

# Penerapan Metode *Dynamic Cell Spreading* (Dcs) Untuk Menyembunyikan Teks Pada Video

*Application of the Dynamic Cell Spreading (DCS) Method to Hide Text on Video*

Muhammad Iqbal Pratama Batubara<sup>\*1</sup>, Rismayanti<sup>2</sup>, Yessi Fitri Annisah<sup>3</sup>

<sup>1,2,3</sup>Teknik Informatika, Universitas Harapan Medan

E-mail: <sup>1</sup>mipb2198@gmail.com, <sup>2</sup>risma.stth@gmail.com, <sup>3</sup>yessy.annisa@gmail.com

## Abstrak

Kemudahan berkomunikasi menimbulkan kebutuhan baru yaitu melakukan pengamanan informasi yang ditransmisikan pada jaringan komunikasi dari pengirim ke penerima. Salah satu bentuk informasi yang dikirimkan adalah gambar. Dengan mudahnya mengirimkan sebuah informasi ke berbagai media sering terjadi penyalagunaan data sehingga Pada penelitian ini penulis akan menggunakan Teknik Steganografi yang merupakan teknik dan seni untuk menyembunyikan pesan atau informasi dalam suatu media, seperti teks, gambar, audio ataupun video yang bertujuan untuk menghindari kecurigaan dari orang yang tidak berhak. Penelitian ini memanfaatkan algoritma dynamic cell spreading (DCS). Cara kerja dari algoritma dcs ialah Penyembunyian pesan dilakukan dengan cara menyisipkannya pada bit rendah LSB (Least Significant Bit) dari data pixel yang menyusun file tersebut menggunakan buffer memori sebagai media penyimpan sementara. Tujuan dari penelitian ini berupa Mengetahui cara merancang dan menganalisa sistem aplikasi keamanan data dengan Teknik steganografi menyembunyikan data pada file video dengan format MP4 dengan menggunakan metode-metode dynamic cell spreading (dcs) dan Mengetahui proses penyisipan data dan pengekstrakan data pada suatu *file* video dengan format mp4. Hasil yang diperoleh berupa sebuah aplikasi yang dapat melakukan pengamanan terhadap file video dengan format Mp4 yang dapat menghindari dari pencurian data

Kata kunci: Data, media, steganografi, algoritma

## Abstract

*Ease of communication creates a new need, namely securing information transmitted on the communication network from sender to receiver. One form of information sent is a picture. Easily sending information to various media often misuses data so that in this study the author will use the Steganography Technique, which is a technique and art to hide messages or information in a medium, such as text, images, audio or video which aims to avoid suspicion from people who not entitled to. This study utilizes a dynamic cell spreading (DCS) algorithm. The way the dcs algorithm works is that the message hiding is done by inserting it in the low LSB (Least Significant Bit) bit of the pixel data that makes up the file using a memory buffer as a temporary storage medium. The purpose of this research is to know how to design and analyze a data security application system with the steganography technique to hide data in video files with MP4 format using dynamic cell spreading (dcs) methods and to know the process of inserting data and extracting data in a video file with the format mp4. The results obtained are in the form of an application that can secure video files with the Mp4 format that can avoid data theft.*

