Jurnal Teknologi Komputer dan Informasi (JUTEKINF)
Vol. 11, No. 1, Januari-Juni 2023, Hal. 1-9

Implementasi *Watermarking* Desain Citra Menggunakan Metode Modifikasi *End Of File* (MEOF)

Cut Mala Azzura[1], Merina Pratiwi[2], Desyanti[3]
[1,2,3]Sekolah Tinggi Teknologi Dumai
[1,2,3)] Program Studi Teknik Industri, Sekolah Tinggi Teknologi Dumai
Email: azzuramala@gmail.com[1], merinapratiwi1920@gmail.com[2], desyanti734@gmail.com[3]

Abstract

Communication and information technology is growing rapidly and has a major influence on all human life. For example, the development of internet technology that can present and unify various types of digital data, photo media, is an image. In this study, steganography is applied as a technique to hide information into data without revealing the existence of the information and raising suspicions that the data inserted with the information has changed. The current implementation of steganography has used digital media as a medium for storing messages or hiding messages, one of which is image media (digital image). In practice, most messages are hidden by making subtle changes to other digital data whose contents will not attract the attention of potential attackers. For example, a secret data is inserted in an image, but in the image there is no visible secret data. However, if it is extracted with a special software, it can be seen that there is secret data in the image. This research resulted in an Implementation of Steganography Implementation With End Of File Modification Method to insert watermarking text on image design that is able to provide security for secret messages that are complicated to solve.

Keywords *: MEOF, MSE, PSNR, Steganography*

Abstrak

Teknologi komunikasi dan informasi sangat berkembang dengan pesat dan memberikan pengaruh besar bagi seluruh kehidupan manusia. Sebagai contoh perkembangan teknologi internet yang dapat menyajikan dan mempersatukan berbagai jenis data digital, media foto, adalah citra atau image. Pada penelitian ini menerapkan steganografi sebagai salah satu teknik untuk menyembunyikan informasi ke dalam suatu data tanpa menampakkan keberadaan informasi tersebut dan menimbulkan kecurigaan bahwa data yang disisipi dengan informasi tersebut telah berubah. Implementasi steganografi saat ini telah menggunakan media digital sebagai media penampung atau penyembunyi pesan, salah satunya media gambar (citra digital). Pada prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial. Misalkan dalam suatu gambar disisipkan suatu data rahasia, tetapi pada gambar tersebut tidak terlihat data rahasia secara kasat mata. Akan tetapi, jika diekstrak dengan suatu software khusus maka terlihat bahwa terdapat data rahasia dalam gambar tersebut. Penelitian ini menghasilkan suatu Penerapan Implementasi *Watermarking* Dengan Metode Modifikasi *End Of File* untuk menyisipkan teks watermarking Pada design citra yang mampu memberikan keamanan pesan rahasia yang rumit untuk dipecahkan. Penelitian ini menghasilkan suatu Implementasi *Watermarking* Dengan Metode Modifikasi *End Of File* untuk Menyisipkan Pesan Teks Pada Citra yang sangat mampu memberikan proteksi keamanan pesan rahasia yang rumit untuk dipecahkan serta dapat diakses online oleh siapapun dengan situs https://app-ku.xyz/Mala.

Kata Kunci : MEOF, MSE, PSNR, Steganografi

1. PENDAHULUAN

Perkembangan teknologi terutama pada sistem pengamanan data dalam menjaga keamanan data informasi telah berkembang pesat. Pada saat tertentu informasi yang di kirimkan tidak ditujukan kepada semua orang namun di tujukan hanya kepada orang tertentu, ancaman terhadap keamanan informasi yang di butuhkan semakin besar, terutama untuk informasi yang di rahasiakan tersebut. Pada saat ini sudah terdapat banyak ancaman di dunia maya, misalnya saja seorang *hacker* yang mampu mengambil data atau informasi orang lain tanpa diketahui. Hal ini menimbulkan kekhawatiran bagi pemilik informasi rahasia tersebut. Kerahasiaan dan keamanan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan atau informasi melalui jaringan atau internet.

