Implementasi Teknik Kriptografi dan Steganografi pada Aplikasi Android

Muhammad Arief Ismirianda[1], Setia Juli Irzal Ismail[2], Anang Sularsa[3]

[1, 2, 3]Prodi D3 Teknologi Komputer, Fakultas Ilmu Terapan, Universitas Telkom

[1]mariefismirianda@student.telkomuniversity.ac.id, [2]jul@tass.telkomuniversity.ac.id,

[3]ananks@gmail.com

Abstrak- Secara umum ada 3 teknik untuk mengamankan data, yaitu kriptografi, steganografi dan watermarking. Pada Kriptografi, data atau informasi akan diamankan dengan menyandikan informasi tersebut sehingga makna aslinya tidak dapat diartikan langsung oleh orang. Data yang dihasilkan dapat dilihat mata manusia secara visual, tetapi makna aslinya tidak diketahui. Karena itulah akan muncul kecurigaan kepada orang yang melihat hasil kriptografi. Teknik Steganografi akan mengamankan data asli dengan menyembunyikan data pada objek tertentu sehingga data tidak dapat dilihat secara visual. Berbeda dengan kriptografi, data yang disimpan menggunakan Teknik steganografi tidak akan menimbulkan kecurigaan dikarenakan penyembunyian data dilakukan pada media lain. Media tersebut bisa berupa citra, audio maupun video. Kedua teknik ini diterapkan pada aplikasi berbasis android sehingga mudah digunakan. Pada aplikasi yang diterapkan, pengguna memasukkan data atau informasi yang ingin diamankan. Kemudian data tersebut diberi sebuah password yang kemudian akan disandikan dengan teknik kriptografi. Hasil kriptografi tersebut kemudian dibungkus dengan media citra sehingga data tersebut tidak bersifat mencurigakan. Pada aplikasi ini, pengguna juga bisa mengembalikan data yang tadi sudah diamankan dengan memasukkan password yang telah dimasukkan sebelumnya pada media steganografi tersebut. Pada penelitian yang telah dilakukan, ada beberapa faktor yang memengaruhi performansi kriptografi dan steganografi, seperti spesifikasi perangkat, kualitas citra, hingga panjang pesan yang disisipkan pada citra.

Kata Kunci: Kriptografi, Steganografi, Android

Abstract- *In general, there are 3 techniques for securing data, that is cryptography, steganography and watermarking. In cryptography, data or information will be secured by encoding the information so that the original meaning cannot be interpreted directly by people. The resulting data can be seen visually by the human eye, but the original meaning is unknown. That's why suspicion will arise for people who see cryptographic results. Steganography technique will secure the original data by hiding data on certain objects so that data cannot be seen visually. Different from cryptography, stored data using steganography techniques will not cause suspicion due to data hiding on other media. The media can be an image, audio or video. Both of these techniques applied to an Android-based application so that they are easy to use. In the application that is applied, the user enters the data or information that he wants to secure. Then the data is given a password which will then be encoded by cryptographic techniques. The cryptographic results are then wrapped in an image so that the data is not suspicious. In this application, the user can also restore the data that was previously secured by entering the password that previously entered on the steganography image. In this research, there are several factors that influence cryptographic and steganographic performance, such as device specifications, image quality, and also the length of messages inserted in the image.*

Keywords: Cryptography, Steganography, Android

1. Pendahuluan

1.1 Latar Belakang

Secara umum ada 3 teknik untuk mengamankan data, yaitu kriptografi, steganografi dan watermarking. [1] Pada kriptografi, data atau informasi akan diamankan dengan menyandikan informasi tersebut sehingga makna aslinya tidak dapat diartikan langsung oleh orang. Data yang dihasilkan dapat dilihat mata manusia secara visual, tetapi makna aslinya tidak diketahui. Karena itulah akan muncul kecurigaan kepada orang yang melihat hasil kriptografi. Teknik Steganografi akan mengamankan

data asli dengan menyembunyikan data pada objek tertentu sehingga data tidak dapat dilihat secara visual. Berbeda dengan kriptografi, data yang disimpan menggunakan Teknik steganografi tidak akan menimbulkan kecurigaan dikarenakan penyembunyian data dilakukan pada media lain. Media tersebut bisa berupa gambar, audio maupun video.

