Correlation between PSNR and Size Ratio in 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 the correlation between PSNR and message to host size ratio that is calculated in an experimental way.

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 [1-4].

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 [5-9].

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 [10-16].

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 [17-21].

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 [22-26].

2 Correlation between Size Ratio and PSNR

In this section the correlation between message to host size ratio and PSNR is studied. However it is obvious that if the ratio of host size to message size is greater, obtained PSNR will be better. That is because if the host size is extraordinarily lager than required size, message bits will be embedded into a portion of host and some part of host will be the same as the original and that makes the PSNR better.

Also this study intends to test the performance of GSBAS (a novel Genetic Substitution Based Audio Steganography that is implemented in this research) in comparison with OSBAS (Ordinary Substitution Based Audio Steganography) as given in last two columns of following tables. This section has two sub-sections: same message is embedded into different hosts, then different message are embedded into the same host.

2.1 Embedding different messages on same host

In this section, the experiments of embedding the different message into the same host are provided for two hosts.

2.1.1 First host

As Table 1 and Figure 1 show, fifteen messages with different size are embedded into a host whose size is 126215470byte.

TABLE 1. FIFTEEN MESSAGES ARE EMBEDDED INTO FIRST HOST

Sample No	Message Size (Byte)	Host Size (Byte)	Host to Message Ratio	Simple 2 Bits Per Sample Substitution	2 Bits Per Sample with GSBAS
1	3	126215470	42071823.33	104.22	105.62
2	7	126215470	18030781.43	99.35	101.19
3	17	126215470	7424439.41	95.06	97.62
4	30	126215470	4207182.33	92.79	95.02
5	35	126215470	3606156.29	92.15	94.36
6	56	126215470	2253847.68	90.23	92.34
7	153	126215470	824937.71	85.81	87.99
8	213	126215470	592560.89	84.33	86.60
9	251	126215470	502850.48	83.35	85.87
10	254	126215470	496911.30	83.09	85.77
11	301	126215470	419320.50	82.88	85.07
12	575	126215470	219505.17	79.09	82.22
13	1961	126215470	64362.81	74.66	76.93
14	2547	126215470	49554.56	72.93	75.78
15	4004	126215470	31522.35	71.49	73.83

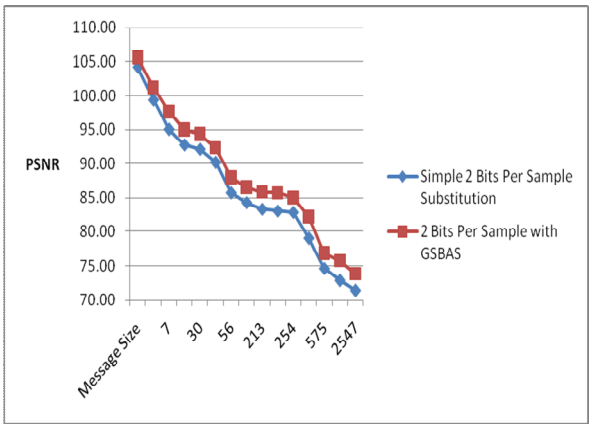

Figure 1. Fifteen messages are embedded into first host

The results show that as the message size is increased, PSNR is decreased. Also, the results show the performance of GSBAS is much better compared to ordinary substation based audio steganography (OSBAS).

2.1.2 Second host

As Table 2 and Figure 2 show, 15 messages with different size are embedded into a host whose size is 81533998 byte.

TABLE 2. FIFTEEN MESSAGES ARE EMBEDDED INTO SECOND HOST

Sample No	Message Size (Byte)	Host Size (Byte)	Host to Message Ratio	Simple 2 Bits Per Sample Substitution	2 Bits Per Sample with GSBAS
1	3	81533998	27177999.33	102.34	103.69
2	7	81533998	11647714.00	97.47	99.34
3	17	81533998	4796117.53	93.17	95.74
4	30	81533998	2717799.93	90.89	93.14
5	35	81533998	2329542.80	90.28	92.49
6	56	81533998	1455964.25	88.33	90.47
7	153	81533998	532901.95	83.94	86.13
8	213	81533998	382788.72	82.45	84.73
9	251	81533998	324836.65	81.49	84.00
10	254	81533998	320999.99	81.22	83.90
11	301	81533998	270877.07	81.04	83.19
12	575	81533998	141798.26	77.23	80.34
13	1961	81533998	41577.77	72.79	75.06
14	2547	81533998	32011.78	71.06	73.91
15	4004	81533998	20363.14	69.62	71.96

