p-ISSN : 2406-7733
e-ISSN : 2597-9922

PENERAPAN ALGORITMA CAESAR CIPHER DAN METODE LEAST SIGNIFICANT BIT UNTUK MENGAMANKAN TEKS DI DALAM VIDEO

M. Iqbal Anata Pane[1], Insan Taufik[2], Hermawan Syahputra[3], Said Iskandar[4], Debi Yandra Niskah[5]
Ilmu Komputer, Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan
Jl. William Iskandar Ps. V, Kenangan Baru, Kec. Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara 20221, Medan
E-mail: iqbalanataa@gmail.com[1], insan.taufik@gmail.com[2], hsyahputra@unimed.ac.id[3], saidiskandar@unimed.ac.id[4], debiyandraniska@unimed.ac.id[5]

Abstrak - Data digital adalah representasi informasi dalam bentuk angka atau simbol yang bisa diproses oleh komputer. Jenis-jenis data digital termasuk teks, gambar, audio, video, spreadsheet, presentasi, dan basis data. Ada data yang umum dan dapat diakses oleh banyak orang, serta data rahasia yang memerlukan perlindungan khusus saat ditransmisikan melalui internet. Penelitian ini bertujuan untuk mengamankan informasi dalam video menggunakan algoritma Caesar Cipher dan metode *Least Significant Bit* (LSB). Melalui analisis dan implementasi, penelitian ini menunjukkan bahwa kombinasi kedua teknik tersebut dapat efektif melindungi teks dalam video tanpa mengubah kualitas visualnya. Hasil penelitian ini memberikan sumbangan bagi pengembangan keamanan informasi digital serta memberikan dasar bagi penelitian lebih lanjut. Selain itu, tantangan utama dalam penelitian ini adalah memperhatikan kecepatan pengolahan video agar dapat diunggah dan diunduh dengan mudah oleh pengguna. Oleh karena itu, penelitian ini tidak hanya menawarkan solusi untuk masalah keamanan informasi, tetapi juga mempertimbangkan aspek praktis dalam penerapannya. Ke depannya, penelitian dapat mengeksplorasi integrasi metode keamanan yang lebih canggih dan efisien untuk meningkatkan perlindungan data digital. Secara keseluruhan, penelitian ini menyajikan solusi yang relevan dan berpotensi untuk diterapkan secara luas dalam konteks keamanan informasi digital yang terus berkembang.

Kata Kunci: Algoritma Caesar Cipher, Teks Dalam Video, Enkripsi, Keamanan Informasi Digital, Metode Least Significant Bit (LSB), Perlindungan Informasi Digital.

I. PENDAHULUAN

Data digital merupakan representasi informasi dalam bentuk angka atau simbol-simbol yang dapat diolah oleh komputer atau perangkat elektronik lainnya. Macam-macam data digital yang umum ditemui meliputi data teks, gambar, audio, video, *spreadsheet*, presentasi, dan basis data. Data teks terdiri dari karakter, huruf, angka, dan simbol lainnya, seperti dokumen teks atau pesan teks. Data gambar adalah representasi digital dari gambar atau grafik, seperti foto atau ilustrasi. Data audio merupakan representasi digital dari suara, seperti file musik atau rekaman suara.

Data video adalah representasi digital dari gambar bergerak dan suara, seperti *file* video atau film. Video merupakan salah satu jenis media audio visual yaitu media yang mengandalkan indera pendengaran dan indera penglihatan, setiap jenis video memiliki ekstensi file yang umum digunakan seperti .mp4, .avi, .mov, dan .wmv, tergantung pada format dan kebutuhan penggunaannya. Data *spreadsheet* terstruktur dalam bentuk tabel atau lembar kerja, digunakan untuk menyimpan data yang terorganisir.

Data presentasi digunakan untuk membuat dan menyajikan materi presentasi. Sedangkan data basis data terorganisir dalam struktur yang terdefinisi dan digunakan untuk menyimpan dan mengelola informasi dalam suatu sistem. Macam-macam data digital ini memiliki format dan jenis yang beragam, tergantung pada sifat dan penggunaannya. Data atau informasi memiliki dua jenis, yaitu yang bersifat publik yang dapat diakses oleh banyak orang, dan yang bersifat pribadi atau rahasia yang hanya dapat diakses oleh orang-orang tertentu (Yusup et al., 2020).

Ketika mengirimkan informasi rahasia melalui internet, keamanan harus diprioritaskan agar informasi tersebut tidak jatuh ke tangan yang salah.Dengan cara ini, informasi tersembunyi dalam citra digital tidak akan menarik perhatian pihak yang mencoba mencuri informasi saat pengiriman melalui internet (Muadzani et al., 2016). Keamanan pengiriman informasi melalui internet merupakan hal vital yang harus diperhatikan dikarenakan banyak terjadi kebocoran data/informasi dalam berbagai sektor, perusahaan telekomunikasi asal Amerika Serikat Verizon dalam laporan risetnya menyebutkan sepanjang tahun 2021 ada 5.212 kasus kebocoran data (Annur. 2022) Badan Siber dan dan Sandi Negara (BSSN) juga melaporkan ada 311 kasus kebocoran data yang terjadi di Indonesia pada tahun 2022. (Mustajab. 2023).

p-ISSN : 2406-7733
e-ISSN : 2597-9922

Penelitian ini bertujuan untuk mengatasi masalah keamanan pengiriman informasi melalui internet dengan memanfaatkan algoritma Caesar Cipher dan Metode *Least Significant Bit* (LSB). Caesar Cipher adalah salah satu teknik enkripsi klasik yang digunakan untuk mengubah teks menjadi teks sandi dengan menggeser setiap huruf dalam teks asli sejumlah langkah tertentu. Algoritma tersebut digunakan untuk menambahkan tingkat keamanan dari pengenkripsian yang akan dilakukan.(Yusup et al., 2020). Selain itu, metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai covertext. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling depan (most significant bit atau MSB) dan bit yang paling akhir (least significant bit atau LSB). (Novianto & Setiawan, 2019).