Kedua teknik ini diterapkan pada aplikasi berbasis android sehingga mudah digunakan. Pada aplikasi yang diterapkan, pengguna memasukkan data atau informasi yang ingin diamankan. Kemudian data tersebut diberi sebuah password yang kemudian akan disandikan dengan teknik kriptografi. Hasil kriptografi tersebut kemudian dibungkus dengan media lain sehingga data tersebut tidak bersifat mencurigakan. Pada aplikasi ini, pengguna juga bisa mengembalikan data yang tadi sudah diamankan dengan memasukkan password yang telah dimasukkan sebelumnya pada media steganografi tersebut.

1.2 Rumusan Masalah

Rumusan masalah dalam penulisan proyek akhir ini adalah sebagai berikut:

1. Bagaimana cara mengkombinasikan teknik kriptografi dan teknik steganografi?
2. Bagaimana performa kedua teknik ini pada aplikasi android?

1.3 Tujuan

Tujuan pengambilan proyek akhir ini adalah sebagai berikut:

1. Melakukan proses kriptografi pada sebuah pesan dan proses steganografi pada media citra aplikasi android.
2. Mengetahui performa algoritma kriptografi dan steganografi yang digunakan pada aplikasi android.

1.4 Batasan Masalah

Batasan masalah yang digunakan dalam pembuatan proyek akhir ini adalah sebagai berikut:

1. Hanya menggunakan metode kriptografi *Advanced Encryption Standard* (AES).
2. Hanya menggunakan metode steganografi Least Significant Bit(LSB).
3. Menggunakan smartphone berbasis Android dalam pengimplementasiannya.
4. Dapat mengamankan, menyembunyikan serta mengembalikan data yang sudah diamankan.
5. Data disembunyikan pada media citra yang diinginkan.
6. Data berupa pesan teks.

2. Tinjauan Pustaka

2.1 Peneliti Sebelumnya

Pada penelitian yang dilakukan sebelumnya [2] hanya melakukan proses steganografi saja tanpa melakukan proses kriptografi terlebih dahulu sehingga keamanan data masih kurang. Selain itu, pada proyek akhir tersebut, teknik steganografi hanya dilakukan pada sebuah program Java sederhana dan dengan metode LSB (*Least Significant Bit*) yang mana dengan cara menyisipkan teks pada bit terakhir di media citra.

Pada penelitian tersebut masih memiliki banyak kelamahan, terutama pada segi keamanannya. Data yang sudah diamankan tadi masih sangat mudah untuk dilacak dengan teknik steganalisis dikarenakan hanya menyembunyikan datanya saja tanpa mengamankannya terlebih dahulu. Selain itu, metode yang digunakan, yaitu LSB memiliki kekurangan pada ukuran data yang bisa disembunyikan. Karena, pada metode ini hanya bisa menyembunyikan data yang lebih kecil dari ukuran citranya.

Pada proyek akhir ini, kelemahan-kelemahan tersebut akan diatasi. Selain itu juga, pengguna akan dipermudah dengan pengimplementasiannya pada aplikasi android.

2.2 Teori

2.2.1 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

Kriptografi berkembang sedemikan rupa sehingga tidak lagi sebatas mengenkripsi pesan, tetapi juga memberikan aspek keamanan yang lain. [3]

Ada dua istilah pada kriptografi, yaitu enkripsi dan dekripsi.

1) Enkripsi (encryption): proses menyandikan plainteks menjadi cipherteks.
2) Dekripsi (decryption): Proses mengembalikan cipherteks menjadi plainteks semula.

2.2.2 Steganografi

Kata steganography (steganografi) berasal dari bahasa yunani yaitu steganos, yang artinya “menyembunyikan”, dan graptos yaitu “tulisan”. Steganografi adalah ilmu pengetahuan dan seni dalam menyembunyikan komunikasi. Suatu sistem steganografi sedemikian rupa menyembunyikan isi suatu data di dalam suatu sampul media yang tidak dapat di duga oleh orang biasa sehingga tidak membangunkan suatu kecurigaan kepada orang yang melihatnya. [2]

