Journal of Computer Science 10 (7): 1249-1252, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1249.1252 Published Online 10 (7) 2014 (http://www.thescipub.com/jcs.toc)

STEGANOGRAPHY APPLICATION PROGRAM USING THE ID3V2 IN THE MP3 AUDIO FILE ON MOBILE PHONE

Afan Galih Salman, Rojali, Bayu Kanigoro and Nayoko

Computer Science Program, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia

Received 2014-01-22; Revised 2014-01-31; Accepted 2014-02-21

ABSTRACT

The MPEG Layer-III File or MP3 can contain the ID3v2 tag which able to store information not only the song and singer's name but also song lyric and alblum cover figure. The steganography technique on audio generally only make use of the main body of the audio file, but has not ever use the part of the ID3v2 to hide an message. This study an steganography technique which make use of this ID3v2 tag space where message is encrypted using McEliece cryptosystem method which applying the public key in the form of matrix then inserted into the MP3 file applying Before All Frames (BAF) method, whereas the public key is inserted into album cover figure which is stored in the ID3v2 tag.

Keywords: MP3, ID3v2 Tag, McEliece Cryptosystem, Before All Frames

1. INTRODUCTION

Steganography comes from the Greek "stego" which means closed and "Graphia" which means writing. Steganography is the art and science of hiding the fact ongoing communication (Krenn, 2004).

One of the triggers in steganography technic development is steganalis attack which is succesful cracking message that hidden by using the widely known stegnogrphy method. It encourage a desire to find an alternative of the message hiding method that has never been thought before.

Most of the traditional methods available today use the pixel bits of an image to hide information and are limited in terms of hiding capacity (Raphael and Sundaram, 2012).

Other research developed an application which can check the Email content of corporate mails by S-DES algorithm along with the neural networks back propagation approach. A new filtering algorithm is also developed which can used to extract only the JPG images from the corporate emails. Experimental research shows that this algorithm is more accurate and reliable than the conventional methods (Anitha, 2012).

This journal would show an alternative method design of steganography which make use of the ID3v2 tag contained on MP3 file . The ID3v2 Tag is used on audio file for storing the additional datasuch as the information of singer's name, song title, album title, even the album cover figure (Nilsson, 1999). It open the possibility that the ID3v2 can be used for hiding a message. On this design, the MP3 file is chosed as file stego due to the MP3 file format has been widely known and has very highly traffic in Internet so that it would not arouse suspicion that there is a hidden message within the file.

The message concealment in the audio file use the Before All Frames (BAF) method where the message partition is hidden before each the MP3frame so that the mesaage can be hidden without spoil the sound quality,therefor this method selected to be used in this design (Atoum *et al*., 2011). As additional security this design apply McEliece cryptosystem which use the relative huge matrix as public key. The this matrix is also hidden in audio file (Cherowitzo, 2002).

In addition to these arrangement, recently the information technology really brings out mobile aspect, therefore this designed audio steganography programme make use of Android mobile platform which also prove that mobile platform can be applied to run steganography program. Android is open-source software toolkit for mobile device developed

Corresponding Author: Afan Galih Salman, Computer Science Program, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia

by Google and Open Handset Alliance (Burnette, 2010). Mobile platform such as android can be used to run steganography programs (Shahreza, 2005).

2. THE ARCHITECTURE SYSTEM

The required program is the audio steganography application program which is running on Android operation system. Broadly speaking the designed program is described as follow:

The operated program able to carry out the two main tasks: Message encryption and decryption shown in **Fig. 1**. When encrypt message, the user shall choose the message that will be inserted and the core file where the message will be inserted in order to produce the file stego that can be sent to the addressee. Conversely, in decryption process user shall select the file stego to read the hidden message.

In technical aspect, the proposed steganography technique requires a message string that will be inserted and a MP3 that contained Tag ID3v2 in the form of the album cover figure as a medium.

In this designed program, firstly the message shall be encrypted by using McEliece cryptosystem method which apply public key that take the form of matrix. Subsequently the encrypted message is inserted to the MP3 file by using the Before All Frames (BAF) method where message partition stored in each before the MP3 file frame MP3, whereas the public key is inserted into the album cover figure stored in the ID3v2 tag by using Least Significant Bit (LSB) method (Krenn, 2004). Alternatively, the encrypted message can be also stored in the ID3v2tag whereas the public key stored in each before the MP3 frame.

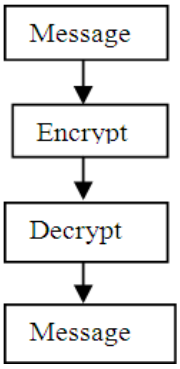

Fig. 1. Steganograpfy flowchart

3. THE DESIGN

This study used a waterfall model as software development life cycle. Water fall model with five stages, namely: Communication, planning, modeling, construction and deployment (Pressman, 2010).

