KOMBINASI ALGORITMA BEAUFORT CIPHER DAN LSB2BIT UNTUK KEAMANAN FILE TEXT

Abdul Halim Hasugian[1], Yusuf Ramadhan Nasution[2], Nadyah Almirah Simanjuntak[3]

[123,]Program Studi Ilmu Komputer UIN Sumatera Utara

Jl. Lapangan Golf No.120, Kp. Tengah, Kec. Pancur Batu, Kabupaten Deli Serdang, Sumatera Utara 20353
[1] abdulhasugian12@gmail.com, [2] ramadhannst@gmail.com, [3] nadyah.almirah@uinsu.ac.id

Abstract

The rapid development of science and technology allows the emergence of new techniques that can be misused by certain parties to threaten the security of an information system. Along with the times, the techniques used to threaten data security are always one step ahead of the techniques used to secure data. Because of that, an idea arose that refers to these problems, namely to create a security system that can protect data that is considered important by encoding the data so that it is difficult to detect by unauthorized parties. One of the well-known science of data security is cryptography and steganography. In this study, the cryptographic and steganographic algorithms used by researchers are the Beaufort and LSB2bit algorithms. The Beaufort algorithm is a variant of the Vigenere cipher method. In Beaufort the key of K is a sequence of letters K = k1...kd where ki is obtained from as many shifts in the I alphabet as in the vegenere cipher. The LSB algorithm is a method of inserting message bits at the lowest bit of an image so that it does not change the image significantly. By using cryptography and steganography techniques, in this study an application developed that can secure messages and insert them into images. So that unauthorized people are not aware of the existence of a secret message in the cover image.

Keywords *: Beaufort Algorithm, LSB Algorithm, Message, Image*

Abstrak

Pesatnya perkembangan ilmu pengetahuan dan teknologi telah memunculkan teknik-teknik baru yang dapat disalahgunakan untuk mengancam keamanan suatu sistem informasi. Dengan perkembangan zaman, teknologi yang mengancam keamanan data selalu satu tingkat lebih maju dari teknologi yang melindungi data. Oleh karena itu, muncul ide dalam menanggapi permasalahan tersebut, bahwa dirasa penting untuk membuat sistem yang aman yang dapat melindungi data dengan cara mengkodekannya sehingga sulit untuk dideteksi oleh pihak yang tidak berwenang. Kriptografi dan steganografi adalah dua ilmu keamanan data yang terkenal. Dalam penelitian ini, peneliti menggunakan algoritma kriptografi dan steganografi Beaufort dan LSB2bit. Algoritma Beaufort adalah metode cipher yang didasarkan pada cipher Vigenere. Di Beaufort, kunci K adalah string karakter K = k1 ... kd di mana ki diperoleh dari transformasi alfabet I sebanyak dalam cipher vegenere.Algoritma LSB adalah cara memasukkan bit pesan ke bit gambar terendah sehingga gambar tidak berubah secara berarti. Penelitian ini menghasilkan sebuah aplikasi yang dapat melindungi pesan dan menyisipkannya ke dalam gambar menggunakan teknik kriptografi dan steganografi. Sehingga orang yang tidak berhak tidak menyadari akan keberadaan suatu pesan rahasia pada citra yang dijadikan cover.

Kata kunci : *Algoritma Beaufort, Algoritma LSB, Pesan, Citra*

1. PENDAHULUAN

Dalam sistem informasi saat ini, keamanan dan dan kerahasiaan data menjadi salah satu aspek yang sangat penting[1]. Hal ini disebabkan oleh pertumbuhan teknologi berbasis pengetahuan saat ini, yang memungkinkan munculnya alat-alat baru yang terutama digunakan oleh institusi terkait untuk memastikan keamanan sistem

informasi tersebut. Ironisnya, teknik yang digunakan untuk mengenkripsi data untuk penyimpanan biasanya lebih kompleks daripada teknik yang digunakan untuk mengenkripsi data untuk transmisi. Oleh karena itu, perlu dibuat sistem perlindungan data yang dapat melindungi informasi sensitif melalui enkripsi data, sehingga menyulitkan pihak yang tidak dapat dipercaya untuk mengakses dan mendekodekannya[2].