2.2.3 Smartphone

Smartphone adalah sebuah telepon genggam yang memiliki fitur atau kemampuan tingkat tinggi, sering kali dalam penggunaanya menyerupai komputer. Fitur - fitur yang dapat ditemukan pada smartphone antara lain telepon, sms, internet, mengedit dokumen dan masih banyak lagi yang lainnya. Pengguna juga dapat menambahkan aplikasi lain kedalam smartphone layaknya memasang aplikasi pada komputer. [4]

2.2.4 Android

Android adalah sebuah sistem operasi untuk perangkat mobile yang mencakup sistem operasi, *middleware* (perangkat lunak penghubung system operasi) dan aplikasi. Android merupakan system operasi berbasis linux dan bersifat *open source* (sumber terbuka) sehingga bisa dikembangkan oleh siapapun secara gratis. [5]

2.2.5 Least Significant Bit

Metode steganografi LSB adalah teknik yang umum digunakan dalam enkripsi dan dekripsi informasi rahasia. Cara kerja metode LSB yaitu dengan mengubah bit redundan gambar pembungkus yang tidak berpengaruh signifikan dengan bit dari pesan rahasia. [2]

Metode ini memiliki beberapa kelebihan, antara lain:

1. Tidak mudah dilihat dengan mata telanjang.
2. Mudah diimplementasikan.
3. *High perpetual transparency*.

Selain itu, metode ini juga memiliki beberapa kekurangan, sebagai berikut:

1. *Robustness*.
2. Sensitif terhadap perubahan gambar, seperti rotasi atau perubahan ukuran gambar.

2.2.6 Advanced Encryption Standard

Algoritma AES merupakan algoritma simetris yaitu mengunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192 dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap proses putaran. [6]

Proses putaran enkripsi AES-128 dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

1. *Addroundkey*.
2. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah: *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*.
3. Final round, adalah proses untuk putaran terakhir yang meliputi *SubBytes*, *ShiftRows*, dan *AddRoundKey*.

Pada proses dekripsi AES-128, proses putaran juga dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

4. *Addroundkey*.

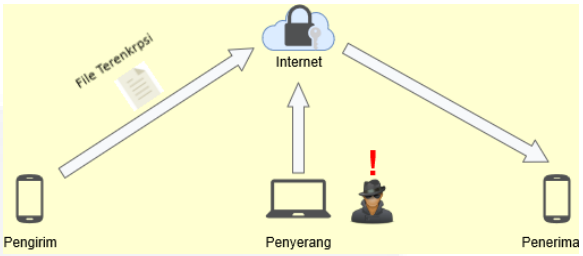
5. Putaran sebanyak a-1 kali, dimana pada setiap putaran dilakukan proses: *InverseShiftRows*, *InverseSubBytes*, *AddRoundKey*, dan *InverseMixColumns*.
6. *Final round*, adalah proses untuk putaran terakhir yang meliputi *InverseShiftRows*, *InverseSubBytes*, dan *AddRoundKey*.

Pada enkripsi dan dekripsi AES-192 proses putaran dikerjakan 12 kali (a=12), sedangkan untuk AES-256 proses putaran dikerjakan 14 kali (a=14). [7]

3. Analisis dan Perancangan

3.1 Analisis

3.1.1 Gambaran Sistem Saat ini



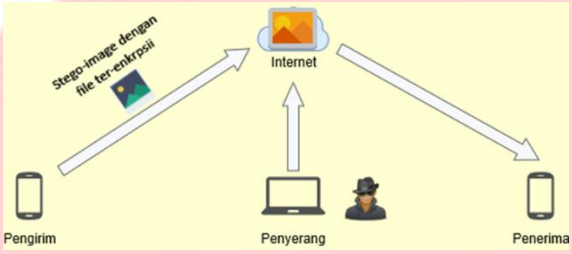
Gambar 3.1 Gambar Sistem Saat Ini

Pada gambar di atas merupakan proses pengiriman data terenkripsi yang dilakukan dari suatu perangkat ke perangkat lainnya. Di sisi lain, ada yang mencoba melakukan penyadapan atau sniffing pada jaringan tersebut. Melihat kecurigaan akan file yang dikirimkan, penyerang mencoba untuk mencuri data tersebut.

Dengan menerapkan Teknik steganografi pada data tersebut, keamanan data menjadi ditingkatkan. Data yang sebelumnya terlihat mencurigakan, diminimalisasi dan terlihat biasa saja sehingga akan diabaikan oleh penyerang.

