Krea-TIF: Jurnal Teknik Informatika
http://ejournal.uika-bogor.ac.id/index.php/krea-tif
p-ISSN: 2338-2910, e-ISSN: 2658-5836
Vol. 13, No. 2, 2025, pp. 59 – 72
DOI: 10.32832/krea-tif.v13i2.21272

Metode Steganografi Teks Berbasis Persamaan Linear dan Manipulasi Ukuran Font

Taufik Tirkaamiasa[1]*, Evin Sofianti[2]
[1]Teknik Komputer, Politeknik Prasetiya Mandiri, Indonesia
[2]Komputerisasi Akuntansi Politeknik Prasetiya Mandiri, Indonesia
*E-mail koresponden: taufiktirkaamiasa.dosen@prasetiyamandiri.ac.id

Diserahkan *17 Agustus 2025;* ***Direview*** *9 November 2025;* ***Dipublikasikan*** *30 Desember 2025*

Abstrak

Perkembangan komunikasi digital ikut meningkatkan risiko terjadinya penyadapan, pemalsuan, dan manipulasi pesan. Atas dasar itulah penelitian ini dilakukan dengan tujuan mengembangkan metode steganografi teks yang mengintegrasikan persamaan linear sebagai mekanisme enkripsi dan manipulasi ukuran font sebagai media penyisipan pesan dalam satu kerangka terpadu. Data uji berupa lima dokumen teks berita kurang lebih 200 kata dengan pesan rahasia sepanjang 10-50 karakter. Plaintext dienkripsi menggunakan persamaan linear (y=3x+1) untuk menghasilkan cipher alphabet, kemudian dikodekan ke variasi ukuran font pada teks penampung. Evaluasi kuantitatif dilakukan menggunakan tiga parameter utama yaitu fidelity, robustness, dan recovery rate. Hasil pengujian menunjukkan nilai fidelity rata-rata sebesar 98,7%, robustness sebesar 96,4% terhadap perubahan format dokumen, dan recovery rate mencapai 100% pada kondisi normal. Berbeda dari metode steganografi teks sebelumnya yang memisahkan proses enkripsi dan penyisipan, penelitian ini memperkenalkan integrasi persamaan linear langsung dengan manipulasi ukuran font sebagai satu mekanisme terpadu yang terbukti meningkatkan kapasitas penyisipan hingga 25% tanpa menurunkan keterbacaan teks. Metode ini berpotensi diterapkan pada sistem komunikasi digital di masa depan.

Kata kunci: *Alfabet Sandi, Algoritma, Persamaan Linier, Steganografi, Ukuran Font*

Abstract

The development of digital communication has also increased the risk of eavesdropping, forgery, and message manipulation. Based on this, this research was conducted with the aim of developing a text steganography method that integrates linear equations as an encryption mechanism and font size manipulation as a message embedding medium within a single, integrated framework. The test data consists of five news text documents, each approximately 200 words long, with a secret message ranging from 10 to 50 characters. Plaintext is encrypted using a linear equation (y=3x+1) to produce a cipher alphabet, which is then encoded into variations of font size on the cover text. Quantitative evaluation was conducted using three main parameters: fidelity, robustness, and recovery rate. The test results showed an average fidelity value of 98.7%, robustness of 96.4% against changes in document format, and a recovery rate of 100% under normal conditions. Unlike previous text steganography methods that separated the encryption and embedding processes, this research introduces the direct integration of linear equations with font size manipulation as a single, unified mechanism that has been proven to increase embedding capacity by up to 25% without reducing text readability. This method has the potential to be applied to digital communication systems in the future.

Keywords: *Code Alphabet, Algorithm, Linear Equations, Steganography, Font Size*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah meningkatkan kecepatan dan kemudahan pertukaran data digital, namun pada saat yang sama juga memperbesar risiko kebocoran informasi, pemalsuan pesan, dan penyadapan komunikasi karena kebutuhan akan keamanan data saat ini semakin kompleks, seiring perkembangan teknologi komunikasi digital modern [20, 25, 35]. Perlindungan informasi tidak lagi hanya menuntut kerahasiaan isi pesan, tetapi juga perlindungan terhadap keberadaan pesan itu sendiri agar tidak mudah terdeteksi oleh pihak yang tidak berwenang, karena teknik kriptografi konvensional saja tidak cukup untuk menyembunyikan fakta bahwa pesan sedang dikirim [6, 36, 39, 42]. Dalam konteks ini, steganografi berkembang sebagai teknik untuk menyembunyikan pesan rahasia di dalam media digital seperti citra, audio, video, dan teks sehingga media tersebut tetap tampak normal bagi pengamat, memungkinkan transmisi informasi *covert* yang tidak menarik perhatian pihak ketiga [30,47].

Steganografi berbasis teks memiliki keunggulan karena mudah didistribusikan dan tidak memerlukan media berukuran besar, sehingga sangat sesuai untuk komunikasi berbasis dokumen dan pesan tertulis [14, 53]. Namun, metode konvensional seperti penyisipan spasi ganda, perubahan tanda baca, atau pengaturan format sederhana memiliki kapasitas penyisipan yang rendah dan rentan terhadap perubahan format dokumen, misalnya akibat proses *copy–paste*, konversi ke PDF, atau pemformatan ulang oleh perangkat lunak pengolah kata. Untuk meningkatkan keamanan, beberapa penelitian mengombinasikan kriptografi dan steganografi, tetapi pada umumnya proses enkripsi dan proses penyisipan masih dilakukan sebagai dua tahap yang terpisah sehingga meningkatkan kompleksitas dan mengurangi efisiensi pengkodean, sebuah tantangan yang terus didiskusikan dalam literatur steganografi teks kontemporer [3, 9, 50].

