JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 1, Februari 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i1.8483
Hal 18-25
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Penyisipan File Audio Pada File Video Dengan Menerapkan Metode Two Sided Side Match

Agustina Hulu

Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: agustinahulu078@gmail.com
Email Penulis Korespondensi: agustinahulu078@gmail.com
Submitted **20-02-2025**; Accepted **28-02-2025**; Published **28-02-2025**

Abstrak

Ketika menyisipkan sebuah pesan ke dalam wadah penampung pesan sering terjadi kebocoran isi pesan tersebut. Seperti halnya penyisipan file ke dalam *file* video sering terjadi kebocoran pesan gambar yang disisipkan dikarenakan adanya serangan pihak yang tidak bertanggung jawab yang dengan sengaja membocorkan pesan rahasia yang terkandung. Selain itu, pesan rahasia berupa gambar yang disisipkan ke dalam *file* video juga rentan terhadap penyerangan pihak-pihak tertentu ketika proses pengiriman *file.* Akibatnya pesan yang dikirm tidak sampai kepada orang yang ditujukan atau bisa saja pesan yang dikirim tersebut dirubah datanya oleh orang-orang tertentu yang dengan sengaja membocorkan isi pesan tersebut. Penyisipan menggunakan Metode *Two Sided Side Match* memungkinkan pesan rahasia yang ingin dikirim ke orang lain akan lebih terjaga keamanannya, karena metode ini menggunakan empat nilai piksel tetangganya untuk memprediksi berapa banyak pesan yang dapat disisipkan pada sebuah piksel. Sehingga penyisipan ini dapat dilakukan sedemikian rupa dan perubahan yang diakibatkan tidak dapat dipersepsi oleh mata manusia bahkan *file* gambar yang telah disisipkan pada video tidak akan bisa dilihat oleh pihak ketiga yang berusaha mencuri data tersebut. Pada penelitian ini menggunakan stego video sebagai media penampung *file* audio yang akan disisipkan. Penelitian ini menghasilkan aplikasi keamanan dan penyisipan *file* audio menunjukkan bahwa pengguna dapat mengamankan datanya tanpa mengandung kecurigaan dari orang lain sehingga tidak mengalami kebocoran data.

Kata Kunci *:* File Audio; Two Sided Side Matc

Abstrak

When embedding a message into a container file, there is often a risk of message leakage. For example, inserting a file into a video file can lead to unintended exposure of the hidden image due to attacks from unauthorized parties attempting to reveal the secret message. Additionally, secret messages in the form of images embedded in video files are vulnerable to interception during the transmission process. As a result, the message may not reach its intended recipient, or the data may be altered by individuals who deliberately leak its contents. The Two-Sided Side Match method enhances the security of secret messages by predicting how much data can be embedded in a pixel using four neighboring pixel values. This method ensures that the embedding process is performed in a way that prevents visible changes, making the hidden data imperceptible to the human eye. Even if a third party attempts to access the embedded image in the video, they will be unable to retrieve the hidden data. This research utilizes stego video as a medium for embedding audio files. The results demonstrate that the developed security and embedding application enables users to protect their data without arousing suspicion, effectively preventing data leaks.

Kata Kunci *:* File Audio; Two Sided Side Match

1.PENDAHULUAN

Dalam komunikasi antara dua pihak, tidak ada satu jaminan yang menyatakan bahwa komunikasi yang terjadi telah aman dari ancaman pihak ketiga. Kehadiran pihak ketiga dalam komunikasi dapat mengganggu kenyamanan kedua belah pihak. Pihak ketiga mampu mengambil informasi-informasi yang penting dari komunikasi yang telah terjadi. Hal ini akan merugikan pihak pertama dan pihak kedua. Atas dasar inilah perlu adanya suatu teknik untuk mengamankan informasi-informasi penting agar terhindar dari ancaman pihak ketiga. Sehingga keamanan terdapat audio yang mengandung informasi penting bagi kita yang menggunakannya[1].

Steganografi merupakan seni menyembunyikan pesan di dalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada suatu audio di dalam media tersebut[2]–[4]. Steganografi ini seni dan ilmu menulis audio tersembunyi atau menyembunyikan audio dengan suatu cara sehingga selain pengirim dan penerima, tidak ada seorang pun yang mengetahui atau menyadari bahwa ada suatu audio rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu audio, tapi tidak menyembunyikan bahwa ada suatu audio. Video merupakan jenis media penyembunyian audio yang potensial dan banyak digunakan. Data yang dapat disisipkan[5].