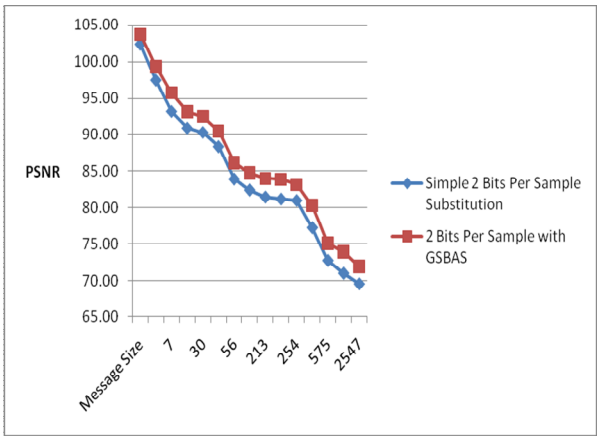

Figure 2. Fifteen messages are embedded into second host

ISBN: 978-1-61804-081-7

The results show that as the message size is increased, PSNR is decreased. Also, the results show the performance of GSBAS is much better compared to ordinary substation based audio steganography (OSBAS).

2.1.3 Third host

As Table 3 and Figure 3 show, a large message whose size is 62655022 bytes is embedded into a large audio file whose size is 541559854 bytes.

TABLE 3. EMBEDDING A LARGE MESSAGE

Sample No	Message Size (Byte)	Host Size (Byte)	Host to Message Ratio	Simple 2 Bits Per Sample Substitution	2 Bits Per Sample with GSBAS
1	62655022	541559854	8.643	43.159	45.677

A large audio file as host and a large message file were selected for embedding to compare the result of PSNR for two bit per sample rate, by GSBAS and OSBAS.

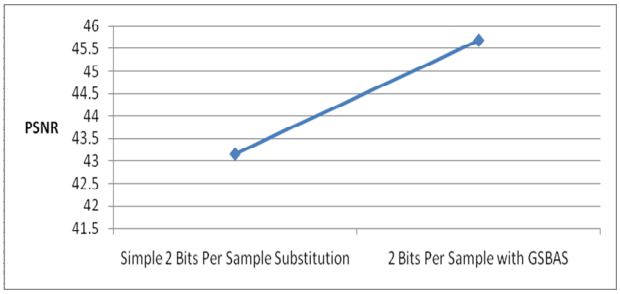

Figure 3. Embedding a large message

2.2 Embedding same message on different hosts

In this section, the experiments of embedding the same message into different hosts are implemented.

2.2.1 First message

As shown in Table 4 and Figure 4, first message which is going to be embedded into 20 audio hosts with different size is a help file of Windows and its size is 10790 byte. The message is embedded into the hosts with GSBAS and ordinary 2 bits per sample substitution. As can be seen from the graph in the figure, the performance of proposed method (GSBAS) is much better compared to ordinary substitution-based audio steganography (OSBAS).

Also, it can be seen that having the same message and different hosts, the larger host size gives higher PSNR because some part of host file will remain the same with the original file, and as a result gives higher PSNR.