Di sisi lain, transformasi matematis seperti persamaan linear telah lama digunakan dalam kriptografi klasik untuk membentuk *cipher alphabet* melalui teknik substitusi monoalfabetik yang sederhana dan efisien, yang dikenal mampu menghasilkan pemetaan deterministik antara *plaintext* dan *ciphertext* serta mudah diimplementasikan dalam berbagai algoritma enkripsi ringan [4]. Transformasi ini memiliki sifat pemetaan yang terkontrol dan mudah diimplementasikan, tetapi pemanfaatannya sebagai kunci enkripsi yang secara langsung diintegrasikan dengan mekanisme penyisipan steganografi teks berbasis format masih relatif terbatas dalam literatur steganografi teks kontemporer, terutama yang memanfaatkan struktur format untuk *embedding* pesan [33, 43, 44]. Dengan demikian, masih terdapat celah penelitian dalam mengembangkan metode steganografi teks yang menggabungkan transformasi matematis dan manipulasi format teks dalam satu mekanisme yang terpadu, efisien, dan *robust*, sebuah gap yang menjadi fokus banyak studi steganografi modern saat ini [11, 25, 36, 39].

Berdasarkan celah tersebut, penelitian ini bertujuan mengembangkan metode steganografi teks yang mengintegrasikan persamaan linear sebagai mekanisme enkripsi dan manipulasi ukuran *font* sebagai media penyisipan pesan rahasia dalam satu kerangka terpadu, sehingga meminimalkan pemisahan antara enkripsi dan *embedding* yang umum ditemukan pada pendekatan steganografi teks konvensional [10, 23, 29, 46, 47]. Pendekatan ini dirancang agar *ciphertext* yang dihasilkan dari transformasi matematis dapat langsung direpresentasikan melalui variasi ukuran *font* pada teks penampung, sehingga meningkatkan kapasitas penyisipan dan ketahanan pesan tanpa mengurangi keterbacaan dokumen dan sesuai dengan tren pengembangan teknik *embedding* adaptif yang memaksimalkan *imperceptibility* dan *robustness* pada media teks digital kontemporer [2, 21, 22, 37].

Kebaruan penelitian ini terletak pada integrasi langsung persamaan linear sebagai mekanisme

enkripsi *monoalphabetic* dengan pemetaan adaptif ukuran *font* sebagai media penyisipan pesan dalam ratu kerangka algoritmik tunggal [1, 15, 26], yang berbeda secara mendasar dari pendekatan steganografi teks konvensional yang memisahkan proses kriptografi dan *embedding* [16, 30, 45]. Metode ini memetakan hasil transformasi matematis langsung ke variasi tipografi yang bersifat tidak mencolok secara visual, sejalan dengan tren teknik *embedding* adaptif yang mempertahankan *imperceptibility* sambil memaksimalkan kapasitas pesan [24, 32, 40]. Integrasi ini menghasilkan peningkatan penyisipan hingga 25% dibandingkan metode berbasis spasi dan tetap mempertahankan PSNR di atas 40 dB serta tingkat ekstraksi di atas 98%, menunjukkan keseimbangan baru antara keamanan, kapasitas, dan keterbacaan teks. Suatu persoalan kunci dalam steganografi teks terus dikaji dalam literatur modern [9, 11, 41]. Selain itu, metode yang diusulkan menunjukkan tingkat *fidelity, robustness,* dan *recovery rate* yang tinggi, sehingga memiliki potensi aplikasi praktis dalam pengamanan dokumen digital dan pengiriman pesan rahasia pada sistem komunikasi berbasis teks [8, 17, 55].

METODE PENELITIAN

Penelitian ini dilakukan melalui enam tahapan utama, yaitu persiapan *cover text* dan *plaintext*, enkripsi *plaintext*, penyisipan *ciphertext*, ekstraksi *ciphertext*, dekripsi, serta evaluasi kinerja metode. Pada tahap awal, *cover text* disiapkan sebagai media penyisipan pesan, sementara *plaintext* digunakan sebagai pesan asli yang akan diamankan. Selanjutnya, *plaintext* dienkripsi menggunakan persamaan linear sehingga menghasilkan *ciphertext*. *Ciphertext* tersebut kemudian disisipkan ke dalam teks dengan memanfaatkan variasi ukuran *font* sebagai teknik steganografi. Setelah terbentuk *stego text*, proses ekstraksi dilakukan untuk memperoleh kembali *ciphertext* yang telah disisipkan. *Ciphertext* hasil ekstraksi kemudian didekripsi untuk memperoleh kembali *plaintext*. Pada tahap akhir, evaluasi dilakukan untuk mengukur kinerja metode berdasarkan keberhasilan proses enkripsi, penyisipan, ekstraksi, dan dekripsi pesan.

Desain Penelitian

Penelitian ini mengusulkan metode steganografi teks berbasis manipulasi ukuran *font* yang dikombinasikan dengan enkripsi *monoalphabetic* menggunakan persamaan linear dalam satu kerangka terintegrasi. Pendekatan ini dirancang untuk menggabungkan proses enkripsi dan penyisipan pesan sehingga meningkatkan efisiensi serta keamanan sistem.
Sistem terdiri dari tiga tahap utama:

1. Enkripsi pesan
2. Penyisipan (*embedding*) ke dalam *cover text*
3. Ekstraksi dan dekripsi pesan

Data dan Parameter Eksperimen

Eksperimen dilakukan menggunakan lima dokumen teks berita sebagai *cover text*, masing-masing ±200 kata. Pesan rahasia (*plaintext*) memiliki panjang 10–50 karakter.
Parameter utama yang digunakan adalah:

1. *Font*: Times New Roman
2. Ukuran *font* dasar: 22 pt
3. Panjang pesan: 10–50 karakter
4. Lingkungan implementasi: Microsoft Excel VBA

Pemilihan teks berita bertujuan untuk menjaga struktur linguistik yang alami sehingga perubahan tipografi tidak mudah terdeteksi secara visual.

Metode Enkripsi

Enkripsi dilakukan dengan *cipher monoalphabetic* berbasis persamaan linear yang ditunjukan pada Persamaan 1.

