DCT & DWT Based Secured Image Transmission Using Steganography

T. Yuvaraja M.E.,
Assistant Professor
Department of Electronics and Communication Engineering
Kongunadu College of Engineering and Technology
Trichy

C. Soundarya Devi, S. Sushmitha,
P. Uvarani, S. Kaviya
UG Scholars, Department of Electronics and Communication
Kongunadu College of Engineering and Technology
Trichy

***Abstract*:- Steganography is the technique of hiding private or sensitive information within the cover image. It is not a rule that we must hide data in image files only, we can also hide data in MP3 and Video files too. It involves hiding information, so it appears that no information is hidden at all. To securely communicate information between parities or locations is not an easy task considering the possible attacks or unintentional changes that can occur during communication. Encryption is often used to protect secret information from unauthorized access. The presence of encrypted information can also entice potential attackers to launch an attack on the secured communication. To achieve high security, the steganography technique is used to provide secrecy. It can be used anytime anywhere to hide data.**

Keywords—DCT,DWT,MSE,PSNR

INTRODUCTION

This template, modified in MS Word 2007 and saved as a "Word 97-2003 Document" for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

I. INTRODUCTION

1.IMAGE PROCESSING

Image processing is a physical process used to convert an image signal into a physical image. The image signal can be either digital or analog. The actual output itself can be an actual physical image or the characteristics of an image. The most common type of image processing is photography. In this process, an image is captured or scans using a camera to create a digital or analog image. In order to produce a physical picture, the image is processed using the appropriate technology based on the input source type. In digital photography, the image is stored as a computer file. This file is translated using photographic software to generate an actual image. The colors, shading, and nuances are all captured at the time the photograph is taken the software translates this information into an image. When creating images using analog photography, the image is burned into a film using a chemical reaction triggered by controlled exposure to light. The image is processed in a darkroom using special chemicals to create the actual image. This process is decreasing in popularity due to the opening of digital photography, which requires less effort and special training to product images. The field of digital imaging has created a whole range of new applications and tools that were previously impossible. Face recognition software, medical image processing and remote sensing are all possible due to the development of digital image processing. Specialized computer programs are used to enhance and correct image.

Applications of Digital Image Processing

- Image sharpening and restoration
- Medical field
- Remote sensing
- Transmission and encoding
- Machine/Robot vision
- Color processing
- Pattern recognition
- Video processing

II. DIGITAL IMAGE PROCESSING

Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subfield of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data, and can avoid problems such as the build-up of noise and signal distortion during processing.

In order to become suitable for digital processing, an image function f(x,y) must be digitized both spatially and in amplitude. Typically, a frame quantize the analogue video signal processing.

Image Acquisition

The first step in the process is image acquisition that is, to acquire a digital image. It highly requires an imaging sensor and the capability to digitize the signal produced by the sensor.

The sensor could be a monochrome or color TV camera that produces an entire image of the problem domain every 1/30 sec.

The imaging sensor could also a line-scan camera that produces a single image line at a time. In this case, the object's motion past the line scanner produces two dimensional image. If the output of the camera or other imaging sensor is not already in digital form, an analog to digital converter digitizes it. The nature of the sensor and image it produces are determined by the application.

Image Processing

The key function of preprocessing is to improve the image in ways that increase the chances for success of the other processes. Preprocessing typically deals with techniques for enhancing contrast, removing noise, and isolating regions whose texture indicate a likelihood of alphanumeric information.

Image Segmentation

The next stage deals with segmentation. Segmentation partitions an input image into its small constituent parts or objects. In general, autonomous segmentation is one of the most difficult tasks in digital image processing. On the one hand, a rugged segmentation procedure brings the process a long way towards the successful solution of an imaging problem. On the other hand, weak or erratic segmentation algorithm.

Image Representation and Description

The output of the segmentation stage usually is raw pixel data, constituting either the boundary of a region r all the points in the region itself. In either case converting the data to a form suitable for computer processing is necessary.

The first decision that must be made, whether the data should be represented a boundary or as a complete region. Boundary representation is appropriate when the focus is on external shape.

