JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i3.9527

STRATEGI PENGAMANAN DATA PADA VIDEO DIGITAL DENGAN METODE RIVEST CODE 4 (RC4) DAN LEAST SIGNIFICANT BIT (LSB)

Riza Afriza Fazrin Butar Butar[1*], Abdul Halim Hasugian[2], Sulindawaty[3]

[1,2,3]Universitas Islam Negri Sumatera Utara; Jl. Lapangan Golf, Durian Jangak, Tuntungan; 6288906021429

Keywords:
Kriptografi, Steganografi, RC4, LSB, Video Digital

Corespondent Email:
simpledevelopt@gmail.com

Abstrak. Dalam era digital, kebutuhan akan keamanan data menjadi sangat penting untuk mencegah terjadinya pencurian maupun penyalahgunaan informasi. Salah satu upaya yang dapat dilakukan adalah dengan menggabungkan teknik kriptografi dan steganografi. Penelitian ini bertujuan untuk mengamankan data teks dengan menerapkan algoritma Rivest Code 4 (RC4) sebagai metode enkripsi dan algoritma Least Significant Bit (LSB) sebagai metode penyisipan data ke dalam media video digital. Metode penelitian yang digunakan adalah System Development Life Cycle (SDLC) dengan model waterfall yang meliputi tahap analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan pengembangan. Aplikasi dibangun berbasis Android menggunakan Android Studio dengan bahasa pemrograman Java dan XML. Proses pengamanan data dilakukan dengan mengenkripsi pesan teks menggunakan RC4, kemudian hasil enkripsi disisipkan ke dalam frame video menggunakan metode LSB. Hasil penelitian menunjukkan bahwa sistem yang dikembangkan mampu mengamankan data teks dengan baik serta menyembunyikannya ke dalam file video berformat MP4 tanpa memengaruhi kualitas visual secara signifikan. Proses enkripsi, penyisipan, ekstraksi, dan dekripsi dapat berjalan dengan baik berdasarkan hasil pengujian yang dilakukan. Berdasarkan hasil tersebut, dapat disimpulkan bahwa kombinasi algoritma RC4 dan LSB efektif digunakan sebagai metode pengamanan data pada video digital, serta aplikasi yang dibangun dapat membantu melindungi informasi dari akses yang tidak sah.

Abstract. *In the digital era, the need for data security has become increasingly important to prevent unauthorized access, data theft, and misuse of information. One approach to enhancing data security is by combining cryptography and steganography techniques. This study aims to secure text data by applying the Rivest Code 4 (RC4) algorithm as an encryption method and the Least Significant Bit (LSB) algorithm as a data embedding technique into digital video media. The research method used is the System Development Life Cycle (SDLC) with the waterfall model, which includes requirement analysis, system design, implementation, testing, and development stages. The application is developed based on the Android platform using Android Studio with Java and XML programming languages. The security process involves encrypting text messages using RC4, then embedding the encrypted data into video frames using the LSB method. The results show that the developed system is capable of securing text data effectively and embedding it into MP4 video files without significantly affecting visual quality. The processes of encryption, embedding, extraction, and decryption run successfully based on the conducted testing. Based on these results, it can be concluded that the combination of RC4 and LSB algorithms is effective for securing data in*

digital video, and the developed application can help protect information from unauthorized access.

1. PENDAHULUAN

Dalam aktivitas komunikasi sehari-hari, individu sering memerlukan suatu mekanisme keamanan guna melindungi informasi pribadi dari potensi penyalahgunaan oleh pihak yang tidak berwenang. Mekanisme tersebut dirancang untuk mencegah terjadinya akses ilegal terhadap data sensitif yang dapat menimbulkan kerugian. Seiring dengan perkembangan teknologi informasi, berbagai pendekatan telah dikembangkan untuk menjaga kerahasiaan data, di antaranya adalah kriptografi dan steganografi.

Kriptografi merupakan teknik pengamanan informasi dengan memanfaatkan algoritma matematika dan kunci tertentu untuk mengubah data menjadi bentuk yang tidak dapat dipahami (ciphertext). Dengan demikian, hanya pihak yang memiliki kunci yang sesuai yang dapat mengembalikan data tersebut ke bentuk aslinya (plaintext), sehingga kerahasiaan informasi tetap terjaga [1].

