# Enhanced Digital Image Hiding Technique Using Integer Wavelet Transform

[1]Dr.Ibraheem Nadher Ibraheem, [2]Inteasar Yaseen Khudhair
*[1]Faculty of Basic Education, Al- Mustansiriya University, Baghdad, Iraq*
*[2]Faculty of Basic Education, University of Diyala, Diyala, Iraq*
*[1]Ibraheemnadher@uomustansiriyah.edu.iq, [2]Ibraheemnadher@gmail.com,*
*[3]Inteasar_yassin@yahoo.com*

### *Abstract*

*The information hiding technique used in our proposed method depends on the biometric features of the image, one of the highly accurate features is the skin color feature that we used in this research. The progress of digital data information increases the need to secure our information and protect the confidingly of them. For that reason, steganography is one of these technologies as art to conceal data within data. Here secret data are hidden in a selected cropped skin region. Before stashed secret message first order Integer Wavelet Transform (IWT) transfer the skin region into four sub-bands (cA, cH, cV, and cD), Pixel Value Differencing (PVD) technique is used to stash the secret information into the cropped region. This process continues until all secret bits are stashed in the selected skin region. Inverse IWT is implemented and merging the cropped region to the cover image to produce stego image. This study shows that the enhancement image concealing method gives a high performance in capacity, invisibility, undetectability, and good MSE & PSNR values.*

## 1. Introduction

The internet made it is easy to share information in different forms like text, audio, and video. Therefore it becomes very necessary to apply protection strategies to protect this information. These strategies include cryptography, steganography, and coding. Steganography refers to concealing secret information in different media types such that images, video or audio in any way that this secret information must be unnoticeable.

Digital images are more accurate media for concealing information because it is quite easy to place any kind of data on it and the availability of adequate redundant regions was useful information could be stashed in an imperceptive way. The image could be used in a spatial or frequency domain to stash secret information. The pixel values are used to stash the secret information in the spatial domain while the coefficients are used to stash secret data in the frequency domain [1,2].

In general, spatial domain, methods are susceptible to perceptual attacks and pixel variation[11], while the transformation domain techniques are more muscular against image processing actions because of its concealing scheme in notable regions of cover images [3].

Many steganography methods features are introduced to measure the hardness and feebleness of these methods. The significance of each feature relies on the application.

- Capacity: it calculates the entire amount of bits that can be concealed in the cover image.
- Robustness: it calculates the ability of the stashed data to still in the act if the stego image attached.
- Undetectable: the stashed algorithm is undetectable if the stego image is convenient with a model of the source from which original images are drawn.
- Invisibility: the stashed message is invisible if the HSV is unable to discern between images that contain stashed data and those that do not.
- Security: the stashed algorithm is secure when stashed information is unable to remove after being discovered by an intruder [4,5].

ISSN: 2005-4297 IJCA

## 2. Wavelets Transform

Wavelets can be practice to withdraw information from many different kinds of data, but certainly not restricted to audio and images. The set of corresponding wavelets is helpful in wavelet-based compression and decompression algorithms where it is desirable to recover the source information with minimal loss. figure 1 shows an example of first-order decomposition wavelet transform.

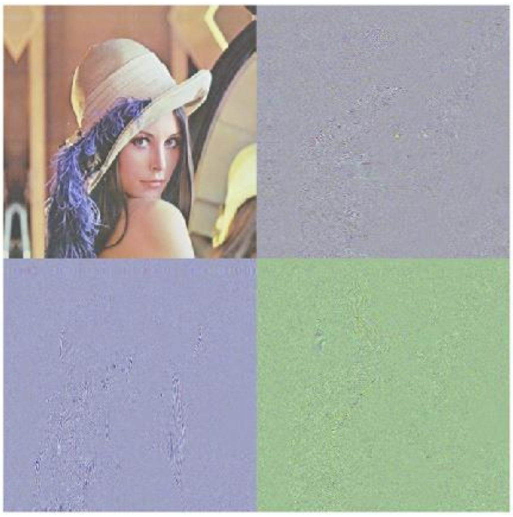

**Figure 1.** First Order Decompsion Wavelet Transform

## 3. Discrete Wavelet Transform (DWT)

The use of DWT will mostly to route the capacity and robustness of the information concealing system features. It labels and applies steganography in the Domain of the wavelet. The hierarchical impression of the Wavelet rendition allows multi-resolution perception of the hidden messages, which is an erratic vector of Gaussian distributed added to all the high passbands in the Wavelet field [6].

