A Secure Image Steganography Technique using DCT, Jsteg and Bayesian Classification

Rajesh Samata[1] Prof. Nilesh Parghi[2] Prof. Daxa Vekariya[3]
[1]P.G. Student [2,3]Assistant Professor
[1,2,3]Department of Computer Engineering
[1,2,3]Noble Group of Institutions, Junagadh, India

Abstract— Security of data is challenging issue and transmitting the secured data. Data is hidden is one of the techniques to the hide of the data in a secured way called Stegnography. 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.

Key words: Stegnography, DCT, Jsteg Algorithm Data Mining Classification

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 a 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.

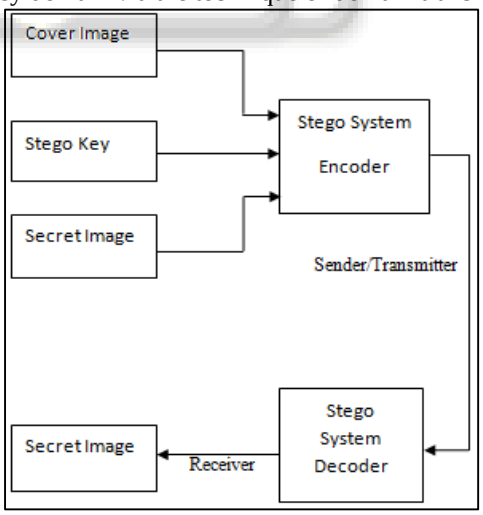

Fig. 1: Steganography steps for Graphical View.

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 Refference [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.

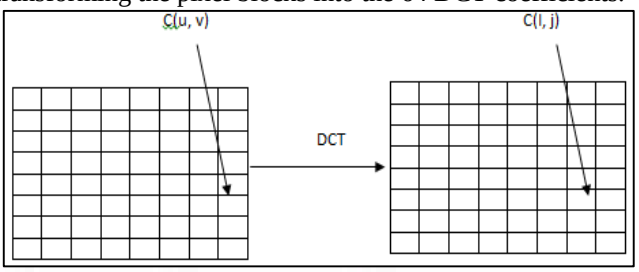

Fig. 1: DCT

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 Refference [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.

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

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

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/√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:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod n$$

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 theorm. 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].

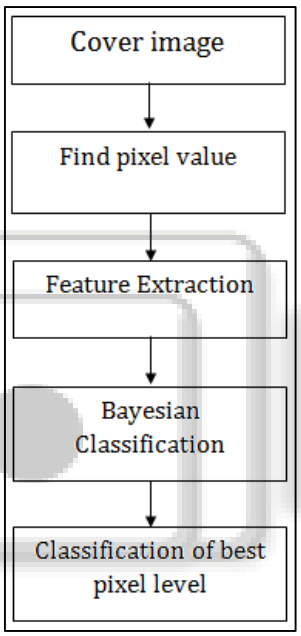

Fig. 2: Classification of image for pixel value

A. *Step for Bayesian Classification:*

- Step1: Read cover image.
- Step2: Find pixel value on cover image.
- Step3: use process for extraction of pixel value on cover image.
- 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.

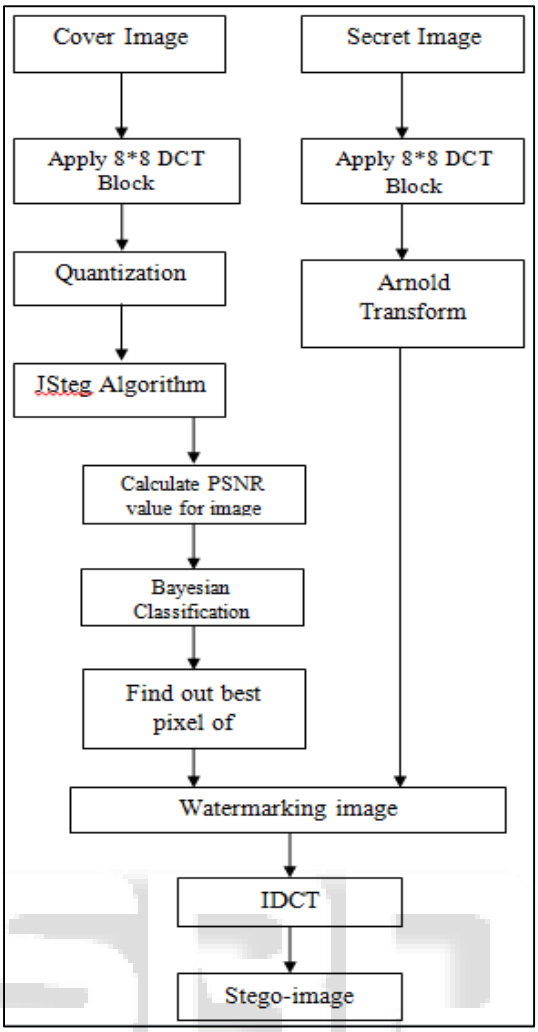

Fig. 3: Overview of proposed system

A. *Steps of Overview of Proposed System as Follows:*

- Step1: Read cover image and secret image.
- Step2: Use the DCT technique to Embedded Secret image with cover image.
- Step3: Find coefficient from cover image using Quantization table and transform Secret image for watermark image using Arnold transforms
- Step4: Apply the JSteg algorithm on cover image.
- Step5: Calculate the PSNR value of cover image.
- Step6: Use Bayesian Classification to classify cover image from above find best pixel value.
- Step7: Used pixel for needed process cover image and digital image use IDCT (Inverse Discrete Transform) to get for cover Image.

