Steganography Implementation on Android Smartphone Using the LSB (Least Significant Bit) to MP3 and WAV Audio

Lindawati
State Polytechnic of Sriwijaya
Palembang, Indonesia
lindawati9111@yahoo.com

Rita Siburian
State Polytechnic of Sriwijaya
Palembang, Indonesia
rita.siburian@yahoo.co.id

***Abstract*—The rapid growth of science and technology in the telecommunications world can come up with new ways for some people bent on abusing for threatening information security as hackers, crackers, carder, phreaker and so on. If the information is on the wrong side will result in losses. Information that must be considered is the security of confidential information. Steganography is a method that can be used to hide a message by using digital media. Digital Steganography using digital media as the container vessel such as images, sounds, text, and video. Hidden secret data can also include images, audio, text, and video. In this final audio steganography implemented. One method that can be used in steganography is the Least Significant Bit (LSB). Steganography implementation will be accompanied by the application of cryptography in the form of encryption and decryption. This method works is messages that have been encrypted beforehand will be hidden evenly on each region in MP3 or WAV already divided, with modify / change the LSB of the media container with the bits of information to be hidden. In making the steganography application, the author uses the Java programming language eclipse, because the program is quite easy and can be run in the Android smartphone operating system.**

Keywords—steganography; audio mp3; wav; LSB method; java eclipse

I. PRELIMINARY

The rapid growth of science and technology in the telecommunications world can come up with new ways for some people bent on abusing for threatening information security as hackers, crackers, carder, phreaker and so on. If the information is on the wrong side will result in losses. Information that must be considered is the security of confidential information [1].

Cryptographic methods to ensure data security of such information by way of encrypting data by turning it into a random codes that are random, making the data can not be read and understood by others [2]. But the use of such encryption methods do not always guarantee the security of such data because the data is messy in other words can be described as unusual and suspicious. To avoid problems it is born steganography for hiding data, which refers to how the inability of third parties to detect the presence of hidden information [3].

Steganography is a security system that emerged from the perceived deficiencies exist in cryptography. The idea is hide secret message into another message in the hope that outsiders are not aware of or suspect any secret messages contained therein [4]. Steganography is a method that can be used to hide a message by using digital media. Digital Steganography using digital media as the container vessel such as images, sounds, text, and video. Hidden secret data can also include images, audio, text, and video. In this final audio steganography implemented.

One method of steganography is the LSB (least significant bit). The author chose to use the LSB method because this method is a simple method and using an algorithm that not too complicated, so it does not require a great resource to use. This method is suitable for use in a wide variety of devices such as computers or mobile phones that have a relatively small memory and can not make the process too cumbersome in quick time. The working principle of the method is the least significant bits change value the lowest bits of an audio sample with bits of the message that will be inserted [5].

II. BASIC THEORY

A. Steganography

The word steganography (steganography) is derived from the greek steganos, meaning hidden or disguised, and graphia, which means writing, so that the meaning of steganography is "writing (writing) veiled". With steganography, we can insert a secret message into other media and send it without being aware of the existence of the message. Steganography is the science that is used to insert data in other media. Steganography requires two media, namely container and the data will be inserted [3].

B. Audio Steganography

Audio steganography is the technique of inserting secret messages in media sound (audio). The process of inserting secret messages in steganographic system is basically done by

978-1-5090-6419-9/17/$31.00 ©2017 IEEE

identifying audio media messenger, ie the redundant bits which can be modified without damaging the integrity of the audio media itself. In applying steganography in audio files can be done with various techniques.

C. *Steganography Methods*

Steganography methods are most common in voice format is Modified Least Significant Bit. Method This widely used for computation are not too the complex and messages hidden quite secure. Strategies used data hiding messages to insert into the audio media is the method of Least Significant Bit (LSB). Where the message data bits will be replaced with the lowest bit in the audio media.

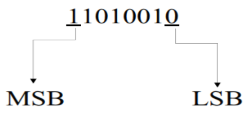

Fig. 1. MSB and LSB

MSB: Most Significant Bit
LSB: Least Significant Bit

In the figure 1, indicating that bit 1 of the next states MSB bit and bit 0 of the last binary number is bit LSB.

1. If the message = 10 bits, then the number of bytes used = 10 bytes

00110011 10100010 10100011 00100110
01011001 01101110 10110101 00010101
11100110 11011010

Suppose the binary of the embedded message: 1110101011
The result of the insertion of the LSB:

00110011 10100011 10100011 00100110
01011001 01101110 10110101 00010100
11100111 11011011

In the example above, only partly changed of Least Significant Bit. Based on the theory it was found that the original file size did not change so large that it is difficult detected by human senses.

