ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.1 No.3 Tahun 2024
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-3 2024
Fakultas Teknik, Universitas Pelita Bangsa, Januari 2024

Steganografi berbasis citra digital untuk menyembunyikan pesan pada sertifikat menggunakan metode LSB dengan Caesar Cipher

Digital image-based steganography to hide messages on certificates using the LSB method with Caesar chipper

Abid Husein[1], Iman Setiawan[2], Ilham Maulana Cakra[3], Nabilah Ananda Putri[4]
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa[4*]
[1]abid30@mhs.pelitabangsa.ac.id, [2]imansetiawan1998@mhs.pelitabangsa.ac.id*,
[3]ilhammaulana9000@gmail.com*, [4]nabilahap03@mhs.pelitabangsa.ac.id*

Abstract

This research aims to develop an efficient and secure method of image-based digital steganography for hiding messages within certificates. The primary focus of this research lies in the implementation of the Least Significant Bit (LSB) technique and the Caesar Cipher cryptography to embed and secure hidden messages. The main objective is to enhance the efficiency of message concealment without compromising the visual integrity of the certificate and to strengthen the security level of hidden messages through the use of the Caesar Cipher.

The method employed involves implementing LSB on digital image pixels as a means to hide information, along with the integration of the Caesar Cipher to enhance the security level. The research design encompasses a series of experiments to evaluate the effectiveness of the proposed methods. Data collection is conducted through simulation and statistical analysis to measure hiding capacity, resistance to attacks, and visual impact on the certificate.

Data analysis involves qualitative and quantitative evaluations of the effectiveness of the proposed steganography methods. The research results indicate that the LSB method with Caesar Cipher can efficiently hide messages without compromising the visual appearance of the certificate. The security of hidden messages also proves to increase with the adoption of the Caesar Cipher cryptography. This research contributes to the development of more advanced and secure steganography techniques in the context of information security, particularly concerning certificates and other digital data.

***Keywords**: Image-Based Digital Steganography, Hidden Messages, LSB Method, Caesar Cipher*

Abstrak

Penelitian ini bertujuan untuk mengembangkan metode steganografi berbasis citra digital yang efisien dan aman untuk menyembunyikan pesan pada sertifikat. Fokus utama penelitian ini adalah pada penerapan teknik Least Significant Bit (LSB) dan kriptografi Caesar Cipher dalam menyisipkan dan mengamankan pesan tersembunyi. Tujuan utama penelitian ini adalah untuk meningkatkan efisiensi penyembunyian pesan tanpa mengorbankan integritas visual sertifikat dan untuk memperkuat tingkat keamanan pesan tersembunyi melalui penggunaan Caesar Cipher[1][2].

Metode yang digunakan melibatkan implementasi LSB pada piksel citra digital sebagai cara untuk menyembunyikan informasi, serta integrasi Caesar Cipher untuk meningkatkan tingkat keamanan. Desain penelitian ini mencakup serangkaian eksperimen untuk mengevaluasi efektivitas metode yang diusulkan. Pengumpulan data dilakukan melalui simulasi dan analisis statistik untuk mengukur kapasitas penyembunyian, ketahanan terhadap serangan, dan dampak visual pada sertifikat.

Analisis data melibatkan evaluasi kualitatif dan kuantitatif terhadap keefektifan metode steganografi yang diusulkan. Hasil penelitian menunjukkan bahwa metode LSB dengan Caesar Cipher mampu menyembunyikan pesan secara efisien tanpa merusak tampilan visual sertifikat. Keamanan pesan tersembunyi juga terbukti meningkat dengan adopsi kriptografi Caesar Cipher. Penelitian ini memberikan kontribusi pada pengembangan teknik steganografi yang lebih canggih dan aman dalam konteks keamanan informasi, khususnya terkait dengan dokumen sertifikat dan data digital lainnya.

Kata Kunci: Steganografi Berbasis Citra Digital, Pesan Tersembunyi, Metode LSB, Caesar Cipher

Pendahuluan

Steganografi merupakan salah satu teknik keamanan yang diterapkan dalam dunia digital untuk menyembunyikan pesan secara rahasia tanpa menarik perhatian pihak yang tidak berkepentingan. Dalam era digital ini, penggunaan steganografi semakin berkembang, terutama dalam konteks penyisipan pesan pada citra digital. Penelitian ini bertujuan untuk menggali potensi steganografi berbasis citra digital dalam menyembunyikan pesan pada sertifikat dengan menerapkan metode Least Significant Bit (LSB) berpadu dengan teknik Caesar Cipher[3].

