

PENERAPAN CHAOS TEORI ARNOLD CAT MAP PADA STEGANOGRAFI PVD UNTUK DATA SECURIT

Reza Putra Ramadhan¹, Haida Dafitri, Rismayanti³

^{1,2,3} Program Studi Teknik Informasi, Fakultas Teknik dan Komputer, Universitas Harapan Medan,

e-mail: ¹reza.putra9190@gmail.com, ²aida.stth@gmail.com, ³risma.stth@gmail.com

ABSTRAK

Pertumbuhan pertukaran data digital melalui jaringan menuntut mekanisme perlindungan informasi yang tidak hanya mengamankan isi pesan, tetapi juga menyamarkan keberadaannya. Steganografi *Pixel-Value Differencing* (PVD) banyak digunakan karena mampu menyisipkan data dengan distorsi visual yang rendah, namun pola penyisipannya yang berurutan masih rentan terhadap analisis pihak yang tidak berwenang. Penelitian ini bertujuan merancang aplikasi yang mengintegrasikan teori chaos, yaitu *Arnold Cat Map* (ACM), dengan steganografi PVD untuk meningkatkan keamanan data pada citra digital. ACM digunakan untuk mengacak posisi piksel citra sehingga distribusi data yang disisipkan menjadi acak dan sulit diprediksi, kemudian data rahasia disisipkan dengan metode PVD yang menjaga kualitas visual citra. Hasil pengujian menunjukkan bahwa algoritma yang diusulkan mampu menyembunyikan data secara efisien dengan tingkat deteksi yang rendah serta kerusakan minimal pada citra asli, dan data tersembunyi sulit diuraikan tanpa kunci yang tepat. Meskipun proses pengacakan berpotensi menurunkan kualitas citra dan menambah waktu komputasi, kedua tantangan tersebut dapat diminimalkan melalui optimasi algoritma. Dengan demikian, kombinasi ACM dan PVD merupakan pendekatan yang andal untuk melindungi informasi sensitif pada komunikasi daring maupun penyimpanan data digital.

Kata kunci: arnold cat map, teori chaos, steganografi, pixel-value differencing, keamanan data

ABSTRACT

The growing exchange of digital data over networks demands protection mechanisms that secure not only the content of a message but also conceal its very existence. Pixel-Value Differencing (PVD) steganography is widely used because it embeds data with low visual distortion, yet its sequential embedding pattern remains vulnerable to analysis by unauthorized parties. This study aims to design an application that integrates chaos theory, specifically the Arnold Cat Map (ACM), with PVD steganography to enhance data security in digital images. ACM scrambles pixel positions so that the distribution of embedded data becomes random and difficult to predict, after which the secret data is embedded using PVD to preserve the visual quality of the image. Test results show that the proposed algorithm hides data efficiently with a low detection rate and minimal damage to the original image, and the hidden data is difficult to recover without the correct key. Although the scrambling process may reduce image quality and increase computation time, these challenges can be minimized through algorithm optimization. Therefore, combining ACM and PVD offers a reliable approach to protecting sensitive information in online communication and digital data storage.

Keywords: arnold cat map, chaos theory, steganography, pixel-value differencing, data security

1. PENDAHULUAN

Keamanan data merupakan aspek krusial dalam era digital yang ditandai dengan pertukaran informasi yang semakin masif dan cepat. Dalam konteks ini, ancaman terhadap kerahasiaan dan integritas data juga meningkat, sehingga diperlukan metode yang mampu melindungi informasi dari akses tidak sah. Dua pendekatan yang banyak dikembangkan untuk meningkatkan keamanan data digital adalah enkripsi dan steganografi. Enkripsi mengubah bentuk data agar tidak dapat dibaca tanpa kunci dekripsi, sedangkan steganografi berfokus pada menyembunyikan data ke dalam media digital seperti gambar, audio, atau video sehingga keberadaannya sulit dideteksi.

Salah satu metode steganografi yang banyak digunakan adalah Pixel-Value Differencing (PVD), yang memanfaatkan perbedaan nilai piksel dalam citra untuk menyisipkan data rahasia [1][2]. Metode ini dikenal efektif dalam menjaga kualitas visual gambar sekaligus memiliki kapasitas penyembunyian yang cukup tinggi. Namun, meskipun efisien, PVD masih memiliki kelemahan dalam hal ketahanan terhadap serangan deteksi atau analisis statistik. Untuk mengatasi keterbatasan tersebut, berbagai penelitian mengusulkan penggabungan antara steganografi dengan konsep teori chaos, yang memiliki karakteristik sensitif terhadap kondisi awal dan menghasilkan pola yang tampak acak namun deterministic [3].

Salah satu penerapan teori chaos yang populer adalah Arnold Cat Map (ACM). Algoritma ini digunakan untuk mengacak posisi piksel pada citra digital secara sistematis sehingga distribusi informasi menjadi tidak teratur dan sulit diprediksi tanpa kunci yang tepat [4][5]. Kombinasi antara Arnold Cat Map dan metode PVD dapat menghasilkan mekanisme penyembunyian data yang lebih aman, karena proses pengacakan chaos mampu meningkatkan kompleksitas dan mengurangi kemungkinan data tersembunyi terdeteksi oleh pihak yang tidak berwenang [6][7].

