BAB IV
HASIL DAN PEMBAHASAN

4.1 Pembahasan

Pada penelitian ini akan dilakukan proses pengamanan pesan dalam bentuk teks yang dapat berupa huruf, angka dan simbol ke dalam sebuah video digital menggunakan kombinasi algoritma RSA dan algoritma LSB2BIT. Alur kerja dari aplikasi yang akan dibangun adalah menggunakan algoritma RSA untuk mengamankan pesan sehingga menghasilkan ciphertext yang selanjutnya akan di sisipkan ke dalam sebuah file video menggunakan algoritma LSB2BIT. Output yang akan dihasilkan oleh aplikasi adalah sebuah file video stego yang telah disisipkan pesan rahasia di dalamnya. Dengan menggunakan aplikasi yang sama, pesan yang telah disisipkan ke dalam file video tersebut dapat di ekstrak dan dikembalikan ke dalam bentuk aslinya.

4.1.1 Analisis Data

Pada penelitian ini data yang digunakan adalah berupa pesan teks dan juga file video. Dimana pesan teks tersebut akan di enkripsi menggunakan algoritma RSA dan selanjutnya hasil enkripsi akan disisipkan ke dalam file video menggunakan algoritma LSB2BIT. Langkah-langkah dari pengamanan dan penyisipan pesan teks ke dalam file video adalah sebagai berikut :

1. Proses Enkripsi Algoritm RSA

   RSA terbagi menjadi tiga proses, yaitu pembangkitan kunci, enkripsi dan dekripsi. Dasar proses enkripsi dan dekripsi pada algoritma RSA yaitu konsep bilangan prima dan aritmatika modulo. Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum (disebut kunci publik), sedangkan kunci untuk dekripsi bersifat rahasia (disebut kunci pribadi).

   Untuk menemukan kunci dekripsi, dilakukan dengan cara memfaktorkan bilangan bulat menjadi faktor-faktor primanya. Namun, memfaktorkan bilangan bulat menjadi faktor primanya tidak mudah karena belum ada cara yang efisien untuk melakukan pemfaktoran. Cara yang paling mungkin dilakukan adalah dengan pohon faktor. Namun

SUMATERA UTARA MEDAN

semakin besar bilangan yang akan difaktorkan maka semakin lama pula waktu yang dibutuhkan untuk menyelesaikannya. Jadi semakin besar bilangan yang akan difaktorkan, semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA. Oleh karena itu, dalam menggunakan algoritma RSA dianjurkan menggunakan bilangan yang sangat besar agar keamanannya dapat terjamin.

Besaran-besaran yang digunakan pada algoritma RSA antara lain :

1. p dan q bilangan prima (rahasia)
2. $n = pq$ (tidak rahasia)
3. $\varphi(n) = (p-1)(q-1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kuni dekripsi) (rahasia)
6. m (plainteks) (rahasia)
7. c (chiperteks) (tidak rahasia)

Berikut ini langkah- langkah dalam membangkitkan dua kunci algoritma RSA.

1. Pilih dua bilangan prima sembarang, $p$dan q.
2. Hitung $n = p.q$.
3. Hitung $\varphi(n) = (p-1)(q-1)$.
4. Pilih kunci publik e, yang relatif prima terhadap $\varphi(n)$.
5. Bangkitkan kunci pribadi dengan menggunakan $e.d \equiv 1\ mod\ \varphi(n)$.

