

KOMBINASI ALGORITMA ATBASH DAN ALGORITMA DYNAMIC CELL SPREADING (DCS) UNTUK KEAMANAN PESAN

Dito Aldyo Giawa^{1*}, Yusuf Ramadhan Nasution², Aidil Halim Lubis³

^{1,2,3}Universitas Islam Negri Sumatera Utara; Jl. Lapangan Golf, Durian Jangak, Tuntungan;
6285363706641

Keywords:

DCS
Atbash
Web

Correspondent Email:

rudidunham@gmail.com

Abstrak. Penelitian ini mengeksplorasi pemanfaatan teknologi informasi dalam memperkuat keamanan pesan pada platform web dengan mengintegrasikan algoritma Atbash dan Dynamic Cell Spreading (DCS). Di tengah meningkatnya ancaman digital seperti peretasan, pencurian data, dan serangan siber, perlindungan informasi selama proses transmisi menjadi sangat krusial. Algoritma Atbash merupakan metode enkripsi substitusi klasik yang bekerja dengan membalik susunan huruf dalam alfabet, sedangkan DCS berfungsi untuk menyisipkan informasi secara dinamis ke dalam citra digital, sehingga menyulitkan proses deteksi dan ekstraksi oleh pihak yang tidak berwenang. Mengacu pada efektivitas masing-masing teknik berdasarkan studi sebelumnya, penelitian ini bertujuan merancang sistem keamanan pesan yang memadukan keduanya. Sistem ini diwujudkan dalam bentuk aplikasi web yang dapat mengenkripsi teks pesan dan menyisipkannya ke dalam gambar digital, sehingga meningkatkan ketahanan pesan terhadap gangguan dan menjaga kerahasiaannya. Implementasi tersebut diharapkan dapat menambah lapisan perlindungan ekstra, menjaga kerahasiaan pesan dari akses ilegal, serta mendukung komunikasi yang aman di lingkungan web.



Copyright © [JITET](http://www.jitet.org) (Jurnal Informatika dan Teknik Elektro Terapan). This article is an open access article distributed under terms and conditions of the Creative Commons Attribution (CC BY NC)

Abstract. This study explores the use of information technology to enhance message security on web-based platforms by integrating the Atbash and Dynamic Cell Spreading (DCS) algorithms. Amid the rising threats of data breaches, information theft, and cyberattacks in the digital era, protecting data during transmission has become crucial. The Atbash algorithm is a classical substitution encryption method that works by reversing the order of the alphabet, while DCS enables dynamic embedding of information into digital images, making it harder to detect and extract by unauthorized parties. Referring to the proven effectiveness of each technique in previous studies, this research aims to design a message security system that combines both methods. The system is implemented as a web application capable of encrypting text messages and embedding them into digital images, thereby enhancing the message's resistance to interference and preserving confidentiality. This implementation is expected to provide an additional layer of security, safeguarding sensitive messages from unauthorized access and ensuring secure communication within web environments.

1. PENDAHULUAN

Pemanfaatan teknologi informasi dalam aktivitas komunikasi, transaksi, dan pertukaran data telah menjadi elemen yang melekat dalam kehidupan sehari-hari. Perkembangan teknologi digital memberikan berbagai kemudahan dalam penyampaian informasi dan pelaksanaan aktivitas bisnis secara cepat dan efisien. Namun, seiring dengan meningkatnya penggunaan teknologi tersebut, risiko terhadap keamanan informasi juga semakin besar, seperti peretasan sistem, pencurian data, kebocoran informasi pribadi, ransomware, serta berbagai bentuk serangan siber yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data [1][2]. Karena itu, diperlukan langkah-langkah untuk memperkuat perlindungan pesan yang dikirim melalui platform berbasis teknologi. Pesan yang dikirim secara digital rentan terhadap berbagai ancaman seperti peretasan, penyadapan ilegal, pencurian data, hingga berbagai bentuk serangan siber lainnya. Ancaman tersebut dapat mengakibatkan kebocoran informasi, penyalahgunaan data pribadi, kerugian finansial, serta terganggunya kerahasiaan dan integritas informasi yang dipertukarkan melalui media digital [3]. Informasi yang bersifat sensitif seperti data pribadi, rahasia perusahaan, dan informasi keuangan berpotensi menjadi sasaran pihak yang tidak bertanggung jawab. Kebocoran maupun penyalahgunaan informasi tersebut dapat menimbulkan kerugian bagi individu maupun organisasi, baik dari aspek finansial, operasional, maupun reputasi. Oleh karena itu, menjaga keamanan data selama proses penyimpanan dan pengiriman menjadi hal yang sangat penting untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi [4], [5].

