ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

A Secure and Efficient Method for Embedding Audio Secret Data on Audio Host using APPM and KBRP

Geethu Gopan[1], Bhraguram T M[2], Dr. Varghese Paul[3]

MTech Student, CSE, Adi Shankara Institute of Engineering and Technology, Kalady, India[1]

Asst.Professor, IT, Adi Shankara Institute of Engineering and Technology, Kalady, India [2]

Dean, CS IT, Cochin University for Science and Technology, Cochin, India [3]

Abstract: This paper proposes an effective method for hiding audio secret data on audio host using the principle of Adaptive Pixel Pair Matching (APPM) and based on KBRP. APPM is a data hiding method. It is based on principle of Pixel Pair Matching (PPM). PPM is a pixel pair adjustment process. In this initially the host audio is sampled and convert into matrix. The secret audio is divided into stream of bits. Then a pair (a, b) of host audio is selected randomly and modulus distance 'D' between secret data 'Sd' and f (a, b) is calculated. Then reference co-ordinate (a, b) is replaced with searched co-ordinate (a+aD, b+bD) inorder to conceal the secret data. A key based random permutation is used inorder to enhance security. KBRP method generates one permutation for a specific size from given key. The generation process consists of three steps namely initialization, elimination and filling. LSB embedding method and Optimal Pixel Adjustment Process (OPAP) were the older methods which employs one pixel as an embedding unit. Exploiting Modification Direction (EMD), Diamond Encoding (DE) and APPM are the variations of PPM. EMD cause distortions to secret data. DE can conceal large amount of data to cover images. But payload of DE is determined by selected notational system. The proposed method causes lesser distortions, provides more security for secret data and exhibits better performance. Moreover this is an effective method which makes secret audio indistinguishable from host audio and secret audio can be correctly retrieved.

Keywords: PPM; LSB; OPAP; EMD; DE; APPM; KBRP

I. INTRODUCTION

Data Security plays an important role in the field of communication. Data should be protected from destructive forces and unauthorized access. Data hiding is associated with digital forms such as cryptography, steganography and watermarking. Cryptography is obscuring the contents of the message, and not communicating the contents of the message. Steganography which means 'covered writing' is hiding the contents of the secret message within cover media. Watermarking adds sufficient metadata to a message.

The aim of thesis is to provide a secure and efficient method for hiding secret audio data into host audio with minimum distortion, more security and better performance. It is based on the principle of Adaptive Pixel Pair Matching [1]. Security is provided by using a key based random permutation [12]. KBRP method generates one permutation for a specific size from given key. The generation process consists of three steps namely initialization, elimination and filling. Moreover the method should make secret audio indistinguishable from host audio and secret audio can be correctly retrieved.
In this initially the host audio is sampled and convert into matrix. The secret audio is divided into stream of bits. Then a pair (a, b) of host audio is selected and modulus distance 'D' between secret data 'Sd' and f (a, b) is calculated. Then reference co-ordinate (a, b) is replaced with searched co-ordinate (a+aD, b+bD) inorder to conceal the secret data.

The main objective is to find out a novel method that support high payload, to reduce distortion caused by embedding, to figure out the method that provide better performance and to ensure high security. The stego audio should not give an idea that a secret audio is included in it and secret audio should be retrieved at extraction portion correctly without distortion.

II. BACKGROUND

There exist various methods for data hiding. Some uses one pixel as an embedding unit and some others use pixel pair as embedding unit. LSB embedding [2] and Optimal Pixel Adjustment Process (OPAP)[20] uses a single pixel as embedding unit. Exploiting Modification Direction (EMD) [3], Diamond Encoding (DE) [4], and Adaptive Pixel Pair Matching (APPM) [1] are the techniques based on pixel pair matching (PPM) [1]. In LSB embedding the pixels with even

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

values will be increased by one or kept unmodified and pixels with odd values will be decreased by one or kept unmodified.

In 2004, Chan et al. proposed a simple and efficient optimal pixel adjustment process (OPAP) [20] method to reduce the distortion caused by LSB replacement.

In 2006 Zhang and Wang proposed EMD[3] method. It is based on PPM. In 2009 Chao et al. proposed a Diamond Encoding (DE) [4] method to enhance the payload of EMD.