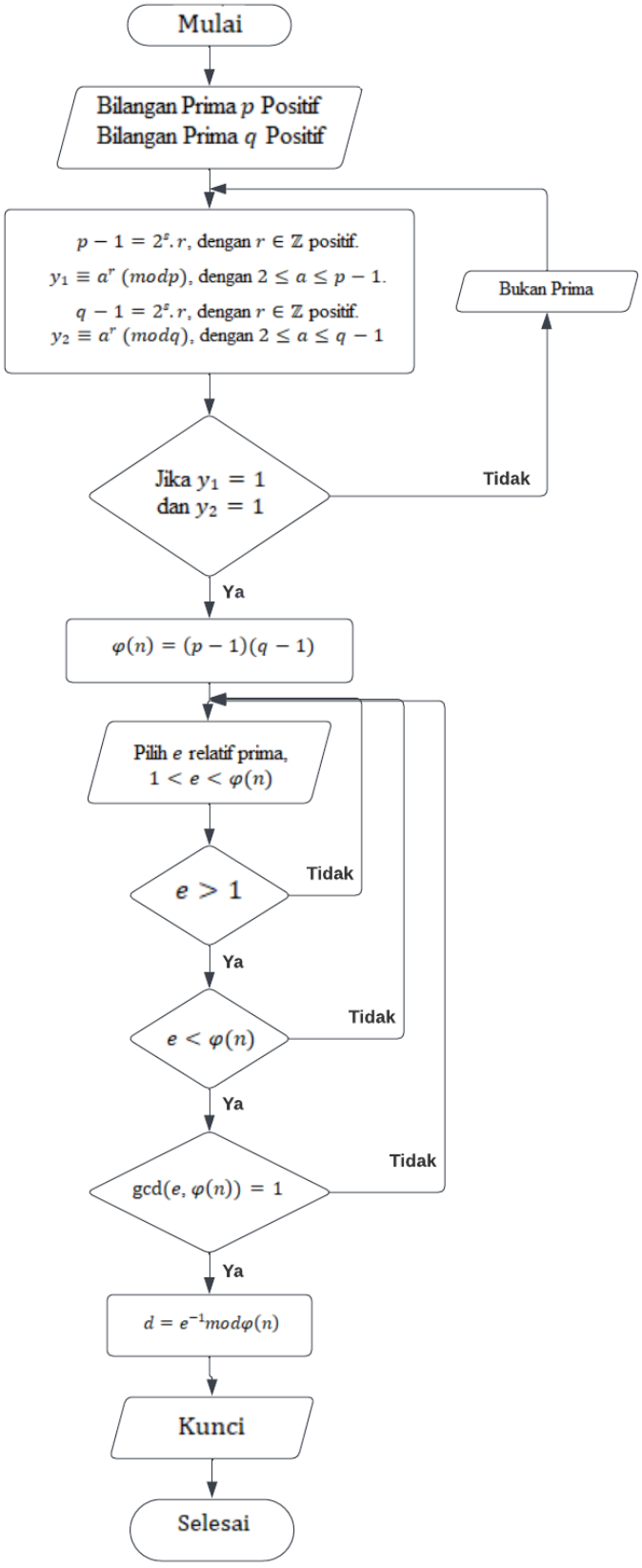
Hasil dari pembangkitan kunci adalah :

Kunci public : pasangan (N,e)

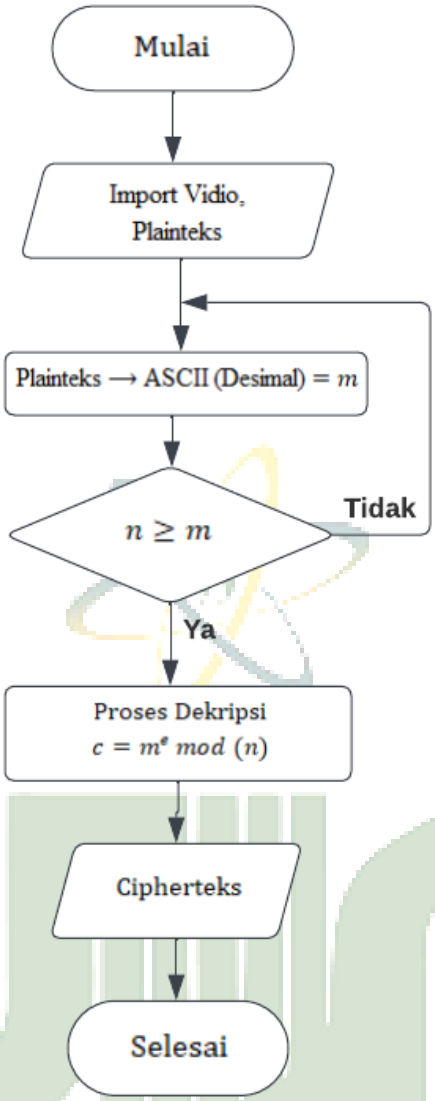
Kunci privat : pasangan (N,d)

Flowchart pembangkitan kunci algoritma RSA dapat dilihat pada gambar 4.1.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN



Gambar 4.1. Flowchart Pembangkitan Kunci Algoritma RSA



Gambar 4.2. Flowchart Algoritma Enkripsi

Contoh :

Misalkan plaintext yang akan dienkripsikan adalah x = ilmu komputer

a. Mengubah plaintext yang akan dienkripsi dalam sistem desimal (pengkodean ASCII) ilmu komputer = 105 108 107 117 107 111 109 112 117 116 101 114

b. Memecah x menjadi blok yang lebih kecil, misalnya x dipecah menjadi delapan blok yang berukuran 3 digit

x_1 = 737 x_5 = 778

x_2 = 677 x_6 = 085

x_3 = 857 x_7 = 846

$x_4 = 579$ $x_8 = 982$

b. Blok-blok plaintext dienkripsikan sebagai berikut :

