KETIK : Jurnal Informatika
ISSN: 3026-183X (Media Online)
Vol. 01, No. 04, Maret 2024 Hal. 22-33
DOI: 10.70404/ketik.v1i04.60
Faatuatua Media Karya
https://jurnal.faatuatua.com/index.php/KETIK

Penyisipan Pesan Terenkripsi Affine Chiper Pada Citra Digital Dengan Menggunakan Metode Pixel Value Differencing

Yep Prie Nofita Zalukhu[1*], Fince Tinus Waruwu[2], Henry Kristian Siburian[3]

[1]Universitas Budi Darma, Indonesia, email: yeprienzalukhu@gmail.com*
[2]Universitas Budi Darma, Indonesia
[3]Universitas Budi Darma, Indonesia
**coressponding author)*

Info Artikel

Diajukan: *26 Maret 2024*
Diterima: *27 Maret 2024*
Diterbitkan: *30 Maret 2024*

Kata Kunci:
Kriptografi;
Affine Cipher;
Citra Digital;
Penyisipan;
Pixel Value Differencing;
Keamanan Data.

Keywords:
Cryptography;
Affine Cipher;
Digital Image;
Insertion;
Pixel Value Differencing;
Data Security.

Abstrak

Sistem informasi dan komunikasi saat ini pemanfaatan dan perkembangnnya sangat cepat. Seperti pada aktivitas pengiriman pesan secara digital yang cukup memudahkan pengguna, dampak dari perkembangan teknologi ini sangat memudahkan kejahatan menyerang komputer dan internet, karena kemajuan atau kejahatan akan selalu beriringan berkembang. Sehingga diperlukan beberapa metode pengamanan data agar tidak mudah diketahui oleh orang yang tidak berkepentingan. Algoritma affine chiper merupakan salah satu bentuk metode pengamanan enkripsi yang dikembangkan dari algoritma caesar chiper dimana cara melakukan enkripsi dan dekripsi hampir sama dengan caesar cipher hanya saja digunakakn formula plaintext dan chipertext. Berdasarkan penelitian terdahulu mengatakan bahwa affine chiper untuk meningkatkan keamanan pesan asli yang di acak sedemikian rupa sehingga menjadi pesan sesuatu yang sulit dimengerti oleh orang lain. Penelitian ini menjelaskan bagaimana metode kriptografi dapat dikombinasikan dengan steganography untuk mengoptimalkan keamanan pesan. Algoritma affine chipper digunakan untuk mengenkripsikan dan deskripsi pesan yang akan disembunyikan saat menggunaan metode pixel value differencing (PDV) menyembunyikan pesan rahasia yang telah terenkripsi pada bentuk citra digital. Proses penyisipan data terenkripsi ke dalam citra digital dapat dilakukan. Menerapkan metode Pixel Value Differencing untuk menyisipkan pesan terenkripsi pada citra digital meberikan nilai dimana sesorang tidak mencurigai gambar tersebut adalah sebuah data yang mengandung sebuah data rahasia.

Abstract

Information and communication systems are currently utilizing and developing very quickly. As in the activity of sending messages digitally which is quite easy for users, the impact of this technological development makes it very easy for crime to attack computers and the internet, because progress or crime will always go hand in hand with development. So that several data security methods are needed so that they are not easily known by unauthorized people. The affine chiper algorithm is one form of encryption security method developed from the caesar chiper algorithm where the way to encrypt and decrypt is almost the same as the caesar cipher only that the plaintext and chipertext formulas are used. Based on previous research, affine chiper is used to increase the security of the original message that is randomized in such a way that it becomes a message that is difficult for others to understand. This research explains how cryptographic methods can be combined with steganography to optimize message security. The affine chipper algorithm is used to encrypt and describe the message to be hidden while using the pixel value differencing (PDV) method to hide the encrypted secret message in the form of a digital image. The process of inserting encrypted data into a digital image can be done. Applying the Pixel Value Differencing method to insert an encrypted message in a digital image provides a value where someone does not suspect the image is a data containing a secret data.

1. PENDAHULUAN

Sistem informasi dan komunikasi saat ini sudah sangat cepat bahkan pengiriman pesan. Dampak dari perkembangan teknologi ini adalah rentan rerhadap serangan komputer dan internet, karena kemajuan atau kejahatan juga semakin meningkat dibidang informasi teknologi. Namun masalah keamanan pesan tidak menjadi fokus terutama pada pesan, sehingga sangat penting untuk mencegah agar tidak jatuh ketangan orang yang tidak bertanggung jawab. Pesan rahasia penting ini adalah sesuatu yang perlu dipertimbangkan ketika berbagi informasi di media, dengan pesan-pesan yang tidak menyadari bahwa pesan rahasia dapat disalahgunakan oleh mereka yang tidak memiliki hak untuk mengaksesnya, dengan tujuan untuk merugikan individu tertentu. Teknik sederhana untuk mengamankan pesan adalah dengan algortima menggunakan algoritma kriptografi. Algoritma kriptografi dapat mengamankan data dengan cara menyandikan data kedalam bentuk yang tidak dapat dipahami. Berdasarkan penelitian terdahulu, mengatakan bahwa kriptografi adalah seni dan ilmu untuk mengamankan tranmisi data dengan mengubahnya menjadi kode rahasia[1].

