**International Refereed Journal of Engineering and Science (IRJES)**
*ISSN (Online) 2319-183X, (Print) 2319-1821*
*Volume 3, Issue 10 (October 2014), PP.64-73*

# Blind Key Steganography Based on Multilevel Wavelet and CSF

Hoda Farag [1], Said E. El-Khamy [2]
[1]*(Department of Electrical Engineering/ Alexandria University/Alexandria, Egypt)*
[2]*(Department of Electrical Engineering/ Alexandria University/Alexandria, Egypt)*

**Abstract:-** Steganography is the art and science of invisible communication as it hides the information message inside cover image In This paper the cover image is decomposed using multilevel wavelet transform and theses wavelet coefficients are statistically weighted according to their perceptual importance (CSF weights) to identify the regions of interest for the embedding. The hiding image is encrypted using secret key based on wavelet coefficients on the last approximation level. Then the encrypted watermark is embedded using CSF weights in the wavelet domain into the cover image. Experimental results denote the feasibility of the proposed method as the stego images has high PSNR and subjective quality which declare that the algorithm gains a good performance in transparency and robustness against noise attacks.

**Keywords:-** Steganography, Wavelet Transform , Watermarking, CSF.

## I. INTRODUCTION

Recent advances in technology have made the distribution of media content easier and due to the rapid development in the information technology, which has posed serious threats to obtain secured data communication. The method of providing more security to data is through the information hiding which is related to both watermarking and steganography.

The digital watermarking is a commercial application can be used as an authentication tool to control the distributed content, and as a method to discourage the unauthorized copying and distribution of electronic documents while the cryptography is a technique for hiding secret messages within another message or carrier as a mean of securing the secrecy of communication and the message is scrambled as it can’t be interpreted and it is used to protect the contents from unauthorized access but sometimes it's not enough to keep the contents of the message secret but it's necessary to keep the existence of the message secret as in steganography as it hides the message itself.

Steganography word is of Greek origin[1] essentially means concealed writing as the protection of the transmitted data from being intercepted or tampered, which has led to the development of various steganographic techniques that can be used for wide range of applications such as, in defense organizations for safe circulation of secret data, in military and intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials.

Steganographic techniques have various features which characterize their strengths and weaknesses that includes the embedding capacity as it refers to the amount of data inserted into the cover media without deteriorating its integrity, the perceptual transparency of the cover image after the embedding which means no significant degradation or loss of perceptual quality of the cover media, Robustness as it refers to the ability of embedded data to remain intact if the stego-image undergoes various transformations , tamper resistance as the difficulty to alter or forge a message once it is embedded in a cover-media and computational complexity of steganographic technique employed for encoding and decoding is another consideration and should be given importance.

The steganographic techniques are classified based on embedding method of secret data into the image into Spatial domain, Frequency domain and Compression domain.

In Spatial domain embedding techniques, cover-image is first decomposed into bits planes and then least significant bit (LSB) of the bits planes are replaced with the secret data bits, it has advantages like high embedding capacity, ease of implementation and imperceptibility of hidden data but the major drawback is its vulnerability to various simple statistical analysis methods while in frequency domain embedding techniques, which first transforms the cover-image into its frequency domain, secret data is then embedded in frequency coefficients which has advantages include higher level of robustness against simple statistical analysis. Unfortunately, it lacks high embedding. In compression domain, secret data is embedded into compression codes of the cover-image which is then sent to the receiver where bandwidth requirement is a major concern.

In this paper, an efficient steganographic technique based on the CSF adaptive wavelet transform is proposed This approach provides a simultaneous spatial localization and frequency spread of the watermark within the host image by using the multilevel wavelet transform and the watermark merging process is adaptive as it depends on the local image characteristics at each resolution level and robust as it embeds the watermark more strongly into more salient components of the image as the system incorporates the sensitivities of the human visual system (HVS) by using adaptive edge CSF all of these factors makes the proposed algorithm more secure compared to other algorithms and the encrypted data hard to attack. Also using the wavelet transform which allows the multi resolution detection of the encrypted hidden image reduces the time of the algorithm and save the network bandwidth.

This paper is organized as follows: Section2 presents a brief review of related work, Section 3 presents some fundamental techniques used in the algorithm the wavelet transform, contrast sensitive function, Section 4 presents the proposed algorithm of Blind key steganography, Section 5 presents the Simulation results and Security analysis which report the effectiveness of our method. At last conclusion of this paper will be drawn in Section 7.

