

# Image Steganography Based on Modified Adaptive Pixel Pair Matching and Discrete Wavelet Transform

**Authors: Nan Mo Kham<sup>1</sup>, Nang Aye Aye Htwe<sup>2</sup>**

<sup>1,2</sup>*Department of computer engineering and Information Technology, Mandalay Technological University,  
The Union of the Republic of Myanmar*

<sup>1</sup>*nanmokhammk7@gmail.com*

<sup>2</sup>*htwe.aye@gmail.com*

## Abstract

Steganography is now more important due to need of secure communication in the area of potential and vulnerable computer users. This system proposes a secure method for hiding image based on discrete wavelet transform (DWT) and modified adaptive pixel pair matching (MAPPM) to reduce the distortion in stego image. The essential idea of modified APPM is to construct the non-repeating embedding sequence using key. According to the key sequence, the values of pixel pair as the reference coordinate are firstly to be searched. And then, the neighborhood set of this pixel pair is calculated according to a secret digit. Then that pixel pair is added with reference coordinate's pixel pair to conceal the digit. Image quality measures used for analysis are Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Histogram after embedding the secret image. The proposed system is implemented using Matlab R2016a programming language.

**Keywords:** Modified Adaptive Pixel Pair Matching (MAPPM), Discrete Wavelet Transform (DWT), Mean Square Error (MSE), Peak Signal to Ratio (PSNR)

## 1. Introduction

As need of Internet-based applications is highly increased, so it is required to use the secrecy in communication. To achieve this goal, there are mainly three techniques are available, cryptography, watermarking and steganography. Steganography is the art of hiding information through original object/carrier in such a manner that the existence of the message is unknown. The term steganography is comes from Greek word Steganos, which means, "Covered Writing". Steganography is different from cryptography. The main objective of cryptography is to secure communications by using encryption techniques. But steganography techniques are used to hide the messages, which makes difficult for a third party / person to find out the message. Watermarking and fingerprinting related to steganography are basically used for intellectual property protection. The five main categories of file formats that can be used for steganography are: text, image, audio and video steganography [1].

Digital images are widely used over the internet as well as that are also popular. Now using this phenomenon the digital images can be used as a cover images/objects for the steganography. Digital image steganography techniques can be divided into Spatial Domain Techniques and Frequency Domain Techniques. There are many versions present in spatial steganography that all are related to make changes directly with some bits of the digital image pixel values to hide data. Frequency Domain Techniques is a more complex technique of hiding information in an image. Most of the strong steganographic algorithms work in the transform domain because the process of embedding data in the frequency domain of a signal is much stronger than any other domain such as time or etc. Transform domain techniques are more advantageous than spatial domain because it hides information in such parts of image that are less exposed to image processing, cropping and compression [2]-[4].

In this system, adaptive pixel pair matching in a spatial domain technique 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 embedding the secret data. Key is also used as a security purpose which determines the embedding sequence. Discrete wavelet transform is used to decompose the cover media before embedding the secret data. As data is embedded in the middle frequencies, coefficients in the low frequency sub-band are preserved unaltered to improve the image quality.

## 2. Related Work

M.LakshmiPrasanna and Mr. Sk.MahaboobBasha proposed a new Extended Adaptive Pixel Pair Matching (EAPPM). As APPM is proved to offer better security against detection and lower distortion, this system takes forward APPM for colored images. In colored images, which consists three different colored layers, in each layer one can embed message bits so that the capacity of the Adaptive Pixel Pair Matching can be improved without any distortion in the original colored image. The R, G, B layers are separated and each is considered as a gray image, referred as Channel Image. The proposed APPM method must satisfy the following requirements. There are exactly B coordinates in  $\emptyset(x, y)$ . The values of extraction function in these coordinates are mutually exclusive. The design of  $\emptyset(x, y)$  and  $f(x, y)$  should be capable of embedding digits in any notational system so that the best can be selected to achieve lower embedding distortion. This system proposed an efficient data embedding algorithm EAPPM, based on APPM, which can successfully embed data into three layers of an RGB image. EAPPM is able to embed three times data more than APPM, without any compromise on MSE and security. The advantages of APPM, like the freedom for user to use any notational system and better image quality are carried to EAPPM [8].