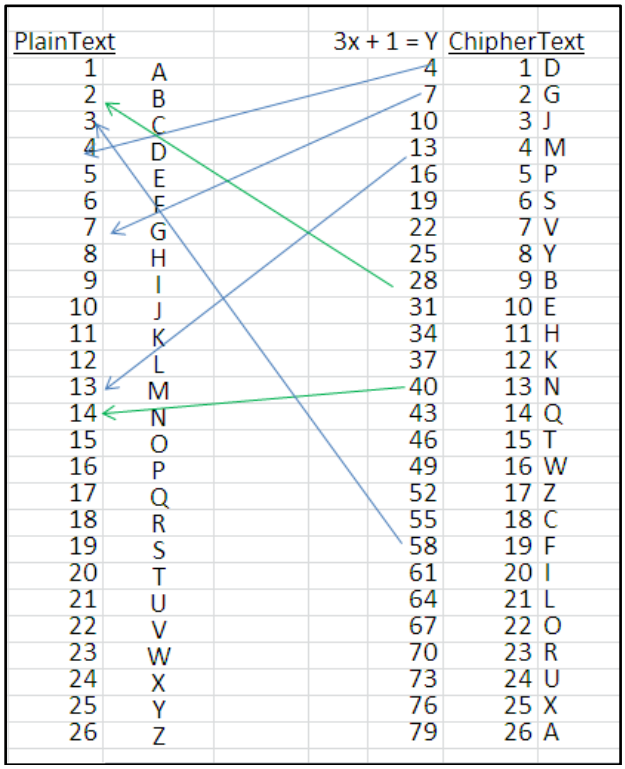
$$y = ax + b \pmod{26} \quad (1)$$

dengan x : posisi huruf plaintext (A = 1, …, Z = 26), y : posisi huruf ciphertext dan a, b: bilangan bulat dengan syarat $gcd(a, 26) = 1$.

Dalam penelitian ini digunakan parameter seperti ditunjukan pada Persamaan 2.

$$y = 3x + 1 \pmod{26} \quad (2)$$

Pemilihan koefisien 3 dan konstanta 1 memastikan pemetaan satu-ke-satu (bijektif), sehingga tidak terjadi *collision* dan proses dekripsi dapat dilakukan secara unik.



Gambar 1 Transformasi linear *plaintext* ke *ciphertext*

Pada Gambar 1 terlihat proses transformasi linear dari *plaintext* ke *ciphertext* menggunakan persamaan $y = 3x + 1$, di mana x merupakan posisi huruf dalam alfabet (1–26). Proses ini menghasilkan pasangan huruf yang unik tanpa pengulangan, sehingga memenuhi kriteria *monoalphabetic substitution cipher* [27]. Setiap huruf dipetakan sebagai berikut:

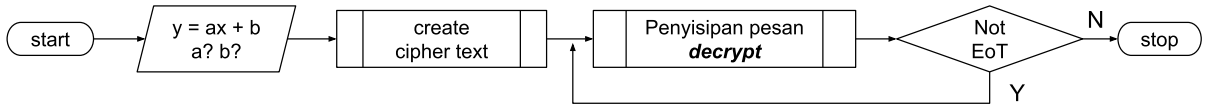
A (1) → D (4)
B (2) → G (7)
C (3) → J (10)
…
Z (26) → A (79 mod 26 = 1)

Ketika hasil y melebihi 26, digunakan operasi *modulo 26* untuk memastikan hasil tetap berada dalam rentang alfabet [34]. Proses ini menghasilkan *cipher alphabet* lengkap yang digunakan pada seluruh proses *embedding*.

Proses Penyisipan (Embedding)

Proses *embedding* dilakukan melalui tahapan berikut:

1. *Plaintex*t dienkripsi menjadi *ciphertext*
2. *Ciphertext* dikonversi menjadi variasi ukuran *font*
3. Variasi ukuran *font* disisipkan ke dalam *cover text*



Gambar 2 *Flowchart* algoritma penyisipan berbasis persamaan linear dan ukuran *font*

Gambar 2 memperlihatkan alur algoritma penyisipan pesan yang diusulkan. Proses dimulai dengan pemilihan persamaan linear $y = ax + b$ sebagai kunci enkripsi, kemudian *plaintext* diubah menjadi *ciphertext* melalui pemetaan *monoalphabetic*. Setiap karakter *ciphertext* dikodekan menjadi variasi ukuran *font* terhadap ukuran dasar 22 pt.
Skema pemetaan:

Alfabet $1 - 13 \rightarrow +(n/2)$ pt
Alfabet $14 - 26 \rightarrow -((n - 13)/2)$ pt

Rentang perubahan: ±0,5 pt sampai ±6,5 pt, agar perubahan tidak mencolok secara visual namun tetap membawa informasi.

Contoh:

Huruf dengan indeks 1 → +0,5 pt
Huruf dengan indeks 13 → +6,5 pt
Huruf dengan indeks 14 → −0,5 pt
Huruf dengan indeks 26 → −6,5 pt

Tahap terakhir dalam proses *embedding* ini yaitu menyisipkan variasi ukuran *font* ke dalam teks penampung (*cover text*).

Proses ini berlangsung secara iteratif hingga seluruh karakter pesan selesai disisipkan (EoT). *Flowchart* di Gambar 2 menunjukkan bahwa proses enkripsi dan penyisipan dilakukan dalam satu alur terpadu dan diotomasi menggunakan VBA (*Visual Basic for Applications*) pada Microsoft Excel.

Algoritma (*Pseudocode*)

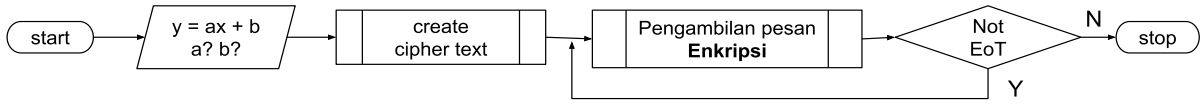
```
Embedding
Input: CoverText, PlainText
CipherText ← Encrypt(PlainText) using y = 3x + 1 mod 26
For each character in CoverText:
    If position matches embedding index:
        Modify font size according to CipherText mapping
Output: StegoText
```

Proses Ekstraksi dan Dekripsi

Ekstraksi dilakukan dengan membaca variasi ukuran *font* pada *stego text* untuk memperoleh kembali *ciphertext*. *Ciphertext* kemudian didekripsi untuk memperoleh *plaintext* menggunakan invers persamaan linear seperti Persamaan 3.

$$x = a^{-1}(y - b) \pmod{26} \quad (3)$$

dengan a^{-1} adalah invers modulo 26 dari a. Seluruh proses ekstraksi dan dekripsi diotomasi menggunakan VBA (*Visual Basic for Applications*) pada Microsoft Excel.



