



CAPACITY ENHANCEMENT OF MESSAGES CONCEALMENT IN IMAGE AND AUDIO STEGANOGRAPHY

Jasril, Ismail Marzuki, Faisal Rahmat

Informatics Department, Faculty of Sciences and Technology

State Islamic University of Sultan Syarif Kasim Riau, Indonesia

Emails: jasril_2000@yahoo.com, ismail.mz@uin-suska.ac.id, faisalrahmat88@gmail.com

Submitted: July 10, 2013

Accepted: Nov. 1, 2013

Published: Dec. 16, 2013

Abstract- Basically, a steganography indicates two of the principal requirements such the messages and the carrier file. Besides, it should have three aspects: capacity, imperceptibility, and robustness. This paper will show how to enhance the capacity of two types of carrier files for embedding message. By using Least Significant Bit method and modifying the four last bits of carrier files, bitmap and wav files could show the increasing of message size to be inserted to the carrier than only modifying the last 1 bit of carrier files. Particularly bitmap file which still had good quality visual showed PSNR value in 31.5460 dB, but wav file was only 3.8929 dB.

Index terms: Capacity Steganography Enhancement, Image and Audio Steganography, LSB Method, Least Significant Bit, Steganography.

I. INTRODUCTION

Many researches have explained about steganography as a technique for hiding a message in a carrier file so the manner that the very existence of the message is unknown. Steganography techniques have been developed in order to achieve the security. The goal of Steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated [1-8]. Message or the hidden secret information which embedded to the carrier file should be difficult to be detected by hackers. It can be done by using method or algorithm embedding. And message can be extracted again by retrieving algorithm. There are some powerful methods or algorithm to be used in this case. It is caused by this study have been started since 1995 to 2006 from the publication statistics of IEEE [9]. But the most popular one is Least Significant Bit Method [10,11]. LSB works by replacing directly the last bit of the media with secret bits to get the stego-image hence this method is supposed as an easy and fast in the algorithm.

In steganography, image has become an essential, potential, and popular file to be used as carrier file for protecting the confidential information [12]. But actually, theory had said that all of the digital files could be used as a carrier file or the message. Besides, there are three important aspects to be considered for steganography [13]: (i) Imperceptibility: means to preserve the details of the carrier file when the secret information is being embedded. (ii) Payload capacity: means the maximum number of bits that can be hidden with an acceptable resultant stego file quality. (iii) Robustness: is the ability of stego file to retain its contents from attacks.

The main focus of this work is how to enhance of capacity message to be hidden inside of carrier file by using Least Significant Bit Method. This project will try to use audio file, wav file, to be carrier also beside image. Both of carriers are uncompressed file. They used because they have close structure of raw data.

We tried to modify as much as four bits of the last bit of carrier file directly to get more space in carrier. The more space is the more message size can be inserted into a carrier. We have tried to do the similar work with the same carrier files, image and audio uncompressed files, by modified the two last bit of the carrier only. In that research we could show that carrier files could accommodate more space as much as two times larger than only modified of 1 bit of the carrier

files [14]. These researches are motivated by Habbes statement (2006) which exploring four bits but not more four bits to larger capability of steganography carrier file to hide message [15].

Related papers to this method study, there are some publications in common year using LSB as their method: Kriti Saroha and Pradeep Kumar Singh (2010) researched steganography with audio file as its cover using LSB [16], Sujay Narayana and Gaurav Prasad (2010) researched the image steganography using LSB [17], Pradeep Kumar Singh and R.K.Aggrawal (2010) using LSB method for hiding image into audio files, Saurabh Singh and Gaurav Agarwal (2010) utilizing LSB for video steganograph [18], Rahul Rishi (2011) researched steganography to the image stegano with Mode and Multiple Technique method which still developed from LSB method [19], and others.

II. METHODS

a. Least Significant Bit Concept

Basically, the computer was created due to binary numbers, known as two numbers, namely 0 and 1. Both of these numbers are often referred to as bits. Then, these bits will continue to form a composite sequential and binary structure into a set of information. Set of information is composed of 8-bit or often referred to as 1 byte.