## II. A REVIEW OF RELATED WORK

Ali Al-Ataby1 and Fawzi Al-Naima [7] proposed an algorithm that calculate the threshold or the size of redundancy in the cover image that can be used to embed the message or part of it and these calculation done using statistical means which are histogram test , contrast correction and color balance correction then encrypting the message using RC4 with key length of 56 and transforming it into the wavelet domain then embedding the DWT of the encrypted image into the wavelet transform of the cover image in the locations specified previously, this method pre-adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered.

A. A. Abdul Latef [8] proposed a steganography algorithm based on discrete wavelet and discrete cosine transforms where the color cover image is divided into equally four parts, for each part select one channel from each part( Red, or Green, or Blue), choosing one of these channel depending on the high color ratio in that part. The chosen part is decomposed into four parts {LL, HL, LH, HH} by using discrete wavelet transform. The hiding image is divided into four part n*n then apply DCT on each part. This method achieves high security by hiding the coefficient of DCT of hiding image in transform domain methods (DWT) and the hidden process is done in one channel in each quarter of the cover image and in HH sub-band only or increasing the amount of payload hidden message by using another sub-band like HL and LH.

In [9] Ch. Samson presented a novel approach for image encryption supported by lossy compression using multilevel wavelet transform by decomposing the input image using multilevel 2-D wavelet transform, and thresholding is applied on the decomposed structure to get compressed image. Then the compressed image is encrypted by using a multilevel 2- dimensional Haar Wavelet Transform at the maximum allowed decomposition level. Reverse operations are performed at the receiving end to reconstruct the original image.

In [10] Yicong Zhou presents a new concept of image encryption which is based on edge information. The basic idea is to separate the image into the edges and the image without edges, and encrypt them using any existing or new encryption algorithm. The user has the flexibility to encrypt the edges or the image without edges, or both of them, then combine the encrypted results to get the encrypted image. Also the user has flexibility to choose any existing method and its threshold for edge detection, select any encryption method and its security keys for encryption process, and encrypt either edges or image without edges, or both of them. Consequently the security keys of the presented image encryption algorithm have infinite number of possible combinations. As a result the encrypted images are extremely difficult for the unauthorized users to decode and the images are protected with high level of security

## III. THE FUNDAMENTAL TECHNIQUES

In this section we presents the basic transforms used in this algorithm the wavelet Transform and the Contrast Sensitive Function(CSF) and Adaptive masking CSF masking in the discrete wavelet domain.

- ***The Wavelet Transform***

The wavelet transform provides the time-frequency representation of a given signal. The transforms are based on small waves, called wavelet [2], of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions which are horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL).

In two dimensional wavelet transform, a two-dimensional scaling function, ϕ (x, y) , and three two-dimensional wavelet function ψH ( x, y) , ψV(x. y) and ψD( x, y) , are required. Each is the product of a one-dimensional scaling function ϕ (x) and corresponding wavelet function ψ (x).

$$\phi(x,y) = \phi(x)\phi(y) \qquad \Psi^{H}(x,y) = \Psi(x)\Phi(y)$$

$$\psi^{V}(x,y) = \phi(x)\psi(y) \qquad \psi^{D}(x,y) = \psi(x)\psi(y)$$

While in Multilevel 2-D Wavelet Decomposition the decomposition of the approximation coefficients at level j in four components the approximation level at level j+1 and the details in three orientations horizontal , vertical and diagonal, Increasing the levels add computational overhead and complexity to the algorithm but also enhance the robustness of the steganography method against various attacks.

- ***The Contrast Sensitive Function***

The contrast sensitivity function (CSF) describes humans' sensitivity to spatial frequencies. Mannos and Sakrison [10] originally presented a model of the CSF for luminance (or grayscale) images to improve the HVS model for better image quality is given as follows:

$$CSF(f) = 1.6(0.192 + 0.114f)e^{-(0.114f)^{1.1}}$$

Where $f = \sqrt{f_x^{\,2} + f_y^{\,2}}$ is the spatial frequency in cycles/degree of visual angle ($f_x$ and $f_y$ are the spatial frequencies in the horizontal and vertical directions, respectively). The HVS is most sensitive to normalized spatial frequencies between 0.025 and 0.125 and less sensitive to low and high frequencies.