Selain risiko teknis, serangan terhadap data digital juga menimbulkan konsekuensi sosial dan ekonomi yang serius. Kebocoran informasi pribadi dapat berdampak pada penyalahgunaan identitas, sedangkan pencurian data perusahaan berpotensi menimbulkan kerugian finansial yang besar, menurunkan reputasi, hingga mengganggu stabilitas operasional organisasi. Pada skala yang lebih luas, meningkatnya frekuensi serangan siber dapat memengaruhi tingkat kepercayaan masyarakat terhadap layanan digital, sehingga menghambat laju transformasi digital yang sedang digalakkan di berbagai sektor.

Untuk mengatasi tantangan tersebut, berbagai pendekatan keamanan telah dikembangkan, salah satunya melalui penerapan kriptografi dan steganografi. Kriptografi berfungsi untuk mengacak data sehingga tidak dapat dibaca tanpa kunci tertentu, sementara steganografi menyembunyikan pesan di dalam media digital seperti gambar atau audio sehingga tidak terlihat mencurigakan. Kombinasi keduanya mampu memberikan lapisan keamanan ganda yang lebih efektif dalam menjaga kerahasiaan serta integritas pesan digital, sekaligus mengurangi potensi ancaman dari pihak yang tidak berwenang.

Di Indonesia, urgensi keamanan data semakin mengemuka dengan disahkannya Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022, yang menegaskan pentingnya perlindungan informasi pribadi dalam setiap aktivitas digital. Regulasi ini menunjukkan bahwa aspek keamanan data tidak hanya menjadi isu teknis, tetapi juga hukum yang wajib dipatuhi oleh individu maupun organisasi. Dengan adanya peraturan ini, setiap bentuk pertukaran data elektronik yang tidak aman dapat menimbulkan risiko hukum dan kerugian finansial.

Selain itu, laporan dan penelitian di bidang keamanan siber menunjukkan bahwa serangan terhadap komunikasi digital terus mengalami peningkatan, termasuk serangan *phishing*, *man-in-the-middle attack*, *ransomware*, serta penyisipan *malware* yang dapat menyebabkan kebocoran maupun pencurian informasi. Kondisi tersebut menunjukkan bahwa perlindungan pesan digital perlu dikembangkan menggunakan pendekatan yang lebih komprehensif, salah satunya melalui penerapan kriptografi untuk mengenkripsi isi pesan dan steganografi untuk menyembunyikan keberadaan pesan sehingga tingkat keamanan komunikasi digital menjadi lebih tinggi [6], [7].

Berbagai penelitian telah membuktikan bahwa pengamanan pesan dapat dilakukan dengan kombinasi teknik enkripsi dan penyembunyian data. Misalnya, penggunaan kriptografi hibrida dengan algoritma substitusi yang dipadukan dengan steganografi citra terbukti mampu meningkatkan keamanan. Teknik steganografi berbasis LSB dengan tambahan enkripsi AES-256 juga efektif dalam menjaga kerahasiaan data, sedangkan

penggunaan metode wavelet diskrit dan Rijndael dapat memberikan perlindungan lebih baik.