Berbagai penelitian sebelumnya telah membuktikan efektivitas pendekatan berbasis teori chaos dalam meningkatkan keamanan citra digital. Zhang dan Liu (2019) melalui penelitian berjudul *"Image Encryption Algorithm Based on Arnold Cat Map and Logistic Map"* menunjukkan bahwa kombinasi Arnold Cat Map dan Logistic Map mampu memperkuat sistem enkripsi dengan menghasilkan kunci chaos yang kompleks dan sulit diretas [8]. Sementara itu, Sharif Shah (2018) dalam *"An Improved Image Steganography Algorithm based on PVD"* mengusulkan metode PVD yang disempurnakan menggunakan deteksi tepi dan pergeseran histogram untuk mempertahankan kualitas gambar sekaligus meningkatkan kapasitas penyembunyian data [9].

Penelitian lain oleh Qi Li, et al (2020) dalam *"A Novel Image Steganography Scheme Based on Chaos Theory and Genetic Algorithm"* membuktikan bahwa penggabungan teori chaos dan algoritma genetik dapat mengoptimalkan proses penyembunyian data serta meningkatkan resistansi terhadap steganalisis [10]. Selain itu, Noor dkk (2018) melalui studi *"Pengacakan Citra Digital Berwarna dengan Kriptografi Arnold CAT MAP (ACM)"* menunjukkan bahwa penerapan Arnold Cat Map dalam domain frekuensi (DCT) dapat menghasilkan citra yang sangat sulit direkonstruksi tanpa kunci yang benar [11].

Berdasarkan hasil-hasil penelitian tersebut, penggabungan Arnold Cat Map dan metode PVD menjadi pendekatan yang menjanjikan dalam menciptakan algoritma steganografi yang lebih aman dan efisien. Melalui pemanfaatan sifat non-linear dan

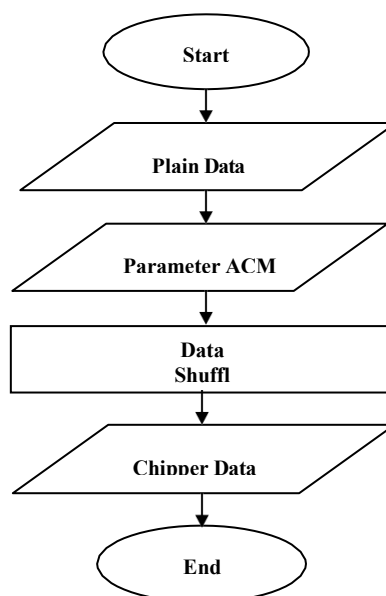
dinamika kompleks dari teori chaos, proses penyembunyian data dapat dilakukan dengan penyebaran informasi yang acak dan sulit dilacak. Dengan demikian, penelitian ini berfokus pada “Penerapan Chaos Teori Arnold Cat Map pada Steganografi PVD untuk Data Security” dengan tujuan menghasilkan sistem steganografi yang memiliki tingkat keamanan tinggi, efisien dalam penyisipan data, serta tetap menjaga kualitas visual citra.

Diharapkan, hasil penelitian ini dapat memberikan kontribusi signifikan dalam pengembangan teknologi keamanan informasi, khususnya dalam bidang steganografi berbasis teori chaos, yang dapat diterapkan pada berbagai konteks seperti komunikasi digital, penyimpanan data rahasia, maupun sistem keamanan siber

2. METODE PENELITIAN

Analisis Enkripsi Arnold Cat Map dan stegano PVD

Proses enkripsi meliputi: *Data shuffle*, *RGB shuffle* dan *encoding*. *Data shuffle* menggunakan Algoritma ACM pada persamaan (1), untuk mengacak susunan *Data* padap *lain Data*, sedangkan *RGB shuffle* dan *encoding* digunakan untuk mengacak nilai RGB pada *plain Data* serta mengubah nilai RGB dengan pengXOR-an yang menggunakan skema *Chaining Block Cipher* (CBC). Proses ini memanfaatkan bilangan acak yang dibangkitkan menggunakan NCA [12]. Gambar 1 dibawah ini menunjukkan Diagram Alir proses enkripsi.



Gambar 1. Enkripsi Metode *Arnold's Cat Map* (ACM)

Dalam tahap enkripsi menggunakan ACM untuk mengacak susunan data. Berikut adalah contoh proses Data shuffle menggunakan plain Dara beurukan 3 Data x 3 Data.

	0	1	2
0	1	2	3
1	4	5	6
2	7	8	9

Parameter Arnold Cat Map yang diinputi yaitu $b=2$, $c=4$, kemudian dilakukan transformasi ACM dan menghasilkan:

$$\begin{bmatrix} 1 & 2 \\ 4 & 9 \end{bmatrix} \times \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \mod 3 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 4 & 9 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 9 \end{bmatrix} \mod 3 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 4 & 9 \end{bmatrix} \times \begin{bmatrix} 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 4 \\ 18 \end{bmatrix} \mod 3 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 4 & 9 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 4 \end{bmatrix} \mod 3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 4 & 9 \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 13 \end{bmatrix} \mod 3 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 4 & 9 \end{bmatrix} \times \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 22 \end{bmatrix} \mod 3 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 4 & 9 \end{bmatrix} \times \begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 8 \end{bmatrix} \mod 3 = \begin{bmatrix} 2 \\ 2 \end{bmatrix}$$