Shanmugam.E and T.K.Thivakaran presented Securing Cipher Information Using Edge Based Adaptive Pixel Pair Matching. The proposed method encrypts the data with crypto module using Blowfish algorithm and then embeds the encrypted data into the cover image using Edge based Adaptive Pixel Pair Matching (EAPPM) method. Blowfish algorithm used in this system is a 64-bit block cipher with a variable length key. There are many edge detection methods like Canny, Fuzzy, Sobel and Laplacian filters which are commonly used and these sharp edges are used to hide the data using steganography method which gives good results than the normal steganography method. For this reason the proposed method embeds the data in sharp areas. Sobel edge detection method is chosen for detecting the sharp areas in the proposed method. Select a pixel from the recorded sharp areas to embed data in it. And then, find the modular distance according to that pixel and calculate neighbourhood pixel. Once the neighbourhood pixel is calculated, it is replaced by the original pixel to embed the secret data. As this paper presented the idea of combining cryptography and steganography, it becomes even harder to get the secret data due to the complexity in the process of extracting the encrypted data from stego file and then deciphering it. This system embedded secret data into sharp area so human visual system cannot notify the alteration of image [5].

## 3. Background Theory

The two main theories used to enhance image security are namely Discrete Wavelet Transform (DWT) method and Modified Adaptive Pixel Pair Matching (MAPPM) algorithm. For more embedding, DWT is used for decomposing the image into higher and lower frequency sub-bands. The proposed system modified the APPM method with the embedding step of the secret data. Modified APPM calculates B-ary notational system, uses key value to select the co-ordinate pair for making new frequency values and embeds the secret data. A more secure MAPPM embedding method is used to keep a secret image with less distortion.

### 3.1 Discrete Wavelet Transform (DWT)

A wavelet is a localized variation of detail in an image. Wavelets can be used for a wide variety of signal processing tasks such as compression, detecting edges, removing noise, and enhancing images. Wavelets are mathematical functions that divide continuous time signal data into different frequency components. If parts of a signal are rapidly changing, they are of a high frequency, and on the other hand, slowly smoothly changing pieces are of low frequency. The proposed system used 2-dimensional Harr- Discrete Wavelet Transform.

Let consider 4\*4 pixel numbers as original image shown in fig 1.(a). At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighbouring pixels. Store the sum on the left and the difference on the right as illustrated in fig 1.(b). Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H) [6-7].

Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in fig 1.(c)

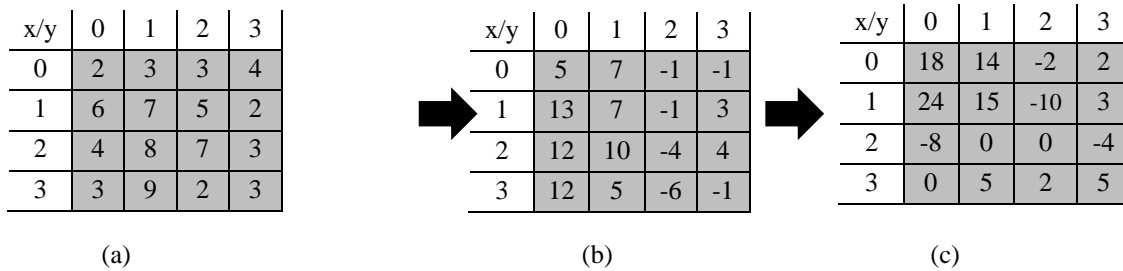


Fig. 2.one level DWT Image

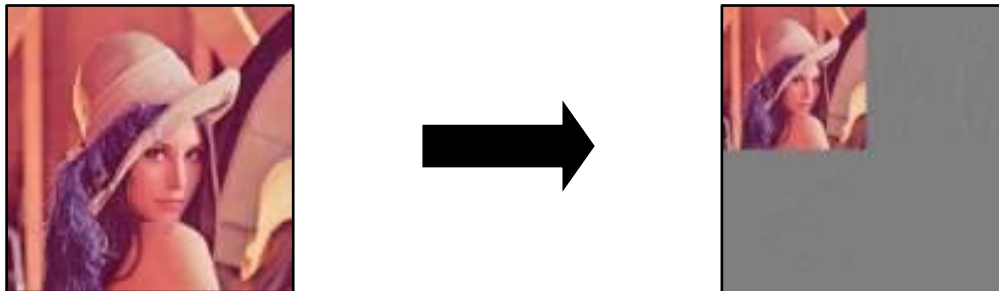


Fig 1. (a) original pixel values (b) results from horizontal computation (c) results from vertical computation

Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The other sub-bands contain information about the edge components. So the proposed system use high frequencies component to embed secret data since the human eye is less sensitive to changes in edges. One level decomposition of DWT is shown in fig 2

### 3.2 Modified Adaptive Pixel Pair Matching (MAPPM)

The basic idea of APPM is to use the pixel pair (x,y) as the coordinate and searching a coordinate (x',y') within a predefined neighborhood set  $\emptyset(x,y)$  such that  $f(x',y')=S_B$  where f is the extraction function and  $S_B$  is the message digit in B-ary notational system to be concealed. The proposed system modified the APPM with some modifications. Step by step procedures are as follow:

#### Embedding Procedure

Input: Cover image of size  $M \times M$ , secret bit stream  $S_B$ , and key K.

Output: Stego image  $I'$ ,  $C_B$ ,  $\emptyset_B(x,y)$

Step 1. Find the minimum B satisfying  $[M \times M / 2] \geq |S_B|$ , and covert S into a list of digits with a B-ary notational system  $S_B$ . To calculate B,  $B=2^{\wedge}(n/(M/2 \times M/2))$  where  $n=(\text{size of secret}) * 8$  bit.

Step 2. Choose  $B=16$  if B value less than 16 and if not choose B.

Step 3. Solve the discrete optimization problem to find  $C_B$  and  $\emptyset_B(x,y)$

Step 4. Construct a nonrepeat random embedding sequence  $Q=[Q=1,2,3,\dots]$  using a key  $K$ .

Step 5. According to the sequence, find  $x$  value and  $y$  value.

$$x = \text{coefficient value of } f(P_{1r}, P_{1c}) \text{ and } y = \text{coefficient value of } f(P_{2r}, P_{2c})$$

where  $P_{1r} = Q_i/M_1$ ,  $P_{1c} = Q_i \% M_1$ ,  $P_{2r} = Q_i / M_1$  and  $P_{2c} = Q_i \% M_1$  for  $i = 1, 2, 3, \dots$

Step 6. Calculate reference coordinate  $f(x,y)$

$$f(x,y) = (x + C_B * y) \bmod B, \text{ where } C_B \text{ is the constant.}$$

Step 7. Calculate the modular distance to embed the secret data

$$d = (S_B - f(x,y)) \bmod B, \text{ where } d \text{ is the modular distance}$$

Step 8. Repeat step 5 to step 7 until all secret bits are embedded.

A simple example is used to illustrate the embedding procedure. Suppose a cover image of size  $512 \times 512$  with embedding requirement of 520 000 bits, secret image of size  $128 \times 128$  and key  $K = 7$ . The minimum  $B$  satisfies  $(512 \times 512) / 2 \geq 64 * 64$ . and the value of  $B$  is 4. The value of  $B$  less than 16, so  $B$  value is 16 and  $C_{16} = 6$  and  $\Phi_B(x,y)$  can be obtained in table 1. According to the key value, non-repeated embedding sequence be 34370, 8359, 16615, 5585, and so on. Next step is to find the value of  $x$  and  $y$ .  $X$  and  $Y$  are the coefficient values of  $f(P_{1r}, P_{1c})$ . So  $P_{1r} = 34370/256 = 134$ ,  $P_{1c} = 34370 \% 256 = 66$ ,  $P_{2r} = 38880/256 = 151$  and  $P_{2c} = 38880 \% 256 = 224$ . Then  $x'$  value will become 21 as  $f(134,66)=20$  and  $y'$  value will become 1 as  $f(151,224) = 1$  according to the pixel value of the original image. Next step is to calculate the coordinate value. So  $f(20,1) = 20 + (16 \times 1) \bmod 16 = 4$ . Modular distance  $d = (S_B - f(x,y)) \bmod B = (1 - 4) \bmod 16 = 13$  and  $(\hat{x}, \hat{y}) = (1, 2)$ . Therefore, the pixel value  $(20, 1)$  replaces by  $(20+1, 1+2) = (21, 3)$ .