Di sisi lain, steganografi adalah metode pengamanan data dengan cara menyembunyikan informasi ke dalam media lain seperti gambar, audio, atau video, sehingga keberadaan pesan tersebut tidak terdeteksi oleh pihak luar. Teknik ini lebih menekankan pada penyamaran keberadaan pesan dibandingkan isi pesan itu sendiri.

Dalam implementasinya, kombinasi antara kriptografi dan steganografi sering digunakan untuk meningkatkan tingkat keamanan data. Informasi terlebih dahulu dienkripsi menggunakan metode kriptografi, kemudian disisipkan ke dalam media menggunakan teknik steganografi. Pendekatan ini dinilai lebih efektif karena tidak hanya menjaga kerahasiaan isi pesan, tetapi juga menyembunyikan keberadaan pesan tersebut dari pihak yang tidak berwenang [2].

Islam merupakan agama yang memberikan perhatian besar terhadap aspek keamanan dan perlindungan. Nilai ini dapat dilihat dalam kisah Nabi Zulkarnaen yang diabadikan dalam Al-Qur'an ketika menghadapi ancaman Ya'juj dan Ma'juj. Dalam kisah tersebut, Nabi Zulkarnaen memperoleh petunjuk dari Allah SWT untuk membangun suatu penghalang yang kokoh dan tinggi sebagai bentuk perlindungan bagi masyarakat dari ancaman kerusakan yang ditimbulkan.

Penghalang tersebut dibangun menggunakan material yang kuat, seperti besi yang disusun berlapis dan diperkuat dengan tembaga cair, sehingga menghasilkan benteng yang tidak mudah ditembus. Upaya ini menunjukkan bahwa konsep keamanan dalam Islam tidak hanya bersifat spiritual, tetapi juga mencakup tindakan nyata untuk melindungi masyarakat dari ancaman yang berbahaya. Dengan demikian, prinsip perlindungan ini menjadi landasan penting dalam berbagai aspek kehidupan, termasuk dalam konteks teknologi modern.

Mengacu pada konsep tersebut, penelitian ini mengadopsi pendekatan keamanan ganda dalam perlindungan data dengan memanfaatkan algoritma kriptografi dan steganografi. Algoritma Rivest Code 4 (RC4) digunakan sebagai metode kriptografi untuk mengenkripsi data sehingga hanya pihak yang memiliki kunci tertentu yang dapat mengakses informasi tersebut. RC4 dikenal sebagai algoritma stream cipher yang memiliki keunggulan dalam kecepatan dan efisiensi proses enkripsi [3].

Selain itu, penelitian ini juga menerapkan metode steganografi Least Significant Bit (LSB), yaitu teknik penyisipan data dengan memodifikasi bit paling rendah pada media digital, seperti citra. Dengan metode ini, keberadaan pesan tersembunyi tidak mudah terdeteksi karena perubahan yang dilakukan tidak terlihat secara kasat mata, sehingga media tetap tampak normal bagi pengamat.

Integrasi antara algoritma RC4 dan metode LSB menghasilkan sistem keamanan yang lebih optimal, karena tidak hanya melindungi isi informasi melalui proses enkripsi, tetapi juga menyembunyikan keberadaan pesan tersebut dalam media tertentu. Pendekatan ini dinilai efektif dalam menjaga kerahasiaan data sensitif dari akses pihak yang tidak berwenang, sejalan dengan prinsip perlindungan yang diajarkan dalam Islam [4].

Berdasarkan latar belakang tersebut, penelitian ini akan mengembangkan sebuah aplikasi yang berfungsi untuk mengamankan data dan menyisipkannya ke dalam file video. Oleh karena itu, judul penelitian ini adalah "Strategi Pengamanan Data pada Video Digital dengan Metode Rivest Code 4 (RC4) dan Least Significant Bit (LSB)".

2. TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu *cryptos* yang berarti tersembunyi dan *graphia* yang berarti tulisan atau ilmu. Secara umum, kriptografi dapat dipahami sebagai suatu disiplin ilmu sekaligus teknik yang digunakan untuk menjaga kerahasiaan informasi dari pihak yang tidak berwenang. Dalam perkembangannya, kriptografi tidak hanya berfungsi untuk menyembunyikan pesan, tetapi juga mencakup aspek penting dalam keamanan informasi seperti kerahasiaan (*confidentiality*), keutuhan data (integrity), keaslian (*authentication*), serta *keabsahan* sumber data (*non-repudiation*) [5].

Kriptografi bekerja dengan memanfaatkan algoritma matematika untuk mengubah data asli menjadi bentuk yang tidak dapat dipahami tanpa kunci tertentu. Oleh karena itu, penerapan kriptografi menjadi sangat penting dalam sistem informasi modern, terutama dalam melindungi data dari ancaman kebocoran, manipulasi, maupun akses ilegal. Selain itu, perkembangan teknologi seperti *blockchain* dan sistem digital lainnya semakin memperkuat peran kriptografi sebagai fondasi utama dalam menjaga keamanan dan privasi data pengguna [6].

2.2 Algoritma Rivest Code 4 (RC4)

RC4 merupakan algoritma kriptografi jenis *stream cipher* yang banyak digunakan dalam sistem keamanan data karena memiliki struktur sederhana dan proses yang cepat. Algoritma ini bekerja dengan menghasilkan *keystream* yang kemudian dikombinasikan dengan *plaintext* menggunakan operasi XOR untuk menghasilkan *ciphertext*. RC4 memproses data dalam satuan byte dan menggunakan array substitusi (S-box) berukuran 256 byte yang diinisialisasi berdasarkan kunci untuk menghasilkan aliran kunci yang bersifat pseudo-random.

Meskipun dikenal efisien, RC4 memiliki beberapa kelemahan, seperti kemungkinan munculnya pola berulang pada *keystream* serta kerentanan terhadap serangan tertentu, misalnya *known-plaintext attack*. Oleh karena itu, dalam penerapannya RC4 sering dikombinasikan dengan metode lain guna meningkatkan tingkat keamanan data [7].

Beberapa penelitian terbaru juga menunjukkan bahwa RC4 tetap relevan digunakan karena kecepatan prosesnya, terutama pada sistem yang membutuhkan efisiensi tinggi, meskipun perlu dilakukan evaluasi keamanan secara menyeluruh sebelum diimplementasikan pada sistem modern [8].

2.3 Steganografi

Steganografi merupakan teknik dalam keamanan informasi yang digunakan untuk menyembunyikan pesan rahasia ke dalam media yang tampak normal, sehingga keberadaan pesan tersebut tidak diketahui oleh pihak yang tidak berwenang. Istilah ini berasal dari bahasa Yunani, yaitu *steganos* yang berarti tersembunyi dan *graphy* yang berarti tulisan, sehingga diartikan sebagai "tulisan tersembunyi". Berbeda dengan kriptografi yang berfokus pada pengamanan isi pesan melalui enkripsi, steganografi lebih menitikberatkan pada penyamaran keberadaan pesan itu sendiri [9].

Dalam implementasinya, steganografi dapat diterapkan pada berbagai media digital seperti citra, audio, dan video dengan cara menyisipkan data pada bagian tertentu yang sulit dideteksi. Teknik ini berkembang dari metode tradisional seperti tinta tak terlihat menjadi metode digital berbasis manipulasi data biner. Oleh karena itu, steganografi sering digunakan sebagai metode tambahan untuk meningkatkan keamanan informasi, terutama jika dikombinasikan dengan teknik kriptografi [10].

2.4 Algoritma Least Significant Bit (LSB)

Metode *Least Significant Bit* (LSB) merupakan salah satu teknik steganografi yang banyak digunakan pada media digital seperti citra dan audio. Teknik ini bekerja dengan memodifikasi bit paling rendah dalam setiap byte data, yaitu bagian yang memiliki pengaruh

paling kecil terhadap perubahan nilai keseluruhan. Karena perubahan tersebut sangat kecil, perbedaan antara media asli dan media yang telah disisipi pesan umumnya tidak dapat dikenali secara visual oleh manusia [11].