Algortima Affine cipher merupakan salah satu bentuk dari Caesar Cipher yang cara enkripsi dan dekripsinya hampir sama dengan Caesar Cipher hanya saja menggunakan rumus plaintext dan chiphertext. Sebelumnya Affine Chiper merupakan deskripsi dari Caesar Cipher menduplikasikan teks biasa dengan suatu nilai dan menambahkannya dengan offset. Berdasarkan penelitian sebelumnya, telah dikemukakan bahwa affine cipher bertujuan untuk meningkatkan keamanan pesan terenkripsi asli sedemikian rupa sehingga tidak dapat dipahami oleh orang lain. [2].

Algoritma kriptografi masih belum dikatakan melindungi dan menjaga pesan dengan baik. Namun ada beberapa algoritma yang dapat dipecahkan

oleh penyerang untuk mengetahui isi pesan tersebut. Kriptografi klasik pada umumnya mengunakan huruf dalam berbagai kombinasi berbeda biasanya digunakan secara bersamaan dengan menggunakan kunci yang telah ditentukan sebelumnya. Berdasarkan penelitian sebelumnya kriptografi klasik merupakan suatu teknik pengamanan data dengan proses yang sederhana sehingga tidak dapat dibaca oleh orang yang tidak berhak walaupun melihat kode sumbernya[3].

Teknik lain yang dapat digunakan untuk mengamankan data selain teknik kriptografi adalah teknik steganography. Teknik steganography merupakan seni dan teknik yang akan digunakan untuk menyisipkan pesan kedalam sebuah media. Teknik stganography dapat mencegah orang untuk mencurigai informasi tersembunyi. Berdasarkan penelitian terdahulu steganography adalah pesan rahasia yang disembunyikan dalam bentuk teks, pesan rahasia yang tidak ada satupun yang mengenal pesan rahasia tersebut[4].

Salah satu metode steganography adalah metode Pixel Value Diffencing (PDV). Metode Pixel Value Differencing adalah teknik untuk menyisipkan informasi dengan memodifikasi selisih nilai pixel dengan bit pesan dan tabel kuantitas selisih nilai keabuan. Berdasarkan penelitian sebelumnya metode Pixel Value Differencing (PDV) ini adalah penyembunyian pesan pada citra digital dapat dihasilkan lebih kecil dari ukuran aslinya mempunyai kualitas yang baik sehingga tidak menimbulkan kecurigaan[5].

Berdasarkan uraian latar belakang diatas, maka penelitian ini menjelaskan bagaimana metode kriptografi dapat dikombinasikan dengan steganography untuk mengoptimalkan keamanan pesan. Algoritma Affine Chiper digunakan untuk mengenkripsikan dan deskripsi pesan yang akan disembunyikan saat menggunakan metode Pixel Value Differencing (PDV).

2. METODE PENELITIAN

2.1 Kerangka Kerja Penelitian

Kerangka kerja penelitian ini merupakan stuktur kerja yang diimplementasikan melalui penelitian, oleh karena itu diperlukan adanya susunan kerangka kerja (framework) yang jelas tahapan-tahapannya.

Gambar 1. Kerangka Kerja Penelitian

Berdasarkan kerangka kerja penelitian yang telah digambarkan diatas, maka dapat di uraikan pembahasan setiap langkah-langkah dalam penelitian adalah sebagai berikut:

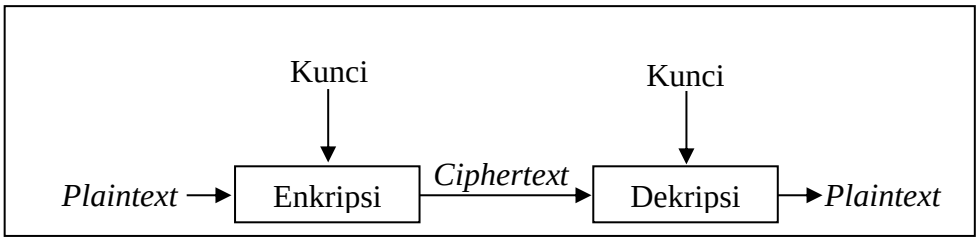
1. Identikasi Masalah
   Langkah pertama adalah mengidentifikasi atau memahami permasalahan mengenai pengamanan pesan yang kurang optimal karena banyaknya pihak-pihak yang menyalah gunakan pesan teks yang dengan tujuan negatif sehingga merugikan pihak-pihak tertentu.

