e-ISSN : 2722-4368

Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode Pixel Value Differencing

Andre Gustiawan[1], Jusuf Wahyudi[2*], Eko Suryana[3]
[1,2,3]Universitas Dehasen Bengkulu, Jalan Meranti Raya No. 32 Sawah Lebar, Bengkulu Indonesia
Email jusuf.wahyudi@unived.ac.id

Abstrak. *Saat ini keamanan data sangat penting terutama keamanan pada bidang sistem informasi, hal ini dikarenakan pengguna komputer pada kehidupan setiap hari telah menjadi kebutuhan utama dalam kegiatan mengelola data dan informasi, dimana kegiatan transaksi data ataupun penyimpanan data sangatlah penting untuk dijaga keamanannya. Salah satu teknik untuk melindungi data dan informasi adalah dengan menggunakan steganografi Pixel Value Differncing (PVD). Algoritma ini bekerja dengan cara membagi citra menjadi blok-blok, dimana setia blok terdiri dari dua pixel yang bertetangga secara horizontal. Metode penelitian yang digunakan adalah menggunakan metode terapan (applied research) Hasil dari penelitian ini adalah proses Steganografi menggunakan metode Pixel Value Differencing dapat bekerja dengan baik dimana proses penyisipan dan ekstraksi dapat berjalan dengan baik dan optimal***..***

Kata Kunci : Keamanan Informasi, Steganografi , Pixel Value Differncing

Abstract. *At present data security is very important, especially security in the field of information systems, this is because computer users in everyday life have become a major requirement in managing data and information activities, where data transaction activities or data storage are very important to maintain security. One of the techniques to protect data and information is to use Pixel Value Differing (PVD) steganography. This algorithm works by dividing the image into blocks, where each block consists of two adjacent pixels horizontally. The research method used is applied method (applied research). The results of this study are that the Steganography process using the Pixel Value Differencing method can work well where the insertion and extraction processes can run well and optimally*

Keyword : Information Security, Steganography, Pixel Value Differncing

PENDAHULUAN

Saat ini keamanan data sangat penting terutama keamanan pada bidang sistem informasi, hal ini dikarenakan pengguna komputer pada kehidupan setiap hari telah menjadi kebutuhan utama dalam kegiatan mengelola data dan informasi, dimana kegiatan transaksi data ataupun penyimpanan data sangatlah penting untuk dijaga keamanannya. Berbagai teknik telah banyak digunakan untuk melindungi data-data penting tersebut, di antara salah satunya adalah steganografi. Steganografi merupakan seni penyembunyian pesan ke dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. Kata steganografi berasal dari bahasa Yunani yaitu *steganos* yang artinya tersembunyi atau terselubung dan *graphein*, yang artinyamenulis, sehingga kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung". Steganografi berbeda dengan kriptografi atau metode keamanan informasi lainnya, metode ini yaitu menyembunyikan informasi atau pesan kedalam media lain seperti citra digital, teks, suara atau video sehingga tidak menimbulkan kecurigaan orang lain. Steganografi membutuhkan dua properti, yaitu informasi dan media penampung. Media penampung yang banyak digunakan untuk menyembunyikan informasi yaitu citra digital. penyisipan informasi pada media citra digital dilakukan pada bit –bit pixel yang terdapat pada citra. Penggunaan citra digital sebagai media penampung mempunyai kelebihan karena indera penglihatan manusia memiliki keterbatasan terhadap warna, sehingga dengan keterbatasan tersebut manusia sulit membedakan citra digital yang asli dengan citra digital yang telah disisipi pesan rahasia.

Steganografi sudah dikenal oleh bangsa Yunani. Penguasa Yunani dalam mengirimkan pesan rahasia menggunakan kepala budak atau prajurit sebagai media. Dalam hal ini, rambut budak dicukur habis, lalu pesan rahasia ditulis di kulit kepala budak tersebut. Ketika rambut budak tumbuh, budak tersebut diutus untuk membawa pesan rahasia di kepalanya. Lain halnya dengan bangsa Yunani, bangsa Romawi mengenal

steganografi dengan menggunakan tinta tak tampak untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu dan cuka. Jika tinta digunakan untuk menulis maka tulisannya tidak tampat. Tulisan di atas kertas tersebut dapat dibaca dengan cara memanaskan kertas tersebut[1]

Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos* yang artinya tersembunyi atau terselubung dan *graphein*, yang artinya menulis, sehingga kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung". Secara umum steganografi adalah ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia[2]

Seiring beragamnya media yang digunakan pada steganografi, makin banyak pula metode steganografi yang dapat digunakan seperti EOF (*End Of File), MSB (Most Significant Bit), LSB (Least Significant Bit), Spread Spectrum, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Bit-Plane Complexity Segmentation (BPCS)*[3]. Selain itu juga ada metode *Pixel Value Differncing* (PVD), metode ini bekerja dengan cara membagi citra menjadi blok-blok, dimana setia blok terdiri dari dua *pixel* yang bertetangga secara horizontal. Pada penelitian tentang steganografi telah banyak dilakukan sebelumnya yaitu membahas steganografi untuk menyisipkan pesan teks ke dalam gambar dengan menggunakan metode LSB *(Least Significant Bit).* Metode LSB merupakan salah satu metode yang digunakan dalam teknik steganografi dengan proses kerja mengubah pesan ke dalam bentuk bilangan biner yang kemudian di urutkan nilai *pixel* gambar sesuai dengan urutan dari yang terkecil[4].

