Performance Improvement of Threshold based Audio Steganography using Parallel Computation

Muhammad Shoaib
Information Technology Department,
Hazara University,
Mansehra, Pakistan

Danish Shehzad
Computer Engineering Department,
Kadir Has University,
Istanbul, Turkey

Arif Iqbal Umar
Information Technology Department,
Hazara University,
Mansehra, Pakistan

Zakir Khan
Information Technology Department,
Hazara University,
Mansehra, Pakistan

Tamer Dag
Computer Engineering Department,
Kadir Has University,
Istanbul, Turkey

Noor Ul Amin
Information Technology Department,
Hazara University,
Mansehra, Pakistan

***Abstract*—Audio steganography is used to hide secret information inside audio signal for the secure and reliable transfer of information. Various steganography techniques have been proposed and implemented to ensure adequate security level. The existing techniques either focus on the payload or security, but none of them has ensured both security and payload at same time. Data Dependency in existing solution was reluctant for the execution of steganography mechanism serially. The audio data and secret data pre-processing were done and existing techniques were experimentally tested in Matlab that ensured the existence of problem in efficient execution. The efficient least significant bit steganography scheme removed the pipelining hazard and calculated Steganography parallel on distributed memory systems. This scheme ensures security, focuses on payload along with provisioning of efficient solution. The result depicts that it not only ensures adequate security level but also provides better and efficient solution.**

Keywords—Steganography; LSB; Steganalysis; Parallel; Pipelining; Processing Efficient; Real time; Security

I. Introduction

The brisk advancement in internet technology and digital information revolutionized the overall technology and information communication. Easy to use and cheap software have enabled major portion of society to get addicted to these communication systems where they can create, manage and exchange multimedia data. Specifically broadband Internet has facilitated transmission of data at much faster and cheaper rate thus helps people to create and share large amount of audio/ video files [1]. These information sharing requires security of private information on internet as it is shared by billions of users. The provisioning of security over internet is most challenging research area as sending and receiving sensitive data through unsecured internet is very critical. There are three main techniques that are being used for information security and are known as encryption, steganography and watermarking [2].

Steganography hides secret information inside another wrapper that may be text, audio, video and protocol. Steganography originated from steganos meaning covered and graphi means writing. Steganography is that branch of information security which deals with embedding secret information inside cover on sender side and retrieving it back on receiver. The purpose of steganography may be personal information sharing, private communication or preventing resources from piracy. Stego-message is amalgamation of cover and host message, where message that is hiding information i.e. user's message is called host message [3].

Audio steganography is type of steganography in which secret information is hidden inside audio signal and audio is modified in imperceptible manner. An overall audio steganography system can have following components.

- Message to be sent
- Cover audio signal
- Encoding technique/algorithm
- Stego signal : Audio combined with secret information is known as
- Decoding technique/algorithm

The steganography allows only communicating parties to see inside that what is being transferred and hides this fact from any other party on the same communication channel [4]. Audio steganography can be divided into four key types, where each of these types is beneficial and vary in implementation mechanisms. Though all techniques are significant and have their own beneficial areas.

A. Least Significant Bit Encoding

In order to encode binary information, least significant bit of each audio frame is modified and information is embedded inside it. This technique is simple and has many advantages as high payload in audio but in contrast has low security. File compressions, conversion or other necessary changes can modify and contaminate hidden information [5].

B. Echo Hiding

This mechanism deceives the perception by modifying frames by adding various kinds of sub-perceptible echoes. Three main parameters of the audio frame are varied which are amplitude of signal, its decay rate and offset as delay. Each parameter is adjusted below human audible threshold so that echo cannot be detected and resolved normally. The offset is different for encoding the binary message, if one offset value represents one the other is representing binary zero. If single information is to be produced from audio signal, single bit information can be encoded only. So, this mechanism audio signal is separated into blocks before encoding, modified and then concatenated to produce the final audio signal [6]. The main drawback of this technique is its low capacity as it is computationally heavy and complex to add echo for each bit.

C. Phase Coding

Phase coding allows replacement of phase components from original audio signal for hiding information inside replaced components. The new amplitude in will not be audible to human. Thus, it results in non-audible encoding of signal to perceived noise ratio (SPNR) resulting in hiding secret message inside audio signal, which cannot be detected by steganalysis based on SPNR [7]. This technique allows controlled phase modifications host in audio to carry secret information.