## 4. Integer Wavelet Transform (IWT)

IWT is a kind of wavelet transform which address integer data set with another integer data set. The cause for choosing IWT over DWT is that IWT draws the integer data set to another integer dataset whereas DWT changes the floating-point values to an integer by truncation process. Truncation product in the lack of data. When the input data is in the kind of integer, ideal reconstruction is viable while applying Inverse transform.

the major advantage of using IWT that its decomposed sub bands values have the same range as the source image pixel values. This makes easier enforcement discernment regarding the size of the variables to be used and the escape to provide for in the coding algorithm [7].

## 5. Integer Haar Wavelet Transform (IHWT)

the advantages of the wavelet transform, mainly IWT, researchers favor using the IHWT via a lifting scheme that has been applied by [17] to works on the image in the frequency domain. This IHWT is expanding from Discrete Haar Wavelet Transform (DHWT) via a lifting scheme. It maps integer pixel values of an image into the integer wavelet coefficients and inversely.

To transform an image into wavelet subbands, an image is split up into 2x2 non-overlapping blocks. Let

$$\begin{bmatrix} p_{i,j} & p_{i,j+1} \\ p_{i+1,j} & p_{i+1,j+1} \end{bmatrix} \tag{1}$$

perform a 2x2 block of the image where pi,j is a pixel at row i and column j on each block of an image. Then, IHWT will be applied on each block of the image to gain wavelet coefficients in subbands cA or LL, cH or HL, cV or LH, and cD or HH, as follows [8,9]:

$$cA = \left\lfloor \frac{\left\lfloor \frac{p_{i,j} + p_{i,j+1}}{2} \right\rfloor + \left\lfloor \frac{p_{i+1,j} + p_{i+1,j+1}}{2} \right\rfloor}{2} \right\rfloor \qquad (2)$$

$$cH = \left\lfloor \frac{p_{i,j} - p_{i,j+1} + p_{i+1,j} - p_{i+1,j+1}}{2} \right\rfloor \qquad (3)$$

$$cV = \left\lfloor \frac{p_{i,j} + p_{i,j+1}}{2} \right\rfloor - \left\lfloor \frac{p_{i+1,j} + p_{i+1,j+1}}{2} \right\rfloor \qquad (4)$$

$$cD = p_{i,j} - p_{i,j+1} - p_{i+1,j} - p_{i+1,j+1} \qquad (5)$$

## 6. Pixel Value Difference (PVD)

In the PVD technique, as advise by Wu et al. [1, 2], a gray-valued cover image is subdivided into non-overlapping regions composed of two continuous pixels, $P_i$, and $P_{i+1}$. For each region, difference value $d_i$ is counted by subtracting $P_i$ from $P_{i+1}$. Since the pixel value scope from 0 to 255, the difference value also scopes from −255 to 255. Therefore, $|d_i|$ scope from 0 to 255 [10].

## 7. Proposed Method

The enhanced method conceals secret Messages into the RGB color image. It uses many techniques to conceal secret messages. In the frequency domain, the image is subdivided into four regions using IWT and then the PVD technique is adopted to conceal secret data in the wavelet coefficients of the three subbands. The cover image is transformed using a 2D IHWT to obtain four sub-regions: cA, cH, cV, and cD. The enhanced method stash data in the coefficients of two sub-regions by using the PVD technique.the proposed method consist of two main part the stashing process and the extraction process and each one included many steps, as follows:

### 7.1. The Embedding Process

In this part, the secret message will be stashed in the cover image to generate stego image, figure 2 illustrates the main steps of this part.

St1: load cover image 256×256 RGB Color Image.
St2: load secret Image 64×64 binary image.
St3: scan the cover image for skin tone color regions and map them.
St4: select a proper region and save their elementary for the stashing process.