Steganografi merupakan seni penyembunyian pesan ke dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. Kata steganografi (steganography) berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau terselubung dan graphein yang artinya menulis, sehingga kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung[5]

Kriteria Steganografi

Adapun kriteria steganografi adalah :

1. *Imperceptibility*, keberadaan pesan rahasia tidak dapat dipersepsi oleh indera. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertext*-nya. Jika *covertext* berupa audio, maka indera telinga tidak dapat mendeteksi perubahan pada audio *stegotext*-nya.
2. *Fidelity*, mutu stegomedium tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat dipersepsi oleh inderawi. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertext*-nya. Jika *covertext* berupa audio, maka audio stegotext tidak rusak dan indera telinga tidak dapat mendeteksi perubahan tersebut.
3. *Recovery*, pesan yang disembunyikan harus dapat diungkapkan kembali. Karena tujuan steganografi adalah data *hiding*, maka sewaktu-waktu pesan rahasia di dalam stegotext harus dapat diambil kembali untuk digunakan lebih lanjut.

Teknik Steganografi

Ada tujuh teknik dasar yang digunakan dalam steganografi[6], yakni :

1. *Injection*, merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik ini sering juga disebut *embedding.*
2. Substitusi, data normal digantikan dengan data rahasia. Biasanya, hasil teknik ini tidak terlalu mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas media yang ditumpangi
3. Transform Domain, teknik ini sangat efektif. Pada dasarnya, transformasi domain menyembunyikan data pada transform space. Akan sangat lebih efektif teknik ini diterapkan pada file berekstensi JPG
4. *Spread Spectrum*, sebuah teknik pengtransmisian menggunakan pseudo-noise code, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (bandwidth) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi
5. *Statistical Method*, teknik ini disebut juga skema steganographic 1bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit. Perubahan statistik

e-ISSN : 2722-4368

ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum
6. *Distortion*, metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia
7. *Cover Generation*, metode ini lebih unik daripada metode lainnya karena cover object dipilih untuk menyembunyikan pesan. Contoh dari metode ini adalah Spam Mimic.

Pixel Value Differencing (PVD)

Metode Pixel Value Differencing merupakan salah satu metode yang dapat digunakan dalam pembuatan steganografi.Metode ini menawarkan kapasitas penyimpanan pesan yang lebih besar, dengan kualitas gambar yang lebih baik dibandingkan dengan metode lainnya[3]. Metode *Pixel Value Differencing* membagi citra menjadi blok-blok, dimana setiap blok terdiri dari dua *pixel* yang bertetangga secara horizontal. Proses penyisipan pada metode ini dilakukan dengan cara membandingkan dua *pixel* yang bertetangga dengan persamaan sebagai berikut :

$$d = | P_i + P_{i+1} | \quad \ldots\ldots (1)$$

Hasil dari perbandingan tersebut digunakan untuk mengetahui berapa banyak bit yang dapat disisipkan kedalam dua *pixel* yang dibandingkan. Metode ini menggunakan skema Wu dan Tsai untuk mengetahui nilai *Continues Range* dari perbandingan pixel sebelumnya. Skema Wu dan Tsai yang digunakan dapat dilihat pada tabel berikut :

Tabel 1. Nilai Continues Range

Kuantitasi 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
7	128-255	127	7

Skema ini digunakan untuk mengetahui terdapat di range mana selisih dari dua *pixel* tersebut, jika telah diketahui dimana letak range nya, maka jumlah bit pesan yang disisipkan dapat diketahui dengan persamaan berikut :

$$t = | \log_2 W_i | \quad \ldots\ldots (2)$$

W_i = Nilai terkecil dari skema wu dan tsai, letak range selisih perbandingan dua *pixel*

Penyisipan pesan dapat dilakukan dengan mengambil sebanyak t bit dari pesan yang akan disisipkan. Selanjutnya dihitung nilai difference value yang baru untuk penyisipan kedalam citra menggunakan persamaan sebagai berikut :

$$d'_i = l_i + b \quad \ldots\ldots (3)$$

Untuk menyisipkan pesan ada beberapa aturan yang harus dipenuhi yaitu :

1. $Jika\ P_i \geq P_{i+1}\ dan\ d_i' > d_i, maka\ \left(P_i' + [m/2],\ P_{i+1} -\ [m/2]\right)$
2. $Jika\ P_i < P_{i+1}\ dan\ d_i' > d_i, maka\ \left(P_i' - [m/2],\ P_{i+1} -\ [m/2]\right)$
3. $Jika\ P_i \geq P_{i+1}\ dan\ d_i' \leq d_i, maka\ \left(P_i' - [m/2],\ P_{i+1} -\ [m/2]\right)$
4. $Jika\ P_i < P_{i+1}\ dan\ d_i' \leq d_i, maka\ \left(P_i' + [m/2],\ P_{i+1} -\ [m/2]\right)$