D. *Audio Mp3*

MPEG-1 Audio Layer 3 or more commonly known as MP3 is a format file coding sound which has a good compression (though this is *lossy*) So that the file size may allow smaller. This file was developed by an engineerGerman Karlheinz Brandenburg, MP3 wearing coding*Pulse Code Modulation* (PCM). MP3 reducing the number ofbeet necessary by using psychoacoustic models to eliminate noise components that did not sound human.

E. *Audio Wav*

WAV is an abbreviation of the term in English waveform audio format is a standard Audio file formats developed by Microsoft and IBM, WAV is a variant of the bitstream format RIFF and similar to the format IFF and AIFF used computer Amiga and Macintosh, Both WAV and AIFF compatible withoperating system Windows and Macintosh, Although it can accommodate WAV audio in compressed form, generally the WAV format is uncompressed audio.

F. *Android*

Android is a mobile phone operating system based on Linux. Android also has an open platform for anyone who wants to create an app for use by a variety of mobile devices. Android is also an operating system for mobile phones as well as on Nokia's Symbian, Palm and Windows Mobile that have previously been known so far. Along with its development, android turned into a platform so quickly in making updates. Initially, Android was developed by Android Inc., which is supported financially from google parties, who then bought it in 2005. In 2007, the operating system has been officially simultaneously with the establishment of the Open hardset Alliance, a consortium of companies hardware, software as well as other telecommunications is not intended to promote an open standard mobile device. Android, Inc. was founded in October 2003 by Andy Rubin, Christ White, Rich Miner and Nick Sears in Palo Alto California that aims to develop smart mobile devices are more aware of the location and user preferences [6].

III. Method

A. *Process Encryption / Encryption of data*

In this process required the input data in the form of audio, messages / data, and the encryption key / insertion be used. The system will process the audio and data encryption using methods LSB(Least Significant Bit),

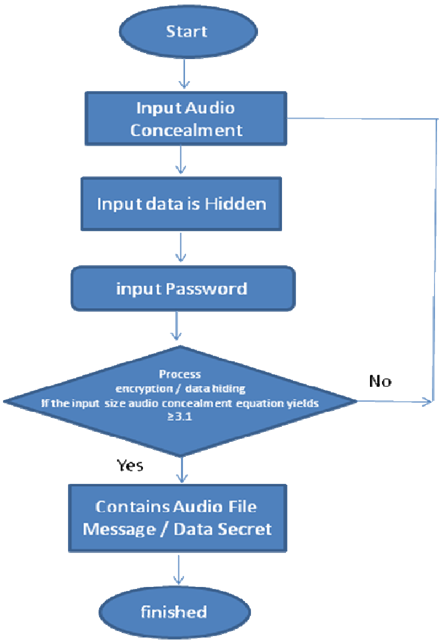
Start
Input Audio Concealment
Input data is Hidden
input Password
Process encryption / data hiding If the input size audio concealment equation yields ≥3.1
No
Yes
Contains Audio File Message / Data Secret
finished

Fig. 2. Encryption Process (insertion) of data

B. *Process Description / extraction of data*

In this process takes the form of an audio input data containing the message / file secret and key for data description. if the keywords are correct then the system will process the audio description, by taking portions of data from the bits of audio using the LSB(Least Significant Bit), Conversely, if the keyword is wrong then the audio is not going through the process descriptions, and get an audio file containing the original message has not been an open secret message.

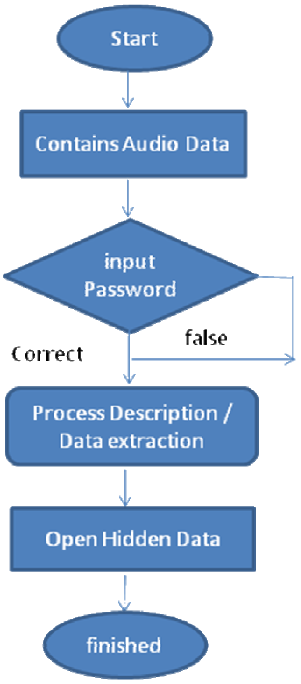

Fig.3. Description Process (extraction) of data

C. *Scenario Audio Quality Measurement*

On the results of steganography object will be noise. This noise occurs due to changes made to the process bit parity coding. Measurement of noise on the object steganography done using PSNR (Peak Signal to Noise Ratio). This noise can be heard immediately when the object steganography media in the run in music player. Mathematically the calculation of noise will wear PSNR value calculation with a value of at least 30 DB. PSNR calculation is done by using an equation [7]:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{P_1^2}{P_1^2 + P_0^2 - 2P_1P_0}\right) \qquad (1)$$

Where P_1 is the signal strength of audio files after the concealment of messages and P_0 is the initial signal strength. If PSNR <30 dB, it can be said that the results of steganography poor audio quality.