<b>B</b>	16	32	48	64
<b>C<sub>B</sub></b>	6	12	7	14

Table 1 : (a) Constant  $C_B$  value

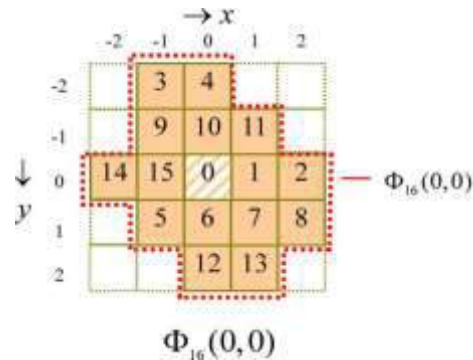


Fig 3. Neighborhood set  $\Phi_{16}(x,y)$

### Extraction Procedure

To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded message digits are the values of extraction function of the scanned pixel pairs.

Input :Stego image  $I'$ ,  $C_B$ ,  $\Phi_B(x,y)$  and Key  $K$ .

Output : Secret bit Stream  $S$ .

Step 1. Construct a nonrepeat random embedding sequence  $Q=[Q=1,2,3,\dots]$  using a key  $K$ .

Step 2. According to the sequence, find  $x$  value and  $y$  value.

$$x = \text{coefficient value of } f(P_{1r}, P_{1c}) \text{ and } y = \text{coefficient value of } f(P_{2r}, P_{2c})$$

where  $P_{1r} = Q_i / M_1$ ,  $P_{1c} = Q_i \% M_1$ ,  $P_{2r} = Q_i / M_1$  and  $P_{2c} = Q_i \% M_1$  for  $i = 1, 2, 3, \dots$

Step 3. Calculate reference coordinate  $f(x,y)$   $f(x,y) = (x + C_B * y) \bmod B$ , where  $C_B$  is the constant.

Step 4. Repeat step 2 to step 3 until all the message digits are extracted.

### 4. The Design and implementation of the Proposed System

The proposed system architecture is organized with two portions : sender side and receiver side as illustrated in fig 4 . At the sender side, the original cover image is firstly decomposed by Discrete Wavelet Transform (DWT) as four sub-bands ( LL, LH,HL, HH). Data is embedded in HL sub-band since the human eye is less sensitive to changes in high frequencies components. Modified Adaptive Pixel Pair Matching is used for embedding secret data to get the stego image. At the receiver side, the original secret image can be retrieved by using decomposing process with DWT and extraction process.