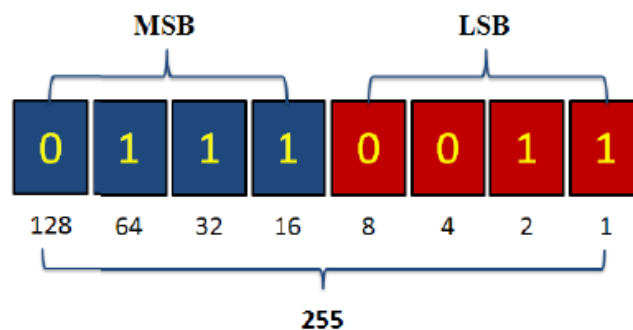


Figure 2. Binary Representation

Binary information bits are classifications based on the sequence and its influence in the byte bits. These bits are divided into 2 groups, the Most Significant Bit (MSB) and the Least Significant Bit (LSB), as shown in figure 2. Most Significant Bit is representation of 4-bits which have a major influence on a range of information, means drastic changes that would occur if these

bits are modified. While the Least Significant Bit is a 4-bit representation of the least influential when the bits are modified and will not be a drastic change, so the possibility of human prejudice against LSB bits are modified very little. Thus, the right, the bits are smaller effect on the integrity of the data contained. Therefore, the 4-bit last modified and became the sticking a steganography digital information.

b. Steganography Testing

This steganography research will be test to find the level of quality stegofile after the message embedded to the carrier. For the bitmap carrier type file tested using the Peak Signal to Noise Ratio (PSNR) formula and the Signal to Noise Ratio (SNR) for wave stegofile which both of these formulas will be counted in decibel (dB). The value of PSNR is good if it is above of 20 dB with formula [16]:

$$PSNR = 10 \text{ Log}_{10} \left(\frac{255^2}{MSE} \right) \quad (1)$$

255 is the highest value of pixel intensity and MSE (Mean Square Error) is the average value of total square of Absolute Error between carrier file and stegofile. MSE can be counted with the formula bellow:

$$MSE = \frac{1}{m n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (2)$$

The SNR formula used to know the distortion ratio that happened after the message inserted to the carrier with the formula [17]:

$$SNR = 10 \text{ Log}_{10} \left\{ \frac{\sum_n X^2(n)}{\sum_n [X^2(n) - Y^2(n)]} \right\} \quad (3)$$

X(n) is the average of RMS (Root Mean Square) value from the carrier file and Y(n) is the average of RMS value from stegofile. The RMS value is the formula to know how big the sample audio out of any audio file. It can be known by using the audio editor application that provides information about quality of RMS audio, for example: Cool Edit Pro 2.0.

III. DISCUSSION

Generally, every steganography application has process to hide or extract the message to the carrier file. So it is the same with this research that shown in figure 7 that has process, input data, and output data just like other steganography:

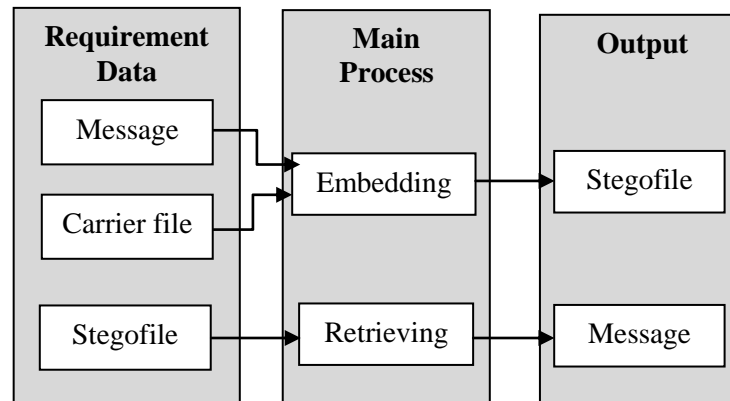


Figure 3. Illustration of General Process System

Based on the figure 3 above can be explained bellow:

1. Requirement data. There are three data need for this application that different with the main process: Message, the cover for hiding message, and data that brings the message.
2. Main process. It used to process every data that input to the application. There are two main processes: Embedding process to hide the message into the carrier file and Retrieving process to extract the message from the carrier.
3. Output is the result from the main process. Embedding output process is called by stegofile, and retrieving output process is the message that inserted in stegofile.

a. Embedding Process

Below is figure 7 to show the embedding process flowchart. Based on figure 4, embedding process can be explained bellow:

1. User must input the carrier file and message to be inserted.
2. Carrier file and message are converted to the binary.
3. Carrier file having converted is parted, such as: file header or file chunk as the important part of file.