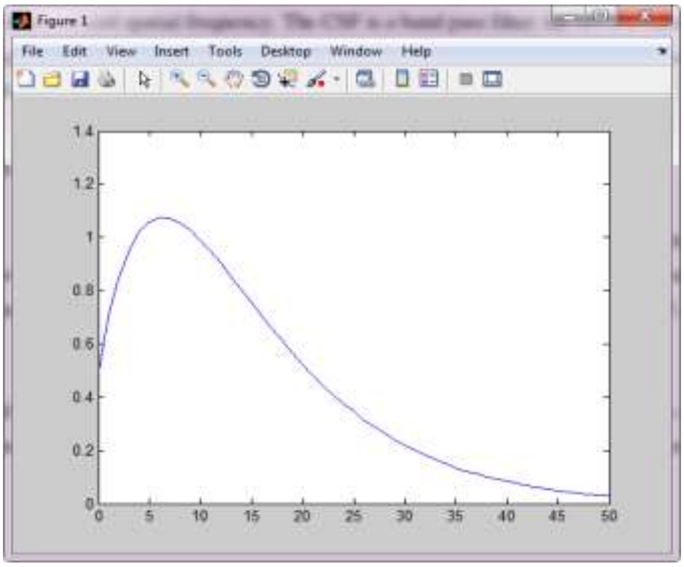


**Figure 1. Luminance Contrast Sensitivity Function**

The property of CSF is a measure of fundamental spatiochromatic of the HVS, and people are more sensitive in mid-frequency regions. Therefore, we need to embed low intensity of visible watermarking in high sensitivity regions and vice versa. Therefore, a good visible watermarking should embed low energy in mid-frequency regions from the plot of inverse CSF to avoid obtrusiveness and affect the visual quality.

- ***Adaptive masking CSF masking in the discrete wavelet domain***

CSF masking in [4],[5] is one way to apply the CSF in the discrete wavelet domain. CSF masking refers to the method of weighting the wavelet coefficients relative to their perceptual importance. The DWT

CSF mask utilizes the information in all of the approximation sub-bands as well as all of the detail sub-bands to yield 11 unique weights in the mask. All of the weights are normalized so that the lowest weight is equal to one. The 11 weights of DWT CSF mask are shown in Figure 2 after 5-level wavelet pyramidal DWT decomposition and the HVS is most sensitive to the distortion in mid-frequency regions (level 3) and sensitivity falls off as the frequency value drifts on both sides (level 1, 2, 4 and 5).

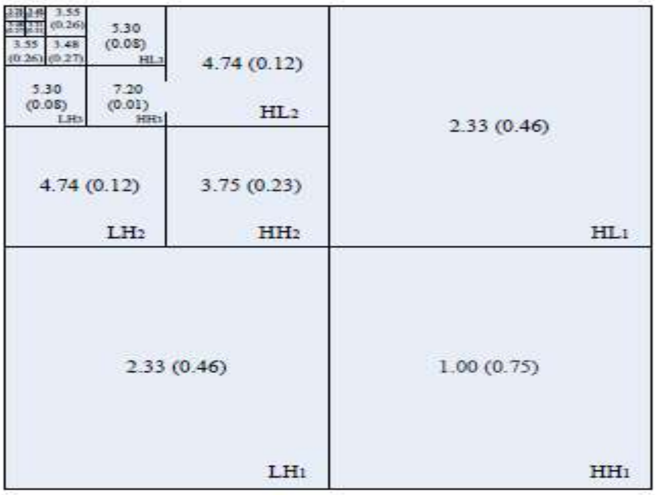


**Figure 2 A five-level wavelet pyramidal decomposition. rλ(βλ,θ) values for each level λ are Indicated at the center of each band.**

## IV. THE PROPOSED ALGORITHM

We present a new Steganography technique based on adequate stochastic modeling of the cover image using the adaptive CSF wavelet transform by applying the wavelet transform on the cover image and encrypting the base image into the cover image Incorporating the sensitivities of the human visual system (HVS) using Adaptive masking (CSF & Edge) which enhance the performance. The combined result of these factors makes the proposed algorithm more robust and Imperceptible compared to other algorithms where the watermarking technique used conceals both the content of the message (cryptography) and the presence of the message (Steganography) so an invisible watermark is very difficult to remove.

In the next sections we present the Adaptive CSF& Edge Detection masking, Encryption technique, the Embedding algorithm and Extraction algorithm.

- ***Adaptive masking (CSF& Edge Detection)***

Wavelets have been utilized as a powerful tool in many fields and the use of this transform addresses the capacity and the robustness of the information hiding system as hierarchical nature of the wavelet representation allows the multi resolution detection of the hidden message.