Metode LSB juga tidak mengganggu visual secara signifikan karena hanya menggunakan bit-bit yang kurang berarti didalam suatu citra. Pada Penelitian sebelumnya (Yusup et al., 2020) menyimpulkan bahwa dari total 5 file dokumen semuanya dapat dienkripsi dengan baik,namun pada saat penyematan hanya 2 dari 5 file dokumen yang dapat disematkan. Dalam penelitian yang dilakukan (Novianto & Setiawan, 2019) menyimpulkan penyisipan informasi berjalan dengan baik dimana informasi yang disisipkan dapat diambil kembali secara penuh dan citra berwarna tidak menunjukkan perubahan yang signifikan.

Tantangan utama dalam penelitian ini adalah menggabungkan kedua metode ini sehingga teks dapat diamankan dengan baik tanpa mengorbankan kualitas visualnya. Selain itu, perlu mempertimbangkan juga kecepatan pengolahan video agar pengguna dapat mengunggah dan mengunduh video dengan mudah.

Berdasarkan pemahaman terhadap konteks sebelumnya serta hasil penelitian yang telah dilakukan, peneliti berencana untuk menjalankan sebuah penelitian dengan judul " Penerapan Algoritma Caesar Cipher dan Least Significant Bit Untuk Mengamankan Teks di dalam Video". Diharapkan bahwa penelitian ini akan memberikan kontribusi yang berharga dan dapat menjadi sumber referensi bagi penelitian-penelitian mendatang.

II. TINJAUAN PUSTAKA

1. Video

Video adalah representasi visual bergerak yang sering disertai dengan audio, yang dapat ditayangkan melalui televisi atau perangkat lainnya. Istilah "video" sendiri berasal dari bahasa Latin, yaitu "video-vidivisium", yang memiliki arti "melihat" atau "memiliki daya pengelihatan". Video merupakan salah satu bentuk dari media audio visual, yang mana jenis media ini bergantung pada kemampuan indra pendengaran dan penglihatan untuk berkomunikasi. (Wayong, 2020). Video dapat direkam menggunakan berbagai perangkat, seperti kamera video, smartphone, tablet, atau kamera digital.

Sejarah video dimulai pada abad ke-19 dengan penemuan teknologi fotografi seperti fenakistiskop dan eksperimen Eadweard Muybridge. Perkembangan berlanjut dengan penggunaan film fleksibel oleh George Eastman pada tahun 1888 dan kemunculan film suara pertama pada tahun 1927. Pada tahun 1956, Ampex Corporation memperkenalkan mesin perekam video pertama menggunakan pita magnetik, yang membuka jalan bagi video rekaman dan pemutaran dengan kualitas yang lebih baik. Era format video rumahan dimulai pada tahun 1970-an dengan munculnya Betamax dan VHS. Perkembangan digital memainkan peran penting, dengan munculnya video digital pada tahun 1990-an dan format video tinggi definisi (HD) serta video 4K. Teknologi video terus berkembang dengan munculnya video 360 derajat dan kemudahan berbagi video melalui platform online. Sejarah video mencerminkan evolusi teknologi rekaman gambar bergerak yang telah menjadi bagian penting dari budaya dan komunikasi masa kini.

2. Algoritma Caesar Cipher

Algoritma adalah urutan langkah logis yang terstruktur dengan jelas dan mengikuti pola tertentu untuk memecahkan masalah tertentu. Algoritma sangat penting untuk menyelesaikan berbagai masalah pemrograman, terutama dalam konteks komputasi numeris. Kehadiran algoritma yang dirancang dengan baik sangat menentukan keberhasilan proses pemrograman, menghindari kesalahan, kerusakan, atau penurunan efisiensi. Bahasa pemrograman merupakan alat utama dalam pembuatan program, yang memiliki beragam jenis seperti C, C++, Pascal, Java, C#, Basic, Perl, PHP, ASP, JSP, J#, J++, dan masih banyak lagi. Meskipun berbeda dalam cara memberikan instruksi, berbagai bahasa pemrograman memiliki tujuan yang sama, yaitu menghasilkan output yang diinginkan.

3. Steganografi

Dalam teknik Steganografi ada banyak metode yang dapat digunakan seperti Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Least Significant Bit (LSB), dan banyak metode lainnya. Namun dalam penelitian ini peneliti akan menggunakan metode Least Significant Bit (LSB) karena dalam penelitian yang dilakukan Batarius tahun 2012 (Batarius, 2012) menunjukkan bahwa hasil dari metode LSB memiliki hasil terbaik dari segi efisiensi waktu serta kualitas gambar.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