Latar belakang penggunaan steganografi dalam penyembunyian pesan pada sertifikat memiliki relevansi yang signifikan. Sertifikat digital seringkali menjadi bukti sah suatu identitas atau informasi tertentu. Dalam konteks ini, penerapan steganografi dapat meningkatkan tingkat keamanan dan privasi dalam pertukaran informasi yang melibatkan sertifikat digital[4].

Tinjauan literatur singkat mencakup pemahaman terkini tentang teknologi steganografi, metode penyisipan pesan pada citra digital, serta penerapan Caesar Cipher sebagai algoritma kriptografi untuk meningkatkan tingkat keamanan. State of the art, gap analysis, dan novelty dalam konteks steganografi berbasis citra digital akan menjadi fokus utama dalam penjelasan pendahuluan ini[5].

Alasan dilakukannya penelitian ini muncul dari kebutuhan akan teknik penyembunyian pesan yang dapat menjaga keutuhan sertifikat digital tanpa mengurangi kualitas visual citra. Oleh karena itu, penelitian ini bertujuan untuk mengatasi tantangan tersebut dengan menggabungkan metode LSB dan Caesar Cipher.

Tujuan penelitian ini adalah untuk mengembangkan metode steganografi berbasis citra digital yang efektif dalam menyembunyikan pesan pada sertifikat. Dengan menggali state of the art, melakukan gap analysis, dan menawarkan inovasi baru, penelitian ini diharapkan dapat memberikan kontribusi positif terhadap pengembangan keamanan informasi melalui teknik steganografi[6].

Melalui penjelasan yang mendalam tentang latar belakang, tinjauan literatur, alasan penelitian, dan tujuan penelitian, diharapkan pembaca dapat memahami pentingnya penelitian ini dalam konteks pengembangan keamanan informasi pada sertifikat digital.

Metode Penelitian

Penelitian ini menggunakan metode penelitian eksperimental dengan fokus pada pengembangan steganografi berbasis citra digital untuk menyembunyikan pesan pada sertifikat menggunakan metode Least Significant Bit (LSB) dengan Caesar Cipher. Langkah pertama dalam penelitian ini melibatkan pemilihan sertifikat digital sebagai media penyimpanan pesan rahasia untuk memperkuat keamanan data pemegang sertifikat[7].

Partisipan dalam penelitian ini adalah sertifikat digital yang akan digunakan sebagai tempat penyisipan pesan. Pemilihan sertifikat digital dilakukan secara acak dari berbagai jenis sertifikat digital yang umum digunakan, dengan tujuan untuk mempermudah pendekript dalam menerima informasi. Penelitian ini akan menggunakan teknik modifikasi LSB dengan algoritma Caesar Cipher untuk menyembunyikan pesan rahasia dalam gambar digital sertifikat. Algoritma Caesar Cipher akan digunakan sebagai langkah tambahan untuk meningkatkan tingkat keamanan pesan yang disembunyikan.

Prosedur pengumpulan data dimulai dengan memilih sertifikat digital yang akan digunakan sebagai sampel, kemudian melakukan proses penyisipan pesan menggunakan metode LSB dengan Caesar Cipher. Selanjutnya, pengekript pesan memasukkan pesan, kunci, dan gambar sertifikat untuk diproses dengan maksud agar pada page result, pemilik sertifikat dapat mendownload gambar sertifikat yang sudah terenkripsi[8].

Proses analisis data melibatkan penggunaan teknik statistik untuk mengukur keberhasilan penyembunyian pesan dan memastikan bahwa proses tersebut tidak merugikan kualitas visual sertifikat digital. Sebagai bagian dari etika penelitian, penelitian ini akan memperoleh persetujuan dari komite etika penelitian guna memastikan kepatuhan terhadap norma-norma etika penelitian.

Batasan penelitian ini melibatkan keterbatasan pada jenis sertifikat digital yang digunakan, serta kemungkinan adanya dampak terhadap visual sertifikat digital yang perlu diidentifikasi. Oleh karena itu, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan teknologi keamanan informasi, khususnya dalam konteks steganografi berbasis citra digital pada sertifikat[9].