Adaptive masking refers to the convolution between CSF weights of the wavelet coefficient and the edges using wavelets with threshold .This mask used to embed the encrypted image into the most salient regions (ROI) of the cover image[10] which strengthen the watermarking technique as the ROI regions are determined efficiently as it adapts the wavelet analysis that is essentially suitable for singularity detection and adds more factors to the algorithm so the security keys of the steganographic algorithm have larger combinations and the encrypted images are extremely difficult for the unauthorized users to decode and the images are protected with high level of security.

- ***The Encryption Technique***

The used Encryption technique is a symmetric key cryptography that uses the same secret key to encrypt and decrypt the messages; we are using the AES Encryption Technique with a variable key length, increasing the key length to strengthen the encryption algorithm by using different factors like CSF weights and wavelet coefficients.

Applying the Multilevel wavelet transform to the eight level and get the wavelet approximation coefficients , rounding the last four coefficients to the integer part , Xoring the generated Key, CSF weights and wavelet coefficients then using these coefficients in the encryption process of the watermarked image keeping the size of the image the same throughout the iterations.

This complicates the encryption as the level of the wavelet is not known to the attackers also the combining technique between these coefficients and the CSF weights.

- ***Embedding Algorithm***

Figure 3 shows a general representation of the proposed steganography method and the steps of the Embedding algorithm is described in details as follows:
Step 1: Convert the cover true color image into gray scale image.
Step 2: Apply the Discrete Wavelet transform up to 5 levels using HAAR wavelet on the cover image
Step 3: Apply an edge detection method on the wavelet coefficient and thresholding the result.
Step 4 Apply the perceptual stochastic model (CSF masking) on the wavelet transform of the cover image using the adaptive masking (CSF &Edge) (weighting the wavelet coefficients relative to their perceptual importance)
Step 5 : Consider logo image, convert true color image into gray scale image that the size of the watermark will match the size of the matrix for embedding the watermark.
Step 6 : Applying the Multilevel wavelet transform to the eight level and get the wavelet approximation coefficients , rounding the last four coefficients to the integer part then using these coefficients as a factor in the incoming encryption process of the watermarked image .
Step 7: Apply Encryption Technique on the wavelet coefficients of the original image using the key extracted from the adaptive mask (CSF &Edge) on the cover image and the factor extracted from step 6.
Step 8: Apply the embedding technique of the encrypted image on the adaptive mask of the wavelet edge detection cover image.

Modify the wavelet coefficients of the cover image with the values of The encrypted watermark where $\lambda_{wi}$ is the wavelet coefficients value of the encrypted watermark, $\lambda_o$ is the wavelet coefficients of the original image and α is the scaling factor, Wi is the weight of each sub band and $\alpha_k$ is the Scaling factor.