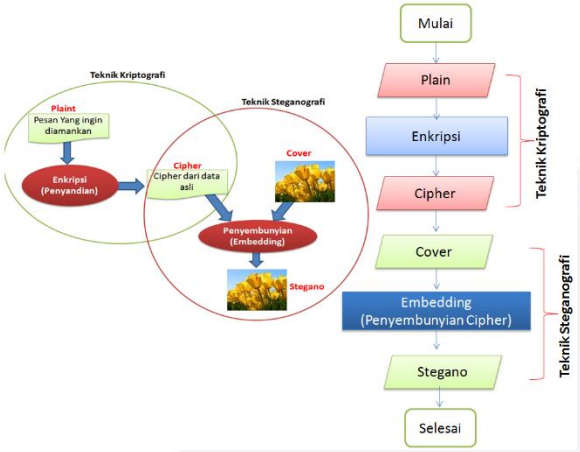
3.2 Perancangan

3.2.1 Gambaran Sistem Usulan



Gambar 3.2 Gambar Sistem Usulan 1

Pada gambar di atas, data yang sudah diamankan sebelumnya dikirimkan melalui internet tanpa menimbulkan kecurigaan. Sehingga data tersebut diabaikan oleh penyerang.



Gambar 3.3 Gambaran Sistem Usulan 2

Gambar di atas merupakan tahapan yang dilakukan pada aplikasi. Data yang akan diamankan dienkripsi terlebih dahulu menjadi chiperteks. Kemudian data yang sudah diamankan tersebut disembunyikan di dalam sebuah media gambar sehingga data tersebut tidak tampak lagi seperti data.

Tahapan Enkripsi

```
Begin
Input: Cover_Image, Secret_Message, Secret_Key;
Transfer Secret_Message into Text_File;
Zip Text_File;
Convert Zip_Text_File to Binary_Codes;
Convert Secret_Key into Binary_Codes;
Set BitsPerUnit to Zero;
Encode Message to Binary_Codes;
Add by 2 unit for bitsPerUnit;
Output: Stego_Image;
End
```

Gambar 3.4 Algoritma Penyisipan Pesan

Sistem yang dibangun menerapkan algoritma yang dikembangkan oleh Rosziati Ibrahim and Teoh Suk Kuan. [8] Pada algoritma tersebut, diharuskan untuk menyiapkan input berupa citra pembungkus, pesan rahasia, dan kunci rahasia. Pesan yang diinputkan akan disimpan ke dalam sebuah berkas bertipe teks. Berkas tersebut akan disimpan ke dalam berkas zip sehingga lebih sulit untuk dideteksi. Berkas zip yang sudah dibuat sebelumnya akan dikonversi menjadi kode-kode biner bersamaan dengan kunci rahasia. Dua digit terakhir setiap kode-kode biner pada citra akan disandikan dengan kode-kode biner berkas zip dan kunci rahasia.

Tahapan Dekripsi

```
Begin
Input: Stego_Image, Secret_Key;
Compare Secret_Key;
Calculate BitsPerUnit,
Decode All_Binary_Codes;
Shift by 2 unit for bitsPerUnit;
Convert Binary_Codes to Text_File;
Unzip Text_File;
Output Secret_Message;
End
```