Kombinasi antara algoritma Atbash dan Dynamic Cell Spreading (DCS) untuk keamanan pesan berbasis web memiliki beberapa keunggulan signifikan. Pertama, sistem ini menyediakan lapisan keamanan ganda dengan menggabungkan kriptografi dan steganografi. Pesan pertama-tama dienkripsi menggunakan algoritma Atbash, kemudian disisipkan ke dalam citra digital menggunakan DCS, sehingga pesan tersebut menjadi lebih sulit diakses oleh pihak yang tidak berwenang. Kedua, algoritma Atbash merupakan teknik substitusi yang sederhana, mudah diimplementasikan, dan efisien dalam proses enkripsi dan dekripsi tanpa memerlukan sumber daya komputasi yang besar. Ketiga, algoritma DCS memungkinkan penyebaran data yang lebih dinamis dan adaptif dalam citra digital, sehingga pesan yang disisipkan menjadi lebih tahan terhadap upaya deteksi dan ekstraksi.

Dengan menerapkan pendekatan kombinasi kriptografi dan steganografi, pesan digital menjadi lebih sulit dipahami atau diekstraksi oleh pihak yang tidak memiliki kunci dekripsi. Proses enkripsi mengubah pesan menjadi bentuk *ciphertext*, sedangkan steganografi menyembunyikan *ciphertext* tersebut ke dalam media digital sehingga keberadaan pesan tidak mudah diketahui. Penelitian terdahulu menunjukkan bahwa integrasi kedua metode tersebut mampu meningkatkan kerahasiaan komunikasi serta memberikan perlindungan yang lebih baik terhadap data pribadi maupun informasi strategis [8], [9]. Oleh karena itu, penelitian ini akan merancang sistem keamanan pesan berbasis web menggunakan kombinasi algoritma Atbash dan DCS.

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*) [10].

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 [11].

2.2 Algoritma Atbash

Algoritma Atbash merupakan salah satu algoritma kriptografi klasik yang termasuk ke dalam kategori monoalphabetic substitution cipher (substitusi monoalfabetik). Algoritma ini bekerja dengan cara mengganti setiap huruf pada plaintext dengan huruf yang posisinya berlawanan dalam alfabet. Sebagai contoh, huruf A diganti menjadi Z, B menjadi Y, C menjadi X, dan seterusnya hingga Z menjadi A. Metode ini tidak menggunakan kunci (keyless cipher), sehingga proses enkripsi dan dekripsi dilakukan menggunakan aturan substitusi yang sama [12].

Secara matematis, jika setiap huruf alfabet direpresentasikan dalam bentuk angka dengan $A = 0, B = 1, \dots, Z = 25$, maka transformasi Atbash dapat dituliskan sebagai :

$$C = 25 - P$$

dengan :

P = nilai huruf plaintext,

C = nilai huruf ciphertext.

Karena fungsi tersebut bersifat simetris, maka proses dekripsi menggunakan rumus yang sama:

$$P = 25 - C$$

Sebagai contoh :

Plaintext	Ciphertext
A	Z
B	Y
C	X
D	W
M	N
Z	A

Misalnya plaintext:

DATA

akan dienkripsi menjadi:

WZGZ

Kemudian ciphertext WZGZ jika diproses kembali menggunakan algoritma Atbash akan menghasilkan plaintext DATA.

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 [13].

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 [14].

2.4 Algoritma Dynamic Cell Spreading (DCS)

Dynamic Cell Spreading (DCS) merupakan metode steganografi yang digunakan untuk menyembunyikan informasi rahasia ke dalam media digital dengan cara menyebarkan data pada beberapa lokasi (*cell*) secara dinamis. Tujuan utama metode ini adalah meningkatkan keamanan penyisipan data dengan mengurangi pola penyisipan yang mudah dikenali serta mempertahankan kualitas media penampung (*cover media*). Dalam implementasinya, proses penyisipan pada DCS dilakukan pada bit-bit data media digital, sehingga prinsip kerjanya memiliki kemiripan dengan metode *Least Significant Bit* (LSB), yaitu memanfaatkan bit dengan bobot paling rendah sebagai lokasi

penyisipan pesan karena perubahan pada bit tersebut memberikan pengaruh yang sangat kecil terhadap kualitas visual media [15].