2. Studi Literatur
   Studi literatur merupakan kegiatan yang melibatkan pengumpulan data atau pengelolaan bahan penelitian yang menjadi landasan pengujian dan analisis penelitian. Dalam kajian pustaka ini beberapa jurnal, skripsi serta artikel yang berhubungan dengan keamanan data, kriptografi, steganografi dan khususnya yang berhubungan dengan metode-metode dalam *Affine Chiper* dan metode *Pixel Value Differrencing* sebagai referensi dalam penelitian.
3. Analisa Masalah
   analisa masalah merupakan tahap berikutnya yang akan dilakukan setelah penelitian berhasil melakukan identifikasi serta mendapatkan literatur yang akan terkait dengan penelitian. Analisa masalah yang akan dilakukan adalah menganalisa terhadap kurangnnya keamanan pesan yang diamankan serta bagaimana solusi untuk menyelesaikan masalah tersebut.
4. Penerapan Metode
   Penerapan metode dilakukan untuk mengimplementasikan uraian permasalahan yang mengkombinasikan metode *Affie Cipher* dan Metode *Pixel Value Differencing* supaya kamanan pesan menjadi lebih optimal. Adapun tahapan penerapan metode yang diterapkan, yaitu:
   a. Enkripsi
      Enkripsi merupakan proses penyadian data menjadi plaintext. Metode yang digunakan untunk melakukan enkripsi adalah *Affine Chiper*. Penerapan metode ini dilakukan untuk melakukan mengamankan pesan asli kedalam bentuk yang tidak dimengerti (*ciphertext*).
   b. *Embedding* (penyembunyian *ciphertext*)
      Embedding merupakan proses penyisipan pesan biner terenkripsi (ciphertext) pada *cover* yang digunakan. *Ciphertex* yanng digunakan dari hasil enkripsi yaitu metode Affine cipher yang akan disembunyikan kedalam bentuk citra digital dengan menggunakan metode *Pixel Value Differencing.*
   c. Ekstrasi (Pengambil Pesan dan kedalam citra)
      Penerapan metode selanjutnya adalah ekstraksi, pesan yang berhasil disembunyikan kedalam bentuk citra digital diambil kembali dalam bentuk asli dengan metode *Pixel Value Differencing*
   d. Dekripsi
      Dekripsi merupakan proses mengubah cipher text menjadi plaintext yang sudah di pisahkan dari citra stegano kedalam bentuk pesan aslinya.
5. Perancangan sistem
   Perancangan sistem merupakan sebuah proses penting dalam membangun suatu aplikasi adanya perancangan sistem maka, dapat diketahui bagaimana sebuah sistem melakukan tugasnya. Pereancangan sistem dalam penelitian ini, dilakukan dengan mengunakan *Use Case Diagram* and *Activity* (UML).
6. Pengujian
   Pengujian yaitu proses yang akan dilakukan untuk menilai apakah sistem yang dibuat telah sesuai dengan apa yang diharapkan. Tahap pengujian ini ialah pengujian terhadap tingkat perbedaan citra asli dengan citra *stegano* yang dievaluasikan setelah *embedding.* Setelah sistem dibangun berdasarkan yang dirancang oleh peneliti, maka penelitian melakukan pengujian mengevaluasikan keunggulan dan kelemahan yang telah dibangun dari sistem untuk mengamankan pesan apakah sesuai yang diharapkan oleh peneliti.
7. Implementasi
   Tahap penerapan sekaligus pengujian bagi sistem baru serta merupakan tahap dimana aplikasi siap dioperasikan pada keadaan yang sebenarnya, efektifitas sistem baru akan diketahui secara pasti, juga untuk semua kelebihan dan kekurangan sistem dan aplikasi program.
8. Dokumentasi/laporan
   Tahap terakhir yaitu dokumentasi/laporan, dimana pada tahap penelitian ini membuat laporan mengenai hasil penelitian. Laporan yang akan dibuat adalah berdasarkan proses pengerjaan penelitian, sehingga dalam laporan nantinya didapatkan kesimpulan apakah kombinasi metode *Pixel Value Differencing* layak memberikan peningkatan untuk keamanan pesan menjadi lebih optimal serta sistem dapar dipergunakan.

2.2 Kriptografi

Kriptografi merupakan proses atau ilmu pengamanan data dengan cara mengenkripsi sedemikian rupa sehingga tidak dapat dengan mudah dipahami oleh orang yang tidak bertanggung jawab. Teknik pemengamanan data kriptografi memiliki dua proses yaitu dengan melakukan enkripsi dan dekripsi serta dikenal dengan istilah plaintext (data yang akan disandikan) dan ciphertext (teks sandi). Proses

enkripsi adalah proses penyadian data, sedangkan dekripsi ialah kebalikannya, yaitu proses yang membaca data ialah dalam bentuk seperti berikut[7].



Gambar 2. Bagan proses enkripsi dan dekripsi

Berdasarkan penelitian terdahulu kriptografi ialah teknik matematika penyembunyian pesan dengan mengamankan informasi kadalam bentuk data yang bersifat rahasia lebih tepat menyediakan keamanan informasi[2]

2.3 Affine Chiper

Affine Chiper adalah teknik enkripsi yang dikelompokan sebagai teknik enkripsi klasik. Algoritma ini merupakan perkembangan dari Caesar cipher[2]. Proses melakukan enkripsi dengan menggunakan persamaan(1) dan dekripsi menggunakan persamaan (2). Dengan melakukan proses rumus sebagai berikut:

$C = (m.P + b)\ mod\ n$ ..... (1)

$P = (m^{-1}.(C - b)\ mod\ n$ ..... (2)

Keterangan :
P = karakter relatif primer terhadap n, serta m dan b berada pada antara satu sampai dengan *n*.
n = karakter yang dapat diakomodasi

Pada Affine Chiper memerlukan kunci yaitu *m* dan *b*, agar hasil enkripsi dapat didenkripsi harus diperlukan m^{-1} merupakan nilai invers dari m. Pada kedua kunci yang berpasangan memiliki satu faktor persekutuan yaitu satu, nilai m^{-1} dapat dihitung menggunakan fungsi kongruen pada persamaan(3), maka nilai m^{-1} yaitu 55. Dengan menggunakan rumus sebagai berikut:

(m^{-1}x m) mod 128 = 1 ..... (3)

Untuk melihat perubahan hasil enkripsi dibandingkan dengan teks asli dapat diuji dengan menggunakan *Mean Absolute Error (MAE)*. *Mean Absolute Error* merupakan mempresentasikan rata-rata kesalahan antara hasil enkripsi atau hasil dekripsi terhadap teks asli. Nilai ini dihitung dengan menggunakan persamaan(4) dengan menggunakan rumus sebagai berikut:

$MAE = \frac{1}{n} \sum_{i=1}^{n} |f_i - y_i|$ ..... (4)

f_i adalah nilai hasil enkripsi dan dekripsi
y_i adalah nilai karakter teks asli
n adalah jumlah seluruh karakter teks.