$737^{39} \bmod 3337 = 105 = y_1$

$677^{39} \bmod 3337 = 2175 = y_2$

$857^{39} \bmod 3337 = 655 = y_3$

$579^{39} \bmod 3337 = 2574 = y_4$

$778^{39} \bmod 3337 = 1046 = y_5$

$085^{39} \bmod 3337 = 1940 = y_6$

$846^{39} \bmod 3337 = 1827 = y_7$

$982^{39} \bmod 3337 = 655 = y_8$

$854^{39} \bmod 3337 = 1048 = y_8$

$972^{39} \bmod 3337 = 2574 = y_8$

$955^{39} \bmod 3337 = 389 = y_8$

$911^{39} \bmod 3337 = 2324 = y_8$

$850^{39} \bmod 3337 = 1947 = y_8$

Jadi, ciphertext yang dihasilkan adalah y = 105 2175 655 2574 1046 1940 1827 655 1048 2574 389 2324 1947.

2. Proses Penyisipan Algoritma LSB2BIT

Pada tahap ini ciphertext yang dihasilkan dari proses enkripsi menggunakan algoritma RSA diubah ke dalam bentuk biner. Selanjutnya data biner tersebut disisipkan ke dalam 2 bit terakhir pada nilai biner yang di dapatkan dari frame yang terdapat pada file video. Proses penyisipan ciphertext adalah sebagai berikut :

a. Mengubah ciphertext ke dalam bentuk biner :

105	= 10111111	2574	= 101000001110
2175	= 10101101110	389	= 110000101
655	= 101110101	2324	= 100100010100
2574	= 100100101101	1947	= 11110011011
1046	= 111001101		

UNIVERSITAS ISLAM NEGERI SUMATERA UTARA MEDAN

1940 = 100111110000

1827 = 11111001110

655 = 100000100011

1048 = 10000011000

b. Melakukan proses penyisipan :

Selanjutnya ciphertext yang telah diubah ke dalam bentuk biner akan disisipkan ke dalam sampel nilai biner frame dari sebuah file video dengan cara mengganti 2 bit biner nilai frame file video terakhir dengan bit biner ciphertext. Sampel nilai biner pada frame yang terdapat pada file video yang akan digunakan adalah sebagai berikut :

Tabel 4.1 Sampel nilai biner pada frame file video

1010011	1010101	1010001	1111010	1000010	1000001	1000001	1000001
1000001	1000001	1000001	1000010	1000001	1000110	1010010	1011001
1010111	1000110	1100111	1000001	1000001	1000001	1000001	1010011
1000001	1000001	1000001	1000100	1100010	1010111	1000110	1110001
1010011	1010101	1010001	1111010	1000010	1000001	1000001	1000001

Setelah proses pergantian tiap-tiap bit terakhir akan dihasilkan biner file audio sebagai berikut :

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

Tabel 4.2 Hasil nilai biner setelah di proses

10100**0** **1**	10101**1** **1**	10100**0** **0**	11110**0** **0**	10000**0** **1**	10000**1** **0**	10000**1** **1**	10000**1** **1**
10000**0** **1**	10000**1** **1**	10000**0** **1**	10000**1** **1**	10000**0** **1**	10001**1** **0**	10100**1** **1**	10110**0** **0**
10101**0** **1**	10001**1** **0**	11001**0** **0**	10000**1** **0**	10000**0** **1**	10000**1** **1**	10000**1** **0**	10100**0** **1**

10000**0** **1**	10000**1** **0**	10000**1** **0**	10001**0** **1**	11000**0** **0**	10101**1** **1**	10001**0** **0**	11100**1** **0**
10100**0** **1**	10101**0** **0**	10100**1** **0**	11110**1** **0**	100001 0	100000 1	100000 1	100000 1

3. Proses Ektraksi Algoritma LSB2BIT

   Hasil file video stego yang memiliki data pesan teks di dalamnya dapat di ekstraksi menggunakan algoritma LSB2BIT. Proses ektraksi dilakukan perbyte data pada nilai biner dari frame file video. Kemudian dari setiap byte pesan yang disisipkan akan digabungkan menjadi pesan rahasia dari awal hingga kalimat terakhir sehingga semua kalimat tersusun sesuai pesan asli. Berikut adalah proses ekstraksi algoritma LSB2BIT :

   a. Bit file audio yang telah disisipkan pesan :