Setiap aktivitas yang membahayakan privasi seseorang dapat diartikan sebagai sarana untuk mengakses, mentransfer, atau menyimpan data pribadi mereka tanpa sepengetahuan mereka[3].

Keamanan adalah keadaan di mana tidak ada ancaman. Istilah ini dapat digunakan dalam kaitannya dengan semua jenis kejahatan dan kecelakaan. Keamanan adalah konsep luas yang mencakup keamanan nasional terhadap teroris, keamanan dunia maya terhadap peretas, keamanan rumah terhadap pencuri dan ancaman domestik lainnya, keamanan finansial terhadap ketidakstabilan ekonomi, dan banyak situasi lain yang saling terkait[4].

Kriptografi dan steganografi adalah dua metode keamanan data yang terkenal. Kriptologi adalah studi tentang bagaimana menganalisis informasi secara non-artistik dengan menggunakan data, informasi, atau sumber lain sebagai bukti[5]. Enkripsi dan dekripsi adalah dua proses utama dalam sebuah citra kriptografi. Dekripsi adalah proses pengubahan ciphertext kembali menjadi plaintext, sedangkan enkripsi adalah pengubahan plaintext menjadi ciphertext. Dekripsi adalah proses membalikkan proses enkripsi dan mengubah data terenkripsi kembali menjadi plaintext. Steganografi adalah teknik yang digunakan untuk menjamin kerahasiaan suatu pesan. Dengan menempatkan informasi tersembunyi dalam file sampel, steganografi mempertahankan statusnya sebagai bentuk media yang sah sehingga tampak seperti teks biasa. Hanya mereka yang mau memahami makna dari pesan yang bersangkutan yang boleh membaca pesan yang telah ditulis.

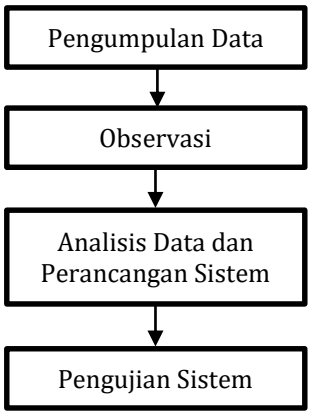
Dalam penelitian ini algoritma kriptografi dan steganografi yang digunakan oleh peneliti adalah algoritma *Beaufort* dan LSB2bit. Algoritma Beaufort adalah satu-satunya variasi paling umum dari metode sandi Vigenère, yang menggunakan jenis skrip klasik tertentu. Di Beaufort, definisi K ditulis sebagai K = k1... Kd. Dimana ki diturunkan dari angka yang sama dengan pergeseran abjad I sebagai cipher Vigenere[6]. Algoritma LSB bukanlah prosedur yang sangat rumit, dan penyimpanan pesan dalam gambar juga sangat besar, sehingga Anda dapat memasukkan data. Metode tersebut mengandalkan bilangan biner yaitu 0 dan 1 untuk mempercepat proses implementasi. Selain itu, metode ini hanya membutuhkan satu bit, dan ini sangat penting karena stego image atau media yang diperoleh hampir sama dengan steganografi yang digunakan sebelumnya karena hanya tersisa satu bit yang perlu dilindungi[7].

Citra adalah kumpulan piksel. Dalam ruang warna 24 bit, setiap piksel memiliki ukuran 3 byte, dengan setiap byte mengubah warna setiap komponen Merah, Hijau, dan Biru[8]. Penggunaan kedua algoritma tersebut bertujuan untuk mengamankan pesan sebelum di sisipkan ke dalam citra sehingga pesan yang akan disisipkan akan memiliki tingkat keamanan yang lebih baik. Berdasarkan latar belakang diatas, pada penelitian ini dibangun sebuah aplikasi untuk mengamankan pesan yang terdapat pada sebuah *file text* dengan cara melakukan enkripsi terhadap pesan yang selanjutnya akan disembunyikan pada sebuah citra[9].

