Huffman Coding based Adaptive Pixel Pair Matching Steganography for Audio files

S.IMACULATE ROSALINE[1]
M.E Communication Systems, 2nd Year, Department of Electronics and Communication Engineering,
Oxford Engineering College, Pirattiyur, Tiruchirapalli,
Pincode – 620009.
[1]imaculaterosaline@gmail.com

C.RENGARAJASWAMY[2]
M.E Communication Systems, 2nd Year, Department of Electronics and Communication Engineering,
Oxford Engineering College, Pirattiyur, Tiruchirapalli,
Pincode – 620009.
[2]rengarajaswamy@gmail.com

Abstract:

Information Hiding is the process of securing data over covert channel. Cryptography and Steganography are two main techniques for accomplishing security. Steganography is the process of concealing secret data within cover media. Substitution techniques like Least Significant Bit Substitution (LSB) and Optimum Pixel Adjustment Process (OPAP) uses one pixel for concealing the secret digit. Pixel Pair Matching (PPM) uses two pixel pairs for accomplishing data hiding. Two variants of PPM are Exploiting Modification Direction (EMD) and Diamond Encoding (DE). PPM achieves better Embedding Capacity than the previous methods. Improved variant of DE is Adaptive Pixel Pair Matching (APPM) where the extraction function is modified than that of the existing PPM techniques to improve the payload capacity and to minimize the Peak Signal to Noise Ratio (PSNR). In this paper, the secret message is first Huffman encoded and then undergoes the existing APPM technique. Huffman Encoding depends on the probability of occurrence of pixel values. It is a kind of lossless compression algorithm. It tends to improve the data embedding capacity. APPM technique employs two pixel values (a, b) and (a’, b’) where one is used as reference co-ordinate and the other is used as search co-ordinate. Depending on the coded secret value, the extraction function is employed to conceal the pixel.

***Keywords* – LSB, OPAP, PPM, EMD, DE, APPM, Huffman Coding.**

1.INTRODUCTION

Transmission of vital information over an insecure communication channel leads to various security threats like Confidentiality, Integrity, Authentication and Availability. All these threats pose a severe danger when the information content to be transmitted is of high value such as the case in law and medical field. Thus to protect such highly confidential data, many techniques have been proposed. Two such methods are Cryptography and Steganography. Cryptography does scrambling of information. It thus makes any intelligible content to unreadable format. Cryptography is obtained by various forms of Encryption. Encryption is a method where the sender uses an encryption key to scramble the original content and then transmitted to the receiver side. Upon reception, the receiver uses the same encryption key to unscramble the encrypted data. This will ensure secured transmission in any covert channel. Data Integrity and Confidentiality is assured with such encryption methods. Authentication can be obtained with another well known method called Digital Watermarking. Watermarking provides owner authentication. Steganography is the art of concealing secret data within the cover media. This kind of information hiding is available even from ancient days, where people used tattoos for conveying their message [1]. Features of Steganography include Payload Capacity, Robustness, Invisibility, Undetectability and security. Classification of Steganographic system includes Substitution Systems, Transform Domain Systems, Spread Spectrum Technique, Statistical methods, Distortion Techniques, Cover generating methods. [2]. Substitution Techniques have gained importance with the advent of Least Significant Bit Substitution (LSB). This is one of the simplest methods where the secret message is concealed into the LSBs of the cover file. This is because only the LSBs contain the low frequency content of the image. Thus, the quality of the cover image is preserved. No third party suspicion can be done in such good quality cover files. However, the Peak Signal to Noise Ratio tends to increase with increasing payload capacity. This problem was overcome by the Optimum Pixel Adjustment Process (OPAP), where the stego pixel value is altered again depending upon the error range [3]. Both the above methods use only one pixel for embedding. However, a different approach was proposed based on two pixel values of the cover image. This method is termed as Pixel Pair Matching (PPM). Among the two pixel values, one is used as reference and the other is used for concealment. Two variants of PPM are Exploiting Modification Direction (EMD) and Diamond Encoding (DE). Exploiting

Modification Direction (EMD) makes use of a (2n+1)-ary sub stream to be embedded into n cover pixels [4].