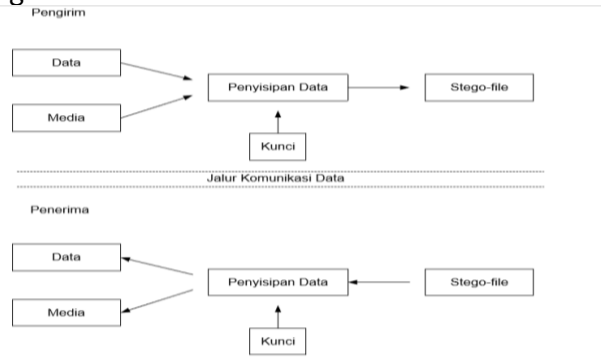
Adanya permasalah tersebut maka informasi yang akan dikirim dapat di jaga melalui teknik penyembunyian data. Salah satu teknik menyembunyikan informasi ini yaitu steganografi. Steganografi ini akan melakukan teknik menyembunyikan informasi yang bersifat pribadi di dalam informasi lainnya yang tidak bersifat rahasia. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, disinilah fungsi dari teknik steganografi yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas.

2. METODE

1. Steganografi

Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos* yang berarti tersembunyi atau terselubung dan I yang artinya menulis, sehingga arti steganografi adalah "menulis (tulisan) terselubung" (Jannah et al., 2018). Steganografi adalah ilmu menyembunyikan teks pada media lain yang telah ada sedemikian sehingga teks yang tersembunyi menyatu dengan media itu. Media tempat penyembunyian pesan dapat berupa media teks, gambar, audio atau video (Damanik, 2018).

Proses steganografi secara umum dengan media citra dapat dilihat pada Gambar yaitu sebagai berikut



Gambar 1.Proses Steganografi

Berdasarkan Gambar proses steganografi menggunakan media citra diawali dengan mengianput pesan dan *cover image* (citra yang digunakan sebagai media penyisipan). Selanjutnya dilakukan proses *embedding* (penanaman pesan kedalam citra), sehingga diperoleh stegi *image* citra yang telah disisipkan pesan). *Stego image* (citra yang sudah ditanam pesan rahasia) inilah yang akan dikirim ke penerima pesan. Penerima pesan melakukan *extraction* (proses pengeluaran pesan pada citra). Setelah melakukan proses *extraction*, maka pesan yang dikirim dapat dibaca. Penilaian sebuah algoritma steganografi yang baik dapat dinilai dari beberapa faktor yaitu (Cahyadi, 2019).

2. *End Of File*

Menurut Penilitian yang dilakukan oleh (Darwis, 2017) Metode ini merupakan metode pengembangan LSB. Dalam metode ini pesan disisipkan diakhir berkas. Teknik EOF atau *End Of File* merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut. Teknik inilah yang akan digunakan penulis dalam penelitian ini. Dalam teknik ini, data disisipkan pada akhir file dengan diberi tanda khusus sebagai pengenal *start* dari data tersebut dan pengenal akhir dari data tersebut.

Kelebihan dari metode *End Of File* yaitu tidak ada batasan dalam menambahkan informasi yang ingin disembunyikan, bahkan jika ukuran informasi itu melebihi ukuran citra penampung. Data informasi akan di sembunyikan/di sisipkan di akhir *file* sehingga *file image* mungkin akan tampak ada perubahan dengan aslinya. Jika dapat dilihat dengan mata, maka perubahan ini akan tampak di baris bawah dari *image*. Dalam metode *end of file* data yang akan di sisipkan akan diberikan penanda khusus untuk menandakan awal dan akhir data tersebut.

