DATA EMBEDDING USING MODIFIED ADAPTIVE PIXEL PAIR MATCHING AND DISCRETE WAVELET TRANSFORM

[1]NAN MO KHAM, [2]NANG AYE AYE HTWE, [3]KHINMYO THANT

Department of Computer Engineering and Information Technology,
Mandalay Technological University, the Republic of the Union of Myanmar
E-mail: [1]nanmokhamnmk7@gmail.com, [2]htwe.aye@gmail.com[3]khinmyothant97@gmail.com

Abstract - Information security is very important part of IT industries in today's life and it's a rapidly growing area in IT sector. Data hiding is one of the emerging techniques that provide for securityby hiding secret information into the multimedia contents by altering some components in the cover file.This paper proposes a secure information system in image steganography based on frequency domain and a secure method for data hiding based on modified Adaptive Pixel Pair Matching. The basic idea of Adaptive Pixel Pair Matching (APPM) is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit. Adaptive Pixel Pair Matching is modified with B-ary notational system and modular distance in this proposed system. Original APPM directly changes the reference coordinate and search coordinate to embed the secret data. Modified APPM chooses reference coordinate with modular distance value if multiple reference coordinate have same search coordinate. So the proposed method getsstego image with less distortion after embedding secret data.Discrete wavelet transform (DWT) is also usedto decomposecover mediaImage quality measures used for analysis are Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) after embedding the secret image.

Keywords - Adaptive Pixel Pair Matching (APPM), Discrete Wavelet Transform(DWT), Mean Square Error (MSE),Peak Signal to Ratio (PSNR)

I. INTRODUCTION

A huge amount of confidential data is being lost every year by the intruders. Various methods have been investigated and developed to protect personal privacy. Cryptography and Steganography are two popular ways of sending vital information in a secret way.

Cryptography is a technique to ensure the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately sometimes this is not smart enough to keep the contents of a message secure or secret. So, cryptography deals with hiding the contents of a message. A major drawback to cryptography is that the existence of data is not hidden.Cryptography encrypts a message so it cannot be understood but Steganography completely hides the message so it cannot be seen.Steganography is different from cryptography[1]. Steganography is the art of hiding information in digital media through the techniques of embedding hidden messages in such a way that no one except the sender and the intended receivers can detect the existence of the messages. Steganography's aim is to make the secret data undetectable, that is,to hide the presence of a secret message.

Image Steganography techniques can be divided into two groups: those in Image Domain and those in Transform Domain. Image Domain also known as spatial domain technique embeds messages in the intensity of the pixel directly. In Transform Domain, also known as frequency domain, images are first transformed and then the message is embedded in the image. The proposed system is intended to keep a secret image with less distortion and more secret data can be embedded[2].

The rest of this paper is organized as follows: In Section II, the related work of the proposed system will be described. In Section III, methods and design of the proposed is explained. Implementation results are described in section IV. The paper is concluded in section V.

II. RELATED WORK

Shanmugam.E, and T.K. Thivakaran presented securing cipher information using edge based adaptive pixel pair matching (EAPPM). The proposed method first encrypts the data using Blowfish encryption algorithm that uses key length values varying from 32 bits to 448 bits. The next step is to embed the encrypted data into an image cover file using EAPPM method. The obtained stego- images from both APPM and EAPPM embedding process are subjected to image quality analysis. The image quality measures used for analysis are Structural Content (SC), Normalized cross correlation (NK) [3].

K Madhuri and Ms C Padmini proposed a secure steganographic technique for Embedding Text using Adaptive Pixel Pair Matching (APPM). APPM uses the values of pixel pair as a reference coordinate, and search a coordinate according to a given message digit and then replaced by the searched coordinate to conceal the digit. This system compared the Optimal Pixel Adjustment Process (OPAP) with APPM. OPAP method is used to reduce the distortion caused by LSB replacement. OPAP effectively reduces the image distortion compared with the traditional LSB method. But in OPAP method, imbalanced

embedding distortion emerges and is vulnerable to steganalysis. APPM method is much better than the other existing data hiding method such as OPAP. [4].
Ketan S and Swati K proposed an image steganography that combines Discrete Wavelet Transform (DWT), Least significant bit (LSB) and Encryption techniques on raw images to enhance the security of secret message. This system uses cryptography and steganography together. First, the system encrypts the message using data encryption standard (DES) algorithm and then hide it in the image. Before hiding, the image is transformed from spatial domain to frequency domain using DWT (Discrete Wavelet Transform) algorithm. In this system, the low frequency components preserve the original image and other frequency components use for embedding data. Data Encryption Standard (DES) algorithm uses 64-bit blocks (8 octet) to encrypt the secret data. After encrypting, the encrypted message is embedded by using Least Significant Bit (LSB). The proposed method combined both cryptography and steganography to prevent data losing [5].