4.2 Tabel 4.3 Hasil nilai biner setelah disisipkan pesan

10100**0** **1**	10101**1** **1**	10100**0** **0**	11110**0** **0**	10000**0** **1**	10000**1** **0**	10000**1** **1**	10000**1** **1**
10000**0** **1**	10000**1** **1**	10000**0** **1**	10000**1** **1**	10000**0** **1**	10001**1** **0**	10100**1** **1**	10110**0** **0**
10101**0** **1**	10001**1** **0**	11001**0** **0**	10000**1** **0**	10000**0** **1**	10000**1** **1**	10000**1** **0**	10100**0** **1**
10000**0** **1**	10000**1** **0**	10000**1** **0**	10001**0** **1**	11000**0** **0**	10101**1** **1**	10001**0** **0**	11100**1** **0**
10100**0** **1**	10101**0** **0**	10100**1** **0**	11110**1** **0**	100001 0	100000 1	100000 1	100000 1

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

   a. Proses penyusunan bit pesan menjadi cipertext :

105	= 10111111	2574	= 101000001110
2175	= 10101101110	389	= 110000101
655	= 101110101	2324	= 100100010100

2574 = 100100101101 1947 = 11110011011

1046 = 111001101

1940 = 100111110000

1827 = 11111001110

655 = 100000100011

1048 = 10000011000

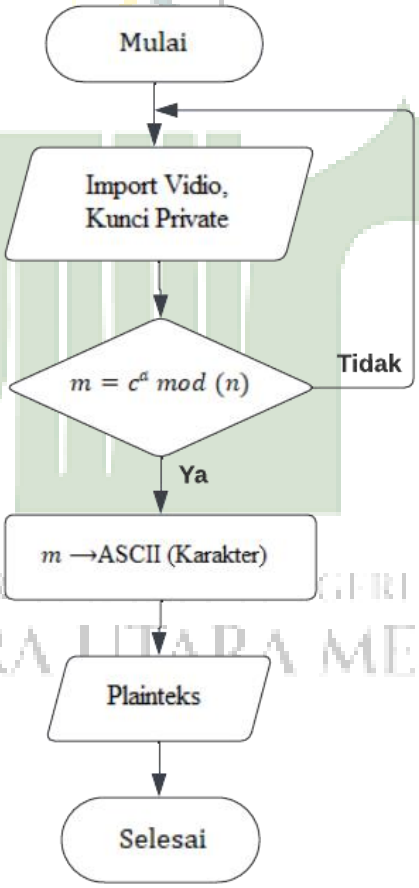
4. Proses Dekripsi Algoritma RSA

Algoritma dekripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut :

a. Gunakan kunci privat untuk menghitung Mi = Ci d mod N

b. Carilah nilai m dengan rumus

$M_i = C_i^d \bmod n$



Gambar 4.3. Flowchart Proses Dekripsi

a. Deskripsi dilakukan dengan menggunakan kunci privat d = 1019

b. Blok-blok ciphertext dideskripsikan sebagai berikut :