D. Spread Spectrum

This method allows spreading of secret information in the spectrum inside audio signal using code which is autonomous to that of actual signal. There are two main types of SS for audio steganography: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). In DSSS, the secret message is spread across the spectrum by constant known as chip rate, and then it is modulated with signal and then interleaved with host signal. In FHSS the frequency of spectrum is modified to allow it to hop briskly between frequencies and allowing fast wrapping of information [6]. The limitation of this method is it introduces distortion to the original audio signal.

The paper is arranged in sections where Section II elaborates the existing work and explains limitations of the existing techniques. In Section III proposed solution is explained with description of encoding and decoding process. Section IV gives the experimental results and comparison that shows the efficiency of the proposed solution. Section V concluded the work.

II. Literature Review

Least significant bit steganography ensures that binary digits are embedded in LSBs in cover file. Various LSB techniques have been developed for ensuring security [9]. GIF based image LSB is explained in [10].Two bits of cover page pixels help to store one bit message in LSB based on Difference Expansion [11]. Hiding behind corners LSB and edge based LSB are important methods adopted in LSB Steganography [6]. LSB steganography has several important methods that are currently used for hiding data.

A. Parity Coding

In this method parity bits are used for embedding data. Complete signal is broken down into separate small samples. If bit to be encoded does not match with sample's parity bit then flip LSB of sample [12].

B. XORing Method

XORing method performs XOR operation on LSBs and the message bit and the result of XOR decides whether to modify or to keep LSB unchanged. This approach increases capacity of cover by 8 times and provides comparatively robust encryption [12].

C. Bit Selection

Varying bits are selected inside each sample to hide secret information. The first two MSBs are used for selection of bits from sample to hide secret data and first three LSBs are used for embedding data. If the first two MSBs are 00 then third bit is used for same purpose. This mechanism confuses the intruder and do not allow to obtain secret information [13].

D. Sample Selection

Specified samples from signal are used for data hiding purpose. Here randomness is achieved by the control of 1st three MSBs. If the current sample is i, last column shows next sample containing hidden bit. The space between two consecutive hidden bits in sample is one more than decimal value of 1st three MSBs [14].

E. Lowest Bit Coding

This method embeds the data using least significant bit. Both wave data and secret information to be sent are in binary form, low bit of wave is replaced with bit by bit of message [7]. This method gives capacity benefit of 12.5% and minimizes the transition.

F. Variable Low Bit Coding

This method increases embedding capacity as it introduced advancement in lowest bit coding. Two thresholds are defined like 1 and 2 so that bits information can be embedded between these ranges. If the range of amplitude is less than 1 then data is not embedded. If the range of amplitude is between threshold values, one bit is used for embedding data and if amplitude range is greater than 2 then data is embedded using 2 bits [7].

G. Average Amplitude Method

Average amplitude data of audio in surrounding is used as threshold value. The average is calculated for 10 audio data and after 5 audio data other than own audio data [7]. If level of amplitude is greater than threshold, then 2 bits are used for embedding in any other case bits are not used and number of embedding bits are limited to 2.

III. Proposed Solution

In this work a novel method is proposed to reduce the processing time of the steganography, and improve the efficiency of the process. There are two basic steps to improve the efficiency, which are:

1) Divide the cover signal into sub signals according to the number of cores of processer.

2) Mack each sample embedding and extraction process independent from other samples.

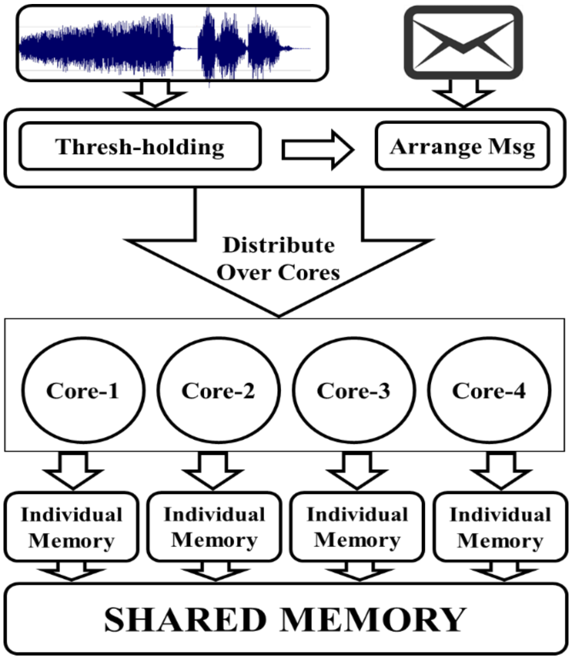

Fig. 1. Distribution of signal over multiple processer cores

In this way the advantage of parallelism and pipelining is achieved as well, which improve the efficiency as compared to all existing techniques. The encoding and decoding process is explained as follows:

A. Encoding Process

The encoding process starts with reading host audio signal then original audio signal is quantized and the samples are converted into discrete form. The formula used for quantization is as follows:

$$\text{Quantized Audio} = \text{Amplitude} \times \left(2^{\text{No\_of\_Bits}-1}\right)$$

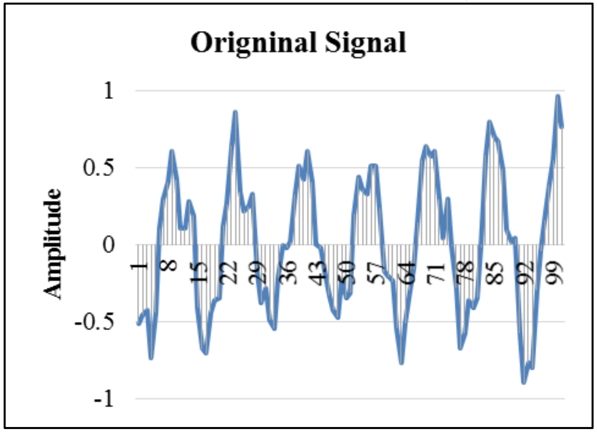

Fig. 2. Original Audio Signal Amplitude

When the numbers of bits in a sample are equal to 16 then quantized value can be calculated as:

$$Quantized\ Audio = Amplitude \times (2^{16-1})$$

$$Quantized\ Audio = Amplitude \times 32768$$

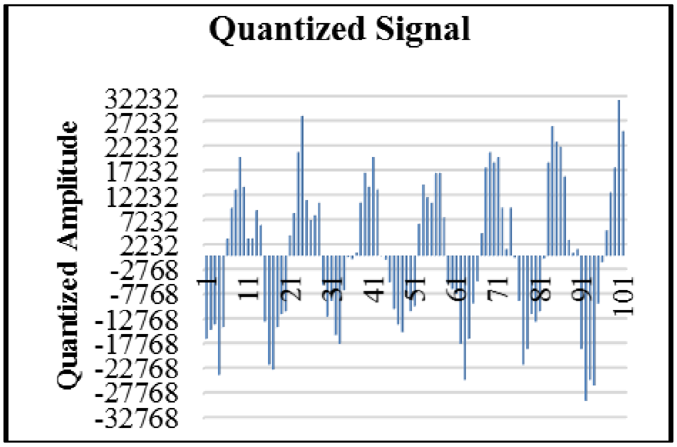

Fig. 3. Quantized Signal Discrete Values

TABLE I. THRESHOLDS FOR 1 TO 8 BITS STEGANOGRAPHY

S. No	Lower Bound	Upper Bound	Stego Bits
1	0	255	8-Bits
2	256	511	7-Bits
3	512	1023	6-Bits
4	1024	2047	5-Bits
5	2048	4095	4-bits
6	4098	8191	3-Bits
7	8192	16383	2-Bits
8	16384	32768	1-Bit

As shown in table 1. Sample capacity is 8 bits but when sample amplitude is greater than 255 then capacity of sample is calculated by following equation as:

$$Capacity\ of\ Sample = 16 - ceil(\log_2 Sample\_Amplitude)$$

After the quantization of audio signal and getting discrete values, binary empty array is created for bits to be stored inside the audio signal. After that samples are selected according to Threshold values. If the values lie within threshold limit further process of Steganography is followed. LSB data according to threshold is selected and converted into binary and is appended in binary array string. When the process is complete binary data is written to file for sending it under cover to the destination.