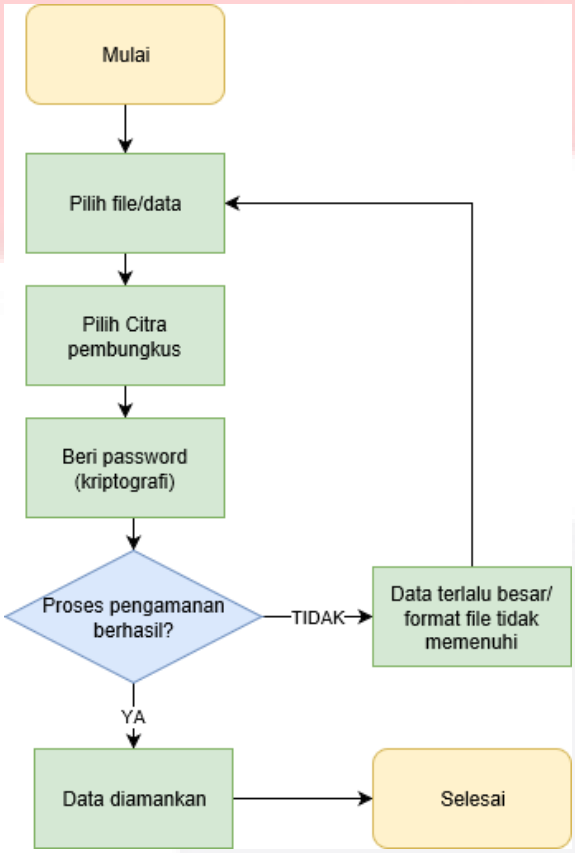
Gambar 3.5 Algoritma Pemulihan Pesan

Proses pemulihan pesan pada citra yang sudah disisipkan pesan memiliki tahapan yang hampir sama dengan proses yang berkebalikan. Kunci rahasia di sini berperan penting dalam pemulihan pesan. Jika kunci yang digunakan sesuai, maka proses akan dilanjutkan. Namun sebaliknya, jika kunci tidak sesuai, maka proses tidak akan bisa dilanjutkan.

3.2.2 Cara Kerja Sistem

Sistem yang dibangun pada aplikasi ini memiliki 2 tahapan, yaitu proses enkripsi (proses pengamanan data) dan proses dekripsi (proses pengembalian data).

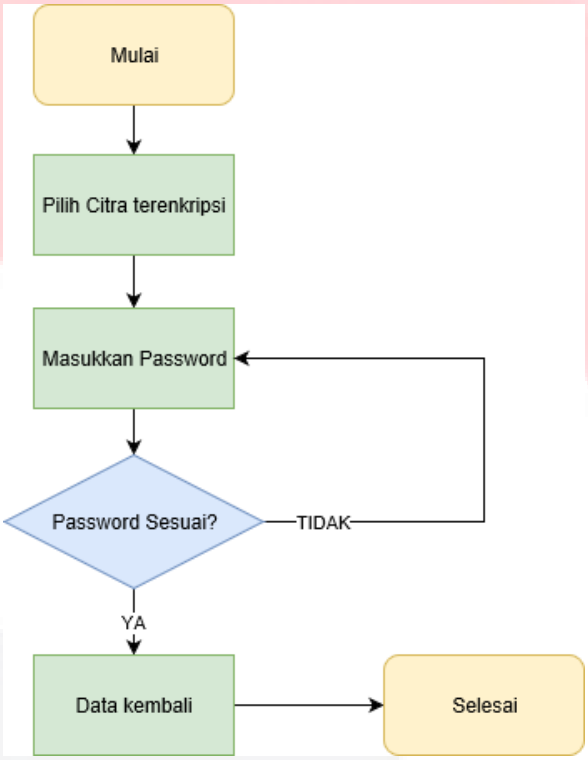
Proses Enkripsi:



Gambar 5.2.1 Proses Enkripsi Data

Pada aplikasi yang dibangun, pengguna bisa mengamankan data yang diinginkan. Sebelum melakukan proses lainnya, pengguna akan menginput teks terlebih dahulu untuk diamankan. Kemudian, pengguna akan memilih citra yang akan membungkus data untuk proses steganografi. Setelah itu, data yang akan dibungkus tadi akan diberikan *password* untuk ditingkatkan keamanannya dengan metode kriptografi. Jika ukuran berkas memenuhi, data akan diamankan pada media citra yang sudah dipilih dengan metode LSB (*Least Significant Bit*).

Proses Dekripsi:



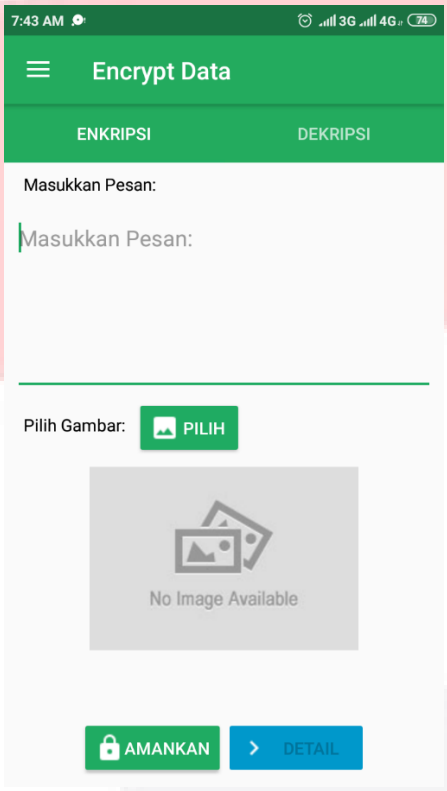
Gambar 5.2.2 Proses Dekripsi Data

Untuk bisa melihat kembali data yang sudah diamankan, maka data tersebut perlu dikembalikan ke bentuk semula. Proses yang dilakukan hampir sama dengan proses enkripsi data, hanya saja proses yang dilakukan berkebalikan dengan proses sebelumnya. Pilih berkas yang sudah diamankan dan sudah berbentuk citra. Setelah itu, masukkan *password* sesuai dengan proses sebelumnya. Data akan dikembalikan ke bentuk semula jika *password* yang dimasukkan benar.

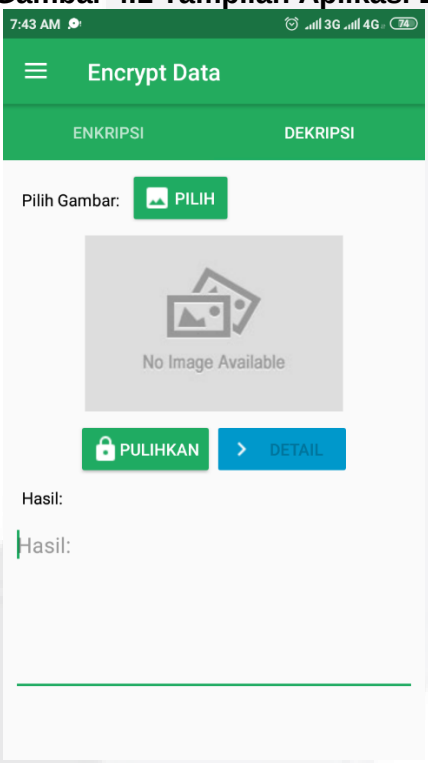
4. Implementasi dan Pengujian

4.1 Implementasi

Implementasi Proyek Akhir ini dilakukan pada beberapa perangkat Android. Berikut tampilan aplikasi yang telah dibuat secara lengkap.



Gambar 4.1 Tampilan Aplikasi 1

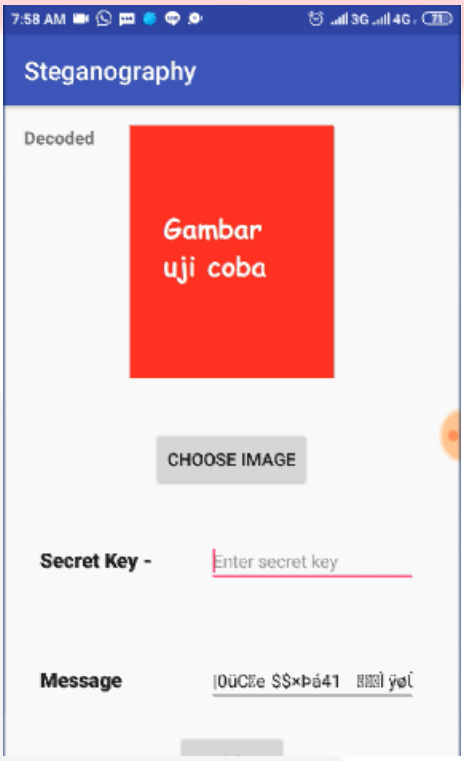


Gambar 4.2 Tampilan Aplikasi 2

4.2 Pengujian

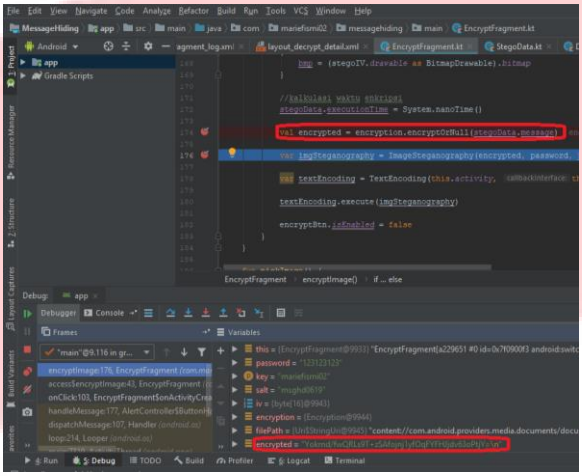
Pengujian bertujuan sebagai pembuktian terhadap skenario pengujian yang telah dibuat dan untuk mengetahui performansi terhadap algoritma yang digunakan pada perangkat Android.