Aplikasi yang dibangun merupakan aplikasi mobile. Android digunakan hampir diseluruh *Smartphone*[10]. Android adalah sistem operasi untuk perangkat mobile berbasis *Linux* yang dirancang untuk perangkat bergerak layar sentuh seperti *Smartphone*[11]. Aplikasi ini menggunakan Java sebagai bahasa pemrograman yang paling umum dalam pengembangan apikasi Android[12]. Dalam pengembangannya, peneliti menggunakan Android Studio sebagai Lingkungan Pengembangan Terintegrasi (IDE) yang dirancang untuk membuat aplikasi untuk sistem Android[13]. Android Studio terintegrasi dengan Android *Software Development Kit* (SDK) untuk *deploy* ke perangkat Android[14]. Selain itu, Dibutuhkan emulator yang dikenal sebagai Perangkat Virtual Android yang digunakan untuk meluncurkan aplikasi Android yang baru dikembangkan tanpa memerlukan perangkat Android fisik. Dengan menggunakan AVD kita dapat melakukan test dan menjalankan aplikasi Android[15].

2. METODOLOGI PENELITIAN

2.1 Skema Alur Penelitian



Gambar 1. Alur Penelitian

2.2 Pengumpulan Data

Sistem yang sedang dibangun tentunya membutuhkan pendataan; ada beberapa metode untuk mengumpulkan data. berikut diantaranya :

a. Studi Literatur, dengan mempelajari tentang sumber-sumber yang relevan dan tulisan yang berkaitan dengan pokok bahasan skripsi. Biasanya referensi yang digunakan antara lain artikel tentang tata cara penulisan skripsi di Universitas Islam Sumatera Utara serta kajian tentang metode yang digunakan dalam penulisan skripsi.
b. Observasi, adalah pengumpulan data dan informasi yang dilakukan melalui penggunaan beberapa contoh aplikasi kriptografi dan steganografi. Simulasi dilakukan dengan melihat contoh script bahasa program yang nantinya akan ditulis dalam bahasa pemrograman Java.

2.3 Analisa Data

Setelah melalui perencanaan, langkah selanjutnya adalah menganalisis kebutuhan yang meliputi kebutuhan perancangan aplikasi, seperti perangkat lunak dan perangkat keras yang dibutuhkan untuk membuat aplikasi. Dalam proses pengembangan aplikasi, komputer atau laptop dan Android Studio IDE sama-sama dibutuhkan untuk membuat aplikasi berbasis Android.

2.4 Perancangan

Menggunakan kombinasi cipher Beaufort dan algoritma LSB2bit untuk mengamankan pesan, beberapa desain antarmuka disajikan dalam tahap ini. Desain apa yang akan digunakan untuk antarmuka perangkat Android?. Setelah menyelesaikan review desain aplikasi, langkah selanjutnya adalah mulai mengimplementasikan desain yang sudah diterjemahkan ke dalam bahasa pemrograman.

2.5 Pengujian

Di tahap ini, pengujian aplikasi sedang dilakukan dengan menggunakan kombinasi cipher Beaufort dan algoritma LSB2bit untuk memastikan keamanan data secara menyeluruh, sekaligus mengatasi masalah kinerja operasional dan aplikasi. Untuk mengetahui bahwa aplikasi yang dibuat telah berjalan sesuai dengan rencana, maka dilakukan pengujian fungsional. Pengujian ketahanan adalah kunci utama agar berhasil berjalan di perangkat Android dengan spesifikasi minimal.

2.6 Penerapan/Penggunaan

Pada tahap ini akan dilakukan perbaikan dan pengembangan aplikasi yang dihasilkan berdasarkan kebutuhan yang teridentifikasi pada tahap pengujian. Perbaikan dilakukan berdasarkan kesalahan yang ditemukan. Selanjutnya akan dilakukan pengembangan untuk memaksimalkan utilitas aplikasi sehingga dapat digunakan secara optimal dalam proses transfer data dari file teks ke dalam sebuah file citra.

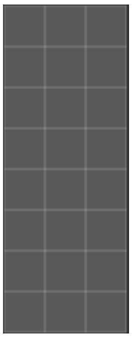
3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

Data yang digunakan pada penelitian ini adalah berupa teks yang terdapat pada sebuah file teks yang selanjutnya akan dilakukan pengamanan dengan teknik enkripsi dan menyisipkan teks tersebut ke dalam sebuah file citra menggunakan kombinasi algoritma beaufort dan LSB2bit.

