

# Efficient Embedding for Audio Steganography

MAZDAK ZAMANI, AZIZAH BT ABDUL MANAF, SHAHIDAN M. ABDULLAH

Advanced Informatics School  
Universiti Teknologi Malaysia  
54100 Kuala Lumpur  
MALAYSIA

mazdak@utm.my, azizah07@citycampus.utm.my, mshahidan@ic.utm.my

**Abstract:** - Steganography is a form of security technique through obscurity; the science and art of hiding the existence of a message between sender and intended recipient. Steganography has been used to hide secret messages in various types of files, including digital images, audio and video. The three most important parameters for audio steganography are imperceptibility (indicated as PSNR), payload (bit rate or capacity), and robustness. Any technique which tries to improve the payload or robustness should preserve imperceptibility. The noise which is introduced due to bit modification would limit payload. This paper presents three analyses on embedding efficiency in audio steganography that is based on experimental results.

**Key-Words:** - artificial intelligence; multimedia security; digital data hiding; steganography; watermarking

## 1 Introduction

Steganography and watermarking techniques embed information in a digital media in a transparent manner. Steganography is a technique for covert information, but digital watermarking may not hide the existence of the message from third persons [1-5].

Watermarking usually requires robustness to withstand against attacks intended to remove or destroy the hidden message from the watermarked media as well as preserving the carrier signal quality. This makes digital watermarking appropriate for those applications where the knowledge of a hidden message leads to a potential danger of manipulation [6-13].

The most well-known examples of steganography go back to ancient times when Histiaus shaved his slave's head, and then he tattooed a message on his scalp. After that his hair had re-grown the tattooed message was disappeared. He was going to call his men to attack to the Persians [14-22].

Steganography is the study of methods for hiding the existence of secondary information in the presence of primary information in a way which neither affects on the size nor results in perceptual distortion. The secondary information is referred to as hidden message, hidden file or hidden information while primary information is referred to as carrier, host or original signal, before embedding and stego signal, file, bit stream or sequence, after embedding [23-30].

Watermarking techniques are principally context-specific, that means, the algorithms must be designed regarding the media type of the data to be watermarked. Therefore, watermarking indicates a specific application of steganographic techniques. Specifically, the additional requirement for robustness of digital watermarks against attacks or manipulations during the data processing entails a lower payload of the watermarking methods compared to steganographic algorithms [31-38].

## 2 Listening Test to Determine the Threshold of Noise Perception

To determine the threshold of noise perception a listening test was performed. 20 musicians and music fans that were familiar of the nature of a noise were conducted in the listening test. The result is shown in the Table 1.

To perform the listening test, professional equipment were provided which consisted of professional headset and professional speaker. Listening test were conducted in an acoustically isolated room. The listeners were asked to tag the audio samples if any noise or difference with the original audios was experienced.

Obviously, the noise perception in 1 bps and 2 bps is negligible and can be considered as imperceptible. On other hand, the noise is quite perceptible in 6 bps and 8 bps. Noise perception in 6 and 8 bps rates is very high and even by improvement will maintain perceptible.

Nevertheless, noise perception in 4 bps rate is neither negligible (similar to 1 and 2 bps) which can be ignored, nor that high (similar to 6 and 8 bps) which is far from getting imperceptible. Thus, 4 bps is selected as the threshold of noise perception in audio steganography. Also the result is illustrated in Figure 1.

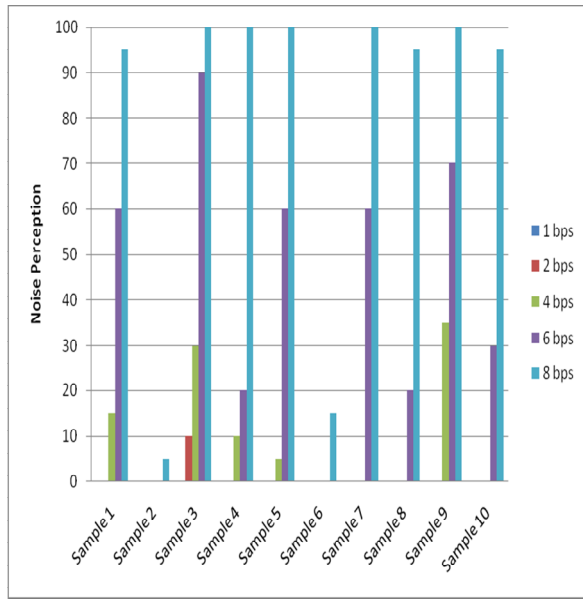


Figure 1. The result of listening test

TABLE 1. THE RESULT OF LISTENING TEST

Sample No.	No. 1	No. 2	No. 3	No. 4	No. 5	No. 6	No. 7	No. 8	No. 9	No. 10	Average Detection %
1 bps	0	0	0	0	0	0	0	0	0	0	0
2 bps	0	0	10	0	0	0	0	0	0	0	1
4 bps	15	0	30	10	5	0	0	0	35	0	9.5
6 bps	60	0	90	20	60	0	60	20	70	30	41
8 bps	95	5	100	100	100	15	100	95	100	95	80.5

