Volume 4, No. 4, March-April 2013

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

High Capacity Image Steganography Using Curvelet Transform and Bit Plane Slicing

Sheshang D. Degadwala*
Dept. Of Computer Engineering
CSPIT Changa, Gujarat, India.
Sheshang13@gmail.com

Amit R. Thakkar
Dept. Of Information Technology
CSPIT Changa, Gujarat, India.
amitthakkar.it@ecchanga.ac.in

Rikin J. Nayak
Dept Of Electronics & Communication
CSPIT Changa, Gujarat, India.
rikinnayak@gmail.com

Abstract: In order to protect copyrighted material from illegal duplication, two typical technologies have been developed. Key-based cryptographic techniques and Steganography which enable the appropriate security during the transmission process. The science and art of hiding information in unremarkable cover media is steganography so as not to arose an eavesdropper's suspicion. Steganography is an application under information security field. Steganography is Classified by having set of measures that rely on strengths attacks that are driven by weaknesses and uncertainty. Now a days, computer and network technologies provide easy-to-use communication channels for Steganography . The curvelet transform is a multiscale directional transform that allows an almost optimal non-adaptive sparse representation of the object with edges. Bit plane slicing technique is used for data compression where the original image is sliced in to 8 planes. Steam cipher RC4 algorithm is used for hiding the message. The effectiveness of the proposed methods has been estimated by computing Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The aim to propose work is to make existence of image stegangoraphy technique based on curvelet transform provide acceptable levels of imperceptibility and distortion in the cover image and high level of overall security.

Keywords: Steganography, security, RC4, curvelet transform, cryptography, Bit Plane Slicing.

I. INTRODUCTION

Data hiding can be done by cryptography, Steganography and watermarking. Here only considering steganography means "concealed writing". The Steganography is science of data hiding within another one, so that its presence is undetectable and suffers less security threats or attacks. It hides the content in cover media as not to provoke any doubt that there is some information or message hidden in the media [1]. Sometimes people mix it with encryption. In encryption the content is not hidden but not readable by the reader if the key is not known to him. But the encrypted content can be intercepted by anyone and chances always present that he will try to decode it or affect it by attempting to decode it for a purpose or just for the sake of curiosity. Whereas, steganography gives us more freedom to communicate and send secret information without leaving any evidence that opponent will intercept and try decoding your information. Oftentimes throughout history, encrypted messages have been intercepted but have not been decoded [2].The interception of the message can be just as damaging because it tells an opponent or enemy that someone is communicating with someone else [2]. Steganography takes the opposite approach and attempts to hide all evidence that communication is taking place [2].

Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity) [2]. The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message [2]. Modern steganography goal is to keep its mere presence undetectable because of their invasive nature leave behind detectable traces in the cover medium through modifying its statistical properties so eavesdroppers can detect the distortions in the resulting stego medium statistical properties [2]. The process of finding these distortions is called statistical steganalysis [2].

II. INFORMATION –HIDING SYSTEM

An information-hiding system is characterized by having three different aspects that contend with each other. These are capacity, security, and robustness as shown in Fig. 1. Capacity refers to the amount of information that can be hidden in the cover medium, security to an detector's inability to detect hidden information and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [2] Generally saying, information hiding relates to both watermarking and Steganography [3]. A watermarking system primary goal is to achieve a high level of robustness-it should be impossible to remove a watermark without degrading the data object's quality [3]. Steganography strives for high security and capacity, which often involves that the hidden information is fragile

[3]. Even trivial modifications to the stego medium can destroy it [3].

There are three basic types of Stego systems are vailable:

a. Pure Stego systems → no key is used.
b. Secret-key Stego systems → secret key is used [2].
c. Public-key Stego systems → public key is used.

The Techniques that is followed in this Paper uses secret key to encrypt a hidden message that is encapsulated inside a cover media.