In 2012 Hong and Chen proposed a novel data embedding method using Adaptive Pixel Pair Matching (APPM) [1]. This is a simple and efficient data embedding scheme based on PPM. It achieves better image quality. This offers smaller mean squared error (MSE). It also offers secure communication.

III. PROPOSED SCHEME

A. Adaptive Pixel Pair Matching Method for Embedding Secret audio over Audio Host

This paper proposes an effective method for hiding audio secret data on audio host using the principle of Adaptive Pixel Pair Matching (APPM) and based on KBRP. In this the host and secret data are audio signals.

There exists different audio file formats such as
1) Uncompressed audio formats.
2) Formats with lossless compression.
3) Formats with lossy compression.

In this method WAV file format is chosen for host audio and secret audio. The host audio 'HA' is sampled and convert into matrix. The secret audio 'SA' is sampled and convert into bits. Then choose each secret bit. 'sd' is the secret message bits to be concealed and the size of sd is |sd|. First we calculate the minimum B satisfying

$[HA*log_2 B]/2=SA$

Such that all the message bits can be embedded. Then the discrete optimization problem should be solved to find cB and neighbourhood of (a, b).

Extraction Function and Neighbourhood Set

The definitions of neighbourhood set, n(a,b) and extraction function f(a,b) significantly affect the stego audio quality. The designs of n(a,b) and f(a,b) have to satisfy the following requirements: All values of f(a,b) in n(a, b) have to be mutually exclusive, the summation of the squared distances between all coordinates in n(a,b) and f(a,b) has to be calculated and it should be the smallest. During embedding,

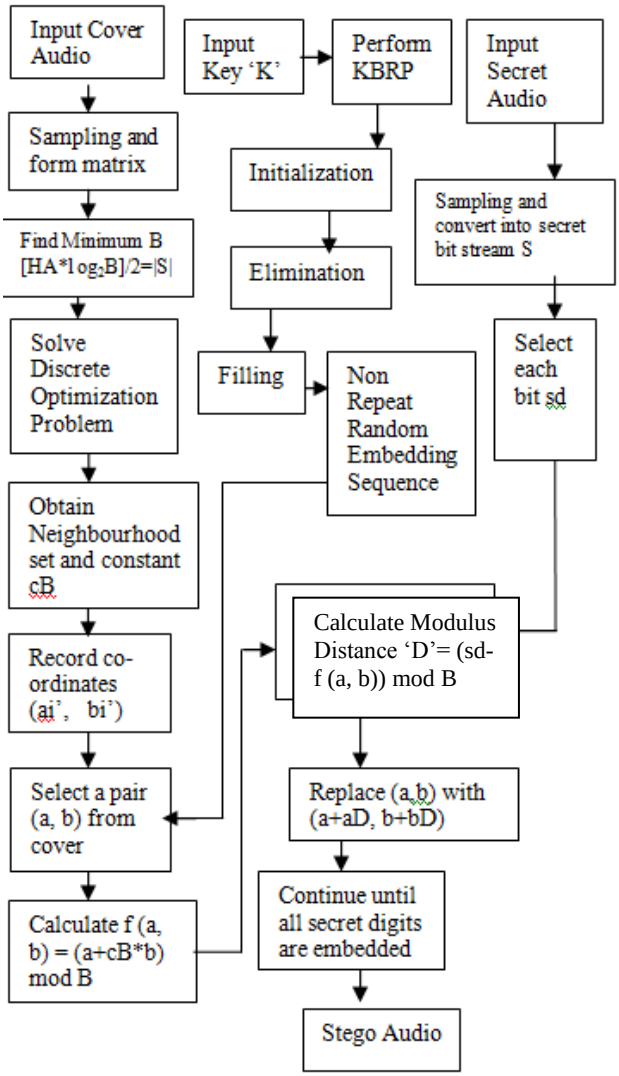

Fig. 1. APPM method for embedding secret audio into host audio based on KBRP

(a, b) is replaced by one of the coordinates in neighbourhood set of (a, b) that matches with the secret digit. The averaged MSE can be obtained by averaging the summation of the squared distance between (a,b) and other coordinates in n(a, b). Thus, given a n(a, b), the expected MSE after embedding can be calculated by

$MSE_n (a, b) = 1/2B [((a_i-a)^2+ (b_i-b)^2)$

An adaptive pixel pair matching (APPM) data-hiding method explores better n(a, b) and f(a, b) so that MSE is minimized. Data is then embedded by using PPM based on these n(a, b) and f(a, b).

