

Aplikasi Penyembunyian Pesan Pada File-File Dokumen Berekstensi .Xls/Xlsx Dengan Metode Modulus Function

Indarmawati Zai*

Program Studi Fakultas Teknik Informatika Universitas Budi Darma Medan

Email: indarmawatizai02@gmail.com

Email Penulis Korespondensi: indarmawatizai02@gmail.com

Abstrak—Pengamanan pesan merupakan salah satu hal yang sangat penting, dikarenakan menghindari pencurian file penting dari pihak yang tidak berwenang. Steganografi adalah salah satu cara untuk menyembunyikan pesan atau penyisipan pesan ke media lain, agar orang lain tidak mengetahui informasi keasliannya.

Diperlukan suatu metode agar data tersebut tidak hilang atau utuh sampai tujuan dalam hal penyimpanan data diperlukan suatu keamanan agar data yang disimpan tidak dapat dibuka, dibaca bahkan diambil oleh orang yang bukan haknya untuk mencoba membukanya. Untuk dapat menyembunyikan pesan namun tidak mengubah wadah dari penampungnya maka diperlukan suatu metode dalam steganografi yang dapat melakukan hal tersebut. Metode Modulus Function (MF) adalah teknik penyisipan pesan yang dilakukan melalui modifikasi nilai sisa hasil bagi (remainder) metode ini menggunakan kuatisasi selisih nilai keabuan untuk menentukan jumlah bit yang akan disisipkan pada selisih nilai tertentu. Kelebihan metode modulus function ini adalah mampu mengurangi perubahan nilai koefisien (coefficient adjustment) sehingga mampu mempertahankan kualitas dari wadah penampung. Sehingga dalam tahap pengujian dengan Software Binary viewer. Dapat membantu dalam Penyembunyian pesan pada File Dokumen

Kata Kunci: Steganografi, Metode Modulus Function (MF) File Dokumen, Aplikasi Pesan Pada File Dokumen, Binary viewer

Abstract—Securing messages is a very important thing, because it avoids theft of important files from unauthorized parties. Steganography is a way of hiding messages or inserting messages into other media, so that other people do not know the authenticity of the information.

A method is needed so that the data is not lost or is intact until it reaches its destination. In terms of data storage, security is needed so that the stored data cannot be opened, read or even taken by someone who does not have the right to try to open it. To be able to hide messages but not change the container that contains them, a steganography method is needed that can do this. The Modulus Function (MF) method is a message insertion technique that is carried out by modifying the residual value of the quotient (remainder). This method uses quantization of the gray value difference to determine the number of bits to be inserted at a certain value difference. The advantage of this modulus function method is that it is able to reduce changes in coefficient values (coefficient adjustment) so that it is able to maintain the quality of the storage container. So it is in the testing stage with Binary viewer software. Can help in hiding messages in document files

Keywords: Steganography, Modulus Function (MF) Method for Document Files, Message Application in Document Files, Binary viewer

1. PENDAHULUAN

Latar belakang aplikasi penyembunyian pesan pada file-file dokumen adalah keperluan untuk mengamankan informasi yang penting dari pengguna. Dengan aplikasi penyembunyian, informasi tersebut dapat disimpan dalam file dokumen yang dapat disembunyikan dengan cara menyisipkan pesan rahasia dalam file-file dokumen. Ini berguna untuk menjamin keamanan data dan menghindari penggunaan data oleh pihak yang tidak berwenang.

Aplikasi penyembunyian pesan pada file-file dokumen menggunakan metode steganografi, dimana pesan rahasia disembunyikan dalam file dokumen dengan cara menyisipkan data yang tidak terlihat pada aplikasi kompresi. File dokumen dienkripsi terlebih dahulu menggunakan algoritma AES, lalu disisipkan dengan data yang akan disembunyikan. File-file dokumen yang biasanya digunakan sebagai cover file adalah file gambar, file audio, atau file video, karena tidak menimbulkan kecurigaan orang lain ketika membukanya. File ZIP dapat juga digunakan sebagai cover file, karena banyak digunakan untuk pertukaran informasi dan dapat menghasilkan file enkripsi lebih kecil dengan dilakukan proses kompresi.

Metode steganografi yang digunakan adalah metode End of File (EOF), dimana pesan rahasia disembunyikan dengan cara menambahkan bit-bit pesan yang akan disembunyikan ke akhir file citra penampung. Ini tidak akan mengganggu kualitas data awal yang akan disisipkan pesan, namun membuat data yang disembunyikan tidak rusak jika dilakukan operasi pengolahan citra. [1]–[3]

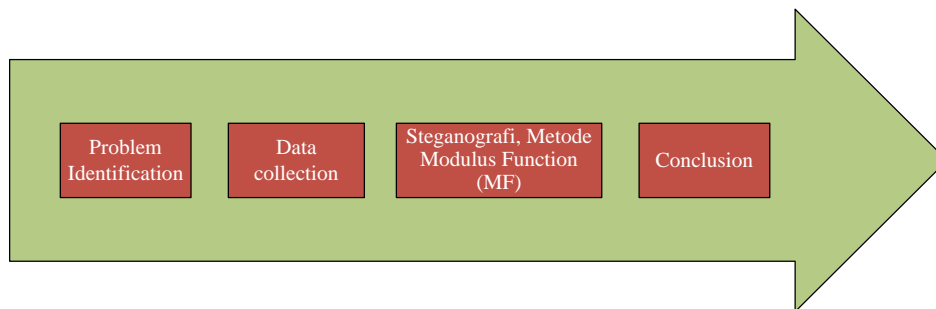
Aplikasi penyembunyian pesan pada file-file dokumen dapat meningkatkan kerahasiaan karena menggunakan kata sandi, menggunakan algoritma kriptografi, dan menggunakan metode steganografi. Ini dapat berguna untuk menyimpan informasi penting yang tidak boleh diakses oleh pihak yang tidak berwenang, seperti perusahaan, perbankan, dan pemerintah. Seiring dengan majunya perkembangan teknologi, banyak tersedia berbagai macam teknik untuk dapat melindungi pesan atau informasi yang dirahasiakan dari orang yang tidak berhak untuk mengakses pesan tersebut seperti pencurian atau percobaan hacking. Dengan berkembangnya teknologi sering kita mendengar atau melihat bahwa pesan-pesan rahasia yang ingin kita kirimkan kepada seseorang telah dilakukan pencurian atau penyadapan oleh orang yang tidak berhak atau orang yang tidak bertanggung jawab.

Maka dari itu dalam pengiriman/ penerimaan informasi, pengguna membutuhkan suatu jaminan keamanan yang dapat meyakinkan bahwa yang diperoleh adalah informasi yang aman dan benar. Sehingga dapat mempersulit para pihak yang tidak bertanggung jawab akan kejahatan komputer.

Untuk itu menjaga kerahasiaan informasi dapat digunakan teknik steganography. Informasi yang akan dikirim disembunyikan dalam file digital (teks, image, audio, video). Kemudian data digital tersebut dikirim seperti data biasa, sehingga pihak ketiga tidak curiga bahwa didalamnya terdapat informasi rahasia. Informasi yang disembunyikan dalam data digital tersebut dapat diekstrak kembali oleh penerima pesan. Informasi tersebut juga harus sama dengan informasi sebelum disisipkan dalam data digital, meskipun data digital tersebut telah mengalami proses manipulasi, seperti pengeditan, pemotongan atau kompresi.

2. METODOLOGI PENELITIAN

2.1 Alur Penelitian



Dalam penelitian ini, berbagai langkah telah dilakukan oleh penulis. Tahapan pengumpulan data yang digunakan untuk memperoleh informasi yang diperlukan mencakup langkah-langkah berikut:

1. Identifikasi Masalah
Pada fase awal ini dilakukan pemecahan masalah dan analisis pola yang terdapat dalam data sebelum proses perancangan dimulai..
2. Pengumpulan Data
Langkah kedua melibatkan pengumpulan data yang dilakukan melalui beberapa metode, termasuk observasi yang bertujuan untuk menetapkan kriteria calon dosen dengan kinerja terbaik..
3. Pengolahan data dengan Steganografi, Metode Modulus Function (MF)
Pada langkah ini, dilakukan analisis penelitian setelah data yang diperlukan terkumpul. Analisis dimulai dengan memeriksa masalah dalam penilaian calon karyawan baru, termasuk evaluasi sistem lama yang masih manual. Selanjutnya, dilakukan analisis terhadap sistem baru yang menggunakan metode Steganografi, Metode Modulus Function (MF) dalam proses perhitungannya
4. Kesimpulan dan Saran
terakhir melibatkan penarikan kesimpulan dari keseluruhan proses penelitian ini. Ini melibatkan evaluasi terhadap apakah hipotesis awal yang diajukan sesuai dengan hasil penelitian serta menjadi inti dari keseluruhan hasil penelitian ini.

2.2 Manfaat Steganografi

Manfaat steganografi yang umum diketahui adalah mengamankan informasi rahasia dalam lalu lintas jaringan komunikasi. Ada banyak Negara yang warga Negaranya tidak bebas dalam berbicara ataupun mengeluarkan pendapat layaknya Negara demokratis. Maka steganografi dapat menjadi sebuah solusi yang memungkinkan terjadinya pertukaran informasi dan berita tanpa disensor dan tanpa perlu khawatir pesan tersebut disadap.

2.3 Karakteristik Steganografi

Dalam steganografi dikenal data hiding atau data embedding, merupakan rangkaian proses dalam menyembunyikan data kedalam berbagai media, seperti citra, audio atau teks dengan meminimalisir penampakan degradasi sinyal media panampung. Hal ini tampak familiar dengan enkripsi.

Penyisipan data rahasia kedalam media digital harus memperhatikan beberapa aspek keamanan sebagai berikut:

1. Fidelity
2. Recovery
3. Robustness
4. Security

2.3 File

File adalah kumpulan dari data dan informasi yang saling berhubungan dan juga tersimpan di dalam ruang penyimpanan sekunder yang dapat juga diartikan sebagai arsip atau data yang tersimpan di dalam komputer.

Jenis – Jenis File

- 1. File System
- 2. File Video
- 3. File Dokumen
- 4. File Gambar
- 5. File Suara

2.4 Xls atau Xlsx

Xlsx merupakan file Microsoft Excel Open XML Spreadsheet (XLSX) yang dibuat oleh Microsoft Excel. Dapat membuka format bentuk file tersebut selain dari Excel, Pada aplikasi spreadsheet lainnya, termasuk Apple Numbers, Google Docs, dan OpenOffice. Mereka disimpan sebagai file Zip terkompresi, yang berisi banyak file lain yang Jenis file tersebut pertama kali diperkenalkan pada Microsoft Office 2007 dalam standar Office Open XML, XLSX adalah format default saat membuat spreadsheet menggunakan versi Excel modern. Microsoft memperkenalkan format terbuka ini terutama karena meningkatnya persaingan dari Open Office dan Open Document Format (ODF). Format XLSX menggantikan format XLS eksklusif yang digunakan Excel sebelumnya digunakan untuk membuka dokumen. sesudahnya. Salah satu kendala yang ada sementara ini untuk format file terbaru (docx) adalah terkait kompatibilitas.

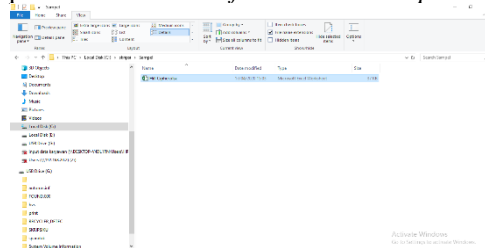
2.5 Modulus Funtion (MF)

Metode ini merupakan pengembangan dari metode PVD. Proses penyembunyian pesan dilakukan melalui modifikasi nilai sisa hasil bagi (remainder) dari piksel bertetangga. Sama seperti metode PVD, metode ini menggunakan kuantisasi selisih nilai keabuan untuk menentukan jumlah bit yang akan disisipkan pada selisih nilai tertentu.

3. HASIL DAN PEMBAHASAN

3.1 Analisa

Contoh kasus yang digunakan dalam penelitian ini adalah file *Excel Hill Cipher.xlsx* seperti pada gambar berikut:



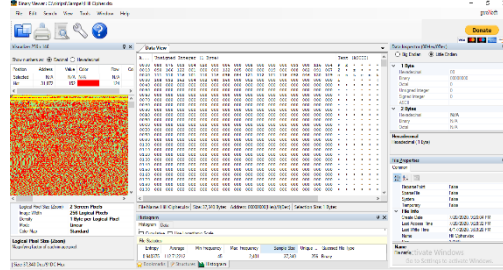
Gambar 1 Sampel file Excel berekstensi .xls/xlsx

Contoh kasus:

Misalnya akan dilakukan penyisipan pesan “16110501” pada file excel sampel di atas dengan menerapkan metode *Modulus Function*.

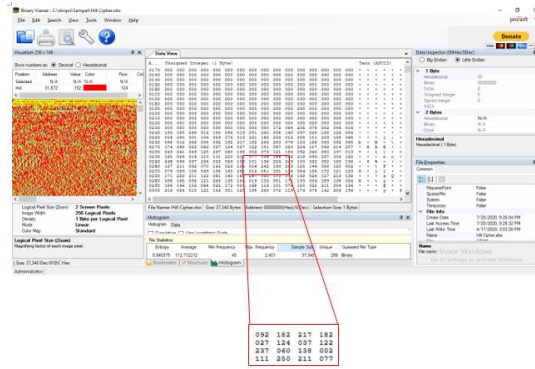
Adapun langkah-langkah penyelesaiannya adalah sebagai berikut :

- 1. Dengan menggunakan aplikasi *Binary Viewer* maka diperoleh nilai biner dari file sampel adalah sebagai berikut :



Gambar 3.2 Nilai decimal file sampel

- 2. Sesuai dengan nilai decimal file sampel di atas, maka akan diambil file stego berukuran 4x4 piksel untuk dilakukan penyisipan pesan seperti pada gambar berikut ini:



Gambar 3.3 File stego ukuran 4x4 piksel

3. Selanjutnya pesan akan disisipi dengan pesan pada nilai biner stego yang berukuran 4x4 piksel berikut:

Nilai Desimal Stego			
92	182	217	182
27	124	37	122
237	69	138	2
111	250	211	77

Gambar 3. 4 Nilai decimal file stego

A. Proses Embedding / Penyisipan

Pesan “16110501” dengan Metode Modulus Function:

Iterasi 1

1. Ubah pesan menjadi bilangan biner.

Pesan “16110501” diubah jadi biner = 1111 0101 1101 0011 1010 0101

2. Hitung selisih 2 piksel bertetangga (g_i', g_{i+1})

$$d_i = |g_{i+1} - g_i|$$

$$d_i = |182 - 92| = 90$$

3. Tentukan batas bawah (I_k) dan jumlah bit n , dengan cara:

$$I_k \leq d_i < I_{k+1}$$

$$64 \leq d_i < 127, n = 6, I_k = 64, 2^n = 64$$

4. Ambil pesan sebanyak n bit, kemudian ubah menjadi desimal (b)

$b = 1111 01 = 61$, sisa pesan = 01 1101 0011 1010 0101

5. Hitung nilai sisa hasil bagi (*remainder*)

$$r = (g_i + g_{i+1}) \bmod 2^n$$

$$r = (92 + 182) \bmod 64$$

$$r = 274 \bmod 64$$

$$r = 18$$

6. Hitung : $m = |r - b|$ dan $m' = |2^n - m|$

$$m = |r - b|$$

$$m = |18 - 61|$$

$$m = 43$$

$$m' = |2^n - m|$$

$$m' = |64 - 43|$$

$$m' = 21$$

7. Tentukan nilai piksel baru (g_i', g_{i+1}').

$r = 18, b = 61, m = 43, \frac{I_k}{2} = 32, g_i = 92, g_{i+1} = 182$, maka yang memenuhi syarat adalah :

Jika $r \leq b$ dan $m > \frac{2^n}{2}$ dan $g_i < g_{i+1}'$ maka

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

$$(g_i', g_{i+1}') = (92 - \lfloor \frac{21}{2} \rfloor, 182 - \lfloor \frac{21}{2} \rfloor)$$

$$(g_i', g_{i+1}') = (92 - 10.5, 182 - 10.5)$$

$$(g_i', g_{i+1}') = (81.5, 171.5)$$

92	182	217	182
27	124	37	122
237	69	138	2
111	250	211	77

⇒

81.5	171.5	217	182
27	124	37	122
237	69	138	2
111	250	211	77

Iterasi 2

- 1) Sisa Pesan = 01 1101 0011 1010 0101
- 2) Hitung selisih 2 piksel bertetangga (g_i', g_{i+1})
 $d_i = |g_{i+1} - g_i|$
 $d_i = |182 - 217| = 35$
- 3) Tentukan batas bawah (I_k) dan jumlah bit n , dengan cara:
 $I_k \leq d_i < I_{k+1}$
 $32 \leq d_i < 63, n = 5, I_k = 32, 2^n = 32$
- 4) Ambil pesan sebanyak n bit, kemudian ubah menjadi desimal (b)
 $b = 01 110 = 14$, sisa pesan = 1 0011 1010 0101
- 5) Hitung nilai sisa hasil bagi (*remainder*)
 $r = (g_i + g_{i+1}) \bmod 2^n$
 $r = (217 + 182) \bmod 32$
 $r = 399 \bmod 32$
 $r = 15$
- 6) Hitung : $m = |r - b|$ dan $m' = |2^n - m|$
 $m = |r - b|$
 $m = 15 - 14$
 $m = 1$

 $m' = |2^n - m|$
 $m' = |2^5 - (1)|$
 $m' = |32 - 1|$
 $m' = 31$
- 7) Tentukan nilai piksel baru (g_i', g_{i+1}').
 $r = 15, b = 14, m = 1, \frac{I_k}{2} = 16, g_i = 217, g_{i+1} = 182$, maka yang memenuhi syarat adalah :
 Jika $r > b$ dan $m \leq \frac{2^n}{2}$ dan $g_i \geq g_{i+1}'$ maka
 $(g_i', g_{i+1}') = (g_i - \lfloor \frac{m}{2} \rfloor, g_{i+1} - \lfloor \frac{m}{2} \rfloor)$
 $(g_i', g_{i+1}') = (217 - \lfloor \frac{1}{2} \rfloor, 182 - \lfloor \frac{1}{2} \rfloor)$
 $(g_i', g_{i+1}') = (217 - 0.5, 182 - 0.5)$
 $(g_i', g_{i+1}') = (216.5, 181.5)$

92	182	217	182
27	124	37	122
237	69	138	2
111	250	211	77

→

81.5	171.5	216.5	181.5
27	124	37	122
237	69	138	2
111	250	211	77

Iterasi 3

- 1) Sisa Pesan = 1 0011 1010 0101
- 2) Hitung selisih 2 piksel bertetangga (g_i', g_{i+1})
 $d_i = |g_{i+1} - g_i|$
 $d_i = |124 - 27| = 97$
- 3) Tentukan batas bawah (I_k) dan jumlah bit n , dengan cara:
 $I_k \leq d_i < I_{k+1}$
 $64 \leq d_i < 127, n = 6, I_k = 64, 2^n = 64$
- 4) Ambil pesan sebanyak n bit, kemudian ubah menjadi desimal (b)
 $b = 1 00111 = 39$, sisa pesan = 010 0101
- 5) Hitung nilai sisa hasil bagi (*remainder*)
 $r = (g_i + g_{i+1}) \bmod 2^n$
 $r = (27 + 124) \bmod 64$
 $r = 151 \bmod 64$
 $r = 23$
- 6) Hitung : $m = |r - b|$ dan $m' = |2^n - m|$
 $m = |r - b|$
 $m = 23 - 39$
 $m = 16$

 $m' = |2^n - m|$

$$m' = |2^6 - (16)|$$

$$m' = |64 - 16|$$

$$m' = 48$$

7) Tentukan nilai piksel baru (g_i', g_{i+1}').

$r = 23, b = 39, m = 16, \frac{I_k}{2} = 32, g_i = 27, g_{i+1} = 124$, maka yang memenuhi syarat adalah :

Jika $r \leq b$ dan $m \leq \frac{2^n}{2}$ dan $g_i \leq g_{i+1}'$ maka

$$(g_i', g_{i+1}') = (g_i + \lfloor \frac{m}{2} \rfloor, g_{i+1} + \lfloor \frac{m}{2} \rfloor)$$

$$(g_i', g_{i+1}') = (27 + \lfloor \frac{16}{2} \rfloor, 124 + \lfloor \frac{16}{2} \rfloor)$$

$$(g_i', g_{i+1}') = (27 + 8, 124 + 8)$$

$$(g_i', g_{i+1}') = (35, 132)$$

92	182	217	182	81.5	171.5	215	180
27	124	37	122	35	132	37	122
237	69	138	2	237	69	138	2
111	250	211	77	111	250	211	77

Iterasi 4

1) Sisa Pesan = 010 0101

2) Hitung selisih 2 piksel bertetangga (g_i', g_{i+1})

$$d_i = |g_{i+1} - g_i|$$

$$d_i = |122 - 37| = 85$$

3) Tentukan batas bawah (I_k) dan jumlah bit n , dengan cara:

$$I_k \leq d_i < I_{k+1}$$

$$64 \leq d_i < 127, n = 6, I_k = 64, 2^n = 64$$

4) Ambil pesan sebanyak n bit, kemudian ubah menjadi desimal (b)

$$b = 010 010 = 18, \text{ sisa pesan} = 1$$

5) Hitung nilai sisa hasil bagi (*remainder*)

$$r = (g_i + g_{i+1}) \bmod 2^n$$

$$r = (37 + 122) \bmod 64$$

$$r = 159 \bmod 64$$

$$r = 31$$

6) Hitung : $m = |r - b|$ dan $m' = |2^n - m|$

$$m = |r - b|$$

$$m = 31 - 18$$

$$m = 13$$

$$m' = |2^n - m|$$

$$m' = |64 - 13|$$

$$m' = 51$$

7) Tentukan nilai piksel baru (g_i', g_{i+1}').

$r = 31, b = 18, m = 13, \frac{I_k}{2} = 32, g_i = 37, g_{i+1} = 122$, maka yang memenuhi syarat adalah :

Jika $r > b$ dan $m \leq \frac{2^n}{2}$ dan $g_i < g_{i+1}'$ maka

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

$$(g_i', g_{i+1}') = (37 - \lfloor \frac{13}{2} \rfloor, 122 - \lfloor \frac{13}{2} \rfloor)$$

$$(g_i', g_{i+1}') = (37 - 6.5, 122 - 6.5)$$

$$(g_i', g_{i+1}') = (30.5, 115.5)$$

92	182	217	182	81.5	171.5	215	180
27	124	37	122	35	132	30.5	115.5
237	69	138	2	237	69	138	2
111	250	211	77	111	250	211	77

Iterasi 5

1) Sisa Pesan = 1

2) Hitung selisih 2 piksel bertetangga (g_i', g_{i+1})

$$d_i = |g_{i+1} - g_i|$$

$$d_i = |69 - 237| = 168$$

- 3) Tentukan batas bawah (I_k) dan jumlah bit n , dengan cara:

$$I_k \leq d_i < I_{k+1}$$

$$128 \leq d_i < 255, n = 7, I_k = 128, 2^n = 128$$

- 4) Ambil pesan sebanyak n bit, kemudian ubah menjadi desimal (b)

$$b = 1 = 1, \text{ sisa pesan} = 1$$

- 5) Hitung nilai sisa hasil bagi (*remainder*)

$$r = (g_i + g_{i+1}) \text{ mod } 2^n$$

$$r = (237+69) \text{ mod } 128$$

$$r = 306 \text{ mod } 128$$

$$r = 50$$

- 6) Hitung : $m = |r - b|$ dan $m' = |2^n - m|$

$$m = |r - b|$$

$$m = 50 - 1$$

$$m = 49$$

$$m' = |2^n - m|$$

$$m' = |2^7 - (49)|$$

$$m' = |128 - 49|$$

$$m' = 79$$

- 7) Tentukan nilai piksel baru (g'_i, g'_{i+1}).

$r = 50, b = 1, m = 49, \frac{I_k}{2} = 128, g_i = 237, g_{i+1} = 69$, maka yang memenuhi syarat adalah :

Jika $r > b$ dan $m \leq \frac{2^n}{2}$ dan $g_i \geq g_{i+1}'$ maka

$$(g'_i, g'_{i+1}) = (g_i - \lfloor \frac{m}{2} \rfloor, g_{i+1} - \lfloor \frac{m}{2} \rfloor)$$

$$(g'_i, g'_{i+1}) = (237 - \lfloor \frac{49}{2} \rfloor, 69 - \lfloor \frac{49}{2} \rfloor)$$

$$(g'_i, g'_{i+1}) = (237 - 24.5, 69 - 24.5)$$

$$(g'_i, g'_{i+1}) = (212.5, 44.5)$$

92	182	217	182	81.5	171.5	215	180
87	124	87	122	35	132	30.5	115.5
237	69	138	2	212.5	44.5	138	2
111	250	211	77	111	250	211	77

B. Proses Extraction
Iterasi 1

81.5	171.5	215	180
35	132	30.5	115
82	72	138	2
111	250	211	77

- 1) Hitung selisih 2 piksel bertetangga (g'_i, g'_{i+1})

$$d_i = |g'_{i+1} - g'_i|$$

$$d_i = |171.5 - 81.5| = 90$$

- 2) Tentukan batas bawah (I_k) dan jumlah bit n , dengan cara:

$$I_k \leq d_i < I_{k+1}$$

$$64 \leq d_i < 127, n = 6, 2^n = 64$$

- 3) Hitung nilai sisa hasil bagi (*remainder*)

$$b_1 = (g'_i + g'_{i+1}) \text{ mod } 2^n$$

$$b_1 = (81.5 + 171.5) \text{ mod } 64$$

$$b_1 = 253 \text{ mod } 64$$

$$b_1 = 61 = 111101 \text{ (6 bit)}$$

Iterasi 2

81.5	171.5	216.5	181.5
130	33	53	138
82	72	138	2
111	250	211	77

- 1) Hitung selisih 2 piksel bertetangga (g'_i, g'_{i+1})

$$d_i = |g'_{i+1} - g'_i|$$

$$d_i = |181.5 - 216.5| = 35$$

- 2) Tentukan batas bawah (I_k) dan jumlah bit n , dengan cara:

$$I_k \leq d_i < I_{k+1}$$

$$32 \leq d_i < 63, n = 5, 2^n = 32$$

3) Hitung nilai sisa hasil bagi (*remainder*)

$$b_2 = (g_i + g_{i+1}) \text{ mod } 2^n$$

$$b_2 = (216.5 + 181.5) \text{ mod } 32$$

$$b_2 = 398 \text{ mod } 32$$

$$b_2 = 14 = 1101 \text{ (4 bit)}$$

Iterasi 3

81.5	171.5	215	180
35	132	53	38
82	72	138	2
111	250	211	77

1) Hitung selisih 2 piksel bertetangga ($g_{x'}, g_{i+1}$)

$$d_i = |g_{i+1} - g_i|$$

$$d_i = |123 - 35| = 97$$

2) Tentukan batas bawah (I_k) dan jumlah bit n , dengan cara:

$$I_k \leq d_i < I_{k+1}$$

$$64 \leq d_i < 127, n = 6, 2^n = 64$$

3) Hitung nilai sisa hasil bagi (*remainder*)

$$b_3 = (g_i + g_{i+1}) \text{ mod } 2^n$$

$$b_3 = (35 + 132) \text{ mod } 64$$

$$b_3 = 167 \text{ mod } 64$$

$$b_3 = 39 = 100111 \text{ (6 bit)}$$

Iterasi 4

81.5	171.5	215	180
35	132	30.5	115.5
82	72	138	2
111	250	211	77

1) Hitung selisih 2 piksel bertetangga ($g_{x'}, g_{i+1}$)

$$d_i = |g_{i+1} - g_i|$$

$$d_i = |132 - 35| = 97$$

2) Tentukan batas bawah (I_k) dan jumlah bit n , dengan cara:

$$I_k \leq d_i < I_{k+1}$$

$$64 \leq d_i < 127, n = 6, 2^n = 64$$

3) Hitung nilai sisa hasil bagi (*remainder*)

$$b_4 = (g_i + g_{i+1}) \text{ mod } 2^n$$

$$b_4 = (35 + 132) \text{ mod } 64$$

$$b_4 = 167 \text{ mod } 64$$

$$b_4 = 39 = 100111 \text{ (4 bit)}$$

Iterasi 5

81.5	171.5	215	180
35	132	30.5	115.5
212.5	44.5	138	2
111	250	211	77

1) Hitung selisih 2 piksel bertetangga ($g_{x'}, g_{i+1}$)

$$d_i = |g_{i+1} - g_i|$$

$$d_i = |44.5 - 212.5| = 186$$

2) Tentukan batas bawah (I_k) dan jumlah bit n , dengan cara:

$$I_k \leq d_i < I_{k+1}$$

$$128 \leq d_i < 255, n = 7, 2^n = 128$$

3) Hitung nilai sisa hasil bagi (*remainder*)

$$b_5 = (g_i + g_{i+1}) \text{ mod } 2^n$$

$$b_5 = (212.5 + 44.5) \text{ mod } 128$$

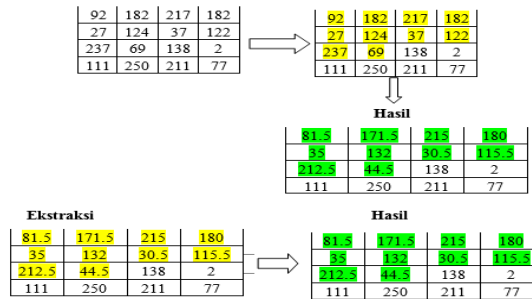
$$b_5 = 257 \text{ mod } 128$$

$$b_5 = 1 = 1 \text{ (1 bit)}$$

$$\text{Maka } B_1 U B_2 B_1 U B_3 U B_4 U B_5 = 111101011101001110100101 = 16110501$$

Dari proses penyisipan dan ekstraksi pesan dengan menerapkan metode *Modulus Function* di atas diperoleh kesimpulan bahwa pesan yang disisipkan (*embedding*) akan kembali ke bentuk semula ketika dilakukan ekstraksi (*Extraction*)

Piksel Embending



4. KESIMPULAN

Dari hasil penelitian dan pembahasan pada bab-bab sebelumnya, maka penulis dapat mengambil suatu kesimpulan sebagai berikut: Dalam pengembangan steganografi terdapat dua algoritma penting yaitu untuk melakukan Embedding dan satu lagi untuk melakukan ekstraksi. Proses embedding merupakan proses untuk menyembunyikan pesan rahasia (secret message) kedalam cover work yang berupa file document maupun teks sebagai media untuk menyembunyikan pesan.. Metode Modulus Function (MF) merupakan metode steganografi yang sederhana dan mudah diimplementasikan. . Metode Modulus Function (MF) Dapat digunakan untuk Penyembunyian pesan suatu data teks kedalam suatu dokumen sehingga dapat disembunyikan dan tidak terlihat oleh orang yang tidak berhak melihatnya.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

REFERENCES

- [1] A. Karim, S. Esabella, K. Kusmanto, S. Suryadi, and E. Purba, "Penerapan Metode Teorema Bayes Dalam Mendiagnosa Penyakit Autoimun," *Build. Informatics, Technol. Sci.*, vol. 5, no. 1, pp. 254–263, 2023, doi: 10.47065/bits.v5i1.3407.
- [2] A. Karim, "Implementation of the Multi-Objective Optimization Method on the Basic of Ratio Analysis (MOORA) and Entropy Weighting in New Employee Recruitment," vol. 5, no. 2, pp. 704–712, 2024, doi: 10.47065/josh.v5i2.4859.
- [3] A. Karim, S. Esabella, M. A. Hanafiah, and ..., "Sistem Pakar Deteksi Penyakit Otitis dengan Perbandingan Metode Certainty Factor, Teorema Bayes, dan Dempster Shafer," *J. Media ...*, vol. 7, pp. 2003–2013, 2023, doi: 10.30865/mib.v7i4.6595.
- [4] R. H. Harahap, N. A. Hasibuan, dan I. Saputra, "penerapan metode modulus function (MF) untuk penyisipan pesan pada citra digital," komik (konferensi Nas. Teknol. Inf. dan Komput., vol. 3, no. 798–807, 2019.
- [5] R. Purba, I. A. Pardosi, H. Darmawan, dan A. A. Sitorus, "pengamanan data teks dengan NTRU dan Modulus Function pada koefision IHWT citra warna," vol. 20, no. 1, hal. 59–70, 2019.
- [6] I. Martono, "PENGGUNAAN STEGANOGRAFI DENGAN METODE END OF FILE (EOF) PADA DIGITAL WATER MARKING," vol. 2, hal. 37, 2013.
- [7] R. Tullah et al., "Perancangan Steganografi Dengan Media Gambar Pada Aplikasi Berbasis Android," vol. 4, no. 2, hal. 1–7, 2014.
- [8] M. K. T. Sutoyo, S.Si., M. K. Edy Mulyono, S.Si., D. V. Suhartono, M. Oky Dwi Nurhayati, dan M. K. Wijanarto, No Title. 2019.
- [9] A. M. ali akbar lubis, Ng poi Wong, Irfan Arfiandi, Immanuel Damanik, "Steganografi pada Citra" *Jurnal Ilmu Komputer dan informatika*, vol. 16, hal. 02, 2015.
- [10] Rama Dasaratha V/ Frederick L. Jones., *Sistem Informasi Akuntansi*. Jakarta., 2008.
- [11] Jogiyanto Hartono, *Analisis & Desain Sistem Informasi*. Yogyakarta, 2005.
- [12] s. s. M. m.Primananda Arif Aditya, *dasar-dasar pemrograman database desktop dengan visual basic.net 2008*. jakarta: pt. elex media komputindo, 2013.