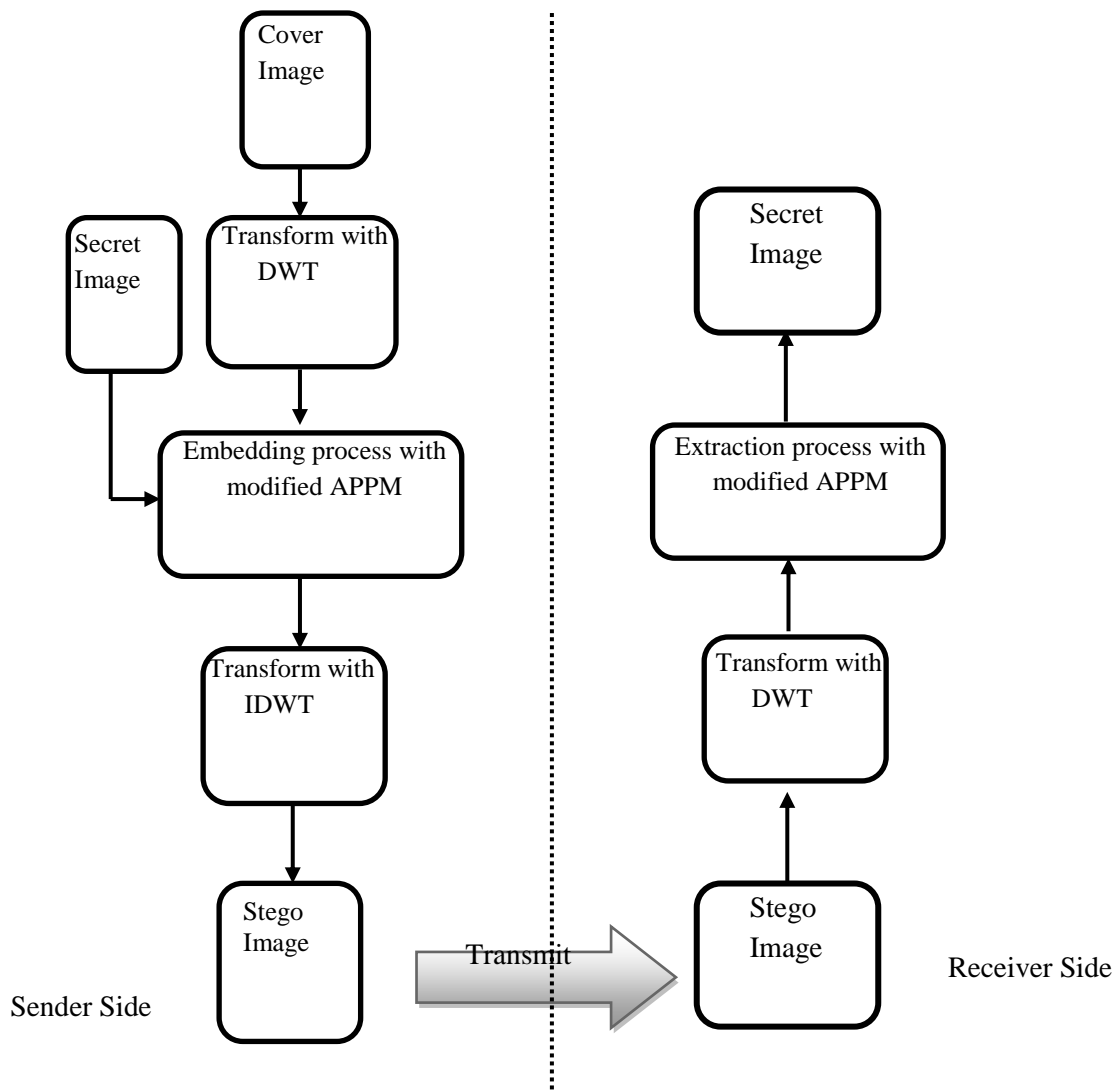


Fig. 4 Block Diagram of Proposed System

#### 4.1 Implementation Results

The implementation results of the proposed work is implemented by using Matlab R2016a programming language. In the sender side, embedding process is performed by six processes shown in fig 6. First , the cover image of size 512\*512 is loaded and then size of 128\*128 is loaded to use the secret image shown in fig 5 (a) and (b). Then, the proposed system calculates the parameter of modified APPM such as  $B$ ,  $C_B$ .



Fig 5. (a) Cover image



(b) Secret Image



Fig 6. Embedding process of modified APPM

Next step is that the original cover image is decomposed by DWT. Then key value which is provided by the user is used to generate the non repeated pixel pair sequence in step 5. Modified APPM embedded the secret data according to the pixel sequence in step 6. After embedding the secret data into the cover media, the generated stego image is saved and mean square error and peak signal to noise ratio between original image and stego image are shown in fig 7.