Gambar 3 Proses pengambilan pesan di media digital

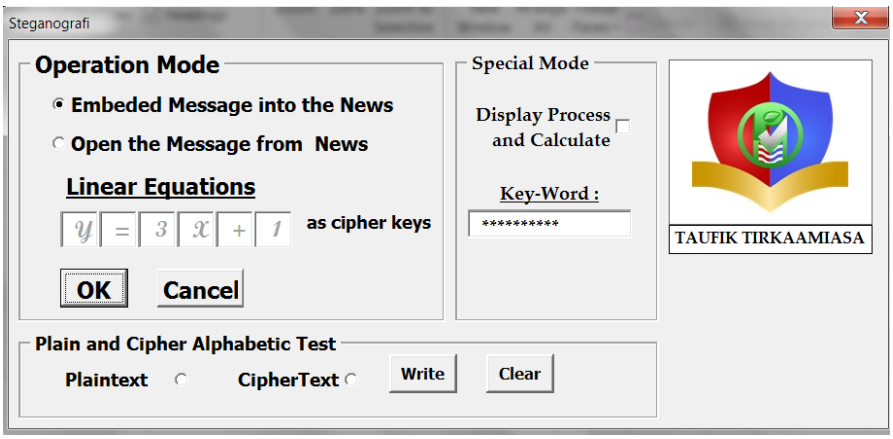
Gambar 3 memperlihatkan alur proses pengambilan kembali pesan rahasia dari *stego-text*. Proses dimulai dengan membaca variasi ukuran *font* yang tersisip pada teks penampung untuk memperoleh representasi *ciphertex*t. Kemudian *ciphertext* tersebut didekripsi menggunakan invers dari persamaan linear $y = 3x + 1$, sehingga diperoleh kembali *plaintext*. Proses ini dilakukan secara iteratif hingga seluruh karakter pesan berhasil dipulihkan *(End of Text)*. Flowchart ini menunjukkan bahwa proses ekstraksi merupakan kebalikan langsung dari proses penyisipan dan memastikan bahwa pesan dapat direkonstruksi secara akurat selama parameter persamaan linear yang sama digunakan.

Implementasi Sistem

Sistem diimplementasikan menggunakan Microsoft Excel VBA yang menyediakan fungsi untuk:

- Input persamaan linear
- Proses *enkripsi* dan *embedding* ke ukuran *font*
- Proses ekstraksi dan dekripsi

Antarmuka sistem pada Gambar 4 memungkinkan seluruh proses dilakukan secara terintegrasi dalam satu lingkungan aplikasi.



Gambar 4 Antarmuka aplikasi steganografi berbasis VBA untuk pemilihan mode operasi dan input persamaan linear sebagai kunci enkripsi

Evaluasi Kinerja

Evaluasi kinerja metode dilakukan terhadap lima *cover text* dan pesan rahasia dengan panjang 10–50 karakter menggunakan tiga metrik utama [13, 21, 31].

1. Fidelity (PSNR)

PSNR digunakan untuk mengukur kualitas *stego text* terhadap *cover text* berdasarkan deviasi ukuran *font* (Persamaan 4) [5][52]. Nilai PSNR ≥ 40 dB dianggap memiliki kualitas tinggi dan

perbedaan hampir tidak terdeteksi oleh pembaca. Meskipun PSNR umumnya digunakan pada citra, pada penelitian ini konsep PSNR diadaptasi untuk teks dengan menghitung selisih ukuran *font* antara *cover text* asli dan *stego text*. Dimana *Fontmax* adalah ukuran *font* terbesar (22 pt) dan MSE adalah *Mean Squared Error* dari variasi ukuran *font*. Nilai PSNR ≥ 40 dB dianggap memiliki kualitas tinggi dan perbedaan hampir tidak terdeteksi oleh pembaca [5].

$$PSNR = 10\log_{10}\left(\frac{MAX_{font}^2}{MSE}\right) \quad (4)$$

2. Robustness

Robustness mengukur ketahanan metode terhadap perubahan format dokumen dengan rumus pada Persamaan 5 [5].

$$Robustness = \frac{\text{jumlah karakter benar setelah modifikasi}}{\text{total karakter}} \times 100\% \quad (5)$$

3. Recovery Accuracy

Recovery accuracy mengukur tingkat keberhasilan pemulihan pesan dimana nilai akurasi ≥ 98% dianggap sangat baik untuk sistem steganografi berbasis teks (Persamaan 6) [13][34].

$$Accuracy = \frac{\text{jumlah karakter benar terdeskripsi}}{\text{total karakter pesan}} \times 100\% \quad (6)$$

HASIL DAN PEMBAHASAN

Pesan rahasia yang akan disampaikan adalah KILL KING TONIGHT yang akan disisipkan pada tulisan UNIVERSITAS BUDI LUHUR. Ditulis di Microsoft Excel menggunakan *font* Times New Roman dengan size/ukuran 22 untuk setiap hurufnya

Setelah disisipkan pesan, maka ukuran *font* teks awal akan berubah masing-masing secara proporsional seperti ditunjukkan pada Gambar 5.

Original Text :	U	N	I	V	E	R	S	I	T	A	S		B	U	D	I		L	U	H	U	R	.
Font Size :	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	
Embeded Text :	U	N	I	V	E	R	S	I	T	A	S		B	U	D	I		L	U	H	U	R	.
Font Size :	28	18.5	18	18		28	18.5	28.5	23		21	17.5	28.5	18.5	23	27.5	21	22.00	22.00	22.00	22.00	22.00	
Added FontSize :	6.00	-3.50	-4.00	-4.00		6.00	-3.50	6.50	1.00		-1.00	-4.50	6.50	-3.50	1.00	5.50	-1.00						
RunningNumber :	12	20	21	21	0	12	20	13	2	0	15	22	13	20	2	11	15						
Secret Message :	K	I	L	L		K	I	N	G		T	O	N	I	G	H	T	.					