4. Bytes can be modified with take the size of carrier twice bigger than the size of message.
5. Bytes of carrier file will be indexed to array that consist 4 bits per index.
6. Looping the process till all the bits message finished to be inserted to the carrier.
7. Gather all file info and parts have been inserted.

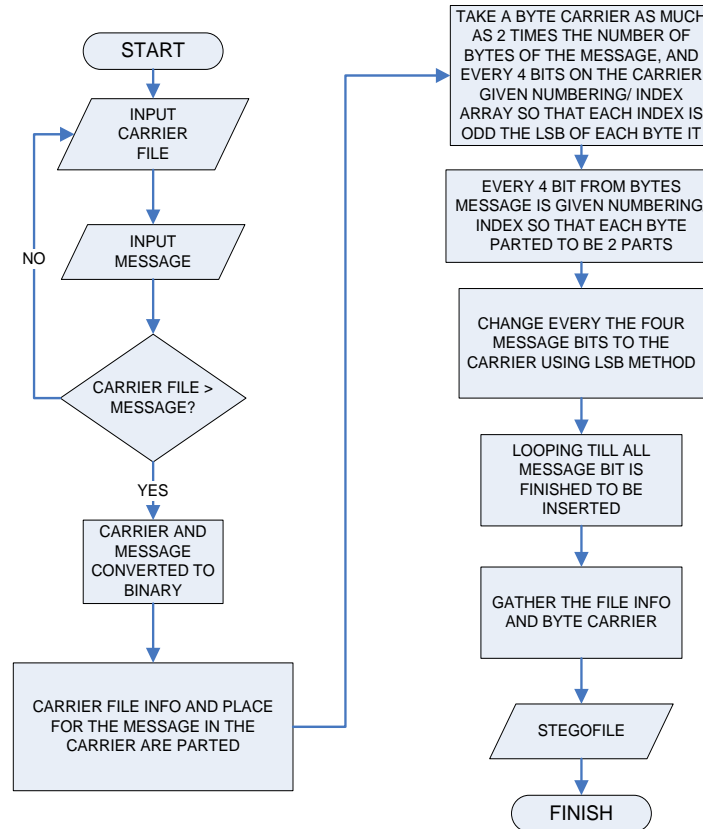


Figure 4. Embedding Flowchart

b. Retrieving Process

Below is figure 5 to show the embedding process flowchart. Based on figure 5, embedding process can be explained:

1. User must input the stegofile
2. Stegofile converted to binary.
3. Bytes of stegofile indexed in every 4 bit.
4. Extract the message from the carrier.
5. Looping the process till all bits collected.
6. Gather all bits to be converted be message
7. Rretrieving Process finished.

