International Journal of Engineering & Technology, 7 (3.28) (2018) 334-336

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Information Hiding Based on Audio Steganography using Least Significant Bit

Fatma Susilawati Mohamad*, Nurul Sahira Mohd Yasin, Musab Iqtait

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Terengganu, Malaysia
**Corresponding author E-mail: fatma@unisza.edu.my*

Abstract

Steganography refers to the concept of disguise special or delicate information or data inside something that shows up with be nothing out of the normal. A few problems arise especially in securing data and information when the information had been lost or stolen from unauthorized user. Traditionally, we give information manually using paper; it is possible that the information could be stolen by unauthorized user. The main objective of this study is to hide secret information in audio, in this way that different persons won't perceive the vicinity of the majority of the data. The proposed method of this study is by using Least Significant Bit (LSB) algorithm to design an audio steganography. In the recommended method, every sound test is changed over bits and then the text information is installed. The expected result of this study will produce a steganography audio that will be able to hide data or information efficiently from unauthorized user, also to ensure the safety of the information in an authorized hand.

Keywords: *Steganography; Audio Steganography; LSB Algorithm.*

1. Introduction

Information security is one of the most challenging problems in today's technological world. In this paper we proposed a technique to disguise the vicinity of mystery message which is called steganography. It is likewise known as "covered writing" Since it utilize a "cover" of a message for posting any essential mystery message. Steganography render as an implies for special, safe and occasionally pernicious correspondence. Steganography will be the symbolization on shroud the altogether vicinity from claiming correspondence toward embedding those mystery message under those harmless searching disguise networking protests, for example, pictures utilizing those human's visual, aural excess alternately networking objects statistical excess. Steganography is a capable device which builds security previously, information transferring and archiving. In the steganographic scenario, those mystery information will be initially disguised inside an additional object which will be known as "cover object", to structure "stego object" after that this new object can a chance to be transmitted or spared. Embedding mystery messages under advanced audio will be known as sound Steganography. In this project, the stegoaudio will be saved in format audio.wav only.

For any steganography technique to be implemented, it must satisfy three condition:

- Capacity means the quantity from mystery data could include inside the host message.
- Transparency evaluates how well a secret information is embedded in the cover audio.
- Robustness measures the ability of secret information to withstand against attacks.

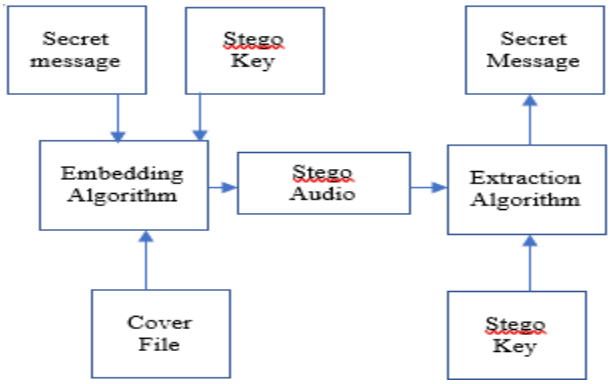


Fig. 1: Block Diagram of Steganography

2. Literature Review

In [12] proposed a method to determining the issue identified with those substitution method about sound steganography. For intimal scale of safety, they utilize RSA algorithm to scramble message, in the following scale, encrypted message will be encoded over on sound information for this they utilized hereditary algorithm rely on substitution system. The fundamental thought behind this work may be with improving the security also heartiness.

- Advantages: The hypothesis of strategy is that basically replant whichever a bit or a few bits in over every test won't be observable of the human eye or ear relying upon the kind about document.
- Disadvantages: the principle issues from claiming sound substitution steganography strategy are respectably low heartiness. There are two sorts of strike to steganography furthermore in this way there would two sorts from claiming hearti-

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ness. You quit offering on that one sort of strike tries to uncover the unobserved message also an alternate sort tries to wreck those unobserved message.

In [2] this algorithm, the duel encryption methodology was implemented. In the initially scale about encryption, a pattern matching algorithm need been utilized to scramble those version message As far as their positional worth. To second scale, the accepted LSB algorithm need been utilized to implant those positional quality in the disguise document. Such A duel encryption strategy will guarantee information security in an effective way.

- Advantages: Permits an expansive volume from claiming information provided for sound or content format to be encoded also information are found in the getting limit over loss-less format..
- Disadvantages: It is easy for the invaders to identify and destroy the information.

In [13] suggested a new methodology for hiding information. The Suggested method will be an amalgamation about quick encryption, sound steganography also sound encryption. In the primary scale, the unique content message will be encrypted utilizing altered Vigenère cipher approach. Those cipher content gets installed under the spread sound utilizing LSB encoding in the next scale. Further, that sound record may be then subjected on transposition making utilization of Blum Shub pseudo arbitrary number generator.