4. Metode *Least Significant Bit*

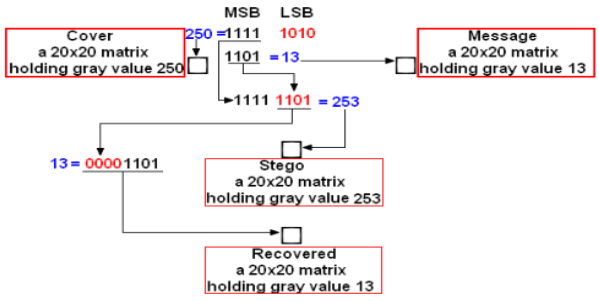
Metode *Least Significant Bit* (LSB) adalah salah satu teknik yang digunakan dalam steganografi. LSB bekerja dengan menambahkan bit data pesan yang ingin disembunyikan ke bit terakhir yang memiliki pengaruh yang paling sedikit atau kurang signifikan. Sebagai contoh, dalam sebuah gambar dengan ukuran 3 piksel, proses LSB akan bekerja sebagai berikut:

$$\begin{pmatrix} 0011111\ 11101001\ 11001000 \\ 0011111\ 11001000\ 11101001 \\ 1100000\ 00100111\ 11101001 \end{pmatrix}$$

biner 10000001, *stego image* yang akan dihasilkan adalah:

$$\begin{pmatrix} 00111111\ 111010010\ 110010000 \\ 00111110\ 110010000\ 111010010 \\ 11000000\ 001001111\ 111010011 \end{pmatrix}$$

Prinsip dasar dari metode *Least Significant Bit* (LSB) adalah dengan mengganti bit-bit yang tidak begitu penting pada gambar asli (cover image) dengan bit-bit dari pesan rahasia. Berikut adalah gambaran mekanisme metode LSB pada gambar dengan kedalaman bit 8, dimana hanya 4 bit LSB yang dimanfaatkan.



Gambar 1. Mekanisme LSB

Metode penelitian menguraikan tentang metode yang digunakan dalam pemecahan permasalahan termasuk metode yang digunakan untuk menganalisis data penelitian. Bagian ini menjelaskan pula bagaimana penelitian dilakukan (tahapan penelitian), rancangan penelitian dalam bentuk diagram alir (*flowchart*), blok diagram, alat/instrumen dan bahan penelitian.

5. Perangkat Pembangun

1. Python

Python sering dipilih oleh para programmer dalam pembuatan program karena memiliki sintaks yang mudah dipahami. Hal ini membuat Python menjadi salah satu bahasa pemrograman tingkat tinggi yang populer. Dalam penulisan kode program dengan Python, terdapat beberapa aturan yang harus diperhatikan untuk mencegah terjadinya *error* atau masalah dalam program yang dibuat. Salah satu aturan penting adalah penulisan *Statement*, yang merupakan instruksi atau kalimat perintah yang akan dieksekusi oleh komputer. Sebagai contoh, perintah "print("Hello World")" merupakan sebuah *statement* dalam Python.

2. Flask

Flask merupakan *microframework* yang memiliki inti yang sangat sederhana dan kecil, tetapi dapat berkembang dengan penambahan fitur-fitur tambahan. Karena itu, jumlah fitur bawaan Flask relatif sedikit, termasuk:

1. Server pengembangan bawaan.
2. Debugger yang responsif.
3. Dukungan terintegrasi untuk pengujian unit.
4. Kompatibilitas dengan mesin aplikasi Google.
5. Penyaluran permintaan RESTful.
6. Templating menggunakan Jinja2.
7. Dukungan untuk cookies yang aman.
8. Berbasis Unicode.
9. Mengikuti standar WSGI 1.0.

Selain itu, Flask juga didukung dengan dokumentasi yang sangat baik dan berbagai forum di internet yang memungkinkan pengguna untuk mendiskusikan masalah terkait Flask.

3. Pustaka (*Library*)

Pustaka (*Library*) merupakan kumpulan kode yang dituliskan oleh orang lain sebelumnya dan biasanya berada pada package modul yang dapat memudahkan pengerjaan pembuatan aplikasi tanpa harus menulis kode dari awal. Berikut adalah contoh dari pustaka:

a) OpenCV (*Computer Vision*)

OpenCV (*Open Computer Vision*) adalah sebuah perpustakaan perangkat lunak sumber terbuka yang dirancang untuk melakukan berbagai fungsi pengolahan citra. Tujuannya adalah untuk memungkinkan komputer untuk melakukan tugas-tugas yang biasanya dilakukan manusia dalam pengolahan data visual. (Ulfah et al., 2023).

b) PIL (Python Image Library)

PIL (Python Image Library) adalah sebuah pustaka (*library*) Python yang populer untuk memanipulasi dan memanajemen gambar. PIL menyediakan beragam fungsi dan metode yang memungkinkan pengguna untuk membaca, menulis, mengedit, dan mengolah berbagai jenis format gambar.

c) Numpy

NumPy merupakan sebuah pustaka fungsi yang memfasilitasi berbagai tugas manipulasi data umum dengan Python. Banyak interaksi antara array NumPy dan Python mirip dengan penggunaan variabel Python biasa. Selain itu, NumPy juga menyediakan fungsi-fungsi untuk tugas yang lebih lanjut seperti aljabar linear, transformasi Fourier, dan operasi matriks. (Tri et al., 2023).

p-ISSN : 2406-7733
e-ISSN : 2597-9922

d) FFMPEG

FFmpeg adalah seperangkat alat dan perpustakaan perangkat lunak sumber terbuka yang sangat kuat dan serbaguna, dirancang untuk merekam, mengonversi, dan memutar audio dan video dalam berbagai format. Dengan tujuan utama menyediakan solusi multimedia yang fleksibel dan platform-agnostik, FFmpeg menawarkan berbagai fitur kunci.