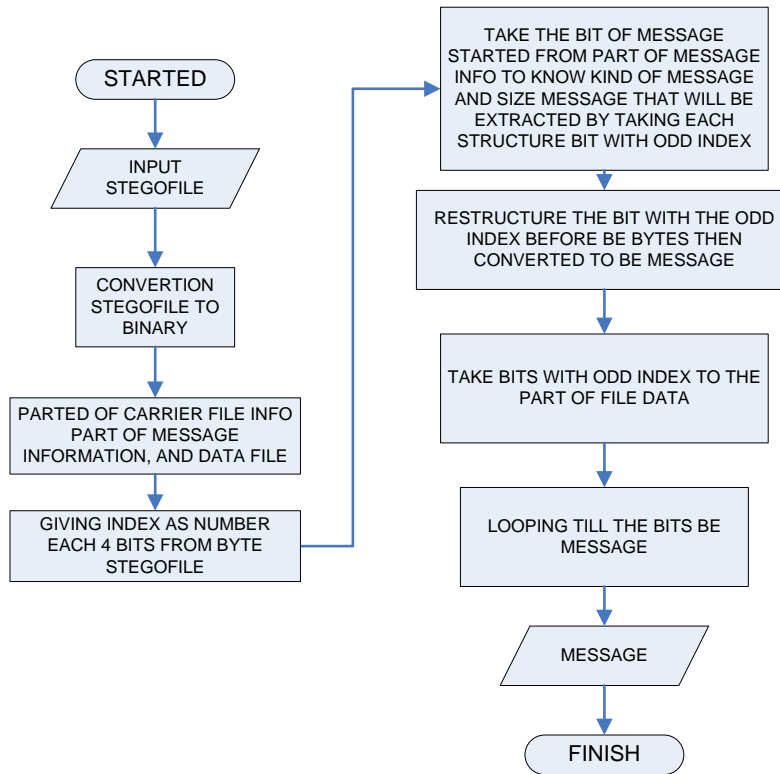


Figure 5. Retrieving Flowchart

III. RESULTS

a. Capacity Steganography Test

Basically, this test is performed to determine the capacity or size of a file before bringing the message (carrier file) with file after carrying the message (stegofile). The trick is to compare size or the capacity of the two files. A good condition for steganography system is when the size or capacity of the file either before or after the inserted is unchanged.

Capacity testing can be seen by using the properties file on Windows operating systems. In accordance with the background already explained in Chapter I, the test will only be performed on files type carrier *.Bmp and *.Wav. Steganography capacity test results can be seen in Table 1. It can be concluded that from the aspect of capacity, system modifications 4bit steganography can be good.

Table 1: Capacity Steganography Test

No	Carrier file	Carrier Size (byte)	Type Message	Message Size (byte)	Stegofie Size (byte)
1	take a train ride_trime d_2.wav	1760668	Text	190	1760668
			animated_avatar.gif	5619	1760668
			human-face-vector-1.jpg	32562	1760668
			animated_avatar.gif	5619	1760668
2	mol_pku2.bmp	571556	pesan_tes_mp2.docx	275643	571556
			animated_avatar.gif	5619	571556
			human-face-vector-1.jpg	32562	571556

b. Quality Steganography Test

The quality testing aspect involves examining and comparing the number of bits error between the carrier files and stegofile. It is done by using PSNR to image files and SNR to audio files.

Table 2: Quality Carrier File Image Steganography Test

No	Carrier file	Color Type	Carrier Size (byte)	Message Size (byte)	MSE (db)	PSNR (db)
1	mol_pku2.bmp	RGB-24bit	571556	479806	24,5726	34,2263
				372166	24,6976	34,2043
				275643	22,6153	34,5868
				165390	13,8572	36,7140
				81004	7,6631	39,2868
				40506	4,5141	41,5851
				19907	2,8787	43,5388
2	UIn_rek.bmp	RGB-24bit	1326654	775207	44,3735	31,6625
				750848	44,3423	31,6626
				661744	44,2827	31,6685
				479806	32,0280	33,0755
				165390	11,2528	37,6182
				81044	5,4467	40,7695
				40506	2,6259	43,9381
3	tugu2_grayscale.bmp	Grayscale-8bit	242680	275643	43,3882	31,7571
				165390	42,7880	31,8176
				120023	42,6700	31,8296
				59353	21,1544	34,8768
				28896	10,7004	37,8368
				14889	5,6936	40,5769

				4378	1,1662	47,4629
4	lontong.bmp	Grayscale-8bit	262292	240448	45,3700	31,5631
				165390	44,5288	31,6444
				130812	45,5489	31,5460
				65116	23,9926	34,3300
				32542	12,7436	37,0779
				15674	6,2909	40,1437
				7321	2,1221	44,8632

In this test, the image file want to use some image files *.bmp which had a different bit depth and level of color who are also different composition. As an example of the calculation of PSNR on the following image file, the image will be used as original picture and tugu2_grayscale.bmp Stegofile (3). Bmp as images that have been inserted messages with dimensions of 602×400 pixel image and it will be seen in Table 2.