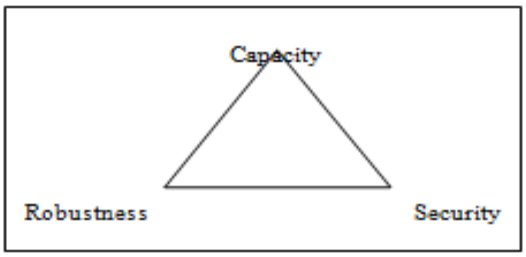

Figure 1: Information-hiding System Features

III. IMAGE STEGANOGRAPHY TECHNIQUES

Image steganography techniques can be classified into two broad categories: Spatial-domain based steganography and Transform domain based Steganography in fig 2.

A. Spatial Domain Method

In spatial domain scheme, the secret messages are embedded directly. Here, the most common and simplest steganography method is the least significant bits (LSB) insertion method. In the least significant bits (LSB) Method, the pixels are replaced by the message bits which are permuted before embedding [4].

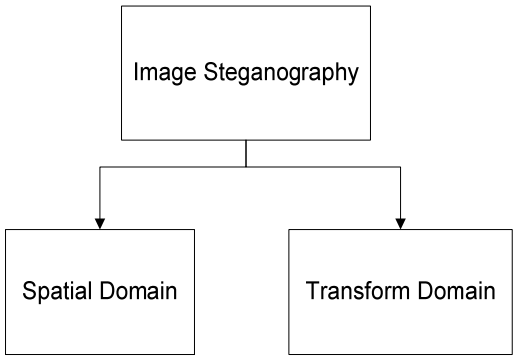

Figure 2: Technique Of Image Steganography

B. Least Significant Bit Method:

Most of steganography software hide information by replacing only the least significant bits (LSB) of an image with bits from the file that is to be hidden. This technique is commonly called LSB encoding. One of the most common techniques is used in steganography. The following Example shows that how the letter "A" can be hidden in the first eight bytes of three pixels in a 24-bit image [4].

Example of Lsb:

Pixels: (10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001)
Secret message: 01000001
Result: (10101110 11101001 10101000)
(10100110 01011000 11101000)
(11011000 10000111 01011001)

The three bold bits are the only three bits that were actually altered. Since the 8-bit letter "A" only requires eight bytes to hide it in the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message. Slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte [4]. This increases the hidden information capacity of the cover-object, it is degraded more, and therefore it is more detectable [4].

Another deviation on this technique includes ensuring that statistical changes in the image do not occur. Some intelligent software also checks for areas that are made up of one solid color. While LSB insertion is easy to implement, it is very easy to be attacked. Slight modifications in the color palette and simple image manipulations will destroy the entire hidden message. Some examples of these simple image manipulations include image resizing and cropping. Since the steganalysis of LSB method is easier. Therefore, it is suggested that the image should be first manipulated before the embedding of the message into it.

C. Transform Domain Method:

For hiding a large amount of data,the transform domain steganography technique is used having high security, a good invisibility and no loss of secret message [4].

The idea is to hide information in frequency domain by altering magnitude of all of discrete cosine transform (DCT) coefficients of cover image. The 2-D DCT converts image blocks from spatial domain to frequency domain. The carrier image is divided into non overlapping blocks of size 8×8 and applies DCT on each of blocks of cover image using forward DCT [5].

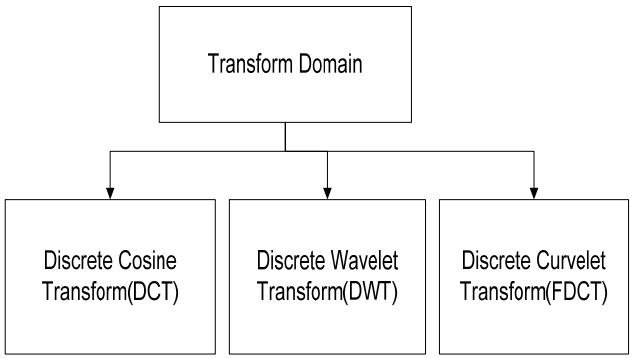

Figure 3: Method for Transform Domain

IV. THE CURVELET TRANSFORM

Basically, Curvelet transform extends the ridgelet transform to multiple scale analysis. Therefore, we start from the definition of ridgelet transform. Given an image $f(x, y)$, the continuous ridgelet coefficients are expressed as:

Here scale a > 0, each position b ∈ R and each orientation Θ ∈ [0, 2Π]. A ridgelet can be defined as [6],

$$\Re_f(a,b,\theta) = \iint \psi_{a,b,\theta}(x,y) f(x,y)\,dx\,dy \quad (1)$$

$$\psi_{a,b,\theta}(x,y) = a^{\frac{1}{2}}\psi\left(\frac{x\cos\theta + y\cos\theta - b}{a}\right) \quad (2)$$

Where θ is the orientation of the ridgelet. Ridgelets are constant along the lines x cosθ + y sinθ = const. The ridgelet based Curvelet transform is shown in figure 4.

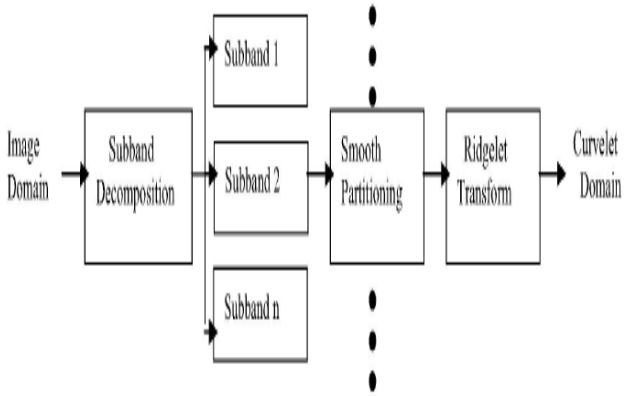

Figure 4: Ridgelet based Curvelet Transform

This ridgelets can be tuned to different orientations and different scales to create the curvelets. Ridgelets take the form of a basis element and obtain a high anisotropy. Therefore, it captures the edge information more effectively. A ridgelet is linear in its edge direction and is much sharper. In this Curvelet approach, input image is first decomposed into a set of subbands each of which is then partitioned into several blocks for ridgelet analysis. The ridgelet transform is implemented using the Radon transform and the 1-D wavelet transform.The whole process is shown in Figure 5.

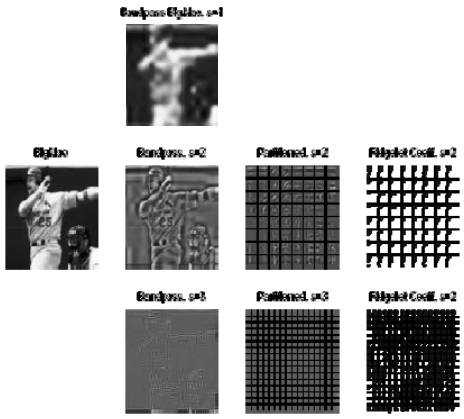

Figure 5: Ridgelet based Curvelet Transform Process on image

Fast discrete Curvelet transform based on the wrapping of Fourier samples has less computational complexity as it uses fast Fourier transform instead of complex ridgelet transform. In this approach, a tight frame has been introduced as the Curvelet support to reduce the data redundancy in the frequency domain. Normally, rideglets have a fixed length that is equal to the image size and a variable width, whereas curvelets have both variable width and length and represent more anisotropy. Therefore, the wrapping based Curvelet transform is simpler, less redundant and faster in computation than ridgelet based Curvelet transform.