### 3 Suitability of Messages Type

To compare the result of categorized type of message in an academic way, a message file which is Help File and has 10790 KB was selected. To compare the result, two Text file with the same size were made and tested these 3 message files on 15 deferent host file.

As Figure 2 shows, not only between two different types of file, but also between two different file with the same type, no rule or regulation that shows this depends on the message file type was observed.

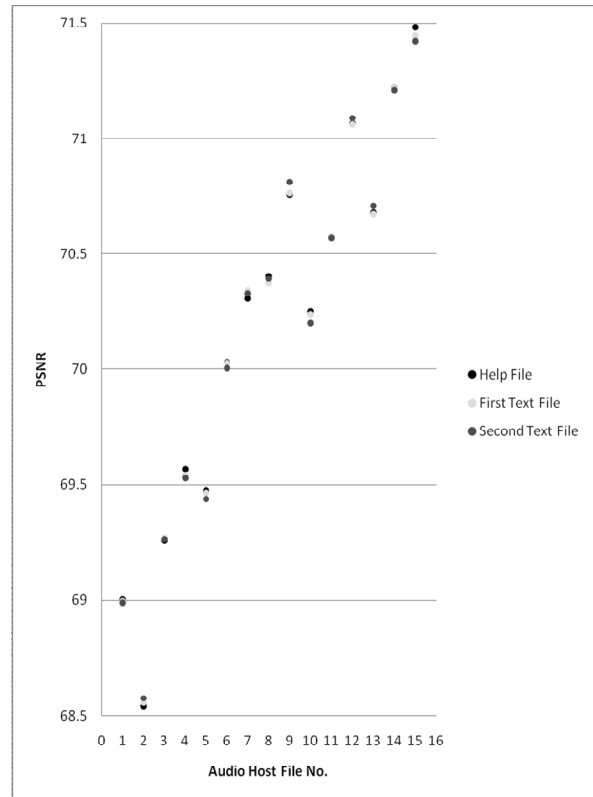


Figure 2. Influence of the types of messages on embedding quality

TABLE 2. INFLUENCE OF THE TYPES OF MESSAGES ON EMBEDDING QUALITY

Sample No	Message Size	Host Size	Host to Message Ratio	PSNR		
				Help File	First Text File	Second Text File
1	10790	119384	11.06	69.00	69.00	68.99
2	10790	129580	12.01	68.54	68.55	68.57
3	10790	154924	14.36	69.26	69.27	69.26
4	10790	159276	14.76	69.57	69.54	69.53
5	10790	171564	15.90	69.48	69.47	69.44
6	10790	178220	16.52	70.03	70.03	70.00
7	10790	179500	16.64	70.31	70.34	70.33
8	10790	179704	16.65	70.41	70.38	70.39
9	10790	190208	17.63	70.76	70.76	70.81
10	10790	191788	17.77	70.25	70.24	70.20
11	10790	198956	18.44	70.57	70.58	70.57
12	10790	207148	19.20	71.07	71.06	71.09
13	10790	214828	19.91	70.68	70.67	70.71
14	10790	227372	21.07	71.22	71.22	71.21
15	10790	239916	22.24	71.48	71.45	71.42

As Table 2 shows, for some hosts the first text file has the least PSNR, for some others the greatest PSNR. Somewhere the second text file has the least PSNR, Somewhere the greatest PSNR. And in some rows the help file has the least PSNR, and for some other rows it has the greatest PSNR.

As a result it can be concluded that the type of message files is not a factor in PSNR. This is due to the fact which the type and content of files are not important in substitution techniques. Substitution techniques work on bits, so bit stream is the only important thing, neither file type nor the content.