This steganography program design in broad terms is divided into some stages as follow:

- Designing MP3 application program by using Android
- Applying the steganografi BAF technique and McEliece to application program
- Designing steganography application program along with screen display

The designed program able to operate two main task that are Message Encryption and Decryption. The basic algorithm of encryption process (encoding) for the designed program shall be as follow shown in **Fig. 2**.

As for the basic algorithm of decryption process (decoding) for the designed program shall be as follow shown in **Fig. 3**.

Examples of display application on mobile device shown in **Fig.4.**

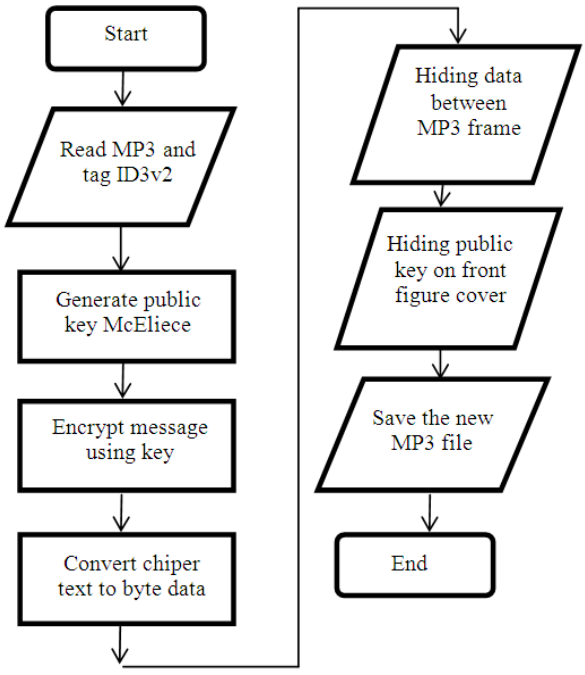

Fig. 2. Encryption process

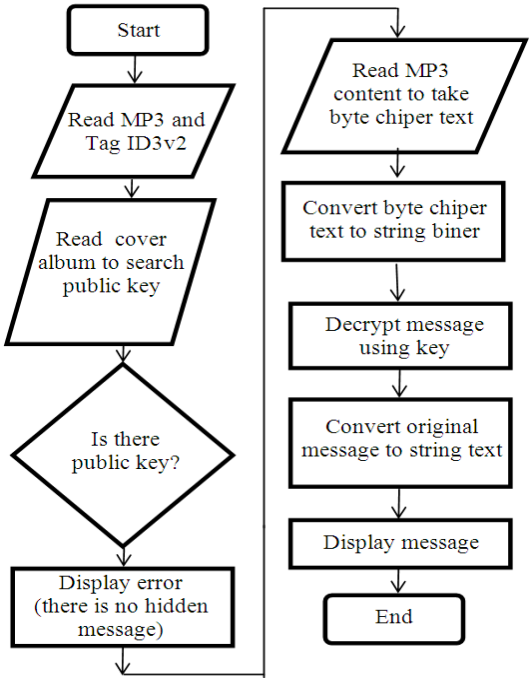

Fig. 3. Decryption process

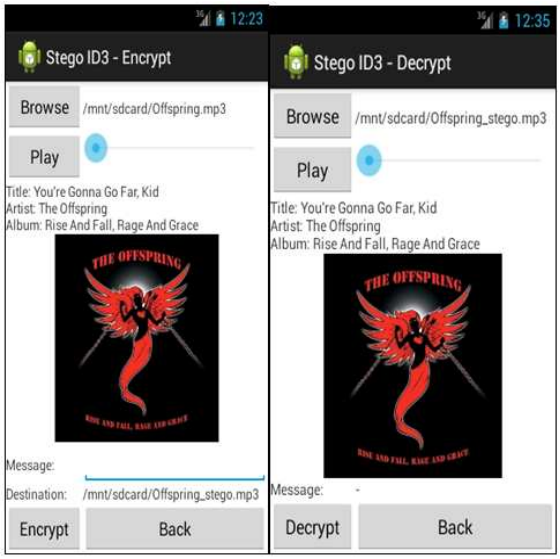

Fig. 4. Display application on mobile device

4. RESULTS

Usage test of this steganography application program resulting in the message can be inserted to the MP3 file and after decrypt the message can be read perfectly without any slightest change.