4. HTML (*Hypertext Markup Language*)

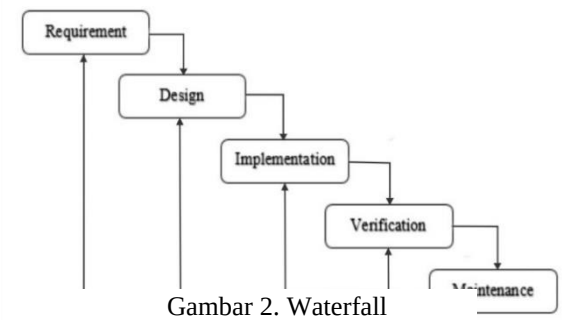
HTML merupakan sebuah bahasa pemrograman yang digunakan untuk membuat halaman web dengan kemampuan untuk menampilkan berbagai informasi, seperti teks dan gambar, pada sebuah web browser. Bahasa HTML terus mengalami perkembangan seiring dengan pertumbuhan pengguna internet yang pesat. Perkembangan ini bertujuan untuk meningkatkan kualitas halaman web agar dapat memenuhi kebutuhan pengguna.

5. CSS (*Casading Style Sheet*)

CSS merupakan bahasa pemrograman web yang digunakan untuk mengontrol dan membangun berbagai komponen dalam sebuah situs web, sehingga tampilannya menjadi lebih terstruktur, rapi, dan seragam. Terdapat dua jenis CSS yang dapat digunakan, yaitu CSS internal dan eksternal. Fungsi utama CSS adalah memberikan pengaturan yang lebih komprehensif agar struktur halaman web yang dibuat dengan HTML dapat terlihat lebih rapi dan menarik.

6. Waterfall

Waterfall, atau sering disebut sebagai air terjun, adalah model yang dirancang untuk pengembangan perangkat lunak. Model ini menggambarkan pengembangan sistem secara sistematis dari satu tahap ke tahap berikutnya, mirip dengan air terjun yang mengalir secara berurutan. Model ini mengusulkan pendekatan yang sistematik dan berurutan dalam pengembangan perangkat lunak, dimulai dari analisis, desain, pengkodean, pengujian, hingga pemeliharaan. (Astriany, 2019).



Gambar 2. Waterfall

III. METODE PENELITIAN

Penelitian ini menggunakan model waterfall untuk desain penelitiannya dimana model ini sendiri pertama kali diperkenalkan oleh Winston Royce sekitar tahun 1970. Model ini dipilih karena setiap pengerjaannya yang tersetruktur dan sistematis sehingga meminimalisir kesalahan. Berikut adalah gambar waterfall model dari penelitian ini:

1. Identifikasi Masalah

Identifikasi masalah adalah langkah awal dalam menentukan masalah dalam suatu penelitian, didalam penelitian kali ini masalah yang timbul adalah besarnya kemungkinan dalam pencurian informasi yang dikirim melalui internet.

2. Pengumpulan Data

Pada tahap ini dilakukan pengambilan data berupa video dan teks yang didapatkan menggunakan smartphone di Laboraturium Universitas Negeri Medan, Selanjutnya setelah data didapatkan dilakukan persiapan data untuk memastikan ekstensi dari video dan data teks.

3. Pengekstrakan Video

Pada tahapan ini dilakukan pembacaan dan pengekstrakan video yang telah disiapkan menggunakan library opencv-python lalu kemudian frame-frame dari video disimpan didalam folder temp untuk selanjutnya dilakukan proses penerapan algoritma dan metode pada tiap frame tersebut.

4. Penerapan Algoritma Caesar Cipher

Pada tahap ini dilakkan penerapan Algoritma Caesar Cipher untuk mempertukar huruf asli dengan huruf lain yang berjarak sesuai kunci yang telah ditentukan, dimana kunci default yang digunakan peneliti adalah 3. Kunci dapat diubah sesuai kepentingan untuk meningkatkan keamanan tetapi juga memerlukan proses dekripsi yang lebih rumit. Adapun proses penerapan Algoritma pada penelitian ini dibagi menjadi 2 yaitu:

1. Proses Enkripsi Pesan

1. Membaca teks yang diinput user.
2. Setiap karakter pesan yang diinput digeser menggunakan rumus dan kunci default yaitu 3.
3. Proses pergeseran karakter pesan diulang hingga seluruh pesan yang diinput user selesai diubah.

2. Langkah-Langkah Dekripsi

1. Membaca teks yang didapat dari frame video hasil pemrosesan LSB.
2. Setiap karakter pesan yang didapat diubah kembali menggunakan rumus dan kunci default 3.
3. Proses diulangi hingga seluruh pesan berhasil dikembalikan sesuai dengan pesan asli.
4. Pesan ditampilkan kepada user.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

5. Penerapan Metode *Least Significant Bit*

Dalam tahap ini Metode *Least Significant Bit* digunakan untuk mempertukar bit yang kurang berarti dari frame video dengan pesan yang telah dienkripsi pada tahap sebelumnya. Dalam penerapan Metode *Least Significant Bit* ini dibagi menjadi 2 yaitu:

1. Proses Penyisipan Pesan
    1. Mengubah karakter pesan menjadi biner
    2. Menghitung kapasitas penyimpanan
    3. Iterasi piksel
    4. Mengubah komponen warna ke biner
    5. Menyisipkan pesan
2. Proses Pengambilan Pesan
    1. Menghitung kapasitas penyimpanan
    2. Membaca komponen warna
    3. Rekonstruksi pesan

6. Pembentukan Ulang Video

Pada tahapan ini akan dilakukan pembentukan ulang video menggunakan library ffmpeg-python pada folder temp setelah seluruh pesan berhasil dienkripsi.

7. Perancangan Sistem

Pada Tahap ini akan dilakukan perancangan antarmuka dengan menggunakan Figma selanjutnya akan disesuaikan dengan sistem penyisipan yang telah dibuat pada tahap sebelumnya.