Pendekatan LSB memanfaatkan keterbatasan persepsi manusia dalam mendeteksi perubahan kecil pada media digital, sehingga pesan dapat disembunyikan tanpa menurunkan kualitas media secara signifikan. Oleh karena itu, metode ini sering digunakan sebagai teknik penyisipan data yang sederhana, efisien, dan cukup efektif dalam menjaga kerahasiaan informasi [12].

2.5 Video Digital

Istilah video berasal dari bahasa Latin *videre* yang berarti melihat. Secara umum, video merupakan media digital yang menyajikan rangkaian gambar bergerak secara berurutan sehingga menghasilkan ilusi gerak. Media ini digunakan sebagai sarana penyampaian informasi, baik untuk tujuan edukasi, komunikasi, maupun hiburan, serta dapat menggabungkan unsur visual dan audio untuk memperkuat penyampaian pesan [13].

Video digital tersusun atas kumpulan gambar statis yang disebut *frame* yang ditampilkan secara berurutan dalam waktu tertentu. Kecepatan penayangan frame dikenal sebagai *frame per second* (FPS), yang memengaruhi kelancaran tampilan video. Setiap frame terdiri dari kumpulan piksel yang membentuk representasi visual, sehingga kualitas video dipengaruhi oleh resolusi dan jumlah frame yang digunakan [14].

3. METODE PENELITIAN

Untuk dapat mengimplementasikan sistem, maka secara garis besar digunakan beberapa metode sebagai berikut :

3.1 Metode Pengumpulan Data

Untuk mendapatkan informasi, data-data penunjang serta teori dalam penyusunan proposal skripsi ini, maka diperlukan teknik pengumpulan data. Teknik pengumpulan data yang dilakukan dalam penelitian ini sebagai berikut :

1. Peneltian Kepustakaan

Dalam penelitian keputusan ini penulis melakukan dengan cara mencari Jurnal dan Ebook untuk mempelajari dan menambah wawasan serta mengumpulkan referensi dasar teori yang diambil dari berbagai artikel dan jurnal pada internet yang dibutuhkan dalam penelitian.

2. Studi Literatur

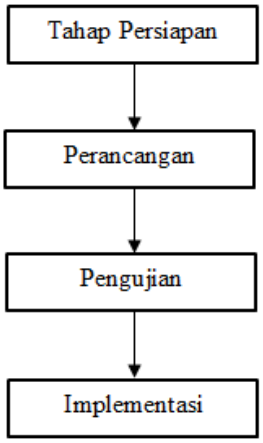
Studi Pustaka (Literatur) merupakan serangkaian yang berkenaan metode pengumpulan daftar pustaka, membaca dan mencatat, serta mengolah bahan penelitian atau menemukan referensi terkait kasus atau isu yang berkaitan dengan tugas akhir. Tujuannya untuk memberikan ide-ide untuk pengembangan kerangka konseptual pada metode penelitian berdasarkan tinjauan pustaka.

3. Observasi

Pengamatan (Observasi) merupakan salah satu teknik pengumpulan data yang efektif untuk mempelajari suatu sistem. Hal ini dilakukan dengan pengamatan secara langsung terhadap proses pengamanan yang dilakukan menggunakan algoritma Atbash. Serta proses penyisipan informasi yang diamankan menggunakan algoritma DCS ke dalam sebuah file citra digital.

3.2 Metode Perancangan Sistem

Pada bagian tahapan ini, proses perencanaan kerja dalam penelitian ini berlangsung dalam beberapa tahap, yaitu tahap persipan, desain, pengujian dan implementasi. Rencana kerja untuk penelitian ini diilustrasikan dalam diagram blok sebagai berikut.



Gambar 1. Diagram Blok Tahap Perencanaan

1. Pada tahap persiapan dilakukan serangkaian kegiatan sebelum memulai tahap pengumpulan data dan pengolahan data.

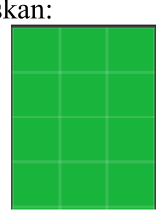
2. Perancangan penelitian ini berisikan tentang perkembangan dari tahap kebutuhan yang diubah kedalam diagram blok, *flowchart*, dan lainnya. Agar peneliti memahami alur dan fungsi rancangan yang akan dibuat.
3. Dalam fase pengujian ini, berbagai tes yang diterapkan pada langkah sebelumnya akan dilakukan dan akan menghasilkan hasil nyata.
4. Tahap implementasi adalah penerapan semua proses yang dirancang dengan baik antara perangkat keras dan perangkat lunak yang telah digabungkan dengan kode sumber.