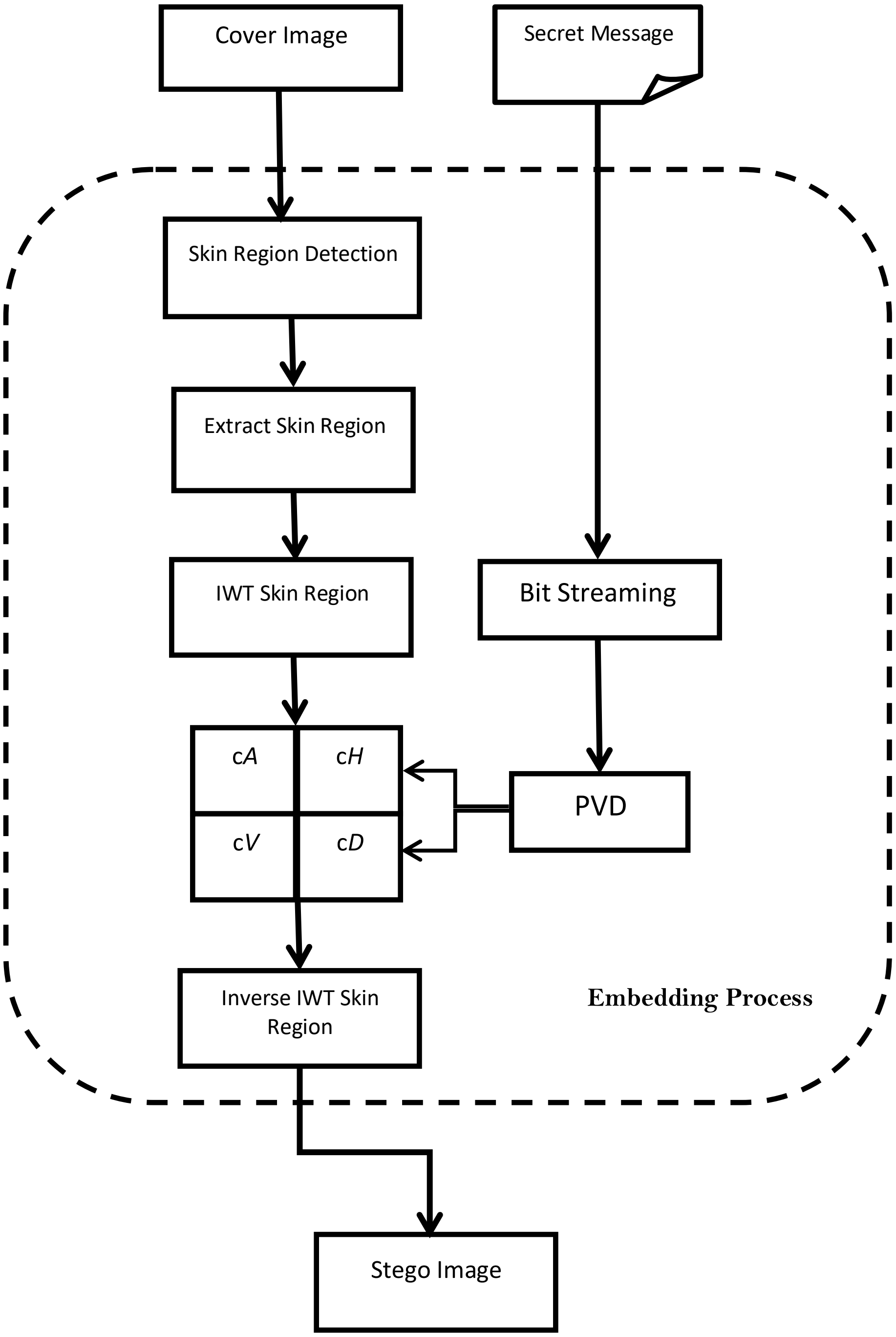

**Figure 2.** The Embedding Process

St5: find the threshold value (T) that preventing pixel values from fall off the scope [0 255] by applying the following equation:

$$p(x,y) = \begin{cases} \propto T & if\ p(x,y) < \propto T \\ 255 - \propto T & if\ p(x,y) > \propto T \end{cases} \tag{6}$$

St6: applying first order IWT on the extracted region only to produce four sub-bands cA, cH, cV, and cD.

St7: translate the secret image to binary stream a set of 0's and 1's.

St8: using PVD classical technique to stashed a secret image bitstream into two selected IWT bands cH and cD from the green and blue planes of the cover extracted region and keep red plane without any stashing because the skin color detector is very sensitive to the red plane and the receiver on the other side will be able to perform the skin color region to extract the secret image.