$$\lambda_i = \lambda_o + \alpha_k \, Wi \, \lambda_{wi}$$

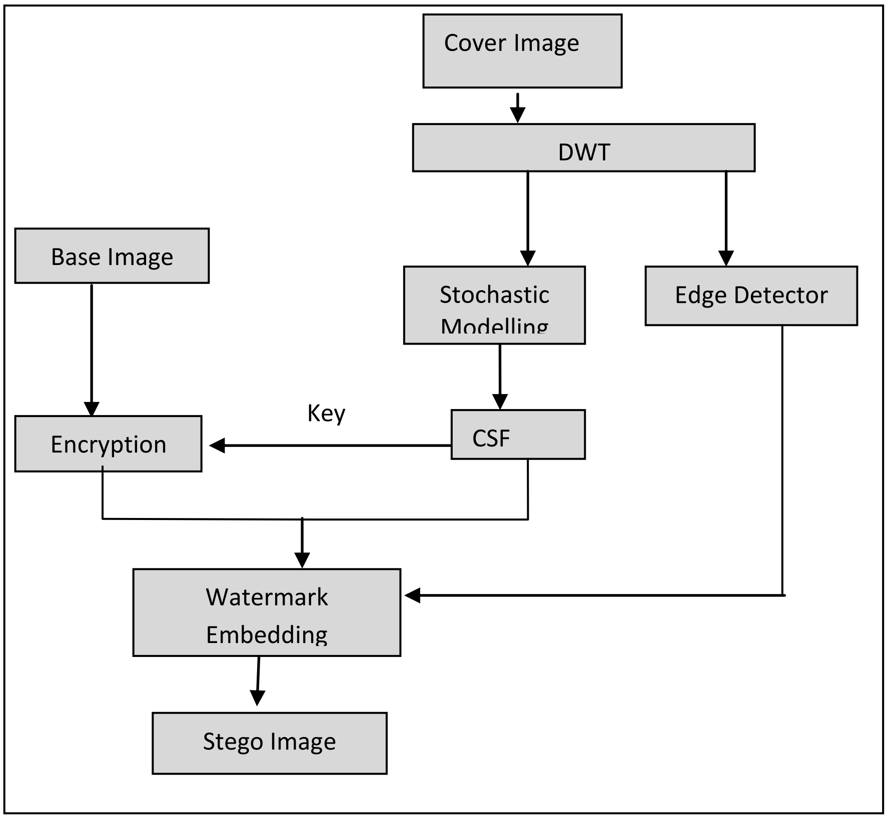


**Figure 3. Block Diagram of the Steganographic Embedding Algorithm**

- ***Extraction Algorithm***

Step 1: Input the Stego image, the key, the Scaling Factor$\alpha_k$.
Step 2: Apply the Discrete Wavelet transform up to 5 levels using HAAR wavelet on the Stego image
Step 3: Apply the perceptual stochastic model (CSF masking) on the wavelet transform of the Stego image using the adaptive masking (CSF &Edge) getting the CSF weights (Wi).

Step 4 : Applying the Multilevel wavelet transform to the eight level and get the wavelet approximation coefficients , rounding the last four coefficients to the integer part then getting these coefficients F2.
Step 5: Apply the extraction Technique using the equation
$\lambda_0 = \lambda_i - \alpha_k \, Wi \, \lambda_{wi}$
Step 6: Apply Decryption Technique on the wavelet coefficients of the extracted image using the input key extracted from the adaptive mask (CSF &Edge) on the cover image and the factor extracted from step 6.

Step 7: convert the extracted watermarked image after decryption from grayscale into color image then restore it to the its original size.

## V. SIMULATION AND SECURITY ANALYSIS

***Security Analysis***

The security level depends mainly on the security key and its space so the security level is low due to lack of security keys or small key spaces and high if the key space is large [3].

In our System the security key space of the Encryption Watermark Embedding Algorithm consists of the type of the edge detectors, wavelet coefficients of the logo to be embedded, CSF weights of the cover image and the encryption method and its security keys for encryption process. Their combination of these factors forms the key space of the presented encryption algorithm. It is impossible for the unauthorized users to decode the encrypted image by deducing the correct combination of the security keys via exhausted searching all possible choices in the security key space. Consequently, the image can be protected with high level of security.

***The performance analysis***

For evaluating the performance of the Encryption system and assure that the original image can be completely reconstructed without any distortion and the reconstructed image is visually the same as the original image. This can be also demonstrated by the histogram of each image (original & Decrypted) Also the image quality is measured using PSNR (Peak Signal to Noise Ratio).

**A. Peak Signal to Noise Ratio (PSNR)** as a measure of visual quality of the Encryption technique system which is calculated as the Mean Square Error (MSE) between the original and the encrypted image

$$\text{PSNR} = 10 \log\frac{255^2}{\text{MSE}}$$

$$\text{MSE} = \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - I^i(i,j)]2$$

M and N are the size of the frame , I(i,j) , $I^i(i,j)$ are the pixel value at location (I,j) of the original and the watermarked image The low PSNR means positive correlation with the degradation in image quality while high PSNR means clear images.