Gambar 5 Perubahan ukuran *font* pada teks atau berita

Hasil Transformasi Enkripsi (Plaintext ke Ciphertext)

Tahap awal penelitian dilakukan dengan mentransformasikan *plaintext* menjadi *ciphertext* menggunakan persamaan linear berbasis *cipher monoalphabetic*. Transformasi ini menghasilkan pemetaan satu-ke-satu antara setiap karakter *plaintext* dan *ciphertext*, sehingga tidak terjadi pengulangan pasangan huruf (*collision*).

Sebagai tahap awal dalam proses penyisipan pesan, *plaintext* terlebih dahulu ditransformasikan menjadi *ciphertext* menggunakan persamaan linear yang berfungsi sebagai kunci enkripsi *monoalphabetic*. Proses ini menghasilkan pemetaan satu-ke-satu antara setiap karakter

plaintext dan karakter *ciphertext*, sehingga memungkinkan pembentukan *cipher alphabet* yang konsisten dan dapat didekripsi kembali. Hasil pemetaan tersebut ditunjukkan pada Tabel 1 yang menunjukkan konversi huruf menggunakan Persamaan 1. Metode ini memungkinkan setiap huruf *cipher* unik dan tidak terjadi pengulangan, sehingga dapat diterapkan sebagai *cipher monoalphabetic* yang aman.

Tabel 1 Konversi *Plaintext* ke *Ciphertext*

	PlainText	Kode ASCII		Cipher Text	Kode ASCII
1	A	65		D	68
2	B	66		G	71
3	C	67		J	74
4	D	68		M	77
5	E	69		P	80
6	F	70		S	83
7	G	71		V	86
8	H	72		Y	89
9	I	73		B	66
10	J	74		E	69
11	K	75		H	72
12	L	76		K	75
13	M	77		N	78
14	N	78		Q	81
15	O	79	$y = 3x + 1$	T	84
16	P	80		W	87
17	Q	81		Z	90
18	R	82		C	67
19	S	83		F	70
20	T	84		I	73
21	U	85		L	76
22	V	86		O	79
22	W	87		R	82
24	X	88		U	85
25	Y	89		S	88
26	Z	90		A	65

Jika digunakan persamaan lain seperti $y = 3x + 2$, $y = 5x + 1$ atau $y = 4x + 1$ beberapa huruf *cipher* akan muncul lebih dari satu kali. Hal ini berarti kunci tidak unik, sehingga berpotensi menyulitkan proses dekripsi. Oleh karena itu, persamaan $y = 3x + 1$ dipilih karena memastikan pemetaan unik untuk semua huruf alfabet, yang sejalan dengan prinsip keamanan *monoalphabetic cipher*.

Hasil Akhir Penyisipan

Pesan rahasia yang akan disampaikan adalah KILL KING TONIGHT yang akan disisipkan pada tulisan POLITEKNIK PRASETIYA MANDIRI. Ditulis di Microsoft Excel menggunakan *font* Times New Roman dengan ukuran *font* 22 pt untuk setiap hurufnya dan untuk spasi diberi bintang dengan warna putih. Setelah disisipkan pesan, maka ukuran *font* teks akan berubah masing-masing huruf secara proporsional seperti ditunjukan pada Gambar 6.

Plain Text	P	O	L	I	T	E	K	N	I	K	*	P	R	A	S	E	T	I	Y	A	*	M	A	N	D	I	R	I
Font Size	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00
Stego-Text	P	O	L	I	T	E	K	N	I	K	*	P	R	A	S	E	T	I	Y	A	*	M	A	N	D	I	R	I
Font Size	28,00	18,50	18,00	18,00	22,00	28,00	18,50	28,50	23,00	22,00	21,00	17,50	28,50	18,50	23,00	27,50	21,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00	22,00
Increased Font Size	6,00	-3,50	-4,00	-4,00	0,00	6,00	-3,50	6,50	1,00	0,00	-1,00	-4,50	6,50	-3,50	1,00	5,50	-1,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Secret Message	K	I	L	L		K	I	N	G		T	O	N	I	G	H	T											

Gambar 6 Perubahan ukuran *font* pada tulisan setelah disisipkan pesan rahasia

Analisis Fidelity (Kualitas Visual)

Kualitas visual *stego text* dievaluasi menggunakan metrik *Peak Signal-to-Noise Ratio* (PSNR), yang mengukur tingkat perbedaan antara *cover text* dan *stego text*. Berdasarkan hasil pengujian,

nilai PSNR berada di atas 40 dB untuk seluruh skenario, dengan nilai tertinggi sebesar 45,8 dB pada pesan sepanjang 10 karakter dan nilai terendah sebesar 40,2 dB pada pesan sepanjang 50 karakter, sebagaimana ditunjukkan pada Tabel 2.

Tabel 2 Hasil evaluasi PSNR, *robustness*, dan *recovery accuracy*

Panjang Pesan	PSNR (dB)	Robustness (%)	Recovery Accuracy (%)
10 karakter	45.8	100	100
20 karakter	44.2	100	100
30 karakter	42.5	98.7	99.3
40 karakter	41.6	97.5	99.0
50 karakter	40.2	96.3	98.4

Nilai PSNR yang tinggi mengindikasikan bahwa manipulasi ukuran *font* tidak menyebabkan perubahan visual yang signifikan. Dengan demikian, *stego text* tetap mempertahankan keterbacaan dan tampilan yang identik dengan *cover text* asli. Hasil ini menunjukkan bahwa metode yang diusulkan memiliki tingkat *imperceptibility* yang tinggi, sehingga pesan dapat disembunyikan tanpa menimbulkan kecurigaan visual.

Analisis Robustness terhadap Perubahan Format

Robustness metode diuji dengan melakukan berbagai modifikasi terhadap dokumen, seperti *copy–paste*, konversi ke PDF, dan pemformatan ulang. Hasil evaluasi menunjukkan bahwa nilai *robustness* berada pada rentang 96,3% hingga 100%, dengan rata-rata di atas 98%. Hal ini menunjukkan bahwa sebagian besar karakter pesan tetap dapat dipertahankan meskipun terjadi perubahan format dokumen. Tingkat robustness yang tinggi mengindikasikan bahwa metode berbasis manipulasi ukuran *font* memiliki ketahanan yang baik terhadap transformasi dokumen yang umum terjadi dalam komunikasi digital.