$105^{949} \bmod 3337$ = 737 = x_1

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

$2175^{949} \bmod 3337 = 677 = x_2$

$655^{949} \bmod 3337 = 857 = x_3$

$2574^{949} \bmod 3337 = 579 = x_4$

$1046^{949} \bmod 3337 = 778 = x_5$

$1940^{949} \bmod 3337 = 085 = x_6$

$1827^{949} \bmod 3337 = 846 = x_7$

$655^{949} \bmod 3337 = 982 = x_8$

$1048^{949} \bmod 3337 = 854 = x_9$

$2574^{949} \bmod 3337 = 972 = x_{10}$

$389^{949} \bmod 3337 = 955 = x_{11}$

$2324^{949} \bmod 3337 = 911 = x_{12}$

$1947^{949} \bmod 3337 = 850 = x_{13}$

c. Akhirnya diperoleh kembali plaintext semula

x = 105 2175 655 2574 1046 1940 1827 655 1048 2574 389 2324 1947

Dalam karakter ASCII P = ilmu komputer

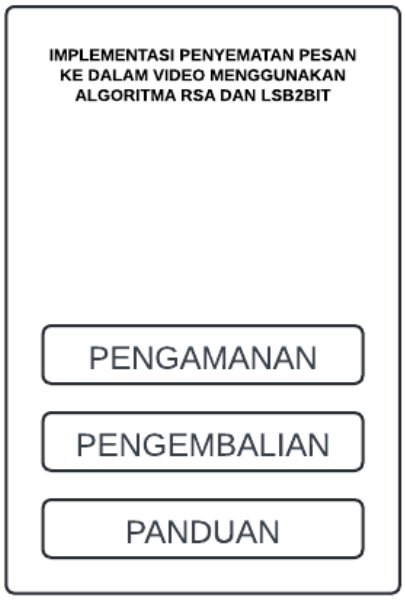
4.1.2 Perancangan Antarmuka

Aplikasi Penyematan Pesan Ke Dalam Video Digital Menggunakan Algoritma RSA Dan LSB2BIT pada penelitian ini dibangun menggunakan perangkat lunak Android Studio menggunakan bahasa pemrograman Java dan XML. Antarmuka pemakai adalah tampilan program yang dapat dilihat, didengar atau dipersepsikan oleh pengguna dan perintah-perintah atau mekanisme yang digunakan pemakai untuk mengendalikan operasi dan memasukkan data. Berikut ini merupakan perancangan antarmuka aplikasi Penyematan Pesan Ke Dalam Video Digital Menggunakan Algoritma RSA Dan LSB2BIT :

1. Desain Halaman Utama

   Halaman utama merupakan halaman yang tampil pertama saat aplikasi dijalankan pada *smartphone* android. Pada halaman utama terdapat menu pengamanan untuk menampilkan halaman pengamanan, menu pengembalian untuk menampilkan halaman pengembalian dan menu panduan untuk menampilkan halaman panduan. Desain halaman utama dapat dilihat pada gambar 4.4.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

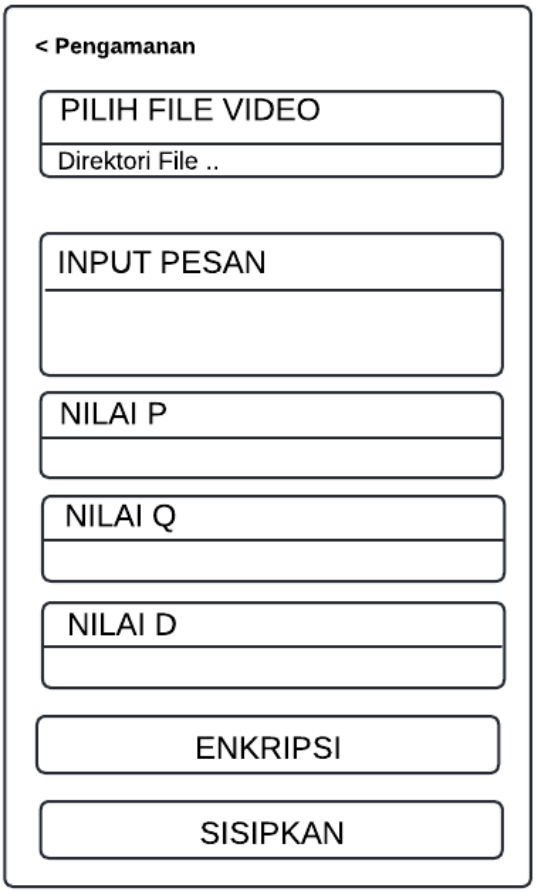


Gambar 4.4. Desain Halaman Utama

2. Desain Halaman Pengamanan

   Halaman pengamanan digunakan untuk proses enkripsi dan penyisipan ciphertext yang dihasilkan ke dalam file video. Desain halaman pengamanan dapat dilihat pada gambar 4.5.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

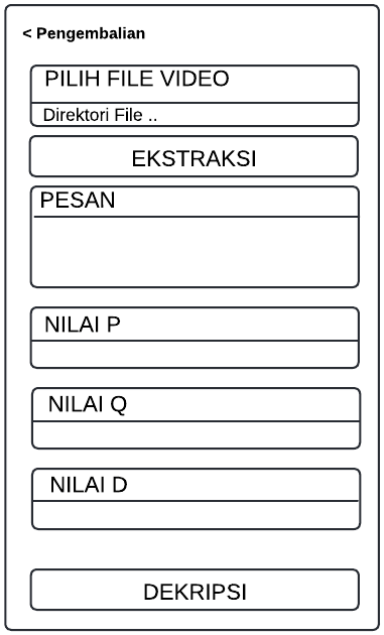


Gambar 4.5. Desain Halaman Pengamanan

3. Desain Halaman Pengembalian

   Halaman pengembalian digunakan untuk melakukan proses ektraksi ciphertext yang terdapat pada file video stego dan melakukan prose dekripsi terhadap ciphertext yang telah di ekstrak agar kembali ke dalam bentuk pesan aslinya. Desain halaman pengembalian dapat dilihat pada gambar 4.6.