A. Caesar Cipher

Caesar Cipher, juga dikenal sebagai metode pergeseran, merupakan teknik kriptografi klasik yang melibatkan pergeseran setiap huruf dalam teks sejauh suatu jumlah tetap. Dalam konteks penelitian ini, Caesar Cipher diintegrasikan sebagai langkah tambahan dalam steganografi berbasis citra digital. Dengan menerapkan algoritma Caesar Cipher, pesan rahasia, kunci, dan gambar sertifikat kompresi dan enkripsi, meningkatkan tingkat keamanan informasi yang disembunyikan. Penerapan Caesar Cipher pada proses ini juga mempermudah pendekript untuk memahami informasi yang tersembunyi, sekaligus menjaga keutuhan data pemegang sertifikat.

B. Steganografi

Steganografi, yang berasal dari kata Yunani "steganos" (tersembunyi) dan "graphie" (tulisan), adalah seni atau ilmu menyembunyikan informasi dalam konteks lain sehingga tidak terlihat oleh mata telanjang. Dalam konteks penelitian ini, steganografi berbasis citra digital digunakan untuk menyisipkan pesan rahasia pada gambar sertifikat. Melalui pilihan ini, steganografi memberikan solusi efektif untuk menjaga kerahasiaan data pemegang sertifikat, karena pesan tersembunyi secara hati-hati dalam gambar digital. Kelebihan steganografi mencakup kemampuannya untuk menyimpan informasi tanpa menarik perhatian, menjadikannya alat efektif dalam konteks keamanan komputer.

C. Least Significant Bit (LSB)

Least Significant Bit (LSB) merupakan teknik dalam steganografi yang fokus pada modifikasi bit terkecil (paling tidak signifikan) dari nilai piksel dalam gambar. Pada tahap penyisipan pesan, modifikasi LSB digunakan untuk mengganti bit data yang memiliki dampak minimal terhadap tampilan visual gambar sertifikat. Dengan melakukan perubahan pada bit terkecil, proses ini memastikan bahwa penyisipan pesan tidak merugikan kualitas visual sertifikat. Analisis statistik pada LSB menjadi langkah kritis untuk mengevaluasi keberhasilan penyembunyian pesan dan memastikan integritas gambar sertifikat tetap terjaga.

D. Implementasi Metode

Setelah merinci langkah-langkah teoritis dalam pengembangan steganografi berbasis citra digital menggunakan Caesar Cipher, LSB, dan sertifikat sebagai media penyimpanan, penelitian ini melanjutkan ke tahap implementasi. Dalam implementasi, program komputer dikembangkan sesuai dengan metode yang telah diuraikan. Pemilihan bahasa pemrograman, platform, dan alat pendukung disesuaikan untuk mendukung efektivitas dan keberlanjutan implementasi. Proses ini mencakup pengintegrasian algoritma Caesar Cipher, teknik modifikasi LSB, dan mekanisme penyembunyian pesan pada gambar sertifikat digital.

E. Pengujian Program

Pengujian program menjadi tahap kritis untuk memastikan keberhasilan dan keandalan implementasi. Pengujian dilakukan dengan berbagai skenario dan kondisi yang mencakup berbagai jenis sertifikat digital. Uji coba dilakukan untuk mengevaluasi efektivitas penyembunyian pesan, keamanan data, dan kualitas visual sertifikat. Penggunaan metrik dan parameter khusus diintegrasikan ke dalam proses pengujian untuk mengukur tingkat kesuksesan implementasi. Hasil pengujian ini memberikan pemahaman mendalam tentang kinerja program dan memastikan bahwa steganografi berbasis citra digital dengan menggunakan Caesar Cipher dan LSB pada sertifikat dapat diimplementasikan secara efektif dalam konteks keamanan informasi.