Penyisipan file audio adalah memasukan file audio kedalam halaman sebuah penampung, tidak hanya file audio saja akan tetapi mp3, video juga bisa dimasukkan kedalam halaman sebuah penampung. Sebuah penmpng akan terlihat kaku, terkesan formal, dan sedikit menjemukan bila tidak disertai dengan file audio. Kita bisa lihat saat ini, yang ada di internet, hampir semuanya memasukan unsur audio dan video untuk menarik dan membuat tercengang para pengunjungnya[6].

File video ini merupakan gabungan image yang bergerak dan audio, yang lebih sulit dideteksi. Keuntungan dari steganografi video adalah banyaknya data yang dapat disembunyikan didalamnya, serta vakta bahwa video merupakan *"streams"* dari beberapa *image* menyebabkan adanya distorsi pada salah satu frame image tidak akan dilihat dengan mata manusia. Akan tetapi semakin banyak data yang disembunyikan, bukan hal yang mustahil jika perubahan pada video menjadi semakin mudah telihat. Bahkan modifikasi kecil kepada media *stego* dapat menghancurkannya.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 1, Februari 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i1.8483
Hal 18-25
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Salah satu teknik steganografi adalah dengan menggunakan metode *Two Sided side match* dengan menyembunyikan pesan pada media digital dengan mempertimbangkan nilai dari dua pixel tetangganya yaitu nilai pixel sisi atas,dan sisi kanan atas[6].

Akan tetapi ketika menyisipkan sebuah pesan ke dalam wadah penampung pesan sering terjadi kebocoran isi pesan tersebut. Seperti halnya penyisipan file audio ke dalam file video sering terjadi kebocoran pesan audio yang disisipkan dikarenakan adanya serangan pihak yang tidak bertanggungjawab yang dengan sengaja membocorkan pesan rahasia yang terkandung. Selain itu, pesan rahasia berupa audio yang disisipkan ke dalam file video juga rentan terhadap penyerangan pihak-pihak tertentu ketika proses pengiriman file. Akibatnya pesan yang dikirim tidak sampai kepada orang yang ditujukan atau bisa saja pesan yang dikirim tersebut dirubah datanya oleh orang-orang tertentu yang dengan sengaja membocorkan isi pesan tersebut.

Untuk menghindari permasalahan yang telah disebut di atas, maka perlu sebuah aplikasi yang mampu menyisipkan pesan berupa file audio ke dalam file video sebagai media penampung pesan. Aplikasi tersebut dibangun dengan menggunakan bahasa pemrograman *Microsoft Visual Studio 2010* dan menerapkan metode *Two Sided Side Match* sehingga keamanan dan kerahasiaan data pesan yang disisipkan terjaga dengan baik. Pesan audio yang disisipkan ke dalam sebuah file video tidak akan mengundang kecurigaan dari pihak-pihak lain yang tidak berkepentingan karena penyisipan pesan audio tersebut tidak merubah isi dan ukuran video sebagai media penampung pesan.

Pada penelitian yang dilakukan oleh Nurul Khairina Tahun 2016 yang di publikasikan pada *jurnal CESSJournal Of Computer Engineering, System And Science* volume 1 nomor 2 yang berjudul "Analisis Steganografi Metode Two Sided Side Match" menyimpulkan bahwa Dari percobaan pernyisipan 5 huruf yang dilakukan pada citra asli yang berukuran 5 x 5, pada metode Two Sided Side Match hanya 2 huruf yang dapat kembali dengan normal saat waktu ekstraksi, Hal ini bisa terjadi karena kemungkinan adanya perbedaan pembulatan nilai decimal saat proses penyisipan pesan dan saat proses ekstraksi pesan, sehingga banyak bilangan biner yang tidak dapat diperoleh kembali[6].

Pada penelitian sebelumnya yg dilakukan oleh G. Swain Dkk Tahun 2013 yang di publikasikan pada jurnal *CSI Transactions on ICT* volume 1 nomor 2 yang berjudul "*Steganography using two sided, side, match methods*" menyimpulkan bahwa Jumlah bit yang tertanam dalam piksel target ditentukan tergantung pada korelasi piksel target dengan piksel tetangganya. Kapasitas persembunyian dari metode yang diusulkan relatif lebih baik. Setelah informasi disematkan, perubahan kualitas gambar tidak terlihat. Nilai PSNR yang diamati juga baik. distorsi lebih rendah dalam metode pencocokan sisi empat sisi dibandingkan dengan metode pencocokan sisi dua dan tiga sisi. Metode-metode ini dapat digunakan dalam berbagai kesempatan di mana komunikasi bersifat rahasia[5].