Cara Kerja Metode EOF

Konsep kerja metode *End of File* (EOF) dalam menyembunyikan pesan ke dalam citra digital adalah melakukan penambahan *pixel* baru setelah data akhir *pixel* dari citra *cover* (citra asli). Jumlah *pixel* yang ditambahkan sama dengan jumlah karakter pesan yang ingin disembunyikan dengan tidak merubah ukuran lebar dari citra *cover* (yang berubah hanyalah ukuran height dari citra). Bila jumlah kolom tidak terpenuhi, maka akan dilakukan penambahan *pixel* sejumlah kolom yang masih kurang pada baris. Proses penambahan *pixel* inilah yang menyebabkan terjadinya perubahan ukuran tinggi dari citra hasil (*stegano image*). Proses pengungkapan (*extraction*) pesan dari dalam stegano image dilakukan dengan mengambil nilai-nilai *pixel* yang baru ditambahkan kemudian dikonversi menjadi karakter.

a. Proses Embedding Pesan Berdasarkan Metode EOF.

Proses *embedding* (penyisipan) pesan dengan metode EOF yaitu dengan tahapan :

1. Memilih citra digital untuk dijadikan sebagai *cover*, kemudian baca nilai desimal *cover*.
2. Setelah itu pesan yang akan disembunyikan dirubah kedalam nilai desimal , lalu lakukan penambahan pixel baru pada kolom setelah data akhir dari citra

cover (citra asli) dan sisipkan pesan yang akan disembunyikan pada kolom baru tersebut. Selanjutnya masukkan *password*.

3. Setelah dimasukkan pesan yang telah disisipkan dan didapatkan *stegano image* nya.

3. *Modifikaksi End Of File (MEOF)*

Teknik penyisipan watermark dengan memanfaatkan padding selanjutnya disebut algoritma MEoF (Modifikasi End of File). Modifikasi yang dilakukan dari algoritma EoF (End of File) yaitu lokasi penyisipan watermark. Untuk penyisipan watermark dilakukan pada piksel terakhir citra, prosesnya dilakukan dengan cara nilai byte citra piksel terakhir digantikan dengan byte watermark. Byte yang mewakili piksel citra ditampilkan dalam bentuk baris, masing – masing baris merupakan kelipatan 4 Byte termasuk padding. Untuk citra dengan ukuran height > 1, masing – masing baris disimpan dalam bentuk Array piksel. Pada format citra digital, citra disimpan dalam bentuk berurutan (sequential). Piksel – piksel disusun mulai dari piksel – piksel baris pertama dan dilanjutkan dengan piksel baris selanjutnya. Jumlah Byte yang dibutuhkan untuk menyimpan satu baris piksel merupakan pembulatan dari kelipatan 4 dapat dikalkulasi dalam bentuk persamaan (Charlamp, 1995),

$$\text{Row Size} = \left[\frac{\text{Bits Per Byte} * \text{Width}}{32}\right] * 4$$

Sehingga jumlah total byte yang dibutuhkan untuk menyimpan Byte piksel dalam Array dapat dikalkulasi dalam bentuk persamaan,

$$\text{Pixel Array Size} = \text{Row Size}.|\text{height}|$$

Kapasitas penyisipan watermark pada citra dengan ukuran width modulo 4 = 0 penyisipan watermark dilakukan pada piksel terakhir untuk setiap width, kapasitas pesan yang mampu disisipkan dapat dikalkulasi dengan persamaan yang ditulis dalam bentuk,

$$\text{Kapasitas pesan} = (3 \text{ Byte} * \text{height}) - \text{number of massage header}$$

Sedangkan ukuran file citra stego yang dihasilkan dapat dikalkulasi dengan persamaan yang ditulis dalam bentuk,

$$\text{Ukuran file} = ((\text{width} * \text{number of bytes for each pixel}) * \text{height}$$