According to the literature and concept of security enhancement approaches which are pointed out from the previous researches, the main aim of this work is to provide better image quality with more embedding data capacity.

III. THE PROPOSED SYSTEM

The proposed system uses image steganography based on frequency domain. Image steganography methods are used to hide the existence of secret data in cover image. To ensure confidentiality of a secret data, the proposed system decomposes the cover media and then embeds the secret data. For more embedding capacity, the cover image is decomposed by DWT and then the secret image is embedded using modified APPM. The proposed system design is shown in Fig 1.

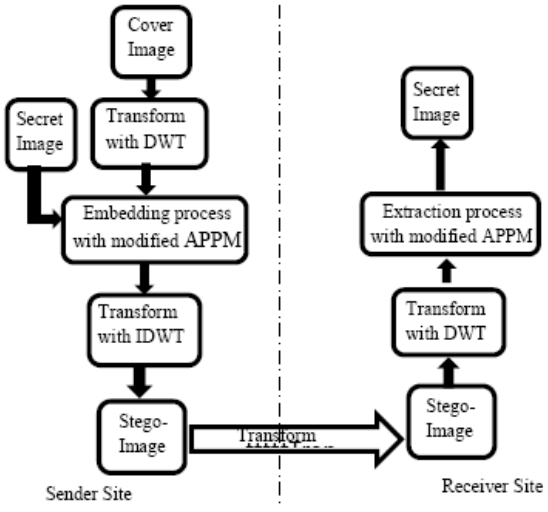

Fig. 1 Proposed System Design

A. Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform (DWT) is a mathematical tool for hierarchically decomposing an image. Wavelets are used in the image steganographic model because the wavelet transform clearly partitions the high-frequency and low-frequency information on a pixel by pixel basis. Discrete Wavelet Transform (DWT) applies filter banks to analyse and reconstruct signal. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients. Input data is passed through set of low pass and high pass filters. The output from low pass filter is an approximate coefficientand the output from the high pass filter is a detail coefficient shown in figure 2.A precise formula for the value of first approximation coefficient, $a^1 = (a_1,a_2,\ldots,a_{N/2})$ in equation :1 at one level for a signal, length N i.e, $f=(f_1,f_2,\ldots,f_N)$ is

$$a_n = \frac{f_{2n-1} + f_{2n}}{\sqrt{2}} \quad n=1,\ 2,\ 3\ \ldots N/2 \qquad (1)$$

and the first detail sub signal, $d^1 = (d_1,d_2,\ldots d_n)$ in equation : 2 at the same level is given as

$$d_n = \frac{f_{2n-1} - f_{2n}}{\sqrt{2}}, \quad n=1, 2, 3\ldots N/2 \qquad (2)$$

With the DWT, the significant part(smooth parts) of the spatial domain image exist in the approximation band that consists of low frequency wavelet coefficients and the edge and texture details usually exist in high frequency sub bands. Human eyes are not sensitive to the small changes in the edges and textures of an image but very sensitive to the small changes in the smooth parts. This allows the secret message/image to be embedded at high frequency sub-bands without being perceived by the human eye [6]-[10].



Fig. 2 Levels of 1D DWT Image

B. Modified Adaptive Pixel Pair Matching

A good data hiding method should be capable of evading visual and statistical detection while providing an adjustable payload. 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 Ø(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. Data embedding is done by replacing (x,y) with (x´,y´). APPM is used to provide security against detection. The proposed method takes forward APPM to reduce

the distortion of the stego image. Step by Step procedures are as follow:
Input: Cover image of size M×M , secret bit stream S, and key K.

Output: Stego image I´, C_B ,$\emptyset_B$ (x,y) ,
Step 1, Find the minimum B satisfying $\lfloor M\times M/2 \rfloor \geq |S_B|$, and To calculate B, $B=2^{n/(M\times M)}$ where n is the number of bits to be embedded. N=(size of secret) *8 bit.
Step 2, In the region defined by $\emptyset_B(0,0)$, record the coordinate $(\hat{x}, \hat{y})$such that $f((\hat{x}, \hat{y}) = i$, $0 \leq i \leq B-1$.
Step 3, To embed a message digit S_B, two pixels (x,y) in the cover image are selectedand then calculate the modulus distance $d=(S_B-f(x,y))\text{mod}B$ between S_B and , then f(x,y) replace f´(x,y) with $(x+\hat{x}_d, y+\hat{y}_d)$.
Step 4, Repeat Step 3 until all the message digits are embedded [11]-[14].