Table 1. File MP3

File name	File size (bytes)	Duration	Frame count	Max capacity (bytes)
Offspring.mp3	5116216	2:57	7142	3571
Sindentosca.mp3	3704908	3:46	9087	4543
Mars.mp3	5853312	4:03	9885	4942
Santana.mp3	5132520	5:19	12757	6378
Jason.mp3	3305472	3:26	8625	4312
Lucky.mp3	10020163	4:08	9453	4726
Call.mp3	6067586	4:00	10745	5372
Roads.mp3	9221496	3:49	9363	4681

Table 2. String message

No.	Message string	Message size (bytes)
-1	Hello world!	24
-2	Attack the hill at seven	48
-3	The quick brown fox jumps over the lazy dog	88
-4	X:34.2 Y:11.4 35	32

Based on human hearing the sound is not changed at all, there is no any disturbing spoiled sound such as noise or crackling. The sound quality doesn't change because the sound is inserted outside the reach of the existing MP3 frames so that it does not change composition of the sound data raw at all.

To see the influence of message inserting process on the main file, the writer try to carry out embedding process in some MP3 file and apply some different message string to be inserted. The following **Table 1** is the information table of the applied MP3 file and **Table 2** is the information table of the inserted message string.

The following is table of the program evaluation result with the MP3 file input and message string according to the above tables. The **Table 3** shows the file size after the message has been inserted, whereas **Table 4** shows the duration of embedding time.

The **Table 1** implies that the maximum capacity of every MP3 file is influenced by the amount of frames contained in the MP3 file body. The character amount (byte) that can be stored is a half of the existing frame amount. It because the cryptography method McEliece with Hamming (Shahreza, 2005) that is applied resulting in cipher text that is twice bigger than the original message.

The **Table 3 and 4** imply that inserting process of the 24-88 byte message into the 3-5 MB MP3 file takes 2000-3000 milliseconds, but it is not depend on the file size, the frame amount or the long of message. Meanwhile, the size of the resulted stego file approximately is the size of the original file added by twice of the message long.

Table 3. Stego file size

		Stego file size (bytes)			
File name	File size (bytes)	-1	-2	-3	-4
Offspring.mp3	5116216	5116249	5116278	5116326	5116254
Sindentosca.mp3	3704908	3704939	3704967	3705027	3704950
Mars.mp3	5853312	5853345	5853375	5853428	5853356
Santana.mp3	5132520	5132552	5132579	5132628	5132562
Jason.mp3	3305472	3305502	3305534	3305588	3305518
Lucky.mp3	10020163	10020195	10020224	10020271	10020207
Call.mp3	6067586	6067619	6067645	6067698	6067626
Roads.mp3	9221496	9221527	9221558	9221608	9221538

Table 4. Embedding time

	Embedding time (ms)			
File name	-1	-2	-3	-4
Offspring.mp3	2496	2339	2478	2409
Sindentosca.mp3	2035	1976	2621	2388
Mars.mp3	3154	3159	2655	2841
Santana.mp3	2464	2676	2515	2771
Jason.mp3	2259	2122	2045	2533
Lucky.mp3	2636	2203	2443	2529
Call.mp3	2344	2086	2506	2607
Roads.mp3	2103	2431	2796	2489

5. CONCLUSION

- The ID3v2 Tag on MP3 file can be used in the steganography technique on audio file.
- The mobile steganography application program to hide message in this MP3 ID3v2 tag is designed by combining BAF (Before All Frames) steganography technique with McEliece cryptosystem so that message and public key can be hidden in the ID3v2 tag and the body of MP3 file itself
- Using the designed method the message can be well hidden, without spoil the sound quality in the least, with the size of file change unobtrusively, take the relative short time and message can be perfectly decrypted

6. REFERENCES

Anitha, P.T., M. Rajaram and S.N. Sivanandham, 2012. A hybrid approach for detecting stego content in corporate mail using neural network based simplified-data encryption standard algorithm. Am. J. Applied Sci., 9: 766-771. DOI: 10.3844/ajassp.2012.766.771

Atoum, M.S., O.A. Al-Rababah and A.I. Al-Attili, 2011. New technique for hiding data in audio file. Int. J. Comput. Sci. Netw. Security, 11: 173-177.

Burnette, E., 2010. Hello android: Introducing Google's Mobile Development Platform. 3rd Edn., The" Pragmatic Bookshelf, Raleigh, ISBN-10: 1934356565, pp: 293.

Cherowitzo, B., 2002. M5410 Mc.Eliece Cryptoststem. Website of Bill Cherowitzo, University of Colorado at Denver.

Krenn, J.R., 2004. Steganography and steganalysis.

Nilsson, M., 1999. ID3 Tag Version 2.3.0. Informal Standard Document for ID3 Tag.

Pressman, R.S, 2010. Software Engineering: A Practitioner's Approach. 7th Edn., McGraw-Hill Higher Education, New York, ISBN-10: 0073375977, pp: 928.

Raphael, A.J. and V. Sundaram, 2012. New approaches to ancient crypto-steganography methods. Am. J. Applied. Sci., 9: 40-46. DOI: 10.3844/ajassp.2012.40.46

Shahreza, M.S., 2005. An improved method for steganography on mobile phone. Allameh Helli Pre-University.