8. Pengujian Sistem

Pengujian sistem akan dilakukan dengan 2 metode yang pertama adalah *Black Box Testing*, dimana metode ini akan berfokus pada fungsionalitas perangkat lunak tanpa memperhatikan detail internalnya. Metode ini mencakup pembuatan data uji, menjalankan aplikasi, dan memeriksa apakah hasil yang dihasilkan sesuai dengan yang diinginkan. Dan pengujian kedua adalah pengujian performa yang dilakukan secara manual dengan menggunakan 2 operasi sistem yaitu Windows dan Linux, serta menggunakan 2 web browser yaitu *Google Chrome* dan *Mozilla Firefox* untuk mengetahui estimasi waktu yang dibutuhkan untuk melakukan penyisipan pesan dan pengambilan pesan yang telah disisipkan menggunakan kedua sistem operasi dan kedua *web browser* tersebut.

9. Penarikan Kesimpulan

Setelah selesai melakukan semua tahapan pada penelitian ini, maka akan ditarik kesimpulan yang didapatkan dari hasil penelitian yang dilakukan.

IV. HASIL DAN PEMBAHASAN

1. Pengumpulan Data

Penelitian ini menggunakan 2 jenis data yaitu data video dan data teks yang bersifat premier karena didapatkan dengan menggunakan smartphone peneliti. Video yang digunakan berekstensi .avi dan berdurasi 5 detik. Berikut adalah gambaran video yang digunakan:

Gambar 3. Cover Video

2. Pengekstrakan Video

Pada tahap ini video yang telah disiapkan dibaca dan diekstrak menjadi frame-frame gambar menggunakan library opencv-python kemudian frame-frame tersebut disimpan kedalam folder tmp untuk selanjutnya akan diakses pada tahapan selanjutnya untuk dilakukan pembacaan piksel dan penerapan Algoritma Caesar Cipher dan Metode Least Significant Bit.

3. Penerapan Algoritma Caesar Cipher

Pada penelitian ini Algoritma Caesar Cipher digunakan untuk mengamankan pesan sebelum disisipkan kedalam frame gambar, pada penelitian ini kunci yang digunakan untuk pergeseran karakter adalah 3 dan kalimat yang akan digunakan sebagai contoh penggunaan adalah: “Nama Saya M Iqbal Anata Pane Mahasiswa Ilmu Komputer Unimed”. Berikut tabel gambaran pergeseran karakter yang menggunakan kunci 3:

Tabel 1. Pergeseran Huruf

Plaintext	ABCDEFGHIJKLMNOPQRSTU
Ciphertext	DEFGHIJKLMNOPQRSTUVWXYZABC

Tabel di atas jika diformulasikan kedalam fungsi matematika menjadi A=0, B=1 C=2, …, Z=25.

1. Proses Enkripsi Pesan

Pada Tahapan ini akan dilakukan pengenkripsian pesan menggunakan rumus:

$$C = E(P) = (P + 3) \% 26$$

Dimana Chipertext (C) sama degan Enkripsi (E) sama dengan Plaintext (P) ditambah 3 modulus 26. Kalimat yang sebelumnya diinput berupa “Nama Saya M Iqbal Anata Pane Mahasiswa Ilmu Komputer Unimed” diubah menjadi “Qdpd Vdbd P Ltedo Dqdwd Sdqg Pdkdvlvzd Lopx Nrpsxwhu Xqlphg”.

2. Proses Dekripsi Pesan

Pada tahapan ini akan dilakukan pengembalian karakter pesan yang telah diacak menggunakan Algoritma Caesar Cipher pada tahapan enkripsi menjadi karakter asli dengan menggunakan rumus:

$$P = D(P) = (C-3) \% 26$$

p-ISSN : 2406-7733
e-ISSN : 2597-9922

Dimana Plaintext (P) sama dengan Dekripsi (D) sama dengan Ciphertext dikurangi 3 modulus 26. Kemudian kalimat yang telah didekripsi akan ditampilkan Kembali kepada user.

4. Penerapan Metode *Least Significant Bit*

Setelah frame diekstrak pada tahap pengekstrakan di sub bab 4.2 dan disimpan dalam folder temp, kemudian selanjutnya akan dilakukan pemrosesan pesan menggunakan Metode Least Significant Bit pada tiap-tiap piksel didalam tiap-tiap frame. Secara garis besar ada dua proses yang akan dilakukan yaitu proses penyisipan pesan dan proses pengambilan pesan, Berikut adalah penjabaran dari kedua proses tersebut:

1. **Proses Penyisipan Pesan**

Setelah frame diekstrak dan disimpan pada tahapan sebelumnya, selanjutnya akan dilakukan penyisipan pesan dengan tahap sebagai berikut:

a) Mengubah Karakter Pesan Menjadi Biner

Pada tahapan ini pertama akan dilakukan perubahan pesan menjadi format yang sesuai di tabel ASCII. Pesan yang akan di sisipkan "Nama Saya M Iqbal Anata Pane Mahasiswa Ilmu Komputer Unimed" yang telah diubah pada proses cipher menjadi "Qdpd Vdbd P Ltedo Dqdwd Sdqh Pdkdvlvzd Lopx Nrpsxwhu Xqlphg". Kemudian pesan yang akan di sisipkan akan diubah menjadi format biner. Berikut adalah contoh perubahan pesan menjadi Biner:

Huruf	ASCII	Biner	Huruf	ASCII	Biner
Q	81	01010001	(Spasi)	32	00100000
d	100	01100100	P	80	01010000
p	112	01110000	(Spasi)	32	00100000
d	100	01100100	L	76	01001100
(Spasi)	32	00100000	t	116	01110100
V	86	01010110	e	101	01100101
d	100	01100100	d	100	01100100
…					

b) Menghitung Kapasitas Penyisipan

Pada tahapan ini akan dilakukan perhitungan kapasitas penyisipan dengan rumus:

$$W \times H \times \alpha \times B$$

- W adalah Weigth atau Lebar gambar dalam piksel
- H adalah Height atau Tinggi gambar dalam piksel
- α adalah faktor yang menentukan berapa banyak bit pesan yang akan disisipkan dalam setiap komponen warna piksel
- B adalah jumlah komponen warna dalam setiap piksel (R,G,B)

Total piksel : $W \times H = 1280 \times 720 = 921{,}600$

Total pesan yang dapat disisipkan dalam 1 piksel : $\alpha \times B = 3 \times 3 = 9$

Total kapasitas penyisipan total : $921{,}600 \times 9 = 8.294{,}400$ bit

c) Iterasi Piksel

Pada tahapan ini akan dilakukan perhitungan untuk iterasi piksel dengan rumus:

$$\text{Iterasi} = i \times W + j + 1$$

- i adalah nomor baris (mulai dari 0 hingga H – 1).
- j adalah nomor kolom (mulai dari 0 hingga W – 1).
- W adalah lebar gambar (jumlah piksel dalam satu baris).

d) Mengubah Komponen Warna

Pada tahapan ini nilai-nilai desimal dari warna akan diubah menjadi biner untuk memanipulasi frame gambar dari video, nilai biner didapatkan dari hasil bagi desimal dengan angka 2 sampai dengan 0, contohnya piksel warna merah dengan nilai 234 dibagi 2 menghasilkan 177 dengan sisa bagi 0, lalu 177 dibagi 2 menjadi 58 dengan sisa bagi 1 sampai dengan 1 dibagi 2 dengan hasil 0 dan sisa bagi 1, kemudian hasilnya diambil untuk menjadi biner yaitu 11101010.

e) Menyisipkan Pesan

Pada tahapan ini akan dilakukan penyisipan pesan dengan terlebih dahulu pesan yang telah diubah menjadi biner dipisah menjadi blok-blok 8 bit selanjutnya piksel warna yang telah diambil diubah ujungnya dengan blok pesan yang telah disiapkan. Berikut adalah contoh dari penerapannya dengan pesan "Nama Saya M Iqbal Anata Pane Mahasiswa Ilmu Komputer Unimed" yang telah diubah pada tahapan sebelumnya dengan algoritma cipher pada menjadi "Qdpd Vdbd P Ltedo Dqdwd Sdqh Pdkdvlvzd Lopx Nrpsxwhu Xqlphg":

p-ISSN : 2406-7733
e-ISSN : 2597-9922

Pesan		Piksel Warna			Hasil		
Huruf	Biner	R	G	B	R	G	B
Q	01010001	234 = 11100110	235 = 11100111	238 = 11101110	11101 [010]	11101 [100]	11101 [011]
d	01100100	234 = 11101010	235 = 11101011	238 = 11101110	11101 [011]	11101 [001]	11101 [001]
p	01110000	234 = 11100110	235 = 11100111	238 = 11101110	11101 [011]	11101 [100]	11101 [001]
d	01100100	234 = 11101010	235 = 11101011	238 = 11101110	11101 [011]	11101 [001]	11101 [001]
…							

Setelah semua pesan berhasil disisipkan maka frame gambar akan disimpan dengan cara menggantikan frame asli dengan frame yang telah disisipkan pesan didalam folder temp lalu kemudian seluruh frame yang ada didalam folder temp dibentuk kembali menjadi video pada tahapan penggabungan frame menjadi video.

2. Proses Pengambilan Pesan

Pada tahapan ini akan dilakukan pengambilan pesan dengan membaca video yang telah dimodifikasi dan diekstrak menjadi frame gambar dengan proses pengekstrakan pada tahapan sebelumnya. Berikut adalah proses yang dilakukan untuk mengambil pesan didalam video modifikasi:

a) Menghitung Kapasitas Penyisipan

Pada tahapan ini akan dilakukan perhitungan kapasitas penyisipan dengan rumus:

$$W \times H \times \alpha \times B$$

- W adalah Weigth atau Lebar gambar dalam piksel
- H adalah Height atau Tinggi gambar dalam piksel
- α adalah faktor yang menentukan berapa banyak bit pesan yang akan disisipkan dalam setiap komponen warna piksel
- B adalah jumlah komponen warna dalam setiap piksel (R,G,B)

Total piksel : W × H = 1280 × 720 = 921,600

Total pesan yang dapat disisipkan dalam 1 piksel : α × B = 3 × 3 = 9

Total kapasitas penyisipan total : 921,600 × 9 = 8.294,400 bit

b) Iterasi Piksel

Pada tahapan ini akan dilakukan perhitungan untuk iterasi piksel dengan rumus:

$$\text{Iterasi} = i \times W + j + 1$$

- i adalah nomor baris (mulai dari 0 hingga H – 1).
- j adalah nomor kolom (mulai dari 0 hingga W – 1).
- W adalah lebar gambar (jumlah piksel dalam satu baris).

c) Membaca Komponen Warna

Pada tahapan ini nilai-nilai desimal dari warna akan diubah menjadi biner untuk memanipulasi frame gambar dari video, nilai biner didapatkan dari hasil bagi desimal dengan angka 2 sampai dengan 0, contohnya piksel warna merah dengan nilai 234 dibagi 2 menghasilkan 177 dengan sisa bagi 0, lalu 177 dibagi 2 menjadi 58 dengan sisa bagi 1 sampai dengan 1 dibagi 2 dengan hasil 0 dan sisa bagi 1, kemudian hasilnya diambil untuk menjadi biner yaitu 11101010.