**B. Visual Quality**

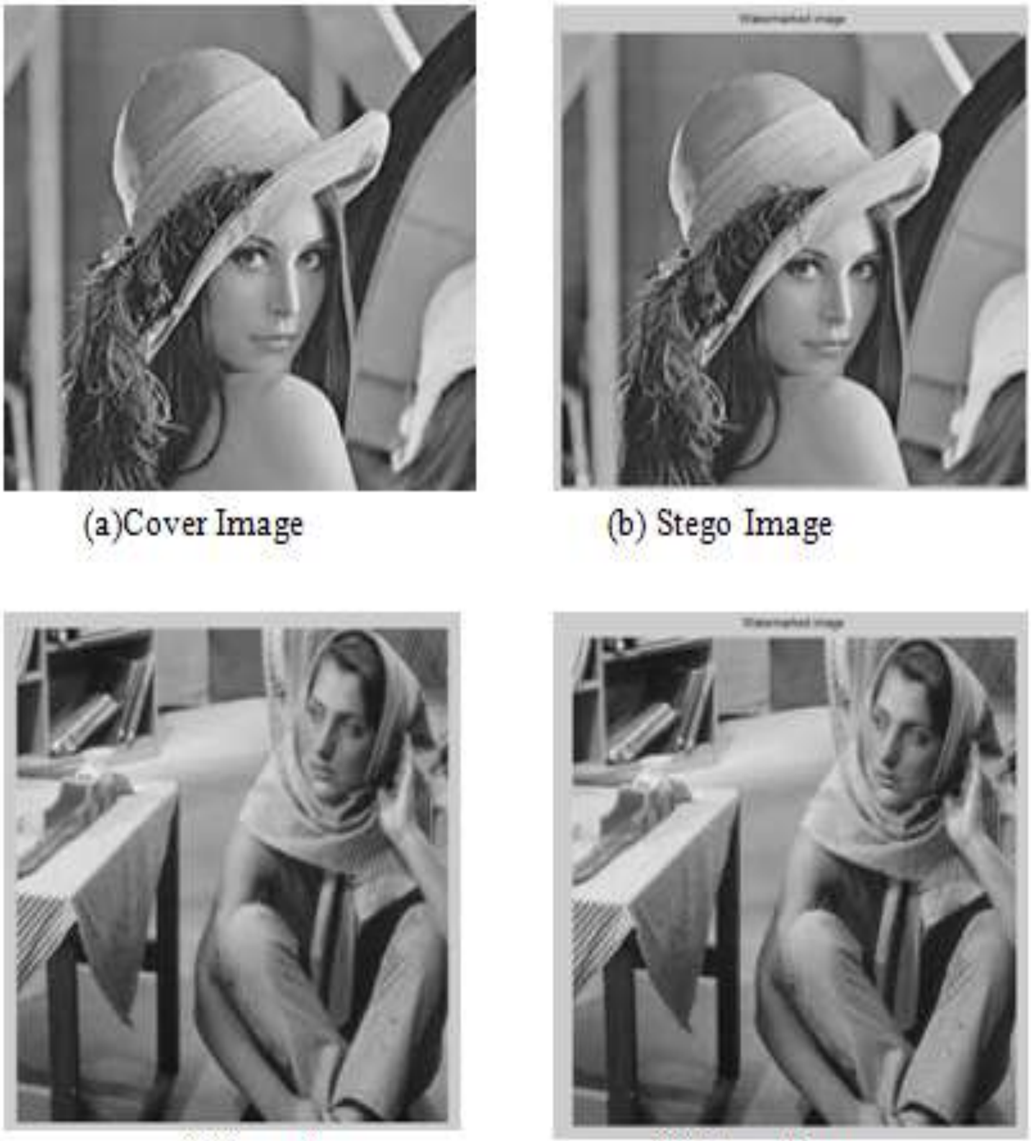
The system incorporates the sensitivities of the human visual system (HVS) which enhance performance so for specifying the visual quality we have two parameters to assess, First one is the visual quality of the encrypted image compared to the original image which can be determined through the image histogram and PSNR, Second parameter is the visual quality of the encryption process itself and the visibility of the encrypted image into the cover image compared to the cover image.

- ***Noise Attacks***

The effective attack handling is essentially required during testing of image after applying the steganographic technique. We here tested the images using one of the attacks which is Pepper-Salt noise Attack [6] which causes on and off pixels adds salt and pepper noise to the image.

The algorithm operates in a transform space is not affected by visual attacks. So the steganographic messages can be seen on the low bit planes of an image as they overwrite visual structures and this is measures using the PSNR values declared in Table(1).