4. MSE (*Mean Square Error)* dan PSNR (*Peak Signal to Noise Ratio*)

Dalam citra digital terdapat suatu standar pengukuran *error* (galat) kualitas citra, yaitu besar PSNR dan MSE. Tingkat keberhasilan dan peforma dari suatu metode *filtering* pada citra dihitung dengan menggunakan *Peak Signal to Noise Ratio* atau biasa disingkat dengan PSNR. Meskipun peforma metode *filtering* juga dapat diukur dengan teknik *visual* (hanya melihat pada citra hasil dan membandingkannya dengan citra yang terdapat *noise*). Namun hasil pengukuran teknik *visual* setiap orang berbedabeda. Sehingga MSE dan PSNR merupakan solusi pengukuran peforma yang baik. *Peak Signal to Noise Ratio* (PSNR) adalah sebuah perhitungan yang menentukan nilai dari sebuah citra yang dihasilkan. Nilai PSNR

ditentukan oleh besar atau kecilnya nilai MSE yang terjadi pada citra. Semakin besar nilai PSNR, semakin baik pula hasil yang diperoleh pada tampilan citra hasil. Sebaliknya, semakin kecil nilai PSNR, maka akan semakin buruk pula hasil yang diperoleh pada tampilan citra hasil. Satuan nilai dari PSNR sama seperti MSE, yaitu *decibel* (dB). Jadi hubungan antara nilai PSNR dengan nilai MSE adalah semakin besar nilai PSNR, maka akan semakin kecil nilai MSE-nya. PSNR secara umum digunakan untuk mengukur kualitas pada penyusunan ulang citra. Hal ini lebih mudah didefinisikan dengan *Mean Square Error* (MSE).

Mean Square Error (MSE) adalah kesalahan kuadrat rata-rata. Nilai MSE didapat dengan membandingkan nilai selisih pixel-pixel citra asal dengan citra hasil pada posisi pixel yang sama. Semakin besar nilai MSE, maka tampilan pada citra hasil akan semakin buruk. Sebaliknya, semakin kecil nilai MSE, maka tampilan pada citra hasil akan semakin baik. (Lestari, 2016) Misal I (x,y) adalah citra masukan I'(x,y) adalah citra keluaran, keduanya memiliki M baris dan N kolom, maka didefinisikan sebagai berikut :

$$\boldsymbol{MSE = \frac{1}{MN}\sum_{y=1}^{M} \quad \sum_{x=1}^{M}[I(x,y) - I'(x,y)]^2}$$

Dimana : MSE = Nilai MSE citra steganografi
M = Panjang citra stego (dalam *pixel*)
N = Lebar citra stego (dalam *pixel*)
x = Ukuran baris dari citra
y = Ukuran kolom dari citra
I = Matriks citra awal
I' = Matriks citra hasil
I(x,y) = Nilai *pixel* dari citra *cover*
I'(x,y) = Nilai *pixel* dari citra *stego*

Rumus menghitung PSNR adalah :

$$PSNR = 20 \times log10\ (Max_i/\sqrt{MSE})$$

Dimana : PSNR = ukuran baris dari citra (dalam db)
Max_i = nilai maksimum piksel
MSE = nilai MSE

3. HASIL DAN PEMBAHASAN

Pada Tahapan ini merupakan gambaran proses analisa suatu masalah dan gambaran dari penerapan metode untuk memecahkan masalah yang dihadapi.

A. Menentukkan proses *Embedding* dan *Ekstraksi*

Proses ini adalah dimana memasukkan pesan rahasia dengan mengubah pesan rahasia menjadi kode ASCII sehingga gambar dapat diproses.

1. Proses *Embedding* Pesan*:*

Berikut adalah uji coba Dalam Ruangan.png yang telah diresize menjadi 5 * 5 *pixels.*

Gambar 2. Data Citra Uji

Input:

- Password : 2
- Pesan Rahasia : MALA
- *Cover Image*/Citra Digital : 5 x 5 *pixels*

Pixel	0			1			2			3			4		
5 x 5 xRGB	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
0	14	16	16	55	42	31	117	97	52	45	34	22	25	23	19
1	13	16	17	29	22	17	55	53	45	48	41	31	8	11	11
2	3	10	12	45	44	34	70	66	45	78	52	30	0	6	10
3	0	6	10	0	4	9	59	54	41	18	17	15	0	6	8
4	0	4	8	0	3	8	46	41	27	39	37	24	6	9	11

Pada gambar merupakan konversi *pixel* citra *cover image* yang dikonversikan ke desimal dan akan dilakukannya penyisipan pesan.

