original message. An authorized person, however, is capable to decipher the cipher text using a decryption algorithm that typically needs a secret decryption key that opponents do not have access to. For technical explanations, an encryption system usually desires a key-generation algorithm to randomly produce keys.

In field of computer science, information hiding is the source of separation of the *design decisions* in a computer program that are most likely to alteration, thus guarding other parts of the program from wide adaptation if the design decision is altered. The defense involves providing a steady interface which protects the rest of the program from the implementation.

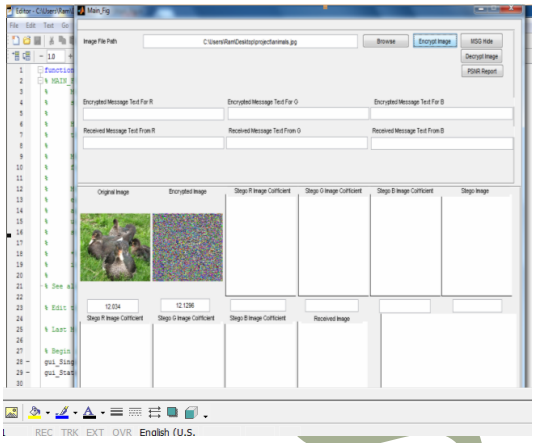

Fig 4.3 Encrypted Images

In below figure any unauthorized user cannot read the message unless provides the required the key value. After providing the key value only it will possible for user to retrieve the message. **Data extraction** is the act or procedure of retrieving data out of sources for further data processing or data storage. The introduction into the intermediate mining system is thus typically followed by data transformation and possibly the addition of metadata prior to export to another stage in the data workflow.

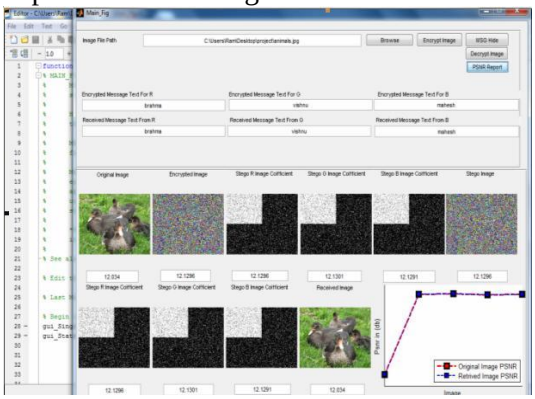

Fig 4.4 decryption of an image and PSNR

Above figure shows the decryption of image for extracting the original image. Reverse case is there to be performed to retrieve the original image at the receiver side.

Decryption is the procedure of taking encoded or encrypted text or other data and altering it back into text that system is able to read and understand. This term

could be used to define a technique of decrypting the data manually by using the keys.

Some of the common objects those can be encrypted include email messages, text files, images, user data and directories. The person who is performing decryption receives a prompt message or key in which a password may be entered to access encrypted information.

In above snapshot we have calculated the **PSNR - Peak Signal to Noise Ratio** Standards in image data compression are the compression ratio and PSNR - Peak Signal to Noise Ratio-. The compression ratio is used to measure the capability of data compression by equating the size of the image being compressed to the size of the original Image.

The greater the compression ratio means the better the wavelet function. PSNR is one of the parameters that can be used to quantify image quality **Peak signal-to-noise ratio**, frequently abbreviated as **PSNR**, is an engineering term for the ratio between the supreme possible power of a signal and the power of corrupting noise that disturbs the loyalty of its illustration. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

CONCLUSION

At the end we can conclude that

after studying various aspects of the image steganography we have implemented the above mentioned application.

In this application we have use BASE 64 technique for encryption and decryption purpose. There are variety of techniques are available for data hiding in images but implemented this one and proved that how it is efficient and effective. . PSNR parameter is often used as a benchmark level of similarity between reconstructed image and the original image. Larger PSNR will produce better image quality[4].PSNR is one success measurement in image data compression. PSNR is used to quantify the image quality. The larger PSNR value means the better its wavelet function is, it means the reconstructed image is so much closer to the original image. Hence we have also proved that PSNR ration is improved successfully.

REFERENCES

1. Chirag Sharma, Deepak Prashar, DWT Based Robust Technique of Watermarking Applied on Digital Images, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012
2. Randy Charles Morin ,"**How to Base64"**
3. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Securing Information Content using New Encryption Method and Steganography"
4. Ch. Samson , V. U. K. Sastry2 An RGB Image Encryption Supported by Wavelet-based Lossless Compressio n
5. Ramchandra S. Mangrulkar1, Pallavi V. Chavan2," Encrypting Informative Image by Key Image using Hill Cipher Technique
6. Petitcolas, F.A.P.: "Introduction to Information Hiding". In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood:Artech House, INC
7. Johnson, N. F. and Jajodia, S.: "Exploring Steganography: Seeing the Unseen." IEEE

Computer, 31 (2): 26-34, Feb 1998.

8. Chang, C. C., Chen, T.S and Chung, L. Z., "A steganographic method based upon JPEG and quantization table modification," Information Sciences, vol.[4], pp. 123-138(2002).