Dimana m didapat dari selisih $d_i'\ dengan\ d_i$, dengan menggunakan persamaan sebagai berikut :

$$m = |d'_i \leq d_i| \quad \ldots\ldots (4)$$

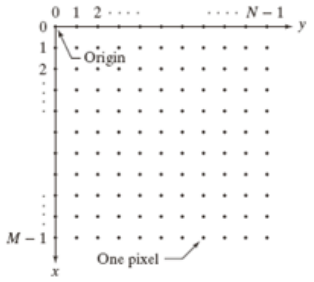
Proses-proses tersebut dilakukan terus hingga bit pesan tersisipi semuanya kedalam citra. Proses ekstraksi pesan dari citra stego menggunakan metode ini dimulai dengan menghitung nilai *difference value* (d_i) antara dua *pixel* yang bertetangga. Nilai *difference value* tersebut digunakan untuk mengetahui nilai *continuous ranges* (R) yang sudah didefinisikan menggunakan skema Wu dan Tsai.

Berdasarkan informasi tersebut dapat diketahui ukuran data rahasia yang disisipkan pada kedua pixel menggunakan persamaan (2), sehingga pesan rahasia yang telah disisipkan didapatkan kembali. Proses ekstraksi ini dilakukan sampai semua data rahasia yang telah disisipkan didapatkan kembali.

Citra Digital

Pengolahan citra merupakan cabang ilmu dalam *Artifical Intelegence* yang menggunakan objek citra dalam bentuk digital untuk penyelesaian kasusnya. Metode dalam citra dapat digunakan baik perhitungan matematis pada objek secara piksel ataupun geometris. Masing-masing objek citra memiliki nilai perbedaan yang dapat diperhitungkan secara matematis, sehingga menunjukkan ciri yang berbeda antara objek satu dengan yang lain. Penciri dari perbedaan setiap objek dapat ditentukan dari warna, tekstur, ataupun bentuk[7]

Citra digital dibentuk oleh kumpulan titik yang dinamakan piksel (*pixel* atau "*picture element*"). Setiap piksel digambarkan sebagai satu kotak kecil. Setiap piksel mempunyai koordinat posisi. Sistem koordinat yang dipakai untuk menyatakan citra digital ditunjukkan pada Gambar 1 berikut :



Gambar 1. Ilustrasi Citra Digital

Sebuah citra digital dapat diwakili oleh sebuah matriks yang terdiri dari M kolom dan N baris, di mana perpotongan antara kolom dan baris disebut piksel, yaitu elemen terkecil dari sebuah citra. Piksel mempunyai dua parameter, yaitu koordinat dan intensitas atau warna. Nilai yang terdapat pada koordinat (x,y) adalah *f*(x,y), yaitu besar intensitas atau warna dari piksel di titik itu. Oleh sebab itu, sebuah citra digital dapat ditulis dalam bentuk matriks berikut

$$f(x,y) = \begin{bmatrix} f(0,0) & \cdots & f(0,M-1) \\ \vdots & \ddots & \vdots \\ f(N-1,0) & \cdots & f(N-1,M-1) \end{bmatrix}$$

Berdasarkan gambaran tersebut, secara matematis citra digital dapat dituliskan sebagai fungsi intensitas *f(x,y)*, di mana harga *x* (baris) dan *y* (kolom) merupakan koordinat posisi dan *f(x,y)* adalah nilai fungsi pada setiap titik (x,y) yang menyatakan besar intensitas citra atau tingkat keabuan atau warna dari piksel di titik tersebut. Pada proses digitalisasi (sampling dan kuantisasi) diperoleh besar baris M dan kolom N hingga citra membentuk matriks MxN dan jumlah tingkat keabuan piksel. Pada kebanyakan kasus, terutama untuk keperluan penampilan secara visual, nilai data visual tersebut merepresentasikan warna dari citra yang diolah, dengan demikian format data citra digital berhubungan erat dengan warna

Jenis Citra

Nilai suatu pixel memiliki nilai dalam rentang tertentu, dari nilai minimum sampai nilai maksimum. Jangkauan yang digunakan berbeda-beda tergantung dari jenis warnanya. Namun secara umum

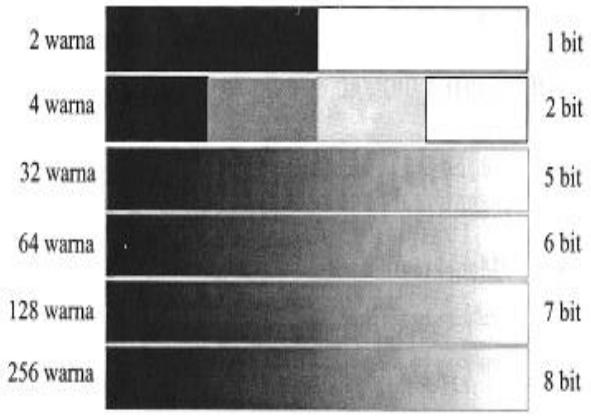
e-ISSN : 2722-4368

jangkauannya adalah 0 – 255. Citra dengan penggambarannyaseperti ini digolongkan kedalam citra integer. Beikut adalah jenis-jenis citra berdasarkan nilai pixelnya.

