



An Improved Image Steganography Technique Using Discrete Wavelet Transform

Richika Mahajan, B.V. Kranthi
Electronics and Communication Engineering
Lovely Professional University
Jalandhar, Punjab, India

Abstract: This paper proposes a new method for hiding a data in frequency domain. In this a spatial domain technique adaptive pixel pair matching is applied on frequency domain with some new modifications in calculating B-ary notational system, selecting the co-ordinate pair for making new frequency values and also in secreting data. Discrete wavelet transform is preferred for embedding the secret data. Data is embedded in the middle frequencies because they are more enormous to attacks than that of high frequencies. Coefficients in the low frequency sub-band preserved unaltered to improve the image quality. The experimental results shows better performance in discrete wavelet transform as compared with the spatial domain.

Index Terms: Discrete Wavelet Transform, Image Steganography, Adaptive Pixel Pair Matching (APPM)

I. INTRODUCTION

In the recent years due to the wide growth of digital communication and information technologies difficulty in ensuring privacy challenges increases. Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. The method which makes the information encrypted so that it is difficult to read till it reaches to the receiver side. This method is known as cryptography. A major drawback to cryptography is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually decrypt the data [1]. A solution to this problem is Steganography. Digital image Steganography plays a very crucial role in secure data hiding. In digital image Steganography, the secret data is embedded within a digital image called cover-image. Cover-image carrying embedded secret data is referred as Stego-image. Steganography can be used as both legal and illegal ways. For example, civilians may use it as privacy protection; while terrorist use it as to spread terroristic data. Fig 1 shows the basic block diagram of image Steganography. In this secret image is embedded into the cover image with an embedding algorithm. A key is used for the security purpose so that the eavesdropper cannot extract the secret data. There are three types of Steganography. (1) Pure Steganography: In this no prior information is required before sending the data therefore no key is used. (2) Secret key Steganography: One key is used by both the sender and receiver. (3) Public key Steganography: Public key Steganography does not depend on the exchange of a secret key. It requires two keys, one of them private and the other public: the public key is stored in a public database, whereas the private key is used in the embedding process [2]. The secret key is used to reconstruct the secret message. This process results into the Stego-image. In extraction algorithm reverse process of embedding algorithm is applied to extract the secret data.

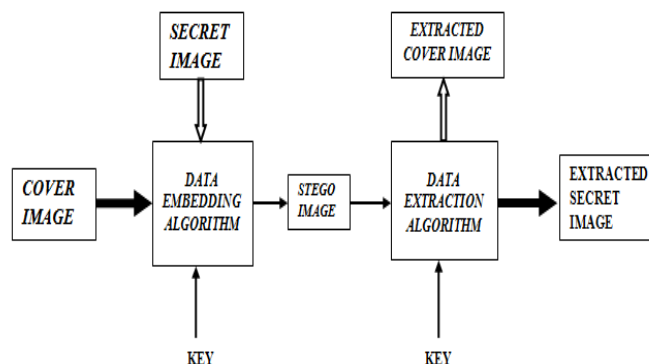


Fig. 1 Basic block diagram of image Steganography

Image Steganography is classified into various domains: spatial domain, frequency domain and spread spectrum [2], [3]. In spatial domain the data is embedded in the intensity value of the pixels directly. It is known as basic