d) Rekonstruksi Pesan

Pada tahapan ini nilai-nilai desimal dari warna akan diubah menjadi biner untuk memanipulasi frame gambar dari video, nilai biner didapatkan dari hasil bagi desimal dengan angka 2 sampai dengan 0, contohnya piksel warna merah dengan nilai 234 dibagi 2 menghasilkan 177 dengan sisa bagi 0, lalu 177 dibagi 2 menjadi 58 dengan sisa bagi 1 sampai dengan 1 dibagi 2 dengan hasil 0 dan sisa bagi 1, kemudian hasilnya diambil untuk menjadi biner yaitu 11101010. Berikut adalah contoh dari pengimplementasiannya pada kasus ini:

Tabel 2. Rekonstruksi Pesan

Piksel Warna			Rekonstruksi bit pesan	Pesan	
R	G	B		Biner	Huruf
11101 [010]	11101 [100]	11101 [011]	010 100 011	01010001	Q
11101 [011]	11101 [001]	11101 [001]	011 001 001	01100100	d
11101 [011]	11101 [100]	11101 [001]	011 100 001	01110000	p
11101 [011]	11101 [001]	11101 [001]	011 001 001	01100100	d

p-ISSN : 2406-7733
e-ISSN : 2597-9922

Setelah semua piksel pada tiap-tiap frame dicek selanjutnya seluruh pesan dikumpulkan dan direkonstruksi ulang menjadi kalimat, kalimat yang didapat dari pengecekan piksel adalah "Qdpd Vdbd P Ltedo Dqdwd Sdqh Pdkdvlvzd Lopx Nrpsxwhu Xqlphg" yang mana selanjutnya pesan yang masih berbentuk Ciphertext tersebut akan memasuki proses dekripsi dengan algoritma Caesar Cipher yang kemudian akan menghasilkan kalimat "Nama Saya M Iqbal Anata Pane Mahasiswa Ilmu Komputer Unimed". Selanjutnya pesan akan ditampilkan kepada user melalui website.

5. Pembentukan Ulang Video

Pada tahapan ini seluruh frame yang ada di folder temp akan disusun kembali menjadi video menggunakan library ffmpeg-python sesuai dengan urutan frame sebelum dilakukan penyisipan pesan.

6. Perancangan Sistem

Pada Tahapan ini akan dilakukan Perancangan Sistem dimulai dari perancangan tampilan pengguna dengan menggunakan figma.

7. Pengujian Sistem

1. *Blackbox Testing*

Blackbox Testing adalah metode pengujian perangkat lunak yang fokus pada fungsi-fungsi dari perangkat lunak tersebut. Tujuannya adalah untuk mengidentifikasi kecacatan dalam fungsi-fungsi tersebut, kesalahan antarmuka, masalah struktur data, masalah kinerja, serta kesalahan dalam tahap inisialisasi dan terminasi.

Blackbox Testing, yang juga dikenal sebagai pengujian berdasarkan fungsional atau spesifikasi aplikasi, tidak melibatkan pemeriksaan atau analisis terhadap source code program. Metode ini sepenuhnya berfokus pada spesifikasi eksternal dari aplikasi. Dalam pengujian ini, hanya dilakukan evaluasi terhadap fungsionalitas aplikasi tanpa memeriksa rincian kode sumber. Pendekatan ini mencakup pengamatan terhadap aspek-aspek dasar dari aplikasi untuk memverifikasi kesesuaian dengan kebutuhan para pemangku kepentingan. Pengujian sistem di penelitian ini menunjukkan hasil valid di setiap halaman *website*.

2. Pengujian Peforma

Pengujian peforma dilakukan dengan cara manual menggunakan *stopwatch* guna mengetahui estimasi waktu yang dibutuhkan untuk melakukan penyisipan pesan dan pengambilan pesan, pada pengujian ini dilakukan dengan 2 sistem operasi yang berbeda dan 2 web browser yang berbeda guna mengetahui pengaruh sistem operasi dan web browser. Dari hasil pengujian dapat disimpulkan disimpulkan bahwa Linux cenderung memiliki peforma yang lebih baik dalam menyisipkan pesan (*Encode*) dengan rata-rata waktu dibawah 42 detik pada kedua browser dan Windows menunjukkan waktu yang lebih lambat dibandingkan dengan Linux, khususnya waktu pengambilan pesan (*Decode*) menggunakan *Google Chrome* dengan rata rata lebih dari 3 menit (200,42 Detik). Secara keseluruhan, Linux memberikan performa yang lebih konsisten dan lebih cepat, terutama dalam hal encode, sementara Windows memerlukan lebih banyak waktu terutama saat decode video.

V. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan proses Penerapan Algoritma Caesar Cipher dan Metode *Least Significant Bit* untuk Mengamankan Teks di dalam Video, dari tahap analisis hingga implementasi, diperoleh beberapa kesimpulan sebagai berikut:

1. Penggunaan kombinasi Algoritma Caesar Cipher dan Metode *Least Significant Bit* (LSB) pada website mampu secara efektif mengamankan informasi berupa teks dalam sebuah video.
2. Kualitas video yang telah dienkripsi dan didekripsi menggunakan kombinasi Algoritma Caesar Cipher dan Metode Least Significant Bit (LSB) tidak mengalami perubahan yang signifikan.