IV. Results and Discussion

The results of the analysis, it has successfully developed software that has a function to insert and extract messages. Then testing to check the correctness of the software, along with the performance of the software. Results of concealment are shown in the following table:

TABLE I. TESTING ENCRYPTION AUDIO MP3

Inserts file (MP3)		**Inserted Files**		**key**	**time Insertion (S)**	**File after insertion (Mp3)**	
Song title	***Size (KB)***	***File name***	***Size (KB)***			***Song title***	***Size (KB)***
Flutter my flag.mp3	3881149	Power.pptx	50,284	1234	101.558	Concealment1.mp3	3881149
		T-REC.pdf	78,059	1234	215.011	Concealment 2.mp3	3881149
		Practicum7 .docx	89,600	1234	270.72	Concealment 3.mp3	3881149
		Lap.xlsx	92 ,160	1234	286.357	Concealment 4.mp3	3881149

In Table 1 we can see, the first concealment size hidden files takes 101 558 50 284 kb s, harboring both size 78 files are hidden, 059kb takes 215. 011s, third concealment size 89,600 kb hidden files takes 270.72s, and concealment last the second concealment hidden file size 92, 160 kb takes 286 357s. The larger the file size that is hidden, the greater the time required. And audio results obtained sizenya unchanged.

TABLE II. TESTING ENCRYPTION AUDIO WAV

Inserts file (.wav)		**Inserted Files**		**key**	**time Insertion (S)**	**File after insertion (Wav)**	
Song title	***Size (KB)***	***File name***	***Size (KB)***			***Song title***	***Size (KB)***
one country one nation.wav	6459632	inframerah.pptx	240,395	1234	2478.037	Concealment1.wav	6459632
		BBC.pdf	293,449	1234	2497.856	Concealment 2.wav	6459632
		Cover.docx	330,730	1234	4398.235	Concealment 3.wav	6459632
		RAB.xlsx	390,498	1234	390498	Concealment 4.wav	6459632

In Table 2 can be seen, the concealment of the first size hidden files 240, 395 kb takes 6,459,632 s, harboring both size hidden files 293, 449kb takes 6,459,632 s, concealment third size hidden files 330, 730 kb takes 6,459,632 s, and last concealment hidden file size 390, 498 kb takes 6459632 s. The larger the file size that is hidden, the greater the time required. And audio results obtained sizenya unchanged.

TABLE III. TESTING MP3 AUDIO DESCRIPTION

File after insertion (Mp3)		**Key**	**Time (S)**	**result**	
Song title	***Size (KB)***			***Filename***	***size (KB)***
Concealment1.mp3	3881149	1234	12.643	Power.pptx	50 284
Concealment 2.mp3	3881149	1234	17.58	T-REC.pdf	78 059
Concealment 3.mp3	3881149	1234	19.602	Practicum7.docx	89,600
Concealment 4.mp3	3881149	1234	20.669	Lap.xlsx	92 160

In table 3 it can be seen, extracting first size files extracted 50 284 kb takes 12 643 s, extracting first size files extracted 78 059 kb takes time 17:58 s, extracting first size files extracted 89,600 kb takes 19 602 s, and extracting first extract the file size 92 160 kb takes 20 669 s. The larger the file size the extract, the greater the time required. And results files are extracted as file hiding. The length of time extracting much faster than on concealment.

TABLE IV. TESTING AUDIO DESCRIPTION WAV

File after insertion (Mp3)		**Key**	**Time (S)**	**Result**	
Song title	***Size (KB)***			***Filename***	***size (KB)***
Concealment1.wav	6459632	1234	48.847	inframerah.pptx	240 395
Concealment 2.wav	6459632	1234	58.251	BBC.pdf	293 449
Concealment 3.wav	6459632	1234	78.851	Cover.docx	330 730
Concealment 4.wav	6459632	1234	141.014	RAB.xlsx	390 498

In table 4 can be seen, extracting first size files extracted 240, 395 kb takes 48 847 s, extracting first size files extracted 293, 449kb takes 58 251 s, extracting first size files extracted 330, 730 kb takes 78 851 s, and the first extraction 390 extracts the file size, 498 kb takes 141 014 s. The larger the file size the extract, the greater the time required. And results files are extracted as file hiding. The length of time extracting much faster than on concealment.