From table 2 can be seen on the images PSNR quality tested showed that the results obtained demonstrate the quality of the image after the modification at the 4-bit-bit LSB is still good, is evident from the quality of PSNR is still above 20 db, thus increasing payload capacity is reached. From table 2, charts can be illustrated to see patterns of change in PSNR quality of the image file as follows:

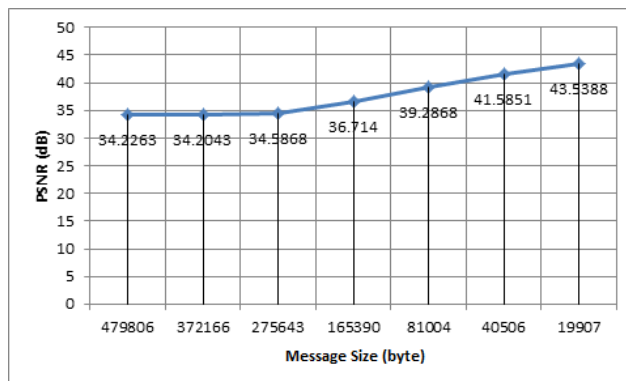


Figure 6. PSNR chart for file mol_pku2.bmp

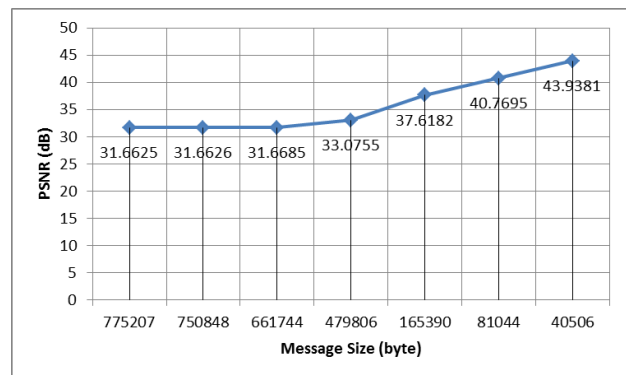


Figure 7. PSNR chart for file UIn_rek.bmp

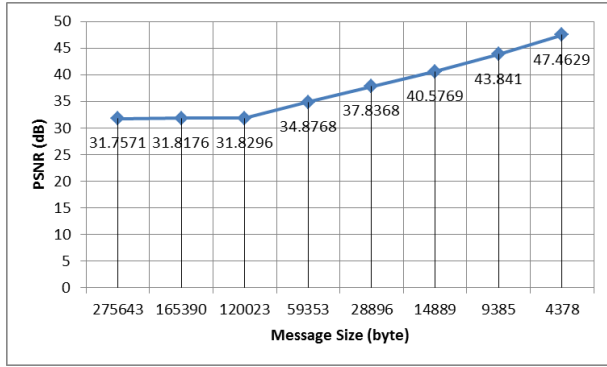


Figure 8. PSNR chart for file tugu2_grayscale.bmp

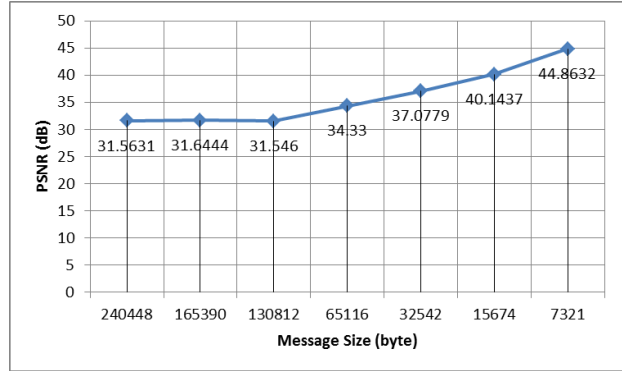




Figure 9. PSNR chart for file lontong.bmp

From the graph in figure 6, 7, 8 and 9 above the known pattern of change in PSNR quality of the image file would be better if the message is inserted in the carrier file smaller than the carrier size. Below is a table to show the visual alteration of carrier file image steganography.