Analisis Recovery Accuracy

Recovery accuracy digunakan untuk mengukur tingkat keberhasilan dalam memulihkan kembali pesan yang telah disisipkan. Hasil menunjukkan bahwa tingkat akurasi pemulihan berada di atas 98% untuk seluruh skenario, dengan tingkat keberhasilan mencapai 100% pada pesan dengan panjang 10 dan 20 karakter. Hal ini menunjukkan bahwa proses ekstraksi dan dekripsi berjalan secara konsisten dan mampu merekonstruksi pesan secara akurat selama parameter enkripsi yang digunakan tetap sama.

Perbandingan dengan Metode Steganografi Teks Konvensional

Dibandingkan dengan teknik steganografi teks berbasis spasi ganda, metode yang diusulkan menunjukkan keunggulan yang signifikan. Pertama, dari sisi kapasitas penyisipan, variasi ukuran *font* memungkinkan representasi lebih banyak simbol tanpa menambah panjang teks, sehingga kapasitas meningkat hingga 25%. Kedua, dari sisi *robustness*, metode ini menunjukkan ketahanan yang lebih tinggi terhadap perubahan format dokumen, yang merupakan kelemahan utama pada teknik berbasis spasi. Ketiga, integrasi persamaan linear sebagai mekanisme enkripsi memberikan lapisan keamanan tambahan karena pesan telah berada dalam bentuk terenkripsi sebelum disisipkan ke dalam media teks.

Diskusi dan Implikasi Metode

Hasil penelitian menunjukkan bahwa kombinasi transformasi matematis berbasis persamaan linear dan manipulasi ukuran *font* mampu menghasilkan sistem steganografi teks yang efektif dan efisien. Pendekatan ini tidak hanya meningkatkan kapasitas penyisipan, tetapi juga mempertahankan keseimbangan antara *imperceptibility, robustness,* dan *recovery accuracy*. Hal ini sejalan dengan temuan Fridrich [12] yang menekankan pentingnya perubahan visual minimal dalam meningkatkan keamanan steganografi.

Selain itu, tingkat keberhasilan ekstraksi yang tinggi juga konsisten dengan penelitian yang menunjukkan bahwa kombinasi teknik enkripsi sederhana dan manipulasi atribut teks dapat menghasilkan sistem penyembunyian informasi yang andal [13]. Dari sisi praktis, metode ini memiliki potensi implementasi pada sistem komunikasi berbasis teks yang membutuhkan keamanan tinggi tanpa mengubah tampilan visual dokumen.

KESIMPULAN

Penelitian ini mengusulkan metode steganografi teks yang mengintegrasikan transformasi matematis berbasis persamaan linear sebagai mekanisme enkripsi dengan manipulasi ukuran *font* sebagai media penyisipan pesan rahasia dalam satu kerangka terpadu. Integrasi ini memungkinkan *ciphertext* hasil transformasi matematis direpresentasikan secara langsung melalui variasi tipografi yang bersifat tidak mencolok, sehingga pesan dapat disembunyikan tanpa mengganggu keterbacaan teks penampung. Pendekatan ini sejalan dengan perkembangan teknik steganografi teks modern yang menekankan integrasi enkripsi dan *embedding* adaptif untuk meningkatkan keamanan komunikasi digital. Hasil evaluasi kuantitatif menunjukkan bahwa metode yang diusulkan mampu mempertahankan kualitas visual teks dengan nilai PSNR di atas 40 dB pada seluruh skenario pengujian, memiliki ketahanan yang tinggi terhadap perubahan format dokumen dengan nilai *robustness* rata-rata serta tingkat *recovery accuracy* lebih dari 96%. Temuan ini menunjukkan bahwa manipulasi ukuran *font* yang dikombinasikan dengan pemetaan deterministik berbasis persamaan linear efektif dalam menjaga keseimbangan antara *imperceptibility, robustness*, dan akurasi ekstraksi, sebagaimana direkomendasikan dalam penelitian steganografi teks mutakhir. Dibandingkan dengan teknik steganografi teks berbasis spasi ganda, metode yang diusulkan memberikan peningkatan kapasitas penyisipan hingga 25% tanpa menambah panjang teks maupun menurunkan kualitas visual dokumen. Selain itu, penggunaan persamaan linear sebagai kunci enkripsi menghasilkan lapisan keamanan tambahan karena pesan yang disisipkan telah berada dalam bentuk terenkripsi sebelum dipetakan ke media teks. Pendekatan keamanan berlapis ini konsisten dengan tren pengembangan *covert communication* dan *information hiding modern* yang menekankan perlindungan tidak hanya pada isi pesan, tetapi juga pada keberadaan dan pola penyampaiannya. Dengan demikian, metode steganografi teks berbasis persamaan linear dan manipulasi ukuran *font* yang diusulkan memiliki potensi aplikasi praktis dalam pengamanan dokumen digital dan sistem komunikasi berbasis teks. Ke depan, penelitian ini dapat dikembangkan lebih lanjut dengan mengeksplorasi variasi transformasi matematis lain, adaptasi ukuran *font* yang lebih dinamis, serta pengujian terhadap skenario serangan steganalisis berbasis pembelajaran mesin untuk meningkatkan ketahanan sistem secara menyeluruh.

DAFTAR PUSTAKA

1. Al-Muhammed, M. J. (2024). Dynamically adjustable computation pattern encryption technique: boosting nonlinearity via integrating block chaotic encoding and color-theory-based key expansion. *Soft Computing*, *28*(23), 13407-13427. https://doi.org/10.1007/s00500-024-10388-9
2. Al-Rekaby, S. N., Khodher, M. A. A. A., Adday, L. K. (2025). A Hybrid Security System for Text Encryption and Steganography in Video Using Multi-Level Chaotic Maps. *International Journal of Safety & Security Engineering*, *15*(3). 521-532. https://doi.org/10.18280/ijsse.150311
3. Alrikabi, H. T., Tuama Hazim, H. (2021). Enhanced Data Security of Communication System Using Combined Encryption and Steganography. *International Journal of*

Interactive Mobile Technologies (iJIM), *15*(16), pp. 144–157. https://doi.org/10.3991/ijim.v15i16.24557