2.4 Steganografi

Steganografi adalah teknik menyembunyikan informasi dengan cara lain untuk menghindari kecuriagaan pencurian data atas informasi yang sudah disembnyikan. Secara umum steganografi digunakan secara bersamaan dengan dua media yang berbeda, yaitu media informasi (Media File) dan media informasi (Media Rahasia). Dalam steganografi terdapat dua teknik pengolahan untuk menyembunykan data informasi yaitu *(embedding)* dan penguraian *(extraction)*. Penyisipan pesan adalah proses menyisipkan pesan informasi kedalam media cover seperti gambar, vidio, dan media lainnya. Sedangkan proses penguraian yaitu menguraikan pesan pada media cover[9]. Tujuan dari steganografi adalah untuk mencooba mengamankan pesan dengan menyembunyikan di suatu media. Media tersebut akan digunakan sebagai penutup untuk menyisipkan pesan kedalam bentuk berupa gambar digital, vidio, suara dan media lainnya. Berdasarkan penelitian sebelumnya dikatakan bahwa jika media yang akan disisipkan sebagai data atau pesan rahasia terlihat mencurigakan maka tujuan dari teknik penyembunyian tersebut tidak akan tercapai[8].

2.5 Metode Pixel Value Differencing (PVD)

Metode *Pixel Value Differencing (PVD)* merupakan teknik steganografi yang digunakan untuk menyembunyikan data pada gambar digital. Dalam metode PVD data yang diubah menjadi urutan bit kemudian disisipkan kedalam piksel gambar digital, melakukan perubahan memanipulasi nilai-nilai piksel secara imperseptibel sehingga perubahan tidak dapat diketahui oleh manusia[11]. Langkah-langkah proses kerja pada Pixel Value Differencing sebagai berikut:

1. Proses penyisipan pesan dengan metode *Pixel Value Differencing*
   a. Ubah pesan menjadi bilangan biner 8 *bit.*
   b. Hitung selisih 2 nilai *pixel* bertetangga($g_{i,}g_{i+1}$) :
   $d_{i,} = g_{i+1-g_i}$.....(5)
   c. Tentukan batas bawah (1_k) dan jumlah bit *n,* dengan cara : $1_k \leq d_i < 1_{k+1}$.
   d. Ambil pesan sebanyak n bit, kemudian ubah menjadi desimal.
   e. Hitung selisihn ilai baru d'=
   $$\begin{cases} lk + b, d \geq 0 \\ -(lk + b), d < 0 \end{cases}$$.....(6)
   f. Hitung : m=d'-d
   g. Hitung nilai *pixel* baru:

$$f(g_i,\ g_{i+1}) = \begin{cases} (g^i - \left\lceil \frac{m}{2} \right\rceil, g^i + 1 + \left\lceil \frac{m}{2} \right\rceil, m = ganjil \\ (g^i - \left\lfloor \frac{m}{2} \right\rfloor, g^i + 1 + \left\lfloor \frac{m}{2} \right\rfloor, m = genap \end{cases} \quad \text{.....(7)}$$

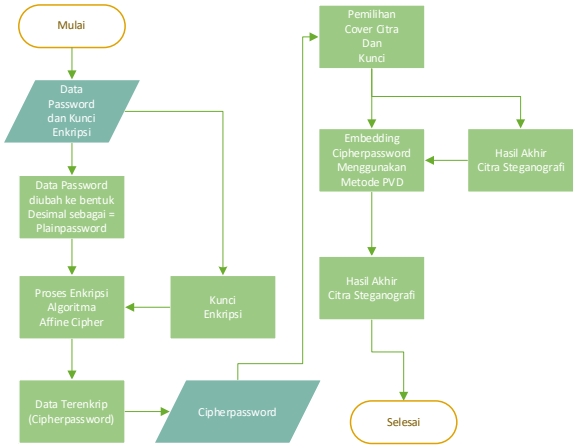
   Keterangan:
   Tanda [ ] adalah pembulatan ke atas
   Tanda [ ] adalah pembulatan ke bawah

2. Proses *ekstration* pesan dengan metode *Pixel Value Differencing*
   a. Hitung selisih 2 *Pixel* bertetangga ($g_{i,}g_{i+1}$)
   b. Tentukan batas bawah (1_k) dan jumlah *bit n,* dengan cara : $1_k \leq d_i < 1_{k+1.}$
   c. Hitung b $|d|$ -1_k
   d. Ubah *b* (desimal) menjadi biner n dengan terakhir adalah ambil pesan = n *bit*.