Table 3: Visual Alteration of Carrier File Image Steganography

File Name	Original Carrier Image file	Stegofile
mol_pku2.bmp	 <p>Size of Original File : 571556 byte Color Type : RGB</p>	 <p>Size of Stego file : 571556 byte Size of Message : 275643 byte PSNR : 34,5868</p>

<p>UIn_rek.b mp</p>	 <p>Size of Original File: 1326654 Color Type: RGB</p>	 <p>Size of Stego file:1326654 Size of Message: 661744 PSNR : 31,6685</p>
<p>tugu2_gray scale.bmp</p>	 <p>Size of Original File: 242680 byte Color Type: Grayscale</p>	 <p>Size of Stego file: 242680 byte Size of Message: 120023 byte PSNR : 31,8296</p>
<p>lontong.bm p</p>	 <p>Size of Original File : 262292 byte Color Type: Grayscale</p>	 <p>Size of Stego file: 262292 Size of Message: 130812 PSNR : 31,5460</p>

Table 4: Quality Carrier File Audio Steganography Test

No	Carrier file	Color Type	RMS Carrier file (dB)	Message Size (byte)	RMS Stegofile (dB)	PSNR (db)
1	Roland-GR-1-Acoustic-Guitar-C4.wav	265262	-21,11	275643	-18,48	6,3143
				165390	-18,5	6,3453
				132002	-18,48	6,3143
				65116	- 20,57	12,9665
				32542	-20,99	19,4551
				15674	-21,04	21,7908
				7321	-21,08	25,4664
				4378	-21,09	27,2263
				3966	-21,1	30,2356
				3324	-21,1	30,2356
				2602	-21,1	30,2356
				2213	-21,11	-
				2098	-21,11	-
				1003	-21,11	-
				671	-21,11	-
				260	-21,11	-
424	-21,11	-				
378	-21,11	-				
2	Nat King Cole - L-O-V-E.wav	486956	-29,53	563118	-22,73	3,8984
				378184	-22,71	3,8873
				242347	-22,72	3,8929
				120023	-25,56	6,0066
				59353	-27,45	8,6674
				28896	-28,5	11,6403
				14889	-29,05	14,9153
				9385	-29,33	18,6967
				4378	-29,42	21,2865
				2098	-29,47	23,9152
				1003	-29,51	28,6835
				671	-29,52	31,6930
				888	-29,51	28,6835
				714	-29,51	28,6835
				699	-29,52	31,6930
				563118	-22,73	3,8984
378184	-22,71	3,8873				
242347	-22,72	3,8929				

The test results in Table 4, it can be described graph to portray the patterns of change in PSNR quality audio files that have been inserted message with 4bit modified LSB method. In stegofile quality testing for wave files, the values of RMS (Root Mean Square) carrier files, as well as the

RMS value of the message files can be obtained with the help of apps Cool Edit Pro 2.0. The RMS value taken from Cool Edit Pro 2.0 is the average value of the RMS that generated by each audio file. From the example of calculating the PSNR can be seen in table 4.