- Advantages: this Blending from claiming cryptography steganography ensures that regardless of the sound record will be intercepted eventually via perusing an unauthorized individual; those representatives don't find those mystery data.
- Disadvantages: That Sound will be encrypted just utilizing transposition.

The authors suggest more secure encryption methods with a chance to be used to content encryption, so that data is not easily stolen by an unauthorized party.
In [11] a review of two simple systems should get a thought of how steganography on sound document meets expectations. LSB adjustment and period encoding system would precise primitive on steganography. A successful sound steganographic plan ought to further bolstering have the next three traits: indiscernibleness from claiming distortion, information rate and heartiness. These aspects are known as the enchantment triangle to information secretion.

- Advantages: this strategy may be simple with implement, be that may be extremely defenseless.
- Disadvantages: this algorithm can be utilized at best a little measure for information needs with make disguised.

In [8, 10] Functioned for content similarly as those disguise medium with the point from claiming expanding heartiness and limit off hidden information. Elitism might have been utilized for that wellness work. Pertinent for content files mainly

- Advantages: this methodology works, accomplishing powerful optimization, security, also heartiness.
- Disadvantages: pertinent for content files mainly.

3. Proposed Work

Slightest noteworthy bit may be algorithm that replaces those any rate noteworthy bit over a few bytes of the spread record on shroud an arrangement for bytes containing those concealed information. It allows for large amount of data encoded. The expected result of this study will produce a steganography audio that will be able to hide data or information efficiently from unauthorized user also to ensure the safety of the information in an authorized hand. So, with the algorithm and concept of the project, the system can be a one recommender system for user who wants to send the information in more secure way.

4. Methodology

To accomplish that objective, orderly technique is utilize in this research approach. Figure 2 shows the sound steganography operation, which is In view of any rate critical bit adjustment. The stream of the algorithm is provided for similarly as demonstrated over figure 2. It will be demonstrating those diverse steps that will be taken after so as on encode and decode the secret message.

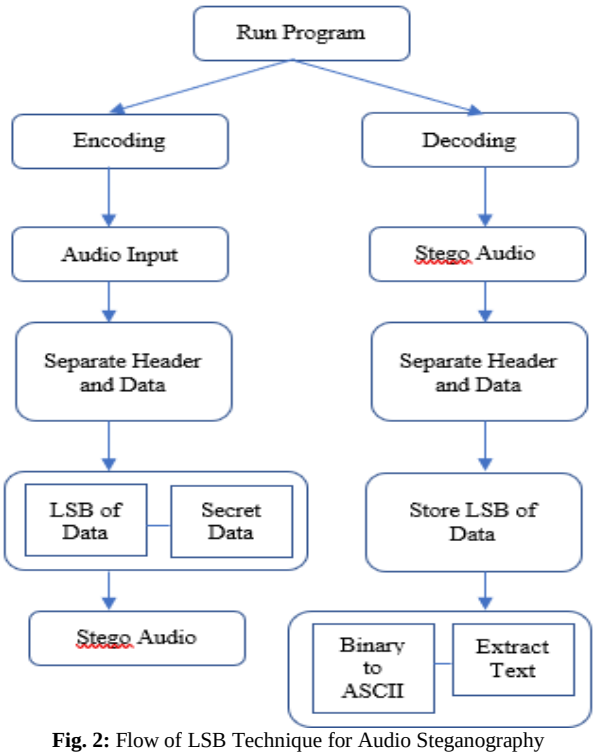


Fig. 2: Flow of LSB Technique for Audio Steganography

4.1. Embedding process (Encoding)

1) Enter audio input
2) Separate the header and data because header in audio file is very sensitive and must not change that
3) Replace the LSB of the data with secret text
4) Finally get stego audio that have secret text

4.2. Extraction Process (Decoding)

1) Receiver receive the stego audio that contain audio and secret data
2) Separate header and the data
3) Store the LSB of the data because LSB contain secret text
4) The LSB will be in binary format, and convert into ASCII format to get the text back

4.3. Least Significant Bit

Least significant bit (LSB) coding will be those simplest manner should implant majority of the data in an advanced sound record. Eventually perusing substituting the slightest important bit of each sampling purpose for a binary message, LSB coding considers an extensive amount about information will make encoded. Over LSB coding, the perfect information transmission rate is 1 kbps for every 1 khz. Over a few usages from claiming LSB coding, however, the two slightest important odds of an example are reinstated for two message bits. These increments the measure of in-

formation that might make encoded, as well as increases the measure about coming about commotion in the sound document. On extract a mystery message from an LSB encoded callous file, those receiver needs entry of the arrangement of example indices utilized within the embedding transform. Normally, that period of the mystery message to a chance to be encoded is more modest over the downright number of specimens done a callous record. Particular case must choose at that point ahead how should pick the subset from claiming tests that will hold numerous the mystery message Furthermore impart that decision of the collector.