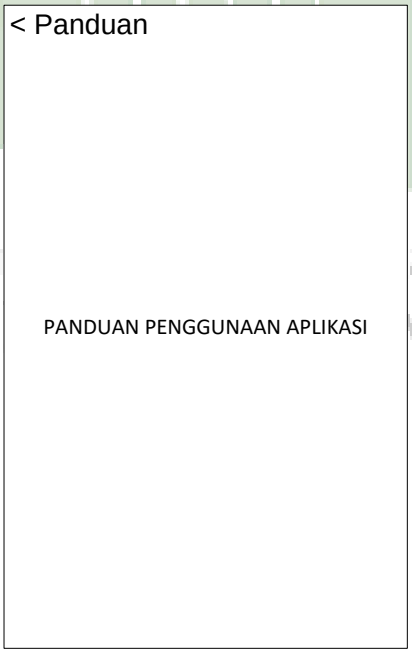
UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN



Gambar 4.9. Desain Halaman Pengembalian

4. Desain Halaman Panduan

   Halaman panduan digunakan untuk menampilkan halaman panduan penggunaan aplikasi dalam mengamankan dan mengembalikan pesan. Desain halaman panduan dapat dilihat pada gambar 4.7.



Gambar 4.7. Desain Halaman Panduan

4.2 Hasil

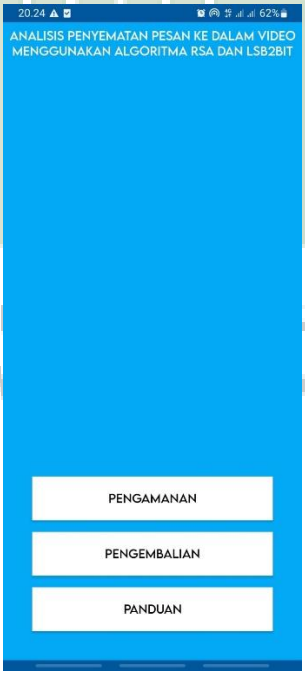
Pada penelitian ini telah dihasilkan sebuah aplikasi yang dapat digunakan untuk mengamankan pesan menggunakan algoritma RSA dan menyisipkan hasil pengemanan pesan ke dalam file video menggunakan algoritma LSB2BIT. Dengan menggunakan aplikasi ini, pengguna dapat memanfaatkan file video untuk melindungi pesan yang bersifat rahasia sebelum dikirimkan ke pihak lain.

4.2.1 Pengujian Aplikasi

Berikut ini merupakan hasil pengujian aplikasi saat dijalankan pada *smartphone* android. Pengujian yang dilakukan adalah berupa menjalankan aplikasi dan menampilkan halaman-halaman yang terdapat dari setiap menu yang ada pada aplikasi yang dihasilkan dari penelitian ini. Hasil pengujian aplikasi adalah sebagai berikut :

1. Tampilan Halaman Utama

   Halaman ini akan tampil pertama saat aplikasi dijalankan pada smartphone android. Halaman utama dari aplikasi dapat dilihat pada gambar 4.8.



Gambar 4.8. Halaman Utama

2. Tampilan Halaman Pengamanan

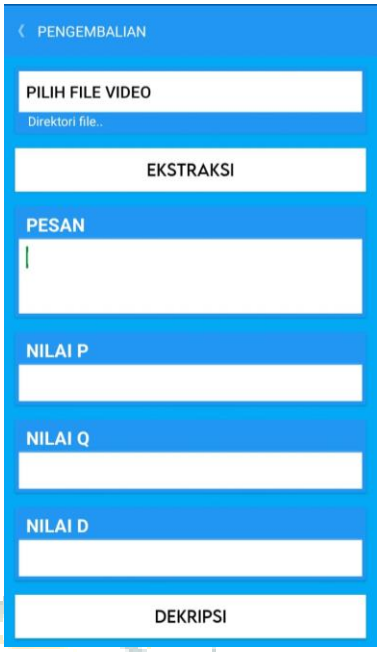
Halaman pengamanan digunakan untuk mengamankan pesan dan menyisipkannya ke dalam file video. Halaman pengamanan dapat dilihat pada gambar 4.9.

Gambar 4.9. Halaman Pengamanan

3. Halaman Pengembalian

   Halaman pengembalian digunakan untuk melakukan proses ekstraksi pesan pada video stego dan melakukan dekripsi terhadap pesan yang telah di ekstrak. Halaman pengembalian dapat dilihat pada gambar 4.10.