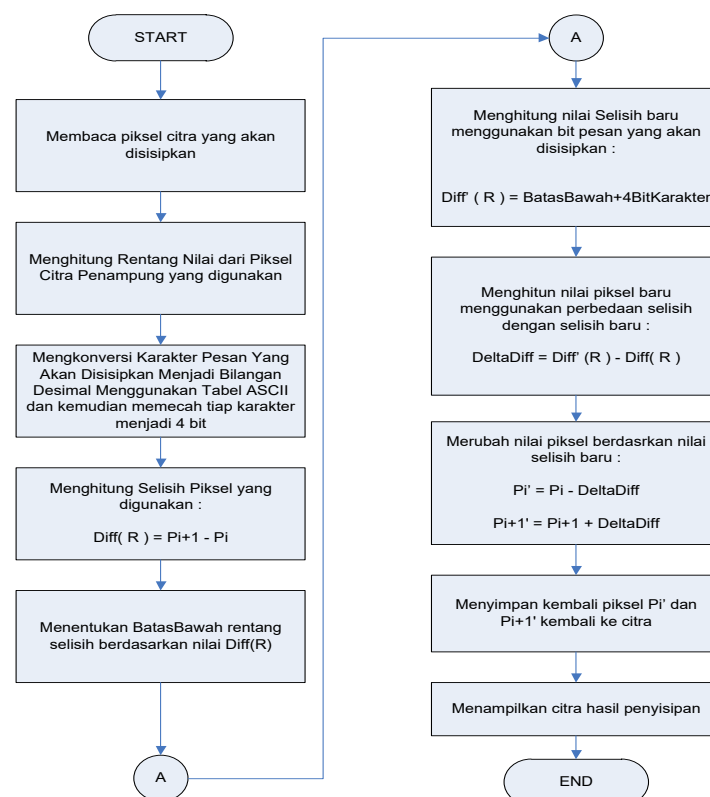
	0	1	2
0	1	2	3
1	4	5	6
2	7	8	9

	0	1	2
0	1	5	9
1	3	4	8
2	2	6	7

1. Tentukan nilai kunci enkripsi berupa dua bilangan bulat a dan b .
2. Lakukan transformasi pada citra dengan menggunakan persamaan berikut:

- i. $x' = (x + y) \bmod N$ $y' = (ax + by) \bmod N$
 dimana x dan y adalah koordinat piksel pada citra, x' dan y' adalah koordinat baru hasil transformasi, a dan b adalah kunci enkripsi, dan N adalah ukuran citra.
3. Ulangi langkah 3 sebanyak t kali, dimana t adalah jumlah iterasi yang ditentukan.
 4. mCitra yang telah diubah posisi pikselnya adalah hasil enkripsi.

Algoritma *PVD* sendiri merupakan teknik steganografi yang memanfaatkan selisih nilai dari piksel pada area tertentu dalam menentukan bit data dan kunci yang akan disisipkan. Adapun rancangan penelitian menggunakan metode PVD dapat dilihat pada gambar 2 berikut.



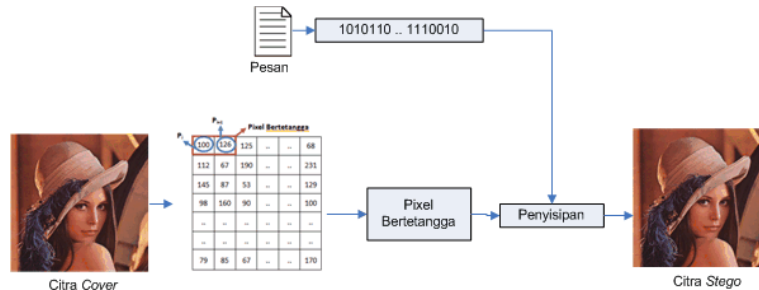
Gambar 2. Rancangan Metode Penelitian PVD

Analisis Metode Pixel Value Differencing (PVD)

Metode *Pixel Value Differencing* (PVD) merupakan salah satu metode steganografi pada citra digital yang beroperasi pada ranah spasial[13]. Konsep dari metode ini yaitu dengan menyisipkan pesan kedalam dua *pixel* yang bertetangga, dengan memanfaatkan perbedaan intensitas warna dari kedua *pixel* yang bertetangga tersebut. Seperti halnya metode steganografi lainnya, pada metode ini terdapat dua proses yaitu proses penyisipan/*embedding* dan pengungkapan/ ekstraksi[14].

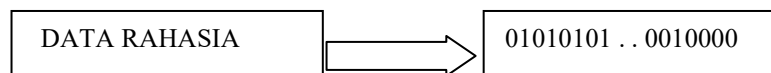
Proses penyisipan yaitu proses menyembunyikan informasi kedalam media penampung, dalam hal ini media penampung berupa citra digital. Proses ini akan

menghasilkan citra yang telah disisipkan pesan (*stego-object*) yang menyerupai dengan citra sebelum disisipkan pesan. Proses penyisipan pada metode *pixel value differencing* terlihat pada gambar 3.



Gambar 3. Proses Penyisipan Pesan

Contoh proses penyisipan, jika diketahui pesan yang akan disisipkan berupa file Uji.txt dengan isi pesan yaitu “DATA RAHASIA”. Tahap awal yang dilakukan yaitu merubah isi pesan kedalam bentuk biner seperti pada gambar 4.