Image Recognition and Interpretation

Recognition is the process that assigns a label to an object based on the information is provided by its descriptors. Interpretation involves assigning meaning to an ensemble of recognized objects.

For example, identifying a character as say c requires associating the descriptors for that character with the label c. Interpretation attempts to assign meaning to a set of labeled entities. For example, a string of five numbers are followed by a hyphen and four more numbers can be interpreted to be a ZIP code.

Types of Digital Image

For photographic purposes, there are two important types of digital images: color and grayscale. Color images are made up of colored pixels while grayscale images are made of pixels in different shades of gray.

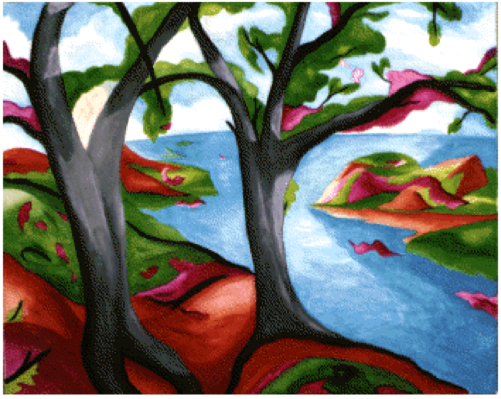
Grayscale Image

A grayscale image is made up of pixels, each of which holds a single number corresponding to the gray level of the image at a particular location. These gray levels span the full range from black to white in a series of very fine steps, normally 256 different grays. Assuming 256 gray levels, each black and white pixel can be stored in a single byte (8bits) of memory.

Fig 1.1 Grayscale Image

Color Image

A color image is made up of pixels, each of which holds three numbers corresponding to the red, green and blue levels of the image at a particular location. Assuming 256 levels, each color pixel can be stored in 3 bytes (24 bits) of memory. Note that for images of the same size, a black and white version will use three times less memory than a color version. characteristics, such as corners and inflections.



Regional representation is appropriate when the focus is on internal properties, such as texture or skeletal shape. In some applications, however, these representation coexist.

This situation occurs in character recognition applications, which often require algorithms based on boundary shape as well as skeletons and other internal properties.

III .HISTORY OF STEGANOGRAPHY

From the ancient times Steganography has carried out in different forms. It originated from the Greece, where initially the kings started sending secret messages written on the tablet covered by wax. The first recorded use of Steganography is from the Histories of Herodotus, where in ancient Greece text was written on wax covered tablets. Herodotus descri6bes how Demeratus wanted to warn Sparta on an imminent invasion from Xerxes.

Image Encryption

Encryption is the process of transforming a piece of information (known as the plaintext) using an algorithm (known as the cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as cipher text.

Type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles. Those are substitution, in which each element in the plain text is mapped into another element and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition.

The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender and the receiver each uses a different key the system is referred to as asymmetric, two key, or public-key encryption.

Confidentiality is the most common aspect of information security. It is not only applies to the storage of information, but also applies to the transmission of information. That means we need to conceal it during the transmission.

PSNR > 36 db, it means a human cannot differentiate between the original image and stego image.

Integrity

Information needs to be changed constantly. Integrity means that these changes need to be done only by authorized entities and through authorized mechanism. Integrity violation is not necessarily the result of a malicious act, an interruption in the system may also create unwanted changes in the information.

Availability

The third component of information security is availability. The information created and stored needs to be available to authorized entities. Information is useless if it is not available Information needs to be changed constantly, which means it must be accessible to authorized entities.

Data Hiding

Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted. This important technique is widely used in medical, military and law forensics, where no distortion of the original cover is allowed. Real reversibility is realized, that is, data extraction and image recovery are free of any error.

Decryption

The data extraction and image recovery proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in decrypted image. Hong ameliorated Zhang's method at the decoder side by further exploiting the spatial correlation using a different estimation and equation and side match technique to achieve much lower error rate. These two methods mentioned above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction. To separate the data extraction from the image decryption, Zhang emptied out space for data embedding following the idea of compressing encryption images. Compression of encrypted data can be formulated as source coding with side information at the decoder, in which the typical method is to generate the compressed data in lossless manner by exploiting the syndromes of a parity-check matrix of channel codes. The method is compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used at the receiver side is also the spatial correlation of decrypted images. All the three methods try to vacate room from the encrypted images directly.