PSNR of EMD can be increased further by using fully Exploited Modification Direction method [5]. DE method is an extension of the previous method. The cover pixels are divided into blocks, and for each block diamond characteristic value is calculated, into which the secret k-ary digit is embedded [6]. In this case, block capacity is equal to $\log_2$ ($2k^2$+2k+1).This method tends to decrease distortion and increase embedding capacity.

This paper focuses on Adaptive Pixel Pair Matching Technique (APPM) [7] using Huffman Coding. Initially, the secret message is Huffman encoded. For this purpose, a table should be constructed containing each symbol with their corresponding frequency of occurrence. Here, the secret information used is an audio file. The symbols are arranged in ascending order and then the first two frequency numbers are added. The table is then re-arranged and the process is repeated. Based on the secret message, a pixel is searched in the neighbourhood of the cover image, which is then concealed into the reference pixel. There are a different number of audio files. Most common are Wave files (wav) and MPEG layer 3 files (mp3) [8]. Thus, an audio file is embedded into an image to obtain the stego image. Here, the neighbourhood set is different to that of the Diamond Encoding method, to improve the embedding capacity. It preserves the image quality with less Detectability.

The rest of the paper is organized as follows. Section II describes the related works such as LSB, OPAP, and EMD, DE, Huffman Coding. The proposed method of hiding audio file using APPM is described in Section III. Experimental results are given in Section IV. Conclusion and Remarks are given in Section V.

2.RELATED WORKS

2.1 Single Pixel Substitution Techniques.

LSB and OPAP are the two methods employing single pixel for concealment. LSB Substitution requires the secret message to be embedded into the LSBs of the cover image. This depends upon the embedding parameter 'k'. The original image is termed here as the cover image and the concealed image is called the stego image. The stego pixel values in turn are obtained with the knowledge of the cover pixel values and the number of embedding secret bits. The pixels of the cover image are represented by C_i and the pixels of the resulting stego Image are represented by S_i. The embedding bits are represented by m_i [3]. The embedding process is defined as

$$S_i = C_i - C_i \bmod 2^k + m_i$$

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) is dependent on embedding parameter k. PSNR is given by the formula:

$$\text{PSNR} = 10 \log_{10} (255^2 / \text{MSE})$$

Here MSE – Mean Square Error. This embedding distortion is minimized by the Optimum Pixel Adjustment Process (OPAP). This minimisation is done using the embedding error range which lies between -2^k to 2^k. The total error range is divided into three partitions lying from -2^k to -2^{k-1}, -2^{k-1} to 2^{k-1} and 2^{k-1} to 2^k [3]. The stego pixel value is altered based on these three error ranges.

Example:

$$\begin{bmatrix} 160 & 161 & 162 \\ 163 & 164 & 165 \\ 166 & 167 & 168 \end{bmatrix} = \begin{bmatrix} 164 & 164 & 164 \\ 164 & 164 & 164 \\ 164 & 164 & 164 \end{bmatrix}$$

LSB Substitution

The example above shows the LSBs of the pixel values on the left hand side is replaced by the value 4. This is simple LSB Substitution. The number of embedding bits here is 4 (0100). So the maximum error that can occur here is ($\pm 2^4$ = ±16).

2.2 Pixel Pair Substitution Techniques.

Pixel Pair Matching (PPM) is the method that uses 2 pixel values namely (x, y) and (x', y'). One pixel is concealed into the other based on the secret data. Exploiting Modification Direction (EMD) and Diamond Encoding (DE) are two variants of PPM.