1. Citra Biner
   Citra biner adalah citra digital yang hanya memiliki dua kemungkinan nilai pixel yaitu hitam dan putih. Citra biner juga disebut sebagai citra *B&W (black and white)* atau citra monokrom. hanya dibutuhkan 1 bit untuk mewakili nilai setiap pixel dari citra biner.

Gambar 2. Contoh Citra Biner

2. Citra Grayscale
   Citra *grayscale* menangani gradasi warna hitam dan putih, yang tentu saja menghasilkan warna abu-abu. Dalam hal ini intensitas berkisar antara 0 sampai dengan 255. Nilai 0 menyatakan hitam dan nilai 255 menyatakan putih. Banyaknya warna tergantung pada jumlah bit yang disediakan dimemori untuk menampung kebutuhan warna ini. Semakin besar jumlah bit warna yang disediakan di memori, semakin halus gradasi warna yang terbentuk. Gambar 2.5 menunjukkan perbandingan gradasi warna untuk jumlah bit tertentu.



Gambar 3. Contoh Citra Grayscale Perbanding 1 bit, 2 bit, 5 bit dan 6 bit

3. Citra Warna
   Setiap piksel pada citra warna memiliki warna yang merupakan kombinasi dari tiga warna dasar RGB (*Red, Green, Blue*). Setiap warna dasar menggunakan penyimpanan 8 bit = 1 byte, yang berarti setiap warna mempunyai gradasi sebanyak 255 warna. Berarti setiap piksel mempunyai kombinasi warna sebanyak 28 . 28 . 28 = 224 = 16 juta warna lebih. Itulah yang menjadikan alasan format ini disebut dengan *true color* karena mempunyai jumlah warna yang cukup besar sehingga bias dikatakan hampir mencakup semua warna di alam. Penyimpanan citra *true color* di dalam memori berbeda dengan citra *grayscale*. Setiap piksel dari citra *grayscale* 256 gradasi warna diwakili oleh 1 byte. Sedangkan 1 piksel

citra *true color* diwakili oleh 3 byte, dimana masing-masing byte merepresentasikan warna merah, hijau dan biru.

Gambar 4. Contoh Citra Warna 8 Bit True Color

METODOLOGI PENELITIAN

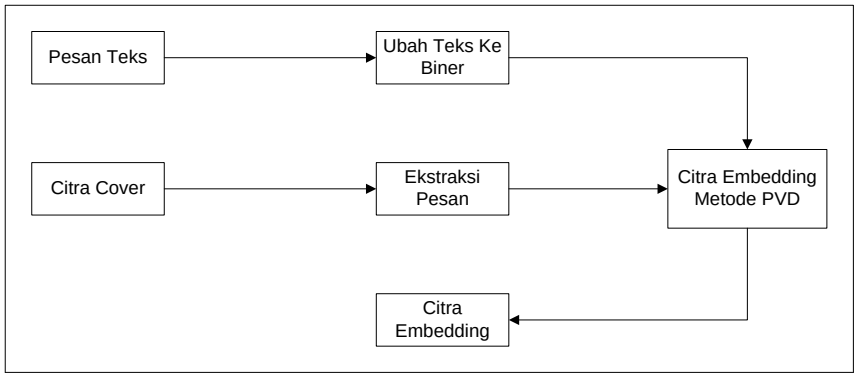
Dalam melakukan penelitian ini, penulis menggunakan metode terapan (*applied research*). Penelitian terapan atau *applied research* dilakukan berkenaan dengan kenyataan-kenyataan praktis, penerapan, dan pengembangan ilmu pengetahuan yang dihasilkan oleh penelitian dasar dalam kehidupan nyata. Penelitian terapan berfungsi untuk mencari solusi tentang masalah-masalah tertentu. Tujuan utama penelitian terapan adalah pemecahan masalah sehingga hasil penelitian dapat dimanfaatkan untuk kepentingan manusia baik secara individu atau kelompok maupun untuk keperluan industri atau politik dan bukan untuk wawasan keilmuan semata.

Dalam melaksanakan penelitian terapan ini terdapat 5 (lima) langkah, diantaranya :

a. Melakukan sesuatu yang sedang diperlukan, dipelajari, diukur, dan diperiksa kelemahannya.
b. Mencari satu dari kelemahan-kelemahan yang diperoleh dipilih untuk penelitian.
c. Mencari dan memberikan solusi dalam melakukan pemecahan masalah
d. Kemudian dilakukan modifikasi sehingga penyelesaian dapat dilakukan untuk diterapkan.
e. Pemecahan dipertahankan dan menempatkannya dalam suatu kesatuan sehingga jadi bagian permanen dalam satu sistem.