Curvelet transform based on wrapping of Fourier samples takes a 2-D image as input in the form of a Cartesian array f[m,n] such that $0 \le m < M, 0 \le n < N$ and generates a number of Curvelet coefficients indexed by a scale j , an orientation *l* and two spatial location parameters (k1 ,k2) as output. Discrete Curvelet coefficients can be defined by [7]: $c^D(j,l,k_1,k_2) =$

$$\sum_{0\le m<M,\ 0\le n<N} f[m,n]\,\varphi^D_{j,l,k_1,k_2}[m,n] \quad (3)$$

Here, each $\varphi^D_{j,l,k_1,k_2}[m,n]$ is a digital Curvelet waveform.

Basically, wrapping based Curvelet transform is a multiscale transform with a pyramid structure consisting of many orientations at each scale. The pyramid structure consists of several subbands at different scales in the frequency domain. Subbands at high and low frequency levels have different orientations and positions.

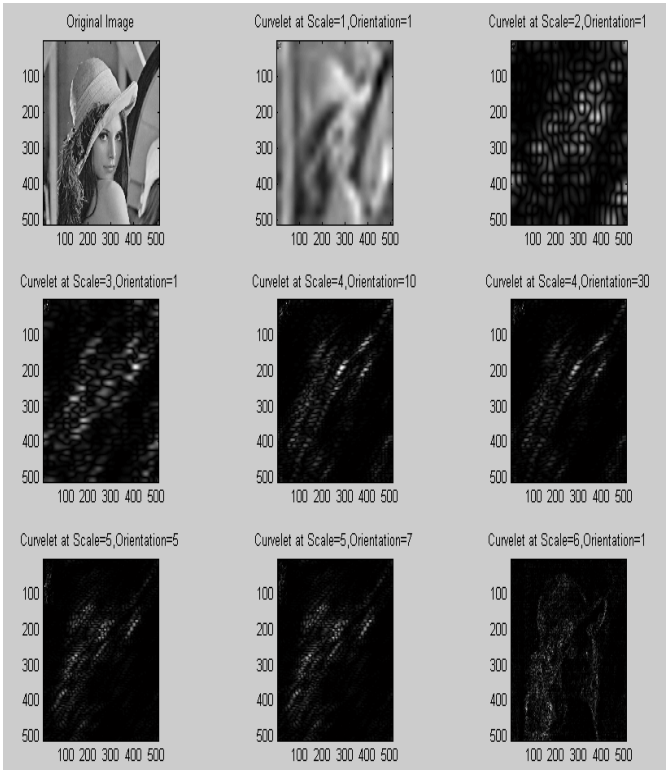

Figure 6: Curvelet Coefficient with different scale and orientation

From figure 6 it can be seen that at high scales, the Curvelet waveform becomes so fine that it looks like a needle shaped element, whereas, the Curvelet is non directional at the coarsest scale. If we combine the frequency responses of curvelets at different scales and orientations, we get a rectangular frequency tiling that covers the whole image in the spectral domain. Thus, the Curvelet spectra completely cover the frequency plane and there is no loss of spectral information.

V. CRYPTOGRAPHY

The use of cryptography as a way to secure the hidden message mainly addresses the security requirement in the Information-Hiding system. For the purpose of steganography, *symmetric encryption* is followed. The symmetric encryption is a method of encryption that uses the same key to encrypt and decrypt a message. If one person encrypts and decrypts data, then this person must keep the key secret. If the data is transmitted between parties, each party must agree on a shared secret key and find a secure method to exchange the key.

The security of encrypted data depends on the secrecy of the key. If someone gains knowledge of the secret key, he or she can use the key to decrypt all the data that was encrypted with the key. Table 1 shows common algorithms for symmetric key encryption.

No encryption method is completely secure. Given knowledge of the algorithm and enough time, attackers can reconstruct most encrypted data. A strong algorithm (the one that is built on sound mathematical methods, creates no predictable patterns in encrypted data, and has a sufficiently long key) can deter most attacks.