Dari uraian permasalahan di atas, penelitian ini akan dilakukan dengan judul "Penyisipan File Audio pada File Video Menerapkan Metode Two Sided Side Match" untuk mengatasi risiko kebocoran data dalam proses penyisipan pesan rahasia. Penelitian ini bertujuan untuk meningkatkan keamanan data dengan menerapkan metode yang mampu menyamarkan penyisipan tanpa terdeteksi oleh pihak yang tidak berwenang. Dengan menggunakan metode Two Sided Side Match, pesan yang disisipkan dalam file video akan lebih terlindungi, sehingga kemungkinan serangan atau perubahan data oleh pihak ketiga dapat diminimalkan. Hasil dari penelitian ini diharapkan dapat memberikan solusi yang efektif dalam bidang keamanan data digital, khususnya dalam steganografi berbasis video.

2. METODOLOGI PENELITIAN

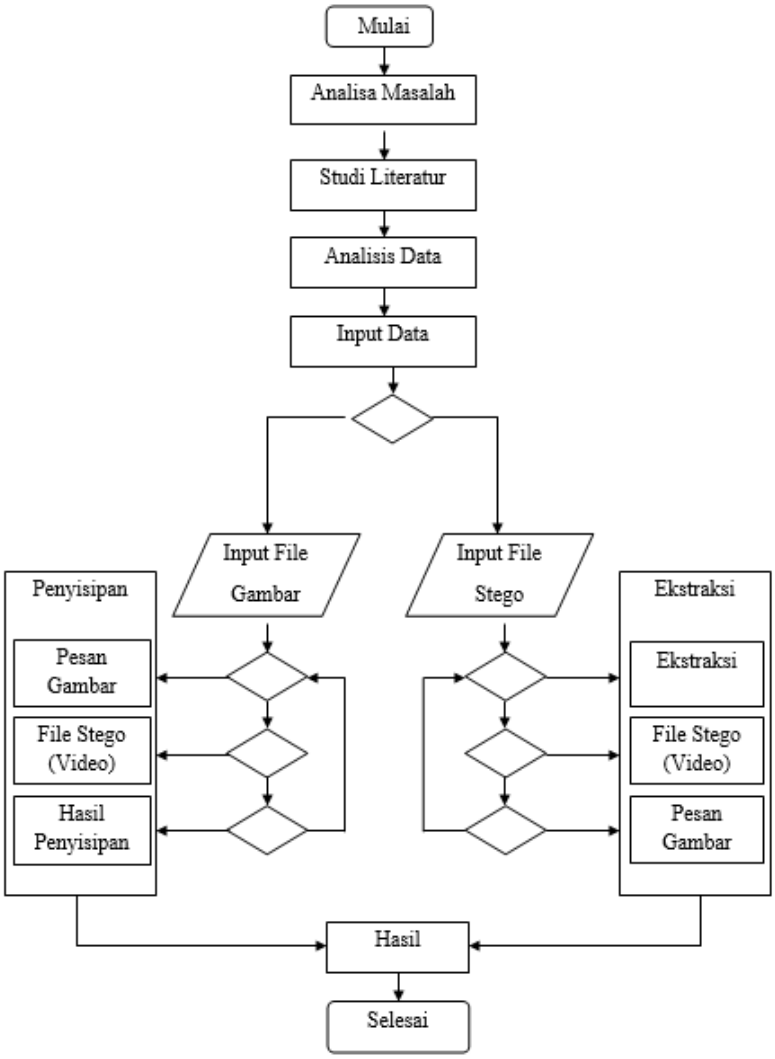
2.1 Kerangka Kerja Penelitian

Di tahap ini akan dijelaskan mengenai tahap-tahapan penelitian yang harus dilakukan untuk mempermudah penyelesaian masalah yang ada, dan untuk melakukan pengumpulan data yang berkaitan dengan penelitian, untuk memperoleh data-data dan informasi harus dilakukan tahapan penelitian seperti berikut:

1. Mengidentifikasi Masalah
   Pada tahap penelitian ini, yang dilakukan adalah mengidentifikasi apa-apa saja yang menjadi permasalahan, sehingga peneliti mengetahui apa yang dibutuhkan dalam perancangan dan pembangunan aplikasi.
2. Study Literatur
   Pada tahapan ini peneliti melakukan apa yang disebut dengan kajian pustaka, yaitu mempelajari buku-buku referensi dan hasil penelitian sejenis sebelumnya yang pernah dilakukan oleh orang lain.
3. Analisa Proses *Embedding* Pada *File* Video
   Pada tahapan ini, peneliti melakukan *embedding* (penyisipan) gambar pada *file* video dengan menerapkan metode *Two Sided Side Match.*
4. Analisa Proses Ekstraksi Pada *File* Video
   Pada tahapan ini, peneliti melakukan proses ekstraksi pada *file* video dengan melakukan dekompresi terhadap *file* hasil embedding video dengan menggunakan metode *Four Sided Side Match.*
5. Perancangan Sistem
   Pada tahapan ini, peneliti menggunakan *tools* Visual Studio 2010 dengan aplikasi *MYSQL* untuk merancang atau mendesain sistem yang berupa langkah-langkah operasi dalam proses pengolahan data.
6. Penerapan Metode *Four Sided Side Match* Pada Aplikasi Yang Dirancang
   Pada tahapan ini, peneliti menerapkan metode *Four Sided Side Match* ke aplikasi penyisipan yang dirancang berupa kode program.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 1, Februari 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i1.8483
Hal 18-25
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