Proses:

a. Proses Konversi Nilai Desimal Pesan

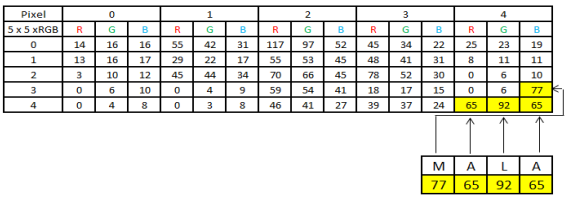
Karakter Pesan dirubah kedalam nilai desimal berdasarkan urutan karakter pada tabel ASCII.

- Pesan Rahasia : MALA

M	A	L	A
65	77	76	65

Pada tabel merupakan sebuah tabel konversi karakter pesan menjadi nilai desimal berdasarkan tabel ASCII.

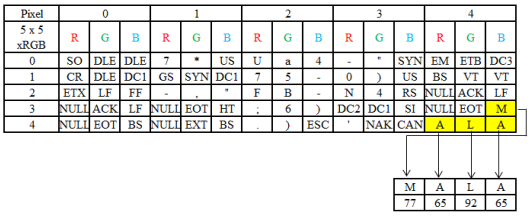
b. Proses Penyisipan/*Embedding*



Gambar 3. Proses Penyisipan/Embedding

Pada gambar dapat dilihat bahwa telah didapat sebuah text watermak di konversikan menjadi bilangan desimal dengan pedoman tabel ascii. Selanjutnya meyisipkan masing-masing nilai acsii dari text watermak pada bagian akhir kolom citra, setiap masing – masing pixel rgb akan di isi dengan nilai dari 1 huruf text watermak. Dalam menyembunyikan pesan kedalam citra gambar adalah dengan melakukan pergantian pixel akhir dari citra cover (citra asli), jumlah pesan yang disembunyikan memiliki batas maksimum, pesan yang akan di input memiliki batas maksimum sesuai panjang kolom terakhir pixel sehingga jumlah karakter pesan yang ingin disembunyikan dengan tidak merubah ukuran dari citra cover.

2. Proses Ekstraksi Pesan



Gambar 4. Proses Ekstraksi Pesan

Pada gambar Proses ekstraksi text watermak yang telah disembunyikan pada citra digital, dilakukan berdasarkan metode Modifikasi End Of File yaitu dengan memasukkan stegano image, setelah itu baca nilai desimal pixel dari stegano image, kemudian nilai desimal dikonversi ke bentuk karakter, maka akan didapatkan hasil text watermark yang disisipkan.

B. Menghitung nilai MSE dan PSNR

Berikut adalah hasil perbandingan antara citra asli dengan citra stegano beserta perhitungan MSE dan PSNR pada uji coba malaex.jpg yang telah diresize menjadi 5 * 5 pixels.

Berikut adalah hitungan MSE dan PSNR pada uji coba Dalam Ruangan.png yang telah diresize menjadi 5 * 5 *pixels.*

MSE = 1/MN ∑_(X= 9) ^ M▒ [I (x,y) – I' (x,y)]2

Password : 2

Pesan Tersisip : MM

String Pesan	ASCII
1	49
-	45
2	50
-	45
-	45
-	45
2	50
M	77
M	77

Mencari nilai ∑∑[I (x,y) – I' (x,y)]2

Untuk baris pertama (1,-,2) = (49,45,50)

Untuk baris kedua (-, - , -) = (45,45,45)

Untuk baris ketiga (2,M,M) = (50,77,77)

RGB Baris 1 = 235, 175, 89

RGB Baris 2 = 220, 162, 89

RGB Baris 3 = 159, 102

Berjarak 3 RGB karena header pesan sebanyak 3 RGB dimulai dari 1.