Table 1:Common Algorithm For Symmetric Key Encryption

Algorithm	Key Length
Data Encryption Standard	56-bit Key
Triple DES	Three DES operation, 168-bit Key
Advanced Encryption Standard(AES)	Variable Key lengths
International Data Encryption Algorithm(IDEA)	128-bit Key
Blowfish	Variable Key lengths
RC4	Variable Key lengths

When a strong algorithm is used, the only way to break the encryption is to obtain the key. An attacker can obtain a key by stealing it, by tricking someone into revealing the key (a form of social engineering), or by trying all possible key combinations. This last method is commonly known as a *brute force attack*. Increasing the key length exponentially increases the time that it takes an attacker to perform a brute force attack.

Going through the details of the encryption algorithms is out of the scope of this paper. In order to utilize the encryption in this work, a Microsoft encryption utility program is used to encrypt the hidden message. This utility encrypts message with different algorithms (IDEA, DES, Triple DES, MDC, and RC4) depending on the user choice. As a case study, RC4 method was used in this paper with 56-bit key.

VI. BIT PLANE SLICING

Bit plane slicing s new way of looking at an image [8]. Bit plane slicing is considered to be a stack of binary images. The image nearest to the bottom are least significant and the images on top are most significant. Instead of exposing intensity ranges, the exposing contribution made to the total image appearance by specific bit might be desired.

Imagine that the image is composed of eight-bit planes, ranging from plane 0 for least significant bit to plane 7 for the most significant bit [8]. Bit-plane slicing reveals that only the five highest order bits contain visually significant data [8]. Also, remark that plane 7, corresponds exactly with an image threshold at gray-level 128.

Given an 8-bit per pixel image, slicing the image at different planes (bit-planes) plays an important role in image processing. In general, 8-bit per pixel images are processed.Image is sliced into the following bit-planes. 0 is the least significant bit (LSB) and 7 is the most significant bit (MSB):

a. which results in a binary image, i.e. odd and even pixels are displayed [14].
b. which displays all pixels with bit 1 set: 0000.0010
c. which displays all pixels with bit 2 set: 0000.0100
d. which displays all pixels with bit 3 set: 0000.1000
e. which displays all pixels with bit 4 set: 0001.0000
f. which displays all pixels with bit 5 set: 0010.0000
g. which displays all pixels with bit 6 set: 0100.0000
h. which displays all pixels with bit 7 set: 1000.0000

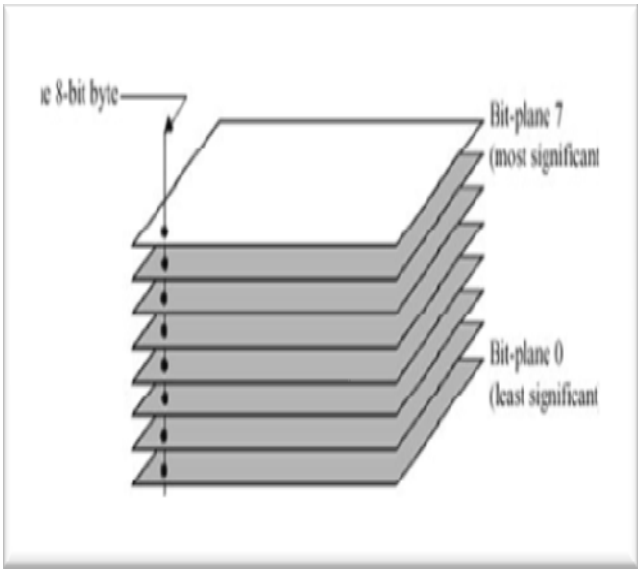

Figure 7: 8-bit plane slicing method.

VII. MEASURMENT OF IMAGE STEGANOGRAPHY

PSNR: The PSNR computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a stego-image. The higher the PSNR, the better the quality of the stego, or reconstructed image [2].