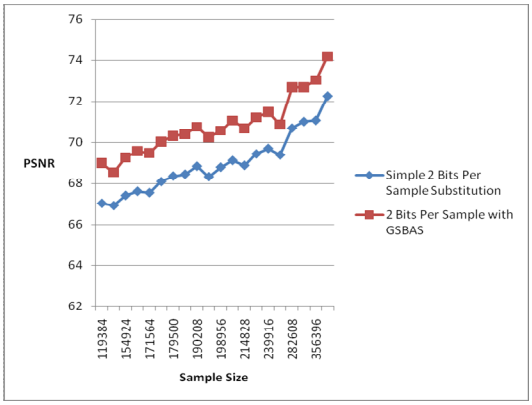

Figure 4. First message embedded into different hosts

TABLE 4. FIRST MESSAGE EMBEDDED INTO DIFFERENT HOSTS

Sample No	Message Size (Byte)	Host Size (Byte)	Host to Message Ratio	Simple 2 Bits Per Sample Substitution	2 Bits Per Sample with GSBAS
0	10790	119384	11.06	67.03	69.00
1	10790	129580	12.01	66.92	68.54
2	10790	154924	14.36	67.42	69.26
3	10790	159276	14.76	67.62	69.57
4	10790	171564	15.90	67.55	69.48
5	10790	178220	16.52	68.09	70.03
6	10790	179500	16.64	68.36	70.31
7	10790	179704	16.65	68.45	70.41
8	10790	190208	17.63	68.84	70.76
9	10790	191788	17.77	68.33	70.25
10	10790	198956	18.44	68.79	70.57
11	10790	207148	19.20	69.12	71.07
12	10790	214828	19.91	68.88	70.68
13	10790	227372	21.07	69.44	71.22
14	10790	239916	22.24	69.71	71.48
15	10790	246828	22.88	69.39	70.87
16	10790	282608	26.19	70.70	72.69
17	10790	353836	32.79	71.02	72.68
18	10790	356396	33.03	71.08	73.03
19	10790	424644	39.36	72.26	74.19

ISBN: 978-1-61804-081-7

2.2.2 Second message

As shown in Table 5 and Figure 5, second message is an image file of Windows and its size is 14049 byte which is going to be embedded into 20 audio files with different size.

The message is embedded into the hosts with GSBAS and ordinary 2 bits per sample substitution. As is shown in the figure, compared to ordinary substitution-based audio steganography (OSBAS), the performance of proposed method (GSBAS) is improved by 2 dB in average.

Based on Figure 5, the performance in term of PSNR is absolutely improved with GSBAS. Apparently, having the same message and different hosts, the larger host size gives higher PSNR because some part of host file will remain the same with the original file, and as a result gives higher PSNR.

TABLE 5. SECOND MESSAGE EMBEDDED INTO DIFFERENT HOSTS

Sample No	Message Size (Byte)	Host Size (Byte)	Host to Message Ratio	Simple 2 Bits Per Sample Substitution	2 Bits Per Sample with GSBAS
0	14049	119384	8.50	65.74	67.82
1	14049	129580	9.22	65.69	67.42
2	14049	154924	11.03	66.15	68.02
3	14049	159276	11.34	66.38	68.45
4	14049	171564	12.21	66.33	68.35
5	14049	178220	12.69	66.87	68.93
6	14049	179500	12.78	67.09	69.16
7	14049	179704	12.79	67.18	69.27
8	14049	190208	13.54	67.51	69.61
9	14049	191788	13.65	67.07	69.11
10	14049	198956	14.16	67.57	69.51
11	14049	207148	14.74	67.83	69.93
12	14049	214828	15.29	67.61	69.58
13	14049	227372	16.18	68.17	70.11
14	14049	239916	17.08	68.45	70.40
15	14049	246828	17.57	68.16	69.95
16	14049	282608	20.12	69.43	71.55
17	14049	353836	25.19	69.79	71.63
18	14049	356396	25.37	69.79	71.84
19	14049	424644	30.23	70.96	73.05

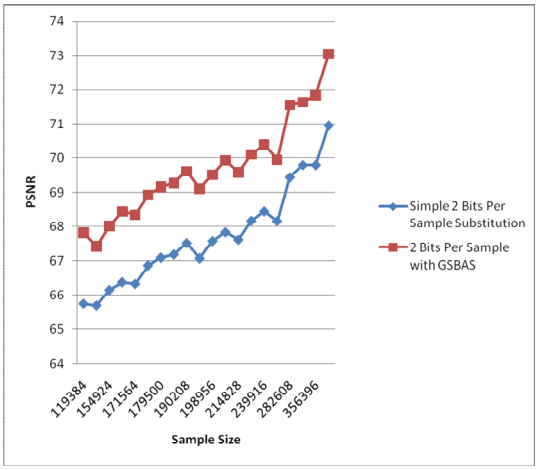

Figure 5. Second message embedded into different hosts

2.2.3 Third message

As Table 6 and Figure 6 show, third message which is going to be embedded into 20 hosts with different size is a GIF image file of Windows and its size is 1060 byte. The message is embedded into the hosts with GSBAS and ordinary 2 bits per sample substitution. As is shown in the figure, compared to ordinary substitution-based audio steganography (OSBAS), the performance of proposed method (GSBAS) is improved by 2 dB in average.