Gambar 4. Perubahan Pesan Teks ke Bit

Tahap selanjutnya yaitu mengambil nilai pixel dari citra yang akan disisipkan pesan. Jika diketahui citra yang digunakan yaitu lena.bmp dengan nilai pixel seperti pada gambar 5.



Gambar 5. Nilai Pixel Dari Citra Cover

Maka tahap selanjutnya yaitu melakukan proses penyisipan menggunakan metode *pixel value differencing* dengan tahapan-tahapan yaitu sebagai berikut[15]:

1. Mengambil pixel yang bertetangga dari citra. Contoh *pixel* yang bertetangga yaitu *pixel*(0,0) dengan *pixel*(0,1) seperti pada gambar 3.6. Nilai dari *pixel* yang bertetangga tersebut diambil untuk dilakukan penyisipan. Jika P_i dan P_{i+1} merupakan *pixel* yang bertetangga, maka $P_i = 100$ dan $P_{i+1} = 126$.

	P_i	P_{i+1}				
	100	126	125	..	..	68
	112	67	190	..	..	231
	145	87	53	..	..	129
	98	160	90	..	..	100
	..	..	..	..	..	..
	..	..	..	..	..	..
	79	85	67	..	..	170

Gambar 6. Pixel yang Bertetangga Dari Citra Cover

- Menghitung nilai *differencing value* dari kedua *pixel* tersebut menggunakan persamaan II.4 yaitu $d = |100 - 126|$, sehingga didapat $d = 26$.
- Mencari letak *continues range* dari nilai *difference value* pada skema wu dan tsai $R = \{[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]\}$. Letak *continues range* yang didapat dari $d = 26$ yaitu $[16, 31]$ dimana $lk = 16$, dan $uk = 31$.
- Menghitung berapa banyak bit dari pesan yang dapat disisipkan kedalam kedua *pixel* yang dibandingkan menggunakan persamaan II.5 yaitu $t = \text{Log}_2(31 - 16)$ sehingga didapat $t = 4$, maka ambil bit dari pesan sebanyak t yaitu 0101.
- Mengubah nilai bit sebanyak t kedalam nilai *decimal*. Bit informasi yang disisipkan yaitu 0101, maka nilai *decimal*-nya yaitu 5 atau $b = 5$.
- Menghitung nilai *differencing value* yang baru menggunakan persamaan II.6, $d' = 16 + 5$ sehingga didapat nilai *differencing value* yang baru yaitu $d' = 21$.
- Melakukan penyisipan dengan mengubah nilai dari *pixel* yang dibandingkan dengan nilai *pixel* yang baru sesuai dengan aturan – aturan yang ada, dimana $m = 5$ didapat menggunakan persamaan II.7 yaitu $M = |21 - 26|$. Aturan yang terpenuhi yaitu $d' < d$ dan $P' < P'$, maka $P' = 100 + \lfloor 5/2 \rfloor$
 $i \quad i+1 \quad i \quad i+1$ dan $P' = 126 - \lfloor 5/2 \rfloor$
- Menyimpan nilai *pixel* yang baru yaitu $P' = 102$ dan $P' = 123$ kedalam
 $i \quad i+1$

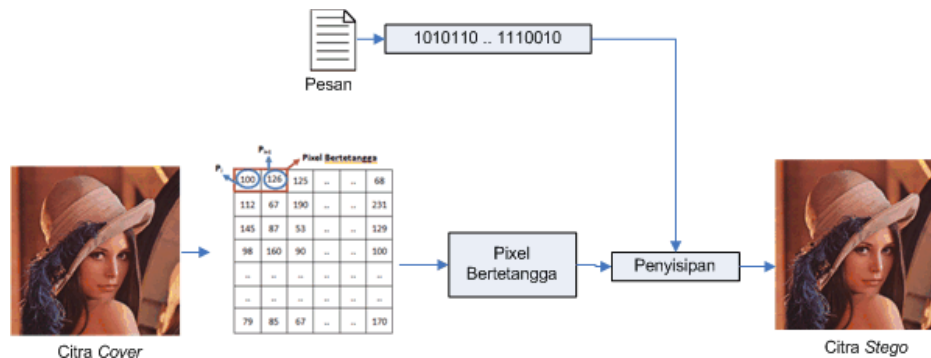
citra. Tahapan ini dilakukan sampai semua pesan tersisipi, sehingga menjadiseperti pada gambar 7.

102	123	123	..	..	69
116	70	192	..	..	232
144	88	55	..	..	128
96	162	91	..	..	99
..	..	..	..	..	..
..	..	..	..	..	..
77	85	68	..	..	172



Gambar 7. Nilai Pixel Citra Setelah Disisipi Pesan Analisis Proses Pengungkapan / Ekstraksi.

Proses ekstraksi yaitu proses pengambilan informasi yang tersembunyi pada citra digital. Proses ini akan menghasilkan *file* informasi yang disembunyikan, dengan masukan berupa citra *stego-object*. Proses ekstraksi pada metode *pixel value differencing* terlihat pada gambar 8.



Gambar 8. Proses Ekstraksi Pesan

Tahap awal pada proses ekstraksi pesan yaitu mengambil nilai *pixel* dari citra yang telah disisipkan pesan. Jika diketahui citra yang digunakan yaitu StegaLena.bmp dengan nilai *pixel* seperti pada gambar 9.