7. Pengujian
   Pengujian yang dilakukan sebanyak dua kali, yaitu pengujian untuk proses *embedding* dan pengujian untuk proses ekstraksi. Pengujian dilakukan untuk melihat kesesuain hasil yang diperoleh aplikasi penyisipan yang telah siap dibuat.
8. Analisa Hasil Pengujian
   Analisa hasil pengujian dilakukan untuk melihat ketercapaian antara hasil pengujian yang dilakukan secara manual dengan hasil pengujian yang dilakukan dengan aplikasi yang telah dirancang.
9. Penulisan Laporan
   Penulisan laporan dilakukan untuk mendokumentasikan seluruh kegiatan penelitian dalam bentuk skripsi yang nantinya juga dibuat dalam bentuk artikel ilmiah yang akan dipublikasikan.



Gambar 1. Kerangka Penelitian

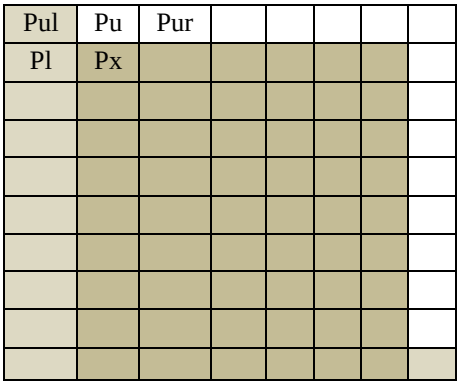
2.2 Penyisipan Pesan

Untuk melakukan penyisipan pesan pada teks, gambar, suara, atau video, diperlukan masukan berupa file digital yang akan disisipkan pesan, pesan yang akan disisipkan (message), dan kunci (key)[7]. Beberapa media yang umum digunakan dalam teknik steganografi adalah teks, gambar, suara, dan video. Pada teks, algoritma steganografi sering menggunakan teknik Natural Language Processing (NLP) sehingga teks yang telah disisipkan pesan rahasia tetap terlihat alami dan tidak mencurigakan. Gambar merupakan format yang paling sering digunakan karena banyaknya algoritma steganografi yang tersedia serta format ini umum dipertukarkan di internet. Format suara juga sering dipilih karena ukuran berkasnya yang relatif besar, memungkinkan penyisipan pesan dalam jumlah yang lebih banyak. Sementara itu, format video memiliki kapasitas penyimpanan yang sangat besar, tetapi kurang praktis digunakan dalam steganografi karena ukurannya yang besar serta terbatasnya algoritma yang mendukung penyisipan pesan pada format ini[8][9][10].

2.3 Metode Four Sided Side Match

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 1, Februari 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i1.8483
Hal 18-25
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Metode Four Sided Side Match menggunakan empat nilai pixel tetangganya untuk memprediksi berapa banyak pesan yang dapat disisipkan pada sebuah pixel[11]. Metode ini menggunakan nilai pixel tetangganya pada sisi atas, sisi kanan atas, sisi kiri atas dan sisi kiri. Berikut ilustrasinya[12]:



Gambar 2. Metode *Four Sided Side Match*

Diasumsikan bahwa P_x adalah *pixel* yang ingin disisipkan pesan dan memiliki nilai *pixel* g_x. Kemudian P_x memiliki *pixel* tetangga sisi atas P_u dengan nilai *pixel* g_u, pixel tetangga sisi kanan atas P_{ur} dengan nilai *pixel* g_{ur} , *pixel* tetangga sisi kiri atas P_{ul} dengan nilai *pixel* g_{ul}, dan *pixel* tetangga sisi kiri P_l dengan nilai *pixel* g_l[4]. Dalam menyisipkan pesan dengan metode Four Sided Side Match ini, harus terlebih dahulu menghitung perbedaan nilai d antar nilai pixel tetangga dengan rumus seperti persamaan (1) dibawah ini:

$$d = \frac{(g_u + g_{ur} + g_{ul} + g_1)}{4 - g_x} \quad (1)$$

Pada sebuah citra, terdapat pixel target P_x dengan nilai 98, dan memiliki *pixel* tetangga P_u, P_{ur}, P_{ul} dan P_1 dengan nilai masing-masing *pixel* g_u, g_{ur}, g_{ul} dan g_1 adalah 100, 120, 100, 124 sehingga diperoleh nilai d = (100+120+100+124) / 4 – 98 = 13.