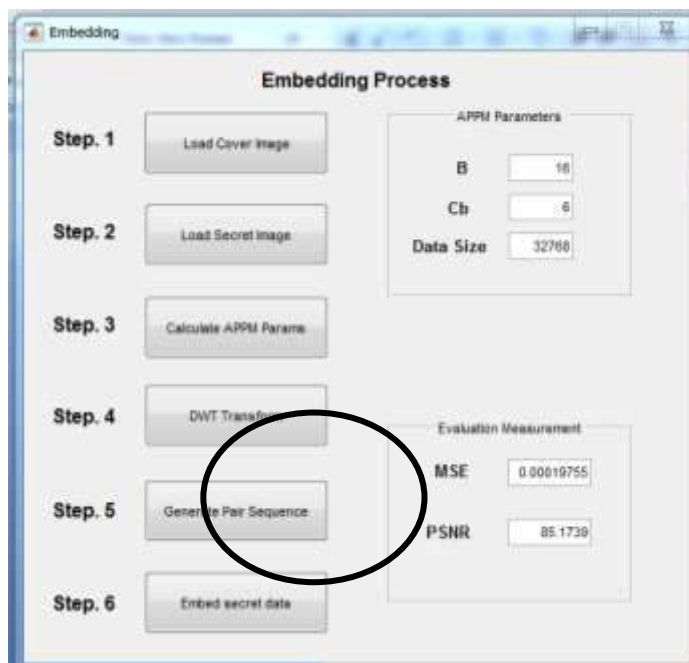


Fig 7. Result of MSE and PSNR After embedding secret image

#### 4.2 Performance Evaluation

In this part, the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and histogram are used to compare the image quality of stego image resulted from embedding method of original APPM and modified APPM. Moreover, the different five cover images in  $512 \times 512$  size shown in fig 8 are tested by the secret size of  $128 \times 128$  pixel size shown in

fig 5 (b). The experimental results of PSNR and MSE for five different cover images are shown in table2 and histogram are shown in fig 9,10and 12. Extracted secret images are shown in fig 12 and 13.