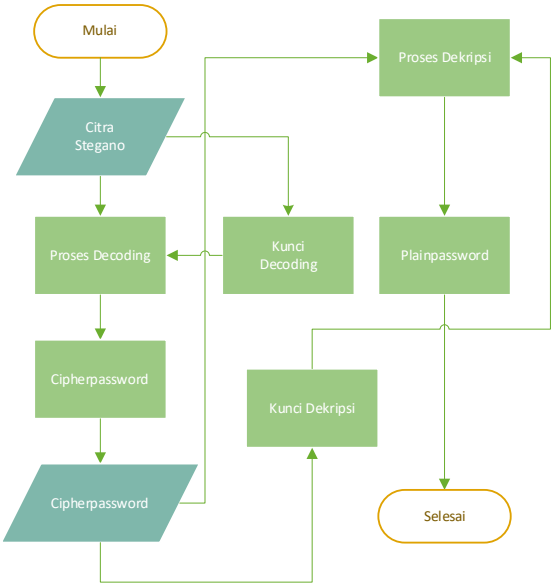
3. HASIL DAN ANALISIS

3.1 Analisis

Terdapat dua proses didalam steganografi yaitu proses *embedding* untuk menyisipkan pesan kedalam *cover-object* dan proses *decoding* untuk ekstraksi pesan dari *stego-object*. Demikian juga dengan kriptografi yaitu proses enkripsi untuk menyandikan pesan dan proses dekripsi untuk mengembalikan pesan ke data asli. Maka proses inilah yang digunakan penulis dalam penelitian yang berjudul "Peyisipan Pesan Terenkripsi Affine Cipher Pada Citra Digital Dengan Menggunakan Metode Pixel Value Differencing" Berikut konsep kerja penggunaan algoritma penyandian dan penyisipan dalam penelitian ini.



Gambar 3. Proses Encryption dan Embedding



Gambar 4. Proses Decoding dan Decryption

Analisis Penerapan Affine Cipher dan Pixel Value Differencing

Adapun pesan teks yang akan digunakan dalam bentuk tes yaitu "putri_256" atau 8 *bytes* (8x8 bit = 64 bit). Citra yang akan digunakan sebagai media penyembunyian untuk dijadikan data sampel yaitu *grayscale* dengan ekstensi jpeg, kedalam *bit* adalah 24 *bit* dan resolusi 1123 x 898 *pixel.* Namun pada pengerjaan contoh kasus nantinya, kebutuhan *pixel* untuk penyembunyian *bit* pesan akan disesuaikan dengan jumlah *bit cipher* yang akan disembunyikan yaitu 64 *bit cipher*.

1. Proses *Encryption* dan *Embedding*
   Proses *encryption* penulis menggunakan algoritma affine cipher dengan rumus:
   $C = (m.P + b)\ mod\ n$
   Penggunaan kunci terhadap proses enkripsi algoritma affine cipher penulis menggunakan angka m = 5 dan b = 2 karena bilangan ini merupak bilangan relatif prima atau saling prima.
   Diketahui:
   Plaintext = Plainpassword = putri_26
   Kunci Proses *encryption*: m = 5, b = 2

Proses Enkripsi:
Pertama *plainpassword* diubah ke nilai desimal sebagai berikut:

Tabel 1. Konversi karakter ke nilai desimal

Karakter	p	u	t	r	i	2	5	6
Desimal	112	117	116	114	105	50	53	54

Maka dari hasil proses enkripsi di atas, berikut nilai *cipherpassword* yang dihasilkan.

Tabel 2. Nilai Cipherpassword

Desimal	209	254	255	239	18	20	55	55
Cipherpassword	Ñ	Þ	ÿ	ï	□	□	7	7

Setelah proses enkripsi affine cipher dilakukan selanjutnya yaitu melakukan proses *embedding* terhadap *cipherpassword* ke citra *stegano* dengan algoritma *Pixel Value Differencing*. Langkah pertama penulis melakukan ekstrasi nilai hexadecimal pada citra sampel *grayscale* yang sudah tetapkan penulis, dengan menggunakan aplikasi matlab, berikut tampilan nilai *hexadecimal* piksel citra *cover*.

Tabel 3. Nilai *pixel* dari citra digital *grayscale* dengan ukuran 8 x 8.

42	43	48	54	56	58	64	72
45	46	49	53	54	55	60	67
49	48	50	53	53	52	56	61
51	49	49	53	54	53	56	60
50	48	49	53	56	57	59	63
50	47	47	53	58	59	61	64
51	47	46	52	57	59	60	61
52	47	45	50	56	57	57	58

Tabel di atas dikonvesikan kebilangan desimal

Tabel 4. Nilai Desimal Cover 6x5

66	67	72	84	86
69	70	73	83	84
73	72	80	83	83
81	73	73	83	84
80	72	73	83	86
80	71	71	83	88

Pesan *cipherpassword* pada tabel 2 menjadi objek utama yang disisipkan kedalam citra cover dengan nilai desimal yang ada pada tabel 4 dengan menggunakan *Pixel Value Differencing*. Berikut proses penerapannya:

1. Merubah nilai desimal *cipherpassword* pada tabel 2 ke bilangan biner.

Tabel 5. Nilai ASCII desimal dari *ciphertex* dan *key*

Ciphertext	Nilai	*Key*	Nilai
Ñ	209	A	65
þ	254	s	115
ÿ	255	s	115
ï	239	a	97
□	18	s	115
□	20	s	115
7	55	i	105
7	55	n	110