4. HASIL DAN PEMBAHASAN

4.1 Analisa Data

Dataset yang digunakan dalam penyelidikan ini mencakup pesan teks, yang mungkin mencakup huruf, angka, dan simbol yang langsung dimasukkan ke dalam sistem, serta file video yang dimaksudkan untuk berfungsi sebagai media untuk menyematkan data yang diamankan. Metodologi yang melibatkan penerapan algoritma RC4 dan algoritma LSB dalam penelitian ini dapat digambarkan sebagai berikut :

Misalnya: Pesan yang direpresentasikan sebagai “HALLO” harus dienkripsi menggunakan kunci “2573”. Ciphertext yang dihasilkan dari prosedur enkripsi akan disematkan dalam bingkai video yang memiliki nilai RGB (R = 25, G = 180, B = 60) dengan cara yang dijelaskan:



Gambar 2. Frame Video Digital

Selanjutnya nilai masing-masing RGB dari frame video tersebut dikonversi ke dalam bentuk biner. Hasil dari konversi nilai desimal RGB tersebut ke dalam biner adalah sebagai berikut :

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

Proses pengamanan data menggunakan kombinasi algoritma RC4 dan LSB dapat dilihat sebagai berikut :

1. Proses Enkripsi Algoritma RC4

Dokumen ini menyajikan penyebaran cipher RC4 menggunakan konfigurasi 4-byte, disesuaikan untuk aplikasi tertentu dan persyaratan sistem terbatas. S-Box didefinisikan memiliki panjang 4 byte, diinisialisasi sebagai S [0] = 0, S [1] = 1, S [2] = 2, dan S [3] = 3, menghasilkan array S menjadi: 0 1 2 3. Array kunci 4-byte, dilambangkan sebagai K, diinisialisasi. Dengan asumsi kunci diatur ke 2 5 7 3, array K oleh karena itu akan terdiri dari elemen 2 5 7 3, dengan maksud untuk mengenkripsi istilah HALO. Variabel i dan j diinisialisasi ke 0, diikuti dengan eksekusi Key-Scheduling Algorithm (KSA) untuk menghasilkan array status acak. Metodologi untuk mengeksekusi KSA dalam kerangka algoritma RC4 digambarkan sebagai berikut :

Iterasi 1
i = 0
j = (0 + S[0] + K [0]) mod 4
= (0 + 0 + 2) mod 4
= 2
Swap (S[0],S[2])
Hasil Array S
2 1 0 3

Iterasi 2
i = 1
j = (2 + S[1] + K [1]) mod 4
= (2 + 1 + 5) mod 4
= 0
Swap (S[1],S[0])
Hasil Array S
1 2 0 3

Iterasi 3
i = 2
j = (0 + S[2] + K [2]) mod 4
= (0 + 0 + 7) mod 4
= 3
Swap (S[2],S[3])
Hasil Array S
1 2 3 0
Iterasi 4
i = 3
j = (3 + S[3] + K [3]) mod 4
= (3 + 0 + 3) mod 4
= 2
Swap (S[3],S[2])
Hasil Array S
1 2 0 3

Setelah pelaksanaan Key Scheduling Algorithm (KSA), Pseudo-Random Generation Algorithm (PRGA) akan digunakan. PRGA akan dieksekusi lima kali, sesuai dengan panjang lima karakter dari plaintext yang dijadwalkan untuk enkripsi. Proses ini diperlukan oleh persyaratan satu kunci kriptografi dan operasi XOR tunggal untuk setiap karakter dalam plaintext. Berikut ini menggambarkan fase yang terlibat dalam pembuatan kunci enkripsi menggunakan PRGA.