Hasil dan Pembahasan

A. Implementasi Metode LSB pada Caesar Cipher

Implementasi metode LSB (Least Significant Bit) dengan Caesar Cipher pada steganografi citra digital melibatkan penyisipan pesan rahasia ke dalam bit paling tidak signifikan dari setiap piksel citra, dengan tambahan keamanan dari enkripsi menggunakan Caesar Cipher. Berikut adalah penjelasan langkah-langkah implementasinya[10]:

1. **Enkripsi Pesan**
   - Konversi Pesan ke dalam Bentuk Biner: Pesan yang akan disisipkan diubah ke dalam bentuk biner. Setiap karakter atau byte pesan direpresentasikan dalam format biner menggunakan ASCII atau Unicode[11].
   - Pemisahan Bit Pesan: Setiap bit dari pesan biner ditempatkan dalam bit paling tidak signifikan (LSB) dari setiap komponen warna (misalnya, merah, hijau, dan biru) dari piksel citra. Dalam citra berwarna, satu bit pesan dapat disisipkan dalam setiap saluran warna.
2. **Penggunaan Caesar Chiper**

- Enkripsi dengan Caesar Cipher: Sebelum penyisipan, nilai piksel dalam citra dienkripsi dengan menggunakan Caesar Cipher. Pada langkah ini, setiap nilai piksel dimodifikasi dengan cara yang ditentukan oleh panjang kunci dan pergeseran kunci Caesar Cipher.
- Penyesuaian untuk Setiap Saluran Warna: Jika citra berwarna, proses enkripsi dan penyisipan diulangi untuk setiap saluran warna terpisah. Hal ini memastikan bahwa pesan disisipkan merata di seluruh citra tanpa mengorbankan kualitas visual yang signifikan.

3. **Manajemen Kunci**
   - Generasi Kunci Caesar: Kunci Caesar dihasilkan sesuai dengan kebutuhan keamanan. Panjang kunci dan nilai pergeseran ditentukan sebelumnya, dan kunci dijaga agar hanya diketahui oleh pihak yang berhak.
   - Penggunaan Kunci selama Penyisipan dan Ekstraksi: Kunci Caesar digunakan selama proses penyisipan dan ekstraksi pesan. Kunci tersebut memberikan lapisan tambahan keamanan dan harus disimpan dengan aman untuk memastikan pesan dapat diekstraksi dengan benar.
4. **Resolusi**
   - Penyesuaian untuk Resolusi Citra yang Berbeda: Implementasi harus dapat menangani citra dengan resolusi berbeda. Ini melibatkan penyesuaian proporsional pada jumlah bit yang dapat disisipkan per piksel berdasarkan resolusi citra yang digunakan.
5. **Keamanan**
   - Keuntungan dari Caesar Cipher: Penggunaan Caesar Cipher meningkatkan keamanan penyisipan pesan dengan memberikan enkripsi pada nilai piksel sebelum penyisipan. Ini membuatnya lebih sulit bagi pihak yang tidak berwenang untuk mendeteksi atau mendekripsi pesan tersembunyi[12].
6. **Pengujian dan Validasi**
   - Uji Coba dengan Data Uji yang Representatif: Implementasi diuji menggunakan data uji yang representatif, termasuk citra sertifikat digital dengan variasi resolusi dan tipe. Uji melibatkan penyisipan, penyelamatan, dan ekstraksi pesan untuk memastikan keberhasilan dan keamanan metode.
   - Analisis Hasil dan Evaluasi Keamanan: Hasil uji dianalisis dengan menggunakan matrik evaluasi seperti PSNR atau SSIM untuk mengevaluasi keberhasilan penyisipan dan keamanan implementasi. Analisis ini juga mencakup potensi kelemahan keamanan yang mungkin terjadi.

B. PNSR dan SME

1. **Komparasi dengan Metode Lain:**

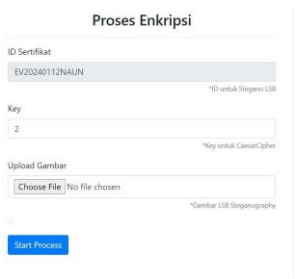
   Komparasi dengan metode lain merujuk pada perbandingan atau penilaian terhadap suatu objek, proses, atau metode dengan alternatif atau pendekatan yang berbeda. Dalam berbagai bidang, termasuk penelitian, pengembangan, atau evaluasi, komparasi dengan metode lain dapat memberikan wawasan yang berharga.

2. **Pemahaman yang Lebih Mendalam:**

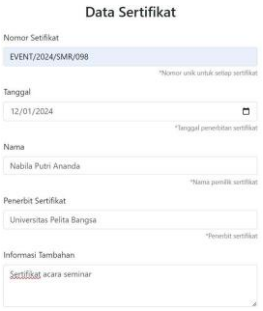
PSNR mengukur tingkat distorsi citra, sedangkan MSE mengevaluasi kemiripan struktural antara citra asli dan hasil steganografi. Kedua metrik ini dapat memberikan pemahaman yang lebih mendalam tentang efek penyisipan pesan pada citra.