substitution system. The advantage of this type of image Steganography is easy computation and less complexity. However, there are some disadvantages that data embedded can be easily. However, there are some disadvantages that data embedded can be easily detected by some attacks of signal processing techniques like addition of noise, rotation, compression etc. For frequency domain, image is first transform into the different frequency components. Frequency domain methods hide message in a significant area of the cover image which makes them more robust to attack, such as adding noise, compression, cropping some image processing. The most important techniques in frequency domain are discrete cosine transform and discrete wavelet transform. In today's scenario, DWT is more preferred due to its Robustness means more robust to the attacks like blocking artifacts and Perceptual transparency means better image quality than that of DCT [4]. Spread spectrum technique spread the narrow band frequency over the wide band and then the embedding is done in noise but due to its complexity it is less used. Therefore, frequency domain is selected for embedding the data. Following are the required features for image Steganography [3]. (1) Embedding Capacity: It refers to the amount of data that can be inserted into the cover-media without changing its integrity. (2) Perceptual transparency: This concept is based on the properties of the human visual system. The embedded information is imperceptible if an average human is unable to distinguish between carriers that do contain hidden information and those that do not contain the information. (3) Robustness: Robustness refers to the ability of the embedded data to remain intact if the Stego-system undergoes transformation, such as linear and non-linear filtering; addition of random noise; and scaling, rotation, and loose compression. (4) Computational complexity: Computational complexity of Steganography technique employed for encoding and decoding is another consideration and should be given importance.

II. LITERATURE REVIEW

The most common and widely used in spatial domain is least significant method. In this directly LSB of the cover image is replaced by the message bits. The major drawback of this method is its vulnerability to various statistical attacks [3]. In [2003] chan [5] *et al.* the limitations of LSB method is improved by optimal pixel adjustment method. This method reduces the image distortion of LSB. In this method some conditions are applied and if the resultant produces less distortion then it is modified unless kept unmodified. Then Pixel pair matching method (PPM) came which uses pixel pair for embedding [6]. The basic idea is replacing the pixel pair (x, y) as a co-ordinate with a new searched co-ordinate (x', y') with in a predefined neighborhood set ϕ (x, y). In [2006] zhang [7] *et al.* proposed exploiting modification direction method in which (2n+1)- ary notational system is introduced according to which only one pixel is increased or decreased by 1. The drawback of this method is lower payload. In [2009] chao [8] *et al.* proposed diamond encoding which increase the payload of EMD method. The drawback of DE is it forms the B- ary notational system of some embedding parameters. When k is 1, 2 and 3 the B- ary is 5, 13 and 25- ary notational system. In [2012] hong [6] *et al.* proposed a new method known as adaptive pixel pair matching. This allows selecting the digit in any B- ary notational system which overcomes the limitation of DE. This method fulfills the basic requirement of PPM fully. (1) There must be exactly B coordinates in neighborhood sets. (2) The characteristic values must be mutually exclusive. (3) The best B must be selected which achieves lower embedding distortions and the design of neighborhood sets and characteristic value should be capable of embedding digits in any B- ary notational system.

For frequency domain, In [2012] P.Rajkumar [9] *et al.* the comparative analysis of spatial and frequency domain techniques. The result of this paper shows spatial domain technique is easy to implement and encode with high payload where as frequency domain is more robust to statistical attack and have low payload capacity. This paper also shows comparison between DCT and DWT. Discrete wavelet transform is more robust in blocking artifacts and also have good perceptual transparency than discrete cosine transform [4]. There are different algorithms for DWT. In [2006] chen [10] *et al.* proposed DWT based approach. In this paper data embedding is done in the LSB's of the frequency components. It also satisfies the requirement of different users. It determines the two modes of embedding data. The mapping technique is applied on the secrete bits for increasing the security. The two embedding modes described in it are varying mode and fix mode. In varying mode the embedding capacity varies however in fix mode embedding capacity do not change. In accordance to these techniques its peak signal to noise ratio varies. It also gives the detail view how data embedded in various sub-bands. The drawback of this is the key matrix used for secret data manipulation is not good because extra data is also embedded therefore new method required to enhance its authentication and improve its embedding capacity by reducing embedding of extra data in the original image. In [2010] song [11] *et al.* proposed a method based on authentication in which chaotic logistic map is used to randomize the secret data. In this first chaotic sequence is generated and then applying some threshold binary sequence formed. Data is embedded in DWT coefficients. In [2011] Ghasemi [12] *et al.* proposed a method to improve the embedding capacity by using genetic algorithm and imperceptibility is improved by using OPAP method. The drawback of this method is computational complexity is high.