$f (a, b) = (a+cB*b) \bmod B$

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

c2	c3	c4	c5	c6	c7	c8	c9	c10	c11	c12	c13	c14	c15	c16	c17	c18
1	1	2	2	2	2	3	3	3	3	4	5	4	4	6	4	4
c19	c20	c21	c22	c23	c24	c25	c26	c27	c28	c29	c30	c31	c32	c33	c34	c35
4	8	4	5	5	5	5	10	5	5	5	12	12	7	6	6	10
c36	c37	c38	c39	c40	c41	c42	c43	c44	c45	c46	c47	c48	c49	c50	c51	c52
15	6	16	7	7	6	12	12	8	7	7	7	7	14	14	9	22
c53	c54	c55	c56	c57	c58	c59	c60	c61	c62	c63	c64					
8	12	21	16	24	22	9	8	8	8	14	14					

Fig. 2. List of constant cB for 2<=B<=64

The solution of n(a, b) and f(a, b) is indeed a discrete optimization problem which is given by

Minimize $(a_i\text{-}a)^2 + (b_i\text{-}b)^2$

Subject to: f (a_i, b_i) element of {0, 1 ...B-1}
f (a_i, b_i) !=f(a_j, b_j), if i!=j
for 0 <= i,j <=B-1

Construct a nonrepeat random embedding sequence Q using a key K. A key based random permutation is used inorder to provide security.

Embedding Phase

In this the host and secret data are audio signals. Suppose the cover audio is 'HA'. The host audio is sampled and convert into matrix. The secret audio 'SA' is sampled and convert into bits. Then choose each secret bit. 'sd' is the secret message bits to be concealed and the size of sd is |sd| . First we calculate the minimum B such that all the message bits can be embedded. Then the discrete optimization problem should be solved to find cB and neighbourhood of (a,b). Construct a nonrepeat random embedding sequence Q using a key K. A key based random permutation is used inorder to provide security. KBRP method generates one permutation for a specific size from given key. The generation process consists of three steps namely initialization, elimination and filling. To embed a message digit sd, coordinates (a, b) in the cover audio is selected according to the embedding sequence Q, and calculate the modulus distance

D=(sd-f(a, b)) mod B

It is between sd and f(a, b), then replace (a, b) with (a+aD , b+bD). The secret audio bits are concealed into coordinates of host audio.

Embedding Algorithm

Input: Cover audio HA is sampled and convert into matrix, Secret Audio 'SA' converted into secret bit stream S, and key K which undergoes KBRP.

Output: Stego audio HA', cB, n(a, b).

1. Find the minimum B satisfying [HA log_2 B]/2=SA

2. Solve the discrete optimization problem to find cB and n (a, b).

3. In the region defined by n (0, 0), record the coordinate (a'i, b'i) such that f (a'i, b'i) = i, 0<=i<=B-1.

4. Construct a nonrepeat random embedding sequence Q using a key K by means of a Key Based Random Permutation.

5. To embed a message digit sd, coordinates (a, b) in the cover audio is selected according to the embedding sequence Q, and calculate the modulus distance D= (sd-f (a, b)) mod B between sd and f (a, b), then replace (a, b) with (a+aD, b+bD).

6. Repeat Step 5 until all the message bits are embedded.

Extraction Phase

The embedded secret audio should be extracted from stego audio. Scan coordinates in the same order as in the embedding procedure. Calculate extraction function of the scanned coordinates inorder to obtain secret message digits. The message bits S can be obtained by converting the extracted message digits into a binary bit stream.

Extraction Algorithm

Input: Stego audio HA', cB , n(a,b), and Key K.

Output: Secret bit stream S.

