



# Penyisipan Gambar Pada File Video Menerapkan Metode Two Sided Side Match

Ledi Firman Zendrato

Fakultas Ilmu Komputer Dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budidarma, Medan, Indonesia  
Email: Vyrman26@gmail.com

**Abstrak**-Saat memasukan pesan kedalam wadah penampung pesan sering membocorkan pesan. Seperti penyisipan gambar pada *file* video, sering kali ada kebocoran pesan gambar yang disisipkan yang diakibatkan adanya pihak yang tidak bertanggung jawab atau sengaja membocorkan pesan yang terkandung. Akibatnya pesan yang akan dikirim akan berubah atau pesan yang akan dikirim tidak bisa terkirim dikarenakan orang-orang tersebut sengaja membocorkan isi pesan yang dikirim. Penyisipan menggunakan metode *Two Sided Side Match* memungkinkan pesan rahasia yang ingin dikirim akan lebih terjaga keamanannya, karena metode ini menggunakan dua nilai piksel tetangganya untuk bisa memprediksi berapa banyak pesan yang akan disisipkan pada sebuah pixel. Sehingga penyisipan dapat dilakukan sedemikian rupa dan *file* gambar yang disisipkan pada video tidak akan bisa diretas orang-orang yang tidak bertanggung jawab. Pada penelitian ini menggunakan stego video sebagai media penampung pesan gambar yang akan disisipkan. Penelitian ini dapat menghasilkan aplikasi keamanan dan penyisipan gambar dapat diamankan datanya tanpa mengandung kecurigaan sehingga tidak mengalami kebocoran data.

**Kata Kunci:** Gambar; Video; Two Sided Side Match

**Abstract**-When entering a message into the message container it often leaks the message. Like the insertion of images in video files, there are often leaks of inserted image messages caused by irresponsible parties or intentionally leaking the messages contained. As a result, the message to be sent will change or the message to be sent cannot be sent because these people deliberately leaked the contents of the message sent. Insertion using the Two Sided Side Match method allows the secret message to be sent to be more secure, because this method uses two neighboring pixel values to be able to predict how many messages will be inserted in a pixel. So that the insertion can be done in such a way and the image files that are inserted in the video cannot be hacked by irresponsible people. This research can produce security applications and image insertion data can be secured without containing suspicion so that data leaks do not occur.

**Keywords:** Image; Videos; Two Sided Side Match

## 1. PENDAHULUAN

Seiring berkembangnya teknologi informasi yang semakin modern pada saat ini maka memerlukan informasi yang cepat dan akurat. Kebutuhann untuk mengirimkan informasi dari suatu tempat ketempat lain menjadi sangat mudah di lakukan pada masa sekarang ini. Teknologi perangkat keras yang digunakan mengalami perkembangan yang sangat pesat, begitu juga dengan kompleksitas dari perangkat lunak yang digunakan didalamnya. Hal ini menyebabkan proses pengiriman informasi menjadi cepat. Jenis informasi yang bisa dikirimkan juga beraneka ragam, seperti video, audio, pesan, dan gambar. Dengan perkembangan teknologi, video, audio, pesan, dan gambar dapat disembunyikan dengan cara steganografi yang berbasis komputer.

Steganografi merupakan sebuah teknik menyembunyikan atau menyisipkan sebuah informasi seperti gambar dan file video dengan menerapkan metode *two sided side match*. Teknik steganografi sangat dekat dengan kriptografi, yang hanya saja pada kriptografi pesan dapat terlihat dengan jelas. Namun sebaliknya steganografi mengamankan file dengan cara menyembunyikannya pada sebuah media, sehingga tidak dapat menimbulkan kecurigaan dari pihak lainnya (Andika & Darwis, 2020) (Tarigan & Dwiatma, 2022).

Berbicara tentang penyisipan gambar pada file video sering mengalami masalah, dimana sering terjadinya pencurian data, penyadapan data dan perubahan data oleh pihak yang tidak bertanggung jawab. Oleh karena itu, perlu cara untuk mengatasi masalah tersebut, supaya dalam melakukan penyisipan tidak ada pihak lain yang mengetahui.