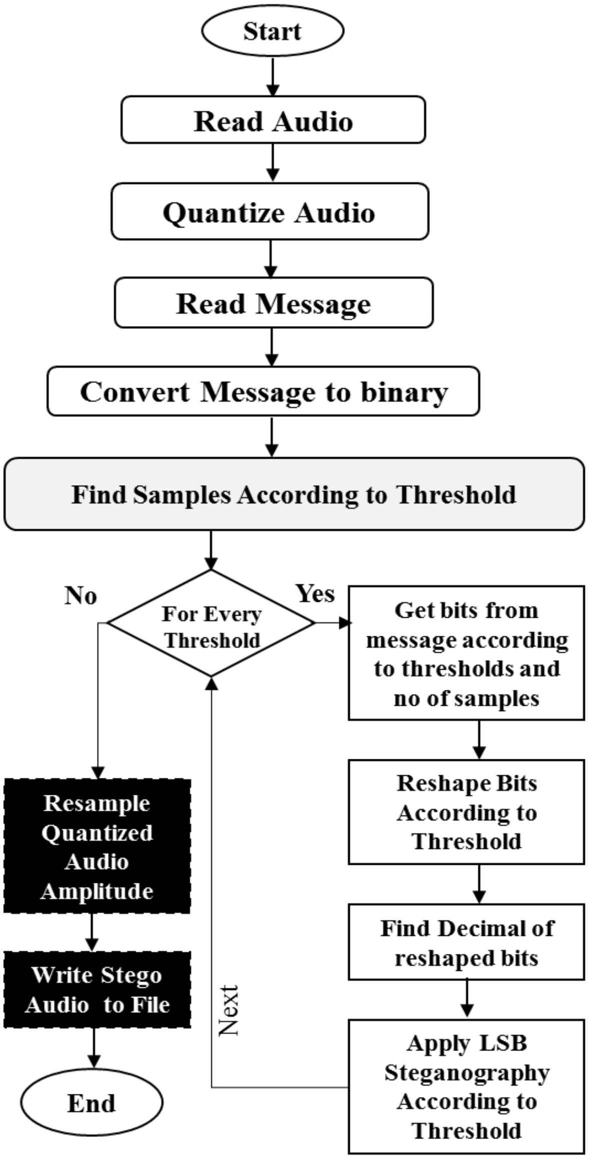
Start
Read Audio
Quantize Audio
Read Message
Convert Message to binary
Find Samples According to Threshold
No
For Every Threshold
Yes
Get bits from message according to thresholds and no of samples
Reshape Bits According to Threshold
Find Decimal of reshaped bits
Apply LSB Steganography According to Threshold
Next
Resample Quantized Audio Amplitude
Write Stego Audio to File
End

Fig. 4. Encoding Process

B. Decoding Process

On receiver side the received audio signal is quantized again using the same process as shown above. An empty array for storage is created for retrieving hidden data storage. After quantization for each threshold least significant bit is obtained and data is uncovered that was hidden during encoding process. After the parallel unfolding of data as shown in Fig4, through various thresholds, complete data is retrieved at destination.

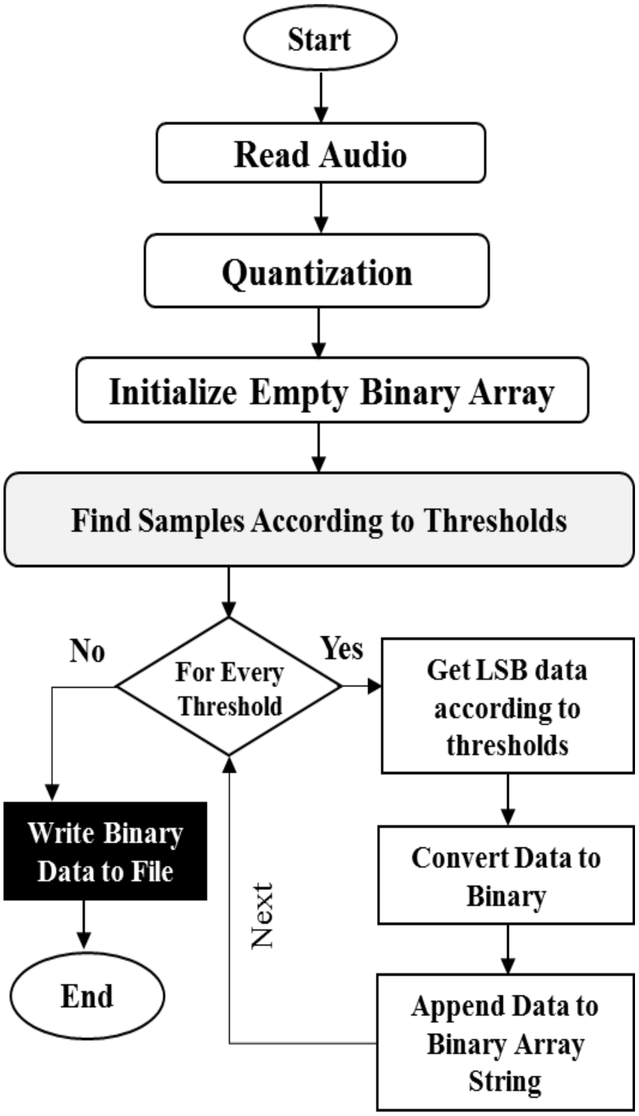
Start
Read Audio
Quantization
Initialize Empty Binary Array
Find Samples According to Thresholds
No
For Every Threshold
Yes
Get LSB data according to thresholds
Convert Data to Binary
Append Data to Binary Array String
Next
Write Binary Data to File
End

