TIFDA JOURNAL
Technology Information and Data Analytic
Journal Website : http://jeptira.id/index.php/tifda
e-ISSN : 3064-0660

Steganography on MP3 Audio files to secure messages using the Least Significant Bit (LSB) and Advanced Encryption Standard (AES) methods

Steven Blanco[1*], Adam Arif Budiman[2*]
[1,2] Information Technology Department, Darma Persada University
[1,2] Jl. Taman Malaka Selatan No 8, East Jakarta, 13450, Indonesia
*ariadam@gmail.com

Abstract — The E-budgeting file code delivery system is one of the right choices for a company to send and store large amounts of data neatly and properly. Currently, Bank XYZ has not yet implemented an Android-based file delivery and storage system, resulting in difficulties in locating previously sent files. To address this issue, Bank XYZ has developed an E-budgeting file code delivery system. This system is Android-based and operates using Android smartphones online. It is also designed to securely store files using AES (Advanced Encryption Standard) encryption and LSB (Least Significant Bit) steganography methods. The purpose of the E-budgeting file code delivery system is to facilitate the secure transmission of these codes to the relevant parties.

Keywords – E-budgeting code, Advanced Encryption Standard, Least Significant Bit, Steganography.

I. INTRODUCTION

A bank is a financial intermediary institution, generally established with the authority to accept deposits, lend money, and issue promissory notes or banknotes [1]. In conducting banking activities, there are several processes that must be carried out. In this case, Bank XYZ also has a process for providing budgets to other regions (Bank XYZ branches, of which there are 18 locations that handle this). One of these processes involves sending an E-budgeting code (an electronic budget preparation system).

The problem encountered was that when the head office sent a letter to the regional office, the letter was supposed to be known only to the regional office concerned, but often there were leaks regarding the code, which resulted in parties without authority deliberately debiting the budget. Due to this problem, an Android application was needed to secure the code, where there were user accounts for all regions to send the E-budgeting code secretly.

The technique of keeping messages confidential is not limited to cryptography [2]. There is another technique that has been used for centuries, namely steganography. Steganography is the science and art of hiding secret messages within other messages so that the existence of the secret message cannot be detected [3].

Steganography comes from the Greek word “steganos,” which means “hidden writing.” Steganography is very different from cryptography [4]. While cryptography conceals the meaning of a message while its existence remains intact, steganography conceals the existence of the message itself [5]. In previous studies, LSB was used because it inserts data into the least significant bits of image pixels. The bit changes are so small that they are undetectable to the human eye and do not affect the image results [6].

Another method for maintaining message confidentiality is encryption. Encryption is the process of securing information by converting it into a format that cannot be read without a specific key. The goal is to protect data from unauthorized access, both when the data is stored (data at rest) and when it is being transmitted (data in transit). One symmetric algorithm with fast operations is the Advanced Encryption Standard (AES) [7][8]. In this study, the AES (Advanced Encryption Standard) method was used, which is a widely popular and widely used symmetric cryptographic algorithm for securing digital data. AES

was established as an encryption standard by the NIST (National Institute of Standards and Technology) in 2001, replacing the DES (Data Encryption Standard), which was deemed no longer secure [9].

Development Method System

In this study, the application development method used is the waterfall method, which is one of the most classic and structured software development process models. The flow is as shown in the Figure 1.

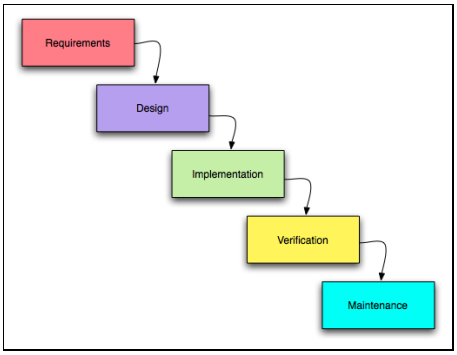

Figure 1. Waterfall method

Use steganography and encryption

This study combines steganography and encryption. In steganography, messages are "hidden" by replacing or adding bits. This bit replacement is known as the Least Significant Bit (LSB) input for each sampling with the encoded data. Meanwhile, encryption is used to "disguise" the messages being sent. In this study, AES is used. The AES algorithm operates on symmetric ciphertext blocks that can encrypt (encipher) and decrypt information [10]. The AES algorithm uses the Rijndael algorithm with cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data.

The system development flow is shown in Figure 2, which is the general flow, and Figure 3 shows the detailed flow below.