1. Construct the embedding sequence Q using the key K by means of KBRP.

2. Select coordinates (a', b') according to the embedding sequence Q.

3. Calculate f (a', b'), the result is the embedded digit.

4. Repeat Steps 2 and 3 until all the message digits are extracted.

5. Finally, the message bits S can be obtained by converting the extracted message digits into a binary bit stream.

Key Based Random Permutation

A key based random permutation is used inorder to provide security. KBRP method generate one permutation for a specific size from given key. The generation process consists of three steps namely initialization, elimination and filling.

Key Based Random Permutation Algorithm

1. Initialization

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

Input: Key K, Array Size N

Output: An array that contain modified ASCII value of input key K

Let P be the array that hold permutation with values 1 to N, Let S be size of key

1. Store the ASCII value of key K in an array A

2. Do step 3 starting from 1 and continue until length of Key

3. Add P[i] and P[i+1]

4. Keep the value at first location of A to P[S]

5. Repeat step 6 to step 10 till S is greater than N

6. Increment value of S and store it in j

7. Repeat step 8 to step 10 for i starting from 1 to S-1

8. Repeat step 9 and 10 for k starting from i to S-1 and the value of j less than or equal to N

9. Add P[i] and P[k+1]

10. Increment value of j

11. Compute P[i] mod N and store result in P[i].

2. Elimination

1. Initialize left with 1 and right with size of array.

2. Repeat steps 3 to 6 until left less than right

3. Repeat step 3.1 and 3.2 for i starting from left+1 to right

3.1. If P[left] == P[i]

3.2. Then set P[i] to zero

4. Repeat step 4.1 and 4.2 for j starting from right-1 to left+1

4.1. If P[right] == P[j]

4.2. Then set P[j] to zero

5. Increment left by 1

6. Decrement right by 1

3. Filling

1. Let A be the array containing missing values in P and m be the number of missing values in A

Let P be the array that hold permutation with values 1 to N

2. Initialize i to 0

3. Repeat the following steps till i is greater than m

4. Store the value of N to j

5. Decrement value of j till P[i] becomes zero and j less than 0.

6. If j greater than zero

6.1. Then store value of A[i] to P[i]

6.2. Increment value of i

7. Initialize k to 1

8. Increment value of k till P[k] becomes zero and k greater than N

9. If k less than equal to N

9.1. Store value of A[i] to P[k]

9.2. Increment value of i

IV. EXPERIMENTAL RESULTS

In the APPM method for embedding secret audio over host audio, both secret data and host data are audios. Powerdown.wav is given as cover audio and goodbye.wav is given as secret audio, which are standard test data from internet. PSNR and Signal-to-Distortion Ratio is computed inorder to analyse performance of the proposed method. Waveform and power spectrum of extracted audio is also plotted. It is then compared with that of secret audio. PSNR between cover audio and stego audio is calculated and that between secret audio and extracted secret audio is performed.

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.

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

MAX is the maximum possible pixel value. MSE is mean squared error.

Then the method is also evaluated with user inputs such as covertest.wav and secrettest.wav. This method is also evaluated using Signal-to-Distortion Ratio.SDR is the ratio of actual signal to the amount of distortion caused to it. It is expressed in terms of decibels. In this consider the actual signal and signal with distortion.

SDR=$10log_{10}$ (Top/Bottom)

Top = 1/size (f, 1)*(sum(f.^2))

Bottom = 1/size (f2, 1)*(sum(f2.^2))

f is sampled data of actual signal and f2 is that of distorted signal.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

Cover Audio	Secret Audio	Method	PSNR Secret	PSNR Cover
powerdown.wav(64 KB)	goodbye.wav(8 KB)	APPM	Infinity	54.24 DB
covertest.wav(80 KB)	secrettest.wav(8 KB)	APPM	Infinity	48.50 DB