- **Simulation results**



(a)Cover Image (b) Stego Image

(a)Cover Image (b) Stego Image

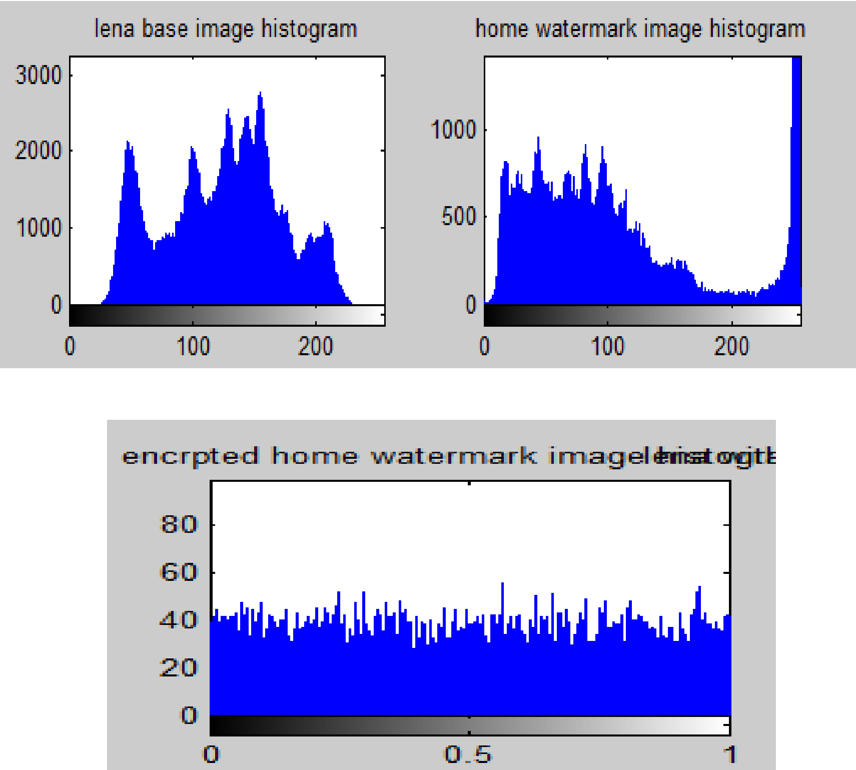
**Figure 4. Cover Image, Stego Image with Steganography algorithm**

**Figure 5. The base image,  Encrypted base image & Decrypted base Image**

We choose Sobel method for edge detection with threshold 0.3.

The proposed method has the closest luminance maintenance compared with the original image which is shown clearly from the photos. The encrypted image just shows some blurring but this blurring doesn't indicate it has a hidden image on it.

The decrypted image has the same quality as the encrypted image as shown in figure 5.



**The histogram of the cover image (Lena image) & base image & encrypted base image**

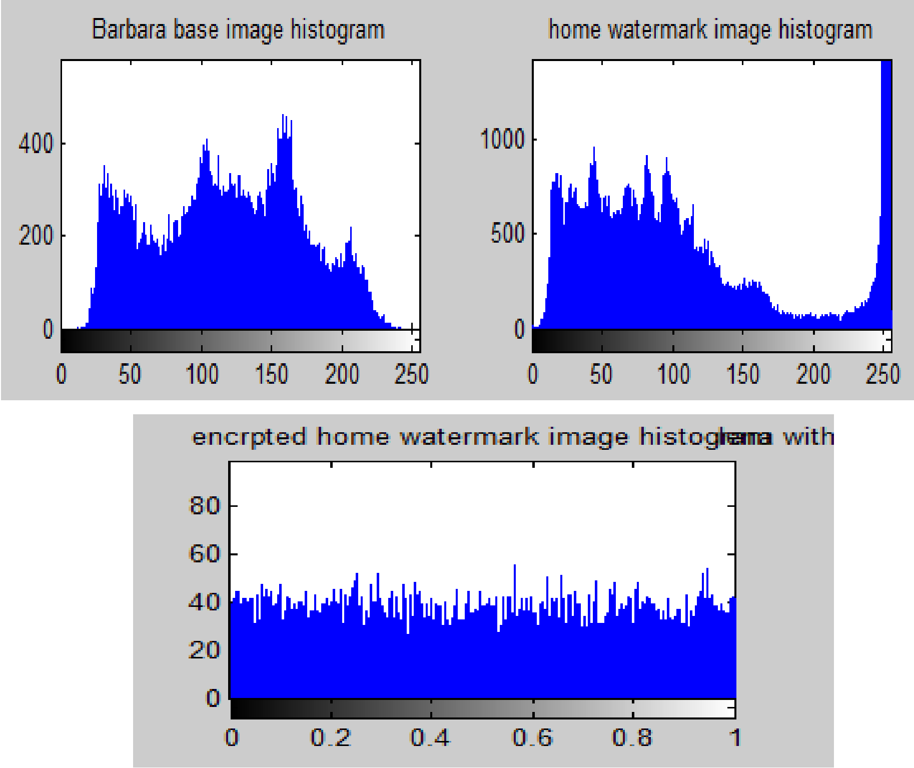


**Figure 6. The histogram of the cover image (Barbara) & base image & encrypted base image**

We applied the salt &pepper attack on the watermarked Image as shown in Figure 7.