Pada penelitian yang mengimplementasikan DCS, mekanisme penyisipan bit mengikuti prinsip dasar LSB, sedangkan perbedaannya terletak pada strategi pemilihan lokasi penyisipan. LSB menyisipkan data secara berurutan pada piksel tertentu, sedangkan DCS menyebarkan data ke beberapa lokasi secara dinamis sehingga distribusi pesan menjadi lebih merata dan lebih sulit dideteksi melalui analisis steganografi. Oleh karena itu, teori mengenai LSB masih relevan digunakan sebagai dasar untuk menjelaskan proses penyisipan bit pada implementasi DCS [16].

2.5 Data Pesan

Data pesan merupakan sekumpulan informasi yang akan dikirimkan dari pengirim kepada penerima melalui suatu media komunikasi. Dalam sistem keamanan informasi, data pesan dapat berupa teks, angka, simbol, gambar, audio, maupun kombinasi dari berbagai jenis data yang memiliki makna tertentu. Seiring dengan perkembangan teknologi informasi, proses pengiriman data pesan menghadapi berbagai ancaman seperti penyadapan, pencurian, modifikasi, dan penyalahgunaan oleh pihak yang tidak berwenang. Oleh karena itu, diperlukan mekanisme pengamanan agar kerahasiaan, keaslian, dan integritas pesan tetap terjaga selama proses penyimpanan maupun transmisi data.

Berdasarkan karakteristiknya, data pesan yang digunakan dalam penelitian keamanan informasi umumnya berupa pesan teks (*plaintext*) yang terdiri atas karakter alfabet, angka, simbol, maupun karakter khusus lainnya. Pesan tersebut kemudian diproses menggunakan algoritma kriptografi sebelum disisipkan ke dalam media penampung menggunakan metode steganografi. Pendekatan ini bertujuan untuk menjaga kerahasiaan informasi sekaligus meminimalkan kemungkinan pesan diketahui oleh pihak yang tidak memiliki hak akses [17].

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. Penelitian 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

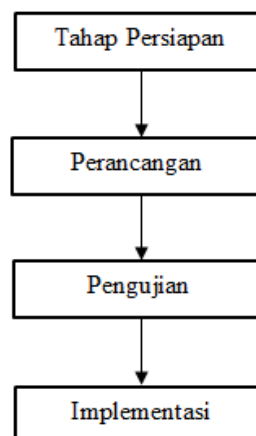
Studi Pustaka (Literatur) merupakan serangkaian yang berkenaan metode pengumpulan daftar pustaka, membaca dan mencatat, serta mengolah bahan penelitian atau menemukan referensi terkait kasus atau isu yang berkaitan dengan tugas akhir. Tujuannya untuk memberikan ide-ide untuk pengembangan kerangka konseptual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

Penelitian ini menggunakan data berupa pesan teks yang akan diamankan dengan algoritma Atbash dan citra sebagai media untuk menyisipkan pesan yang telah diamankan menggunakan algoritma DCS. Pesan yang akan diamankan adalah “UJI COBA

PENGAMANAN DENGAN ALGORITMA ATBASH”, yang akan dienkripsi menggunakan algoritma Atbash dan hasilnya akan disisipkan ke dalam sebuah citra dengan bantuan algoritma DCS. Sebagai contoh, proses pengamanan dan penyisipan pesan teks pada sistem yang akan dikembangkan dalam penelitian ini adalah sebagai berikut:

Algoritma Atbash berfungsi dengan membalikkan urutan huruf dalam alfabet. Misalnya, 'A' menjadi 'Z', 'B' menjadi 'Y', dan seterusnya. Berikut adalah tabel substitusi yang digunakan dalam algoritma Atbash :

Tabel 1. Tabel Substitusi Algoritma Atbash

Pesan	A	B	C	D	E	F	G	H	I	J	K	L	M
Substitusi	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
Pesan	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Substitusi	M	L	K	J	I	H	G	F	E	D	C	B	A

Berdasarkan tabel substitusi dari algoritma Atbash, hasil enkripsi dari pesan “UJI COBA PENGAMANAN DENGAN ALGORITMA ATBASH” menghasilkan ciphertext berupa “FQR XLYZ KVM TZNZM ZM WVMTZM ZOTLIRGNZ ZGYZHS”.