Array S
1 2 0 3
Inisialisasi
i = 0
j = 0
Iterasi 1
i = (0 + 1) mod 4
= 1
j = (0 + S[1]) mod 4
= (0 + 2) mod 4
= 2
swap (S[1],S[2])
1 0 2 3
K1= S[(S[1] + S[2]) mod 4]
= S[2 mod 4]
= 2
K1= 00000010
Iterasi 2
i = (1 + 1) mod 4
= 2
j = (2 + S[2]) mod 4
= (2 + 2) mod 4
= 0
swap (S[2],S[0])
2 0 1 3
K2= S[(S[2] + S[0]) mod 4]
= S[3 mod 4]
= 3
K2= 00000011
Iterasi 3
i = (2 + 1) mod 4
= 3
j = (0 + S[3]) mod 4
= (0 + 3) mod 4
= 3
swap (S[3],S[3])
2 0 1 3
K3= S[(S[3] + S[3]) mod 4]
= S[6 mod 4]
= 2
K3= 00000010
Iterasi 4
i = (3 + 1) mod 4
= 0
j = (3 + S[0]) mod 4
= (3 + 2) mod 4
= 1
swap (S[0],S[1])
0 2 1 3
K1= S[(S[0] + S[0]) mod 4]
= S[2 mod 4]
= 2
K4= 00000010

Setelah menentukan kunci yang sesuai dengan setiap karakter, operasi XOR dijalankan antara karakter plaintext dan kunci yang dihasilkan. Disediakan di bawah ini adalah tabel ASCII yang mewakili setiap karakter yang ada dalam plaintext yang digunakan.

Huruf	(Binary 8 bit)
H =	01001000
A =	01000001
L =	01001100
O =	01001111

Berikut adalah proses peng-XOR-an dari plaintext dengan key yang telah didapat :

HALO = 01001000 01000001 01001100 01001111
Key = 00000010 00000011 00000010 00000010 ⊕
Ciphertext = **01001010 01000010 01001110 01001101**

2. Proses Penyisipan

Proses penyisipan dilakukan dengan cara menggantikan nilai bit paling kanan dari setiap nilai R (Red), G (Green) dan B (Blue) dengan nilai biner ciphertext sehingga di hasilkan :

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

10	01	11	10	01	11	10	01	11
00	01	00	00	01	00	01	00	00
00	10	00	00	10	00	00	10	00
01	11	11	01	11	11	01	11	11
10	01	11	10	01	11	10	01	11
01	00	00	00	00	01	00	00	01
00	10	00	00	10	00	00	10	00
01	11	11	01	11	11	01	11	11
10	01	11	10	01	11	10	01	11
00	00	01	01	01	00	00	01	00
00	10	00	00	10	00	00	10	00
01	11	11	01	11	11	01	11	11
10	01	11	10	01	11	10	01	11
00	01	01	00	01	00	01	00	00

Hasil penyematan ciphertext diilustrasikan dalam representasi bit berwarna (RGB) yang disebutkan di atas. Nilai piksel dalam gambar yang dimodifikasi diubah semata-mata dalam bit yang paling tidak signifikan, sehingga menjaga integritas visual gambar digital.

3. Proses Ekstraksi

Prosedur ekstraksi dilakukan dengan memanfaatkan nilai masing-masing bit paling kanan individu dari nilai R (Merah), G (Hijau), dan B (Biru), kemudian mengubah setiap 8 bit yang memenuhi syarat menjadi representasi karakter sesuai dengan skema pengkodean ASCII, sehingga menghasilkan ciphertext yang dihasilkan :

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

01001010 = J
01000010 = B
01001101 = M
01001110 = N

Dari proses ekstraksi di dapatkan ciphertext berupa “JBMN”

4. Proses Dekripsi

Dekripsi ciphertext melalui penerapan algoritma RC4 mencerminkan prosedur penjadwalan kuncinya. Untuk mendapatkan plaintext, ciphertext mengalami operasi XOR dengan byte pseudo-random yang dihasilkan sebelumnya. Operasi XOR ini melibatkan byte pseudo-acak dan ciphertext selama fase dekripsi, khususnya.