Gambar 9. Nilai Pixel Dari Citra Stego

Maka tahap selanjutnya yaitu melakukan proses ekstraksi menggunakan metode *pixel value differencing* dengan tahapan-tahapan yaitu sebagai berikut:

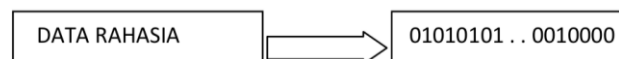
1. Mengambil pixel yang bertetangga dari citra. Contoh *pixel* yang bertetangga yaitu *pixel*(0,0) dengan *pixel*(0,1) seperti pada gambar III.9. Nilai dari *pixel* yang bertetangga tersebut diambil untuk dilakukan penyisipan. Jika P_i dan P_{i+1} merupakan *pixel* yang bertetangga, maka $P_i = 102$ dan $P_{i+1} = 123$.

102	123	123	..	..	69
116	70	192	..	..	232
144	88	55	..	..	128
96	162	91	..	..	99
..	..	..	..	..	..
..	..	..	..	..	..
77	85	68	..	..	172

Gambar 10. Pixel yang Bertetangga Fari Citra Stego

2. Menghitung nilai *differencing value* dari kedua *pixel* tersebut menggunakan persamaan II.4 yaitu $d = |102 - 123|$, sehingga didapat $d = 21$.
3. Mencari letak *continues range* dari nilai *difference value* pada skema wu dan tsai $R = \{[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]\}$. Letak *continues range* yang didapat dari $d = 21$ yaitu $[16, 31]$ dimana $lk = 16$, dan $uk = 31$.
4. Menghitung berapa banyak bit dari informasi yang disisipkan kedalam kedua *pixel*. Banyak bit tersebut dihitung menggunakan persamaan II.5 yaitu $t = \log_2(31 - 16)$ sehingga didapat $t = 4$, atau terdapat 4 bit pesan yang disisipkan pada kedua *pixel*.
5. Menghitung nilai b atau nilai *decimal* dari bit pesan yang disisipkan dengan menggunakan persamaan II.6 yaitu $b = 21 - 16$ sehingga didapat nilai $b = 5$ atau nilai *decimal* dari bit pesan adalah 5.
6. Mengubah nilai b atau nilai *decimal* pesan kedalam bentuk bit sebanyak t , maka didapat bit pesan 0101.

Tahapan-tahapan pada metode *pixel value differencing* tersebut diulang hingga semua pesan yang terdapat di dalam citra terekstrak. Tahap selanjutnya setelah semua pesan terekstrak yaitu merubah pesan dalam bentuk biner ke bentuk semula. Jika pesan yang disisipkan berupa pesan teks, maka diubah kedalam bentuk teks seperti pada gambar 11.



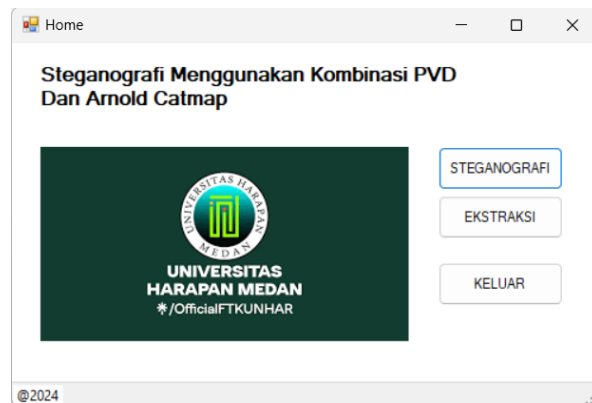
Gambar 11. Perubahan Pesan Bit ke Teks

3. HASIL DAN PEMBAHASAN

Pada Penerapan Chaos Teori Arnold Cat Map Pada Steganografi Pvd Untuk Data Security terdapat beberapa *interface* atau antarmuka yang di desain untuk mempermudah *user* atau pemakai dalam menggunakan atau menjalankan aplikasi ini. Adapun *interface* atau antarmuka adalah sebagai berikut:

1. Halaman Utama

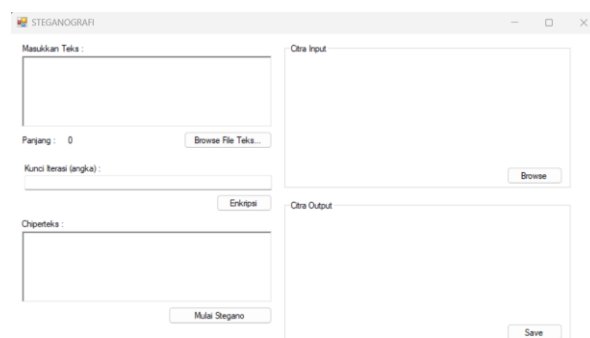
Halaman utama sendiri adalah sebuah halaman yang akan digunakan sebagai halaman navigasi yang akan mengarahkan pengguna untuk dapat memilih halaman enkripsi atau dekripsi. Adapun tampilan dari halaman *login* admin dapat dilihat pada gambar berikut:



Gambar 12. Halaman Utama

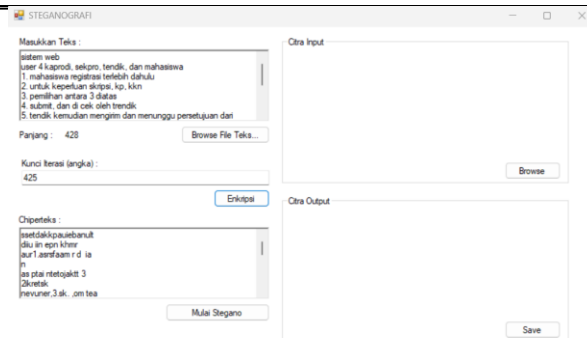
2. Menu Steganografi

Halaman menu Steganografi adalah halaman yang dkhhususkan untuk proses pengamanan data dengan menyisipkan informasi yang telah melewati proses pengacakan. Adapun tampilan dari halaman steganografi dapat dilihat pada gambar 13.