Tabel 2. Tabel Hasil Enkripsi Algoritma Atbash

Pesan	U	J	I	C	O	B	A	P	E	N	G	A	M	A	N	A
Ciphertext	F	Q	R	X	L	Y	Z	K	V	M	T	Z	N	Z	M	Z
Pesan	N	D	E	N	G	A	N	A	L	G	O	R	I	T	M	A
Ciphertext	M	W	V	M	T	Z	M	Z	O	T	L	I	R	G	N	Z
Pesan	A	T	B	A	S	H										
Ciphertext	Z	G	Y	Z	H	S										

Setelah memperoleh ciphertext tersebut, tahap selanjutnya adalah melakukan proses penyisipan ke dalam citra digital. Proses ini dimulai dengan mengubah ciphertext ke dalam bentuk biner, kemudian setiap bit dari biner tersebut disisipkan ke dalam representasi biner dari masing-masing piksel pada citra digital. Penyisipan dilakukan pada bit-bit rendah (Least Significant Bit) dari komponen warna dalam citra.

1. Pilih citra yang akan digunakan sebagai media penyisipan ciphertext



2. Ubah pixel dari citra ke dalam bentuk biner :

[(01111011, 11101010, 00101101), (01000011, 01011001, 11010010), (00100010, 00111000, 01001110), (01011010, 01111011, 10010001)], [(10010110, 11001000, 11111010), (01111011, 00111100, 01011010), (00101101, 01000011, 01011001), (01001110, 01011010, 01100100)], [(11010010, 10110100, 10010110), (01100100, 01111000, 10001100), (11001000, 11010010, 11011100), (00001010, 00010100, 00011110)], [(00011110, 00101000, 00110010), (00111100, 01000110, 01010000), (01011010, 01100100, 01101110), (01111000, 10000010, 10001100)]

3. Ubah ciphertext ke dalam bentuk biner
4. Ganti bit terakhir dari setiap bit pixel citra dengan bit ciphertext

Penyisipan Bit Ciphertext ke dalam DCS dari Setiap Komponen RGB. Misalkan kita menyisipkan bit biner dari ciphertext ke dalam DCS dari setiap komponen warna (R, G, B) secara berurutan.

1. Piksel pertama (123, 234, 45) = (01111011, 11101010, 00101101)
 - a. R : 01111011 = ganti DCS dengan bit pertama pesan (0) = 01111010 (122)
 - b. G : 11101010 = ganti DCS dengan bit kedua pesan (1) = 11101011 (235)
 - c. B : 00101101 = ganti DCS dengan bit ketiga pesan (0) = 00101100 (44)
 - d. Hasil piksel setelah penyisipan : (122, 235, 44)
2. Piksel kedua (67, 89, 210) = (01000011, 01011001, 11010010)
 - a. R : 01000011 = ganti LSB dengan bit keempat pesan (0) = 01000010 (66)
 - b. G : 01011001 = ganti LSB dengan bit kelima pesan (1) = 01011001 (tetap 89)
 - c. B : 11010010 = ganti LSB dengan bit keenam pesan (0) = 11010010 (tetap 210)
 - d. Hasil piksel setelah penyisipan : (66, 89, 210)
3. Piksel ketiga (34, 56, 78) = (00100010, 00111000, 01001110)
 - a. R : 00100010 = ganti LSB dengan bit ketujuh pesan (0) = 00100010 (tetap 34)

- b. G : 00111000 = ganti LSB dengan bit kedelapan pesan (1) = 00111001 (57)
- c. B : 01001110 = ganti LSB dengan bit kesembilan pesan (1) = 01001111 (79)
- d. Hasil piksel setelah penyisipan : (34, 57, 79)
4. Piksel keempat (90, 123, 145) = (01011010, 01111011, 10010001)
 - a. R : 01011010 = ganti LSB dengan bit kesepuluh pesan (0) = 01011010 (tetap 90)
 - b. G : 01111011 = ganti LSB dengan bit kesebelas pesan (1) = 01111011 (tetap 123)
 - c. B : 10010001 = ganti LSB dengan bit keduabelas pesan (0) = 10010000 (144)
 - d. Hasil piksel setelah penyisipan : (90, 123, 144)