Ciphertext = 01001010 01000010 01001110 01001101
Key = 00000010 00000011 00000010 00000010 ⊕
Plaintext = 01001000 01000001 01001100 01001111

Selanjutnya mengubah biner plaintext yang di hasilkan ke dalam bentuk karakter sehingga akan di dapatkan pesan :

(Binary 8 bit)	Huruf
01001000	= H
01000001	= A
01001100	= L
01001111	= O

4.2 Pengujian Aplikasi

Berikut ini merupakan hasil pengujian aplikasi saat dijalankan pada smartphone android. Hasil pengujian dari masing-masing halaman dapat dilihat sebagai berikut :

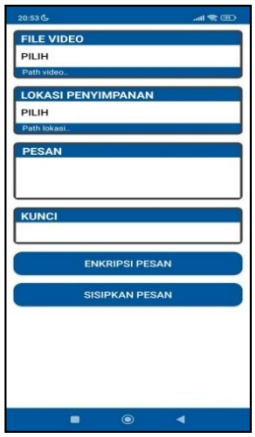
1. Tampilan Halaman Utama

Halaman utama dari aplikasi dapat dilihat pada gambar 3 sebagai berikut :

Gambar 3. Tampilan Halaman Utama

2. Tampilan Halaman Mengamankan Data

Halaman mengamankan data digunakan dalam proses mengamankan data pesan dan menyisipkannya ke dalam sebuah file video. Tampilan halaman mengamankan data dapat dilihat pada gambar 4.



Gambar 4. Tampilan Halaman Mengamankan Data

3. Tampilan Halaman Mengembalikan Data

Halaman mengembalikan data digunakan untuk melakukan ekstrak data pesan yang terdapat pada file video steganografi dan melakukan proses dekripsi untuk mengembalikan data ke dalam bentuk aslinya. Tampilan halaman mengembalikan data dapat dilihat pada gambar 5.

Gambar 5. Tampilan Halaman Mengembalikan Data

4. Tampilan Halaman Tentang

Halaman tentang menampilkan informasi peneliti. Tampilan halaman tentang pada aplikasi dapat dilihat pada gambar 6.

Gambar 6. Tampilan Halaman Tentang

5. KESIMPULAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan yang telah dihasilkan pada penelitian ini, dapat disimpulkan :

1. Penelitian ini telah berhasil mengkombinasikan teknik kriptografi dan steganografi untuk mengamankan data.
2. Algoritma yang dikombinasikan untuk mengamankan data pada penelitian ini adalah algoritma Rivest Code 4 (RC4) dan algoritma Least Significant Bit (LSB).
3. Pada penelitian ini telah dibangun sebuah aplikasi berbasis android yang dapat digunakan untuk melakukan proses pengamanan data dengan kombinasi algoritma RC4 dan algoritma LSB.
4. Data yang dapat diamankan menggunakan aplikasi pada penelitian ini adalah berupa data pesan teks yang dapat terdiri dari huruf, angka dan simbol.
5. Media yang digunakan untuk menyisipkan data yang telah diamankan adalah file video dengan ekstensi mp4.
6. Aplikasi pada penelitian ini dibangun menggunakan perangkat lunak Android Studio dengan bahasa pemrograman Java dan XML.

5.2 Saran

Untuk menyempurnakan aplikasi ini maka diberikan saran :

1. Diharapkan aplikasi ini agar dikembangkan agar dapat juga digunakan pada perangkat desktop.
2. Diharapkan untuk penambahan fitur untuk dapat mengirimkan file video yang telah memiliki data rahasia di dalamnya secara langsung melalui aplikasi.
3. Diharapkan untuk penambahan jenis ekstensi lainnya untuk dapat digunakan sebagai media penyisipan data yang telah diamankan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Islam Negeri Sumatera Utara (UINSU) yang telah memberikan dukungan,

fasilitas, dan lingkungan akademik yang kondusif sehingga penelitian ini dapat terlaksana dengan baik.

DAFTAR PUSTAKA

[1] M. M. Cynthia, E. P. Cynthia, and D. N. Cynthia, "Perbandingan Algoritma Kriptografi Modern dalam Melindungi Data Transmisi," *J. ILMU Komput. DAN Tek. INFROMATIKA*, vol. 2, no. 1, pp. 29–35, 2026.

[2] R. Sagala, A. Siallagan, and E. Telaumbanua, "Implementasi Keamanan Perangkat Lunak Menggunakan Algoritma Kriptografi dan Steganografi berbasis Web," *J. Quancom*, vol. 3, no. 1, pp. 25–31, 2025.