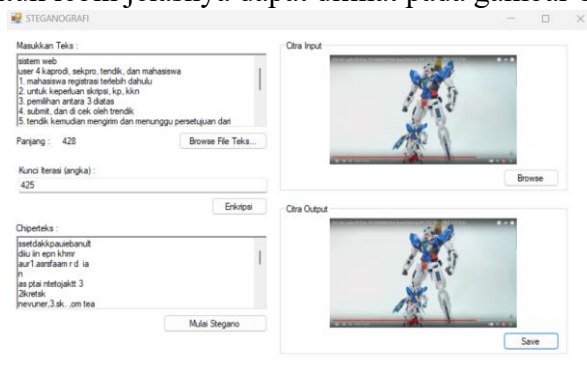
Gambar 13. Halaman Steganografi

Dalam penggunaannya system membutuhkan beberapa komponen wajib yang digunakan untuk kebutuhan system. Pertama system membutuhkan data yang akan dirahasiakan, untuk ini system dapat menerima inputan langsung ketikan kedalam system atau dengan menggunakan data teks yang sudah di save terlebih dahulu. Setelah data teks diinput kedalam system, langkah selanjutnya adalah meinputkan kunci iterasi yang dibutuhkan oleh algoritma Arnold Cat Map. Setelah kedua komponen tersebut lengkap, maka sleanjutnya akan dapat dilaksanakan proses pengamanan data untuk menghasilkan chiperteks. Untuk lebih jelasnya dapat dilihat pada gambar berikut:



Gambar 14. Halaman Stegano Input Teks dan Enkripsi Teks

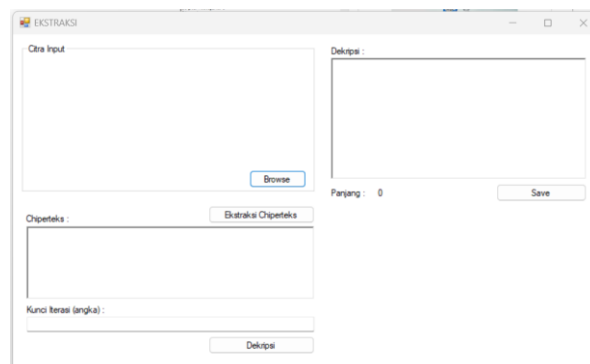
Setelah proses enkripsi data teks selesai dilakukan, langkah selanjutnya adalah melakukan proses steganografi. Untuk proses ini user terlebih dahulu memilih citra yang akan digunakan untuk menjadi citra penampung informasi. Disarankan ukuran gambar minimal 4 sampai 5 kali lebih besar dibandingkan dengan ukuran teks untuk memastikan data yang diinputkan tidak akan memberikan efek yang *visible* terhadap citra penampung. Untuk lebih jelasnya dapat dilihat pada gambar berikut:



Gambar 15. Halaman Stegano Penyisipan Data Kedalam Citra

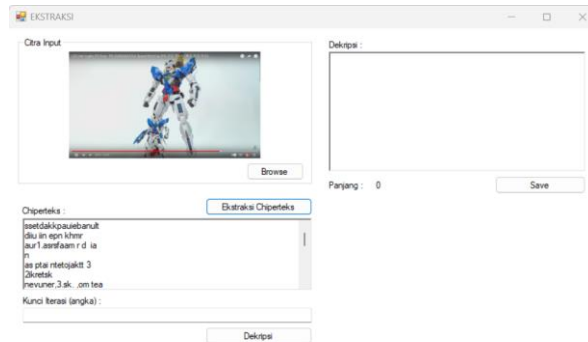
3. Halaman Ekstraksi Pesan

Setelah proses stegano selesai dilakukan, langkah selanjutnya adalah proses ekstraksi pesan teks yang ada didalam citra stegano. Adapun tampilan dari halaman ekstraksi dapat dilihat pada gambar berikut :



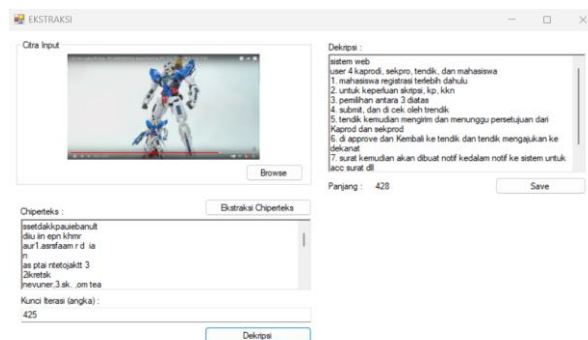
Gambar 16. Halaman Ekstraksi

Pada selanjutnya setelah membuka halaman ekstraksi, pengguna akan menginputkan citra stegano yang sudah berisi pesan rahasia yang sebelumnya sudah disisipkan kedalam citra. Dalam proses ekstraksi pesan, apa bila berhasil akan menampilkan pesan yang terenkripsi. Untuk lebih jelasnya dapat dilihat pada gambar berikut:



Gambar 17. Halaman Ekstraksi Proses Ekstraksi Pesan Rahasia

Setelah proses ekstraksi pesan rahasia selesai dilakukan, maka langkah selanjutnya adalah mengembalikan posisi data teks atau pesan rahasia yang sebelumnya tidak bisa dibaca (chiperteks) menjadi data atau pesan rahasia yang bisa dibaca (Plainteks). Proses enkripsi mengharuskan pengguna untuk menggunakan kunci yang sama pada saat proses pengacakan data atau pesan rahasia pada saat proses steganografi untuk pengujian ini kunci yang digunakan adalah 425 untuk lebih jelasnya dapat dilihat pada gambar berikut :



Gambar 18. Halaman Ekstraksi Dekripsi Pesan Rahasia

Pengujian Sistem

Pengujian yang dilakukan pada aplikasi ini adalah dengan menggunakan teknik *black box*, teknik *black box* ini merupakan teknik pengujian yang berfokus pada keluaran hasil dari respon, atau secara simpel untuk mengetahui apakah ada *error* atau ada fungsi yang tidak berjalan sesuai dengan harapan. Tujuan dari pengujian ini adalah untuk menjamin bahwa perangkat lunak yang dibangun memiliki kualitas yang handal, yaitu mampu mempresentasikan kajian pokok dari spesifikasi analisis, perancangan dan pengkodean dari perangkat lunak itu sendiri. Berikut tabel pengujian *black box*.

Tabel 1. Hasil Pengujian

No	Skenario Pengujian	Harapan	Hasil
1.	Klik tombol Steganografi	Akan Masuk ke menú Stegano	Sesuai dengan yang diharapkan
2.	Klik Menu Ekstraksi	Menampilkan halaman Ekstraksi	Sesuai dengan yang diharapkan
3.	Klik Menu Browse File Teks	Menampilkan direktori untuk load data teks	Sesuai dengan yang diharapkan
4.	Klik Menu Enkripsi	Memulai proses enkripsi	Sesuai dengan yang diharapkan
5.	Klik Menu Memulai Stegano	Memulai Proses Steganografi	Sesuai dengan yang diharapkan
6.	Klik Tombol Browse	Menampilkan Directory untuk load citra	Sesuai dengan yang diharapkan
7.	Klik Tombol Save	Akan menampilkan direktori tempat menyimpan data	Sesuai dengan yang diharapkan
8.	Klik Tombol Browse	Menampilkan direktori citra stegano	Sesuai dengan yang diharapkan
9.	Klik Ekstraksi Chiperteks	Akan melakukan proses ekstraksi teks	Sesuai dengan yang diharapkan
10.	Klik tombol Dekripsi	Memulai Proses Dekripsi	Sesuai dengan yang diharapkan
11.	Klik Tombol Save	Menyimpan Teks hasil dekripsi	Sesuai dengan yang diharapkan

Pengujian aplikasi yang mengintegrasikan teknik steganografi dan dekripsi data menunjukkan bahwa seluruh fitur berfungsi sesuai harapan. Navigasi antar menu seperti “Steganografi” dan “Ekstraksi” berjalan lancar, menandakan sistem responsif dan user-friendly. Proses pemilihan file teks, enkripsi, serta penyisipan data ke dalam citra melalui tombol “Mulai Stegano” dan “Save” juga bekerja dengan baik. Pada tahap ekstraksi dan dekripsi, aplikasi mampu menampilkan direktori, mengekstrak teks terenkripsi, mendekripsinya, dan menyimpan hasil dengan sempurna. Secara keseluruhan, tidak ditemukan kesalahan fungsi, sehingga aplikasi dinyatakan stabil, mudah digunakan, dan siap diimplementasikan.

4. KESIMPULAN

Berdasarkan proses perancangan Aplikasi Penerapan Chaos *Teori Arnold Cat Map* Pada Steganografi Pvd Untuk *Data Security*, maka dapat diambil beberapa kesimpulan yaitu:

1. Integrasi Arnold Cat Map dalam Steganografi PVD: Teori chaos, terutama Arnold Cat Map, dapat diintegrasikan dengan metode steganografi PVD untuk meningkatkan keamanan data yang disembunyikan dalam citra digital. Arnold Cat Map digunakan untuk mengacak posisi piksel gambar, sehingga pola distribusi data yang tersembunyi menjadi lebih sulit dideteksi oleh pihak yang tidak berwenang.

Hal ini menambah tingkat kompleksitas dalam penguraian data oleh pihak ketiga, meningkatkan keamanan dan ketahanan data yang disisipkan.

2. Tantangan dalam Penggabungan Teori Chaos dan Steganografi PVD: Penggabungan Arnold Cat Map dengan steganografi PVD menghadapi beberapa tantangan, termasuk penurunan kualitas gambar yang disebabkan oleh proses pengacakan serta potensi peningkatan waktu komputasi. Tantangan ini dapat diatasi dengan optimasi algoritma pengacakan dan penggunaan metode kompresi yang tepat untuk menjaga kualitas visual gambar sembari tetap mempertahankan tingkat keamanan yang tinggi.
3. Efisiensi dan Keamanan Algoritma yang Diusulkan: Algoritma yang diusulkan menunjukkan kemampuan untuk memanfaatkan sifat kekacauan dari Arnold Cat Map dalam menyembunyikan informasi secara efisien dan aman dalam gambar. Algoritma ini berhasil menjaga keseimbangan antara keamanan data, kualitas gambar, dan efisiensi proses penyembunyian data. Hasil pengujian menunjukkan bahwa algoritma ini efektif dalam menyembunyikan data dengan tingkat deteksi yang rendah oleh pihak ketiga, sekaligus meminimalkan kerusakan pada gambar asli.