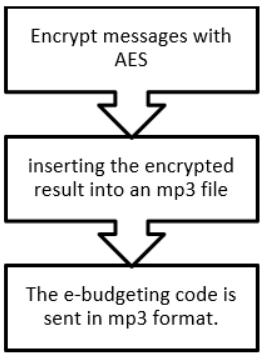

Figure 2. The process of creating encrypted and steganographic files

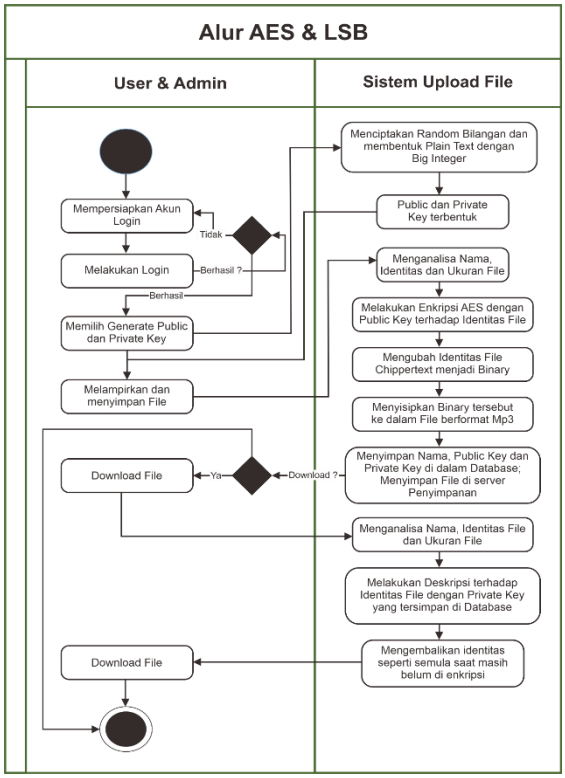

Figure 3. Detailed flow

RESULTS AND DISCUSSION

When the application is first launched, the main login page is used to verify the user, whether the user is an admin or a user, as shown in Figure 4 below.

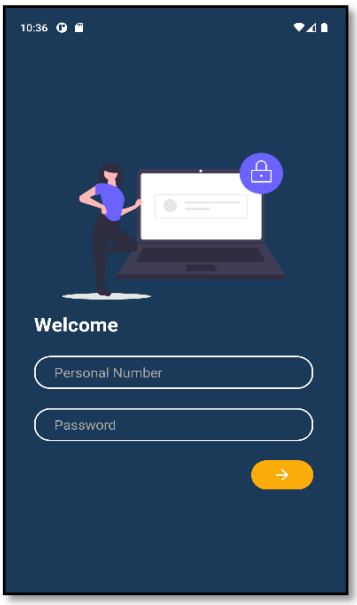

Figure 4. Login Menu

Continue with main menu for uploading files to be encrypted, as shown in Figure 5 below.

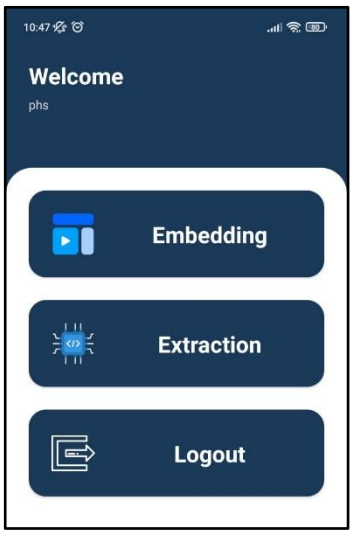

Figure 5. Main menu

The MP3 file will be uploaded via the embedding menu, which is used as a "*carrier*" file for the code, as shown in Figure 6 below. This is followed by filling in the secret message in the form of an e-budgeting code with a password that works with the AES and LSB algorithms. Then click the hide button to save it to the database, so that the data can be sent to the user by accessing the database.

Figure 6. Upload file Menu

On the *Extraction* menu, users decrypt encrypted files. This page is quite simple; users just need to attach the encrypted file, then enter the key or password. After that, click the *READ FILE* button and the message will be readable, as shown in the display menu in Figure 7.

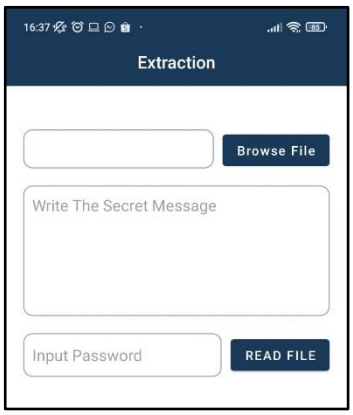

Figure 7. Read message or file

The test was conducted by comparing the size of MP3 files before and after encryption and steganography processes. The test results are shown in the table below.