1. Analisis Proses Penyisipan/Embedding

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 5 berikut :



Gambar 5. Proses Penyisipan Pesan

Tabel 2. Nilai Continues Range Dari Nilai Difference Value

Kuantitasi 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
7	128-255	127	7

Contoh proses penyisipan, jika diketahui pesan yang akan disisipkan "Universitas Dehasen", dengan wadah penampung citra ukuran 4 x 4 pixel.

130	156	142	239
149	243	147	240
153	209	151	240
155	188	159	221

Gambar 6. Nilai Pixel Citra Penampung

Adapun tahapan penyelesaian penyisipan pesan adalah sebagai berikut :

a. Mengubah pesan ke dalam bentuk Biner

PESAN	BILANGAN ASCII	BINER
U	85	01010101
n	110	01101110
i	105	01110101
v	118	01110110
e	101	01100101
r	114	01110010
s	115	01110011
i	105	01110101
t	117	01110101
a	97	01100001
s	115	01110011
Spasi	32	00100000
D	68	01000100
E	101	01100101
H	104	01101000
A	97	01100001
S	115	01110011
E	101	01100101
N	110	01101110

b. Menyatukan semua biner pesan
0101010101101110011101010111011001100101011100100111001101110101010111010101100001011100110010000001000100011001010110100001100001011100110110010101011101110

c. Menghitung nilai d, yakni : d = |130 – 156| = 26

d. Mencari letak nilai *continues range* dari nilai *difference value* berdasarkan tabel 3.2 diatas, maka letak nilai d= 26 yaitu [16,31] dimana l_k = 16 dan u_k = 31

e. Menghitung banyaknya bit pesan yang dapat disisipkan ke dalam kedua pixel yang dibandingkan menggunakan persamaan t = | log $_2$ W_i |, sehingga t = |$\log_2$ (16 – 32)| = 4. Maka diambil bit dari pesan sebanyak *t* = 0101

f. Mengubah bit t ke dalam nilai desimal
Bit informasi yang disisipkan yaitu 0101, maka nilai desimalnya yaitu 5 atau $b=5$
g. Menghitung nilai *differencing value* menggunakan persamaan $d_i' = l_i + b$, sehingga diperoleh $d_i' = 16 + 5 = 21$, maka didapatkan nilai $d_i' = 21$ yang merupakan nilai *differencing value* yang baru
h. Melakukan penyisipan dengan mengubah nilai dari *pixel* yang dibandingkan dengan nilai *pixel* yang baru sesuai dengan aturan-aturan yang ditetapkan, dimana $m=5$, didapat menggunakan persamaan $m = |d_i' \leq d_i|$, $m = |21 \leq 26|$. Aturan terpenuhi yaitu :

$$Jika\ P_i < P_{i+1}\ dan\ d_i' \leq d_i, maka\ \left(P_i' + \left[\frac{m}{2}\right],\ P_{i+1} - \left[\frac{m}{2}\right]\right)$$

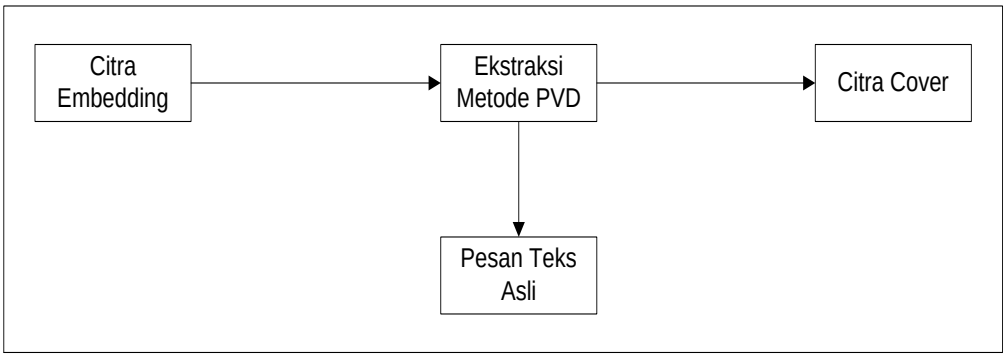
i. Menyimpan nilai *pixel* yang baru yaitu : $P_i' = 132$ dan $P_i = 153$ kedalam citra. Tahapan ini dilakukan sampai semua pesan tersisipi, sehingga menjadi seperti berikut :

132	153	142	239
149	243	147	240
153	209	151	240
155	188	159	221

Gambar 7. Nilai *Pixel* Citra Setelah Disisipi Pesan

2. Analisis Proses Ekstraksi Pesan

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 berikut :



Gambar 8. Proses Ekstraksi Pesan

Tahap awal pada proses ekstraksi pesan yaitu mengambil nilai *pixel* dari citra yang telah disisipkan pesan.