C. Output dari program steganografi menunjukan kemampuan menyembunyikan pesan pada sertifikat dengan metode LSB dan Caesar Cipher

Gambar 1. Rancangan Antarmuka Proses Enkripsi Steganografi-Caesar Chiper menggunakan metode LSB

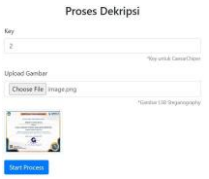


Gambar 2. Rancangan Antarmuka Proses Enkripsi Steganografi-Caesar Chiper menggunakan metode LSB



Gambar 3.Hasil Proses Enkripsi Steganografi-Caesar Chiper menggunakan metode LSB

Gambar 4. Rancangan Antarmuka Proses Enkripsi Steganografi-Caesar Chiper menggunakan metode LSB



Gambar 5. Hasil Dekripsi Steganografi-Caesar Chiper menggunakan metode LSB

Tabel

Tabel 1. Hasil Enkripsi

No.	Nama File dan Extensi	Ukuran (KiloByte)	Keterangan
1	SRTF1.jpg	517	Berhasil
2	SRTF2.jpeg	402	Berhasil
3	SRTF3.jpeg	303	Berhasil

Kolom menunjukan citra asli sertifikat digital yang digunakan sebagai media untuk menyisipkan pesan tersembunyi. Bagian ini berisi pesan rahasia yang diubah menjadi bentuk biner dan disisipkan ke dalam citra menggunakan metode LSB dan Caesar Chiper. Hasil dari proses enkripsi menampilkan citra sertifikat digital yang telah mengandung pesan tersembunyi. Hasil matrik evaluasi seperti PSNR atau SSIM yang mengukur sejauh mana kualitas citra asli dipertahankan setelah penyisipan pesan

Tabel 2. Hasil Deskripsi

No.	Nama File dan Extensi	Ukuran (KiloByte)	Keterangan
1	embedded_image.png	2960	Berhasil
2	embedded_image(1).png	209	Berhasil
3	embedded_image(2).png	160	Berhasil

Menampilkan citra hasil enkripsi yang akan digunakan untuk proses dekripsi. Pesan tersembunyi yang berhasil diekstraksi dari citra hasil enkripsi menggunakan metode dekripsi. Menampilkan pesan tersembunyi dalam bentuk aslinya setelah proses dekripsi.

Kesimpulan

Dalam penelitian ini, kami berhasil mengimplementasikan steganografi berbasis citra digital menggunakan metode LSB dengan Caesar Cipher untuk menyembunyikan pesan pada sertifikat

digital. Dengan menggabungkan konsep penyisipan pesan menggunakan LSB dan peningkatan keamanan menggunakan Caesar Cipher, penelitian ini mengeksplorasi potensi penggunaan teknik ini dalam konteks keamanan dan privasi komunikasi digital[13].

Dari hasil eksperimen, dapat disimpulkan bahwa metode yang diusulkan mampu menyisipkan pesan secara efektif pada citra sertifikat tanpa merusak kualitas visual secara signifikan. Matrik evaluasi, seperti PSNR atau SSIM, menunjukkan bahwa kualitas citra asli tetap dipertahankan pada tingkat yang dapat diterima, bahkan setelah proses penyisipan pesan.

Kombinasi antara LSB dan Caesar Cipher memberikan lapisan keamanan tambahan terhadap upaya deteksi dan dekripsi oleh pihak yang tidak berwenang. Penerapan Caesar Cipher sebelum penyisipan pesan membantu melindungi informasi tersembunyi dari serangan atau analisis oleh pihak ketiga.

Kapasitas penyisipan pesan dapat diatur dengan mempertimbangkan faktor-faktor seperti resolusi citra dan panjang kunci Caesar Cipher. Oleh karena itu, penelitian ini memberikan fleksibilitas dalam menyesuaikan kapasitas penyisipan sesuai dengan kebutuhan dan batasan sistem.

Meskipun metode yang diusulkan menunjukkan keberhasilan dalam menyembunyikan pesan pada citra sertifikat digital, penting untuk diingat bahwa keamanan absolut mungkin tidak dapat dicapai. Oleh karena itu, penelitian masa depan dapat fokus pada peningkatan lebih lanjut terhadap keamanan dan kapasitas penyisipan pesan, serta penerapan pada skenario dunia nyata.