Langkah-langkah penyisipan ini dilakukan secara berurutan hingga seluruh bit dari ciphertext berhasil disisipkan ke dalam citra yang berfungsi sebagai media penyimpanan pesan. Sebagai contoh, hasil citra berukuran 4x4 piksel setelah proses penyisipan 12 bit pertama dari ciphertext pada komponen warna RGB melalui metode Dynamic Cell Spreading (DCS) adalah sebagai berikut :

[(01111010, 11101011, 00101100), (01000010, 01011001, 11010010), (00100010, 00111001, 01001111), (01011010, 01111011, 10010000)], [(10010110, 11001000, 11111010), (01111011, 00111100, 01011010), (00101101, 01000011, 01011001), (01001110, 01011010, 01100100)], [(11010010, 10110100, 10010110), (01100100, 01111000, 10001100), (11001000, 11010010, 11011100), (00001010, 00010100, 00011110)], [(00011110, 00101000, 00110010), (00111100, 01000110, 01010000), (01011010, 01100100, 01101110), (01111000, 10000010, 10001100)]

Dari hasil citra tersebut, tidak ditemukan perbedaan visual yang signifikan secara kasat mata. Hal ini menunjukkan bahwa penyisipan pesan tidak menyebabkan perubahan warna yang mencolok, sehingga tidak menimbulkan kecurigaan terhadap keberadaan pesan yang tersembunyi, terutama bagi pihak yang tidak memiliki otoritas.

4.2 Pengujian Aplikasi

Pengujian aplikasi dilakukan dengan menjalankan sistem pada peramban (*web browser*) Firefox melalui perangkat laptop. Tujuan pengujian ini adalah untuk memastikan bahwa setiap halaman dan menu yang tersedia dalam aplikasi dapat berjalan sebagaimana mestinya. Berikut adalah uraian hasil pengujian dari masing-masing halaman pada aplikasi :

1. Tampilan Halaman Beranda

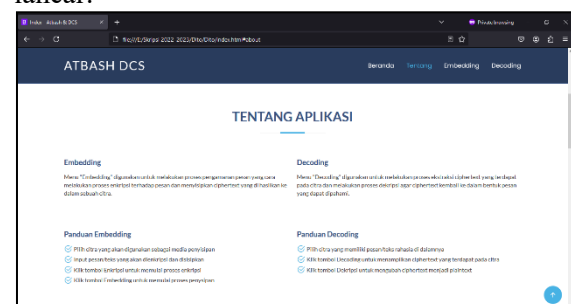
Halaman ini merupakan tampilan awal saat aplikasi pertama kali dijalankan melalui web browser. Fungsi utamanya adalah sebagai titik masuk bagi pengguna sebelum melanjutkan ke menu lainnya. Pengujian menunjukkan bahwa halaman ini tampil secara otomatis dan berjalan dengan baik tanpa kendala.



Gambar 3. Tampilan Halaman Beranda

2. Tampilan Halaman Tentang

Halaman ini memuat informasi penjelasan mengenai fungsi dari menu *Embedding* dan *Decoding* beserta langkah-langkah penggunaannya. Pengujian terhadap halaman ini menunjukkan bahwa informasi ditampilkan secara utuh dan navigasi antar elemen berjalan lancar.

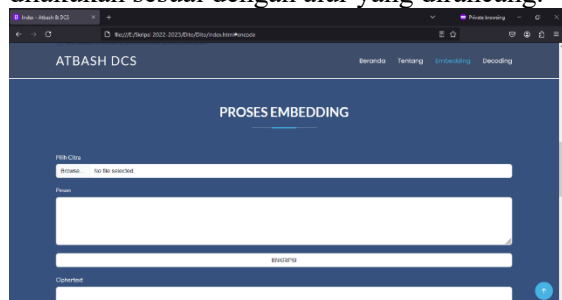


Gambar 4. Tampilan Halaman Tentang

3. Tampilan Halaman Embedding

Halaman ini digunakan untuk menjalankan proses pengamanan dan penyisipan pesan ke dalam citra digital. Pada saat pengujian, proses enkripsi pesan dengan algoritma Atbash dan penyisipannya menggunakan algoritma