1.Pengujian Algoritma



Gambar 4.2 Pengujian Algoritma Steganografi

Pada gambar di atas, citra yang sudah dienkripsi sebelumnya didekripsi menggunakan aplikasi lain yang menggunakan algoritma yang sama. Saat didekripsi, pesan pada citra tersebut berhasil dipulihkan, tetapi pesan tersebut tidak terbaca dengan benar. Hal itu disebabkan karena pesan yang ada di dalam citra tersebut masih terenkripsi dengan kunci dan metodei yang berbeda, sehingga pesan tidak bisa terbaca.



Gambar 4.3 Pengujian Algoritma Kriptografi

Untuk membuktikan apakah pesan terenkripsi dengan metode AES, di sini digunakan fitur *breakpoint* pada Android Studio, yaitu fitur yang berfungsi untuk menghentikan proses algoritma pada titik tertentu dan melihat proses yang terjadi disaat itu juga. Pada gambar di atas, terlihat jika pesan yang sebelumnya berbentuk plain teks berubah menjadi cipher teks AES.

2. Pengujian Performa

No	Perangkat	Format	Pesan	Ukuran		Lama Waktu
				Sebelum	Sesudah	
1	Xiaomi Redmi Note 5A (RAM 2GB/Android N/)	JPG	4 Karakter	2757KB	14863KB	24,2 s
		JPG	4 Karakter	247KB	2114KB	4,1 s
		PNG	4 Karakter	82KB	97KB	2,1 s
		JPG	44 Karakter	247KB	2114KB	4,2 s
		JPG	44 Karakter	2757KB	14863KB	24,2s
		PNG	44 Karakter	82KB	97KB	2,2 s
		PNG	432 Karakter	82KB	99KB	2,1 s
		PNG	628 Karakter	82KB	100KB	2,3 s
		PNG	1555 Karakter	82KB	103KB	2,2 s
		GIF (*Single*)	10 Karakter	50KB	68KB	1,4s
		GIF (*Multi*)	10 Karakter	360KB	21KB	0,5s
		BMP	10 Karakter	497KB	6KB	1,2s
2	Nexus 4 (RAM 1GB/Android L)	JPG	4 Karakter	2757KB	15230KB	45,1 s
		JPG	4 Karakter	247KB	1999KB	5,7 s
		PNG	4 Karakter	82KB	97KB	2,4 s
		JPG	44 Karakter	2757KB	15230KB	49,9 s
		JPG	44 Karakter	247KB	1999KB	5,5 s
		PNG	44 Karakter	82KB	97KB	2,6 s
3	Galaxy Nexus (RAM 1,5GB/Android P)	JPG	4 Karakter	2757KB	14863KB	42,1 S
		JPG	4 Karakter	247KB	2114KB	8,2 S
		PNG	4 Karakter	82KB	97KB	8,2 s
		JPG	44 Karakter	2757KB	14863KB	49 s
		JPG	44 Karakter	247KB	2114KB	8,8 s
		PNG	44 Karakter	82KB	97KB	5,3 s