Also, it can be seen that having the same message and different hosts, the larger host size gives higher PSNR because some part of host file will remain the same with the original file, and as a result gives higher PSNR.

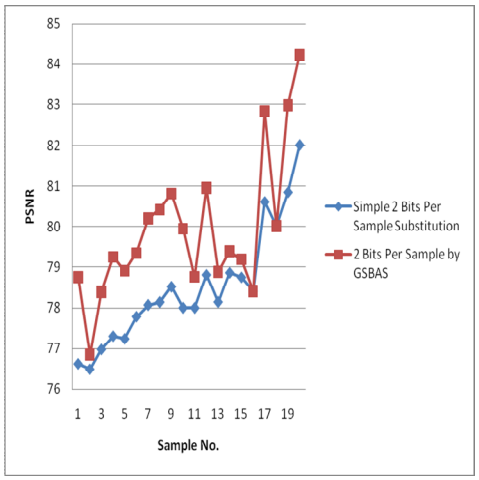

Figure 6. Third message embedded into different hosts

ISBN: 978-1-61804-081-7

TABLE 6. THIRD MESSAGE EMBEDDED INTO DIFFERENT HOSTS

Sample No	Message Size (Byte)	Host Size (Byte)	Host to Message Ratio	Simple 2 Bits Per Sample Substitution	2 Bits Per Sample by GSBAS
0	1060	119384	112.63	76.62	78.75
1	1060	129580	122.25	76.49	76.85
2	1060	154924	146.15	76.98	78.38
3	1060	159276	150.26	77.31	79.25
4	1060	171564	161.85	77.24	78.90
5	1060	178220	168.13	77.79	79.34
6	1060	179500	169.34	78.07	80.20
7	1060	179704	169.53	78.14	80.42
8	1060	190208	179.44	78.51	80.82
9	1060	191788	180.93	78.00	79.94
10	1060	198956	187.69	78.00	78.75
11	1060	207148	195.42	78.80	80.96
12	1060	214828	202.67	78.14	78.87
13	1060	227372	214.50	78.85	79.39
14	1060	239916	226.34	78.74	79.19
15	1060	246828	232.86	78.40	78.40
16	1060	282608	266.61	80.61	82.83
17	1060	353836	333.81	80.01	80.01
18	1060	356396	336.22	80.84	82.97
19	1060	424644	400.61	82.01	84.23

3 Conclusion

This study shows that if host to message ratio increases then higher PSNR yields which is calculated in average in last two rows. In the other words, having the same host, if the size of chosen message file increases, then PSNR is decreased. With the same message, if size of chosen host files increases, then PSNR is increased.

Acknowledgment

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

References:

[1] 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.

[2] 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.

[3] 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.

[4] Mazdak Zamani, Hamed Taherdoost, Azizah A. Manaf, Rabiah B. Ahmad, and Akram M. Zeki. "An Artificial-Intelligence-Based Approach for Audio Steganography". MASAUM Journal of Open Probelms in Science and Engineering (MJOPSE). Volume: 1 Issue: 1 Month: October 2009. Pages 64-68.

[5] 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.

[6] 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.

[7] Mazdak Zamani, Azizah Abdul Manaf, Hossein Rouhani Zeidanloo, and Saman Shojae Chaeikar. "Genetic Subtitution-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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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).

[14] 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.

[15] 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.

[16] 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.

[17] Asha Vijayan, Amrita Vishwa Vidyapeetham. A Genetic Algorithm Approach for Audio Steganography. Computer Science Journals.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] Krishna Bhowal, Debnath Bhattacharyya, Anindya Jyoti Pal and Tai-Hoon Kim. A GA based audio steganography with enhanced security. Journal Name: Telecommunication Systems.