Pesan dapat disisipkan ke dalam sebuah *pixel* citra apabila memiliki nilai d ≥ 2 dan d ≤ -2, dan *pixel* akan diabaikan dalam arti tidak akan disisipkan pesan apabila nilai d = -1, 0 dan 1. Karena pada perhitungan sebelumnya diperoleh nilai d = 13, maka pesan yang dapat disisipkan akan lebih dari 1 bit. Selanjutnya, akan dihitung berapa banyak bit pesan (n) yang dapat disisipkan pada sebuah *pixel* dengan rumus seperti persamaan (2) dibawah ini:

$$n = log_2|d|, if|d| > 1 \quad (2)$$

Dari hasil perhitungan d yang telah dilakukan sebelumnya, diperoleh d = 13. Kemudian dilakukan perhitungan nilai n = log_2 |13| = 3,7004, kemudian nilai n diblatkan kebawah *(floor)* sehingga diperoleh n = 3. Setelah mendapatkan nilai n, maka selanjutnya bit pesan akan dikonversikan ke bilangan *integer* b dan diperolahlah nilai d' yang baru dengan rumus seperti persamaan (3) dibawah ini:

$$d' = \begin{cases} 2^n + b, if\ d > 1 \\ -2^n + b), if\ d > 1 \end{cases} \quad (3)$$

Dari perhitungan nilai d, kita misalkan hasil konversi nilai b adalah 3, maka dapat dilakukan perhitungan d' = 2^3 + 3 = 11. Kemudian diperolehlah nilai pixel $g_x{}'$ yang baru, yang merupakan hasil dari penyisipan pesan pada *pixel* P_x dengan rumus seperti persamaan (4) dibawah ini:

$$g'_x = \frac{(100+120+100+124)}{4-11} = 100 \quad (4)$$

3. HASIL DAN PEMBAHASAN

3.1 Analisa Penerapan Metode

Analisis adalah langkah pertama yang dilakukan dalam menyelesaikan danmelakukan identifikasi masalah yang akan terjadi supaya lebih mudah untukdipahami dan diambil kesimpulan. Melakukan analisa sangat penting perannya dalam tahapan analisis untuk mendapatkan hasil yang sesuai dalam suatu sistem.

Analisa yang dilakukan dalam penelitian ini yaitu penyisipan pesan audio pada *file* video dengan menerapkan Metode *Two Sided Side Match*, penerapan metode ini dilakukan dengan mengubah pesan *file* audio yang akan disisipkan menjadi bentuk biner dan mengubah *file* video yang menjadi penampungnya ke bentuk desimal. Proses penyisipan bergantung pada seberapa besar selisih antar desimal pada *file* video dan dari selisih tersebut menentukan banyaknya biner pesan yang bisa disisipkan, proses tersebut terus berlangsung hingga semua biner pesan tersisipkan pada desimal file video. Metode *Two Sided Side Match* menggunakan empat nilai *pixel* tetangganya untuk memprediksi berapa banyak pesan yang

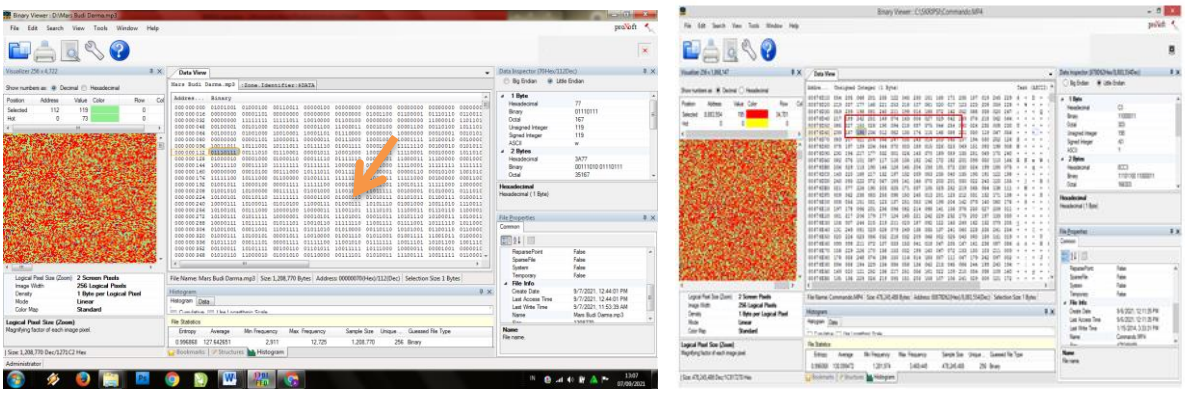
JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 1, Februari 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i1.8483
Hal 18-25
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

dapat disisipkan pada sebuah *pixel*. Metode ini menggunakan nilai *pixel* tetangganya pada sisi atas, sisi kanan atas, sisi kiri atas dan sisi kiri.

