International Journal of Research in Engineering, Science and Management
Volume-3, Issue-4, April-2020
www.ijresm.com | ISSN (Online): 2581-5792

Effective Audio Steganography Based On LSBMR Algorithm

B. Sharmila
Assistant Professor, Department of Computer Science and Engineering, Vivekanandha College of Technology for Women, Tiruchengode, India

***Abstract*: Steganography is used to embed secret data into cover thereby no one can realizes the secret data apart from the sender and intended recipients. Different carrier file formats are employed for steganography, here we consider audio files. There are several steganographic techniques exist for hiding secret information in audio. This paper presents the results of analyzing the performance of data hiding at high power of the audio [11]. Moreover, to increase the complexity for intrusion detection [12]-[14], encryption and preprocess is done. The adaptive steganography for audio file is experimented with .WAV file. The algorithms performance is compared on the basis of evaluation parameters like Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE). This method can select the samples depending on the length of secret message, and the high pitch of audio. For length of message is short, only small samples are utilized while on leaving others. If the data rate enhances, more samples are used for hiding the data by adjusting the parameters.**

***Keywords*: Least Significant Bit (LSB) based steganography, Segmentation, Data Embedding, Data Extraction, Embedding Unit (EU), Threshold.**

1. Introduction

Information hiding is one of the important areas of information security, which includes various methods like cryptography, steganography and watermarking.

Incryptography encryption is done results in a disordered and perplexing message. Though the message cannot read by the third party but attract eavesdroppers easily. To conquer this issues, Steganography is used through hiding the secret information behind a cover media (video, audio or image). Steganography is used to embed secret data into cover thereby no one can realizes the secret data apart from the sender and intended recipients. A few key properties must be taken into consideration when creating a digital data hiding system.

(1) Imperceptibility: Imperceptibility is the primary goal of steganography. When a person views a cover, he or she should be unable to distinguish the cover with embedded information from an image without embedded information.

(2) Embedding Capacity: Capacity denotes the amount of information can be embedded by using a particular system.

(3) Robustness: Robustness denotes the degree of difficulty needed to destroy embedded information without affecting cover work itself.

(4) Undetectability: detectability refers to the ability to determine whether or not a cover medium contains embedded information using statistical or technological means. This paper is arranged as follows section 2 describes the limitations of relevant approaches and propose some strategies. In Section 3 data embedding and data extraction details are given. Section 4 discusses the experimental results.

2. Analysis of limitations of relevant approaches

Many algorithms are dealt with the audio steganography. Mainly the LSB algorithm is the was simplest and effective in the steganographic concepts. LSB plane of cover is overwritten with the secret bit stream. On average, LSB needs only half bits in cover be varied. By using the steganalytic algorithms namely Chi-squared attack [3] and Regular/Singular groups (RS) analysis [4], the existence of hidden message even at a minimal embedding rate is detected. LSB matching (LSBM) scheme utilizes slight modification to LSB replacement. If the secret bit does not match the LSB of cover then +1 or -1 is randomly added to the corresponding LSB. For analyzing the LSBM, several steganalytic algorithms are introduced. LSB Matching Revisited (LSBMR) [2] algorithm is used for image, that utilizes pair of pixels as embedding unit, where the LSB of first pixel carries one bit of secret message, and relationship (odd–even combination) of two pixel values carries another bit of secret message. In this paper LSBMR algorithm is applied for audio samples. In [1] Weiqi Luo et al., use this LSBMR algorithm for hiding data in edges of images. Likewise, our proposed method uses LSBMR algorithm for hiding data in high power audio. Perception-based data hiding schemes for audio are influenced by properties of the human auditory system (HAS). For data hiding/watermarking in audio data [5]–[7], various perception-based algorithms were proposed in the past. These algorithms are classified based on the underlying technique of data embedding: perceptual masking [6], direct sequence spread spectrum (DSSS) [3], [4] and phase coding [6], [7]. The phase coding [6]-[8] algorithms performs well as far as imperceptibility of embedded data is concerned, however experiences certain issues e.g. some of them failed to perform well against standard data manipulations and most of them have minimal payloads i.e. amount of information embedded. For instance, the phase coding technique [6] can embed 16-32 bits of data in one-second duration audio samples. The algorithm

based on echo-based coding [9] can embed about 40-50 bits of data in one-second duration of an audio signal. Here the main key issue is choosing the region for data hiding and imperceptible payload. In [11] efficient power adaptive scheme based on LSBMR algorithm, though the data's are embedded in high power, they are not encrypted for audio is analyzed. In this paper those issues are rectifies and additional security is provided for the embedded data using public key cryptography.