2. Proses penyisipan dengan *Pixel Value Differencing*
   Mengikuti ketentuan sebagai berikut,

Tabel 6. Nilai rentang keabuan

Kuantisasi ke-k	Batas Bawah – Batas Atas $l_k - u_k$	Rentang Nilai	Jumlah Bit n
1	0-7	8	3
2	8-15	8	3
3	16-31	16	4
4	32-63	32	5
5	64-127	64	6
6	128-255	128	7

a. Jika hasil d = minus, maka penetapan nilai keabuan tetap dianggap positif.
b. Jika m = ganjil, maka nilai batas atas diambil dari nilai yang terbesar, batas bawah diambil dari nilai terkecil.
c. Jika m = genap, maka nilai batas atas dan batas bawah tetap sama.
d. Jika nilai *d* lebih kecil dari 0 (nol) maka $d' = -(l_k + b)$
e. Jika nilai *d* lebih besar sama dengan 0 (nol) maka $d' = (l_k + b$

Proses *Embedding* terhadap biner pesan ..... (Iterasi Ke-1)
Pesan = 00111100 00001111 11111011 00101000 11011101 11111100 00010000 00011010

a. Piksel bertetangga pada *cover* stegano (lihat tabel 4.4) = 49 dan 65
b. d = 43 - 42 = 1
c. tentukan nilai rentang keabuan berdasarkan nilai "*d*" (lihat tabel 4.6) nilai kuantitas yang digunakan adalah nilai ke - 3
d. $1 \leq d \leq 31$ menjadi $1 \leq 16 \leq 31$
e. Nilai l_k = 16 dan n = 4
f. Ambil n = 4 bit dari pesan maka nilai b = 0011 = 3
g. Mencari nilai selisih $d' = l_k + b$ = 16 + 3 = 19
h. Menghitung nilai $m = d' - d$ = 19 - 16 = 3
i. karena *m* ganjil (lihat ketentuan pada nomor 2) maka nilai piksel baru sebagai berikut:

$$g_i', g_{i+1}' = g_i - \frac{m}{2}, g_{i+1} + \frac{m}{2}$$

$$g_i', g_{i+1}' = 49 - \frac{3}{2}, 65 + \frac{3}{2} = 49 - (2), 65 + (2) = \mathbf{47}\ dan\ \mathbf{67}$$

Lakukan Proses Embedding terhadap biner pesan (iterasi Ke-2 sampai iterasi Ke-4)

Proses *Embedding* terhadap biner pesan ..... (Iterasi Ke-15)

1. Pesan = 00111100000011111111101100101000110111011111110000010000 000011 010
   Keterangan : 00111100000011111111101100101000110111011111110000 1000000011→ *bilangan biner yang sudah disisipkan*
2. Piksel bertetangga pada *cover* stegano selanjutnya (lihat tabel 4.4) sama dengan = 53 dan 54
3. d = 54 - 53= 1
4. tentukan nilai rentang keabuan berdasarkan nilai "*d*" (lihat tabel 4.6) nilai kuantitas yang digunakan adalah nilai ke - 2
5. $08 \leq d \leq 15$ menjadi $08 \leq 1 \leq 15$
6. Nilai l_k = 8 dan n = 3
7. Ambil n = 3 bit dari pesan maka nilai b = 010 = 2
8. Mencari nilai selisih $d' = l_k + b$ = 8 + 3 = 11
9. $m = d' - d$ = 11 - 1 = -10
10. karena *m* genap (lihat ketentuan pada nomor 2) maka nilai piksel baru sebagai berikut:

$$g_i', g_{i+1}' = g_i - \frac{m}{2}, g_{i+1} + \frac{m}{2}$$

$$g_i', g_{i+1}' = 10 - \frac{-1}{2}, 22 + \frac{-1}{2} = 10 - (-0{,}5), 22 + (-0{,}5) = \mathbf{11}\ dan\ \mathbf{21}$$

Tabel 7. nilai *pixel* citra awal dan nilai *pixel* citra akhir setelah dilakukan penyisipan

matrikx citra *cover*

42	43	48	54	56	58	64	72
45	46	49	53	54	55	60	67
49	48	50	53	53	52	56	61
51	49	49	53	54	53	56	60
50	48	49	53	56	57	59	63
50	47	47	53	58	59	61	64
51	47	46	52	57	59	60	61
52	47	45	50	56	57	57	58

matrikx citra stegano

35	49	45	57	52	62	60	75
38	53	45	57	47	62	56	71
56	42	44	59	58	47	51	65
54	46	45	57	60	48	54	62
56	43	47	55	52	61	54	67
56	42	45	52	52	65	55	69
51	47	46	52	57	59	60	61
52	47	45	50	56	57	57	58

Berdasarkan nilai citra awal dan nilai citra akhir, maka dapat dihitung nilai MSE (*Mean Square Error*) dan PSNR (*Peak Signal-to-Noise Ratio*) untuk mengetahui berapa nilai perbandingan citra awal dan citra akhir. Berikut ini adalah penghitungan MSE dan PSNR pada penelitian ini.
Menghitung MSE (*Mean Square Error*) :

$$\text{MSE} = \frac{(42-35)^2 + (43-49)^2 + (48-45)^2 + \ldots\ldots\ldots\ldots + (58-58)^2}{8\ x\ 8}$$

MSE = $\frac{1.128}{64}$ = 17.625

Menghitung PSNR (*Peak Signal-to-Noise Ratio*) :

PSNR = 20 $log_{10}\frac{72}{\sqrt{17.625}}$ = 24,68536 atau 25 dB

Berdasarkan nilai MSE dan PSNR yang dihasilkan maka dapat disimpulkan bahwa kualitas gambar yang dihasilkan setelah dilakukan penyisipan *ciphertext* cukup baik.