Security Parameters

Mean Square Error

Mean Square Error measures the average of the squares of the errors or deviations that is, the difference between the estimator and what is estimated.

General steps to calculate the mean squared error from a set of X and Y values:

1. Find the regression line.
2. Insert your X values into the linear regression equation to find the new Y values (Y').
3. Subtract the new Y value from the original to get the error.
4. Square the errors.

5. Add up the errors.
6. Find the mean.

MSE is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Peak Signal to Noise Ratio

Peak signal to noise ratio, often abbreviated PSNR, is an engineering term for ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

WORKING

- In this existing system steganography methods are used for data hiding.

- This method encrypt the plaintext into the cipher text the meaningless random data of the cipher text may also arouse the suspicion from the attacker.
- In this existing system image compression process and the data hiding process are to independent modules on the server so two independent may cause a lower efficiency.
- In this the Least Significant Bit (LSB) algorithm is used for obtaining the stego-image.
- For encrypting the data XOR operation is used.

The component of the cover image is extracted and the secret message resized to the cover image are XOR'ed. Thus the stego image is obtained and it is transmitted in the channel. The receiver enters the secret key which is matched with the transmitted secret key, only then the extracting algorithm is performed on the stego image. To extract the secret message, the decryption is performed on the encrypted image. Finally, the message is extracted.

To Maintain Security

These are performed to maintain the security in the network:

- If there is no difference between the plotted histograms of cover image and the embedded image the embedded message will not be known the intruder.
- So the secret message can be transmitted to the receiver.

IV .STEGANOGRAPHY ALGORITHM

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. It does not replace cryptography but rather boosts the security using its obscurity features. Steganography has various useful applications. However, like any other science it can be used for ill intensions.

Histogram Data Hiding

Histogram based data hiding is another commonly used data hiding scheme. Lossless data hiding using the difference value of adjacent pixels. It is classified under +1 or -1 data embedding algorithm .It exploits the correlation between adjacent pixels that eventually results in a compact histogram that is characterized by a normal Gaussian distribution.

Disadvantages

- Less efficiency.
- Less accuracy.
- Security wise low.
- Easily attack the data.

How to display an image in MATLAB

Here are a couple of basic MATLAB commands (do not require any tool box) for displaying an image.

Displaying an image given on matrix form

Operation	**MATLAB command**
Display an image represented as the matrix X.	Imagesc(X)
Adjust the brightness. s is a parameter such that -1<s<0 gives a darker image, 0<s<1 gives a brighter image.	brighten(s)
Change the colors to gray.	colormap(gray)

Sometimes your image may not be displayed in gray scale even though you might have converted it into a gray scale image. You can then use the command colormap(gray) to "force" MATLAB to use a gray scale when displaying an image.

If you are using MATLAB with an Image processing tool box installed, I recommend you to use the command imshow to display an image.

Displaying an image given on matrix form with image processing tool box

Operation:	**MATLAB command**
Display an image represented as the matrix X.	imshow(X)
Zoom in (using the left and right mouse button).	zoom on
Turn off the zoom function.	zoom off

Images formats supported by MATLAB

The following image formats are supported by MATLAB:

- BMP
- HDF
- JPEG
- PCX
- TIFF
- XWB

Most images you find on the Internet are JPEG-images which is the name for one of the most widely used compression standards for images. If you have stored an image you can usually see from the suffix what format it is stored in. For example, an image named myimage.jpg is stored in the JPEG format and we will see later on that we can load an image of this format into MATLAB.

V. PROPOSED SYSTEM

INTRODUCTION

The problem of hiding in another host image is the large amount of data that requires a special data embedding techniques to obtain enough capacity, transparency and robustness. Our proposed Steganography system, which embeds secret image into cover image which applies a discrete wavelet transform (DWT) s to achieve a robust and multilayer security system with a high invisibility. The pre-embedding is proceeded by the two important stages: 1. Secret image selection and processing stage 2. Best cover image selection and processing stage.