3. Proposed scheme

Here we suggest, an efficient pitch adaptive scheme using LSBMR algorithm [1] for audio is analyzed. The flow diagram of our proposed data embedding and extraction is illustrated in figure 1 and figure 2. (Modified version of [11]).

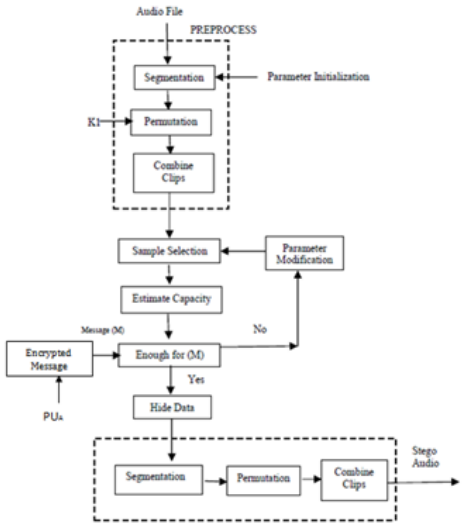

Fig. 1. Data embedding

In this paper, the high pitch audio are chosen, because of more complicated features are present and are highly dependent on the audio file. Moreover, it is more difficult to observe changes at the high pitch of audio samples than those in low pitch audio samples. Embedding of data is done through following phases [11], [15]

In the data embedding stage, first initialize some parameters (segmentation size & threshold), which are used for subsequent data pre-processing and sample selection. Here to improve the security concern text message is encrypted by receiver's public key (PUa), on the receiver side data is decrypted using receiver private key (PRa). Now, estimate the capacity of those selected samples. If the samples are large enough for hiding the given text message, then data hiding is performed on the selected samples. Thereafter, post processing is done to obtain the stego audio. Or else, the parameters values get changed, and then sample selection and capacity estimation process is reiterate until the text message can be embedded completely. Here the secret message is hidden using parameters, which are different for different audio file and encrypted text message. We need them as side information to guarantee the validity of data extraction. In this paper, adaptive scheme to the spatial LSB domain is used. High pitch of audio signal which is represented by means of large values of sample is chosen as the criterion for region selection and use LSBMR as the data hiding algorithm.

LSBMR [2] utilizes a pixel pair (xi, xi+1) in cover image as embedding unit. After message embedding, the unit is modified as (x'i, x'i+1) in the stego image which satisfies the condition,

$$LSB(x'i) = mi,\ LSB((x'i/2) + x'i+1) = mi+1 \quad (1)$$

Here the function LSB(x) denotes the LSB of the pixel value x. mi and mi+1 are the two secret bits to be embedded. We use this LSBMR algorithm applied in image pixels, for samples in audio. In data extraction, the scheme extracts the parameters from the stego audio. The pre-processing is performed based on the side information and identifies the samples used for data hiding. It obtains the data according to the corresponding extraction algorithm. In data extraction, it creates a travelling order through the PRNG with shared key. Two bits are extracted for every embedding unit with the order. The first secret bit is the LSB of the first sample value, and the second bit can be obtained by calculating the relationship between the two samples.

The data embedding and data extraction algorithms details are as below [11].

A. Data Embedding

Step 1: Parameter Initialization

The cover audio file of size of m is first divided into non-overlapping clips of Cz Samples. For that the Clip size is randomly selected from the range between {from 1 to length of audio sample}, and the threshold is chosen based on amplitude of audio file.

Step 2: Preprocess

Step 2a: Segmentation

The audio file is segmented into clips as determined by the parameter Cz. For Example, when we choose the clip size as 4, 6 or 100,

Step 2b: Permutation

After the segmentation, each of the samples in individual small clips is permutated in a pseudorandom order as per the shared key1 k1. With permutation the samples are rearranged as per the key1

Benefits obtained by the random permutation is that, we can prevent the detector from getting the correct embedding units without the permutation key1, and thus security is improved and also permutation complex the operation of brute force method of attack.

Step 3: Sample Selection

Based on the LSBMR [2] scheme, 2 secret bits are embedded into every embedding unit. Therefore, for a given message (M), the threshold T for sample selection can be determined as follows.

When, EU (t) is the set of sample pairs whose absolute values are higher than or equal to a parameter T [1].

$$EU(t) = \{(xi, xi+1) \parallel xi, xi+1 | \geq T, \text{ for all } (xi, xi+1) \in V\} \quad (2)$$

Step 4: Capacity Estimation

We calculate the threshold [1] by

$$T=\max \{2 x \mid EU(t)| \geq | E(M) |\} \quad (3)$$

Where T ∈ {amplitude of audio}, |E (M)| is the size of the message E (M), EU (t) and denotes the total number of elements in the set of EU (t).