Keywords: Data, media, steganography, algorithm



## 1. PENDAHULUAN

Kemudahan berkomunikasi menimbulkan kebutuhan baru yaitu melakukan pengamanan informasi yang ditransmisikan pada jaringan komunikasi dari pengirim ke penerima. Salah satu bentuk informasi yang dikirimkan adalah gambar [1][2]. Keamanan adalah sebuah keadaan yang ingin bebas dari segala bentuk serangan apapun dan bertujuan untuk melindungi data maupun informasi dari berbagai tindakan kejahatan *cyber* seperti yang dilakukan oleh para *hacker* dan *cracker*[3][4], keamanan memiliki dua Teknik yaitu *kriptography* dan *steganography*[5]. Berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak, salah satunya adalah Teknik *steganography*. *Steganography* sebagai suatu seni penyembunyian pesan ke dalam pesan lainnya yang telah ada sejak sebelum masehi dan kini seiring dengan kemajuan teknologi jaringan serta perkembangan dari teknologi digital, *steganography* banyak dimanfaatkan untuk mengirim pesan melalui jaringan Internet tanpa diketahui orang lain dengan menggunakan media digital berupa *file image* (Heryani, 2011). Enkripsi citra merupakan Teknik untuk melindungi citra dengan cara menyandikan citra (*plain-image*) sehingga tidak dapat dikenali lagi (*chiper-image*)[6][7]. *Chaos* dipilih karena karakteristik yaitu sensitivitas terhadap kondisi awal, berkelakuan acak, dan tidak memiliki periode berulang. *arnold catmap* digunakan untuk mengacak susunan *pixel-pixel*, sedangkan *logistic map* digunakan sebagai pembangkit *keystream*[8].

Adapun pendekatan Teknik selektif yaitu hanya mengenkripsi sebagian elemen di dalam citra namun efeknya keseluruhan citra terenkripsi. Pada penelitian ini penulis akan menggunakan Teknik *Steganography* yang merupakan teknik dan seni untuk menyembunyikan pesan atau informasi dalam suatu media, seperti teks, gambar, audio ataupun video yang bertujuan untuk menghindari kecurigaan dari orang yang tidak berhak[9] penelitian ini akan melakukan pengamanan data teks pada video menggunakan metode *dynamic cell spreading*. Pada penelitian ini akan menggunakan file berformat mp4 dikarenakan dalam menyembunyikan pesan format mp4 akan dibaca oleh program yang akan dibangun, metode tersebut memiliki konsep yang hampersama dengan metode *Least Significant Bit (LSB)* sehingga relatif mudah diaplikasikan. Peneliti sebelumnya [10] menjelaskan bahwa Keamanan dokumen merupakan salah satu hal yang sangat penting dalam penukaran data, khususnya pertukaran data di dunia maya yang didalamnya terdapat banyak ancaman pada saat proses itu Aplikasi yang dibangun dapat menerapkan metode pertukaran kunci Diffie Hellman dan menghasilkan kunci baru dan Aplikasi ini dapat melakukan enkripsi dan deskripsi Elgamal dengan menggunakan kunci yang telah dibangkitkan dengan metode Diffie Hellman

## 2. METODE PENELITIAN

Tujuan dari tahapan penelitian adalah memberikan panduan dan kerangka kerja yang terstruktur untuk melaksanakan penelitian dengan jelas. Tahapan penelitian ini memiliki peran penting dalam membantu peneliti merumuskan pertanyaan penelitian, memilih metode penelitian yang tepat, mengumpulkan data, menganalisis data, serta menyusun kesimpulan. Dalam penelitian ini, terdapat beberapa tahapan yang akan dijalani, yaitu: selanjutnya disebutkan tahapan-tahapan tersebut, sesuai dengan penelitian yang dimaksud seperti berikut:





Gambar 1. Tahapan Penelitian

**2.1 Analisis sistem**

Pembuatan sistem ini adalah bertujuan membuat aplikasi *steganography* dengan menggunakan metode *dynamic cell spreading* (DCS) pada data teks dan video. Sistem yang dapat mengamankan data *file* teks dan video dengan maksimal sesuai dengan proses metode yang digunakan. Metode yang digunakan pada sistem ini adalah dengan *dynamic cell spreading* (DCS). Desain dan implementasi sistem mengamankan *file* teks dan video ini meliputi desain data, deskripsi sistem, desain proses dan implementasi dan semua yang diperlukan dalam aplikasi *steganography* yang dirancang penulis.