APPM directly changes the reference coordinate and search coordinate to embed the secret data. APPM is modified by choosing the reference coordinate with less modular distance in this proposed system. In step 3, f(x,y) replaces f´(x,y) with $(x+\hat{x}_d, y+\hat{y}_d)$. If reference coordinates have same search coordinate to embed same secret data, choose search coordinate and reference coordinate with less modular distance. And then, repeat step 3 until all the message digits are embedded.

Suppose cover image of size 4×4 shown in figure 3 and secret image of size 2×1. Number of bits to be embedded can be calculated as 2*1*8=16 bits. So the value of B-aryis16 and $C_B$is 6. Let consider 5 and 7 secret digit to conceal in frequency components f(1,2) and f(2,1). First find the characteristic value of f(x,y)is $f(x,y)= (x+C_B*y)\text{mod } B$. So f (1,2) = 13 and d=(5-13)mod16 is 8. The coordinate set of 8 is (2,1). New frequency components are (1+2 ,2+1) = f(3,3).

x/y	0	1	2	3
0	2	3	3	4
1	6	7	5	2
2	4	8	7	3
3	3	9	2	3

DWT

x/y	0	1	2	3
0	18	14	-2	2
1	24	15	-10	3
2	-8	0	0	-4
3	0	5	2	5

Fig. 3 Original 4*4 pixels, **Fig. 4 result from DWT to embed secret data**

Original APPM directly changes the reference coordinate and search coordinate to embed the secret data. The proposed method found that three reference coordinates have same search coordinate when 5 secret digits embeds. The proposed method chooses reference coordinate with less modular distance to embed secret data shown in table1.Comparing figure 7 and 9, stego image embedded with modified APPM gets better image quality.

Pixel number	Secret Digit
f(0,1) =24	7
f(2,3) =2	5

x/y	0	1	2	3
0	18	14	-2	2
1	24	15	-10	3
2	-8	0	0	-4
3	0	5	2	5

Fig.5before embedding

x/y	0	1	2	3
0	18	14	-2	2
1	24	15	-10	3
2	-8	5	0	-4
3	0	5	2	0

Fig.6 after embedding with Original APPM

x/y	0	1	2	3
0	2	3	3	4
1	6	7	5	2
2	7.75	4.25	3.25	6.75
3	6.75	5.25	0.75	-5.7

Fig.7 stego image using Original APPM

x/y	0	1	2	3
0	18	14	-2	2
1	15	24	-10	3
2	-8	0	0	-4
3	0	5	5	2

Fig.8 after embedding with modified APPM

x/y	0	1	2	3
0	2	3	3	4
1	6	7	5	2
2	2.5	5	8.5	6
3	0	0.75	5	4.5

Fig.9 stego image using modified APPM

IV. IMPLEMENTATION RESULTS

In this section, some experiments are carried out to prove the efficiency of the proposed system. A set of 4-bit gray-scale images of size 512×512 are used as covered-image and secret image of size is 256×128. The figure10 (a)-(d) are taken for the experiment process as cover image. In order to embed secret image in cover image, figure 11 is used. The figure 12 shows the stego images which do not show any artifacts after applying modified APPM to the cover image to hide the secret data into it.



Fig10. Original image (a) Lena (b) Baboon (c) Airplane (d)Boat



Fig.11 Secret Image to be embedded



Fig 12.Stegoimage(a) Lena (b) Baboon (c) Airplane (d)Boat

Image quality is a characteristic of an image that measures the perceived image degradation. For image quality analysis, the proposed system used Mean Square Error and Peak Signal-to-Noise Ratio [15].

Mean Square Error (MSE) is defined as the squares of error between the stego-image and the cover image. MSE is calculated usingequation:3,

$$MSE = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} (f(i, j) - (f'(i, j))^2 \quad (3)$$

Where f(i,j) is the intensity value of the pixel in the original image and f′(i,j) is the intensity value of the pixel in the stego-image. A large value for MSE means that the image is poor quality.

Peak Signal-to-Noise Ratio (PSNR) measures the statistical difference between stego image and cover image using equation:4.

$$PSNR = 10\log_{10}(\frac{255^2}{MSE}) \quad (4)$$

Comparison of MSE between the proposed method and APPM method is shown table II. From table III, the PSNR of the proposed method is better than original APPM method for the same capacity.