Tahapan awal dari penelitian ini adalah melakukan penyisipan *file audio* pada *file video* menggunakan metode *Two Sided Side Match* dengan menerapkan teknik Steganografi. *File* audio akan disisipkan pada *file video* namun, terlebih dahulu audio diekstraksi kemudian disisipkan pada video dengan format mp3. Suatu metode penelitian memiliki rancangan penelitian tertentu, Rancangan ini menggambarkan prosedur atau langkah-langkah yang harus ditempuh, waktu penelitian, sumber data dan kondisi arti apa data dikumpulkan, dan dengan cara bagaimana data tersebut diolah. Kegiatan penelitian juga merupakan suatu proses memperoleh atau mendapatkan suatu pengetahuan atau memecahkan permasalahan yang dihadapi, yang dilakukan secara ilmiah, sistematis dan logis.

3.1.1 Penerapan Metode Two Sided Side Match

Berikut ini merupakan analisa penyisipan file audio pada file video menerapkan metode *Two sided side match* untuk penyisipan pesan pada file audio dengan sampel *file audio pada file video*. Dengan menggunakan tools binnary viewer maka diperoleh nilai decimal dari file sampel audio Mars Budi Darma.mp3 dengan stego video Tiara Andini-Maafkan Aku.mkv sebagai berikut:



Gambar 3. Nilai Pixel dan nilai Sampel Stego

Dari gambar diatas, maka akan disisipkan pesan gambar dengan sample biner yang diambil "01110111" kedalam sebuah video dengan nilai pixel sebaga berikut:

215	177	131	15	66	64	77	126	140	73
105	98	48	46	49	87	66	140	73	68
98	88	86	49	115	164	144	49	50	51

Gambar 4. Nilai Piksel Stego

1. Proses Embedding (Penyisipan)

A. Penyisipan Tahap-1

Penyisipan pesan dimulai dari koordinat x,y = (2,2). Pixel tersebut diasumsikan sebagai P_x yang mempunyai nilai g_x = 98. Dimana nilai pixel tetangga atas P_u yang mempunyai nilai g_u = 177, dan nilai pixel tetangga kanan atas P_{ur} yang mempunyai nilai g_{ur} = 131. Maka proses penyisipan dapat dilakukan seperti berikut :

215	177	131	15	66	64	77	126	140	73
105	98	48	46	49	87	66	140	73	68
98	88	86	49	115	164	144	49	50	51

Gambar 5. Penyisipan pesan pada piksel koordinat (2,2)

1. Hitung nilai d dengan $d = \frac{gu + gur}{2} - gx$

   $d = \frac{177+131}{2} - 98$

   $d = 56$
2. Hitung nilai n dengan $n = \log_2 |d| = \log_2 |56| = 5.80 = 5$ (dibulatkan ke bawah)
3. Karena nilai n = 5, maka ambil 5 bit pesan pertama dari "01110111", yaitu "01110" sehingga sisa peshan "111"
4. Konversikan 5 bit pesan yang akan disisipkan tersebut ke dalam integer, maka b = 14
5. Hitung nilai d' baru dengan

   $d' = 2^n + b = 2^5 + 14 = 46$
6. Hitung nilai gx' baru dengan

   $gx' = \frac{gu + gur}{2} - d'$

   $Gx' = \frac{177 + 131}{2} - 46$

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 1, Februari 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i1.8483
Hal 18-25
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

$Gx' = 108$
Sehingga nilai g_x yang awalnya adalah 98, sekarang nilai g_x menjadi 108.

215	177	131	15	66	64	77	126	140	73
105	108	48	46	49	87	66	140	73	68
98	88	86	49	115	164	144	49	50	51

B. Penyisipan Tahap -2
Penyisipan pesan dimulai dari koordinat x,y = (2,3). Pixel tersebut diasumsikan sebagai P_x yang mempunyai nilai g_x = 48. Dimana nilai pixel tetangga atas P_u yang mempunyai nilai g_u = 131, dan nilai pixel tetangga kanan atas P_{ur} yang mempunyai nilai g_{ur} = 15. Maka proses penyisipan dapat dilakukan seperti berikut :

215	177	131	15	66	64	77	126	140	73
105	98	48	46	49	87	66	140	73	68
98	88	86	49	115	164	144	49	50	51

