JDSP
Jurnal Data Science Penusa

APLIKASI KEAMANAN DATA PENGIRIMAN PESAN RAHASIA MENGGUNAKAN MEDIA GAMBAR DENGAN METODE (BPCS)

Yogi Tri Aditya[1)*], Baringin Sianipar [2)]
[1,2)] Program Studi Teknik Informatika, STMIK Pelita Nusantara, Medan
[1,2)] yogiaditya070@gmail.com, aniparbaringin87@gmail.com

Received: 06 September 2024 Accepted: 12 Oktober 2024 Published: 27 Oktober 2024
Pg. 142-154

OPEN ACCESS

***Yogi Tri Aditya**

Kata Kunci: KEAMANAN DATA, PENGIRIMAN PESAN, GAMBAR, STEGANOGRAFI, BPCS.

JDSP: Jurnal Data Science Penusa is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Abstrak : Steganografi adalah suatu teknik untuk menyembunyikan suatu informasi yang rahasia atau sensitif agar tidak terlihat seperti semestinya. Data rahasia disembunyikan dengan cara disisipkan pada *file* citra sehingga tidak terlihat bahwa dalam citra tersebut disembunyikan suatu informasi. *Bit-Plane Complexity Segmentation* (BPCS) adalah salah satu metode steganografi, di mana metode ini memiliki kapasitas penyisipan pesan yang relatif besar jika dibandingkan dengan metode lain seperti *Least Significant Bit* (LSB). Pada penelitian ini, akan dirancang aplikasi steganografi dengan menggunakan metode BPCS guna untuk menyembunyikan pesan rahasia dari orang yang tidak berhak untuk mengakses informasi itu. Selain itu dilakukan pengujian hasil terhadap aplikasi steganografi tersebut. Aplikasi steganografi dengan metode BPCS ini dapat diharapkan sebagai aplikasi untuk menyisipkan pesan terhadap *file* citra guna untuk menyembunyikan informasi dari orang yang tidak berhak mengaksesnya, dan aplikasi ini juga dapat digunakan untuk mengambil kembali pesan yang disisipkan tersebut. Hasil Penelitian menyimpulkan Steganografi dengan metode BPCS dapat diterapkan pada citra JPEG tanpa adanya modifikasi pada proses penyisipan sampai proses ekstraksi pesan. Proses rancang bangun sistem pengiriman pesan rahasia pada media gambar menggunakan alat bantu dalam perancangan sistem menggunakan UML (*Unified Modeling Language*) sehingga memudahkan dalam proses menganalisa setiap kebutuhan-kebutuhan dalam membangun sistem informasi berbasis.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia. Salah satu inovasi yang menonjol adalah kemampuan untuk mengirim dan menerima informasi secara cepat dan efisien. Teknologi ini telah mengubah cara kita berkomunikasi, bekerja, dan bahkan bertransaksi. Namun, dengan kemajuan tersebut, muncul pula tantangan baru, terutama dalam hal keamanan data. Keamanan data menjadi isu krusial di era digital saat ini, mengingat semakin banyaknya informasi sensitif yang disimpan dan ditransmisikan melalui jaringan elektronik. Keamanan data adalah aspek yang sangat penting dalam teknologi informasi, terutama ketika berkaitan dengan pengiriman pesan rahasia. Keamanan data bertujuan untuk melindungi informasi dari akses pihak yang tidak berwenang (Habibi Z, 2018).

Salah satu metode pengiriman pesan yang semakin populer adalah dengan menggunakan media gambar. Penggunaan gambar sebagai media untuk menyembunyikan pesan memiliki beberapa keunggulan, termasuk kemampuannya untuk menyamarkan keberadaan pesan itu sendiri. Namun, metode ini juga memiliki tantangan tersendiri. Salah satu masalah utama adalah bagaimana memastikan bahwa pesan yang

disembunyikan dalam gambar tersebut tetap aman dan tidak mudah diungkap oleh pihak yang tidak berwenang. Selain itu, proses penyembunyian pesan harus dilakukan sedemikian rupa sehingga kualitas gambar tidak terganggu dan pesan dapat dengan mudah diekstrak oleh penerima yang sah.

Solusi yang potensial untuk masalah ini adalah dengan menggunakan metode Bit-Plane Complexity Segmentation (BPCS). BPCS adalah teknik steganografi yang memanfaatkan kompleksitas bit-plane dalam gambar digital untuk menyembunyikan pesan rahasia. Metode ini bekerja dengan cara menggantikan bitplane dengan kompleksitas tinggi dalam gambar dengan bitplane dari pesan rahasia. Keunggulan utama BPCS adalah kemampuannya untuk menyembunyikan jumlah data yang lebih besar dibandingkan dengan metode steganografi tradisional, serta menjaga kualitas visual gambar tetap baik. Dengan BPCS, pesan yang disembunyikan dapat dilindungi dengan lebih efektif dan tidak mudah diungkap oleh pihak yang tidak berwenang. Implementasi metode ini diharapkan dapat meningkatkan tingkat keamana pesan terlindungi dengan baik.

TINJAUAN LITERATUR

1. KEAMANAN DATA

Keamanan data sangat diperlukan dalam sebuah perangkat, agar data-data yang diperlukan tidak dicuri atau dihapus oleh oknum-oknum tidak bertanggungjawab. Jika dilihat secara sederhana, keamanan data adalah tindakan yang perlu dilakukan oleh suatu perusahaan atau individu untuk melindungi ekosistem teknologi informasi. Adanya keamanan data ini, perusahaan atau individu tidak perlu khawatir lagi apabila terjadi pelanggaran keamanan. Karena biar bagaimanapun, data merupakan dokumen penting yang terkadang berisikan informasi pribadi. Jika data data berhasil dicuri, bukan tidak mungkin dokumen tersebut akan digunakan untuk tindakan-tindakan kriminal (M & Ramli, 2023).

2. STEGANOGRAFI

Steganografi yaitu suatu teknik yang dapat menyisipkan pesan kedalam citra digital seperti gambar, video, dan teks, dengan kapasitas data yang disisipkan direpresentasikan dalam bentuk bit per pixel. Steganografi biasanya sering disamakan dengan kriptografi karena keduanya sama-sama bertujuan untuk melindungi informasi yang berharga dan rahasia. Perbedaan yang mendasar antara keduanya terletak pada proses merahasiakan data dan hasil akhir dari proses tersebut. Kriptografi melakukan proses pengacakan data asli sehingga dihasilkan data terenkripsi yang benar-benar acak dan berbeda dengan aslinya(Ifan Rizqa & Safitri, 2022).

3. *Bit-Plane Complexity Segmentation* (BPCS)

Teknik BPCS ini adalah teknik steganografi yang tidak berdasarkan teknik pemrograman, tetapi teknik yang menggunakan sifat penglihatan manusia. Proses penyisipan pesan dilakukan pada segmen yang memiliki kompleksitas yang tinggi. Segmen yang memiliki kompleksitas tinggi ini disebut noise-like regions. Pada segmen-segmen ini penyisipan dilakukan tidak hanya pada least significant bit, tapi pada seluruh bitplane yang termasuk noise-like regions. Oleh sebab itu, pada teknik BPCS, kapasitas data yang disisipkan dapat mencapai 50% dari ukuran coverobject-nya (Ratnasari & Dwiyanto, 2020).

4. UML (UNIFIED MODELLING LANGUAGE)

UML (*Unified Modeling Language*) adalah bahasa pemodelan untuk sistem atau perangkat lunak yang berparadigma (berorientasi objek) (Kholifah & SitiNurmiati, 2022). Pemodelan (modeling) sesungguhnya digunakan untuk penyederhanaan permasalahan permasalahan yang kompleks sedemikian rupa sehingga lebih mudah dipelajari dan dipahami (Widyastuti & Widiyastuti, 2022).

5. FLOWCHART

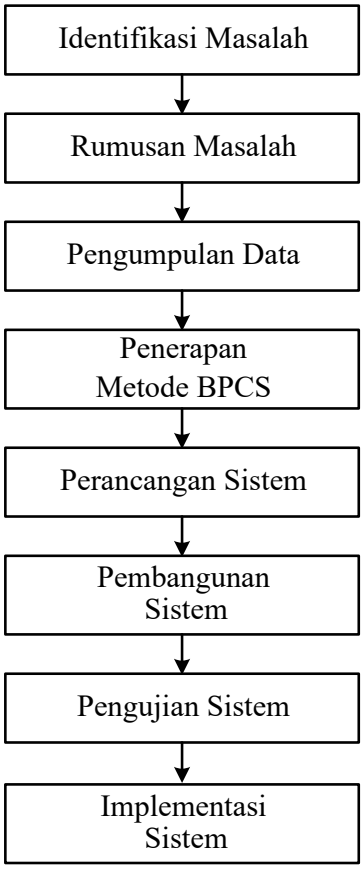
Flowchart adalah representasi secara simbolik dari suatu algoritma atau prosedur untuk menyelesaikan suatu masalah, dengan menggunakan flowchart akan memudahkan pengguna melakukan pengecekan bagian-bagian yang terlupakan dalam analisis masalah, disamping itu flowchart juga berguna sebagai fasilitas untuk berkomunikasi antara pemrogram yang bekerja dalam tim suatu proyek(Santoso & Nurmalina, 2017).

6. VISUAL BASIC

Visual Basic adalah sebuah pemrograman yang berpusat pada objek (Object Oriented Programming) dan digunakan dalam pembuatan aplikasi Windows berbasis Graphical User Interface (GUI). Secara umum, bahasa pemrograman adalah kumpulan perintah atau instruksi yang dimengerti oleh komputer untuk melakukan tugas-tugas tertentu. Visual Basic, sebagai salah satu bahasa pemrograman komputer, memiliki karakteristik yang membedakannya dari bahasa pemrograman lainnya (Laksmi, Gani, & Budiantoro, 2015).

METODE PENELITIAN

Metode penelitian diartikan sebagai cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Kerangka kerja penelitian merupakan langkah-langkah yang akan dilakukan dalam penyelesaian masalah yang akan dibahas. Adapun kerangka kerja dalam penelitian ini sebagai berikut:



Gambar 1 Kerangka Kerja Penelitian

HASIL PENELITIAN

Algoritma BPCS digunakan untuk menyisipkan pesan rahasia terhadap citra (cover image) untuk mendapatkan citra yang sudah disisipi pesan (*stego image*), metode BPCS ini juga digunakan untuk mendapatkan kembali pesan rahasia yang disisipkan atau yang sering disebut ekstraksi pesan.

Gambar yang digunakan sebagai cover image adalah gambar yang telah di pre processing dengan format JPG yang menggunakan jenis pewarnaan grayscale dengan kedalaman 8 bit dan pesan yang disisipkan merupakan pesan teks. Langkah-langkah dalam penyisipan pesan adalah sebagai berikut:

1. Gambar terlebih dahulu di pre-processing untuk mendapatkan cover image dan dilakukan pembagian gambar menjadi beberapa segmen berukuran 8x8 piksel setiap segmen.

Tabel 1 Nilai Intensitas dari Segmen Pertama

226	226	223	223	226	226	228	227
226	226	223	223	226	226	228	227
226	226	223	223	226	226	228	227
226	226	223	223	226	226	228	227
226	226	223	223	226	226	228	227
227	227	227	222	226	228	226	230
228	228	255	254	225	229	229	229
223	223	226	221	227	225	226	228

2. Nilai intensitas dari masing-masing kedalaman piksel direpresentasikan dengan nilai binernya dan nilai biner tersebut diubah dari sistem PBC menjadi CGC

Tabel 2 Representasi Biner dengan Sistem PBC Dari Nilai Intensitas Piksel

11100010	11100010	11011111	11011111	11100010	11100010	11100100	11100011
11100010	11100010	11011111	11011111	11100010	11100010	11100100	11100011
11100010	11100010	11011111	11011111	11100010	11100010	11100100	11100011
11100010	11100010	11011111	11011111	11100010	11100010	11100100	11100011
11100010	11100010	11011111	11011111	11100010	11100010	11100100	11100011
11100011	11100011	11100011	11011110	11100010	11100100	11100010	11100110
11100100	11100100	11100001	11100000	11100001	11100101	11100101	11100101
11011111	11011111	11100010	11011101	11100011	11100001	11100010	11100100

Representasi biner dengan sistem CGC dari nilai intensitas setiap piksel, dapat dilihat seperti tabel 3

Tabel 3 Representasi Biner dengan Sistem CGC dari Nilai Intensitas Piksel

10010011	10010011	10110000	10110000	10010011	10010011	10010110	10010010
10010011	10010011	10110000	10110000	10010011	10010011	10010110	10010010
10010011	10010011	10110000	10110000	10010011	10010011	10010110	10010010
10010011	10010011	10110000	10110000	10010011	10010011	10010110	10010010
10010011	10010011	10110000	10110000	10010011	10010011	10010110	10010010
10010010	10010010	10010010	10110001	10010011	10010110	10010011	10010101
10010110	10010110	10010001	10010000	10010001	10010111	10010111	10010111
10110000	10110000	10010011	10110011	10010010	10010001	10010011	10010110

3. Kemudian dilakukan proses bit-plane slicing untuk membagi gambar menjadi bit-plane.
4. Hitung nilai kompleksitas (α) dari masing-masing bit-plane, untuk menghitung nilai kompleksitas bit-plane.
   Hasil bit-plane slicing dari nilai intensitas piksel adalah sebagai berikut :
   Bit-plane 1

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

   Nilai kompleksitas (α) = 0
   Bit-plane 2

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

   Nilai kompleksitas (α) = 0

   Bit-plane 3

0	0	1	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0
1	1	0	1	0	0	0	0

Nilai kompleksitas (α) = 20 / 112 = 0.18

Bit-plane 4

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

Nilai kompleksitas (α) = 0

Bit-plane 5

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Nilai kompleksitas (α) = 0

Bit-plane 6.

0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	0
0	0	0	0	0	1	0	1
1	1	0	0	0	1	1	1
0	0	0	0	0	0	0	1

Nilai kompleksitas (α) = 26 /112 = 0.2

Bit-plane 7

1	1	0	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	0	1	1	1	0
1	1	0	0	0	1	1	1
0	0	1	1	1	0	1	1

Nilai kompleksitas (α) = 29 / 112 = 0.26

Bit-plane 8

1	1	0	0	1	1	0	0
1	1	0	0	1	1	0	0
1	1	0	0	1	1	0	0
1	1	0	0	1	1	0	0
1	1	0	0	1	1	0	0
0	0	0	1	1	0	1	1
0	0	1	0	1	1	1	1
0	0	1	1	0	1	1	0

Nilai kompleksitas (α) = 37 / 112 = 0.33

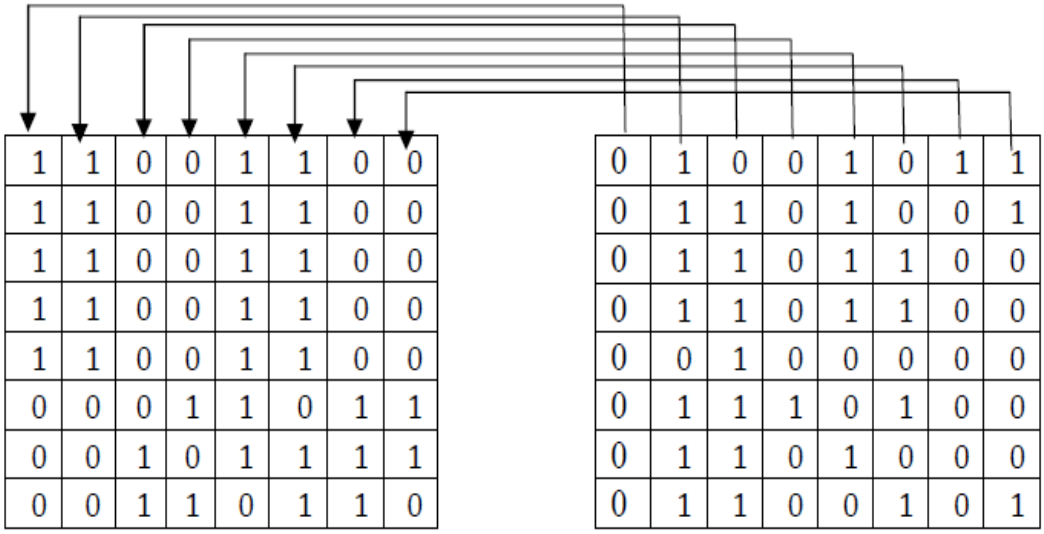
5. Tentukan bit-plane yang noise-like region dan informative region dengan threshold (α0) = 0,3.
6. Baca pesan rahasia sebagai string pada karakter ASCII dan representasikan dengan nilai binernya, kemudian bentuk pesan rahasia menjadi blok 8x8 dan hitung nilai kompleksitas (α) dari setiap blok.
   Pesan rahasia : Kill the king tonigh
   Nilai ASCII : 75 105 108 108 32 116 104 101 32
   Representasi biner pesan rahasia :
   01001011 01101001 01101100 01101100 00100000 01110100 01101000 01100101

   Blok pesan rahasia adalah sebagai berikut:

0	1	0	0	1	0	1	1
0	1	1	0	1	0	0	1
0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	0
0	0	1	0	0	0	0	0
0	1	1	1	0	1	0	0
0	1	1	0	1	0	0	0
0	1	1	0	0	1	0	1

   Nilai kompleksitas (α) = 49 / 112 = 0.44

7. Penyisipan pesan dilakukan dengan cara mengganti bit-plane yang noise- like pada gambar dengan blok-blok pesan rahasia. Dari perbandingan nilai threshold yang dilakukan diatas maka bit-plane 8 merupakan noise-like region dan bit-plane pesan memiliki nilai kompleksitas yang sudah kompleks sehingga proses langsung dilanjutkan dengan menggantikan bit-plane 8 dengan blok pesan rahasia, seperti proses yang ditunjukkan pada gambar 1.



Gambar 2 Proses menggantikan bit-plane 8 dengan blok pesan rahasia

Sehingga isi bit-plane 8 menjadi :

0	1	0	0	1	0	1	1
0	1	1	0	1	0	0	1
0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	0
0	0	1	0	0	0	0	0
0	1	1	1	0	1	0	0
0	1	1	0	1	0	0	0
0	1	1	0	0	1	0	1

8. Sebagai peta konjugasi, blok pesan Wc pada gambar 1 akan disisipkan pada akhir penyisipan pesan. Karena nilai bit-plane 8 diganti dengan blok 1 pesan rahasia, maka nilai bit kedelapan yang merepresentasikan nilai intensitas setiap piksel berubah, dalam sistem CGC menjadi seperti tabel 4.

Tabel 4 Representasi Biner dengan Sistem CGC dari Hasil Penyisipan Pesan

10010010	10010011	10110000	10110000	10010011	10010010	10010111	10010011
10010010	10010011	10110001	10110000	10010011	10010010	10010110	10010011
10010010	10010011	10110001	10110000	10010011	10010011	10010110	10010010
10010010	10010011	10110001	10110000	10010011	10010011	10010110	10010010
10010010	10010010	10110001	10110000	10010010	10010010	10010110	10010010
10010010	10010011	10010011	10110001	10010010	10010111	10010010	10010100
10010110	10010111	10010001	10010000	10010001	10010110	10010110	10010110
10110000	10110001	10010011	10110010	10010010	10010001	10010010	10010111

9. Nilai biner sistem CGC diubah menjadi PBC, pengubahan dilakukan menggunakakan persamaan 2.2. Kemudian nilai biner sistem PBC diubah menjadi nilai intensitas piksel.
   Representasi biner dengan sistem PBC dari nilai intensitas setiap piksel setelah disisipi pesan dapat dilihat pada tabel 4.

Tabel 5 Representasi Biner dengan Sistem PBC dari Hasil Penyisipan Pesan

11100011	11100010	11011111	11011111	11100010	11100011	11100101	11100010
11100011	11100010	11011110	11011111	11100010	11100011	11100100	11100010
11100011	11100010	11011110	11011111	11100010	11100010	11100100	11100011
11100011	11100010	11011110	11011111	11100010	11100010	11100100	11100011
11100011	11100011	11011110	11011111	11100011	11100011	11100100	11100011
11100011	11100010	11100010	11011110	11100011	11100101	11100011	11100111
11100100	11100101	11100001	11100000	11100001	11100100	1110010	11100100
11011111	11011110	11100010	11011100	11100011	11100001	11100011	11100101

Nilai intensitas segmen pertama pada gambar setelah disisipi pesan dapat dilihat pada tabel 5.

Tabel 6 Nilai Intensitas dari Segmen Pertama Setelah Disisipi Pesan

227	226	223	223	226	227	229	226
227	226	222	223	226	227	228	226
227	226	222	223	226	226	228	227
227	226	222	223	226	226	228	227
227	227	222	223	227	227	228	227
227	226	226	222	227	229	227	231

228	229	255	254	225	228	228	228
223	222	226	220	227	225	227	229

Proses ekstraksi pesan merupakan kebalikan dari proses penyisipan diatas. Langkah awal dalam proses ekstraksi ini yaitu mengetahui kedalaman bit yang digunakan oleh dokumen JPG agar tidak terjadi kesalahan dalam proses pengambilan pesan. Langkah ekstraksi pesan dengan metode BFCS dilakukan dengan tahapan-tahapan proses sebagai berikut :

1. Ambil nilai nilai intensitas dari setiap segmen yang merepresentasikan stego image pada setiap piksel.
2. Nilai intensitas dari masing-masing kedalaman piksel direpresentasikan dengan nilai binernya dan nilai biner tersebut diubah dari sistem PBC menjadi CGC pengubahan dilakukan menggunakan persamaan 2.1.
3. Kemudian dilakukan proses bit-plane slicing untuk membagi gambar menjadi bi-tplane, seperti yang dilakukan pada proseses penyisipan dengan menggunakan persamaan 2.3.
4. Hitung nilai kompleksitas (α) dari masing-masing bit-plane, untuk menghitung nilai kompleksitas bit-plane dapat dilakukan menggunakan persamaan 2.5.
5. Input nilai threshold yang sama dengan nilai threshold saat penyisipan pesan, karena nilai yang berbeda akan mengakibatkan ekstraksi yang tidak sempurna.
6. Bandingkan nilai kompleksitas (α) dengan nilai threshold, setiap bit-plane yang memiliki kompleksitas lebih besar dari nilai threshold merupakan bit-plane yang telah digantikan dengan blok pesan.
7. Proses perbandingan kompleksitas dengan nilai threshod akan berhenti disaat kompleksitas dari bit-plane = 1
8. Bit-plane yang merupakan blok pesan dengan indeks pertama sama dengan 1, akan dilakukan konjugasi dengan menggunakan persamaan 2.3 untuk mendapatkan pesan yang sebenarnya.
9. Ubah gambar biner 8 x 8 kedalam rangkaian 64 bit , dan lakukan konversi biner ke desimal dan pesan rahasia akan di tampilkan sebagai string pada karakter ASCII.

Gambaran proses ekstraksi pesan dengan algoritma BPCS dapat dideskripsikan dalam bentuk flowchart dengan nilai threshold yang di input dan digunakan sebagai nilai pembanding terhadap nilai kompleksitas yang sudah di dapatkan, untuk menentukan bit-plane yang termasuk blok pesan atau bit-plane yang bukan bagian dari pesan.

PEMBAHASAN

Hasil yang didapatkan dari pembahasan yang ada adalah terciptanya sebuah sistem Aplikasi Keamanan Data Pengiriman Pesan Rahasia Menggunakan Media Gambar. Dalam pembahasan ini, akan dibahas bagaimana langkah-langkah penggunaan aplikasi Keamanan Data Pengiriman Pesan Rahasia Menggunakan Media Gambar

1. Tampilan Form Utama

Form menu utama merupakan interface antara pengguna dengan aplikasi sistem kemanan data, pada menu utama terdapat beberapa menu yang dapat digunakan oleh pengguna yaitu :

a. Penyisipan Pesan, Menu ini merupakan menu yang dapat digunakan untuk melakukan proses penyisipan pesan ke dalam media gambar dengan beberapa langkap tahapan penyisipan pesan ke media gambar. Jika pengguna mengklik menu penyisipan pesan, makan akan muncul form penyisipan pesan.
b. Ektrasi Pesan, Menu ini merupakan menu yang dapat digunakan untuk melakukan proses ekstraksi pesan yaitu membaca pesan yang ada pada media gambar yang sudah disisipkan pesan dengan beberapa tahapan. Jika pengguna mengklik menu ektrasi pesan, makan akan muncul form ektraksi pesan.

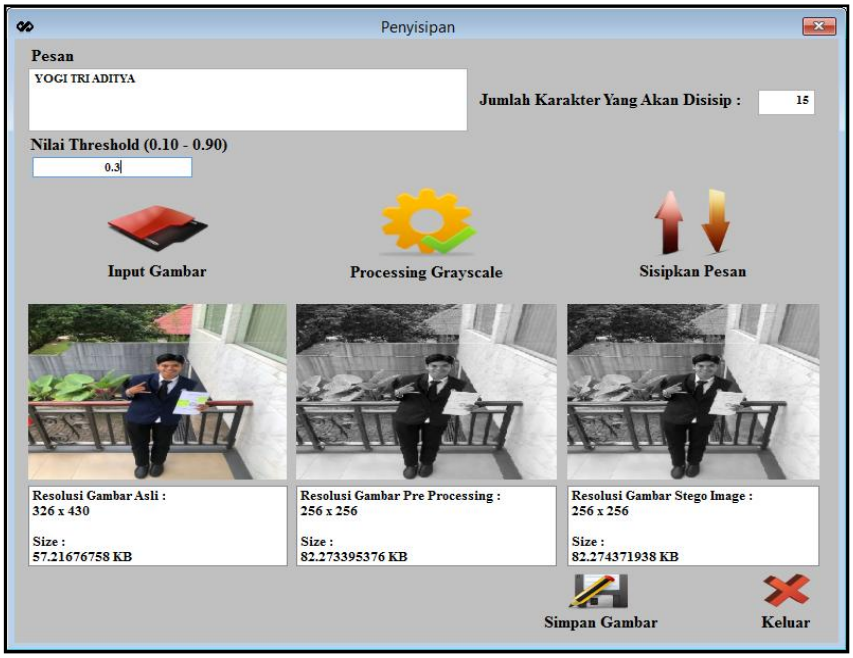
c. Exit, merupakan sub menu yang dapat digunakan untuk user untuk menutup program aplikasi



Gambar 3 Tampilan Form Utama

2. Tampilan Form Penyisipan Pesan

Form penyisipan pesan merupakan form yang digunakan melakukan penyisipan pesan rahasia kedalam media gambar.



Gambar 4 Tampilan Form Penyisipan Pesan

Pada penyisipan pesan terdapat beberapa tombol yang memiliki fungsi sebagai berikut ini :

a. Input Gambar, merupakan tombol yang digunakan untuk menginput media gambar yang akan digunakan.
b. Precessing Grayscale, merupakan tombol yang digunakan untuk melakukan perubahan pada media gambar.
c. Sisipkan Pesan, merupakan tombol yang digunakan untuk melakukan penyisipan pesan kedalam media gambar.
d. Simpan Gambar, merupakan tombol yang digunakan untuk menyimpan gambar hasil penyisipan pesan.
e. Keluar, merupakan tombol yang digunakan untuk keluar dari form penyisipan pesan

3. Tampilan Form Extraksi Pesan

Form ektraksi pesan merupakan form yang digunakan melakukan ektraksi pesan yang ada pada media gambar sehingga dapat diketahui pesan yang tersembunyi didalam gambar tersebut. Pada penyisipan pesan terdapat beberapa tombol yang memiliki fungsi sebagai berikut ini :

a. Input Stegano Gambar, merupakan tombol yang digunakan untuk menginput media gambar yang sudah disisipkan pesan rahasia didalam gambar tersebut.
b. Ekstrak Pesan, merupakan tombol yang digunakan untuk melakukan pembacaan pesan yang ada didalam media gambar yang sudah disisipkan pesan.
c. Keluar, erupakan tombol yang digunakan untuk keluar dari form ekstraksi pesan.



Gambar 5 Tampilan Form Ektraksi Pesan

KESIMPULAN

Berdasarkan hasil perancangan aplikasi keamanan data pengiriman pesan rahasia menggunakan media gambar dengan metode BPCS (Bit-plane Complexity Segmentation) ini, penulis dapat menarik kesimpulan sebagai berikut:

1. Steganografi dengan metode BPCS dapat diterapkan pada citra JPEG tanpa adanya modifikasi pada proses penyisipan sampai proses ekstraksi pesan.
2. Proses rancang bangun sistem pengiriman pesan rahasia pada media gambar menggunakan alat bantu dalam perancangan sistem menggunakan UML (Unified Modeling Language) sehingga memudahkan dalam proses menganalisa setiap kebutuhan-kebutuhan dalam membangun sistem informasi berbasis.

REFERENCES

Habibi Z. (2018). Implementasi Metode Bit Plane Complexity Segmentation pada Citra Digital dalam Penyembunyian Pesan Rahasia. *MEANS (Media Informasi Analisa Dan Sistem)*, *3*(2), 159–165.

Ifan Rizqa, & Safitri, A. N. (2022). Kriptostegano Menggunakan Data Encryption Standard dan Least Significant Bit dalam Pengamanan Pesan Gambar. *Jurnal Masyarakat Informatika*, *13*(2), 111–120.

Kholifah, S. B. N., & SitiNurmiati. (2022). Rancangbangun Sisteminformasi Pemesananjasa Make-Up Artist(Mua) Berbasis Web. *Jurnal Rekayasa Informasi*, *11*(2), 146–152.

Laksmi, Gani, & Budiantoro. (2015). *Manajemen perkantoran modern*. Jakarta: Rajawali Pers.

M, W. H., & Ramli, H. (2023). Analisa Clustering PhisingUntuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar. *Vokatek*, *1*(1), 28–33.

Ratnasari, A. P., & Dwiyanto, F. A. (2020). Metode steganografi citra digital. *Sains, Aplikasi, Komputasi Dan Teknologi Informasi*, *2*(2), 52–56.

Santoso, S., & Nurmalina, R. (2017). Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas. *Jurnal Integrasi*, *9*(1), 84. https://doi.org/10.30871/ji.v9i1.288

Widyastuti, R., & Widiyastuti, A. A. (2022). Penerapan Sistem Informasi Akademik Di Smk Yaspen Jakarta. *PROSISKO*, *9*(2), 9–24.