Berdasarkan penelitian yang dilakukan oleh N Khairina pada tahun 2016 yang berjudul “Analisis Steganografi Metode *Two Sided Side Match*”. Dapat disimpulkan bahwa Metode *Two Sided Side Match* adalah salah satu metode yang menggunakan dua sisi pixel tetangganya yaitu sisi atas dan sisi kanan atas.

Cara kerja penyisipan pesan dan ekstraksi pesan metode *Two Sided Side Match* mengukur citra hasil penyisipan terhadap citra asli (Khairina, 2016).

Berdasarkan penelitian yang dilakukan oleh R Rulin pada tahun 2007 yang berjudul “Perancangan Program Menggunakan Metode *Two Sided Side Match* Pada Citra Digital”. Dapat disimpulkan untuk meningkatkan keaamanan data, steganografi yang bersifat tidak terlihat, merupakan salah satu alternatif yang harus memberikan kapasitas yang besar untuk data embedding dan meminimalisasi distorsi pada *stego-image* (Rulin, 2007).

Berdasarkan penelitian yang dilakukan oleh A. Ratnasari, F. Dwiyanto pada tahun 2020 yang berjudul “Metode Steganografi Citra Digital”. Disimpulkan bahwa hasil Metode *Two Sided Side Match* menyembunyikan pesan pada media digital dengan mempertimbangkan nilai dari dua *pixel* tetangganya yaitu : nilai *pixel* sisi atas, dan sisi kanan atas. sementara itu, metode *four sided side match* yang merupakan pengembangan dari metode *Two Sided Side Match* mempertimbangkan nilai dari empat *pixel* tetangganya, yaitu : nilai *pixel* sisi atas dan sisi kiri.

Menurut penelitian yang dilakukan oleh menganalisis metode *Two Sided Side*, *Three Sided Side*, dan *Four sided match*. Masing-masing metode ini memprediksi berapa banyak pesan yang mampu ditambah pada sebuah *pixel*



tetangganya. Hasil penelitian ini menunjukkan bahwa metode-metode tersebut memiliki kapasitas menyembunyikan pesan yang besar memiliki tingkat keamanan pesan yang cukup baik (Ratnasari & Dwiyanto, 2020).

Menurut penelitian yang dilakukan oleh G. Swain, S. Lenka pada tahun 2013 yang berjudul “*Steganography Using Two Sided, Three Sided, And Four Sided Side Match Methods*” (Swain & Lenka, 2013).

## 2. METODOLOGI PENELITIAN

### 2.1 Tahapan 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:

Berdasarkan tahapan penelitian yang telah digambarkan diatas, maka dapat diuraikan pembahasan masing-masing tahap dalam penelitian adalah sebagai berikut:

#### 1. Analisa Masalah

Pada tahapan ini peneliti melakukan pemecahan masalah yang dibahas pada skripsi ini, mengenali masalah yang ada pada objek yang diteliti serta mengetahui metode yang digunakan.

#### 2. Studi 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. Analisis Data

Pada tahapan ini peneliti melakukan cara untuk mengolah data yang telah dikumpulkan sehingga data tersebut bisa dipahami dan bermanfaat untuk solusi permasalahan.

#### 4. *Input Data*

Pada tahapan ini peneliti memasukkan data yang dibutuhkan untuk penyelesaian permasalahan yaitu *file* gambar dan *file* Stego (video).

##### a. *Input File* Gambar

Pada tahapan ini peneliti memasukkan *file* gambar yang akan dilakukan penyisipan. Penyisipan pesan gambar dengan ekstensi jpeg/jpg yang berukuran tidak lebih dari 15 MB dan akan disisipkan pada *file* stego atau video dengan ukuran tidak lebih dari 500 MB dengan format video .mp4 sehingga diperoleh hasil penyisipan *file* gambar.

##### b. *Input File* Stego

Pada tahapan ini peneliti memasukkan *file* stego berupa video yang akan dilakukan ekstraksi. Ekstraksi merupakan tahapan mengekstrak ciri/informasi dari objek di dalam citra yang ingin dikenali/dibedakan dengan objek lainnya. Pada tahapan ini proses ekstraksi dilakukan pada *file* video dan pesan gambar sampai penyelesaian sampel biner yang peneliti tentukan terselesaikan dengan menggunakan metode *Four Sided Side Match*.