**2.2 Analisa Metode DCS**

Penyisipan data teks kedalam data citra bisa dilakukan dengan cara merubah nilai bit pada citra kedalam bentuk biner. Sebagai contoh diambil citra dengan ukuran 3x3, dengan data teks yang akan disisipkan yaitu UNHAR

**Tabel 1** Nilai Bilangan Decimal Pada Video

Data Video					
20	32	21	19	20	21
10	15	20	21	18	17
25	21	20	19	17	18



23 16 3121 25 15  
16 17 21

**Tabel 2** Data Teks Yang Akan Disisipkan

Data Teks	Bilangan Desimal
U	85
N	78
H	72
A	65
R	82

Berdasarkan tabel 3.1 dan tabel 3.2 maka dalam melakukan penyisipan pesan teks akan dijelaskan penyelesaian Langkah Langkah metode *dynamic cell spreading* (DCS) sebagai berikut:

1. Konversi Data Video Kedalam Biner Nilai bit video yang telah didapatkan sebelumnya di konversi kedalam bilangan biner, karena nilai nilai bit yang telah di konversi tersebut nantinya akan digunakan untuk poses penyisipan data teks

**Tabel 3** Hasil Konversi Data Video Kedalam Biner

Data Video	Hasil Konversi
20 32 21	00010100, 00100000, 00010101
19 20 21	00010011, 00010100, 00010101
10 15 20	00001010, 00001101, 00010100
21 18 17	00010101, 00010010, 00010001
25 21 20	00011001, 00010101, 00010100
19 17 18	00010011, 00010001, 00010010
21 25 15	00010101, 00011001, 00001101
16 17 21	00010000, 00010001, 00010101

2. Konversi Data Teks Kedalam Biner

Setelah bit citra dikonversi, maka data teks juga harus dikonversi kedalam bilangan biner

**Tabel 4** Hasil Konversi Data Teks Kedalam Biner

Data Teks	Bilangan Desimal	Hasil Konversi
U	85	01010101
N	78	01001110
H	72	01001000
A	65	01000001
R	82	01010010

3. Proses Penyisipan Data Teks Pada Video Langkah Selanjutnya dilakukan penyisipan pada bit video. Proses dapat dilihat sebagai berikut :

Data Teks:

U = 85 (01010101)

N = 78 (01001110)

H = 72 (01001000)

A = 65 (01000001)

R = 82 (01010010)



Data Video :

(00010100), (00100000), (00010101)  
 (00010011), (00010100), (00010101)  
 (00001010), (00001101), (00010100)  
 (00010101), (00010010), (00010001)  
 (00011001), (00010101), (00010100)  
 (00010011), (00010001), (00010010)  
 (00010111), (00010000), (00011111)  
 (00010101), (00011001), (00001101)  
 (00010000), (00010001), (00010101)

Hasil Penyisipan Data Teks Pada Data Video (UNHAR) :

(00010100) (10100000) (00010101)  
 (00010011) (10010100) (00010101)  
 (00001010) (10001101) (00010100)  
 (10010101) (00010010) (10010001)  
 (00011001) (10010101) (00010100)  
 (00010011) (00010001) (10010010)  
 (00010111) (00010000) (10011111)  
 (10010101) (00011001) (10001101)  
 (00010000) (00010001) (00010101)

Ini adalah hasil penyisipan data teks ke dalam video. Bisa dilihat perubahan nilai bit pada video setelah dilakukan penyisipan data teks.

### 3. HASIL DAN PEMBAHASAN

Pada bab ini akan dilakukan implementasi dan pengujian terhadap sistem. Tahapan ini dilakukan setelah perancangan selesai dilakukan dan selanjutnya akan diimplementasikan pada bahasa pemrograman. Setelah diimplementasikan maka dilakukan pengujian terhadap sistem dan dilihat kekurangan-kekurangan pada - aplikasi untuk pengembangan sistem selanjutnya. Pada penelitian ini dalam mengembangkan suatu sistem dalam melakukan penerapan metode *dynamic cell spreading* (DCS) untuk menyembunyikan teks pada video yang bertujuan untuk Mengetahui cara merancang dan menganalisa sistem aplikasi keamanan data dengan Teknik steganografi menyembunyikan data pada *file* video dengan format MP4 dengan menggunakan metode-metode *dynamic cell spreading* (DCS) dan Mengetahui proses penyisipan data dan mengekstrakan data pada suatu *file* video dengan format mp4. Maka pada bab ini penulis akan menampilkan (*screen capture*) setiap tampilan dari *software* yang sudah diimplementasikan. Setelah sistem dianalisis dan didesain secara rinci, maka akan menuju tahap implementasi. Implementasi merupakan tahap meletakkan sistem sehingga siap untuk dioperasikan. Implementasi bertujuan untuk melakukan mengkonfirmasi modul-modul perancangan, sehingga pengguna dapat memberikan masukan kepada pembangun sistem. Hasil penelitian yang dilakukan penulis berupa sebuah program atau aplikasi yang dapat melakukan pengamanan teks pada *file* video