This paper proposed a method in which a spatial domain technique APPM with some modification is applied in discrete wavelet transform of frequency domain. In this technique of APPM pixel pair is selected to embed with all conditions satisfied of PPM. Here data is embedded in the pair of frequency coefficients. The proposed

method improves the robustness and imperceptibility than APPM. The rest of this paper is organized as follows. Section III reviews some correlated area and describes the proposed work. Section IV shows the simulation results and analysis. Section V includes the concluding remarks.

III. PROPOSED WORK

In this section, Haar- Discrete wavelet transform and proposed method followed are discussed in detail.

A. Haar- Discrete wavelet transform

Haar wavelet is the simplest wavelet and most commonly used. It is applied in two ways: one is horizontal way and other is vertical way. First, scan the pixels from left to right in horizontal direction. Then perform addition and subtraction operation on neighboring pixels also multiply with the scaling function for Haar wavelet is $1/\sqrt{2}$. Store the result of addition on left half and addition on the right half. Let us consider the starting pixel A and neighboring pixel B.

$$\text{Sum on left side} = \frac{A+B}{\sqrt{2}} \quad (1)$$

$$\text{Difference on right side} = \frac{A-B}{\sqrt{2}} \quad (2)$$

Repeat the process until it covers all the rows. The pixel sum is represented by low frequency and difference is represented by high frequency. Secondly, scan the pixels from top to bottom in vertical direction. Then perform addition and subtraction operation also multiply by $1/\sqrt{2}$. Store the result of addition on top and subtraction result on bottom. For doing these operations filter bank is used as analysis and synthesis [13].



Fig. 2 Input image with different sub-bands after applying DWT

B. Embedding procedure

STEP 1: Secret data is the data we want to conceal. In this data to be concealed is image. In this step we first convert the secret image grayscale pixel values into binary bit stream. Then according to the embedding requirement we divide these bits into several groups like 2, 3, 4 etc. and its embedding on the frequency sub-bands of cover image in which we want to hide data depend on key. Key k is used as a security purpose which determines the embedding sequence.

STEP 2: Let the cover image of size $M \times M$. Apply Haar- DWT to separate low, high and middle frequencies each of size $M/2 \times M/2 = M1 \times M1$. Data is embedded in middle frequency components.

STEP 3: Adaptive pixel pair matching is used for embedding the data with some modifications. Find the B- ary notational system by using

$$B = 2^{\wedge} (n / (M1 \times M1)) \quad (3)$$

Here n is the number of bits to be embedded. Number of bits is calculated by

$$n = (\text{size of secret image} \times 8) \text{ bits} \quad (4)$$

Now calculate the bits per pixel which is calculated by

$$\text{Bits per pixel} = \frac{\text{number of bits to be embedded (n)}}{M1 \times M1 \times 2} \quad (5)$$

Bits per pixel determine the matrix size required to cover the value equal to B-ary notational system. Find characteristic values $f(x,y)$ where x and y are the coordinates of the B-ary notation formed.

$$f(x,y) = (x + C_B \times y) \bmod B/10 \quad (6)$$

C_B is constant and can be obtain by solving the given pair (x, y) and given integer value B. Then find the neighborhood sets $\phi(x,y)$, where x and y are the co-ordinates of the center value, x_i and y_i are the other co-ordinates along (x, y).

$$\text{Minimize: } \sum_{i=0}^{(B-1)/10} (x_i - x)^2 + (y_i - y)^2$$

$$\text{Subject to: } f(x_i, y_i) \in \{0, \dots, (B-1)/10\}$$

$$f(x_i, y_i) \neq f(x_j, y_j) \quad \text{if } i \neq j \text{ for } 0 \leq i, j \leq (B-1)/10 \quad (7)$$