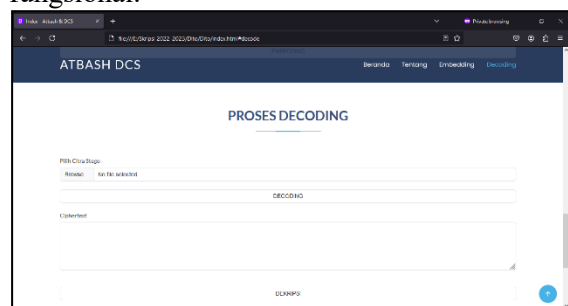
Dynamic Cell Spreading (DCS) dapat dilakukan sesuai dengan alur yang dirancang.



Gambar 5. Tampilan Halaman Embedding

4. Tampilan Halaman Decoding

Halaman decoding berfungsi untuk melakukan proses ekstraksi pesan dari citra digital serta dekripsi pesan yang sebelumnya telah disisipkan. Berdasarkan pengujian, halaman ini mampu mengekstrak informasi tersembunyi dan menampilkannya dalam bentuk teks asli tanpa mengalami gangguan fungsional.



Gambar 6. Tampilan Halaman Decoding

5. KESIMPULAN

5.1 Kesimpulan

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

1. Penelitian ini berhasil menghasilkan sebuah aplikasi berbasis web yang dapat dijalankan melalui web browser, di mana aplikasi tersebut berfungsi untuk mengamankan pesan teks dan menyisipkannya ke dalam citra digital.
2. Mekanisme pengamanan pesan dilakukan melalui proses enkripsi menggunakan algoritma Atbash, sedangkan proses penyisipan pesan ke dalam citra digital dilaksanakan dengan menerapkan algoritma *Dynamic Cell Spreading* (DCS).
3. Jenis pesan yang dapat diamankan dalam sistem ini terbatas pada karakter

huruf kapital dari 'A' hingga 'Z'. Karakter di luar rentang tersebut tidak akan diproses untuk enkripsi, melainkan dikembalikan dalam bentuk aslinya.

4. Media penyisipan yang digunakan dalam penelitian ini berupa citra digital berwarna, yang memungkinkan modifikasi bit tingkat rendah untuk penyisipan pesan tanpa mengubah tampilan citra secara signifikan.
5. Aplikasi yang dikembangkan dalam penelitian ini dibangun menggunakan perangkat lunak Visual Studio Code dengan memanfaatkan bahasa pemrograman HTML dan JavaScript, yang mendukung pengembangan antarmuka pengguna yang interaktif dan dinamis pada platform web.

5.2 Saran

Untuk menyempurnakan aplikasi ini maka diberikan saran :

1. Disarankan agar pada pengembangan selanjutnya ditambahkan teknik kriptografi yang memanfaatkan penggunaan kunci (*key-based cryptography*), seperti algoritma Vigenère, AES, atau RSA. Hal ini bertujuan untuk meningkatkan tingkat keamanan pesan yang dienkripsi dan mencegah kemungkinan pembacaan pesan oleh pihak yang tidak berwenang.
2. Disarankan agar aplikasi yang telah dibangun dilakukan proses *hosting* ke dalam *platform server* atau layanan penyedia *web hosting*. Dengan demikian, aplikasi dapat diakses secara daring (*online*) dan digunakan secara luas oleh masyarakat umum sebagai alat bantu dalam menjaga kerahasiaan informasi digital.