Step 5: Data Hiding

RSA algorithm is employed to encrypt the data's.

Perform data hiding on the Encrypted data

EU (t) = {(xi, xi+1) || xi, xi+1 | ≥ T, for all (xi, xi+1) ∈ V} [1]

Embedding units are processed in pseudorandom order measured by secret key k2 for every unit, (xi, xi+1). These sample pairs are converted to binary. The data hiding is performed according to the following four cases.

Case 1:

LSB (xi) = mi & LSB (f (xi, xi+1) = mi+1 then (xi', xi+1') = (xi, xi+1)

Case 2:

LSB (xi) =mi & LSB (f (xi, xi+1)) ≠ mi+1 then (xi', xi+1') = (xi, xi+1+ r).

{Where r = 0.001}

Case 3:

LSB (xi) ≠ mi & LSB (f (xi-1, xi+1)) = mi+1 then (xi', xi+1') = (xi-1, xi+1)

Case 4:

LSB (xi) ≠ mi & LSB (f (xi-1, xi+1)) ≠ mi+1 then (xi', xi+1') = (xi+1, xi+1) where mi and mi+1 denote two secret bits to be embedded. The function 'f' is defined as

f (a, b) = (a/2) +b.

r is a random value in {-0.001,+0.001} and (xi' , xi+1') denotes the sample pair after data hiding. After the above modifications xi' and xi+1' may be less than the threshold T. In such cases, we need to readjust them as (x''i, x''i+1) by

x'i = xi'+k1

x''i+1 = x'i+1 +k2

k1 and k2 posses the value of either 0.001 or 0.002 finally, we have LSB (xi '') = mi & LSB (f (x''i, x''i+1) = mi+1

Step 6: Postprocess

After data hiding, the resulting audio is divided into nonoverlapping Cz clips. The clips are then inverse permuted based on key1.The process is very similar to preprocess except that the rearrangement are opposite. Then we embed the two parameters (Cz & T) into a preset region which has not been used for data hiding.

Step 7: Preset Region

There are two parameters in this approach. The first one is the clip size Cz used for audio segmentation in data preprocessing; another is the threshold T for selection of embedding samples. Cz is randomly selected and T depends on amplitude of audio and is determined by the type of audio and the size of secret message M.

The preset region chosen may be in the unused samples or flat/smooth/low power region. Otherwise the region is decided between sender and receiver the suitable place to hide these parameters.

B. Data Extraction

The receiver has to perform the same procedure as sender, and the steps done are as follows,

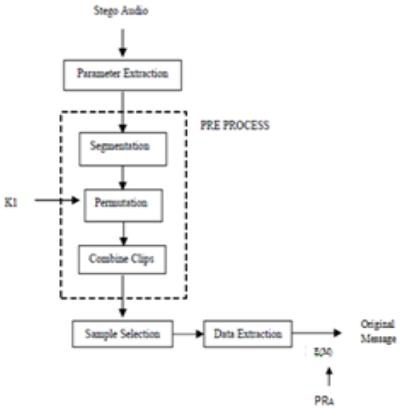

Fig. 2. Data Extraction

Step 1: Parameter Extraction

To get secret data, first extract the side information, i.e., the clip size Cz, and the threshold from the stego audio. Execute the same things as step 1 in data embedding.

Step 2: Preprocess

The stego audio is segmented into Cz clips and are then permuted by the secret key k1 the resulting clips are then combined.

Step 3: Sample Identification

Travel the embedding units whose values are higher than or equal to threshold T on the basis of pseudorandom order with secret key2, until each hidden bits are extracted.

Step 4: Data Extraction

For each qualified embedding unit, say, (x'I , x'i+1), where | x'I - x'i+1 | ≥ T, we extract the two secret bits mi and mi+1 as follows:

mi = LSB (x''i) & mi+1 = LSB ((xi/2) +x'i+1)

Step 5:

Convert these bits into ASCII value followed by changing it into characters.

Now we obtain the encrypted message, this encrypted value is reviled by receiver's private key (PRa)

4. Conclusion and future work

In this paper, performance of adaptive audio steganography for .wav audio [11] file is analyzed. In addition to that, encryption [18]-[21] is performed before the data hiding is performed. This process is mainly performed for improving the security. The audio quality after data embedding is very important for better performance of steganography [16], [17] methods. The audio quality is evaluated by Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

The following conclusions can be made from this analysis:

1) This method applies the public key cryptographic

approach to provide additional security.