Contoh : Terdapat teks berupa "**PENELITIAN SKRIPSI**" yang akan diamankan menggunakan kunci "**SAVE**" dan selanjutnya hasil enkripsi algoritma beaufort tersebut akan disisipkan ke

dalam sebuah citra berukuran 3x8 pixel yang memiliki nilai RGB (R = 89, G = 89, B = 89) sebagai berikut:



Gambar 2. Contoh Citra Digital

Selanjutnya nilai masing-masing RGB dari citra tersebut dikonversi kedalam bentuk biner sehingga di dapat nilainya sebagai berikut :

TABEL 1. KONVERSI NILAI RGB KE DALAM BINER

R	G	B	R	G	B	R	G	B
01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01
01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01
01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01
01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01
01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01
01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01
01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01
01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01	01 01 10 01

Proses pengamanan pesan menggunakan kedua algoritma tersebut dapat dilihat sebagai berikut :

a. Proses Enkripsi

Plaintext (P) : PENELITIAN SKRIPSI

Kunci (K) : SAVE

C1 = (K1 - P1) mod 26
= (S - P mod 26
= (18 - 15) mod 26
= 3
= D

C2 =(K2-P2) mod 26
= (A - E) mod 26
= (0 - 4) mod 26
= 22
= W

C3 = (K3 - P3) mod 26
= (V - N) mod 26
= (21 - 13) mod 26
= 8
= I

C4 = (K4-P4) mod 26
= (E - E) mod 26
= (4 - 4) mod 26
= 0
= A

C5 = (K5 - P5) mod 26
= (S - L) mod 26
= (18 - 11) mod 26
= 7
= H

C6 =(K6 - P6) mod 26
= (A- I) mod 26
= (0 - 8) mod 26
= 18
= S

C7 = (K1 - P7) mod 26
= (V - T mod 26
= (21 - 19) mod 26
= 2
= C

C8 =(K2 - P8) mod 26
=(E-I) mod 26
=(4-8)mod 26
= 22
= W

C9 = (K3 - P9) mod 26
= (S - A) mod 26
= (18 - 0) mod 26
= 18
= S

C10=(K4-P10)mod 26
= (A - N) mod 26
= (0 - 13) mod 26
= 13
= N

C11= (K5 - P11) mod 26
= (V - S) mod 26
= (21 - 18) mod 26
= 3
= D

C12=(K6–P12) mod 26
= (E- K) mod 26
= (4 - 10) mod 26
= 20
= U

C13= (K1 - P13) mod 26
= (S - R) mod 26
= (18 - 17) mod 26
= 1
= B

C14=(K2-P14) mod 26
= (A - I) mod 26
= (0 - 8) mod 26
= 18
= S

C15= (K3 - P15) mod 26
= (V - P) mod 26
= (21 - 15) mod 26
= 6
= G

C16=(K4-P16)mod 26
= (E - S) mod 26
= (4 - 18) mod 26
= 12
= M

C17= (K5 - P17) mod 26
= (S - I) mod 26
= (18 - 8) mod 26
= 10
= K

Dari proses enkripsi di dapatkan cipertext berupa "**DWIAHSCWSN DUBSGMK**"

b. Proses Penyisipan

Langkah pertama ubah ciphertext ke dalam bentuk biner sebagai berikut :

D = 0 1 0 0 0 1 0 0
W = 0 1 0 1 0 1 1 1

I	**=**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**
A	**=**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**
H	**=**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**
S	**=**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**
C	**=**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**1**
W	**=**	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**1**
S	**=**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**
N	**=**	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**0**
D	**=**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**
U	**=**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**
B	**=**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**
S	**=**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**
G	**=**	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**1**
M	**=**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**1**
K	**=**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**1**

TABEL 2. PENYISIPAN CIPHERTEXT

R	G	B	R	G	B	R	G	B
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
01	**00**	**01**	**00**	**01**	**01**	**01**	**11**	**01**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
00	**10**	**01**	**01**	**00**	**00**	**01**	**01**	**00**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
10	**00**	**01**	**01**	**00**	**11**	**01**	**00**	**00**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
11	**01**	**01**	**01**	**11**	**01**	**01**	**00**	**11**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
01	**00**	**11**	**10**	**01**	**00**	**01**	**00**	**01**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
01	**01**	**01**	**01**	**00**	**00**	**10**	**01**	**01**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
00	**11**	**01**	**00**	**01**	**11**	**01**	**00**	**11**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
01	**01**	**00**	**10**	**11**	11	01	01	01