I (x,y)	I' (x,y)	[I (x,y) – I' (x,y)]	[I (x,y) – I' (x,y)]²	Jumlah
R = 235 G = 175 B = 89	R = 49 G = 45 B = 50	R = 186 G = 130 B = 39	R = 34596 G = 16900 B = 1521	53017
R = 220 G = 162 B = 89	R = 49 G = 45 B = 45	R = 175 G = 117 B = 44	R = 30625 G = 13689 B = 1936	46250
R = 159 G = 102 B = 59	R = 49 G = 77 B = 77	R = 110 G = 25 B = 18	R = 12100 G = 625 B=324	13049
Jumlah				113216

MSE = 1/MN ∑_(y= 2) ^M▒ ∑_(x= 9) ^M▒ [I (x,y) – I' (x,y)]2
= 1/(5 x 5 x 3) x 113216
= (112316)/(5 x 5 x 3) = 1.497.54
PSNR = 20 x log10 (Maxi / √MSE)
= 20 x log10 (255 / √1497.54)
= 20 x log10 (38698062)
= 20 x log10 (6.589477)
= 16,3770189

4. SIMPULAN

Berdasarkan Penelitian ini menghasilkan suatu Penerapan Implementasi Steganografi Dengan Metode End Of File Untuk Menyisipkan Pesan Teks Pada Gambar yang mampu memberikan keamanan pesan rahasia yang rumit untuk dipecahkan dan Algoritma Modifikasi End of File (MEoF) telah berhasil memperbaiki kelemahan algoritma End of File, yaitu pada penyisipan pesan dengan algoritma MEoF secara visual manusia kualitas citra stego masih tampak seperti citra aslinya. Sedangkan dengan algoritma EoF kualitas citra mengalami perubahan. Hasil pengujian noise yang dihasilkan algoritma MEoF lebih baik, serta Algoritma MEoF menunjukkan panjang pesan yang mampu disisipkan ditentukan oleh ukuran width dan height citra.

DAFTAR PUSTAKA

Aryanto, D., Riadi, I., Teknologi, M., Universitas, I., Dahlan, A., Significant, M. L., & Pendahuluan, I. (2017). *STEGANOGRAFI VIDEO DIGITAL DENGAN ALGORITMA MODIFIKASI END OF FILE DAN RC4. 2012*.

Asroni, O., & Ricardo Serumena, D. (2021). Pengamanan Hak Cipta Citra Digital dengan Teknik Watermarking Menggunakan Metode Hybrid SVD dengan DWT. *Jurnal Health Sains*, *2*(11), 2145–2157. https://doi.org/10.46799/jsa.v2i11.334

Cahyadi, T. (2019). Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra. *ScientiCO : Computer Science and Informatics Journal*, *1*(2), 47. https://doi.org/10.22487/j26204118.2018.v1.i2.11221

Enterprise, Jubilee. *Otodidak Pemrograman JavaScript*. Elex Media Komputindo, 2017.

Febriani, S. R. (2016). *Implementasi Digital Watermarking pada Citra Menggunakan Metode Least Significant Bit*. *21*(3), 8–18.

Irawan, M. (2013). Penggunaan Steganografi dengan Metode End of File (EOF) pada Digital Watermarking. *Jurnal Teknologi Informasi Komputer*, *2*(1), 36–42.

Madcoms, Tim. "Pemrograman PHP dan MySQL untuk pemula." *Yogyakarta: CV Andi Offset* (2016).

Goodchild, Michael F. "Citizens as sensors: web 2.0 and the volunteering of geographic information." *GeoFocus. Revista Internacional de Ciencia y Tecnología de la Información Geográfica* 7 (2007): 8-10.

Sarosa, S. (2017). *Metodologi Pengembangan Sistem Informasi* (B. Sarwiji (ed.); 1st ed.). Indeks Jakarra Permata Puri Media.

Wahyuningsih, S., Pandex, T. V. D., & Stefanny, V. (2018). Implementasi Visible Watermarking Dan Steganografi Least Significant Bit Pada File Citra Digital. *Jurnal TELEMATIKA MKOM*, *8*(2), 140–145.