DISCRETE COSINE TRANSFORM

The DCT represents an image as a sum of sinusoids of varying magnitudes and frequencies. The dct2 function computes the two-dimensional discrete cosine transform of an image. The DCT has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications. For example, the DCT is at the heart of the international standard lossy image compression algorithm known as JPEG.

Embedding Algorithm

Embedding is nothing but hiding the information in the object. In image steganography, this object can be of any digital form such as images ,text, audio and video. Embedding techniques are carried out in order to protect the secret message from the intruder while transmission.

Analysis of Data

Validate
MSE
PSNR

Fig 4.1 Data Analysis

Finally the data is analysed using MSE and PSNR method. The experimental result show that satisfactory performance for hiding capacity, compression ratio and decomposition quality.

BLOCK DIAGRAM

Sender Side

- The cover image is embedded with secret message
- Then the key are selected and transform techniques are carried out
- The embedded image is taken as stego image

Receiver Side

- For extraction reverse process is done
- The secret messages retrieved by inverse transform technique
-

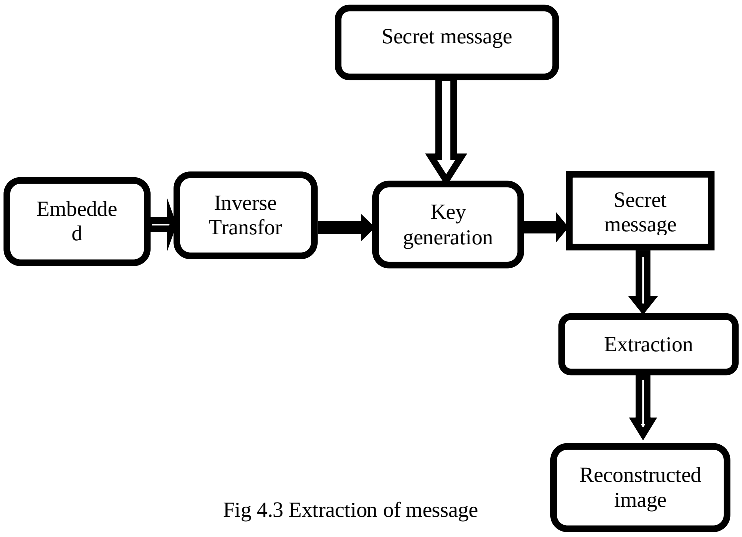


Fig 4.3 Extraction of message

DISCRETE WAVELET TRANSFORM

The idea on which the Discrete Wavelet Transform (DWT) performance is based that one dimensional signal will be divided into two parts, one is a high frequency part and another is a low frequency part. Later the low frequency part will be split into two additional parts and the analogous process will go on until reaching the desired level. As for the high frequency part of the signal .In each level of the DWT decomposition, an image will separate into four other parts such as the approximation image (LL) in addition to the horizontal (HL), the vertical (LH) and the diagonal (HH) for a detailed components. On the other hand, the subjective fidelity of the image quality is improved. Provides less computation time.

The discrete wavelet transform di

The discrete wavelet transform divides the image into four parts as in the following procedure:

- (P1) The scaling function ϕ(x) ϕ(y) produces the top left part.
- (P2) The vertical wavelet function ψ(x) ϕ(y) produces the top right part.
- (P3) The horizontal wavelet function ϕ(x) ψ(y) produces the bottom left part.
- (P4) The diagonal wavelet function ψ(x) ψ(y) produces the bottom right part.

The top left part is called an approximation because it is smooth and has large values. The other three parts are called details because they emphasize horizontal, vertical, and diagonal edges, respectively. These three parts have small absolute values except for edges.