Secara keseluruhan, penelitian ini menyimpulkan bahwa penggabungan teori chaos dengan metode steganografi PVD memberikan pendekatan yang kuat dalam peningkatan keamanan data digital. Hasil yang diperoleh dapat menjadi dasar untuk pengembangan lebih lanjut dalam aplikasi keamanan data pada media digital.

DAFTAR PUSTAKA

- [1] Y. Firdaus and I. M. Suartana, "Implementasi Steganografi Dengan Metode Pixel Value Differencing (PVD) pada Gambar JPG dan PNG," *J. Informatics Comput. Sci.*, vol. 1, no. 03, pp. 157–164, 2020, doi: 10.26740/jinacs.v1n03.p157-164.
- [2] R. I. Adam, M. Garho, and M. Roba'i, "Interpolasi Dalam Proses Penyisipan Pesan Dengan Metode Pixel Value Differencing (Pvd)," *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 2, p. 148, 2022, doi: 10.26798/jiko.v6i2.275.
- [3] S. M. Hameed, Z. H. Ali, G. K. AL-Khafaji, and S. Ahmed, "Chaos-based Color Image Steganography Method Using 3 D Cat Map," *Iraqi J. Sci.*, vol. 62, no. 9, pp. 3220–3227, 2021, doi: 10.24996/ijcs.2021.62.9.34.
- [4] B. A. Wijaksono, "Steganografi Pada Citra Digital Dengan Metode Catmap Dan Outguess," *J. String*, vol. 1, no. 3, pp. 167–186, 2017.
- [5] Iqbal, Kusri, and A. Nasiri, "Komparasi Hasil Enkripsi Arnold Cat Map Dan Logistic MAP pada Citra Digital," *Univ. Cokroaminoto Palopo Fak. Tek. Komput.*, vol. Vol 10 No, no. 10, 2020.
- [6] T. A. S. Yusri and D. Rudhistiar, "Enkripsi Citra Digital Berbasis Kombinasi Arnold Cat Map Termodifikasi Dan DNA Encoding," *J. Mnemon.*, vol. 5, no. 2, pp. 173–177, 2022, doi: 10.36040/mnemonic.v5i2.4901.
- [7] M. Hamdani and N. Listiyani, "Implementasi Metode Arnold's Cat Map dan Logistic Map Pada Proses Enkripsi-Dekripsi Untuk Keamanan Pengiriman Citra," *Sainstech J. Penelit. Dan Pengkaj. Sains Dan Teknol.*, vol. 29, no. 1, pp. 15–24, 2019, doi: 10.37277/stch.v29i1.312.

-
- [8] A. Saini and S. Dua, "Image Encryption Algorithm Based On Arnold Cat Map And Logistic Mapping," *i-manager's J. Pattern Recognit.*, vol. 1, pp. 1–4, May 2014, doi: 10.26634/jpr.1.1.2819.
 - [9] S. S. N. Bhuiyan, N. A. Malek, O. O. Khalifa, and F. D. A. Rahman, "An improved image steganography algorithm based on PVD," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 10, no. 2, pp. 569–577, 2018, doi: 10.11591/ijeecs.v10.i2.pp569-577.
 - [10] Q. Li *et al.*, "A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks," *IEEE Access*, vol. 8, pp. 168166–168176, 2020, doi: 10.1109/ACCESS.2020.3021103.
 - [11] N. A. Setiyanto, E. H. Rachmawanto, and D. R. I. M. Setiadi, "Pengacakan Citra Digital Berwarna Dengan Kriptografi Arnold Cat Map (Acm)," *Pros. Sains Nas. dan Teknol.*, vol. 1, no. 1, 2018, doi: 10.36499/psnst.v1i1.2410.
 - [12] N. H. Masruri, Kusriani, and A. Sunyoto, "Meningkatkan Keamanan Pesan Menggunakan Enkripsi Arnold Cat Map Dan Steganografi Pixel Value Differencing," *Semnas Inotek*, vol. 3, no. 1, pp. 113–118, 2021.
 - [13] A. Gustiawan, J. Wahyudi, and E. Suryana, "Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode Pixel Value Differencing," *JUKI J. Komput. dan Informatika*, vol. 5, pp. 151–163, 2023.
 - [14] P. A. Surya, "Penyisipan Pesan Pada File Dokumen PDF Dengan Metode Pixel Value Differencing," *Bull. Inf. Syst. Res.*, vol. 1, no. 3, pp. 92–98, 2023, doi: 10.62866/bios.v1i3.27.
 - [15] Y. P. N. Zalukhu, F. T. Waruwu, and H. K. Siburian, "Penyisipan Pesan Terenkripsi Affine Cipher Pada Citra Digital Dengan Menggunakan Metode Pixel Value Differencing," *KETIK J. Inform.*, vol. 1, no. 04, pp. 22–33, 2024, doi: 10.70404/ketik.v1i04.60.