Table 1. Testing

No	Isi Pesan Rahasia	Hasil AES	Key	Ukuran File Enkripsi		Durasi
				Sebelum	Sesudah	
1	uji coba pertama	cGorJNX6uMYJ5O/uWEgJo7JiLZGaOcrOnbWiCe/vI/E=	12345	859 KB	839 KB	1,1 Detik
2	coba sembunyikan	MMvq6LN61j0P/ZSUhniApm9RPs85copOT17LKZVQ0hg=	aku123	415 KB	406 KB	0,4 Detik
3	ini pesan rahasia	vYRSttJSfyMvcCHT2AlAbgnyaGCVO7+Pbx0obCwO/U4=	5123	415 KB	406 KB	0,2 Detik
4	rahasia sekali	9xZcSIi5iHJkcuMvl1XoaA==	saya67	2,84 MB	2,84 MB	2,1 Detik
5	harga saham sekarang	AEcGf3f6snib1gXS7VMCktFBfr3SZSEfNLTqsv4MrEI=	89pio	2,70 MB	2,70 MB	2,1 Detik
6	kenaikan gaji karyawan	v89BHfXsWyslmZ1a+Axend0U2uS0f7CD454g/L2smCg=	secret	675 KB	651 KB	0,4 Detik
7	pengeluaran hari ini	9AiKvppgBS3Fm0iMf7JJlXeXaVquTyZUuYfpyd2h6iQ=	5012	3,95 MB	3,95 MB	2,5 Detik
8	pendapatan hari ini ada	uwudPErtB1ewYGCf8am9cv8a4OetLKAYmPshsYnQOXc=	goals	6, 13 MB	6, 13 MB	3,2 Detik
9	perubahan kebijakan kerjasama	wDeu+Km/gcnEb75BZvlyHzTc+pQiE3gAvba87VWdgvA=	kebijakan	9,14 MB	9,14 MB	4,7 Detik
10	uji coba aplikasi	bzoFOz6Ua4pUGUDkypqNio0ECwRUXuRZ0QzpRCnqbBM=	9876	1,32 MB	1,32 MB	1,2 Detik

The table below compares the binary code of an MP3 file before and after encryption. Since the binary code in an MP3 file is very large, only a portion of the binary code is displayed.

Table 1. Comparison of binary encryption

Perbandingan Binary Enkripsi	
Sebelum	Sesudah
"11100111	"11100110
"1100010",	"1100011",
"10100011	"10100010
"11111001	"11111001
"10101001	"10101001
"11011101	"11011101
"10110110	"10110111
"10101100	"10101100
"1111011",	"1111011",
"10101110	"10101110
"111111",	"111111",
"11111110	"11111111
"11001000	"11001000
"110001",	"110001",
"0",	"1",
"0",	"1",
"11110000	"11110001
"0",	"1",
"1000000",	"1000000",
"1101001",	"1101000",

CONCLUSION

This application provides a sense of security when sending confidential files that are only intended to be viewed by administrators or certain individuals who have been granted access rights and this application is an android-based application. However, it can also be developed as a web-based application.

This app can only hide text data up to 1000 characters. To achieve maximum and fast results in the encryption process, the MP3 files used must have a minimum capacity of 6.5 Kb to 5 Mb.

REFERENCES

[1] K. Sonin, "Economics of banks and financial markets (Nobel Memorial Prize in Economic Sciences 2022)," Voprosy Economiki, no. 2, pp. 5–17, Feb. 2023, doi: 10.32609/0042-8736-2023-2-5-17.

[2] Lovebbi, D. Z. Sudirman. 2012. "Rancang Bangun Aplikasi Steganografi dengan Metode Least Signicant Bit di Audio pada Sistem Operasi Android". Ultimatics, Vol 4, No 1. 7-16.

[3] M. S. Atoum, "NEW TECHNIQUE FOR HIDING DATA IN AUDIO FILE", 2011.

[4] Fachmi Salim,"KRIPTOGRAFI PADA FILE AUDIO MP3 MENGGUNAKAN METODE PENGEMBANGAN TRANSPOSISI", Prosiding Seminar Ilmu Komputer dan Teknologi Informasi Vol. 1, No. 1, September 2016

[5] Paramita dkk,"Kriptografi Audio MP3 Menggunakan RSA dan Transposisi Kolom", JURNAL RESTI,Vol. 5 No. 3 (2021) 483 – 488

[6] Chaerul Umam,"Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna",2st Proceeding STEKOM 2022, Volume 2 No 1 2022 E-ISSN: 2809-1566 P-ISSN: 2809-1574.

[7] Y. Kim and S. C. Seo, "Efficient Implementation of AES and CTR_DRBG on 8-Bit AVR-Based Sensor Nodes," IEEE Access, vol. 9, pp. 30496–30510, Feb. 2021, doi: 10.1109/ACCESS.2021.3059623.

[8] Z. Wang, S. Wei, G.-L. Long, and L. Hanzo, "Variational quantum attacks threaten advanced encryption standard based symmetric cryptography," Science China Information Sciences, vol. 65, no. 10, Jul. 2022, doi: 10.1007/s11432-022-3511-5.

[9] A. Menezes and D. Stebila, "The Advanced Encryption Standard: 20 Years Later," vol. 19, no. 6, pp. 98–102, Oct. 2021, doi: 10.1109/MSEC.2021.3107078.

[10] R. Ueno et al., "High Throughput/Gate AES Hardware Architectures Based on Datapath Compression," IEEE Transactions on Computers, vol. 69, no. 4, pp. 534–548, Apr. 2020, doi: 10.1109/TC.2019.2957355.