3.2 Implementasi

Tampilan sistem merupakan penampilan kinerja akhir dari interface sistem aplikasi yang telah dirancang. Tampilan sistem tersebut terdapat 4 tampilan halaman yaitu Menu Utama, Form Embedding, Form Ekstrasi Dan Form MSE dan PSNR.

1. Tampilan Menu Utama
   Melalui menu utama, maka pengguna dapat memili proses yang dilakukan seperti proses enkripsi dan embedding dengan memilih form embedding, proses ekstraksi dan dekripsi dengan memilih form ekstrasi serta proses MSE dan PSNR. Semua sudah tersedia pada menu utama.

Gambar 5. Menu Utama

2. Tampilan Form Embedding
   Melalui form ini, maka pengguna dapat melakukan proses enkripsi pesan serta proses penyembunyian *(embedding) ciphertext* yang dihasilkan pada *citra cover*.

Gambar 5. *Form Embedding*

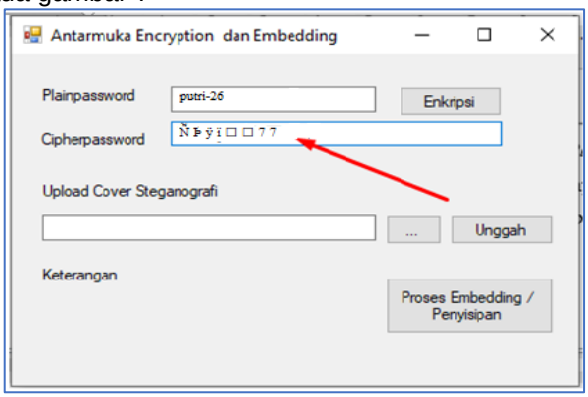
3.3 Hasil Pengujian

Tujuan pengujian sistem adalah untuk mengetahui bagaimana sistem yang dibangun bekerja. Sistem ini dirancang sesederhana mungkin agar pengguna dapat mengoperasikannya dengan mudah. Berikut ini tampilan *print out* saat sistem sedang berjalan.

Proses pengujian dilakukan terhadap form *Encryption* dan *Embedding* langkah awal pertama dilakukan proses enkripsi dengan memasukan nilai *plainpassword* kemudian dilakukan proses enkripsi dengan menekan tombol "Enkripsi" lebih jelasnya dapat dilihat pada gambar 6

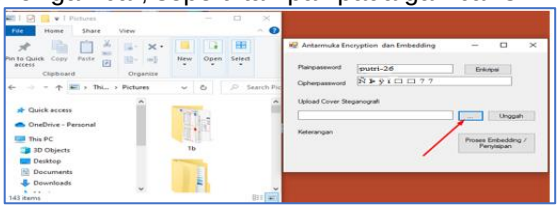
Gambar 6. Proses Enkripsi Terhadap Plainpassword

Setelah tombol "Enkripsi" ditekan maka proses penyandian terlaksana sehingga menampilkan nilai *cipherpassword* seperti pada gambar 7



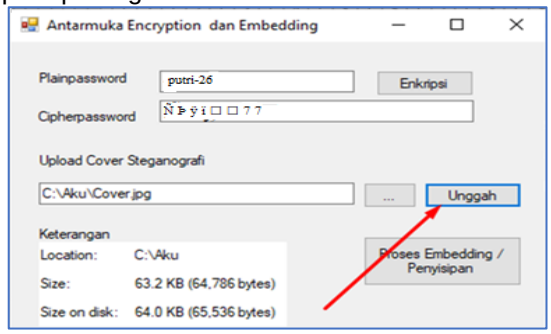
Gambar 7. Tampilan Cipherpassword Setelah Enkripsi

Setelah nilai *cipherpassword* tampil proses selanjutnya adalah melakukan proses *embedding cipherpassword* kedalam *cover* gambar, seperti tampak pada gambar 8



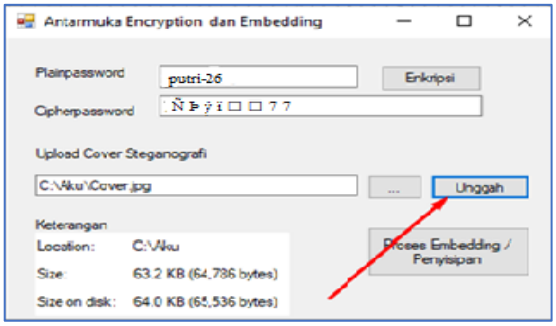
Gambar 8. Mencari Gambar di Explorer Sebagai Cover Embedding

Setelah gambar *cover embedding* ditemukan di *explorer*, maka langkah selanjutnya adalah dengan menekan tombol unggah seperti pada gambar 9



Gambar 9. Unggah Cover Embedding dari Explorer ke Form

Setelah diunggah maka tampilan form akan menampilkan deskripsi *cover* gambar yang digunakan seperti pada gambar 10



Gambar 10. Deskirpsi Cover Gambar Setelah Diungga

Tabel 8. Hasil Pengujian Enkripsi dan Deskripsi

Cover Image		plaintext	Ciphertext	Stegano Image	MSE	PSNR
1.	 *Size* : 82,4 Kb *Resolution* : 1280 x 1600	Putri-26	Ñþÿï □□77	 *Size 84,0* Kb *Resolution* : 1280 x 1600	17,84375	34 db