Langkah selanjutnya adalah mengganti setiap 2 bit paling kanan dari setiap nilai R (Red), G (Green) dan B (Blue) dengan nilai biner ciphertext sehingga di hasilkan :

Hasil penyisipan ciphertext dapat dilihat pada nilai bit yang diwarnai diatas (RGB). Nilai piksel pada gambar yang berubah hanyalah pada 2 bit paling akhir sehingga tidak mengubah citra digital secara kasat mata.

c. Proses Ekstraksi

Proses ekstraksi dilakukan dengan mengambil nilai setiap 2 bit paling kanan dari setiap nilai R (Red), G (Green) dan B (Blue) dan mengubah setiap 8 bit yang di dapat ke dalam nilai ASCII sehingga di dapatkan ciphertext sebagai berikut :

TABEL 3. EKSTRAKSI CIPHERTEXT

R	G	B	R	G	B	R	G	B
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
01	**00**	**01**	**00**	**01**	**01**	**01**	**11**	**01**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
00	**10**	**01**	**01**	**00**	**00**	**01**	**01**	**00**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
10	**00**	**01**	**01**	**00**	**11**	**01**	**00**	**00**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
11	**01**	**01**	**01**	**11**	**01**	**01**	**00**	**11**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
01	**00**	**11**	**10**	**01**	**00**	**01**	**00**	**01**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
01	**01**	**01**	**01**	**00**	**00**	**10**	**01**	**01**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
00	**11**	**01**	**00**	**01**	**11**	**01**	**00**	**11**
01	01	01	01	01	01	01	01	01
01	01	01	01	01	01	01	01	01
10	10	10	10	10	10	10	10	10
01	**01**	**00**	**10**	**11**	11	01	01	01

0	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**=**	**D**
0	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**=**	**W**
0	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**=**	**I**
0	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**=**	**A**
0	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**=**	**H**
0	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**=**	**S**
0	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**=**	**C**
0	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**=**	**W**
0	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**=**	**S**
0	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**=**	**N**
0	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**=**	**D**
0	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**=**	**U**
0	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**=**	**B**
0	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**=**	**S**
0	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**=**	**G**
0	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**=**	**M**
0	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**=**	**K**

Dari proses ekstraksi di dapatkan ciphertext berupa "**DWIAHSCWSN DUBSGMK**"