[3] S. R. V. Hutahuruk and M. Khairani, "Aplikasi Pengamanan Data Inventaris Menggunakan Algoritma Kriptografi Tripple DES dan RC4," *J. Comput. Sci. Inf. Technol.*, vol. 5, no. 2, pp. 13–22, 2025.

[4] S. S. Yunus, Y. S. Belutowe, and B. J. Belalawe, "PENERAPAN STEGANOGRAFI LSB DAN KRIPTOGRAFI AES- 256 DALAM KEAMANAN FILE GAMBAR," *J. Publ. Manaj. Inform.*, vol. 5, no. 2, pp. 104–119, 2026.

[5] S. I. Azzahwa, E. Maulinda, P. N. Oktavia, I. A. Fahrezi, M. Mahtuah, and Khildania, "Implementasi Sistem Keamanan Data Menggunakan Algoritma Kriptografi Simetri IDEA," *J. Ilmu Komput.*, vol. 1, no. 2, pp. 33–39, 2025.

[6] Kelvin *et al.*, "Analisis Pengaruh Blockchain Terhadap Keamanan dan Privasi Sistem Pembayaran Kriptografi," *Indones. J. Educ. Comput. Sci.*, vol. 2, no. 3, pp. 172–180, 2024.

[7] A. A. Haz and Mushlihudin, "Analisis Keamanan Pesan Teks Menggunakan Kriptografi Hybrid CBC dan RC4," *J. Sarj. Tek. Inform.*, vol. 12, no. 2, pp. 70–80, 2024.

[8] S. K. Dewi, "Perbandingan Cryptography Klasik Vigenere Cipher Dengan Cryptography Modern RC4 Dalam Tingkat Keamanan Jaringan Komputer," *J. MULTI MEDIA DAN IT*, vol. 8, no. 2, pp. 130–137, 2024.

[9] I. G. N. F. A. Krisna and A. E. Karyawati, "Penerapan Teknik Steganografi LSB pada Format Gambar Modern," *J. Nas. Teknol. Inf. dan Apl.*, vol. 2, no. 4, pp. 673–680, 2024.

[10] A. W. Laksono, S. Suhada, and A. Zakaria, "IMPLEMENTASI METODE LEAST SIGNIFICANT BIT (LSB) DALAM TEKNIK STEGANOGRAFI PADA CITRA DIGITAL MENGGUNAKAN MATLAB," *Diffus. J. Syst. Inf. Technol.*, vol. 4, no. 1, 2024.

[11] J. R. Maulidina, N. Bin Idris, and Djumhadi, "IMPLEMENTASI STEGANOGRAFI DAN STEGANALISIS MENGGUNAKAN METODE LSB (LEAST SIGNIFICANT BIT) PADA FILE GAMBAR," *Forbis J. Forensic Bus. Inf. Syst.*, vol. 1, no. 1, 2024.

[12] M. N. Al Jum'ah and Arifin, "Analisis Pengaruh Kompresi File Pada Media Sosial Terhadap Ketahanan Image Steganografi Pada Metode Least Significant Bit (LSB)," *CyberSecurity dan Forensik Digit.*, vol. 8, no. 1, pp. 97–106, 2025.

[13] J. P. Sianturi, N. S. Pratiwi, M. A. Raihan, and D. Ariwibowo, "IMPLEMENTASI TEKNOLOGI MULTIMEDIA DALAM PEMBUATAN VIDIO MOTIVASI 'EKSPRESI MUDA BENTUK NYATA UNTUK INDONESIA,'" *J. MEDIA Akad.*, vol. 3, no. 11, 2025.

[14] A. Hidayat and F. Piliang, "Rancang Bangun Sistem Informasi Penyewaan Lahan Parkir Berbasis Web Gis," *J. Sist. Inf. dan Sains Teknol.*, vol. 1, no. 1, pp. 1–9, 2019, doi: 10.31326/sistek.v1i1.320.

[15] Nugraha, S. N. (2024). Penerapan algoritma kriptografi ElGamal pada aplikasi pengamanan pesan berbasis website. *Jurnal Informatika dan Teknik Elektro Terapan*, *12*(3).