#### 5. Hasil

Hasil yang diperoleh peneliti yaitu dari hasil *input* data baik penyisipan atau ekstraksi yang dilakukan. Dari hasil ini dapat diketahui hasil yang didapatkan apakah sesuai dengan maksud dan tujuan penelitian dalam menyelesaikan permasalahan.

### 2.2 Steganografi

Steganografi (*steganography*) berasal dari bahasa Yunani yaitu “*steganos*” yang berarti “tersembunyi” atau “terselubung” dan “*graphein*” yang artinya “menulis”. Steganografi dapat diartikan “tulisan tersembunyi” (*convered writing*). Steganografi merupakan ilmu yang mempelajari tentang penyembunyian pesan rahasia didalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui dan tidak menyadari keberadaan dari pesan rahasia tersebut. Steganografi membutuhkan dua properti, yaitu media penampung dan pesan rahasia (Kusrini, 2012) (Darwis & Pasaribu, 2020). Media penampung yang umum digunakan adalah gambar, suara, video, dan teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, kode program, atau pesan lain. Proses penyisipan pesan kedalam media *covertext* diamankan *encoding*, sedangkan ekstraksi pesan dari *stegotext* dinamakan *decoding*. Ada beberapa istilah yang berkaitan dengan steganografi antara lain (Pamungkas et al., 2020) (Hafiz, 2019).

### 2.3 JPEG (*Joint Photographic Experts Group*)

Dalam ilmu komputer, JPEG adalah metode kompresi yang umum digunakan untuk gambar-gambar fotografi. JPEG merupakan singkatan dari *Joint Photographic Experts Group*, yang telah disahkan sebagai ISO 10918-1. Standar JPEG memberikan spesifikasi *codec* kompresi data kedalam *stream* data *byte* dan pendekompresian kembali ke bentuk gambar serta format data penyimpanannya. File JPEG memiliki ekstensi berupa jpg, jpeg, jpe, jfif, dan jif (Winanti, 2009) (Azarianpour & Sadri, 2019).



## 2.4 Video

Video adalah sebuah filem atau gambar hidup yang dihasilkan dengan rekaman orang dan benda dengan menggunakan kamera, dan memiliki fungsi dua dimensi yang terbentuk dari penglihatan dalam suatu tempat yang merupakan basis dari pembentukan video. Secara umum video dibagi dua macam yaitu, *Analog* video hasil tangkapan kamera terhadap tempat (*scene*) yang *discene* secara *vertical* dan *horizontal* oleh video kamera. *Digital*, yaitu video yang dipersentasikan sebagai sebuah *matriks* yang masing-masing elemennya mempresentasikan nilai intensitas (Manullang, 2019) (Bross et al., 2021).

## 2.5 Penyisipan Pesan

Dalam melakukan penyisipan pesan yang baik dan benar pada pesan teks, gambar, suara, dan video membutuhkan masukan berupa *file digital* yang akan disisipkan (*message*), dan kunci (*key*) (Ii, 2001).

## 2.6 Metode Two Sided Side Match

Metode *Two Sided side Match* merupakan metode steganografi yang menggunakan dua sisi nilai pixel tetangganya yaitu sisi atas dan sisi kanan, dengan memprediksi berapa banyak pesan yang dapat disisipkan pada sebuah pixel. Untuk lebih jelasnya dengan metode *Two Sided side Match* berikut ilustrasinya (Khairina, 2016)

### 1. Metode Two Sided Side Match

Dalam menyisipkan pesan dengan metode *Two Sided Side Match* ini, harus terlebih dahulu menghitung Perbedaan nilai  $d$  antara nilai *pixel* tetangga dengan rumus seperti persamaan (1) dibawah ini:

$$d = (g_u + g_{ur}) / 2 - g_x \quad (1)$$

Pada sebuah citra, terdapat nilai *pixel* target  $p_x$  dengan nilai 72, dan memiliki *pixel* tetangga  $p_u$  dan  $p_{ur}$  dengan nilai masing-masing *pixel*  $g_u$  dan  $g_{ur}$  adalah 80 dan 76, sehingga diperoleh nilai  $d = (80 + 76) / 2 - 72 = 6$ .