TABLE V. TESTING PSNR AUDIO MP3

Original Audio			**Audio Results**			**Test result**	
Song title	**Size (KB)**	**P0**	***Song title***	***Size (KB)***	***P1***	***subjective***	***PSNR***
Flutter my flag.mp3	3881149	-17.2386	Concealment1.mp3	3881149	-17.4790	Good	37.2291
			Concealment2.mp3	3881149	-18.0283	Bad	27.1699
			Concealment3.mp3	3881149	-18.5209	Bad	23.1933
			Concealment4.mp3	3881149	-18.448	Bad	23.6887

In Table 5 it can be seen, PSNR values obtained in the first audio is 37.2291 a good audio, the second audio is 27.1699 a bad audio, audio third is 23.1933 a bad audio, the second audio is 23.6887 a poor audio. The larger the data is inserted, the smaller PSNR then concentrated in poor audio.

TABLE VI. TESTING PSNR AUDIO WAV

Original Audio			**Audio Results**			**Test result**	
Song title	**Size (KB)**	**P0**	***Song title***	***Size (KB)***	***P1***	***subjective***	***PSNR***
one country one nation.wav	6459632	-16.7474	Concealment1.wav	6459632	-16.7474	Good	Inf
			Concealment 2.wav	6459632	-16.7474	Good	Inf
			Concealment 3.wav	6459632	-16.7474	Good	Inf
			Concealment 4.wav	6459632	-16.7474	Good	Inf

In table 6 can be seen, PSNR values obtained in the first to last audio is not visible, it is because no changes were found in the value of P1 and P0. Then all the better audio results.

From the above test results can be analyzed at concealment, the larger the file size that is hidden, the greater the time required. And audio results obtained sizenya unchanged. While at the time the greater extraction extract the file size, the greater the time required. And results files are extracted as file hiding. The length of time extracting much faster than on concealment. In testing the PSNR, there are linkages between PSNR objective with subjective values. The greater the value of PSNR is objeyektif the better the audio quality subjectively. If the value of PSNR obtained less than 30 dB it will sound very disturbing to the audio output if heard by the human ear. PSNR itself affected by two things: the size of the hidden message and steganography media structure. In this journal WAV audio concealment are better quality than the

MP3. And the shape of the hidden files either docx, pdf, .xlsx, and .pptx no effect.

V. CONCLUSION

When concealment, the larger the file size that is hidden, the greater the time required. Results concealment sizenya audio unchanged. when extracting the larger the file size the extract, the greater the time required. And results files are extracted as file hiding.

The length of time extracting much faster than on concealment. WAV audio PSNR values are better quality than the MP3. And the shape of the hidden files either docx, pdf, .xlsx, and .pptx no effect.

References

[1] Prima, Nikken and Bahtiar, Nurdin, "*Kriptografi Hill Chiper dengan Menggunakan Operasi Matriks"* in Seminar Nasional Ilmu Komputer Universitas Diponegoro ,2010 . ISSN 978-602-97737-0-5J.

[2] Nikken Prima Puspita., 2013. Kriptografi Hill Cipher Dengan Menggunakan Operasi Matriks. Universitas Diponegoro.

[3] Y. Kurniawan., Kriptografi Keamanan Internet dan Jaringan Telekomunikasi, Bandung: Informatika, 2004

[4] Munir, Rinaldi., 2004. *Kriptografi.* Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.

[5] Lovebbi, Dodick Z.S.," Rancang Bangun Aplikasi Steganografi dengan Metode Least Significant Bit di Audio pada Sistem Operasi Android", library.umn.ac.id, ISSN 2085-4552,Mei.2012.

[6] Guslita, Marsha., 2016. Aplikasi Enkripsi dan Deskripsi sebagai Keamanan Data dan SMS menggunakan Metode Vigenere chiper berbasis Android

[7] Yoga BP, dkk., 2012. Implementasi Kriptografi dan Steganografi pada File Audio Menggunakan Metode DES dan Parity Coding