#### 4 An Analysis on Bit per Sample

Regarding the size of message, and the ratio between message size and host size, the host size must be large enough that the message can be embedded into. In other word, the size of host and the size of message are related to each other. For example, if the size of message is 20% of the host size, 1 bps, 2 bps and 3 bps cannot be used because their maximum payload are correspondingly 6.25%, 12.5%, and 18.75%, but 4 bps whose nominal payload is 25% and above can be used.

In addition to the result of embedding by ordinary substitution audio steganography, the results of GSBAS (a novel Genetic Substitution Based Audio Steganography that is implemented in this research) are given in the columns of Table 3.

TABLE 3. THE BEST PAYLOAD WHEN ALL PAYLOADS ARE POSSIBLE

WAV Size (bytes)	Message Size (Byte) 1bps	PSNR 1bps	PSNR 2bps by GSBAS	PSNR 2bps	PSNR 3bps by GSBAS	PSNR 3bps	PSNR 4bps by GSBAS	PSNR 4bps	PSNR 6bps	PSNR 8bps
837300	51261	72.03	70.25	67.95	66.29	63.54	61.47	58.69	48.36	37.66
35453998	2205801	72.39	70.58	68.30	66.61	63.78	61.79	58.91	48.62	37.79

Sometimes a small message can be embedded into a host by any bit rate per sample. Since the amount of embedded message for either of bit per sample rates is the same, PSNR should be the main criteria. To answer which bit per sample rates is

better, the same message and the same host with different algorithms were tested.

#### 5 Conclusion

As Figure 3 shows, in the same situation, embedding of fewer bits into more samples causes better PSNR rather than embedding more bits into fewer samples.

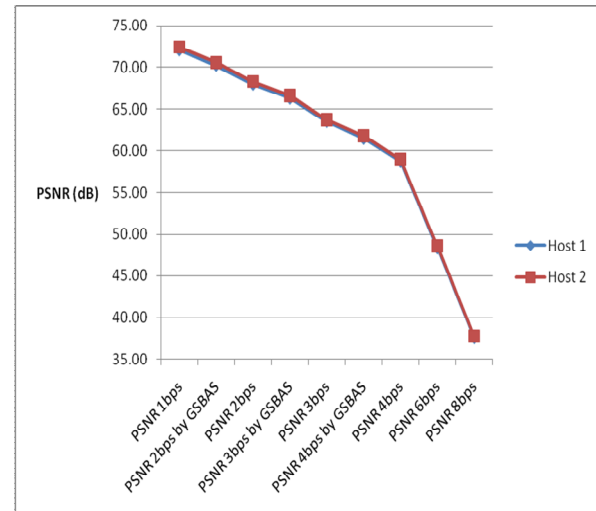


Figure 3. The best payload when all payloads are possible

#### Acknowledgment

This work is part of research done at the Universiti Teknologi Malaysia, with support from the Ministry of Higher Education, Malaysia.

#### References:

- [1] Abduljabbar Shaamala, Shahidan M. Abdullah and Azizah A. Manaf, Study of the effect DCT and DWT domains on the imperceptibility and robustness of Genetic watermarking, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011
- [2] Abduljabbar Shaamala, Shahidan M. Abdullah and Azizah A. Manaf, The Effect of DCT and DWT Domains on the Robustness of Genetic Watermarking ICIEIS 2011, Part I, CCIS 251, pp. 310–318, 2011, Springer.
- [3] Akram M. Zeki, Azizah A. Manaf, and Mazdak Zamani. Bit-Plane Model: Theory and Implementation. Engineering Conference 2010 (EnCon2010). 14-16 April 2010. Kuching, Sarawak, Malaysia.