2) Uses segmentation and permutation process which uses shared key k1, further creates second level of security.
3) Also threshold value is used hence only required samples alone involve for modification.
4) This algorithm is applied for the samples a high pitch, which is insensible to modification.

References

[1] Weiqi Luo, fangjun Huang, Jiwu Huang, 'Edge Adaptive Image Steganography Based on LSB Matching Revisited', IEEE transaction on Information forensics and security, vol. 5, no. 2, 2010.
[2] Mielikainen J. 'LSB matching revisited', IEEE signal Process. vol. 13, no. 5, pp. 285-287, 2006.
[3] Westfeld A and Pfitzmann A, 'Attacks on steganographic systems', in Proc. 3rd Int. Workshop on Information Hiding, vol. 1768, 1999.
[4] Fridrich J., Goljan J., and Du R., 'Detecting LSB steganography in color, and gray-scale images', IEEE Multimedia, vol. 8, no. 4, pp. 22–28, 2001.
[5] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, "Information Hiding – A Survey," Proc. of IEEE, vol. 87, no. 7, pp. 1062-1078, July 1999.
[6] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, 1996.
[7] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking," Signal Processing, vol. 66, pp. 337-355, 1998.
[8] Y. Yardimci, A. E. Cetin, and R. Ansari, "Data hidingin speech using phase coding," Proc. Eurospeech Conference, 1997.
[9] Fatitha Djebbar, Brghdd Ayad, "A view on latest audio Steganography techniques", IEEE 2011.
[10] Rashid Ansari, Hafiz Malik, "Data hiding using frequency selective phase alteration", IEEE 2004.
[11] Sharmila B, Shanthakumari. "Power Aware Audio Steganography Based on LSBMR Algorithm", OSIET journal of Information Technology, May 2012.
[12] Santhosh Babu A. V, Meenakshi Devi P, Sharmila B, 'Efficient enhanced Intrusion identification and response system for MANETs', International Journal of Business Information Systems, vol. 29, no. 4, pp. 535-546, 2018.
[13] Santhosh Babu A. V, Meenakshi Devi P, "Energy aware Intrusion Detection System for MANETs", International Journal of Applied Engineering Research, 2015
[14] Pavanya U, Ramya M, Surya N & Santhosh Babu A. V, 'Protecting Location Privacy for Task Allocation', International Journal of Innovative Research in Information Security, vol. 6, no. 3, pp. 208-214, 2019.
[15] Santhosh Babu A. V, Meenakshi Devi P, Sharmila B and Suganya D, 'Performance Analysis on Cluster based Intrusion Detection Techniques for Energy Efficient and Secured Data Communication in MANET', International Journal of Information Systems and Change Management, vol. 11, no. 1, pp. 56-69, 2019.
[16] Santhosh Babu A. V. and Meenakshi Devi P, 'Swarm Optimized Energy Hubness Clustering to Detect and Respond Intrusive Attack Variants in MANET', International Journal of Business Innovation and Research, vol. 18, no. 3, pp. 369-391, 2019.
[17] Birundha K, Harini S, Hemalatha G, Kalaiselvi P and Santhosh Babu A V, 'A New Technique for Secured Authentication with PC Control through SMS', International Journal of Engineering Research in Computer Science and Engineering, vol. 5, no. 3, pp. 445-447, 2018.
[18] Santhosh Babu A V, Meenakshi Devi P and Sharmila B, 'Efficient enhanced Intrusion identification and response system for MANETs', International Journal of Business Information Systems, vol. 29, no. 4, pp. 535-546, 2018.
[19] Santhosh Babu A. V. and Meenakshi Devi P, 'Gene Populated Spectral Clustering for Energy Efficient Multiple Intrusion Detection and Responsive Mechanism for MANET' Journal of Electrical Engineering, vol. 17, no. 4, pp. 1-13, 2017.
[20] Santhosh Babu A. V., Meenakshi Devi P and Sudhakar K, 'Performance Enhancements for Pre-emptive Ad- Hoc On-demand Multipath Distance Vector Routing', International Journal of Latest Research in Engineering and Computing, vol. 1, no. 1, pp. 21-25, 2013.
[21] Santhosh Babu A. V, Meenakshi Devi P and Sharmila B, 'Comparative Study of MANET Routing Protocols', Asian Journal of Research in Social Sciences and Humanities, vol. 6, no. 6, pp. 1924-1934, 2016.