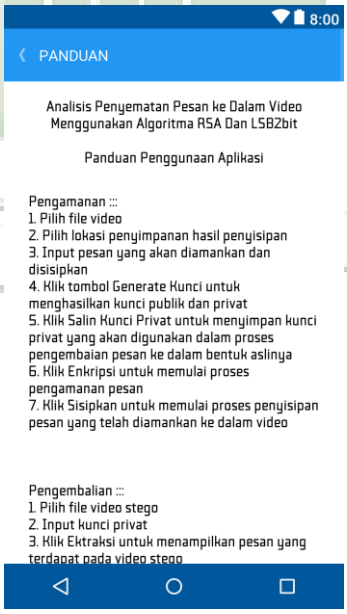
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA MEDAN



Gambar 4.10. Halaman Pengembalian

4. Halaman Panduan

   Halaman panduan digunakan untuk menampilkan halaman panduan yang berisikan informasi tentang cara penggunaan aplikasi dalam mengamankan dan mengembalikan pesan. Halaman panduan dapat dilihat pada gambar 4.11.



Gambar 4.11. Halaman Compare Audio File

4.2.3 Hasil Pengujian Aplikasi

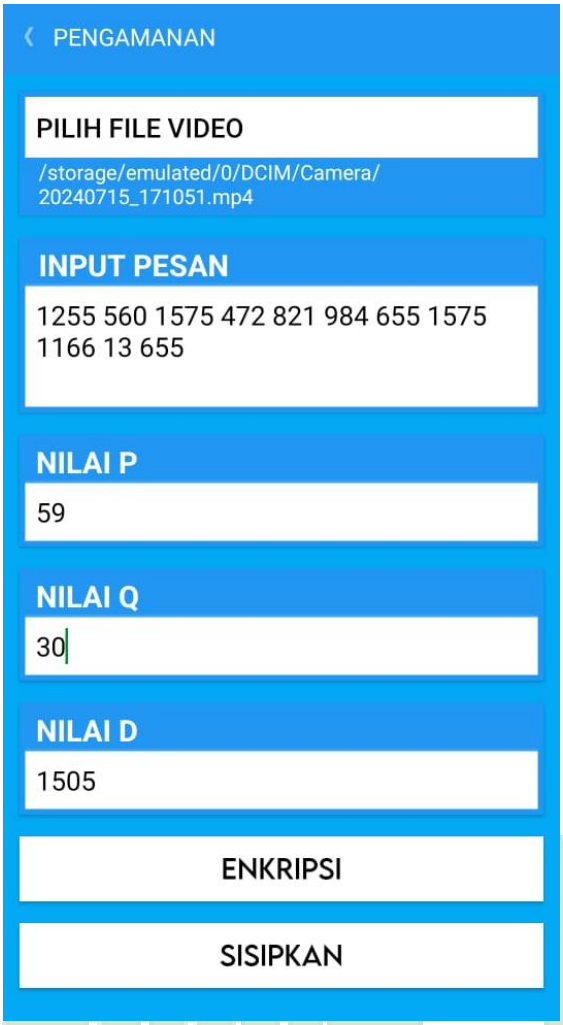
Pada tahap ini dilakukan pengujian dengan cara melakukan proses enkripsi dan penyisipan ke dalam file audio. Selanjutnya melakukan proses ekstraksi dan dekripsi terhadap pesan hasil ekstraksi dari file audio stego. Pengujian aplikasi dapat dilihat sebagai berikut :

1. Pengujian Pertama

   File Audio : ujicoba.mp4
   Ukuran : 1,27MB
   Pesan : Universitas
   Hasil Enkripsi : 1255 560 1575 472 821 984 655 1575 1166 13 655
   Nilai P : 59
   Nilai Q : 30
   Nilai D : 1505
   Ukuran File Hasil : 1,27MB
   Hasil Dekripsi : Universitas

   Hasil pengujian tersebut dapat dilihat pada gambar sebagai berikut :

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN



Gambar 4.12. Hasil Pengujian Pengamanan Pertama

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

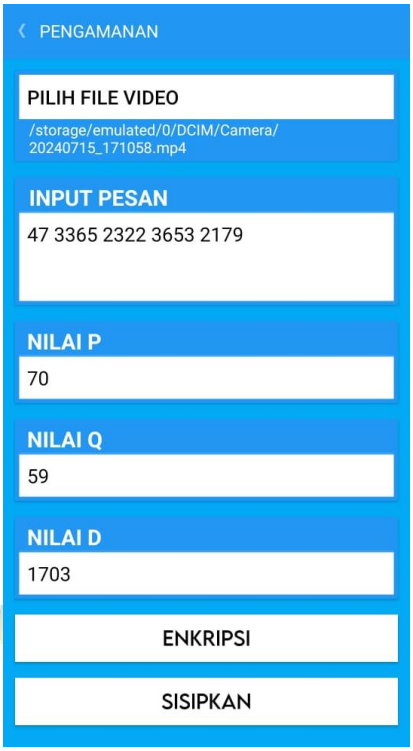
Gambar 4.13. Hasil Pengujian Pengembalian Pertama