- [4] Mazdak Zamani, Azizah Abdul Manaf, Rabiah Ahmad, Farhang Jaryani, Hamed Taherdoost, Saman Shojae Chaeikar, H. Rouhani "A Novel Approach for Genetic Audio Watermarking". *Journal of Information Assurance and Security* 5 (2010). Pages 102-111.
- [5] Mazdak Zamani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, Saman Shojae Chaeikar and Hossein Rouhani Zeidanloo. "Genetic Audio Watermarking". *International Conference on Recent Trends in Business Administration and Information Processing*. March 26-27, 2010. Trivandrum, Kerala, India.
- [6] Mazdak Zamani, Hamed Taherdoost, Azizah A. Manaf, Rabiah B. Ahmad, and Akram M. Zeki. "An Artificial-Intelligence-Based Approach for Audio Steganography". *MASJUM Journal of Open Problems in Science and Engineering (MJOPSE)*. Volume: 1 Issue: 1 Month: October 2009. Pages 64-68.
- [7] Mazdak Zamani, Azizah Abdul Manaf, Rabiah Ahmad, Farhang Jaryani, Hamed Taherdoost, Saman Shojae Chaeikar, and Hossein Rouhani Zeidanloo. "Genetic Audio Steganography". *International Journal on Recent Trends in Engineering & Technology [IJRTET]*, Volume 3, Issue 2, 2010. Pages 89-91.
- [8] Awodele Oludele. *Artificial Intelligence and Security*. *International Journal of Computational Intelligence and Information Security* Vo. 1 No. 3, May 2010.
- [9] Muhammad Asad, Junaid Gilani, Adnan Khalid. An Enhanced Least Significant Bit Modification Technique for Audio Steganography. 2011 International Conference on Computer Networks and Information Technology (ICCNIT). Abbottabad. 11-13 July 2011. 143 – 147.
- [10] Mazdak Zamani, Azizah Abdul Manaf, Hossein Rouhani Zeidanloo, and Saman Shojae Chaeikar. "Genetic Substitution-Based Audio Steganography for High-Capacity Applications". *International Journal for Internet Technology and Secured Transactions*. Pages 97-110. Volume 3 Issue 1, April 2011. Inderscience Publishers, Geneva, Switzerland.
- [11] Shahidan M. Abdullah, Azizah A. Manaf, and Mazdak Zamani. Recursive Reversible Image Watermarking Using Enhancement of Difference Expansion Techniques. *Journal of Information Security Research*. Volume 1 Number 2. June 2010. Pages 64-70.
- [12] Akram M. Zeki, Azizah A. Manaf, Adamu A. Ibrahim and Mazdak Zamani. A Robust Watermark Embedding in Smooth Areas. *Research Journal of Information Technology*. Year: 2011. Volume: 3. Issue: 2. Page No.: 123-131.
- [13] Mazdak Zamani, Azizah Abdul Manaf, and Rabiah Ahmad. "Knots of Substitution Techniques of Audio Steganography". *The 2009 International Conference on Telecom Technology and Applications*. Pages 415-419. June 6-8, 2009. Manila, Philippines.
- [14] Mazdak Zamani, Azizah Abdul Manaf, and Rabiah Ahmad. "Current Problems of Substitution Techniques of Audio Steganography". *The 2009 International Conference on Artificial Intelligence and Pattern Recognition*. Pages 154-160. 13-16 July 2009. Orlando, Florida, USA.
- [15] Asha Vijayan, Amrita Vishwa Vidyapeetham. A Genetic Algorithm Approach for Audio Steganography. *Computer Science Journals*.
- [16] R. Darsana and Asha Vijayan. Audio Steganography Using Modified LSB and PVD. *Trends in Network And Communications. Communications in Computer and Information Science*, 2011, Volume 197, Part 1, 11-20.
- [17] Mazdak Zamani, Azizah Abdul Manaf, Rabiah Ahmad, Akram Zeki, and Shahidan Abdullah. "Genetic Algorithm as an Approach to Resolve the Problems of Substitution Techniques of Audio Steganography". *The 2009 International Conference on Genetic and Evolutionary Methods*. 13-16 July 2009. Pages 170-175. Las Vegas, Nevada, USA.
- [18] Wasan Shaker Awad and Huda Kadim Al Jobori. Non-Homogeneous Steganography Using Genetic Simulated Annealing. *International Journal of Information Science and Computer Mathematics*. Volume 2, Issue 1, Pages 61 - 73 (August 2010).
- [19] Zanganeh, O. & Ibrahim, S. 2010, "Image steganography based on adaptive optimal embedding". *5th International Conference on Computer Sciences and Convergence Information Technology, ICCIT 2010*. 2010, Article number 5711125, Pages 600-605.
- [20] Mazdak Zamani, and Azizah Abdul Manaf. "Azizah's Formula to Measure the Efficiency of Steganography Techniques". *2nd International Conference on Information and Multimedia Technology (ICIMT 2010)*. December 28-30, 2010. Hong Kong, China.
- [21] Mazdak Zamani, and Azizah Abdul Manaf. "Mazdak's Method to Estimate the PSNR of Audio Steganography Techniques". *International Conference on Computer and*