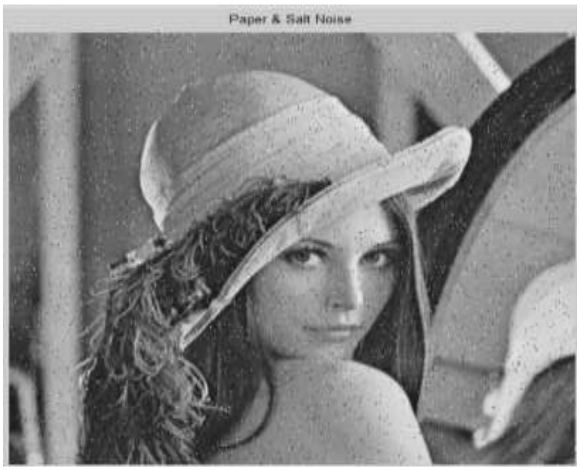


**Figure 7 Salt & Peeper Attack on the Stego Image**

Extracting the Embedded base image after the attack and measuring the PSNR for the encrypted base Image its value is 19.81 which is reasonable value

| | Stego Image | Stego after noise attack | Extracted Secret Image | Extracted Secret After Attack |
|---|---|---|---|---|
| **Lena** | 24 | 20.75 | 21.53 | 19.81 |
| **Barbara** | 23.62 | 19.45 | 21.24 | 18.76 |

**Table 1: The PSNR Values in dB of (the stego image with respect to cover image). (Extracted secret image with respect to original secret image) and after the noise attack.**

## VI. CONCLUSIONS

In this paper, we have proposed an efficient steganographic technique based on the CSF adaptive wavelet transform. and The proposed algorithm provides additional security to the encrypted image based on two levels first the physical level as the cover image look normal as the watermarking technique is highly imperceptible as it depends on the stochastic features of the wavelet transform and CSF weights and the second level is the encryption technique itself increasing the difficulty of detecting the encrypted image as we have large key space and the difficulty in detection of the encryption key as it depends on the multilevel wavelet coefficients ,The experimental results show that the algorithm has good subjective quality and the PSNR is high for the decrypted image.

Thereby, this technique could greatly strengthen the enforcement of copyright law on the Internet also using the wavelet transform on the encrypted image reduces the time for encryption and save the network bandwidth.

## REFERENCES

[1]. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, " Steganography And Digital Watermarking",2004

[2]. "Wavelet Domain Watermarking Capacity Analysis", Fan Zhang and Hongbin Zhang, The College of Computer Science, Beijing University of Technology, Beijing 100022, China 2001

[3]. NF Johnson, Z Duric, S Jajodia - , "Information Hiding: Steganography and Watermarking-Attacks and Countermeasures",2000

[4]. Min-Jen Tsai and Jung Liu Institute of Information Management ,"The Adaptive Content and Contrast-aware Technique for Visible Watermarking" ,2011

[5]. Sviatoslav Voloshynovskiyyz, Alexander Herrigely, Nazanin Baumgaertnery, and Thierry Punz ,"A Stochastic Approach to Content Adaptive Digital Image Watermarking",1999

[6]. T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier ," AN OVERVIEW OF IMAGE STEGANOGRAPHY ", Information and Computer Security Architecture (ICSA) Research Group 2003

[7]. Ali Al-Ataby1 and Fawzi Al-Naima," A Modified High Capacity Image Steganography techniques based on wavelet transform ", 2010.

[8]. A. A. Abdul Latef "color image steganography based on discrete wavelet and discrete cosine transforms ", 2011.

[9]. Long Bao, Yicong Zhou*, and C. L. Philip Chen ,"Image Encryption in the Wavelet Domain",2013

[10]. Ch. Samson, V. U. K. Sastry, "A Novel Image Encryption Supported by Compression Using Multilevel Wavelet Transform" , (IJACSA) Vol. 3, No. 9, 2012

[11]. J.L. Mannos and D.J. Sakrison, "The effects of a visual fidelity criterion on the encoding of image," IEEE Transactions on Information Theory, vol. 20, no. 4, pp. 525–536, July 1974.

[12]. Yicong Zhou*a, Karen Panettaa, Sos Agaianb," Image Encryption Based on Edge Information" 2009