An Enhanced Image Steganography Technique using DCT, Jsteg and Data Mining Bayesian Classification Algorithm

Rajesh Samata  
PG Student  
Department of Computer Engineering  
Noble Group of Institutions, Junagadh, India

Prof. Nilesh Parghi  
Assistant Professor  
Department of Computer Engineering  
Noble Group of Institutions, Junagadh, India

Prof. Daxa Vekariya  
Assistant Professor  
Department of Computer Engineering  
Noble Group of Institutions, Junagadh, India

Abstract

Security of data is a challenging issue and transmitting the secured data. Data is hidden is one of the techniques to hide the data in a secured way called Steganography. In this paper we proposed secret image is hidden behind the cover image using Discrete Cosine Transform (DCT) and JSteg algorithm. In this algorithm all of the DCT coefficients are manipulated sequentially to hide secret image.

Keywords: Stegnography, DCT, Jsteg Algorithm Data Mining

I. INTRODUCTION

Image stenography is the art of data hidden into cover image the process of hiding secret image within another image. The word steganography comes from the Greek steganos, meaning of covered or secret and graphy, meaning of writing or drawing. It is hiding secret information within another carrier as images, videos, text and graphics to obtain the stego object so that it is not affected after insert.

“stego-image = secret image + cover image”

Steganography is classified into two domains such as spatial and frequency domain. In the first spatial domain the modifications are made on the pixel of the original image. The secret image is inserted directly in the pixel Reference [1][2]. In the second frequency domain the carrier image is transform from the spatial domain to the frequency domain via the technique of domain transform.

Fig. 1: Steganography steps for Graphical View
By using steganography technique there is a chance to send image so that can detect the existence of the image. In the image of steganography the cover is the object that will hide the secret data or image, which may also be encrypted using a stego key Reference [2]. This file is sent to the Encoder unit in the first step. When the Encoder must be design and implemented with the high precision to hiding the secret image with a few distortion and change in the cover image. In the next step this package are applied to Decoder unit when the output of the Decoder unit is delivered in the receiver side.

II. DISCRETE COSINE TRANSFORM (DCT)

The basic idea of the Discrete Cosine Transform (DCT) in image processing is to multi-differentiated embedded the cover image into secret image of different spatial domain and frequency domain Reference [5][2]. The DCT is a signal from an image representation into a frequency representation the image pixel into 8*8 pixel blocks and transforming the pixel blocks into the 64 DCT coefficients.

DCT is used in steganography as image is broken into 8*8 blocks of pixels Reference[6]. The working from left to right and top to bottom. DCT each block is compressed through quantization table to scale the DCT coefficients and image is embedded in DCT coefficients.

III. JSTEG ALGORITHM

Basically the JSteg algorithm is based on the LSB (Least Significant Bits) replacement scheme in the DCT domain. This method also used for the LSB for hiding image or data Reference [3]. In this algorithm the image or data bits are hidden in the LSB of the DCT coefficients instead of the real values of the pixels.

\[
F(u, v) = \frac{1}{4}C(u)C(v)
\]

\[
\sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2y+1)v\pi}{16}.
\]

In this equation x,y,u,v ϵ {0,1,…….,7}, f(x,y) is the particular pixel of color space component , \(C(u) = 1/\sqrt{2}\) if u=0 and C(u)=1. This transformation of an 8*8 blocks included 64 DCT coefficient from 8*8 block of image. The JSteg algorithm is based on the well know embedding method called LSB replacement it replace the LSB of quantized DCT coefficients that differ from 0 and 1 with bits of message. The DCT coefficients are randomly chosen in the JSteg algorithm.

IV. ARNOLD TRANSFORM

An image transformation is done to randomize the actual pixel positions of the image. After several iterations the actual image reappears. The numbers of iterations taken to change the pixel positions is defined as Arnold’s period. The Arnold’s Transformation is represented as:

\[
\begin{bmatrix}
x' \\
y'
\end{bmatrix} = \begin{bmatrix}
1 & 2 \\
1 & 1
\end{bmatrix} \begin{bmatrix}
x \\
y
\end{bmatrix} \mod n
\]
Arnold’s transformation which is used to change all pixels coordinates of the image being taken. After all the coordinates have been transformed, we got a secret image.

V. BAYESIAN CLASSIFICATION

Bayesian classifiers are statical classifiers they can predict class membership probabilities, such as the probability that a given tuple belongs to a particular class. Bayesian classification is based on Baye’s theorem. Bayesian classification algorithms have a comparing to found a simple Bayesian Classifier known as the naïve Bayesian classifier to be comparable in performance with decision tree and selected nearual network classifiers Reference [4].

Step for Bayesian classification:
1) Step1:- Read cover image.
2) Step2:- Find pixel value on cover image.
3) Step3:- use process for extraction of pixel value on cover image.
4) Step4:- use Bayesian classification to classify on cover image find the best pixel value.

VI. PROPOSED SYSTEM

In this section we are using DCT for hiding stego image in cover image. For higher security used Arnold transform and image can be secret and after stego-image.
C. Step of Extraction Process as follows:
1) Step 1: Use the DCT technique on watermark image.
2) Step 2: Watermark image extract on cover image and Secret image.
3) Step 3: Transform on secret image for watermark Image using Arnold transform.
4) Step 4: Apply IDCT on secret image and cover image and get original image and secret image.

Fig. 5: Extracting Process In Watermark image

VII. Objective Analysis

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

It is easily defined via the mean squared error (MSE) which for two mxn monochrome images I and K where one of the image is considered a noisy approximation of the other is defined as:

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

The PSNR (in dB) is defined as:

\[ PSNR = 10 \cdot \log_{10} \left( \frac{MAX_i^2}{MSE} \right) \]
\[ = 20 \cdot \log_{10} \left( \frac{MAX_i}{\sqrt{MSE}} \right) \]

VIII. Conclusions

The proposed system helps to transmit and received the secret image in a highly secured manner by using DCT and Arnold transform.
REFERENCES