St9: apply the inverse IWT on the four subbands to reconstruct the skin region.

St10: combine the reconstructed skin region with the original image to create the stego image.

### 7.2. The Extraction Process

Secret message (64×64) will be extracted from stego image (256×256) as a final step of the proposed technique, figure 3 illustrate the main steps of this part.

St1: load stego image 256×256 RGB Color Image.

St2: scan the cover image for skin tone color regions and map them.

St3: select the region that contains the secret information (the method saves some eliminator that the receiver can gain this region directly).

St4: applying first order IWT on the extracted region only to produce four sub-bands cA, cH, cV, and cD.

St5: using the Inverse PVD technique to extract a secret image bitstream from the two selected IWT bands cH and cD from the green and blue planes of the cover extracted region.

St6: reconstruct the secret image from the bitstream.

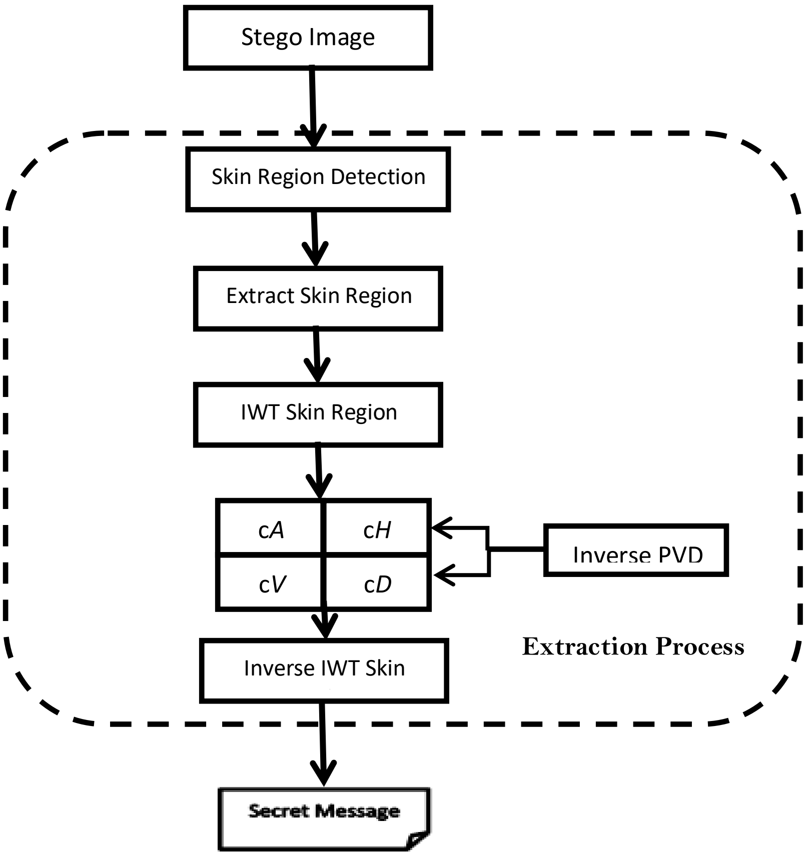

**Figure 3.** The Exraction Process

### 8. the Experimental Results

Testing the proposed enhance image concealing technique over four differents 256×256 color image sees figure 4,

**Figure 4.** Four Tested Cover Images

with two different 64×64, secret images see figure 5.

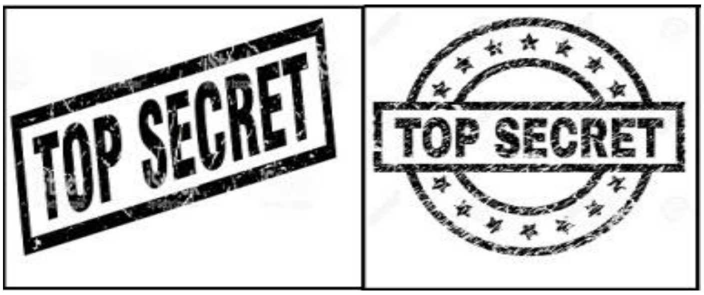

**Figure 5.** Two Tested Secret Images

These are implemented by matlab7.1. the results in table 1 show that the method gives a high performance in capacity, invisibility, undetectability, and good MSE & PSNR values, also the T value that satisfies the number of secret bits that can be stash into the cover image.