2. Pengujian Kedua

   File Audio : ujicoba2.mp4
   Ukuran : 1,86MB
   Pesan : Islam
   Hasil Enkripsi : 47 3365 2322 3653 2179
   Nilai P : 70
   Nilai Q : 59
   Nilai D : 1703
   Ukuran File Hasil : 1,86MB
   Hasil Dekripsi : Islam

   Hasil pengujian tersebut dapat dilihat pada gambar sebagai berikut :

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN



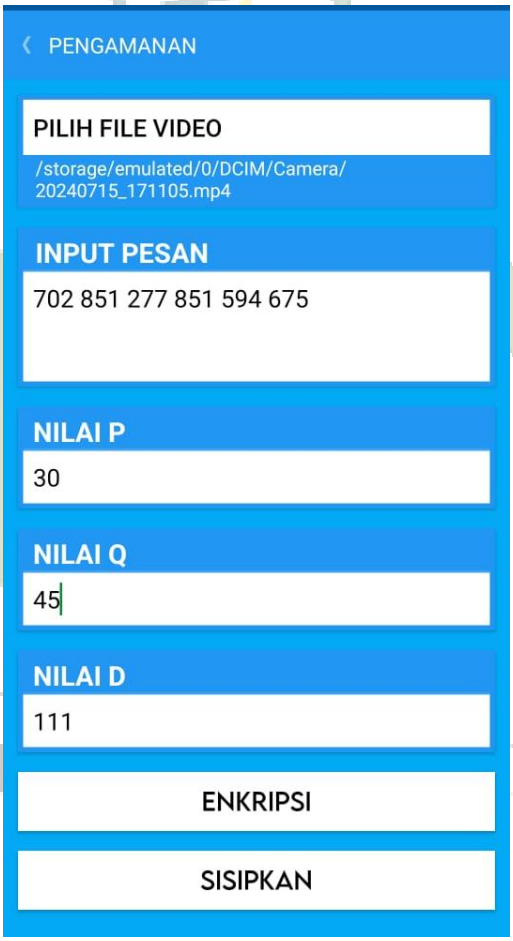
Gambar 4.14. Hasil Pengujian Pengamanan Kedua

Gambar 4.15. Hasil Pengujian Pengembalian Kedua

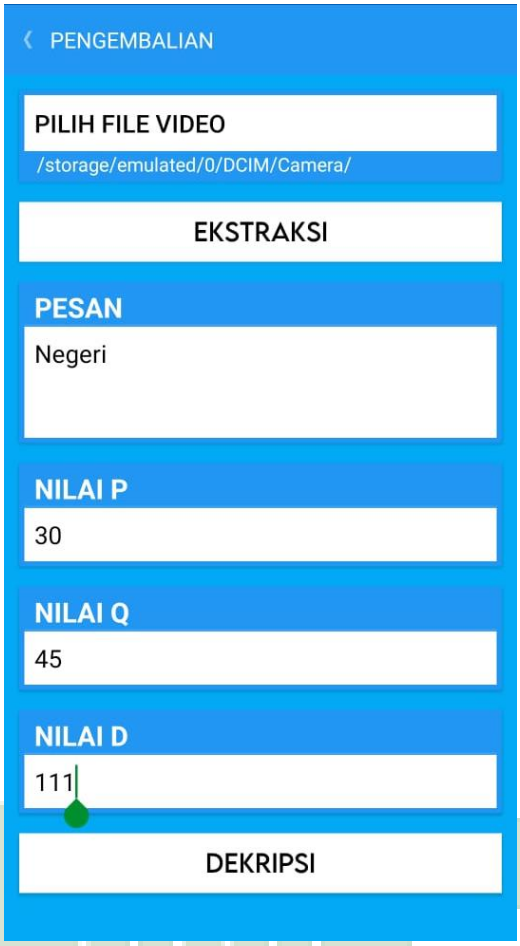
3. Pengujian Ketiga

File Audio : ujicoba3.mp4
Ukuran : 8,63MB
Pesan : Negeri
Hasil Enkripsi : 702 851 277 851 594 675
Nilai P : 30
Nilai Q : 45
Nilai D : 111
Ukuran File Hasil : 8,63MB
Hasil Dekripsi : Negeri

Hasil pengujian tersebut dapat dilihat pada gambar sebagai berikut :



Gambar 4.16. Hasil Pengujian Pengamanan Ketiga



Gambar 4.16. Hasil Pengujian Pengembalian Ketiga

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN