[RACE: March 2017]
ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

DWT AND SVD BASED IMAGE STEGANOGRAPHY

Jyothi K.*
*Assistant Professor, Department of Electronics & Communication Engineering, College of Engineering Trikaripur, Cheemeni, Kerala 671 313

ABSTRACT

Security and privacy are the main concern with the growth of electronic communication. Steganography is aimed to hide the existence of the hidden message. Image steganography is the process of hiding a secret message within an image called cover image in such a way that someone cannot know the presence or contents of the hidden message. Many different cover file formats can be used, but digital images are the most popular because of their frequency on the internet. Singular Value Decomposition (SVD) improves the perceptual and statistical robustness to withstand manipulations that arises in an untrusted medium such as internet. Discrete Wavelet Transform (DWT) can be used in steganography to partition the image into blocks without the blocking artefacts that is with discrete cosine transform and therefore there is no information loss. The proposed system combining steganography with cryptography to improve the strength of steganography. This paper proposes an advanced method for image steganography to conceal gray scale images using DWT and SVD to increase the embedding capacity while maintaining the robustness and symmetric key cryptosystem to enhance the security of communication over an open channel.

Keywords- *SVD, DWT, cryptography, steganography*

I. INTRODUCTION

All the major government organizations and financial firms stress upon the issue of cyber security in today's world. Sensitive data of military and intelligence agencies has been the target of the most notorious hackers of the world. Illegal access by an unauthorized person is the most devastating thing that could happen to an organization for its sensitive data.

Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, but also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography [1].

Steganography is the process of secret or covert communication. Steganography come from two Greek words *stegnos* means *secret* and *graphein* means *writing*. The steganography process utilizes the property of human visual system that is blind to very complex binary patterns [2]. The main characteristic required for steganography is imperceptibility.

The terminologies used in steganography are cover object, secret message, key and stego object. Cover object is the carrier for the secret message and message is the actual information which is to be hided. The cover object carrying the secret message is called the stego object and in steganography it is same as the cover object in appearance. The secret message is extraction at the receiver side is based on the key. There are mainly four types of steganography based on the cover object used and it is shown in figure 1.

Steganography is the process of hiding a text file, image, audio or video within another text file, image, audio or video. Image steganography deals images as the cover object whereas in audio steganography, the cover object is an audio file. Many different cover object formats can be used, but digital images are the most popular because of their frequency on the internet. The basic image steganography model is shown in figure 2.

ISSN 2348 – 8034
Impact Factor- 4.022

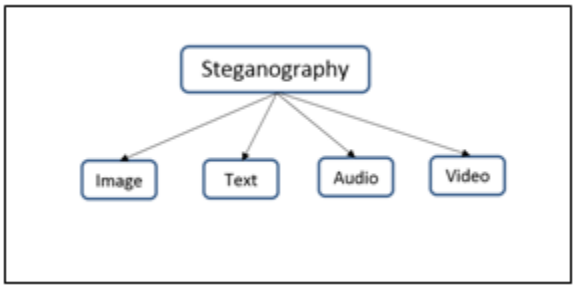

Fig.1. Types of steganography

Cryptography and steganography are the commonly used data hiding techniques. The major difference between these two are, cryptography technique encrypts the secret message and send over an untrusted medium whereas in steganography the existence of secret message is a secret. The strength of steganography can be increased by combining it with cryptography.

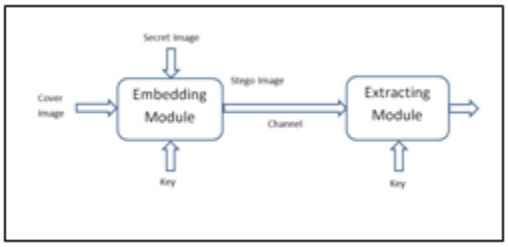

Fig.2. Basic image steganography model

The rest of the paper is organized as follows. Section II presents the current state of the art related to image steganography. Section III discusses the various methods of image steganography. Section IV, section V and section VI discusses about singular value decomposition, discrete wavelet transform and data encryption standard respectively. Section VII proposes DWT and SVD based image steganography method for secure data communication. Section VIII focuses on the simulation results of the proposed system.

II. CURRENT STATE OF THE ART

The image steganography is not a new research area in the field of data hiding. There are so many literature found in image steganography it hide both text and images as secret message.

Samy Ghoniemy et. al [2] proposed an adaptive steganography algorithm based on DCT and spread spectrum methods. To increase the data hiding capacity above 50%, the bit plane complexity segmentation (BPCS) embedding technique is used. The principle of BPCS technique is that, the image is divided into informative region and noise-like region, the secret message is hiding in noise-like or textured region. The secret message used in this paper is a text message.

Yambem Jina Chanu et. al [7] propose a steganography technique that computes the SVD of the image, then embeds the secret message in the left singular vectors, singular values and right singular vectors. This paper focus on the black and white image hiding in color images.

Hemalatha S. et. al [3] proposed a method based on integer wavelet transform in which color image as the cover image and focus mainly on key generation. This approach results in high quality stego image having high PSNR values compared to other methods.

The research paper by Shrikant S. Khaire et. al [8] focuses on implementation of a steganography technique that has hiding capacity up to 50% using bit plane complexity segmentation steganography. This paper focuses on the grey image hiding in color image.

Hsiao-Shan Huang et. al [9] proposed block-wise pixel value differencing method, by comparing the difference values between the adjacent four pixels, the one with more edge like modes is decided as the chosen mode. Due to the characteristics of human vision resolution which have a larger tolerance in edge areas than in smooth areas, the main idea of the proposed method can find more edge areas in order to hide more secret data. But this method is used to embed data in gray scale images only.

The research paper by Hao-tian Wu et. al [10], proposed JPEG image steganography in which secret message embedded more into the low and middle frequency bands of DCT coefficients than high frequency band. This paper focuses on text embedding in JPEG cover images.

III. METHODS OF IMAGE STEGANOGRAPHY

Steganography in images are classified into two categories: spatial-domain based steganography and the transform domain based Steganography [11].

Spatial Domain Method

In spatial domain scheme, the secret message is embedded directly in the cover image. There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Some of the spatial domain techniques are: Least significant bit (LSB), Pixel value differencing (PVD), Edges based data embedding method (EBE), Histogram shifting methods method.

Transform Domain Method

The transform domain steganography technique is used for hiding a large amount of data and provides high security, a good invisibility and no loss of secret message. This is a complex way of hiding information in an image. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. The goal behind that 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 cover image is divided into non overlapping blocks of size 8 x 8 and applies DCT on each of blocks of cover image using forward DCT.

Another transform domain technique is discrete wavelet transform (DWT) based steganography methods. Discrete wavelet transforms are used to convert the image in spatial domain to frequency domain, where the wavelet coefficients so generated, are modified to conceal the image. In DWT, the image is passed through low-pass and high-pass filters and the high and low frequency wavelet coefficients are generated by taking the difference and average of the two pixel values respectively. The DWT technique describes the decomposition of the image into four non overlapping sub-bands CA (Approximation sub band), CH (Horizontal sub band), CV (Vertical sub band) and CD (Diagonal sub band) [3][13].The most important requirement is that a steganography algorithm has to be imperceptible. For imperceptibility of an algorithm following criteria are obeyed:

- Invisibility- It is the ability to be unnoticed by human eye. That is, the steg fo image should be identical to the cover image in appearance.
- Hiding capacity- Steganography requires sufficient embedding capacity than watermarking.
- Hiding capacity=$\frac{No.of\ bits\ embedded\ \ in\ the\ cover\ \ image}{No.of\ \ bits\ in\ the\ cover\ \ image}$
- Robustness –T is the ability of the stego image to withstand the image manipulations such as cropping, compression, rotation, filtering etc.

ISSN 2348 – 8034
Impact Factor- 4.022

IV. SVD (SINGULAR VALUE DECOMPOSITION)

In the linear algebra the SVD is a factorization of a rectangular real or complex matrix into three matrices and it is a stable and an effective method to split the system into a set of linearly independent components [14]. In SVD a matrix A of size m×n can be factored into U, S, V such that

A=USV^T

Where U is orthogonal m×m matrix and the columns of U are the orthonormal eigenvectors of AA^T, V is orthogonal n×n matrix and the rows of V^T are the eigenvectors of A^TA. The matrix S is m×n diagonal matrix and its elements are called singular values (SV)[12]. Singular value vector has the entire energy of the matrix A. U and V represent the geometrical shape of the image. This is called singular value decomposition, because the factorization finds eigen values that make the following characteristic equation singular. That is, $|AA^T-\lambda I|$=0.

V.DWT (DISCRETE WAVELET TRANSFORM)

The continuous wavelet transform (CWT) of a function f (t) ∈ L^2 (set of square integrable functions) with respect to some analyzing wavelet ψ is defined as:

$$W_\psi f(b,a) = \int_{-\infty}^{\infty} f(t)\psi_{b,a}(t)dt$$

where

$$\psi_{b,a}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right);\ a>0$$

The parameters b and a are called translation and dilation parameters respectively. For ψ to be a window function and to recover f(t) from its CWT, ψ(t) must satisfy the following condition

$$\psi(0) = \int_{-\infty}^{\infty} \psi(t)dt = 0$$

By taking a =2^{-s} and b=$k2^{-s}$, where k, s ∈ Z, the CWT equation becomes

$$W_\psi f(k2^{-s},2^{-s}) = 2^{s/2}\int_{-\infty}^{\infty} f(t)\psi(2^s t-k)dt$$

After discretizing the function f(t) in the above equation assume with sampling rate to be 1 becomes the DWT equation [15].

$$W_\psi f(k2^{-s},2^{-s}) \approx 2^{s/2}\sum_n f(n)\psi(2^s t-k)$$

VI. DES (DATA ENCRYPTION STANDARD)

The DES is a cryptographic algorithm which is use to encrypt and decrypt the data. In the modern cryptography, there are two types of cryptographic algorithms called symmetric key cryptography and public-key cryptography. DES is a symmetric key cryptographic algorithm developed by Horst Feistel at IBM and adopted as standard in the USA in 1977. In symmetric key algorithm both the sender and the receiver share the same key which is used to encrypt the data. DES has been shown to be highly resistant to the attacks in the medium. Figure 3 depicts the structure proposed by Feistel[4].

ISSN 2348 – 8034
Impact Factor- 4.022

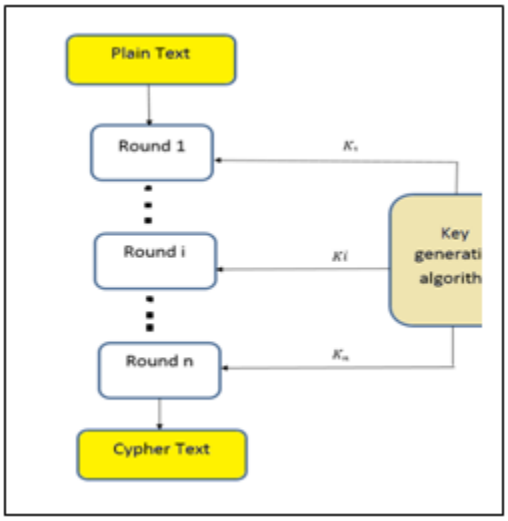

Fig. 3. DES encryption block diagram

VII. PROPOSED SYSTEM

An image steganography system that is based on transform domain technique DWT and SVD can be used to increase the hiding capacity, security and the robustness of stego image. SVD improves the perceptual quality even in the presence of image manipulations like noise addition in the channel, attacks by the intruder etc. So the robustness of the steganography system can be improved. DWT can be used to improve the hiding capacity by concealing the secret image in all four sub bands of the cover image.

Embedding Section

The embedding section block diagram of the proposed system is shown in figure 4. Let X be the secret image hiding in the cover image A which is used as the carrier in the image steganography. DWT is applied to the cover image and then the carrier image is decomposed into four non overlapping sub-bands cA, cH, cV and cD. Singular value decomposition is applied to the coefficients of each sub band. The secret image is encrypted using Feistel encryption algorithm with key2 and further decomposed using SVD and applied to embedding process. In embedding process, singular values of each sub band of cover image is modified with the singular values of the encrypted secret image (cipher image) blocks by using scaling factor, αk. Then IDWT (Inverse DWT) of the embedded wavelet coefficients are taken to get the stego image