In the case of EMD method, each secret digit in a (2n+1) ary notational system is carried by n cover pixels, where n is the system parameter [4]. The secret message is first divided into a sequence of digits in the (2n+1) notational system. Each secret digit is then embedded into the cover pixel based on the extraction function

$$f(g_1, g_{2,\dots,}g_n) = \left[\sum_{i=1}^{n}(g_i \,.\, i)\right] \bmod (2n+1)$$

Here, the vector $[g_1, g_{2,\dots,}g_n]$ represents the gray values of the cover pixels. The equation above represents the weighted response of the cover pixels. Distance is calculated as d= s – f (g_1, g_2) mod (2n+1), where s represents the secret data. Based on the resulting d value, pixel concealing is done.

In the case of DE, the data hider can hide digits in ($2k^2$+2k+1)-ary notational system, where k is the embedding parameter [6]. This method offers higher embedding capacity than the previous method.
Similar to the EMD method, DE also segments the secret message into digits and conceal each digit into the cover pixel. The difference lies in the fact of calculating the Diamond Characteristic Value (DCV) which is given as

$$f(x, y) = ((2k+1) * x + y) \bmod l$$

Here, l = ($2k^2$+2k+1). For a given cover image, two pixel values are selected and their DCV is calculated using the formula given above. Then, each secret digit is embedded using Diamond Encoding, and a stego image is obtained. [10]

3. PROPOSED METHOD

A novel scheme for embedding secret message into the cover image using APPM technique along with Huffman coding is proposed. The secret message is initially converted to sequence of binary bits and they are in turn grouped to form digits in a B-ary notational system.
Each digit constructed will appear with certain frequency. These digits are then arranged in ascending order and the symbols are added taking two at a time and the process is repeated. The contents of the header of the WAV audio file are retrieved as separate fields; RIFF, total length of package, WAVE, fmt, length of format chunk and length of data to follow. Each field is then converted to bit format and Adaptive Pixel Pair Method is employed to conceal them into an image file [8].

Pixel Pair Matching is mainly concerned with a pixel pair (x,y) and (x',y'). One of the pixels is used as reference co ordinate and the other is used as the search co ordinate. Based on the secret data from a B-ary notational system, a pixel co ordinate (x',y') is searched in the neighbourhood set S(x,y) to conceal (x,y). Adaptive Pixel Pair Matching (APPM) differs from the above in the use of different extraction function f(x,y). Three main features of a PPM method is that there are only exactly B co ordinates in the neighbourhood set S(x,y), and all the co ordinates will be mutually exclusive to each other, and the extraction function f(x,y) should be chosen such that it will minimize the mean square distortion given by,

$$\mathrm{MSE}_{S(x,y)} = \frac{1}{2B}\sum_{i=0}^{B-1}((x_i - x)^2 + (y_i - y)^2$$

The extraction function for APPM is

$$f(x,y) = (x + C_B * y) \bmod B$$

The neighbourhood set for APPM is

$$S(x,y) = \{ (x',y') \| x' - x + y' - y \| \} \leq k$$

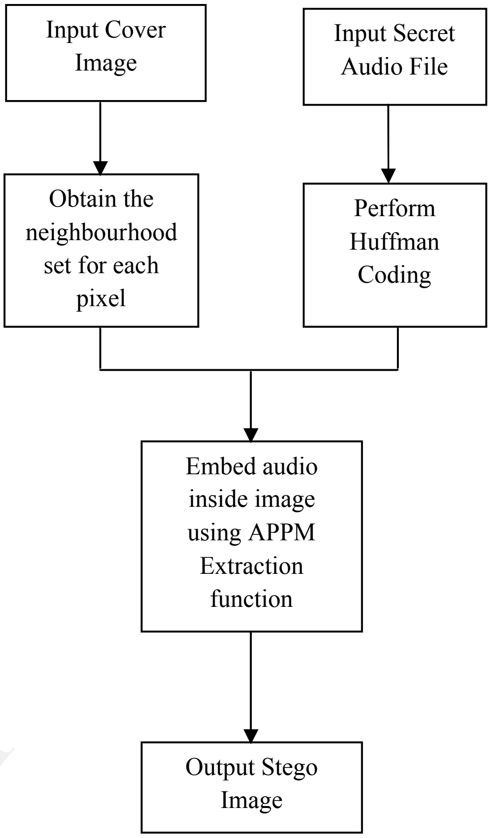

Input Cover Image
Input Secret Audio File
Obtain the neighbourhood set for each pixel
Perform Huffman Coding
Embed audio inside image using APPM Extraction function
Output Stego Image

Fig.1 Hiding audio inside image using APPM and Huffman Coding.