To compute the PSNR, the block first calculates the mean-squared error using the following equation [2] :

$$MSE = \frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}[J(i,j) - J'(i,j)]^2 \quad (4)$$

In the previous equation, m and n are the number of rows and columns in the input images, where J' is the pixel in the stego image, J is the cover image respectively. Then computes the PSNR using the following equation [2]:

$$PSNR = 10 * \log_{10}(S^2/MSE) \quad (5)$$

Where,

$$S^2 = \frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n} f^2(i,j) \quad (6)$$

VIII. THE PROPOSED METHOD

Proposed Approach is use for hiding large amount of message inside image using curvelet transform and bit plane slicing. First step color image is convert into the 3 different images like red Color image, blue color image and green color image and apply Bit Plane Slicing and generate total 24 images from the 3 images and find the minimum information image from the 24 images using PSNR value. And apply the curvelet transform on the minimum information image.RC4 algorithm on to the message and apply curvelet transform on to the strong key encryption and coefficient Replacement process between message curvelet image and curvelet transform of minimum information image. And apply inverse curvelet transform and generate Stego image.

Fig.8 shows a general representation of the proposed steganography method. At the receiving end, opposite operations are followed to get the hidden message. The proposed method contains the following steps:

Step1: cover image to separate R-G-B

Input: cover image

Output: Generate different R image, G image, B image

Action: Generate different color image. separate different color from the cover image.

Step2: Apply bit plane slicing on R-G-B

Input: different R-image, G -image ,B- image

Output: Generate different 24 images to apply bit plane slicing.

Action: apply the bit plane slicing on the R-G-B separate image. Get the 24 images from the R-G-B separate image.

Step3: finding the minimum information from different 24 images.

Input: different 8 R-image , 8 G -image , 8 B- image

Output: Generate one less information image from the 24 different images

Action: finding the minimum information as per psnr value between original one image.

Step 4: FDCT-wrapping Transformation:

Input: Generate one less information image from the 24 different images

Output: FDCT-wrapping transformed cover image

Action: Convert the pre-processed cover image to curvelet domain through 2D curvelet transform FDCT-wrapping

End

Step 5: Threshold Calculation/Identification of the size of redundancy:

This step calculates the threshold (T) that is used to define what is the size (the space) of the redundancy in the cover image, that can be used to embed the message (or part of the message) in. Calculation of the threshold is done via statistical means. The following is one of the possibilities that have been followed in this paper:

$$T = \frac{\alpha}{N}\sum^{N}|J_W| \quad (7)$$

Where Jw s are the coefficients of the FDCT-wrapping for the cover image, N is the number of coefficients. From practical best practice, it was found that this equation should be scaled by a correction factor α (between 0 and 1). Note that this factor is a function of the message nature and affects the size of the cover image that is used to embed the hidden message. The step is summarized as follows:

Input: FDCT-wrapping transformed cover image

Output: Size of the information (s) that can be hidden inside the cover image, FDCT-wrapping of the cover image

Action: Threshold (T) calculation

For each pixel in the transformed cover image **do**

get next FDCT-wrapping coefficient

if the value of the **FDCT-wrapping coefficient < T,**

then store the index of the coefficient, s=s+1

end

End

Step 6: Message Partitioning:

Input: Value of s, secret message

Output: 1D bit stream of the message with size s

Action: Convert the message to 1D bit stream

End

Step 7: Strong Key Encryption:

Input: 1D bit stream of the message with size s

Output: Encrypted bit stream of the message

Action: Encrypt the 1D bit stream of the message with RC4, **key length=56**

End

Step 8: Encrypted Message FDCT-wrapping Transformation:

Input: Encrypted bit stream of the message

Output: FDCT-wrapping transform of the encrypted message.

Action: Transform the encrypted bit stream of the message to curvelet domain

End

Step 9: Stego Image Formation:

Input: FDCT-wrapping of the cover image (Step 5), FDCT-wrapping transform of the encrypted message.

Output: Stego image

Action:

Place the FDCT-wrapping coefficients of the encrypted message in the location specified previously in the FDCT-wrapping of the cover message.

Inverse FDCT-wrapping transform the result.