| Stego Image | MSE | | | PSNR | | |
|---|---|---|---|---|---|---|
| | T=1 | T=2 | T=3 | T=1 | T=2 | T=3 |
| Lena | 0.01607 | 0.024 | 0.05152 | 66.068 | 64.328 | 61.02 |
| Boat | 0.01675 | 0.02521 | 0.05046 | 65.888 | 64.113 | 61.1 |
| Women | 0.01561 | 0.02355 | 0.04455 | 66.068 | 64.409 | 61.642 |
| Sad Women | 0.01547 | 0.02315 | 0.04251 | 66.235 | 64.484 | 61.845 |

**Table 1. Stego Image Quality**

## 9. Conclusions

Advanced picture steganography gets to be an vital way to stow away the presence of a mystery message. This paper proposes a strategy to stow away the information on the IHWT Transofmation space by calculating the contrast between two neighboring wavelet coefficients. In this coefficient contrast computed unbounded accuracy number is found to be reasonably consistent with the IWT. Three threshold values are utilized to implant the message into cover pictures. The exploratory comes about appear that the threshold values of 1 gives superior picture qualities and more vigor, whereas the threshold values of 2 and 3 give bigger capacity

## References

[1] D.-C.Wu andW.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[2] H. C. Wu, N. I. Wu, C. S. Tsai, and M.-S. Hwang, “Image steganographic scheme based on pixel-value differencing and LSB replacementmethods,” IEE Proceedings—Vision, Image and Signal Processing, vol. 152, no. 5, pp. 611–615, 2005.

[3] S. Bhattacharyya and G. Sanyal, “Data Hiding in Images in Discrete Wavelet Domain Using PMM,” World Acad. Sci. Eng. Technol., vol. 44, pp. 597–605, 2010.

[4] Alaa Taqa, A.A Zaidan, B.B Zaidan ,“New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm”, International Journal of Computer and Electrical Engineering (IJCEE),Vol.1 ,No.5, ISSN: 1793-8163, p.p.566-571 , December (2009). Singapore.

[5] B.B Zaidan , A.A Zaidan ,Alaa Taqa , Fazidah Othman ,“ Stego-Image Vs Stego-Analysis System”, International Journal of Computer and Electrical Engineering (IJCEE),Vol.1 ,No.5 , ISSN: 1793-8163, pp.572-578 , December (2009), Singapore.

[6] B.Alhayani,H.Ilhan, (2010). Efficient cooperative imge transmission in one-Way mult-hop sensor network,” International Journal of Electrical Engineering Education,vol. 6, pp. 1–17.

[7] B.Alhayani, H. Ilhan, (2020). “Image transmission over decode and forward based cooperative wireless multimedia sensor networks for Rayleigh fading channels in medical internet of things (MIoT) for remote health-care and health communication monitoring,” Journal of Medical Imaging And Health Informatics, vol. 10, pp. 160-168.

[8] B.Alhayani, Milind Rane. (2014). ”face recognition system by image processing” International journal of electronics and communication engineering & technology (IJCIET),vol.5, no.5, pp. 80–90.

[9] B.ALhayani, Haci Ilhan (2017). “Hyper spectral image classification using dimensionality reduction techniques”, International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering,, vol.5, pp.71-74.

[10] Huang J., Kim H. J., Xiang. S., (2008), ‘Audio watermarking robust against time-scale modification and MP3 compression,’ IEEE Journal on Signal Processing, Vol.88, No.10, pp. 2372–2387.

[11] Jayasudha.S.,(2010),’Integer Wavelet Transform based on Steganographic method using OPA'.

[12] J. Xu, A. H. Sung, P. Shi, and Q. Liu, “JPEG Compression Immune Steganography Using Wavelet Transform,” in International Conference on Information Technology: Coding and Computing (ITCC), Volume: 2, 2004, pp. 704–708.

[13] D. Wu and W. Tsai, “A Steganographic Method for Images by Pixel-Value Differencing,” Pattern Recognit. Lett., vol. 24, no. 9–10, pp. 1613–1626, 2003.

[14] H. C. Wu, N. I. Wu, C. S. Tsai, and M.-S. Hwang, “Image steganographic scheme based on pixel-value differencing and LSB replacementmethods,” IEE Proceedings—Vision, Image and Signal Processing, vol. 152, no. 5, pp. 611–615, 2005.