Here, x', y', x, y are pixel vectors related to the reference and searched co ordinate. K is the embedding parameter. The distance of the searched co ordinate from the reference co ordinate in the neighbourhood set should be lesser than or equal to the embedding parameter k. The solution of S(x, y) and f(x, y) is a discrete optimization problem:

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

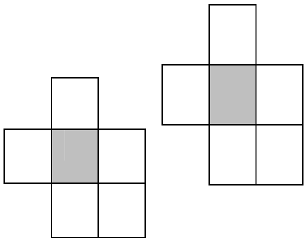
$$\text{Subject to}: f(x_i, y_i) \in \{0,1 \ldots\ldots B-1\}$$

$$f(x_i, y_i) \neq f(x_j, y_j), \text{if } i \neq j$$

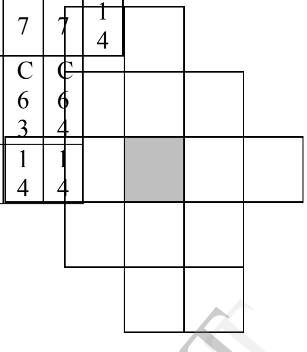
$$\text{for } 0 \leq i,j \leq B-1.$$

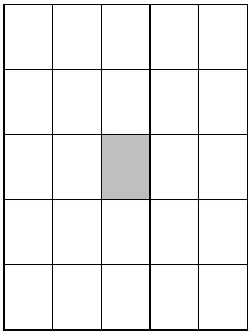
C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17
1	1	2	2	2	2	3	3	3	3	4	5	4	4	6	4
C18	C19	C20	C21	C22	C23	C24	C25	C26	C27	C28	C29	C30	C31	C32	C33
4	4	8	4	5	5	5	5	10	5	5	5	12	12	7	6
C34	C35	C36	C37	C38	C39	C40	C41	C42	C43	C44	C45	C46	C47	C48	C49
6	10	15	6	16	7	7	6	12	12	8	7	7	7	7	14
C50	C51	C52	C53	C54	C55	C56	C57	C58	C59	C60	C61	C62	C63	C64	
14	9	22	8	12	21	16	24	22	9	8	8	8	14	14	

Table I List of constants C_B



$S_4, c_4 = 2$ $S_5, c_5 = 2$

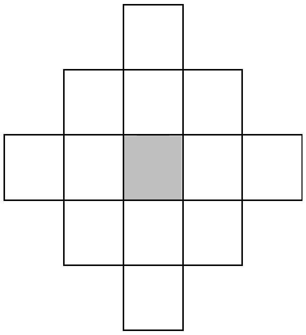


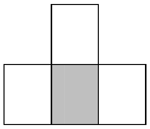


Neighbourhood Set S(x,y)

$S_{13}, c_{13} = 5$

Fig. 2



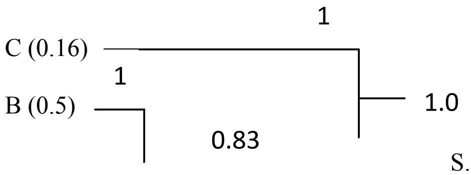


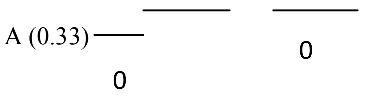
3. 1 Algorithm for Embedding.

(i) Read the input Cover image of size M X M.