Pesan dapat disisipkan kedalam sebuah *pixel* citra apabila memiliki nilai  $d \geq 2$  dan  $d \leq -2$ , dan *pixel* akan diabaikan dalam antrian tidak akan disisipkan pesan apabila nilai  $d = -1, 0$ , dan 1. Karena pada perhitungan sebelumnya diperoleh nilai  $d = 6$ , maka pesan yang akan 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 :

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

Dari hasil perhitungan  $d$  yang telah dilakukan sebelumnya, diperoleh  $d = 6$ . Kemudian dilakukan perhitungan nilai  $n = \log_2 |6| = 2,585$ , kemudian nilai  $n$  dibuatkan kebawah (*floor*) sehingga diperoleh  $n = 2$ . Setelah mendapatkan nilai  $n$ , maka bit pesan akan dikoverensikan kebilangan integer  $b$ , dan diperoleh nilai  $d'$  yang baru seperti persamaan (3) dibawah ini :

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

Kemudian, kita misalkan nilai  $b$  adalah 2, maka dapat dilakukan perhitungan  $d' = 2^2 + 2 = 6$ . Kemudian diperoleh nilai *pixel*  $g_x'$  yang baru, yang merupakan hasil dari penyisipan pada *pixel*  $P_x$  dengan rumus seperti persamaan (4) dibawah ini:

$$g_x' = (g_u + g_{ur}) / 2 - d' \quad (4)$$

Tahapan terakhir adalah perhitungan nilai  $g_x'$  yang baru merupakan nilai *pixel* hasil penyisipan pesan. Perhitungan  $g_x'$  dilakukan dengan melibatkan nilai *pixel* tetangga sebelumnya, yaitu dengan perhitungan  $g_x' = (80 + 76) / 2 - 6 = 72$ .

### 2. Ekstraksi Metode Two Sided Side Match

Dalam ekstraksi pesan dengan metode *Two Sided Side Match* ini, diasumsikan bahwa *pixel* yang telah disisipkan pesan adalah  $P_x^*$  dengan nilai *pixel*  $g_x^*$ , *pixel* tetangga sisi atas  $P_u^*$  dengan nilai *pixel*  $g_u^*$ , dan *pixel* tetangga sisi kanan atas  $P_{ur}^*$  dengan nilai *pixel*  $g_{ur}^*$ . Untuk mengetahui berapa banyak bit pesan yang telah disisipkan, terlebih dahulu dihitung perbedaan nilai  $d^*$  antar nilai *pixel* tetangga dengan rumus seperti persamaan (5) dibawah ini (Ii, 2001) :

$$d^* = (g_u^* + g_{ur}^*) / 2 - g_x^* \quad (5)$$

Dari perubahan nilai *pixel* pada proses penyisipan sebelumnya, dapat kita hitung kembali perbedaan nilai  $d^* = (80 + 76) / 2 - 72 = 6$ . Dari setiap *pixel* akan dihitung berapa banyak bit pesan ( $n$ ) yang telah disisipkan dengan rumus (6) dibawah ini :

$$n = \log_2 |d^*|, \text{ if } |d^*| > 1 \quad (6)$$

Sebelumnya telah diperoleh nilai  $d^* = 6$ , maka selanjutnya dapat dihitung nilai  $n = \log_2 |6| = 2,585$ , kemudian nilai  $n$  dibulatkan kebawah (*floor*) sehingga diperoleh  $n = 2$ . Setelah mendapatkan nilai  $n$ , maka selanjutnya dapat dihitung nilai  $b$  dengan rumus (7) dibawah ini :