Pengujian terhadap gambar stegano di atas, maka disimpulkan bahwa hasil proses *enkripsi* dan dekripsi telah dilakukan dan berhasil dengan metode beaufort cipher, serta proses *embedding* dan ekstrasi telah dilakukan juga dinyatakan berhasil dengan menggunakan metode *pixel value differencing*. Maka, dengan hasil pengujian di atas tingkat kemiripan antara citra *cover* dan citra stegano dengan penyisipan pesan pada citra berdasarkan metode *Pixel Value Differencing* (PVD) menghasilkan kualitas gambar yang baik dengan ditunjukkan oleh nilai PSNR yang tinggi 34 db dan nilai *error* (MSE) antara citra stegano dengan citra asli yang sangat rendah.

4. KESIMPULAN

Setelah melakukan penelitian dengan peyisipan pesan terenkripsi affine cipher pada citra digital dengan menggunakan metode pixel value differencing menghasilkan kesimpulan sebagai berikut: Proses penyisipan data terenkripsi ke dalam citra digital dapat dilakukan. Menerapkan metode *Pixel Value Differencing* untuk menyisipkan pesan terenkripsi pada citra digital memberikan nilai dimana seseorang tidak mencurigai gambar tersebut adalah sebuah data yang mengandung sebuah data rahasia. Aplikasi enkripsi dan *embedding* dapat membantu setiap orang yang ingin menyembunyikan pesan rahasianya ke dalam sebuah gambar tanpa harus dicurigai oleh orang lain.

REFERENSI

[1] A. Amrulloh and E. I. H. Ujianto, “Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher,” *J. CoreIT*, vol. 5, no. 2, pp. 71–77, 2019.

[2] H. Februariyanti, Wahyudi, A. Susanto, and Rihartanto, “Steganografi Pesan Terenkripsi Affine Cipher Menggunakan Metoda LSB Dengan Pola Genap Ganjil,” *Proceeding SINTAK*, pp. 411–419, 2019.

[3] A. Rambe, “Modifikasi Metode Affine Ciphers Pada Kriptografi Klasik,” *Ready Star*, no. m, pp. 256–261, 2019, [Online]. Available: https://ptki.ac.id/jurnal/index.php/readystar/article/view/64

[4] S. P. Manalu, “Implementasi Penyisipan Pesan Teks Terenkripsi Dengan Algoritma Modifikasi Vigenere Cipher Pada Citra Digital Menggunakan …,” *Inf. dan Teknol. Ilm.*, vol. 7, no. 1, pp. 69–

74, 2019, [Online]. Available: http://ejurnal.stmik-budidarma.ac.id/index.php/inti/article/view/1817
[5] R. Andri, R. K. Hondro, and K. Tampubolon, "Implementasi Metode Pixel Value Differencing Untuk Penyembunyian Pesan Pada Citra Digital," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 3, no. 1, pp. 355–361, 2019, doi: 10.30865/komik.v3i1.1613.
[6] S. Wulandari, P. Studi, and T. Informatika, "Pengamanan Pesan Teks E-Mail Menggunakan Metode Algoritma Bifid Dan Feedback Cipher," vol. 6, no. 5, pp. 523–530, 2019.
[7] J. Karman, A. Nurhasan, P. Studi, S. Informasi, and U. B. Insan, "perancangan sistem keamanan data inventory barang di toko nanda berbasis web menggunakan metode kriptografi vigenere cipher," vol. 11, no. 01, pp. 29–36, 2019.
[8] A. Rachmadsyah, A. Perdana, and A. B. S. T, "Kombinasi Algoritma Beaufort Cipher Dan Vigenere Cipher Untuk Pengamanan Pesan Teks Berbasis Mobile Application," vol. 9, no. September, pp. 12–17, 2020.
[9] P. Fitriani and T. S. Alasi, "Pengamanan Pesan Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit Pada Citra Digital," *J. Inf. Komput. Log.*, vol. I, no. 2, pp. 35–38, 2019, [Online]. Available: http://ojs.logika.ac.id/index.php/jikl/article/download/34/39
[10] A. A. Fikhri and H. Hendrawaty, "Implementasi Steganografi Text To Image Menggunakan Metode One Bit Least Significant Bit Berbasis Android," *J. Infomedia*, vol. 3, no. 1, pp. 10–17, 2018, doi: 10.30811/jim.v3i1.623.
[11] A. Lestari, A. S. Sembiring, T. Zebua, and R. Parapat, "teknik penyembunyian pesan teks terenkripsi algoritma merkle- hellman knapsack menggunakan metode pixel value differencing," vol. 3, pp. 204–212, 2019, doi: 10.30865/komik.v3i1.1590.
[12] L. P. Malese, P. Studi, T. Informatika, and U. Tribuana, "976-Article Text-2657-1-10-20211012," vol. 7, no. 5, pp. 343–354, 2021, doi: 10.5281/zenodo.5563416.
[13] A. Nasiri, "Pendahuluan Landasan Teori," vol. 10, pp. 10–16, 2020.
[14] M. A. Maricar and M. O. Widyantara, "Pemampatan Citra Pas Foto Dengan Menggunakan Algoritma Kompresi Joint-Photograpic Experts Group (JPEG) dan Principal Component Analysis (PCA)," vol. 17, no. 1, pp. 102–106, 2018.