IMAGES	MSE		MSE IMPROVEMENT
	APPM	Proposed Method	
Lena	2.664	2.544	0.12
Baboon	2.682	2.601	0.081
Airplane	2.67	2.6	0.07
Boat	2.698	2.617	0.075
Average	2.6785	2.5905	0.0865

Table II:- Mse comparison between appm and proposed method with cover size 512*512 of various types of images

IMAGES	APPM		proposed method	
	capacity (bits)	psnr (dB)	capacity (bits)	psnr (dB)
Lena	507856	46.0882	507856	55.83
Baboon	507856	45.9961	507856	54.92
Airplane	507670	46.1948	507670	55.46
Boat	507867	46.1385	507867	53.78
Average	207812.3	46.1044	507812.3	54.9975

Table III:- Psnr comparison between appm and proposed method with cover size 512*512 of various types of images

It is clear from the table II and IIIthat, the proposed method provides less MSE and greater PSNR values. The averaged MSE and PSNR of stego image embedded with APPM are 2.6785 and 46.1044 whereas the averaged MSE and PSNR of modified APPM are 2.5905 and 54.9975. As the average of MSE improvement is 0.0865,the proposed method gives least distortion.So modified APPM is better compared to the original APPM.

CONCLUSION

In this paper, image steganography makes difficult for the intruders to attack or steal sensitive information.As data is embedded in frequency coefficients, this system can support more secure and perceptual to HVS (Human Visual System).Original APPM directly changes the reference coordinate and search coordinate to embed the secret data. The proposed method chooses reference coordinate with less modular distance value if multiple reference coordinates have same search coordinate.So the proposed system gets stego image with less distortion after embedding secret image. The proposed system provides high data embedding capacity with better image quality.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.

ACKNOWLEDGMENT

The author would like to thank to Dr. Nang Aye AyeHtwe, Professor and Head, Dr.KhinMyo Thant, Lecturer, and all teachers from Department of Computer Engineering and Information Technology, Mandalay Technological University, for their effective guidance, helpful suggestion and supervision for this paper.

REFERENCES

[1] Z.V.Patel and S.A.Gadhiya, “ASurvey Paper on Steganography and Cryptography”,2015 RHIMRJ, ISSN:2349-7637.

[2] B.V. Kranthi and R. Mahajan, “An Improved Image steganography Technique Using Discrete Wavelet Transform”. IJETCAS, 9 (1) June 2014.pp. 76-82.

[3] k.Shanmugan.E, T.K.Thivakaran, “Securing Cipher Information Using Edge Based Adaptive Pixel Pair Matching”, IJCSNS, VOL 15 No.7, July 2015.

[4] K Madhuri and Ms C Padmini, “A Secure Steganographic Technique for Embedding Text using Adaptive Pixel Pair Matching”, Global Journal of Research in Engineering, Volume 14 Issue 6, 2014.

[5] M Elbayoumy, M Elmogy, A aboueIfetouh and R. Elhadary, “A Proposed Technique for Hiding Data Into Video Files”,IJCS, ISSN:1694-0814, 2014.

[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] Monknika R and Alka V, “Discrete Wavelet Transform for image compression” IJCSME, Volume2, Issue4, April 2015.

[8] M.A. Wakure, A.N Holambe, "A Discrete Wavelet Transform : A Steganographic Method for Transmitting Images", IJCA (0975-8887) Volume 129-No5 November 2015.

[9] Ketan S and Swati K, "Image Steganography combining Discrete Wavelet Transform, Least Significant Bit and Encryption Technique", JGRCS, ISSN-2229-371X, Volume 5, No.5.May 2014.

[10] K. Shan, S. kaulM.S.Dhande, "Image Steganography using DWT and Data Encryption Standard, IJSR, ISSN: 2319-7064, Volume3 Issue 5, May 2014.

[11] T.Lakshmi, P.GangaBhavani, "APPM: A Narrative Data Embedding Method Using Adaptive Pixel Pair Matching", IJIRCCE, (An ISO 3297:2007 Certificate Organization) Vol, 1, Issue 7 September 2013.

[12] Shalkh Salman, Prof.S.R.Kinge, "Data Hiding Method Using Adaptive Pixel Pair Matching",IJSR, ISSN:2319-7064, Volume 4 Issue 8, August 2015.

[13] Salful Islam, Manget R Modi and Phalguni Gupta, "A Secure SteganographicTechinque for Embedding Text using Adaptive Pixel Pair Matching", IJIRCCE, EURASIP Journal on Information Security, 2014.

[14] J.Desai, Hemalatha and Shishira SR, "Pixel Pair Based Data Hiding", zijcdmr volume, issue 4,Apirl2015.

[15] S. Bhattacharuya and G.Sanyal, "A Robust Image Steganography using DWT Difference Modulation (DWTDM), I.J Computer Network and Information Security,2012 ,7, 27-40.

★★★