Gambar 6. penyisipan pesan pada piksel koordinat (2.3)

1. Hitung nilai d dengan
   $d = \frac{gu + gur}{2} - gx$
   $d = \frac{131+15}{2} - 48$
   $d = 25$
   2. Hitung nilai n dengan n = $\log_2 |d| = \log_2 |25| = 4{,}64 = 4$ (dibulatkan ke bawah)
   3. Karena nilai n = 4, maka ambil 4 bit pesan pertama dari "111" (0111 bit padding) yaitu "111" sehingga pesan telah habis.
   4. Konversikan 4 bit pesan yang akan disisipkan tersebut ke dalam integer, maka b = 7
5. Hitung nilai d' baru dengan
   $d' = 2^n + b = 2^4 + 7 = 23$
6. Hitung nilai gx' baru dengan
   $gx' = \frac{gu + gur}{2} - d'$
   $Gx' = \frac{131 + 15}{2} - 23$
   $Gx' = 50$
   Sehingga nilai g_x yang awalnya adalah 48, sekarang nilai g_x menjadi 50.

215	177	131	15	66	64	77	126	140	73
105	98	50	46	49	87	66	140	73	68
98	88	86	49	115	164	144	49	50	51

1. Proses Extraction (Ekstraksi)

A. Estraksi tahap 1
Ekstraksi pesan dimulai dari koordinat x, y = (2,2). Pixel tersebut diasumsikan sebagai P_x yang mempunyai nilai g_x = 108. Dimana nilai pixel tetangga atas P_u yang mempunyai nilai g_u = 177, nilai pixel tetangga kanan atas P_{ur} yang mempunyai nilai g_{ur} = 131. Maka proses ekstraksi dapat dilakukan seperti berikut:

215	177	131	15	66	64	77	126	140	73
105	108	48	46	49	87	66	140	73	68
98	88	86	49	115	164	144	49	50	51

Gambar 7. Ekstraksi Pesan Pada Piksel Koordinat (2,2)

1. Hitung nilai d dengan
   $d = \frac{g_u + g_{ur}}{2} - g_x$
   $d = \frac{177+131}{2} - 108$
   d = 46
2. Hitung nilai n dengan n = $log_2 |d| = log_2 |46| = 5{,}52 = 5$ (dibulatkan ke bawah)
3. Hitung nilai b dengan b = d* - 2^n = 46 - 2^5 = 14
4. Konversikan nilai b ke bilangan biner, b = 14 = 1110
5. Dari hasil ekstraksi yang telah dilakukan sebelumnya, diperoleh bit pesan rahasia yang telah disisipkan, yaitu "01110".

B. Ekstraksi Tahap-2
Ekstraksi pesan dimulai dari koordinat x, y = (2,3). Pixel tersebut diasumsikan sebagai P_x yang mempunyai nilai g_x = 50. Dimana nilai pixel tetangga atas P_u yang mempunyai nilai g_u = 131, nilai pixel tetangga kanan atas P_{ur} yang mempunyai nilai g_{ur} = 15. Maka proses ekstraksi dapat dilakukan seperti berikut:

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 1, Februari 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i1.8483
Hal 18-25
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

215	177	131	15	66	64	77	126	140	73
105	98	50	46	49	87	66	140	73	68
98	88	86	49	115	164	144	49	50	51

Gambar 8. Ekstraksi Pesan Pada Piksel Koordinat (2,3)

1. Hitung nilai d dengan
   $d = \frac{g_u + g_{ur}}{2} - g_x$
   $d = \frac{131 + 15}{2} - 50$
   d = 23
2. Hitung nilai n dengan n = log_2 |d| = log_2 |23| = 4,52 = 4 (dibulatkan ke bawah)
3. Hitung nilai b dengan b = d* - 2^n = 23 - 2^4 = 7
4. Konversikan nilai b ke bilangan biner, b = 7 = 111
5. Dari hasil ekstraksi yang telah dilakukan sebelumnya, diperoleh bit pesan rahasia yang telah disisipkan, yaitu “111”.

3.2 Implementasi

Implementasi program merupakan tahapan uji coba dari sistem yang di bangun. Pada bagian ini membahas spesifikasi perangkat keras, perangkat lunak dan hasil dari tampilan sistem ketika sedang berjalan.

Hasil pengujian juga dilakukan terhadap dua *file* yang ada pada sampel data di bab sebelumnya. Hasil yang didapatkan dalam pengujian *embedding* dan ekstraksi pada sampel data tersebut dapat dilihat pada tabel berikut.