132	153	142	239
149	243	147	240
153	209	151	240
155	188	159	221

Gambar 9. Nilai *Pixel* Citra yang Telah Disisipi Pesan

Maka tahap selanjutnya yaitu melakukan proses ekstraksi menggunakan metode *pixel value differencing* dengan tahapan-tahapan yaitu sebagai berikut :
a. Mengambil pixel yang bertetangga dari citra. Contoh *pixel* yang bertetangga yaitu *pixel* (0,0) dengan *pixel* (0,1) seperti pada gambar 3.4. Nilai dari *pixel* yang bertetangga adalah $P_i = 132 \text{dan} P_{i+1} = 153$
b. Menghitung nilai *differencing value* dari kedua *pixel* tersebut

e-ISSN : 2722-4368

d = |132 – 153| = 21

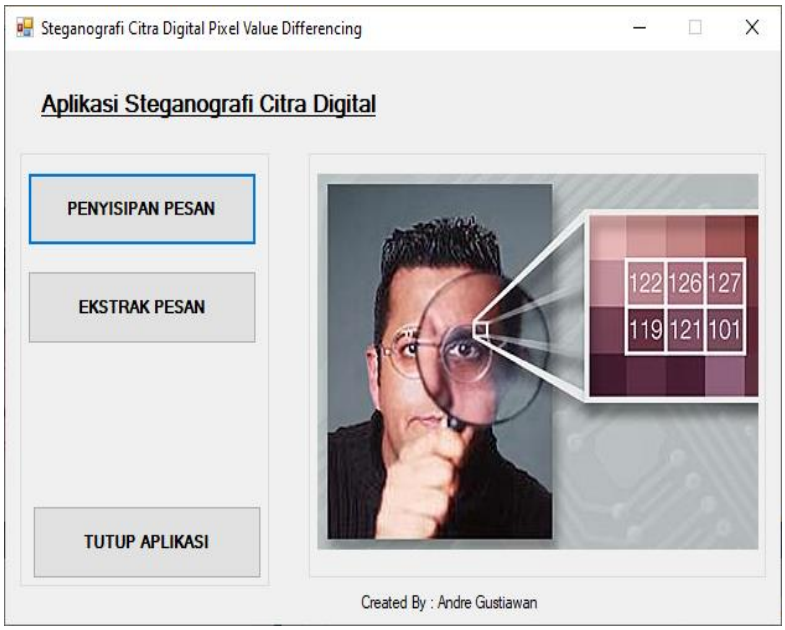
c. Mencari letak nilai *continues range* dari nilai *difference value* berdasarkan tabel 3.2 diatas, maka letak nilai d= 21 yaitu [16,31] dimana $l_k = 16$ dan $u_k = 31$
d. Menghitung berapa banyak bit dari pesanyang dapat disisipkan kedalam kedua *pixel* yang dibandingkan menggunakan persamaan $t = \lfloor \log_2 W_i \rfloor$, sehingga $t = \lfloor \log_2 (16 - 32) \rfloor = 4$. Maka diambil bit dari pesan sebanyak *t* = 0101
e. Mengubah bit t ke dalam nilai desimal, Bit informasi yang disisipkan yaitu 0101, maka nilai desimalnya yaitu 5 atau *b=5*
f. 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
01010101011011100111010101110110011001010111001001110011011101010111010101100001011100110010000001000100011001010110100001100001011100110110010101011011 10

⇨ Universitas Dehasen

HASIL DAN PEMBAHASAN

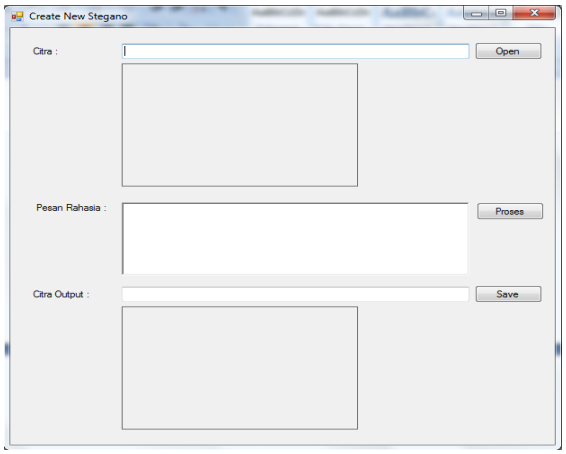
Halaman utama sistem yang dikembangkan seperti yang terlihat pada gambar 4.1 dapat dilihat antarmuka dari sistem yang dikembangkan yang merupakan aplikasi berbasis *desktop*. Pada halaman utama dapat dilihat terdapat logo dan judul dari aplikasi yang dikembangkan.seperti terlihat pada gambar 10 berikut :

1. Penyisipan Pesan Teks



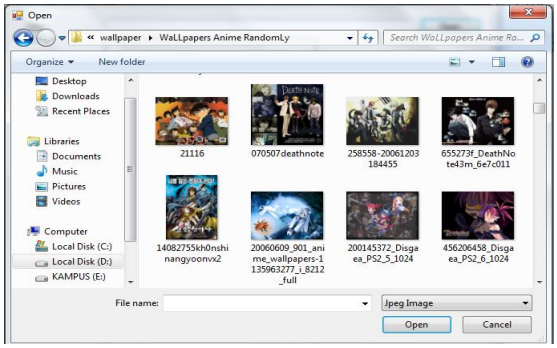
Gambar 10. Tampilan Halaman Awal

Jika dipilih tombol penyisipan pesan, maka program selanjutnya menampilkan form pemilihan gambar dengan tampilan sebagai berikut :