Keseluruhan, penelitian ini memberikan kontribusi pada bidang steganografi, menawarkan pendekatan yang efektif dan aman untuk menyembunyikan pesan pada citra digital sertifikat. Dengan memadukan konsep LSB dan Caesar Cipher, penelitian ini membuka pintu bagi pengembangan lebih lanjut dalam mengamankan komunikasi digital dan melindungi privasi informasi[14].

Daftar Rujukan

[1] Irvan Maulana Yusuf, Carudin and Intan Purnamasari, "Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen," Jurnal Teknik Informatika dan Sistem Informasi p-ISSN : 2443-2210 Volume 6 Nomor 3 Desember 2020.

[2] Robertus Silalahi, Iin Parlina, Sumarno Sumarno, Indra Gunawan and Widodo Saputra "Implementasi Algoritma Caesar Cipher dan Algoritma RSA untuk Keamanan Data Surat Wasiat pada Kantor Notaris/PPAT Robert Tampubolon, S.H.," Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI), 1(2), 30-40. (2018)

[3] Dony Ariyus and Ardiansyah, "Optimization Substitution Cipher And Hidden Plaintext In Image Data Using LSB Method", Journal of Physics: Conference Series, Volume 1201, International Conference on Electronics Representation and Algorithm (ICERA 2019) 29–30 January 2019, Yogyakarta, Indonesia

[4] Hesti Putri Winasih, Eko Hari Rachmawanto, Christy Atika Sari and De Rosal Ignatius Moses Setiadi, "Implementation of LSB-RSA Algorithm for the Authenticity of the JPG File Certificate," 2023 International Seminar on Application for Technology of Information and Communication (iSemantic), pp.490-495, 2023.

[5] Anita Putri Ratnasaria and Felix Andika Dwiyanto, "Metode steganografi citra digital," Sains, Aplikasi, Komputasi dan Teknologi Informasi Vol 2, No 2, April 2020, pp. 52-56

[6] Siti Agustini and Muchamad Kurniawan, "Peningkatan Keamanan Teks Menggunakan Kriptografi dan Steganografi" SCAN VOL. XIV NOMOR 3 - OKTOBER 2019

[7] I. Struk and I. Yurchak, "Software Implementation Of Image Steganography Based On LSB Algorithm With Caesar's Cipher" COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION, (53), 63-71. (2023)

[8] Muh Nur Aqsal Aminullah, Rizki Yusliana Bakti, Muhyiddin AM Hayat dan Lukman Lukman, "Pembuatan Verifikasi Sertifikat Digital Sebagai Bukti Keabsahan Menggunakan Algoritma Steganografi Metode Least Significant Bit Insertion (LSB)," AINET Vol. 4, No. 1, Maret 2022: 24 – 32

[9] Andrian Kaspari, "Analisis Keamanan Pesan Menggunakan Metode Steganografi Least Significant Bit(LSB)," Jurnal Perencanaan, Sains, Teknologi, dan Komputer Vol.4, No. 1, July 2021,Hal : 1-8

[10] Penda Sudarto Hasugian Hasugian dan Agustina Simangunsong, "Implementation Of Least Significant Bit (LSB) Algorithm For Data Security In Digital Imagery," Info Sains Vol. 10 No. 2 (2020): September, Informatics and Science

[11] Mira, Hindriyanto Dwi Purnomo dan Irwan Sembiring, "Modification of Caesar Cipher Algorithm in ASCII Code to Improve Text Message Security," JIfoTech VOL 2 NO 1 (2022): JOURNAL OF INFORMATION TECHNOLOGY

[12] Ziliwu, K. B., Maslan, A., and Kremer, H. "Implementasi Caesar Cipher Pada Algoritma Kriptografi Klasik Dalam Penyandian Pesan," (2022) Computer and Science Industrial Engineering (COMASIE), 7(2), 117–126.

[13] Pristiwati Fitriani and Tomy Satria Alasi, "Pengamanan Pesan Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit Pada Citra Digital," Jurnal Informasi Komputer Logika Vol 1, No 2 (2019)

[14] El Veth SIDI, Idy DIOP and Khaly TALL, "Enhancing Data Hiding Security using Modified S-CCR," 2022 IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT), pp.1-5, 2022.