From the above equation the neighborhood values having minimum distance are selected and other values get neglected. For embedding the secret digit S_B , take the two pixel pair from cover image according to embedding sequence. Find $f(a,b)$ where a and b are pair of frequency components. Determine the modulus distance d between S_B and $f(a,b)$. Repeat the process until data get embedded. Apply inverse discrete wavelet transform to obtain the stego- image.

$$d = S_B - f(a, b) \bmod B/10 \quad (8)$$

Let us explain with the help of example, consider cover image of size 512×512 ; ($M \times M$). After applying DWT on cover image of size 512×512 it became 256×256 each ($M1 \times M1$). Let secret image of size 256×128 . Number of bits can be calculated as $256 \times 128 \times 8 = 262144$ bits. B-ary calculated is 16. Hence we make the secret data according to it. Here C_B is constant its value for B-ary 16 is 6. If (x, y) are $(-0.1, -0.2)$ then $f(x, y)$ is $(-0.1 + 6 \times (-0.2)) \bmod 1.6$ equal to 0.3.

Table I: Constant Values C_B for $2 \leq C_B \leq 64$

C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}
1	1	2	2	2	2	3	3	3	3	4	5	4	4	6	4
C_{18}	C_{19}	C_{20}	C_{21}	C_{22}	C_{23}	C_{24}	C_{25}	C_{26}	C_{27}	C_{28}	C_{29}	C_{30}	C_{31}	C_{32}	C_{33}
4	4	8	4	5	5	5	5	5	10	5	5	5	12	12	7
C_{34}	C_{35}	C_{36}	C_{37}	C_{38}	C_{39}	C_{40}	C_{41}	C_{42}	C_{43}	C_{44}	C_{45}	C_{46}	C_{47}	C_{48}	C_{49}
6	6	10	15	6	16	7	7	6	12	12	8	7	7	7	7
C_{50}	C_{51}	C_{52}	C_{53}	C_{54}	C_{55}	C_{56}	C_{57}	C_{58}	C_{59}	C_{60}	C_{61}	C_{62}	C_{63}	C_{64}	
14	14	9	22	8	12	21	16	24	22	9	8	8	14	14	

It is based on B-ary which is 16. Therefore we require matrix of 5×5 . Here in equation x and y are the coordinates of matrix. After calculating all the values of $f(x, y)$ for all x and y we have a matrix as shown below.

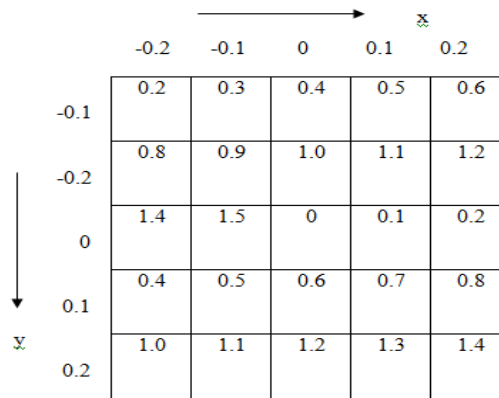


Fig. 3 Characteristic values $f(x, y)$

Therefore the co-ordinates having less values of neighborhood set are considered. Hence we have matrix as shown below.