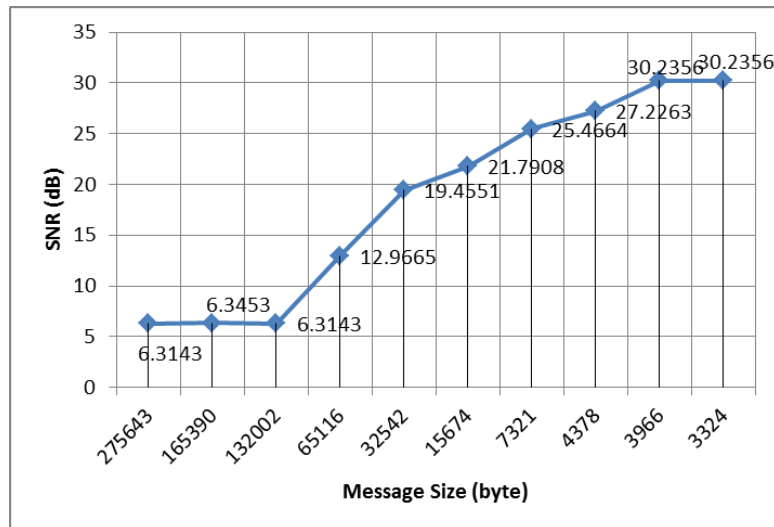


Figure 10. PSNR chart for file Roland-GR-1-Acoustic-Guitar-C4.wav

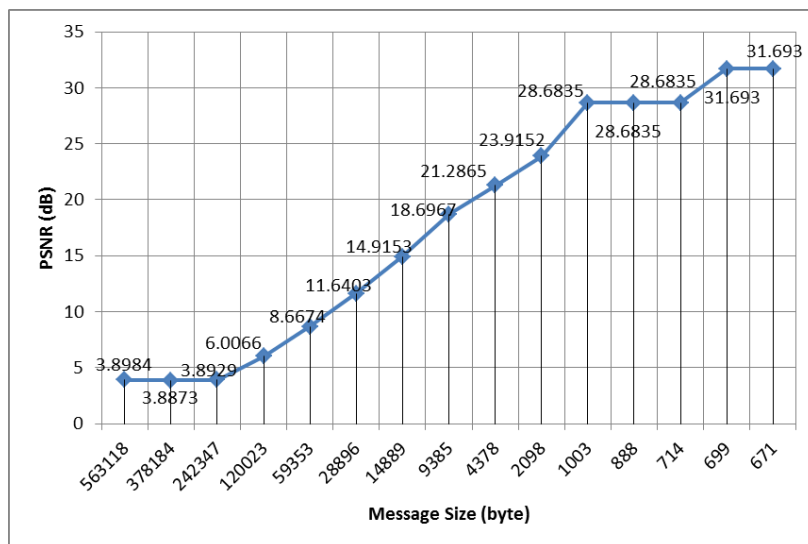


Figure 11. PSNR chart for file Nat King Cole - L-O-V-E.wav

From the graph 10 and 11 can be seen that applying LSB method with modifications 4bit audio file on the media for the purpose of increasing payload capacity is not reached because the messages can be inserted without damaging the quality of the audio file size is relatively small compared to the size of the carrier file. The maximum message size can be only 1% of the size of the carrier file. Below is a table to show the visual alteration of carrier file audio steganography.

VI. CONCLUSIONS

Below are some of the conclusions derived from this research:

1. Steganography files which has successfully made the message insertion and retrieving the digital media are image files *. Bmp, and sound files *. Wav with 4-bit LSB modifying the carrier file.
2. The most out of the method 4-bit LSB modification found in the image file because the goal of increasing payload capacity without causing major changes in the quality of the file can be achieved. Whereas the results of the method 4-bit LSB modifications in the sound file can be said to be bad and unreached.

REFERENCES

- [1] Prasad. M. Sitaram, Naganjaneyulu. S, Krishna. CH. Gopi, Nagaraju. C. "A Novel Information Hiding Technique for Security by Using Image Steganography," Journal of Theoretical and Applied Information Technology (JATIT), vol. 8, no. 6, pp. 35-39, 2005 - 2009.
- [2] YANG. Hengfu, SUN. Xingming, SUN. Guang. "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution," Radioengineering, vol. 18, no. 4, pp. 509-516, December 2009.
- [3] Bender. W, Gruhl. D, Morimoto. N, Aiguo. LU. "Techniques for data hiding," IBM Systems Journal, vol. 35, no. 3-4, pp. 313-336, 1996.
- [4] Jasril, Marzuki. Ismail, Rahmat. Faisal. "Modification Four Bits of Uncompressed Steganography Using Least Significant Bit (LSB) Method". International Conference of Advance Computer and Information Systems (ICAC SIS), pp. 287-292, Universitas Indonesia, Depok (Indonesia), 2013.
- [5] YIP. Shu-Kei, AU. Oscar. C, WONG. Hoi-Ming, HO. Chi Wang. "Block-Based Lossless Data Hiding in Delta Domain," Multimedia and Expo, IEEE International Conference, Toronto, Ontario (Canada), pp. 857-860, 2006.
- [6] YANG. Ching-Yu. "Based Upon RBTC and LSB Substitution to Hide Data," In Proc. First International Conference on Innovative Computing, Information and Control (ICICIC'06), Beijing (China), vol. 1, pp. 476-479, 2006.