4. Banoth, R., Regar, R. (2023). *Classical and Modern Cryptography for Beginners* (pp. 1-215). Springer. https://doi.org/10.1007/978-3-031-32959-3
5. Bender, W., Gruhl, D., Morimoto, N., Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal, 35*(3.4), 313–336. https://doi.org/10.1147/sj.353.0313
6. Bokhari, M. U., Gulfam, & Hanafi, B. (2025). Quantifying the impact of adversarial attacks on information hiding security with steganography. *International Journal of Information Technology*, *17*(1), 409-422. https://doi.org/10.1007/s41870-024-02191-4
7. Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., Kalker, T. (2008). *Digital watermarking and steganography* (2nd ed.). Morgan Kaufmann.
8. Darwis, D., Pamungkas, N. B. (2021). Comparison of least significant bit, pixel value differencing, and modulus function on steganography to measure image quality, storage capacity, and robustness. In *Journal of Physics: Conference Series* (Vol. 1751, No. 1, p. 012039). IOP Publishing.
9. Dhawan, S., Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective*, *30*(2), 63–87. https://doi.org/10.1080/19393555.2020.1801911
10. Driss, M., Berriche, L., Atitallah, S. B., Rekik, S. (2025). Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions. *IEEE Access*. DOI: 10.1109/ACCESS.2025.3564120
11. Evsutin, O., Melman, A., Meshcheryakov, R. (2020). Digital steganography and watermarking for digital images: A review of current research directions. *IEEE Access*, *8*, 166589-166611. DOI: 10.1109/ACCESS.2020.3022779
12. Fridrich, J. (2009). *Steganography in digital media: Principles, algorithms, and applications*. Cambridge University Press.
13. Gutub, A. A., Al-Ghamdi, J., Al-Haidari, S., Khan, F., Al-Haidari, S. (2010). Improved text steganography in SMS. *Journal of Information Hiding and Multimedia Signal Processing, 1*(4), 297–313.
14. Hilal, A. M., Al-Wesabi, F. N., Abdelmaboud, A., Hamza, M. A., Mahzari, M., Hassan, A. Q. (2022). A hybrid intelligent text watermarking and natural language processing approach for transferring and receiving an authentic english text via internet. *The Computer Journal*, *65*(2), 423-435. https://doi.org/10.1093/comjnl/bxab087
15. Iqbal, N. Image encryption using Queen. *Multimed Tools Appl* 83, 10551–10585 (2024). https://doi.org/10.1007/s11042-023-15674-6
16. Jain, V. (2021). A review on different types of cryptography techniques "should be replaced by" exploring the potential of steganography in the modern era. *ACADEMICIA: An International Multidisciplinary Research Journal*, *11*(11), 1139-1146. DOI: 10.5958/2249-7137.2021.02569.6
17. Jagielski, M., Carlini, N., Berthelot, D., Kurakin, A., & Papernot, N. (2020). High accuracy and high fidelity extraction of neural networks. In *29th USENIX security symposium (USENIX Security 20)* (pp. 1345-1362).
18. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer, 31*(2), 26–34. https://doi.org/10.1109/2.660187
19. Kessler, G. C. (2015). An overview of steganography for the computer forensics examiner. *Forensic Science Communications, 6*(3).
20. Knight, R., Nurse, J. R. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, Vol. 99, 102036.

https://doi.org/10.1016/j.cose.2020.102036
21. Kumar, P., Chand, S. (2016). Steganography: A data hiding technique. *International Journal of Computer Applications, 144*(5), 1–6. https://doi.org/10.5120/ijca2016910522
22. Kumar, A., Rani, R., & Singh, S. (2023). A survey of recent advances in image steganography. *Security and Privacy*, *6*(3), e281. https://doi.org/10.1002/spy2.281
23. Li, Z., Zhang, Q. Li, X. (2024). A novel large capacity coverless image steganography method based on hybrid framework of image generation-mapping. *Multimedia Systems* **30**, 345. https://doi.org/10.1007/s00530-024-01550-2
24. Ma, X., Gao, Y., Wang, Y., Wang, R., Wang, X., Sun, Y., Ding, Y., Xu, H., Chen, Y., Zhao, Y., Huang, H., Li, Y., Wu, Y., Zhang, J., Zheng, X., Bai, Y., Wu, Z., Qiu, X., Zhang, J., . . . Jiang, Y. (2025). Safety at Scale: A Comprehensive Survey of Large Model and Agent Safety. *ArXiv*. https://arxiv.org/abs/2502.05206
25. Majeed, M. A., Sulaiman, R., Shukur, Z., Hasan, M. K., Majeed, M. A., Sulaiman, R., Shukur, Z., Hasan, M. K. (2021). A Review on Text Steganography Techniques. *Mathematics*, *9*(21). https://doi.org/10.3390/math9212829
26. Mardon A, Varghese N, Pham J, Di Martino A, Chana I. Cryptography Online. Golden Meteorite Press. 2021;
27. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.
28. Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R. M., Acosta Del Campo, O. (2017). A novel technique for image encryption using Latin squares. *Multimedia Tools and Applications, 76*(6), 8825–8845. https://doi.org/10.1007/s11042-016-3489-3
29. Osman, O. M., Kanona, M. E. A., Hassan, M. K., Elkhair, A. A. E., Mohamed, K. S. (2022). Hybrid multistage framework for data manipulation by combining cryptography and steganography. *Bulletin of Electrical Engineering and Informatics*, *11*(1), 327-335. DOI: https://doi.org/10.11591/eei.v11i1.3451
30. Pandey, B. K., Pandey, D., Wairya, S., Agarwal, G., Dadeech, P., Dogiwal, S. R., Pramanik, S. (2022). Application of Integrated Steganography and Image Compressing Techniques for Confidential Information Transmission. Cyber Security and Network Security. 169-191. https://doi.org/10.1002/9781119812555.ch8
31. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—A survey. *Proceedings of the IEEE, 87*(7), 1062–1078. https://doi.org/10.1109/5.771065
32. Puttegowda, K., Ravikiran, H. N., Metan, J., Mathapati, M., Champa, C. H., Sunil Kumar, D. S. (2025). Analysis and Comparison of Various Steganography Methods for Secure 6G Communication. In *6G Cyber Security Resilience: Trends and Challenges* (pp. 147-166). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-85008-0_7
33. Riddhi, G. P., Sharma, V. (2025). A Comprehensive Review of Digital Video Watermarking Techniques in Spatial, Frequency, and Compressed Domain. *Archives of Computational Methods in Engineering*, 1-37. Doi :10.1007/s11831-025-10443-0
34. Shirali-Shahreza, M., Shirali-Shahreza, S. (2008). Text steganography in SMS. *2008 International Conference on Convergence and Hybrid Information Technology, 1*, 605–610. https://doi.org/10.1109/ICCIT.2008.281
35. Safitra, M. F., Lubis, M., Fakhrurroja, H., Safitra, M. F., Lubis, M., Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, *15*(18). https://doi.org/10.3390/su151813369
36. S. Rahman et al., (2023). A Comprehensive Study of Digital Image Steganographic Techniques," in IEEE Access, vol. 11, pp. 6770-6791, doi: 10.1109/ACCESS.2023.3237393.