Fig 4 neighborhood sets $\phi(x, y)$

Table II: Shows Different Neighborhood Co-Ordinates $f(x', y')$

$f(x_{0.1}, y_{0.1})$ = (0.1, 0)	$f(x_{0.5}, y_{0.5})$ = (-0.1, 0.1)	$f(x_{0.9}, y_{0.9})$ = (-0.1, -0.1)	$f(x_{1.3}, y_{1.3})$ = (0.1, 0.2)
$f(x_{0.2}, y_{0.2})$ = (0.2, 0)	$f(x_{0.6}, y_{0.6})$ = (0, 0.1)	$f(x_{1.0}, y_{1.0})$ = (0, -0.1)	$f(x_{1.4}, y_{1.4})$ = (-0.2, 0)
$f(x_{0.3}, y_{0.3})$ = (-0.1, -0.2)	$f(x_{0.7}, y_{0.7})$ = (0.1, 0.1)	$f(x_{1.1}, y_{1.1})$ = (0.1, -0.1)	$f(x_{1.5}, y_{1.5})$ = (-0.1, 0)
$f(x_{0.4}, y_{0.4})$ = (0, -0.2)	$f(x_{0.8}, y_{0.8})$ = (0.2, 0.1)	$f(x_{1.2}, y_{1.2})$ = (0, 0.2)	

Now make the secret data in between the range 0 to $(B-1)/10$. As discussed above cover image is divided into different sub-bands. According to the payload capacity decomposition level can be increased. Here we want to embed 262144 bits we want to embed. After making different groups of four bits in binary we left with 65536 bits. Now these bits we want to embed. Then we are having two frequency sub-band HL and LH in which we want to hide data. Each can embed $(M1 \times M1) / 2$. Therefore half on one rest on other sub- band. Let we have 0.7 secret digit to conceal in frequency coefficients $(-2.4, 5.2)$. Therefore first find the characteristic value $f(a, b)$ where a and b are the frequency components we want to conceal data. $f(-2.4, 5.2) = 0$ and now determine the modulus distance. $d = (0.7 - 0) \bmod 1.6$ is 0.7. Now we find the co- ordinates of 0.7 from Fig.4.3 they are (0.1, 0.1). New frequency components are $(-2.4 + 0.1, 5.2 + 0.1) = (-2.3, 5.3)$. Scan all the frequency components according to key k and repeat till all data get embedded.

C. Extraction procedure

STEP1: Stego- image contains the secret data. Here Steganography is based on transform domain. Therefore data is constrained inside the frequency coefficients. DWT is applied on it. Then data extraction procedure is followed to extract the data.

STEP 2: In extraction scan the frequency components of the sub-bands of middle frequencies in which data is embedded according to the key k. Then calculate the $f(a', b')$ the result obtained is embedded values. Make the value in the range of 0 to $(B-1)$ and form a binary bit stream. According to the input bit sequence make them into different groups of 2, 3 and 4 etc. and convert them to decimal. Hence the secret image is extracted. Let us continue the above example having new frequency components $(-2.3, 5.3)$. $f(a,b) = (-2.3 + 6 \times 5.3) \bmod 1.6$ is 0.7 continue this process till all the data is extracted.

IV. SIMULATION RESULT AND ANALYSIS

In this section, the simulation results and performs some data analysis. The results are performed on four cover images. Each of size 512×512 , gray level images is shown below. To calculate the results two evaluation parameters are PSNR and MSE. Comparison of PSNR and MSE between APPM and Proposed method is shown. Result on different images with payload of 1bits per pixel for constant value of C_B . Data embedding capacity for different B- ary is also shown.

A. Peak signal to noise ratio (PSNR):

The PSNR is commonly used to determine the quality of the stego-image. An approximation to human perception of reconstruction quality, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR. In Steganography it must be above '30dB'.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (9)$$

B. Mean square error (MSE):

It stands for mean square distance between the cover image and stego-image.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (a_{ij} - b_{ij})^2 \quad (10)$$

Where a_{ij} are pixel value at position i and j in the cover image and b_{ij} of stego- image. Smaller the value of mean square error PSNR value is larger.