d. Proses Dekripsi

Ciphertext (C) : DVIZHSCWSN DUBSGMK
Kunci (K) : SAVE

P1 = (K1 - C1) mod 26
= (S - D mod 26
= (18 - 3) mod 26
=15
= P

P2 = (K2 - C2) mod 26
= (A - W) mod 26
= (0 - 22) mod 26
= 4
= E

P3 = (K3 - C3) mod 26
= (V - I) mod 26
= (21 - 8) mod 26
= 13
= N

P4 = (K4 - C4) mod 26
= (E - A) mod 26
= (4 - 0) mod 26
= 4
= E

P5 = (K5 - C5) mod 26
= (S - H) mod 26
= (18 - 7) mod 26
= 11
= L

P6 =(K6-C6) mod 26
= (A- S) mod 26
= (0 - 18) mod 26
= 8
= I

P7 = (K1 - C7) mod 26
= (V - C mod 26
= (21 - 2) mod 26
= 19
= T

P8 =(K2-C8) mod 26
= (E - W) mod 26
= (4 - 22) mod 26
= 8
= I

P9 = (K3 - C9) mod 26
= (S - S) mod 26
= (18 - 18) mod 26
= 0
= A

P10=(K4-C10)mod 26
= (A - N) mod 26
= (0 - 13) mod 26
= 13
= N

P11=(K5-C11) mod 26
= (V - D) mod 26
= (21 - 3) mod 26
= 18
= S

P12=(K6–C12)mod 26
= (E- U) mod 26
= (4 - 20) mod 26
= 10
= K

P13=(K1-C13) mod 26
= (S - B) mod 26
= (18 - 1) mod 26
= 17
= R

P14=(K2-C14) mod 26
= (A - S) mod 26
= (0 - 18) mod 26
= 8
= I

P15=(K3-C15) mod 26
= (V - G) mod 26
= (21 - 6) mod 26
= 15
= P

P16=(K4-C16) mod 26
= (E - M) mod 26
= (4 - 12) mod 26
= 18
= S

P17=(K5-C17) mod 26
= (S - K) mod 26
= (18 - 10) mod 26
= 8
= I

Dari proses dekripsi di dapatkan plaintext berupa "**PENELITIAN SKRIPSI**"

3.2 Hasil

Pada penelitian ini telah dihasilkan sebuah aplikasi yang dapat digunakan untuk mengamankan pesan yang terdapat pada sebuah file text menggunakan kombinasi algoritma beaufort dan LSB2bit.

3.2.1 Desain Antarmuka

a. Tampilan Halaman Utama

Halaman utama dari aplikasi dapat dilihat pada Gambar 2 sebagai berikut :

Gambar 3. Halaman Utama

b. Tampilan Halaman Sisipkan

Halaman sisipkan digunakan dalam proses enkripsi pesan dan menyisipkannya ke dalam sebuah citra digital. Proses enkripsi dan penyisipan pesan dapat dilihat pada Gambar 3.

Gambar 4. Halaman Sisipkan

c. Halaman Ekstraksi

Halaman ekstraksi digunakan untuk menampilkan teks yang telah disisipkan ke dalam citra dan melakukan proses dekripsi. Proses ekstraksi dan dekripsi teks dapat dilihat pada Gambar 4.

Gambar 5. Halaman Ekstraksi

d. Halaman Tentang

Halaman tentang menampilkan informasi peneliti. Proses menampilkan halaman tentang pada aplikasi dapat dilihat pada Gambar 5.

Gambar 6. Halaman Tentang

3.2.2 Hasil Pengujian Aplikasi

Berdasarkan pengujian aplikasi, dihasilkan sebuah *stego image* dari proses pengamanan pesan dan *plaintext* dari proses ekstraksi *stego image*.

Gambar 7. Citra Digital

Gambar 8. Plaintext

Gambar 9. Hasil Enkripsi

Gambar 10. Stego Image

Gambar 11. Ekstraksi Pesan

Gambar 12. Hasil Dekripsi

4. Kesimpulan dan Saran

Berdasarkan hasil dan pembahasan yang telah dihasilkan pada penelitian ini, dihasilkan sebuah aplikasi yang dapat digunakan untuk mengamankan pesan teks yang terdapat pada sebuah file teks dan menyisipkannya pada citra digital. Proses pengamanan dan penyisipan teks pada sebuah file teks ke dalam citra digital dilakukan menggunakan kombinasi teknik kriptografi dan steganografi.

Algoritma yang digunakan untuk proses pengamanan teks adalah algoritma beaufort cipher dan proses penyisipan pesan menggunakan algoritma LSB2bit. Aplikasi keamanan pesan ini dikembangkan menggunakan perangkat lunak Android Studio dengan bahasa pemrograman Java dan XML.

Adapun citra digital yang dapat digunakan dalam proses keamanan dan penyisipan pesan adalah citra digital dengan ekstensi .jpeg dan .png. Citra yang telah dihasilkan menggunakan aplikasi pada penelitian ini akan tersimpan dalam format .png.

Adapun saran yang diberikan penulis untuk menyempurnakan aplikasi adalah diharapkan agar aplikasi dikembangkan sehingga dapat juga digunakan pada perangkat desktop. Selain itu, diharapkan penambahan fitur untuk dapat mengirimkan citra yang telah disisipkan pesan secara langsung setelah proses penyisipan pesan, serta penambahan jenis media yang dapat disisipkan pesan seperti pada media video dan audio.

5. UCAPAN TERIMA KASIH

Penulis ucapkan terima kasih kepada Bapak Abdul Halim Hasugian, M.Kom dan Bapak Yusuf Ramadhan Nasution, M.Kom selaku dosen pembimbing yang telah membantu penulis selama melakukan penelitian.