- [7] CHANG. Chin-Chen, LIN. Chia-Chen, TSENG. Chun-Sen, TAI. Wei-Liang. "Reversible Hiding in DCT-Based Compressed Images," *Information Sciences*, vol. 177, no. 13, pp. 2768-2786, 2007.
- [8] YANG. You, YU. Ping, XU. Jiangfeng. "An Improved LSB Algorithm Based on Multi-Transformation," In *Proc. International Symposium on Information Science and Engineering (ISISE'08)*. Shanghai (China), vol. 1, pp. 487-49, Dec. 20-22, 2008.
- [9] Singh. Pradeep Kumar, Aggrawal. R.K. "Enhancement of LSB Based Steganography for Hiding Image in Audio," *International Journal on Computer Science and Engineering (IJCSE)*, vol. 02, no.05, pp. 1652-1658, 2010.
- [10] THIEN. C. C, LIN. J. C. "A Simple and High-Hiding Capacity Method For Hiding Digit-by-Digit Data in Images Based on Modulus Function," *Pattern Recognition*, vol. 36, no. 12, pp. 2875-2881, December 2003.
- [11] CHANG. Chin-Chen, LIN. Min-Hui, HU. Yu-Chen. "A Fast and Secure Image Hiding Scheme Based on LSB Substitution," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 16, no. 4, pp. 399-416, 2002.
- [12] Sathisha. N, et al "Embedding Information in DCT Coefficients Based on Average Covariance". *International Journal of Engineering Science and Technology (IJEST)*, vol. 3 no. 4, pp. 3184-3194, April 2011.
- [13] Hussain. Hanizan Shanker, et al. "A Novel Hybrid Fuzzy SVM Image Steganographic Model," *International Symposium in Information Technology*, vol. 1, pp. 1-6, June 2010.
- [14] Jasril, Marzuki. Ismail. "Application Design to Embed Text and File to Uncompressed File with Least Significant Bit". *Journal of Computer Science*, vol. 8 no. 2 pp. 137-151, Univeristas Pelita Harapan, Tangerang, (Indonesia), 2012.
- [15] Habes. Alkhraisat. "Information Hiding in BMP Image Implementation, Analysis and Evaluation," *Saint Petersburg Institute for Informatics and Automation, Russian Academy of Sciences, Saint Petersburg, Russia*, vol. 6, no. 1, pp. 1-10, February 2006.
- [16] Saroha. Kriti, Singh. Pradeep Kumar. "A Variant of LSB Steganography for Hiding Images in Audio," *International Journal of Computer Applications*, vol. 11, no.6, pp. 12-16, December 2010.
- [17] Narayana. Sujay, Prasad. Gaurav. "Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions," *Signal & Image Processing: An International Journal (SIPIJ)*, vol.1, no.2, pp. 60-73, December 2010.

- [18] Singh. Saurabh, Agarwal. Gaurav. "Hiding image to video: A new approach of LSB replacement," International Journal of Engineering Science and Technology, vol. 2, no. 12, pp. 6999-7003, December 2010.
- [19] Rahul. Rishi, Sudhir. Batra, Rajkumar. "Mode and Multiple Technique: A New Image Steganography Method for Capacity Enhancement of Message in Image," International Journal of Computer Applications, vol. 13, no. 4, pp. 10-16, January 2011.
- [20] Abu-Marie. Walaa, Gutub. Adnan, and Abu-Mansour. Hussein. "Image Based Steganography Using Truth Table Based and Determinate Array on RGB Indicator". International Journal of Signal and Image Processing, vol. 1, no. 3, pp. 196-204, 2010.
- [21] Eric. Cole. "Hiding in Plain Sight: Steganography and the Art of Covert Communication," Published by Wiley Publishing, Inc., Indianapolis, Indiana, Published simultaneously in Canada. 2003.