Fig. 5. Decoding Process

IV. Experimental Results

The experiments were conducted in Matlab 2015 on Intel core i5 with 4 cores and using 8 GB RAM for computing the efficiency of the proposed parallel scheme, and the results were compared with existing Hakeem. et al scheme. Results depicts that the proposed scheme is much efficient than existing scheme. The exiting scheme was calculating threshold for each sample, then hiding the data but serially according to threshold was consuming most of the time. This scheme parallelize it by finding threshold, then arranging samples according to threshold and parallel on multiprocessing systems hiding data through steganography.

TABLE II. PROPOSED SCHEME VS. HAKEEM. ET. AL AUDIO STEGANOGRAPHY EFFICIENCY COMPARISON

Sound	Hakeem	Proposed	Total Efficiency	Efficiency Per Sec
Chirp	110.255	0.889	123.963	77.346
Gong	372.828	0.903	412.977	80.496
Handel	579.918	1.093	530.370	59.426
Laughter	429.817	0.900	477.734	74.356
Splat	85.708	0.871	98.431	80.629
Train	110.889	0.822	134.859	85.772

Table 2 shows that as compared to existing Hakeem. et.al scheme when experiments conducted on different sounds, the proposed scheme is much more times efficient than existing scheme.

V. CONCLUSION

Audio steganography is used to send secret information inside the cover of audio signal for secure transmission. There are various schemes ensuring adequate and efficient security, but due to serial dependency efficiency of existing schemes were causing the computational overhead. The proposed scheme enhanced the existing scheme by eliminating the serial dependency and running the steganography calculations on parallel machines in efficient manner. The result shows that it not only ensures adequate security level but also provides much better and efficient solution.

REFERENCES

[1] J. Johnston and K. Brandenburg, 1992, *"Wideband Coding Perceptual Consideration for Speech and Music"*. Advances in Speech Signal Processing, S. Furoi and M. Sondhi, Eds. New York: Marcel Dekker.

[2] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, *"Techniques for data hiding",* IBM Systems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.

[3] Robert Krenn, *"Steganography and steganalysis*", An Article, January 2004.

[4] F.A.P.Petitcolas, R.J.Anderson, G.Kuhn: *"Information Hiding- a Survey",* Process of IEEE, vol.87, no.7, pp.1062-1078, July, 1999.

[5] P.K.Singh, R.K.Aggrawal, 2010*,"Enhancement of LSB based Steganography for Hiding Image in Audio"*, International Journal on Computer Science and Engineering, Vol. 02, No. 05.

[6] F.Djebbar, B.Ayady, H.K.Abed Meraimx, 2011*,"A view on latest audio steganography techniques",* International Conference on Innovations in Information Technology.

[7] P.Dutta1, D.Bhattacharyya, and T.Kim, June 2009" *Data Hiding in Audio Signal: A Review",* International Journal of Database Theory and Application,Vol. 2.

[8] F.Djebbar, B.Ayady, H.K.Abed Meraimx, 2011*," A view on latest audio steganography techniques"*, International Conference on Innovations in Information Technology.

[9] Thomas, P. "*Literature survey on modern image steganographic techniques*". In International Journal of Engineering Research and Technology. 2013. ESRSA Publications.

[10] Bender, W., et al., *Techniques for data hiding.* IBM systems journal, 1996. **35**(3.4): p. 313-336.

[11] Tian, J., *Reversible data embedding using a difference expansion.* IEEE Trans. Circuits Syst. Video Techn, 2003. **13**(8): p. 890-896.

[12] H.B.Kekre, A.Athawale, S.Rao, U.Athawale, October 2010" *Information Hiding in Audio Signals",* International Journal of Computer
Applications, (0975 – 8887) Volume 7– No.9.

[13] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, October 2010, *Information Hiding in Audio Signals,* International Journal of Computer Applications (0975 – 8887) Volume 7– No.9.

[14] M.Asad, J.Gilani, A.Khalid, 2011," *An Enhanced Least Significant Bit Modification Technique for Audio Steganography"*, IEEE978-1-61284-941-6/111.

[15] Hakeem, N. Amin, M. Shah, Z.Khan & A.Qadir, *"Threshold Based LSB Audio Steganography",* Int'l Conf. on Chemical Engineering & Advanced Computational Technologies, 2014. South Africa.