(ii) Read the secret audio file. Convert the secret image into sequence of binary bits. Let the number of bits to be embedded be I. Apply Huffman Coding.
Example of Huffman Coding:
If the symbol occurring is ABCBBA, Huffman Code can be constructed as follows:
Frequency of A = 1/3 = 0.33
Frequency of B = 1/2 = 0.5
Frequency of C = 1/6 = 0.16

Arrange these symbols in ascending order of their frequency of occurrence.





The constructed code is:

C = 1

B = 01

A = 00

(iii) Find the minimum B satisfying the condition $\lfloor M \times M/2 \rfloor = |I|$ (or) [MxM $\log_2$ B]/2 = I. For example if MxM = 256 x 256, and I = 50000, then B = 4.

(iv)Find the corresponding C_B value from the table, which shows $C_4 = 2$.

(v) Find the co ordinate (x_i, y_i) such that $f(x_i, y_i) = i$, $0 \leq i \leq B - 1$.

(vi) To embed a secret digit I_B, a pixel (x , y) is chosen in the neighbourhood set S(x,y) based on the distance d = (I_B – f(x,y)) mod B. For example, if (x,y) = (4,5) then f(x,y) = (4+2*5) mod 4 = 2. Now, find (x_i, y_i) such that $f(x_i, y_i) = 2$.

The contents of the header of the WAV audio file are retrieved as separate fields; RIFF, total length of package, WAVE, fmt, length of format chunk and length of data to follow. Each field is then converted to bit format and Adaptive Pixel Pair Method is employed to conceal them into an image file [8].
It employs an extraction function denoted as

$$f(x, y) = (x + C_B * y) \bmod B$$

Where C_B is a constant based on B ary notational system.

-1 0 1

1

0

f (0,0) = 0

f(0,1) = 2

f(1,0) = 1

f(-1,0) = 3

Fig. 6 Neighbourhood set for B=4

From the above example we infer that, f(0,1) = 2. Suppose the secret digit to concealed is $I_B = 3_4$. Calculating the modulus distance, d = (3 – 2) mod 4 = 1. Here, the searched co ordinate is (1,0). Hence the given co ordinate (4,5) has to be replaced with (4+1, 5+0) = (5, 5). Thus, audio embedding using Adaptive Pixel Pair Matching is accomplished. The stego image obtained is very similar to the cover image. Thus, any kind of third party attack can be prevented by maintaining the original image quality. [10]

3. 2 Audio Extraction.

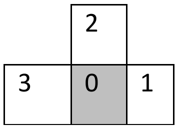
Extraction procedure is very similar to the embedding process in reverse manner.

(1) Using the Huffman dictionary, perform Huffman Decoding at the receiver.

(2) Obtain the new pixel value (x, y). In the above example, this co ordinate corresponds to the value (5,5).

(3) From this co ordinate value, find the concealed digit from the extraction function f(x,y) . Hence, f(5,5) = (5+ 2*5) mod 4 = 3. Thus, the secret digit is revealed as 3_4.