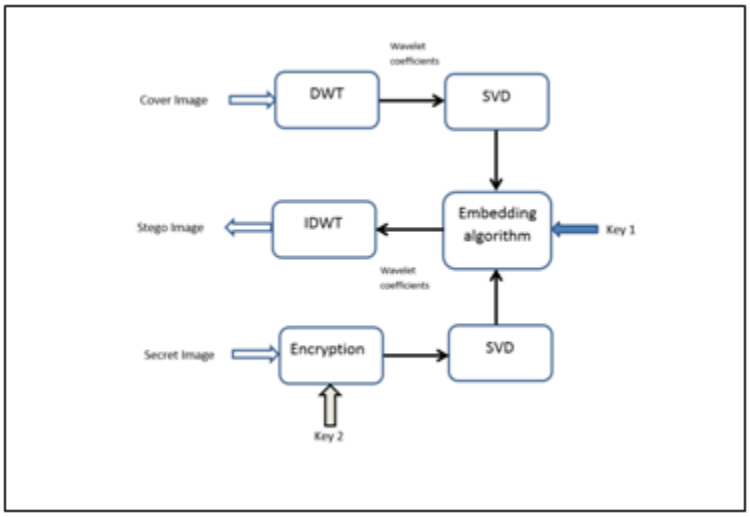

Fig. 4. Embedding Section block diagram

Embedding Algorithm

1. Input the cover image A.
2. Apply DWT to the cover image C then 4 sub bands CA, CH, CV and CD are formed.
3. Apply SVD to each sub band image:

$$A^k = U_a^k S_a^k V_a^{kT}$$

where k=1,2,3,4 for cA, cH, cV, ol/cD sub bands.
Let λ_i^k are the singular values (SV) of S_a^k for i=1 to n (n ≤ 256).

4. Input the secret image and divided into 4 blocks.
5. Input the 3 digit encryption key and generates the key matrix.
6. Encrypt the secret image using key matrix.
7. Apply SVD to the encrypted image X:
   a. $X = U_x S_x V_x^T$

Let λ_{xi} are the singular values (SV) of S_x for i=1 to n (n ≤ 256).

8. Modify the SV of each subband of cover image with the SV of the encrypted image X:
   a. $\lambda_i^* = \lambda_i^k + \alpha_k \lambda_{xi}$

where $0 < \alpha_k < 1$.

9. From the modified SV's, obtain four sets of DWT coefficients:
   a. $A^{*k} = U_a^k S_a^{*k} V_a^{kT}$

where k=1,2,3,4.

10. Apply IDWT to the four sets of modified DWT coefficients to produce the stego image A*.

ISSN 2348 – 8034
Impact Factor- 4.022

Extraction Section

The stego image with some attack introduced is inputted to the extraction section. Figure 5 shows the extraction section block diagram of the proposed system. DWT of the stego image is done and singular value decomposition is applied to the coefficients of each sub band of the stego image. The singular values of the cipher image is extracted using the stego key (key1). After IDWT, decryption using Feistel algorithm is performed with the same key used in encryption (key 2) and the secret image is extracted.

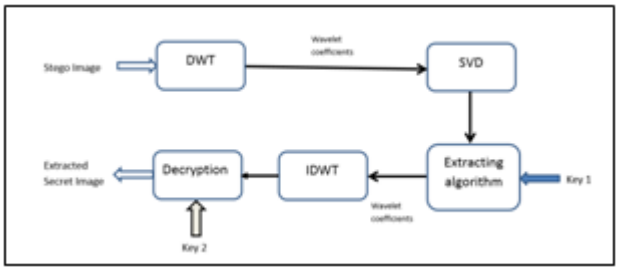

Fig. 5. Extraction Section block diagram

Extracting Algorithm

1. Using DWT, decompose the stego image A* into four sub bands.
2. Apply SVD to each sub band image:
$$A^{*k} = U_a^k S_a^{*k} V_a^{kT}$$
where k=1,2,3,4 for cA, cH, cV, cD sub bands of A*.
3. Extract SV from each sub band:
$$\lambda_{xi}^k = \frac{\lambda_i^* - \lambda_i^k}{\alpha_k}$$
where k=1,2,3,4 and i=1 to n (n ≤ 256).
4. Construct the cipher image using the above SV vectors:
$$X^k = U_x S_x^k V_x^T$$
where k=1,2,3,4.
5. Decrypt the cipher image using the same key used for encryption to get the extracted image.