Table. 1. Result of APPM Method for embedding secret audio over host audio

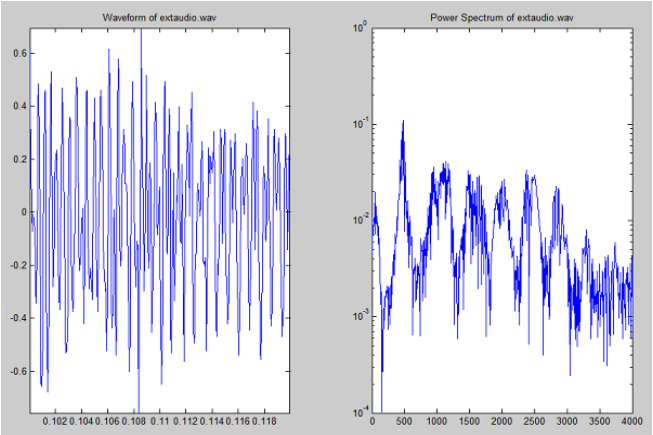

Fig. 3. Waveform and power spectrum of extracted audio when secret audio is goodbye.wav

V. CONCLUSION

A Secure and Efficient Method for Embedding Audio Secret Data on Audio Host using APPM and KBRP is an efficient and secure method for embedding secret audio over host audio. Since it provides security by means of KBRP and secret audio is extracted without any distortion. MSE is very low. High PSNR value is obtained. From stegoaudio it's not able to detect the presence of secret audio. Secret audio is indistinguishable from host. The proposed method causes lesser distortions, provides more security for secret data and exhibits better performance. KBRP method generates one permutation for a specific size from given key. The generation process consists of three steps namely initialization, elimination and filling. The proposed method is efficient and secure for embedding audio secret data on audio host. It exhibits better performance. But the execution of this method takes some time. There is time delay for key processing. In future adopt an efficient method for generating random embedding sequence using a key with lesser processing time. The next work that can be done is compare the performance of "A Secure and Efficient Method for Embedding Audio Secret Data on Audio Host using APPM and KBRP" using different audio file formats. Here the method is implemented using .wav audio file formats. Then this method can be implemented on video. Video should be first converted to image sequence. Then APPM method can be implemented and performance is evaluated. The method is separately implemented in audio and image. Research can be carried out by implementing this method on video that has sound.

REFERENCES

[1] W.Hong and T.S.Chen, "A Novel Data Embedding Method using Adaptive Pixel Pair Matching," IEEE Trans. Inf. Forensics Security, vol. 7, no.1, pp. 469–474, 2012.

[2] 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.

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

[4] 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.

[5] J. Wang, Y. Sun, H. Xu, K. Chen, H. J. Kim, and S. H. Joo, "An improved section-wise exploiting modification direction method," Signal Process., vol. 90, no. 11, pp. 2954–2964, 2010.

[6] W. Zhang, X. Zhang, and S. Wang, "A double layered plus-minus one data embedding scheme," IEEE Signal Process. Lett., vol. 14, no. 11, pp. 848–851, Nov. 2007.

[7] T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 215–224, Jun. 2010.

[8] J. Fridrich, M.Goljan, and R.Du, "Reliable detection of LSB steganography in color and grayscale images," in Proc. Int. Workshop on Multimedia and Security, 2001, pp. 27–30

[9] A. D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005.

[10] L.Tawade, R.Mahajan, C.Kulthe "Efficient and Secure Data Hiding using Secret Reference Matrix", IJNSA,Vol.4, No.1, Jan 2012

[11] G.Bindu, K.Srilakshmi "A Novel Approach of LSB Steganography for Retrieving Text from Audio", IJCTA, Vol.3, Aug 2012

[12] S.M.Hussain, N.M.Ajlouni "Key Based Random Permutation", Journal of Computer Science 2 (5): 419-421, 2006

[13] R.Amirtharajan, R.Akila, P.Deepikachowdavarapu "A Comparative Analysis of Image Steganography" International Journal of Computer Applications (0975 – 8887),Volume 2 – No.3, May 2010

[14] S.I.Rosaline, M.A.Raj "Adaptive Pixel Pair Matching Based Steganography for Audio Files", IEEE Trans. Inf. Forensics Security, vol. 4, no.13,2013

[15] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," Signal Process., vol. 90, pp. 727–752, 2010.

[16] 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.

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

[18] K. Gopalan, "Audio steganography using bit modification", Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, pp. 421-424, April 2003.

[19] J. Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett., vol. 13, no. 5, pp. 285–287, May 2006.

[20] Chi-Kwong Chan, L.M. Cheng, Improved hiding data in images by optimal moderately significant-bit replacement, IEE Electron. Lett. 37 (16) (2001) 1017–1018.