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] I. Dermawan, A. Baidawi, and S. M. Dewi, "Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia," *J. Inf. dan Teknol.*, vol. 5, no. 3, pp. 20–25, 2023, doi: 10.60083/jidt.v5i3.364.
- [2] C. S. S. Silalahi, A. M. V. Manullang, N. M. Nasution, L. O. Pandiangan, and G. N. Butar Butar, "Analisis Keamanan Siber Perbankan dan Peran OJK: Studi Kasus Serangan Ransomware pada Bank Syariah Indonesia Tahun 2023," *MANTAP J. Manag. Accounting, Tax Prod.*, vol. 4, no. 1, pp. 167–174, 2026.
- [3] G. W. Jonimandala, D. K. G. Sondakh, and J. Sondakh, "Peran Direktorat Tindak Pidana Siber (DITTIPIDSIBER) Bareskrim Polri Dalam Melakukan Penegakan Hukum Terhadap Kejahatan Pencurian dan Penyalahgunaan Data Pribadi," *Innov. J. Soc. Sci. Res.*, vol. 3, no. 4, pp. 680–692, 2023.
- [4] T. A. Kurniawan, W. Syahputra, and Safrizal, "IMPLEMENTASI ALGORITMA LEAST SIGNIFICANT BIT MACHING UNTUK MENGAMANKAN DATA RAHASIA PERUSAHAAN," *J. Ilm. Fak. Tek.*, vol. 18, no. 1, pp. 1–7, 2022.
- [5] R. A. Antoine, N. S. Farizqa, A. H. Hasna, and M. Pasaribu, "Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT . Bank Syariah Indonesia)," *J. Multidisiplin Ilmu Akad.*, vol. 2, no. 1, pp. 316–327, 2025.
- [6] D. Ramalinda, Jayadi, and A. R. Raharja, "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi," *J. Int. Multidiscip. Res.*, vol. 2, no. 6, pp. 665–671, 2024.
- [7] M. Manik, S. S. P. Pardosi, and I. M. Situmorang, "Pengujian dan Analisis Teknik Steganografi Menggunakan Metode Playfair , ElGamal , dan LSB untuk Penyembunyian Data pada Gambar Digital dalam Aplikasi Modern," *J. Quancam*, vol. 2, no. 2, pp. 17–22, 2024.
- [8] J. A. Harahap, M. Aulia, M. R. Alfarisi, and S. Sohaimi, "Implementasi Pengamanan Data Menggunakan Kombinasi Algoritma Kriptografi AES - 256 dan Teknik Steganografi End - of - File (EOF) Pada Media Citra Digital," *JIKUM J. Ilmu Komput.*, vol. 2, no. 1, pp. 97–101, 2026.
- [9] S. Hidayat and P. N. Andono, "Analisis Keamanan Steganografi Multi-Layer dengan Enkripsi Vigenère dan Caesar Cipher pada Citra Digital Security Analysis of Multi-Layer Steganography with Vigenère Encryption and Caesar Cipher on Digital Images," *J. Pendidik. dan Teknol. Indones.*, vol. 5, no. 3, pp. 869–880, 2025.
- [10] 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.
- [11] 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.
- [12] K. Wardini, R. Marwati, and D. Rachmatin, "PENGAMANAN PESAN MENGGUNAKAN KRIPTOGRAFI HYBRID ATBASH , AUTOKEY CIPHER , DAN ALGORITMA EL GAMAL," *Equator J. Math. Stat. Sci.*, vol. 3, no. 1, pp. 32–42, 2024.
- [13] 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.
- [14] 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.
- [15] O. M. Hammad, I. Smaoui, A. Fakhfakh, and M. M. Hashim, "An Overview of Image Steganography Techniques : Historical Development , Methodologies , and Evaluation Criteria," *Penins. Publ. LLC*, pp. 74–87, 2024.
- [16] A. E. Prayogo, A. Nugraha, F. Novanto, and J. C. Kurniawan, "Enhancing Least Significant Bit Steganography Image Fidelity Using Brotli Compression," *Sink. J. dan Penelit. Tek. Inform.*, vol. 8, no. 1, pp. 285–295, 2024.
- [17] R. A. Akmal, M. Furqan, and R. K. R, "Implementasi Metode Least Significant Bit Dalam Teknik Steganografi pada Berkas Audio Dengan Stego Citra Digital," *G-Tech J. Teknol. Terap.*, vol. 7, no. 2, pp. 543–553, 2023.