Fig. 5 Four gray scale images used as cover medium

Table IV: MSE and PSNR Comparison Between APPM and Proposed Method

Methods		APPM		Proposed work	
Payload	B- ary	MSE	PSNR	MSE	PSNR
1	4	0.3754	52.3859	0.0019	75.3945
2	16	1.344	46.847	0.0067	69.8518
3	64	5.1923	40.9772	0.0259	63.994
4	256	20.44	35.495	0.104	57.9585
1.171	5	0.4	52.1102	0.002	75.079
1.831	13	1.077	47.8086	0.005	71.1175



Fig. 6 Four Stego Images

Table V: MSE and PSNR of Images (C_4 , 1 bpp)

	APPM		Proposed method	
Parameters	MSE	PSNR	MSE	PSNR
Lena	0.3762	52.377	0.0019	75.3945
Living room	0.3754	52.3754	0.0019	75.4172
Baboon	0.3747	52.3944	0.0019	75.4175
Private	0.3747	52.3935	0.0019	75.3949

Table VI: Data Embedded Capacity

B-ary	Constant	Embedding capacity
4	2	131072
16	6	262144
64	14	393216
256	60	524288

Table IV depicts the comparison of MSE and PSNR between proposed method in DWT and adaptive pixel pair matching. The result show that proposed method has good results than APPM for different B- ary. For high

payload and 256-ary proposed method shows very small MSE which improves the stego-image quality than that of APPM. Table V shows the results on various images at payload of 1 bpp. Table VI gives the embedding capacity for different B-ary.

V. CONCLUSION

A new Steganography scheme is proposed in this research. A spatial domain technique adaptive pixel pair matching is implemented in frequency domain. As in frequency domain data is embedded in the frequency coefficients which make them more secure and perceptual transparency to human visual system. So, data is hidden in the middle frequencies. Key is used to more secure. The proposed method results shows good peak signal to noise ratio in comparison with the adaptive pixel pair matching. In future work, better security key can be used for decreasing the time duration. More data can be embedded by using some compression techniques and by increasing the decomposition level. Other wavelets can be used for good results.

REFERENCES

- [1] Ankita Agarwal "Security enhancement scheme for image Steganography using S-DES technique" International Journal of Advanced Research in Computer Science and Software Engineering, April 2012.
- [2] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, "Overview: Main Fundamentals for Steganography" Journal of computing, Volume 2, Issue 3, MARCH 2010, ISSN 2151-9617.
- [3] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images" Defence Science Journal Vol. 62, No. 1, January 2012, pp. 11-18, 2012.
- [4] V.Srinivasa rao¹, Dr P.Rajesh Kumar², G.V.H.Prasad³, M.Prema Kumar⁴, S.Ravichand⁵ "Discrete Cosine Transform Vs Discrete Wavelet Transform: An Objective Comparison of Image Compression Techniques for JPEG Encoder" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011 ISSN (Online): 1694-0814.
- [5] Chi-Kwong Chan, L.M. Cheng "Hiding data in images by simple LSB substitution" 2003 Pattern Recognition Society. Published by Elsevier Ltd.
- [6] Wien Hong and Tung-Shou Chen "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching" IEEE Trans., Vol. 7, No.1, February 2012
- [7] Xinpeng Zhang and Shuozhong Wang "Efficient Steganographic Embedding by Exploiting Modification Direction" Xinpeng Zhang and Shuozhong Wang, IEEE Comm. letters, Vol. 10, No.11, November 2006.
- [8] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image datahiding scheme with diamond encoding," EURASIP J. Inf. Security, vol.2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.
- [9] P. Rajkumar , R. Kar , A. K. Bhattacharjee, H. Dharmasa "A Comparative Analysis of Steganographic Data Hiding within Digital Images" International Journal of Computer Applications (0975 – 8887) Volume 53– No.1, September 2012.
- [10] Po-Yueh Chen* and Hung-Ju Lin "A DWT Based Approach for Image Steganography" International Journal of Applied Science and Engineering 2006. 4, 3:275-290.
- [11] Chuanmu Li Haiming Song "A Novel Watermarking Scheme for Image Authentication in DWT Domain" Natural Science Foundation of Fujian Province, China (No. 2008J0197 and No. JA08139).
- [12] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm" International multiconference of engineers and Computer scientists 2011, Vol. I, Hong Kong.