37. Shahzad, K., Zia, T., Qazi, E.-u.-H. (2022). A Review of Functional Encryption in IoT Applications. Sensors, 22(19), 7567. https://doi.org/10.3390/s22197567
38. Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.
39. S. Rahman *et al*., "A Comprehensive Study of Digital Image Steganographic Techniques," in *IEEE Access*, vol. 11, pp. 6770-6791, 2023, doi: 10.1109/ACCESS.2023.3237393.
40. Shayegani, E., Mamun, M. A., Fu, Y., Zaree, P., Dong, Y. (2023). Survey of Vulnerabilities in Large Language Models Revealed by Adversarial Attacks. *ArXiv*. https://arxiv.org/abs/2310.10844
41. Subramanian, N., Elharrouss, O., Al-Maadeed, S., Bouridane, A. (2021). Image steganography: A review of the recent advances. IEEE access, 9, 23409-23423. DOI: 10.1109/ACCESS.2021.3053998
42. Taleby Ahvanooey, M., Zhu, M. X., Mazurczyk, W., Li, Q., Kilger, M., Choo, K. R., Conti, M. (2022). CovertSYS: A systematic covert communication approach for providing secure end-to-end conversation via social networks. *Journal of Information Security and Applications*, *71*, 103368. https://doi.org/10.1016/j.jisa.2022.103368
43. Tran, D. N., Zepernick, H. J., Chu, T. M. C. (2022). Lsb data hiding in digital media: a survey. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, 1-50. https://doi.org/10.4108/eai.5-4-2022.173783
44. Varol Arısoy, M. (2022). LZW-CIE: a high-capacity linguistic steganography based on LZW char index encoding. *Neural Computing and Applications*, *34*(21), 19117-19145. https://doi.org/10.1007/s00521-022-07499-5
45. Wahab, O. F. A., Khalaf, A. A., Hussein, A. I., Hamed, H. F. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. *IEEE access*, *9*, 31805-31815. DOI: 10.1109/ACCESS.2021.3060317
46. Wang, H., Wang, S. (2004). Cyber warfare: Steganography vs steganalysis. *Communications of the ACM, 47*(10), 76–82. https://doi.org/10.1145/1022594.1022633
47. Wang, Z., Byrnes, O., Wang, H., Sun, R., Ma, C., Chen, H., ... & Xue, M. (2023). Data hiding with deep learning: A survey unifying digital watermarking and steganography. *IEEE Transactions on Computational Social Systems*, *10*(6), 2985-2999. DOI: 10.1109/TCSS.2023.3268950
48. Xiang, L., Wang, R., Yang, Z., Liu, Y. (2022). Generative linguistic steganography: A comprehensive review. *KSII Transactions on Internet and Information Systems (TIIS)*, *16*(3), 986-1005.
49. Yan, R., Chu, C., Yang, Z., Murawaki, Y. (2025). A Comprehensive Survey on Linguistic Steganography: Methods, Countermeasures, Evaluation, and Challenges.
50. Zainab, A., Arslan, M., Aslam, N., Fuzail, M., & Shaikh, A. (2025). A Hybrid Approach to Data Security: Integrating Cryptography and Steganography For Enhanced Protection of Eye Disease Data. *Kashf Journal of Multidisciplinary Research*, *2*(07), 55-74. https://doi.org/10.71146/kjmr534
51. Zakeri, M., Zakeri, F., Aliahmadi, A. (2021). Review of digital steganography methods. *Multimedia Tools and Applications, 80*(5), 7859–7890. https://doi.org/10.1007/s11042-020-09852-w
52. Zhang, W., Li, X., Yu, N., Zhao, Y. Q. (2015). Improving embedding efficiency of covering codes for applications in steganography. *IEEE Transactions on Information Forensics and Security, 10*(2), 219–232. https://doi.org/10.1109/TIFS.2014.2368355
53. Zhao, J., Masood, R., Seneviratne, S. (2021). A review of computer vision methods in network security. *IEEE Communications Surveys & Tutorials*, *23*(3), 1838-1878. doi:

10.1109/COMST.2021.3086475
54. Z. Wang et al. (2023). Data Hiding With Deep Learning: A Survey Unifying Digital Watermarking and Steganography," in IEEE Transactions on Computational Social Systems, vol. 10, no. 6, pp. 2985-2999, doi: 10.1109/TCSS.2023.3268950
55. Zimmer, L., Lindauer, M., Hutter, F. (2021). Auto-pytorch: Multi-fidelity metalearning for efficient and robust autodl. *IEEE transactions on pattern analysis and machine intelligence*, *43*(9), 3079-3090. DOI: 10.1109/TPAMI.2021.3067763
56. Putranti, Nurrohmah Chang, Shyang-Jye & Raffiudin, Muhammad. (2025). Revitalizing Art with Technology: A Deep Learning Approach to Virtual Restoration. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 10(1), pp. 87–99. doi:10.14421/jiska.2025.10.1.87-99.
57. Tombari, F., Di Stefano, L., Mattoccia, S., Galanti, A. (2008). Performance Evaluation of Robust Matching Measures. International Conference on Computer Vision Theory and Applications, 1, 473–478. https://cris.unibo.it/handle/11585/60782.