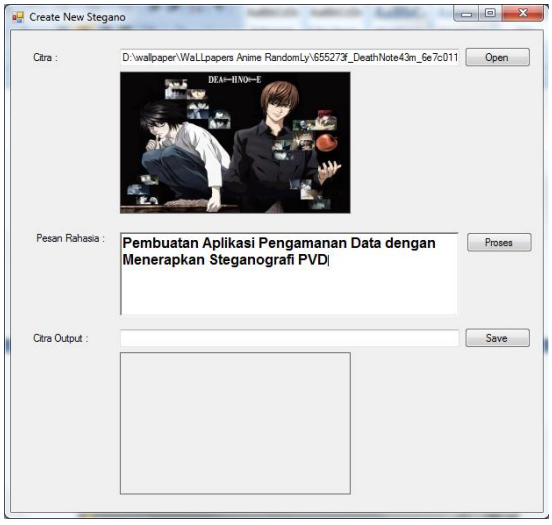
Gambar 11. Tampilan Form Pemilihan Gambar

Pada gambar 11 di atas, setelah tombol "Open" di klik maka akan muncul dialog untuk memilih gambar yang akan digunakan sebagai media penyisipan seperti yang terlihat pada gambar 12 berikut :



Gambar 12. Tampilan Form Penentuan Lokasi File Gambar

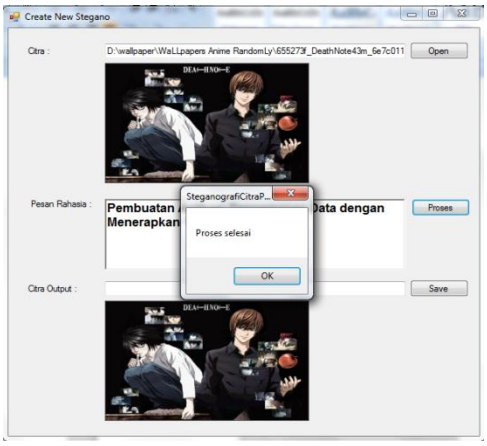
Setelah salah satu gambar dipilih, program selanjutnya meminta pengguna melakukan pengisian pesan teks seperti terlihat pada gambar 13 berikut :



Gambar 13. Pengisian Teks Yang Akan Disisipkan

Setelah pesan teks diisikan dan dilanjutkan dengan penekanan tombol proses, selanjutnya pada bagian bawah

(area hasil) akan terlihat tampilan seperti gambar 14 berikut :



Gambar 14. Tampilan Gambar Setelah Disisipi Teks

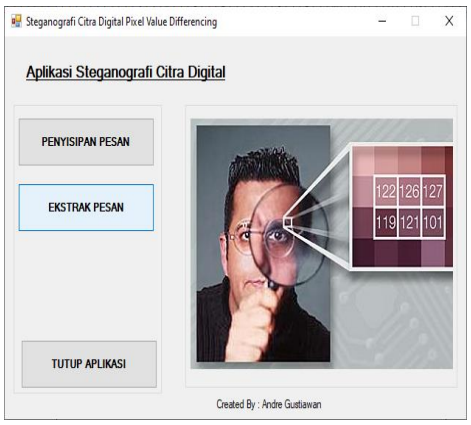
Gambar 15a. Tampilan Gambar Asli

Gambar 15b. Tampilan Gambar Telah Disisipi

Dari kedua tampilan gambar 15a dan gambar 15b terlihat keduanya memiliki tampilan yang sama, meskipun pada kenyataannya gambar 15b telah memiliki sisipan teks pesan.

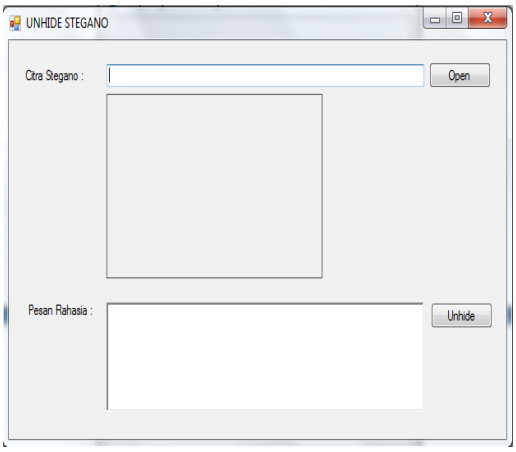
2. Ekstraksi Pesan Teks

Seperti proses penyisipan teks, dari menu (halaman) utama program, diklik tombol Ekstrak Pesan, dan program selanjutnya membuka form penentuan lokasi gambar yang akan diekstrksi seperti gambar 16 berikut

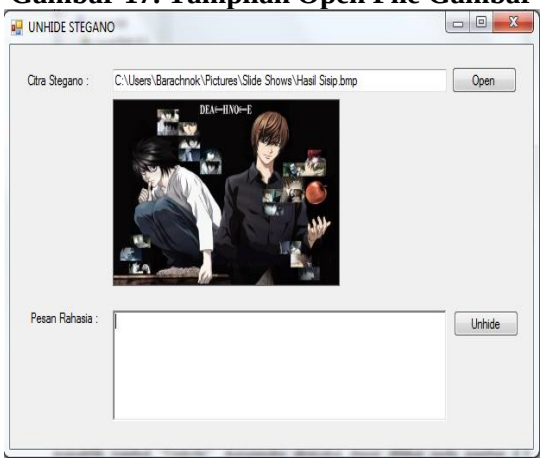


Gambar 16. Tampilan Halaman Ekstraksi Pesan

e-ISSN : 2722-4368

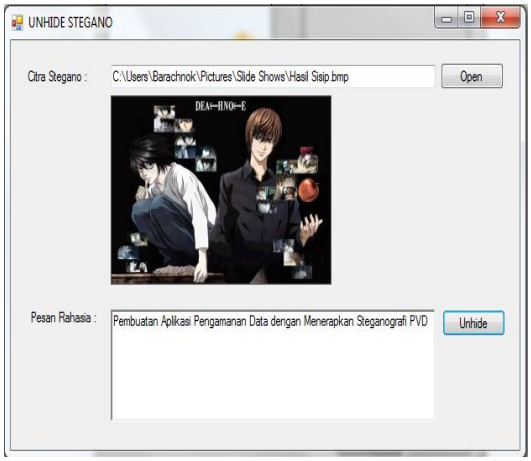


Gambar 17. Tampilan Open File Gambar



Gambar 17. Tampilan Setelah Penentuan Gambar Yang Akan Diekstrak

Pada gambar 17 di atas terlihat setelah gambar yang akan diekstrak dipilih, kemudian tombol Unhide menjadi Enable untuk diklik agar didapatkan pesan teks nya seperti gambar 18 berikut ini



Gambar 18. Pesan Teks Muncul setelah tombol Unhide diklik

KESIMPULAN

Berdasarkan penelitian pengembangan aplikasi steganografi menggunakan metode PVD maka dapat diambil beberapa kesimpulan yaitu:

1. Pengamanan steganografi pada citra digital menggunakan metode *Pixel Value Differencing* dilakukan dengan menghitung selisih nilai piksel yang bertetangga yang kemudian nilai selisih tersebut akan dijumlahkan dengan nilai bit pada pesan yang akan disembunyikan pada kanal warna R dan G yang masing – masing menampung delapan bit dari data rahasia.
2. Algoritma yang digunakan dalam proses steganografi PVD yang dilakukan pada penelitian ini adalah menghitung nilai selisih antar bit data rahasia dengan bit citra penampung. Berdasarkan nilai selisih baru tersebut, nilai piksel kemudian disesuaikan sehingga nilai piksel yang baru berubah dan mengandung bit dari informasi yang disembunyikan.
3. Berdasarkan penelitian yang dilakukan maka aplikasi yang dibangun pada penelitian ini menggunakan metode *Pixel Value Differencing* dapat bekerja dengan baik dimana proses penyisipan dan ekstraksi dapat berjalan dengan baik dan optimal.

DAFTAR PUSTAKA

[1] Moch. Alfian Ichsan, "Implementasi Algortima Kriptografi Rsa , Kompresi Data Huffman , Dan Steganografi Eof Pada Media Video Untuk," *Kilat*, 2017.

[2] A. Hafis, "Steganografi Berbasis Citra Digital untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB)," *J. Cendikia*, vol. XVII, no. April, pp. 194–198, 2019.

[3] A. P. Ratnasari and F. A. Dwiyanto, "Metode Steganografi Citra Digital," *Sains, Apl. Komputasi dan Teknol. Inf.*, vol. 2, no. 2, p. 52, 2020, doi: 10.30872/jsakti.v2i2.3300.

[4] A. Aryasanti, R. Ujiandari, and ..., "Implementasi Keamanan File Menggunakan Metode Kriptografi Base-64 dan Steganografi Least Significant Bit (LSB) Random 2-Bit Berbasis Web," *J. Ticom ...*, vol. 11, pp. 113–118, 2023, [Online]. Available: https://jurnal-ticom.jakarta.aptikom.or.id/index.php/Ticom/article/view/78.

[5] A. S. Manalu, "Implementasi Algoritma Kompresi Pada Steganografi Citra Digital Dengan Metode Modifikasi LSB," *J. TEKINKOM*, vol. 1, no. 2, pp. 69–79, 2018.

[6] N. Nurmaesah *et al.*, "Aplikasi Steganografi Untuk Menyisipkan Pesan DALAM MEDIA IMAGE," *J. TAM (Technology Accept. Model.*, vol. 8, no. 1, pp. 13–17, 2017.

[7] J. Jumadi, Y. Yupianti, and D. Sartika, "Pengolahan Citra Digital Untuk Identifikasi Objek Menggunakan Metode Hierarchical Agglomerative Clustering," *JST (Jurnal Sains dan Teknol.*, vol. 10, no. 2, pp. 148–156, 2021, doi: 10.23887/jstundiksha.v10i2.33636.