4.4. Example

Character to be embedded – "A"
ASCII value of "A": 65
8-bit binary representation of the ASCII value: 01000001
8 consecutive audio frames in binary format (consider 8 bit)
10010010 01010101 10010101 11101010 10000100
11110011 10100000 11010101

Table 1: Embedding Process

Each Bit to be Embedded	8 Consecutive Audio Frames	
	Before Embedding	After Embedding
0	10010010	10010010
1	01010101	01010101
0	10010101	10010100
0	11101010	11101010
0	10000100	10000100
0	11110011	11110010
0	10100001	10100000
1	11010101	11010101

5. Results and Discussion

Those steganography will be a standout amongst those most secure types of information transmissions in this digital world. Over the proposed method, a sound steganography using least significant bit is proposed and tested. It will produce a steganography audio that will be able to hide data or information efficiently from unauthorized user also to ensure the safety of the information in an authorized hand. In conclusion, by using this method, The content might make installed under those cover record also it may be acknowledged in the accepting conclusion without whatever change. So, it will be reasoned that the integument also caliber of the message would great upheld.

6. Conclusion

Future domain about this work is the possibilities about upgrades to sound steganography framework for admiration to different strategy for information concealing in sound. This work basically condensed around best. Wav format for sound files and might stretched out on a level such and such it might be utilized to the different sorts of sound wave document formats like. au. Mp3, wma and so forth throughout this way, Also, noisy sound files might make acknowledged to making correlations about SNR and PSNR then afterward embedding message under the same.

Acknowledgement

Special thanks go to Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin for the support of this work.

References

[1] Kulkarni, S. A., Patil, P. S., & Patil, B. S. (2012). A optimized and secure audio steganography for hiding secret information-review. Journal of Electronics and Communication Engineering, 1, 12-16.

[2] Chowdhury, R., Bhattacharyya, D., Bandyopadhyay, S. K., & Kim, T. H. (2016). A view on LSB based audio steganography. International Journal of Security and Its Applications, 10(2), 51-62.

[3] Adhiya, K. P., & Patil, S. A. (2012). Hiding text in audio using LSB based steganography. Information and Knowledge Management, 2(3), 8-14.

[4] Nehru, G., & Dhar, P. (2012). A detailed look of audio steganography techniques using LSB and genetic algorithm approach. International Journal of Computer Science Issues, 9(1), 402-406.

[5] Rahmani, M. K. I., Arora, K., & Pal, N. (2014). A crypto-steganography: A survey. International Journal of Advanced Computer Science and Application, 5, 149-154.

[6] Kaur, N., & Behal, S. (2014). Audio steganography using LSB edge detection algorithm. Proceedings of the International Conference on Communication, Computing and Systems, pp. 180-183.

[7] Pradhan, K., & Bhoi, C. (2012). Robust audio steganography technique using AES algorithm and MD5 hash. International Journal of Innovative Research in Advanced Engineering, 1(10), 282-287.

[8] Chandrakar, P., Choudhary, M., & Badgaiyan, C. (2013). Enhancement in security of LSB based audio steganography using multiple files. International Journal of Computer Applications, 73(7), 1-4.

[9] Sakthisudhan, K., Prabhu, P., & Thangaraj, P. (2012). Secure audio steganography for hiding secret information. Proceedings of the International Conference on Recent Trends in Computational Methods, Communication and Controls, pp. 33-37.

[10] Chadha, A., & Satam, N. (2013). An efficient method for image and audio steganography using Least Significant Bit (LSB) substitution. International Journal of Computer Applications, 77(13), 37-45.

[11] Bandyopadhyay, S. K. & Banik, B. G. (2012). Multi-level steganographic algorithm for audio steganography using LSB modification and parity encoding technique. International Journal of Emerging Trends and Technology in Computer Science, 1(1), 71-74.

[12] Singh, G., Tiwari, K. & Singh, S. (2014). Audio steganography using RSA algorithm and genetic based substitution method to enhance security. International Journal of Scientific and Engineering Research, 5(5), 703-707.

[13] Sinha, N., Bhowmick, A., & Kishore, B. (2015). Encrypted information hiding using audio steganography and audio cryptography. International Journal of Computer Applications, 112(5), 49-53.