DWT decomposes image into four non overlapping multi resolution sub bands:

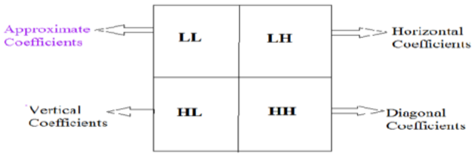


Fig 4.4 DWT Decomposing

LL1 (Approximate sub band), HL1 (Horizontal sub band), LH1 (Vertical sub band) and HH1 (Diagonal Sub band). Here, LL1 is low frequency component whereas HL1, LH1 and HH1are high frequency (detail) components. Embedding watermark in low frequency coefficients can increase robustness significantly but maximum energy of most of the natural images is concentrated in approximate (LL1) sub band. Hence modification in this low frequency sub band will cause severe and unacceptable image degradation. Hence watermark is not embedded in LL1 sub band. The good areas for watermark embedding are high frequency sub bands (HL1, LH1 and HH1), because human naked eyes are not sensitive to these sub bands.

They yield effective watermarking without being perceived by human eyes. Hence HH1 is also excluded. The rest options are HL1 and LH1. But Human Visual System is less sensitive in horizontal than vertical. Hence Watermarking is done in HL1 region.

Haar-Discrete Wavelet Transform

Haar wavelet transform is the simplest and most commonly employed wavelet. It can perform in two ways first is the horizontal way and the second is the vertical way. Haar wavelet function by scanning the pixels from left to right in a horizontal direction, next it will perform the addition and subtraction operation on the neighboring pixels which is multiplied by a scaling function. The process must be repeated until it can cover all the rows, while all the pixels sum will be represented by a high frequency. After accomplishing the previously described steps, it is possible to scan the pixels from top to bottom in a vertical direction. At the end the addition and subtraction operation will be multiplied by (1/1.414) and the result of the addition on the top and the subtraction.

VI. REFERENCES

1. Asna Furqan and Munish Kumar(2015), ‘Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique Using MATLAB’, IEEE International Conference on Computational Intelligence & Communication Technology, vol.5, no. 12, pp.1124-1524.
2. Gopi Krishna A and Dr. Mallikarjuna Prasa A (2013), ‘Adaptive Histogram Modification Based Reversible Data Hiding Algorithm for Color Images’, International Journal of Research in Computer and Communication Technology, vol.2, no.7, issue , ISSN: 2278-5841, pp: 2320-5156.
3. Hamad A. Al-Ataby, Majid A. Al-Taee and Waleed Al-Numaimy(2016), ‘Highly Efficient Image Steganography Using HAAR DWT for Hiding Miscellaneous Data’, Jordanian Journal of Computers and Information Technology (JJCIT), vol.2, no.1, pp.537-613.
4. Javier Franco-Contreras, MemGouenou Coatrieux, Fréderic Cuppens, Nora CuppensBoulahia, and Christian Roux (2014), ‘Robust Lossless Watermarking of Relational Databases Based on Circular Histogram Modulation’, IEEE transactions on information forensics and security, vol.9, no.3, pp. 3-9.
5. Kanthi Kiran Karasla, Syed Akhtar and P. Babu(2013), ‘Enhancing Reversible Data Hiding Schemes for Marked Covers’, International Journal of Engineering Sciences & Management, vol.3,no. 2, pp.34-39.
6. Mirza Abdur Razzaq and Riaz Ahmed Shaikh(2017), ‘Digital Image Security: Fusion of Encryption, Steganography and Watermarking’, International Journal of Advanced Computer Science and Applications, vol.8, no.5, pp.469-562.
7. Linjie Guo and Wenkang Su(2015), ‘Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited’, ‘IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 211-217.
8. Terence Johnson and Dr. Santosh Kumar Singh(2016), ‘Improved Steganography using Enhanced K Strange Points Clustering’, International Journal of Applied Engineering Research ISSN 0973-4562, vol. 11, no. 9, pp. 721-963.
9. Vojteh Holub and Jessica Fridrich(2015), ‘Low Complexity Features for JPEG Steganalysis using Undecimated DCT’, IEEE Transactions on Information Porensics and Security, vol.10, no.2, pp. 13912-6111.
10. Vijay Kumar Sharma, Dr. Devesh Kr Srivastava and Dr. Pratistha Mathur(2017), ‘A Study of Steganography Based Data Hiding Techniques’, International Journal of Emerging Research in Management & Technology, ISSN: 2278-9359, vol.6, Issue-4, pp. 111-214.