4.4 Tabel Pengujian Enkripsi

No	Perangkat	Ukuran	Pesan	Waktu
1	Xiaomi Redmi Note 5A (RAM 2GB/Android N)	14863KB	44 karakter	1,644 s
		2114KB	44 karakter	0,372 s
		97KB	44 karakter	0,327 s
		14863KB	4 karakter	2, 572 s
		2114KB	4 karakter	0,527 s
		97KB	4 karakter	0,272 s
		103KB	1555 karakter	0,362 s
		100KB	628 karakter	0,270 s
		99KB	432 karakter	0,262 s
2	Nexus 4 (RAM 1GB/Android L)	15230KB	44 karakter	6,62 s
		1999KB	44 karakter	1,367 s
		97KB	44 karakter	1,40 s
		15230KB	4 karakter	6,300 s
		1999KB	4 karakter	1,211 s
		97KB	4 karakter	0,686 s
3	Galaxy Nexus (RAM 1,5GB/Android P)	14863KB	44 karakter	5,913 s
		2114KB	44 karakter	2,157 s
		97KB	44 karakter	2,104 s
		14863KB	4 karakter	5,351 s
		2114KB	4 karakter	1,791 s
		97KB	4 karakter	2,724 s

4.4 Tabel Pengujian Dekripsi

Pengujian dilakukan berdasarkan skenario pengujian yang dibuat. Pada pengujian di atas, telah dilakukan pengujian pengamanan data, pemulihan data, format citra, serta panjang pesan yang bisa disisipkan.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Dari uraian-uraian di atas dapat ditarik beberapa kesimpulan sebagai berikut:

1. Spesifikasi perangkat akan mempengaruhi proses enkripsi dan dekripsi teknik kriptografi pada perangkat Android. Semakin baik perangkat yang digunakan maka semakin cepat proses dilakukan.

2. Gambar berformat JPEG akan menghasilkan *stego image* dengan penambahan ukuran cukup signifikan. Hal ini disebabkan karena gambar berformat JPEG merupakan gambar berformat *lossy compression*, yaitu format gambar dengan rasio kompresi yang cukup tinggi. Metode LSB membutuhkan gambar berformat *lossless compression*, *yaitu* gambar berformat kompresi rendah atau tidak menghilangkan informasi saat kompresi untuk kualitas yang lebih baik, seperti PNG.
3. Semakin panjang pesan yang disisipkan pada gambar, maka semakin besar pula ukuran *stego image* yang dihasilkan.
4. Teknik steganografi dengan metode LSB memiliki kelemahan, yaitu jika *stego image* dimodifikasi (seperti diperbesar, diperkecil, dikompresi) dan akan didekripsi, pesan yang disisipkan pada *stego image* tersebut akan menghilang.

5.2 Saran

Saran yang dapat diberikan agar proyek akhir ini menjadi lebih baik yaitu:

1. Menggunakan algoritma dengan validitas yang lebih tinggi yang dapat mengatasi kelemahan dari metode LSB.

6. Daftar Pustaka

[1] H. V. Desai, "Steganography, Cryptography, Watermarking: A Comparative Study," *Journal of Global Research in Computer Science,* vol. 3, no. 12, p. 33, 2012.

[2] M. A. Andriawan, Implementasi Steganografi pada Citra Digital File Gambar Bitmap (BMP) Menggunakan Java, Bandung: Politeknik Telkom, 2012.

[3] R. Munir, "Pengantar Kriptografi," ITB, Bandung, 2018.

[4] UTopi Computers, "Apa itu Smartphone ? Ini Pengertian Dan Apa Perbedaannya Dengan HP?," 21 June 2017. [Online]. Available: https://www.utopicomputers.com/apa-itu-smartphone-ini-pengertian-dan-apa-perbedaanya-dengan-hp/. [Accessed 29 March 2018].

[5] Android Developer, "Plarform Architecture," Google, [Online]. Available: https://developer.android.com/guide/platform/index.html. [Accessed 5 May 2018].

[6] Y. P. Ermadi Satriya Wijaya, "KONSEP HIDDEN MESSAGE MENGGUNAKAN TEKNIK STEGANOGRAFI DYNAMIC CELL SPREADING," vol. 2, no. 1, pp. 24-25, 2004.

[7] D. Surian, "Algoritma Kriptografi AES Rijndael," *TESLA,* vol. 8, no. 2, pp. 97-98, 2006.

[8] R. Ibrahim and T. S. Kuan, "Steganography Algorithm to Hide Secret Message inside," *Computer Technology and Application 2,* vol. II, no. 2, pp. 102-108, 2011.

[9] V. Lusiana, "IMPLEMENTASI KRIPTOGRAFI PADA FILE DOKUMEN MENGGUNAKAN ALGORITMA AES-12," *Jurnal Dinamika Informatika,* vol. 3, no. 2, p. 1, 2011.