Daftar Pustaka:

[1] R. A. Megantara and F. A. Rafrastara, "Super Enkripsi Teks Kriptografi menggunakan Algoritma Hill Cipher dan Transposisi Kolom," *Pros. SENDI_U 2019*, pp. 85–92, 2019.

[2] Z. Basim and P. Painem, "Implementasi Kriptografi Algoritma RC4 Dan 3DES dan Steganografi Dengan Algoritma EOF Untuk Keamanan Data Berbasis Desktop Pada SMK As-Su'udiyyah," *Skanika*, vol. 3, no. 4, pp. 45–52, 2020, [Online]. Available: http://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/1739

[3] Suhardi, "Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-or (Xor)," *J. Teknovasi*, vol. 03, no. 2, pp. 23–31, 2016.

[4] H. Santoso and M. Fakhriza, "Perancangan Aplikasi Keamanan File Audio Format Wav (Waveform) Menggunakan Algoritma Rsa," *Algoritm. J. Ilmu Komput. dan Inform.*, vol. 2, no. 1, pp. 47–54, 2018, [Online]. Available: http://jurnal.uinsu.ac.id/index.php/algoritma/article/view/1615

[5] M. F. Syawal, D. C. Fikriansyah, and N. Agani, "Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB," *J. TICOM*, vol. 4, no. 3, pp. 91–99, 2016.

[6] A. Rachmadsyah, A. Perdana, and A. Budiman, "Kombinasi Algoritma Beaufort Cipher dan Vigenere Cipher untuk Pengamanan Pesan Teks Berbasis Mobile Application," *J. Minfo Polgan*, vol. 9, no. September, pp. 12–17, 2020.

[7] E. Nirmala, "Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 36, 2020, doi: 10.32493/informatika.v5i1.4646.

[8] E. R. Djuwitaningrum and M. Apriyani, "Text Message Steganography Using Least Significant Bit Method & Linear Congruential Generator Algorithm," *Juita*, vol. IV, no. 2, pp. 79–85, 2019.

[9] Verawati and P. D. Liksha, "Aplikasi Akuntansi Pengolahan Data Jasa Service Pada Pt. Budi Berlian Motor Lampung," *J. Sist. Inf. Akunt.*, vol. 1, no. 1, pp. 1–14, 2018.
[10] T. I. Pramadana, S. Soro, and R. D. Siswanto, "Pengembangan Aplikasi Bangun Datar Sederhana (Bandara) Matematika Berbasis Android Pada Materi Bangun Datar Sederhana di Tingkat SMP," *Pros. Semin. Nas. Teknoka*, vol. 3, no. 2502, p. 13, 2019, doi: 10.22236/teknoka.v3i0.2894.
[11] Y. R. Nasution and M. Furqan, "Aplikasi Mobile Media Pembelajaran Dasar Algoritma dan Pemrograman Berbasis Android," *Syntax J. Softw. Eng. Comput. Sci. Inf. Technol.*, vol. 1, no. 1, pp. 45–51, 2020, doi: 10.46576/syntax.v1i1.791.
[12] N. S. Sibarani, G. Munawar, and B. Wisnuadhi, "Analisis Performa Aplikasi Android Pada Bahasa Pemrograman Java dan Kotlin. In Prosiding Industrial Research Workshop and National Seminar," vol. 9, no. December, 2018.
[13] I. Al Fikri, "Aplikasi Navigasi Berbasis Perangkat Bergerak dengan Menggunakan Platform Wikitude untuk Studi Kasus Lingkungan ITS," *J. Tek. ITS*, vol. 5, no. 1, pp. 48–51, 2016, doi: 10.12962/j23373539.v5i1.14511.
[14] S. Andriyani, "Aplikasi Akademik Online Berbasis Mobile Android," *J. Sains dan Teknol. Utama, Vol. XI, Nomor 1, April 2016*, vol. XI, no. 152, pp. 15–26, 2017.
[15] E. Maiyana, "Pemanfaatan Android Dalam Perancangan Aplikasi Kumpulan Doa," *J. Sains dan Inform.*, vol. 4, no. 1, pp. 54–65, 2018, doi: 10.22216/jsi.v4i1.3409.