Tabel 1. Hasil Pengujian

No	Nama File	Proses Embedding	Hasil Proses Ekstraksi
1	Mars Budi Darma.mp3	√	√
2	Tiara Andini-Maafkan Aku.mkv	√	√

Dari hasil pengujian di atas, maka disimpulkan bahwa penyisipan audio pada *file* video dengan menerapkan metode *Two Sided Side Match* dapat dilakukan dan memperoleh audio hasil ekstraksi yang sama dengan pesan ketika disisipkan ke dalam *file* video. Metode *Two Sided Side Match* merupakan salah satu metode yang bisa menjadi alternatif solusi untuk penyisipan pesan pada *file* video.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa penyisipan file audio ke dalam file video menggunakan metode Two Sided Side Match dapat dilakukan dengan aman dan efektif. Metode ini memungkinkan penyisipan pesan rahasia dengan tingkat keamanan yang lebih tinggi, karena memanfaatkan empat nilai piksel tetangga untuk memprediksi jumlah pesan yang dapat disisipkan dalam setiap piksel. Dengan cara ini, perubahan yang terjadi akibat penyisipan tidak dapat dipersepsi oleh mata manusia, sehingga pesan tetap tersembunyi dan tidak mudah terdeteksi oleh pihak yang tidak berwenang. Selain itu, penelitian ini menunjukkan bahwa metode Two Sided Side Match mampu menjaga integritas pesan yang disisipkan, di mana audio yang diekstraksi dari file video tetap memiliki kualitas yang sama dengan file aslinya. Dengan menggunakan stego video sebagai media penampung, pengguna dapat mengamankan data tanpa menimbulkan kecurigaan. Hasil penelitian ini membuktikan bahwa metode Two Sided Side Match dapat menjadi alternatif solusi yang efektif dalam penyisipan pesan rahasia ke dalam file video, sekaligus mengurangi risiko kebocoran data akibat serangan pihak yang tidak bertanggung jawab.

REFERENCES

[1] D. Ariyus, *Pengantar ilmu kriptografi: teori analisis & implementasi*. Penerbit Andi, 2008.
[2] A. Rohmanu, “Implementasi kriptografi dan steganografi dengan metode algoritma DES dan metode End Of File,” *J. Inform. SIMANTIK*, vol. 2, no. 1, pp. 1–11, 2017.
[3] A. A. Permana and H. Amna, “Implementasi Steganografi File Citra Digital Menggunakan Metode Least Significant Bit,” *J. Tek.*, vol. 11, no. 1, 2022.
[4] S. Nur’aini, “Steganografi Pada Digital Image Menggunakan Metode Least Significant Bit Insertion,” *Walisongo J. Inf. Technol.*, vol. 1, no. 1, pp. 75–90, 2019.
[5] G. Swain and S. K. Lenka, “Steganography using two sided, three sided, and four sided side match methods,” *CSI Trans. ICT*, vol. 1, no. 2, pp. 127–133, 2013, doi: 10.1007/s40012-013-0015-3.
[6] N. Khairina, “Analisis Steganografi Metode Two Sided Side Match,” *CESSJournal Comput. Eng. Syst. Sci.*, vol. 1, no. 2, pp. 7–11, 2016.
[7] S. (Siti) Rohayah, G. W. (Ginanjar) Sasmito, and O. (Oman) Somantri, “Aplikasi Steganografi Untuk Penyisipan Pesan,” *J. Inform. Ahmad Dahlan*, vol. 9, no. 1, p. 102820, Jan. 2015, doi: 10.26555/JIFO.V9I1.A2038.
[8] E. Saragih, D. Siregar, and H. Dafitri, “Implementasi Penyisipan Pesan Teks Terenkripsi Menggunakan Kriptografi ElGamal pada Citra Digital Menggunakan Steganogarafi LSB,” *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 22, no. 2, pp. 464–473, 2023.
[9] H. Setiawan, B. B. Wijaya, and D. Sartika, “Metode Spread Spectrum untuk Penyisipan Pesan pada Citra Digital,” *Bull. Comput.*

Sci. Res., vol. 4, no. 1, pp. 101–111, 2023.

[10] F. Kurniasih, R. Marwati, and R. Sispiyati, "Penggabungan Affine Cipher dan Least Significant Bit-2 untuk Penyisipan Pesan Rahasia pada Gambar," *J. EurekaMatika*, vol. 11, no. 2, pp. 79–88, 2023.

[11] N. Khairina, "Analisis Perbandingan Metode Steganografi Two Sided Side Match Dengan Four Sided Side Match Pada Citra Multilayer TIFF." 2016.

[12] C. Eric, "Hiding in plain sight, Stegnography and the art of Covert Communication," *Wiley, Indianapolis, Indiana, ISBN*, vol. 10, p. 471444499, 2003.