Fig 8 : cover image of (a) Princess (b) Bird (c) Lena (d) Baboon (e) Living Room

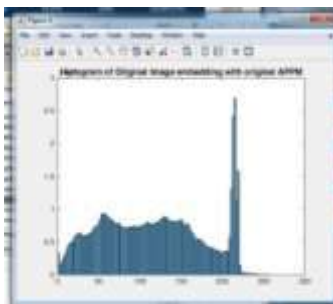


Fig 9. Histogram of original image embedding

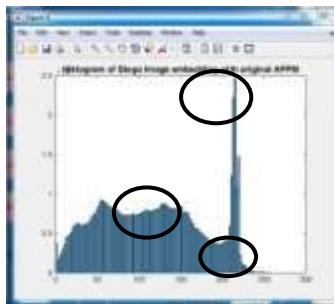


Fig 10. Histogram of stego image embedding with Original APPM



Fig 11. Histogram of stego image embedding with Modified APPM

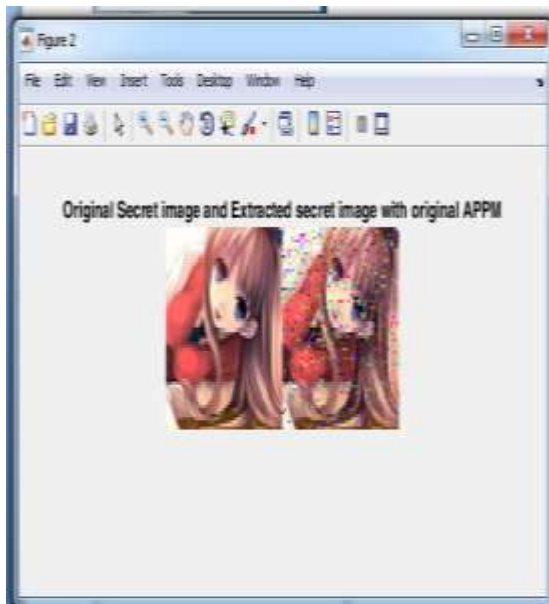


Fig 10. Histogram of stego image embedding with Original APPM

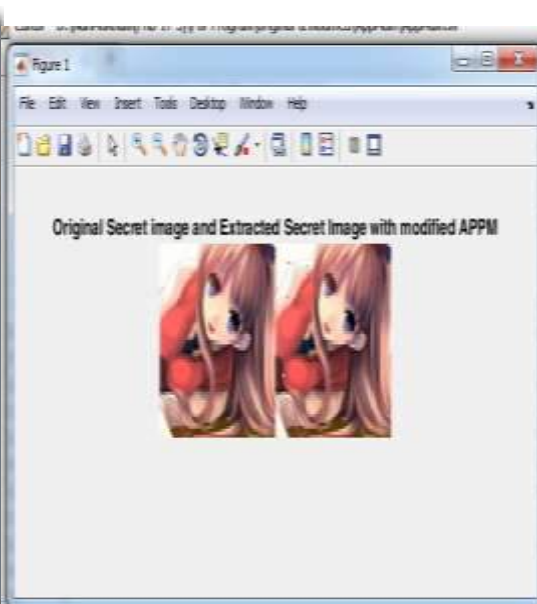


Fig 10. Histogram of stego image embedding with Modified APPM

Table 2. PSNR and MSE comparison between APPM and Proposed Method

Cover Image (size of 512×512)	Secret Image (size of 128 × 128)			
	APPM		Proposed Method	
	PSNR	MSE	PSNR	MSE
Princess	45.2074	1.9604	60.3863	0.05949
Bird	39.5376	7.2331	58.5391	0.091026
Lena	40.9574	5.216	60.3863	0.092369
Living Room	38.8853	8.4043	58.5746	0.090286
Baboon	45.2074	7.2211	58.4755	0.098709
Average	41.95902	6.00698	59.27236	0.086376

According to the experimental results, the stego images resulted from embedding modified APPM have lower MSE and higher PSNR values. MSE values are significantly decreased in embedding with Modified APPM. The proposed system can reduce 60% in MSE values with average value from 6.00698 to 0.086376. The cover image with less color changes gets higher PSNR values such as Princess and Baboon. In percentage, embedding with modified APPM can increase 20% in PSNR values. In histogram, more changes were found in embedding with original APPM and less changes were found in MAPPM. So the proposed method gives least distortion in stego image compared to the original APPM.

## 5. Conclusion

The proposed system used a secure method for hiding image based on discrete wavelet transform (DWT) and modified adaptive pixel pair matching (MAPPM). APPM directly changes the reference coordinate and search coordinate to embed the secret data. In MAPPM, two pixels from non-repeated pixel sequence are scanned as an embedding unit and a specially designed neighborhood set is employed to embed secret image with a smallest notational system. The proposed system also provides a better image quality because MAPPM does not produce any artifacts in stego images. The MAPPM technique is also able to hide all different image types to it like JPG, PNG and TIFF etc. In future work, the steganography can also be used to enforce on a digital medium such as in a music/audio file or video file.

## 6. Reference

- [1] K. Shan, S. kaul M.S. Dhande, "Image Steganography using DWT and Data Encryption Standard, IJSR, ISSN: 2319-7064, Volume 3 Issue 5, May 2014.
- [2] Shalkh Salman, Prof. S.R. Kinge, "Data Hiding Method Using Adaptive Pixel Pair Matching", IJSR, ISSN: 2319-7064, Volume 4 Issue 8, August 2015.
- [3] J. Desai, Hemalatha and Shishira SR, "Pixel Pair Based Data Hiding", zijcdmr volume, issue 4, April 2015.
- [4] Z.V. Patel and S.A. Gadhiya, "A Survey Paper on Steganography and Cryptography", 2015 RHIMRJ, ISSN: 2349-7637.

- 
- [5] k.Shanmugan.E, T.K.Thivakaran, "Securing Cipher Information Using Edge Based Adaptive Pixel Pair Matching", IJCSNS, VOL 15 No.7, July 2015.
- [6] Parul , Manju , Dr Harish Rohil, "Optimized Image Steganography using Discrete Wavelet Transform (DWT)", IJRDET, ISSN2374-6435 (Online) Volume 2, Issue 2, February 2014.
- [7] M.A. Wakure, A.N Holambe, "A Discrete Wavelet Transform : A Steganographic Method for Transmitting Images", IJCA (0975-8887) Volume 129-No5 November 2015.
- [8] M.LakshmiPrasanna , Mr. Sk.MahaboobBasha , "Extended Adaptive Pixel Pair Matching" ,IJERA, ISSN:2248-9622 Vol.2, Issue ,May 2013