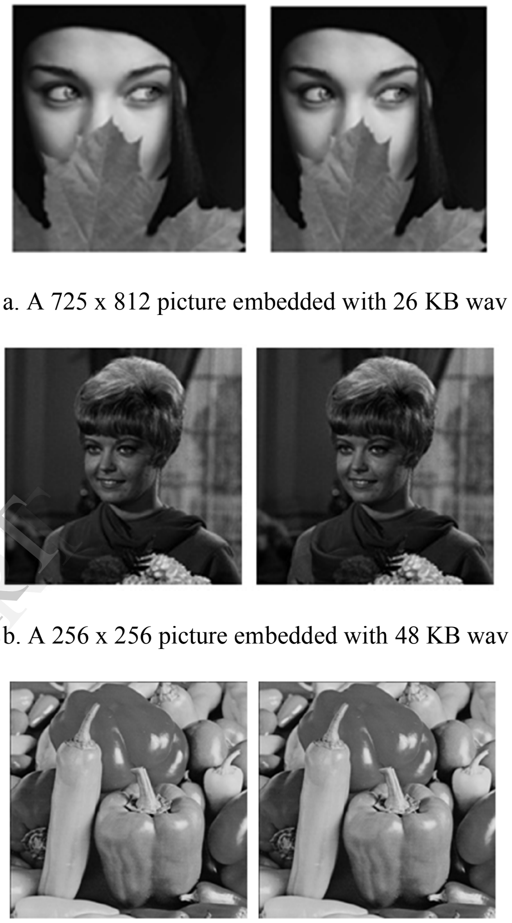
4. IMPLEMENTATION RESULTS



The proposed method is experimented with different images with different file sizes. Embedding capacity is greatly increased with smaller audio file sizes. With increasing embedding rate, PSNR value, seems to decrease. Thus a trade off exists between PSNR and Embedding rate[10]. The Peak Signal to Noise Ratio of such Stego images is given by the expression:

$$PSNR = 10 \log_{10} (255^2 / MSE)$$

In the first result, a 725 x 812 picture is embedded with a 26KB audio file. In the second result, a 256 x 256 picture is embedded with a 48KB audio file and in the third result; a 512 x 512 picture is embedded with a 48KB audio file.



a. A 725 x 812 picture embedded with 26 KB wav file

b. A 256 x 256 picture embedded with 48 KB wav file

c. A 512 x 512 picture embedded with 48 KB wav file.

Fig 7. Implemented Outputs

The goal of Steganography is to evade the detection of hidden information. Mean Square Error is generally not a good measure of Steganalysis. Though single pixel embedding methods like LSB Substitution and OPAP are computationally simple, they do not provide a good measure against Steganalysis [10]. The stego output of the proposed method (Adaptive Pixel Pair Matching), with Huffman Coding has better image quality, it resembles very similar to the original cover image, thus reducing any third party detection. The Mean Square Error of the proposed method is comparatively lower than the already existing systems. The results above clearly depict that the stego image son the right side of every picture resembles very close to the original cover image.

5. CONCLUSION

This paper proposes a novel method for hiding a secret wave file inside a cover image using Adaptive Pixel Pair Matching using Huffman Coding for secret files. Initially, the secret file is converted to bit pattern and then divided into a sequence of digits, after which Huffman coding is employed. At the same time, the extraction function is applied to each pixel of the cover image and their corresponding neighbourhood values are also found. A neighbouring pixel with a distance lesser than the embedding parameter is chosen to be concealed into the reference pixel. The stego image quality is greatly preserved when compared with the previous Steganographic methods. This method not only resolves the problem of increased embedding distortion, also improves the lower payload capacity which was predominant in the previous methods.

6.REFERENCES

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to Steganography," *IEEE Security Privacy*, vol. 3, no. 3, pp. 32–44,May/Jun. 2003..

[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] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474, 2004.

[4] X. Zhang and S. Wang, "Efficient Steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.*, vol. 10, no. 11, pp. 781–783, Nov. 2006.

[5]Ki-Hyun Jung, Yeungjin Republic of Korea Kee-Young Yoo, "Improved Exploiting Modification Direction Method by Modulus Operation", *International Journal of Signal Processing, Image Processing and Pattern* Vol. 2, No.1, March, 2009

[6] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," *EURASIP J. Inf. Security*, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[7] Wien Hong and Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", *IEEE Transactions on Information Forensics and Security*, vol. 7, February 2012

[8]M.I. Khalil, "Image Steganography: Hiding short Audio messages within digital images", *JCS&T* Vol. 11 No. 2

[9] K.P.Adhiya Swati A. Patil, "Hiding Text in Audio Using LSB Based Steganography". *Information and Knowledge Management* ISSN 2224-5758 (Paper) ISSN 2224-896X ,Vol 2, No.3, 2012.

[10] Imaculate Rosaline S and Ashok Rak M, " Adaptive Pixel Pair Matching based Steganography for Audio Files", *IEEE Explore, ISBN : 978-1-4673-5301-44, Jan 2013*