- Computational Intelligence (ICCCI 2010). December 25-26, 2010. Nanning, China.
- [22] H. B. Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale. Information Hiding in Audio Signals. International Journal of Computer Applications. Number 9 - Article 4. Year of Publication: 2010.
- [23] Anguraj S., Dr. Shantharajah S.P., Arul Murugan R., Balaji E., Maneesh R., Prasath S. A Fusion of A-B MAP Cipher and ASET Algorithms for the Enhanced Security and Robustness in Audio Steganography. IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011. MIT, Anna University, Chennai. June 3-5, 2011.
- [24] Mazdak Zamani, Azizah Abdul Manaf, Rabiah Ahmad, Akram Zeki, and Shahidan Abdullah. "A Genetic-Algorithm-Based Approach for Audio Steganography". International Conference on Communities and Communications. World Academy of Science, Engineering and Technology 54 2009. Pages: 359-363. 24-26 June 2009. Paris, France.
- [25] Tewari, T.K., Saxena, V. & Gupta, J.P. 2011, "Audio watermarking: Current state of art and future objectives", International Journal of Digital Content Technology and its Applications, vol. 5, no. 7, pp. 306-314.
- [26] Mayank Srivastava, Mohd Qasim Rafiq. A Novel Approach to Secure Communication Using Audio Steganography. Advanced Materials Research Vols. 403-408 (2012) pp 963-969. November, 2011.
- [27] Mazdak Zamani, Azizah Abdul Manaf, Rabiah Ahmad, and Akram Zeki. "An Approach to Improve the Robustness of Substitution Techniques of Audio Steganography". 2nd IEEE International Conference on Computer Science and Information Technology 2009. Volume 2. Pages 5-9. 8 - 11 August 2009. Beijing, China.
- [28] R. Darsana and Asha Vijayan. Audio Steganography Using Modified LSB and PVD. Trends in Network and Communications. Communications in Computer and Information Science, 2011, Volume 197, Part 1, 11-20.
- [29] Mazdak Zamani, Hamed Taherdoost, Azizah Abdul Manaf, Rabiah Ahmad, and Akram Zeki. "Robust Audio Steganography via Genetic Algorithm". Third International Conference on Information & Communication Technologies ICICT2009. Pages 149 - 153. 15-16 August 2009. Karachi, Pakistan.
- [30] Mazdak Zamani, Azizah Abdul Manaf, Rabiah Ahmad, Akram Zeki, and Pritheega Magalingam. "A Novel Approach for Audio Watermarking". Fifth International Conference on Information Assurance and Security. Pages 83-86. 18-20, August 2009. Xi'an, China.
- [31] Mazdak Zamani, Azizah Abdul Manaf, Rabiah Ahmad, Farhang Jaryani, Hamed Taherdoost, and Akram Zeki. "A Secure Audio Steganography Approach". The 4th International Conference for Internet Technology and Secured Transactions. Pages 501-506. 9-12 November 2009. London, UK.
- [32] Najaf Torkaman, M.R., Nikfard, P., Sadat Kazazi, N., Abbasy, M.R. & Tabatabaiee, S.F. 2011, Improving hybrid cryptosystems with DNA steganography. Communications in Computer and Information Science. Volume 194 CCIS, 2011, Pages 42-52.
- [33] Nuha Omran Abokhdair, Azizah Bt Abdul Manaf, Mazdak Zamani. Integration of Chaotic Map and Confusion Technique for Color Medical Image Encryption. 6th International Conference on Digital Content, Multimedia Technology and its Applications (IDC2010). 16-18 August 2010. Seoul, Korea.
- [34] Shahidan M. Abdullah, Azizah A. Manaf, and Mazdak Zamani. Capacity and Quality Improvement in Reversible Image Watermarking Approach. 6th International Conference on Networked Computing and Advanced Information Management. 16-18 August 2010. Seoul, Korea.
- [35] Kekre, H.B., Athawale, A., Rao, B.S. & Athawale, U. 2010, "Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding". 3rd International Conference on Emerging Trends in Engineering and Technology, ICETET 2010. 2010, Article number 5698319, Pages 196-201.
- [36] Krishna Bhowal, Anindya Jyoti Pal, Geetam S. Tomar, P.P. Sarkar. Audio Steganography Using GA. 2010 International Conference on Computational Intelligence and Communication Networks. Bhopal, India.
- [37] Krishna Bhowal, Debnath Bhattacharyya, Anindya Jyoti Pal and Tai-Hoon Kim. A GA based audio steganography with enhanced security. Journal Name: Telecommunication Systems.
- [38] Ei Thin Su. Robust Data Embedding Based Probabilistic Global Search in MDCT Domain. Informatics Engineering and Information Science. Communications in Computer and Information Science, 2011, Volume 251, Part 2, 290-300.