#### 3.1 Tampilan Menu Login admin

Pada menu *login* diharuskan untuk menginputkan *username* dan *password* pada *form* yang sudah tersedia pada Gambar 2:



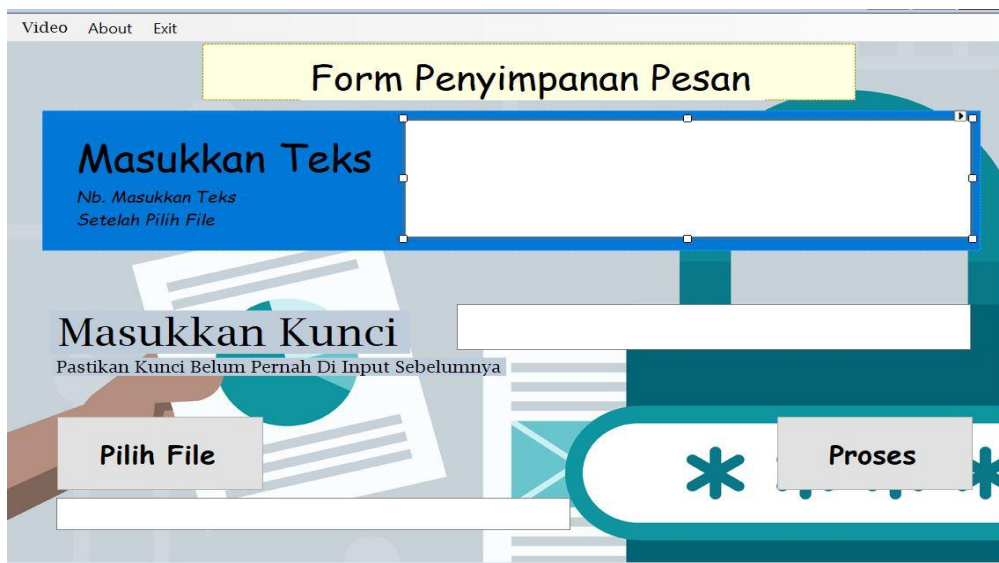


Gambar 2 Tampilan Menu Login Sistem

Gambar diatas menjelaskan proses login yang dilakukan oleh aktor *admin*. *Admin* melakukan login dengan memasukkan *username* dan *password* pada *form login*. Sistem akan melakukan verifikasi atau pengecekan data ke dalam *database* apakah *username* dan *password* sudah benar. Apabila verifikasi gagal, maka sistem akan menampilkan pesan gagal. Sebaliknya, apabila verifikasi berhasil, maka sistem akan menampilkan halaman menu utama *admin*.

### 3.2 Tampilan menu utama sistem

Pada sistem menu utama system steganografi menggunakan metode *spread spectrum* terdapat menu untuk mendukung sistem yang ada, semua menu itu dapat menampilkan informasi dan melakukan penyisipan pesan didalam media audio dan video. Lihat pada gambar 3:

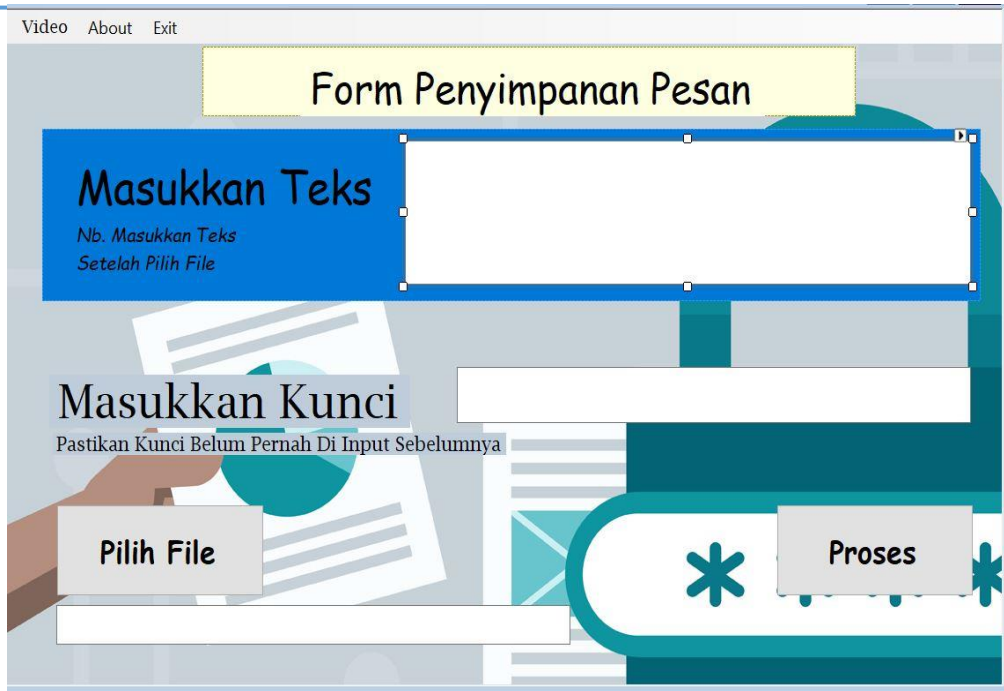


Gambar 3 Tampilan menu utama

### 3.3 Tampilan membuka menu video

Tampilan membuka video sebagai wadah dalam melakukan penyisipan pesan didalam media video, system akan menyediakan *button pilih file* kemudian user dapat memilih jenis video sesuai dengan keinginan atau kebutuhan sistem, seperti pada gambar 4 berikut ini:

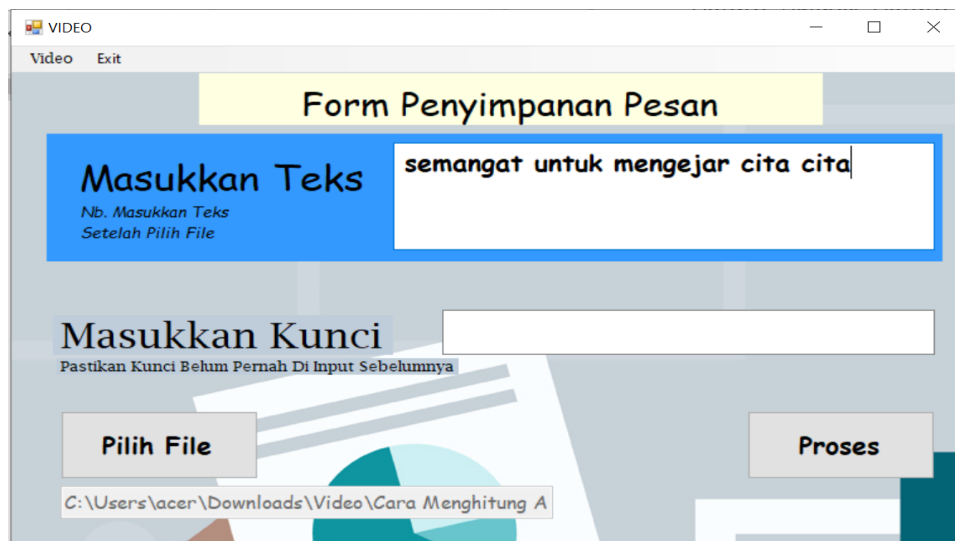




Gambar 4 Tampilan menu video

### 3.4 Tampilan penyisipan pesan

Tampilan menu penyisipan pesan merupakan menu yang digunakan untuk melakukan penyisipan pesan didalam media video, pengguna tinggal memasukan pesan apa yang ingin disisipkan didalam video, seperti pada gambar 5 berikut ini:

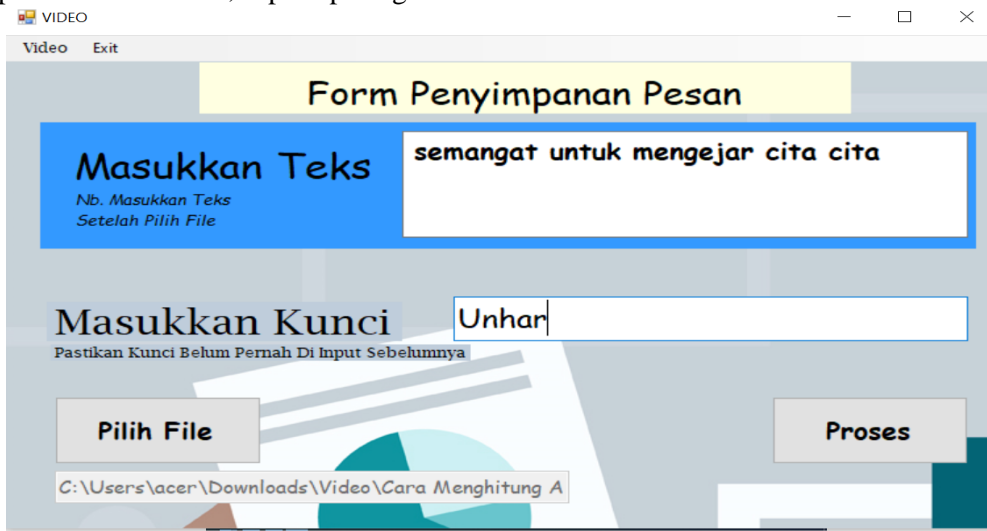


Gambar 5 Tampilan menu penyisipan pesan

### 4 Tampilan input kunci



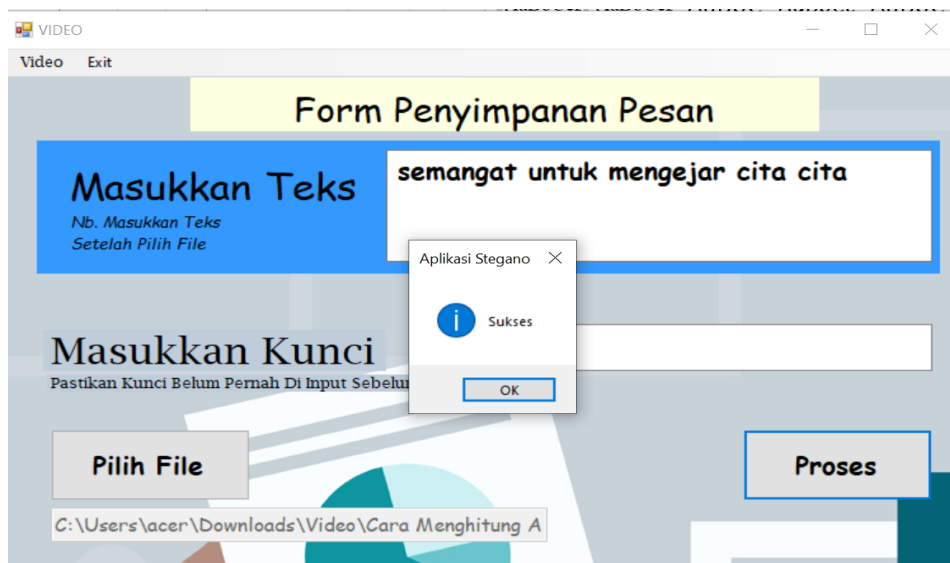
Tampilan menu input kunci merupakan menu yang digunakan untuk memasukan kunci ketikan melakukan penyisipan pesan didalam video, pengguna tinggal memasukan kunci apa yang ingin disisipkan didalam video, seperti pada gambar 6 berikut ini:



Gambar 6 Tampilan menu input kunci

5 Tampilan penyisipan pesan sukses

Tampilan menu penyisipan pesan sukses merupakan proses yang digunakan untuk memasukan pesan didalam video, , seperti pada gambar 7 berikut ini:



Gambar 7 Tampilan penyisipan sukses

4. KESIMPULAN DAN SARAN

Penelitian ini menghasilkan Sistem Steganografi untuk keamanan pesan menerapkan metode dynamic cell spreading yang mempunyai kelebihan pada tingkat keamanannya, Sistem dapat melakukan proses penyisipan data pada suatu *file* video dengan format mp4 dan Video yang





berhasil disisipkan sebuah pesan tidak akan merubah ukuran video dikarenakan pakan mengganti bilangan biner ke dalam RGB setiap pixel dengan bit pesan serta Perancangan aplikasi penyembunyian teks terenkripsi pada file video merupakan langkah yang memberikan dampak positif dalam mengamankan data, dimana dampak positif tersebut berupa kemudahan dan efektifitas waktu yang dipergunakan dalam melakukan proses penyandian dan penyembunyian data, kelemahannya adalah bila perubahan bit-bit pixel citra cover terlalu banyak, maka akan berdampak pada perubahan penurunan kualitas citra hasil, tetapi tidak berubah pada pada ukuran file.

#### DAFTAR PUSTAKA

- [1] A. R. Lubis, S. Prayudani, M. Lubis, and O. Nugroho, "Sentiment Analysis on Online Learning During the Covid-19 Pandemic Based on Opinions on Twitter using KNN Method," in *2022 1st International Conference on Information System & Information Technology (ICISIT)*, 2022, pp. 106–111.
- [2] O. Nugroho and G. A. Hutagalung, "Design and Implementation of Android-Based Public Transport Trayek using Cloud Computing Infrastructure," *Al'adzkiya Int. Comput. Sci. Inf. Technol. J.*, vol. 1, no. 1, 2020.
- [3] M. Azman and N. P. Sastra, "Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi," *Maj. Ilm. Teknol. Elektro*, vol. 17, no. 1, p. 59, 2018, doi: 10.24843/mite.2018.v17i01.p08.
- [4] A. P. N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia," *Jesik*, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com
- [5] Niti Ravika Nasution, "QUERY : Jurnal Sistem Informasi Volume : 01 , Nomor : 01 , April 2017 ISSN 2579-5341 ( online ) Kombinasi RSA-CRT dengan Random LSB untuk Keamanan Data QUERY : Jurnal Sistem Informasi Volume : 01 , Nomor : 01 , April 2017 ISSN 2579-5341 ( online )," vol. 5341, no. April, pp. 32–42, 2017.
- [6] R. Rahim, "Penyisipan Pesan Dengan Algoritma Pixel Value Differencing Dengan Algoritma Caesar Cipher Pada Proses Steganografi," *Times*, vol. 5, no. 1, pp. 6–11, 2016.
- [7] M. I. Zulfikar, G. Abdillah, A. Komarudin, J. Informatika, and F. Sains, "Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA)," *Semin. Nas. Apl. Teknol. Inf. 2019*, vol. 2, no. 1, pp. 19–26, 2019.
- [8] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.
- [9] E. Gunadhi and A. P. Nugraha, "Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection," *J. Algoritma.*, vol. 13, no. 2, pp. 391–398, 2016.
- [10] A. T. Susilo, H. Setiawan, R. A. Saputro, T. Purwadi, and A. Saifudin, "Penggunaan Metode Naïve Bayes untuk Memprediksi Tingkat Kemenangan pada Game Mobile Legends," *J. Teknol. Sist. Inf. dan Apl.*, vol. 4, no. 1, pp. 46–51, 2021.