Saran

Untuk meningkatkan kinerja sistem Penerapan Algoritma Caesar Cipher dan Metode *Least Significant Bit* untuk Mengamankan Teks di dalam Video, disarankan untuk mempertimbangkan hal-hal berikut:

1. Menyesuaikan aplikasi agar lebih fleksibel dengan mempertimbangkan format video lain seperti .mp4, .mov, dll. Hal ini akan memperluas kemampuan aplikasi dalam mengamankan teks pada berbagai jenis video.
2. Untuk meningkatkan keamanan dalam penyisipan teks, disarankan untuk mengeksplorasi penggunaan algoritma enkripsi lain selain Caesar Cipher. Dengan mempertimbangkan algoritma enkripsi yang lebih kuat, dapat meningkatkan tingkat keamanan dalam menyisipkan dan mengamankan teks dalam video.

DAFTAR PUSTAKA

Adi, I. S. (2018). Enkripsi Data Penggajian Dengan Algoritma Caesar Cipher Dan Vigenere Cipher pada PT. Kemasindo Cepat Nusantara. *Jurnal Sistem Komputer dan Teknik Informatika*, 399-404.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

Antonius, A. S. (2019). Rancang Bangun Aplikasi UNSRAT E-Catalog. *Jurnal Teknik Informatika* , 1-9.

Apriliando, A. (2021). Implementasi Framework Laravel pada Rancang Bangun Website IAKN Palangka Raya Dengan Metode Prototype. *Jurnal Sains Komputer dan Teknologi Informasi*, 87-96.

Astriany, A. R. (2019). Perancangan Sistem Informasi Perekrutan Karyawan Berbasis Web Menggunakan PHP dan MYSQL di PT. Ria Indah Mandiri. *Jurnal Manajemen Informatika*, 49-57.

Azlansyah, M. B. (2019). Penyisipan Pesan Pada Citra Digital Menggunakan Metode Least Significant Bit . *Jurnal Sains dan Seni*, A1-A6.

Bahri, G. (2019). Perancangan dan Implementasi Sistem Manajemen Peminjaman Mobil dengan Metode Scrum di Universitas Internasional Batam. Undergraduate thesis, Universitas Internasional Batam. *Jurnal Teknologi Informasi*.

Batarius, P. M. (2012). Perbandingan Metode dalam Teknik Steganografi. *Seminar Nasional Teknologi dan Komunikasi Terapan* , 307-313.

Christian, A. S. (2018). Rancang Bangun Website Sekolah Dengan Menggunakan Framework Bootstrap (Studi Kasus SMP Negeri 6 Prabumulih). *Jurnal Sistem Informasi dan Komputer* , 22-27.

Dwi, Y. P. (2019). Penerapan Kriptografi Caesar Cipher pada Fitur Chatting Sistem Informasi Freelance. *Jurnal Informasi dan Komputer*, 87-94.

Eka, D. P. (2019). Penyisipan Pesan ke dalam File Video Menerapkan Metode Chinese Remainder Theorem. *Konferensi Nasional Teknologi Informasi dan Komputer*, 108-117.

Harjumawan, I. G. (2021). Program Menghitung Banyak Bata pada Ruangan Menggunakan Bahasa Python. *TIERS Information Teknology Journal*, 1-10.

Hermiati, R. A. (2021). Pembuatan E-Commerce Pada Raja Komputer Menggunakan Bahasa Pemrograman PHP dan Database MYSQL. *Jurnal Media Infotama*, 54-66.

Lestari, E. P. (2020). *Konsep Dasar Algoritma Dan Pemrograman Dengan Bahasa Java* . -: Poliban Press.

Noviana, R. (2022). Pembuatan Aplikasi Penjualan Berbasis Web Monja Store Menggunakan PHP dan MYSQL . *Jurnal Teknik dan Science*, 112-124.

Pelipus, L. M. (2021). Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB). *Jurnal Ilmiah Wahana Pendidikan* , 343-354.

Rahadian, I. (2018). Penggunaan Python Web Framework Flask Untuk Pemula. -, 1-4.

Siswanto, E. (2021). *PHP UNCOVER (Kupas Tuntas PHP).* Semarang: Yayasan Prima Agus Teknik.

Suganda, A. G. (2017). *Steganografi dengan Least Significant Bit (LSB).* Jakarta Barat: Binus.

Wahyu, I. U. (2019). Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher Dan Vigenere Cipher. *Jurnal Sistem Informasi, Teknologi Informasi dan Komputer*, 142-149.

Wayong, N. K. (2020). Perkembangan Videography dari Ilmu Hingga Menjadi Sebuah Profesi. *Jurnal Desain Komunikasi Visual Asia* , 79-86.

Yudhi, M. P. (2020). Responsive Web Design Menggunakan Bootstrap Dalam Merancang Layout Website. *Information System For Educator and Profesionals*, 61-70.

Rumah Editor. (2019). Bahas Tuntas Perbedaan Frame Rate 24p/25p/30p/60p/…). Diakses. Diakses 18 Juli 2023 https://rumaheditor.com/apa-itu-frame-rate/

Annur, Cindy Mutia. (2022). Kebocoran Data Sering Terjadi di 10 Sektor Industri Ini. Diakses 15 November 2023 dari https://databoks.katadata.co.id/datapublish/2022/09/06/kebocoran-data-sering-terjadi-di-10-sektor-industri-ini

Mustajab, Ridhwan.(2023). BSSN: Ada 311 Kasus Kebocoran Data di Indonesia pada 2022. Diakses 15 November 2023 dari https://dataindonesia.id/internet/detail/bssn-ada-311-kasus-kebocoran-data-di-indonesia-pada-2022