VIII. RESULTS AND DISCUSIONS

Simulation of the proposed system is performed in Intel(R) Core(TM) I3-2450M processor operating at 2.5 GHz using MATLAB R2015a (8.5.0.197613). For simulation 256 X 256 colour image is used as cover, a 256 X 256 gray scale image as secret, a three digit encryption key and a two digit stego key are used. Preprocessing the cover and secret image is done to obtain the DWT and secret image blocks respectively.

- **Peak Signal to Noise Ratio (PSNR)**

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 affects the fidelity of its representation. A higher PSNR generally indicates that the reconstruction is of higher quality[5]. The PSNR for an image of size M X N with the maximum possible pixel value in the image R and Mean Square Error (MSE) is defined as,

$$PSNR = 10 * log_{10}\left[\frac{R^2}{MSE}\right]$$

$$MSE = \frac{1}{M*N}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[I_1(m,n) - I_2(m,n)]^2$$

where I_1 is the cover image and I_2 is the stego image.

ISSN 2348 – 8034
Impact Factor- 4.022

PSNR values falling below 30dB indicate a fairly low quality stego image. i.e. distortion caused by embedding is severe. However a high quality stego image should possess the PSNR value more than 40dB.

- **Embedding Section Results**

Figure 6 shows the decomposed sub bands of the cover image, in which the approximation (cA) band carries most significant information in the time domain. The most important requirement of steganography is the algorithm has to be imperceptible. For imperceptibility of an algorithm invisibility criterion is obeyed. It is the ability to be unnoticed by human eye. That is, the stego image should resemble the cover in appearance.

Fig. 6. Decomposition of the cover image using DWT

Figure 7 shows the block division of 256 X 256 secret image into four 128 X 128 blocks and each block is concealed in corresponding DWT sub band of cover.

Fig. 7. The secret image division into 4 blocks

Figure 8 and 9 shows the encryption of the secret image and the embedding section output respectively.

Fig. 8. Encryption of the secret image

In figure 9, stego image is similar to cover but the secret image is concealed in it.

ISSN 2348 – 8034
Impact Factor- 4.022

Fig. 9. Embedding section inputs and output

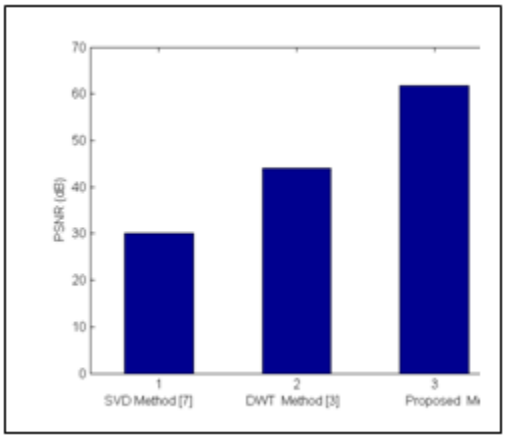

Fig. 10. Comparison of PSNR (in dB) of the stego image in different methods

Figure 10 compares the PSNR values of the stego image in the proposed method with that of two papers by Yambem Jina Chanu et. al 2012 [7] and Hemalatha S. et. al 2013 [3].

ISSN 2348 – 8034
Impact Factor- 4.022

- **Attacks**

The robustness of the method against steganographic attacks is tested by adding noise and blur to the stego image and it is shown in figure 11.

Fig. 11. Attacks to the stego image

- **Extracting Section Results**

The extraction section output without and with steganographic attack is shown in figure 12 and 13.

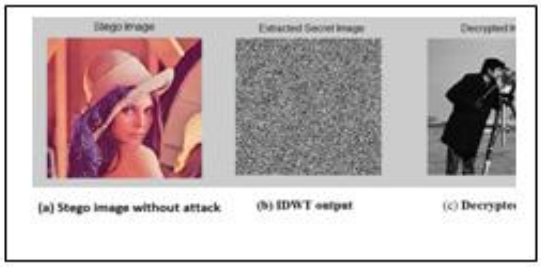

Fig. 12. Extraction without attack

Fig. 13. Extraction with attack

ISSN 2348 – 8034
Impact Factor- 4.022

The noisy stego image is given as the input and the extracted output is similar to the embedded secret image. Steganography requires sufficient hiding capacity. In this method, the embedding capacity achieved is 33%.