B. *Steps of embedding process of proposed System as follows:*

- Step 1: Read secret image and cover image.
- Step 2: Use the DCT technique to embedded Secret image and cover image.
- Step 3: Apply the JSteg algorithm on cover image and transform secret image for watermark using Arnold transform.
- Step 4: Use Bayesian Classification to find proper Pixel on embedded scrambled image with cover image.

– Step 5: Use proper pixel for watermarking image and scrambled image used IDCT to get for stego-image.

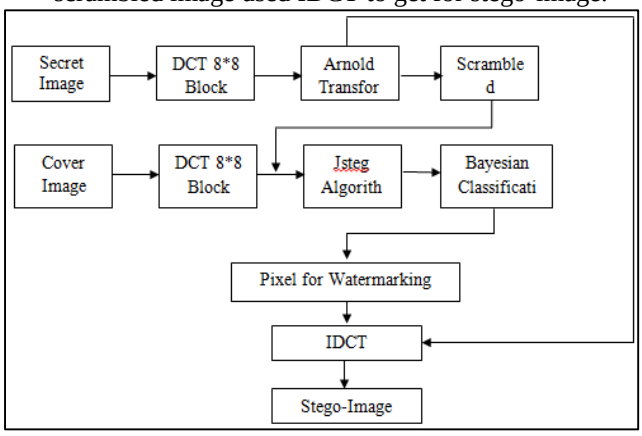

Fig. 4: Embedding Process in Steganography

C. Step of Extraction Process as follows:

– Step 1: Use the DCT technique on watermark image.
– Step 2: Watermark image extract on cover image and Secret image.
– Step 3: Transform on secret image for watermark Image using Arnold transform.
– Step 4: Apply IDCT on secret image and cover image and get original image and secret image.

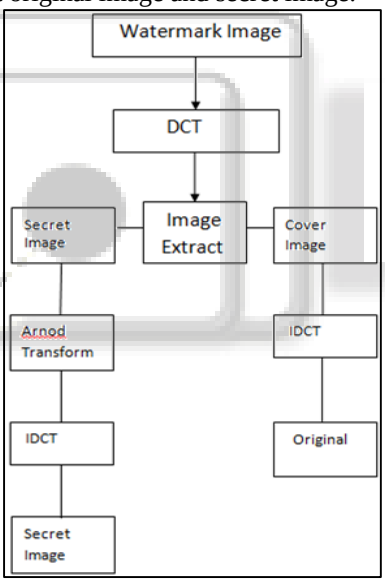

Fig. 5: Extracting Process In Watermark image

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.

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

The PSNR (in dB) is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

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

A. Displaying Result:

The MATLAB product can be utilized to export project results as plots or as complete reports. It is conceivable to export plots to all popular graphics file formats and then import the plots into other packages, for example, Microsoft Word or Microsoft PowerPoint. MATLAB is an intelligent graphics user interface is very user friendly, embedded with default demo capabilities, tool tips, and alternate ways.

The MATLAB Window consists of following components:

– Workspace browser
– Command history
– Command window

The workspace program is a graphical client interface that permits us to view and manage the contents of the MATLAB workspace. It gives a graphical representation of the variables, their size and class and permits the client to perform the equivalent of the clear, load open and save functions.

The command history window displays a list of previous commands that a user has entered in the command window. The list of previous commands can extend back to previous execution of the project. Commands remain in the list until they are erased. To re-execute any command, double-click it with the left mouse button.

The command window is one of the fundamental instruments used to enter data, run MATLAB capacities and scripts, additionally used to display results. When MATLAB is installed the standalone editor is automatically associated with the files being an .m extension in Windows platform. The stand-alone editor opens for editing the code with double click on an Mfile (.m file).

In this part we will show the implementation of my proposed work and result analysis. We are using DCT and Jsteg Algorithm for hiding secret image in cover image and used Arnold transform and after embed stego image into original image. And Bayesian classification used to select the proper pixel to cover the image.

Fig. 6: Cover Image

Fig. 7: Secret Image

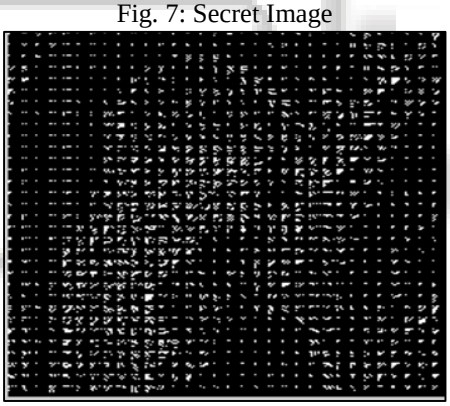

Fig. 8: DCT Apply

Gray Scale Image

watermark image	PSNR
Lena	37.9049

Table 1: Gray Scale image pixel value

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

[1] Milia Habib, Basem Bakhache, ”Enhancement using chaos of a steganography method in DCT Domain”, 2015 IEEE
[2] Ahmed Elsayed, Abdelrahman Elleithy,”Highly Secure Image Steganography algorithm using courvelet transform and DCT encryption.”2015 IEEE
[3] Hossein sheisi, Jafar Mesgarian and Mostafa Rahmani, ”Steganography: DCT coefficient replacement method and compare with JSteg algorithm” (IJCEE), vol 4, Aug-2012.
[4] Tanu Priya, Saurabh Prasad,” Superpixels for spatially reinforced Bayesian Classification of hyperspectral images”. (IEEE) vol.12, may-2015
[5] Deepika Bansal, RitaChhikara,”An improved DCT based steganography technique”. (IJCA), September – 2014.
[6] Edmund Y.Lam, Joseph W.Goodman, “A Mathematical Analysis of the DCT Coefficient Distributions for images”. Vol.9 , October 2000 (IEEE).
[7] sidharth sinh and tanveer,“A seurity enhanced robust steganography algorithm for data hiding” (IJCSI), vol 9 may-2012