End

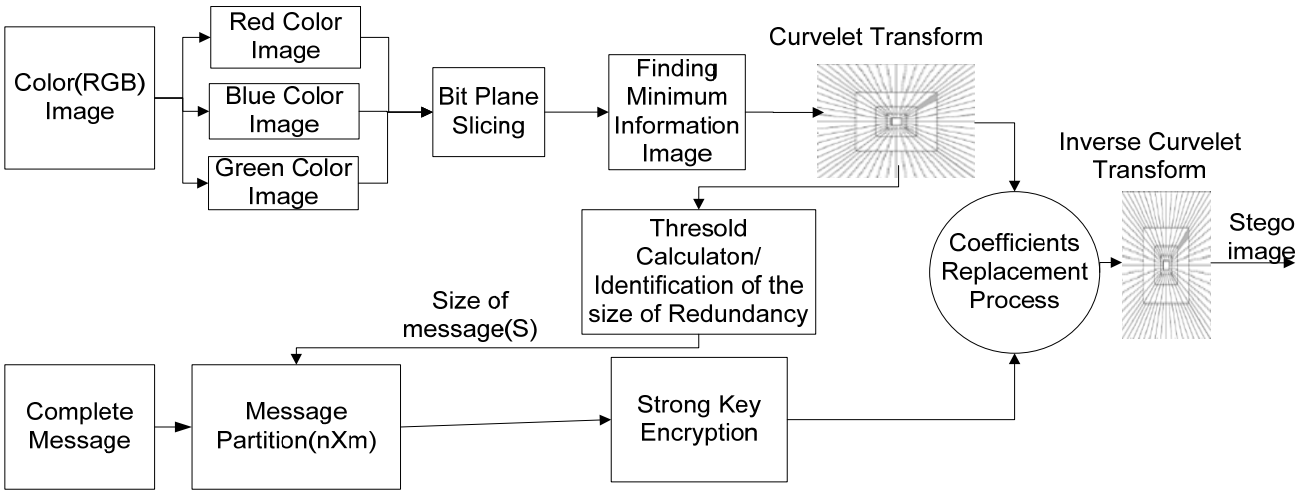

Figure 8: Proposed Method

IX. CONCLUSION AND FUTURE EXTENSIONS

Hereby it is concluded that Image Steganography Using Curvelet Transform is more robust and more secure. The security level of this method can be measured based on the PSNR value. Applying the RC4 algorithm on to the message and provide security. for storing more payload Curvelet transfer must be used and bit plane Slicing on to the cover image and also check the robustness of the image based on the Some Type of Attack.

Firstly this proposed work will be implemented for its practical feasibility. A future extension to this work is to apply on the different size of images. And take image rather than the message. And implement watermarking based on this type of approach. Apply block cipher rather than the steam cipher. Check the robustness based on the rotation, blurred and another type of operation.

X. REFERENCES

[1] Saddaf Rubab, M. Younus, "Improved Image Steganography Technique for Colored Images using Wavelet Transform", International Journal Of Computer Application Volume 39-No.14, February 2012.

[2] Ali A. Al-Ataby ,Fawzi M. Al-Naima, "High Capacity Image Steganography Based on Curvelet Transform", 2011 IEEE.

[3] Ali A. Al-Ataby ,Fawzi M. Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[4] Jagvinder Kaur , Sanjeev Kumar, "Study and Analysis of Various Image Steganography Techniques", IJCST Vol. 2, Issue 3, September 2011.

[5] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview Of Image Steganography", in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically).

[6] Jean-Luc Starck, Emmanuel J. Candès, David L. Donoho, "The Curvelet Transform for Image Denoising".

[7] Emmanuel Cand`es, Laurent Demanet, David Donoho, Lexing Ying", Fast Discrete Curvelet Transforms".

[8] S.Bhargav Kumar, K.Esther Rani, "FPGA Implementation of 4-D DWT and BPS based Digital Image Watermarking", International Journal of Engineering Trends and Technology-Volume 3 Issue2- 2012.