If the decryption key is not matched with encryption key, a message box shown in figure 14 is displayed.

Fig. 14. Message box showing key mismatch

IX. CONCLUSION

This paper has presented an image steganography technique and it has explained the algorithm to embed and recover an image using the singular value decomposition and discrete wavelet transform. There are different approaches existing in image steganography and also seen different methods proposed by different authors. Many ideas to maintain visual imperceptibility and robustness have been evaluated and discussed. DWT can be used to improve the embedding capacity by concealing the secret image in all four sub bands of the cover image. The embedding capacity obtained in proposed method is better than the existing methods. Steganography and cryptography are the techniques used to protect information from unwanted parties but independently the two technologies are used, they result lesser PSNR.

The strength of steganography increases by combining it with cryptography. This is achieved in the proposed system by incorporating data encryption standard (DES) cryptosystem. Therefore, the PSNR value is increased to 62dB which improves the security of the proposed system.

REFERENCES

[1] *Alvaro Martín, Guillermo Sapiro, and Gadiel Seroussi, "Is Image Steganography Natural?", IEEE Transactions on Image Processing, Volume 14, 2005.*

[2] *Samy Ghoniemy,Omar H. Karam and Osman Ibrahim, "Robust and Large Hiding Capacity Steganography using Spread Spectrum and Discrete Cosine Transform", International Journal of Image Processing and Visual Communication, Volume 1 , Issue 4 , February 2013.*

[3] *Hemalatha S, U Dinesh Acharya, Renuka A and Priya R. Kamath,"A Secure Color Image Steganography In Transform Domain, " International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013.*
[4] *William Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall, 2005.*
[5] *Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh and Eero P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity", IEEE Transactions on Image Processing, Volume 13, Issue 4 , April 2004.*
[6] *Barnali Gupta Banik and Samir K. Bandyopadhyay, "A DWT Method for Image Steganography" , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.*
[7] *Yambem Jina Chanu and T. Tuithung, "Steganography technique basedon SVD", InternationalJournalofResearchinEngineering and Technology (IJRET), 2012.*
[8] *Shrikant S. Khaire and Sanjay L. Nalbalwar , "Review: Steganography Bit Plane Complexity Segmentation (BPCS) Technique", International Journal of Engineering Science and Technology, Vol. 2, 2010, pp. 4860-4868.*
[9] *Hsiao-Shan Huang, Chin-Song Wu, Ming-Hsin Chang, and Gan-How Chang , "An Image Steganographic Method Based on Block-wise PixelValue Differencing", International Journal of Science and Engineering, Vol.4 ,2014,pp. 141-144.*
[10] *Hao-tian Wu, Jiwu Huang, "Secure JPEG Steganography By LSB+ Matching And Multi-band Embedding", 18th International Conference on Image Processing, 2011.*
[11] *Falesh M. Shelke, Ashwini A. Dongre, Pravin D. Soni, "Comparison of different techniques for Steganography in images", International Journal of Application or Innovation in Engineering and Management, Volume 3, Issue 2, February 2014.*
[12] *K. A. Navas, M. C. Ajay, M. Lekshmi, T. S. Archana and M. Sasikumar, "DWT-DCT-SVD based watermarking", 3rd International Conference on Communication Systems Software and Middleware and Workshops, 2008, pp. 271 - 274.*
[13] *Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, "Implementation of Image Steganography using 2-Level DWT Technique", International Journal of Computer Science and Business Informatics , Vol 1, No 1 , 2013.*
[14] *Rowayda A. Sadek, "SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges ," International Journal of Advanced Computer Science and Applications, Vol. 3, No. 7, 2012.*
[15] *J. C. Goswami and A. K. Chan, Fundamentals of wavelets: Theory, Algorithms and Applications, Wiley-Interscience Publication, John Wiley & Sons Inc., 1999.*