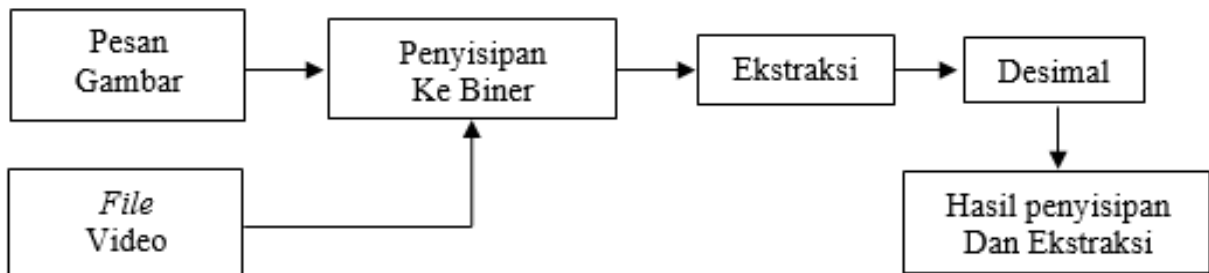
$$b = \begin{cases} d * -2n, & \text{if } d * > 1 \\ -d * -2n, & \text{if } d * < 1 \end{cases} \quad (7)$$

Tahapan terakhir adalah menghitung nilai b dengan mempertimbangkann nilai d\* dan nilai n, maka b dapat dihitung dengan  $b = 6 - 2^2 = 2$ . Pada akhir proses ekstraksi, nilai b dikonversi ke nilai biner untuk mendapatkan pesan yang telah disisipkan.

### 3. HASIL DAN PEMBAHASAN

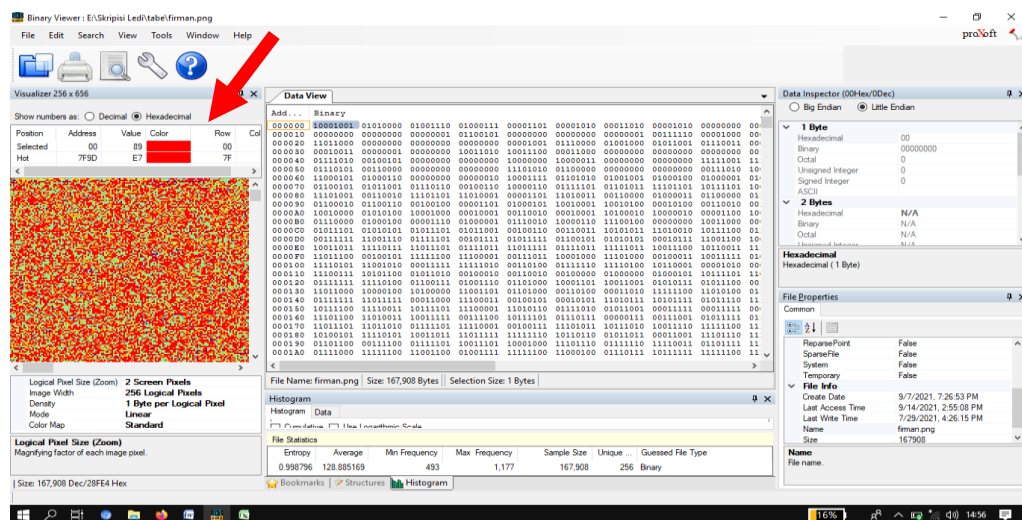
Masalah yang sering dihadapi dalam melakukan penyisipan pesan kedalam wadah penampung pesan sering terjadi kesulitan dalam menyisipkan isi pesan. Seperti halnya pada penyisipan gambar kedalam file video yang sering mengalami kendala dalam melakukan penyisipan pesan yang dikarenakan adanya serangan pihak yang tidak bertanggung jawab atau membocorkan isi pesan rahasia yang telah disisipkan. Akibatnya gambar yang akan dikirim tidak akan sampai pada pengguna yang dituju, atau bisa saja pesan yang akan dikirim tersebut akan diubah datanya oleh orang-orang yang sengaja membocorkan isi pesan rahasia tersebut.

Dalam menangani masalah penyisipan gambar pada file video, yang mengalami kendala yang diakibatkan bocornya isi pesan rahasia tersebut , pengguna dapat melakukan berbagai metode, diantaranya metode *Two Sided side Match* yang menggunakan dua nilai pixel tetangganya untuk memprediksi berapa banyak pesan yang dapat disisipkan pada sebuah pixel. Untuk mengetahui prosedur penyisipan dan ekstraksi dalam file video dapat dilihat pada gambar 4.1 dibawah ini:



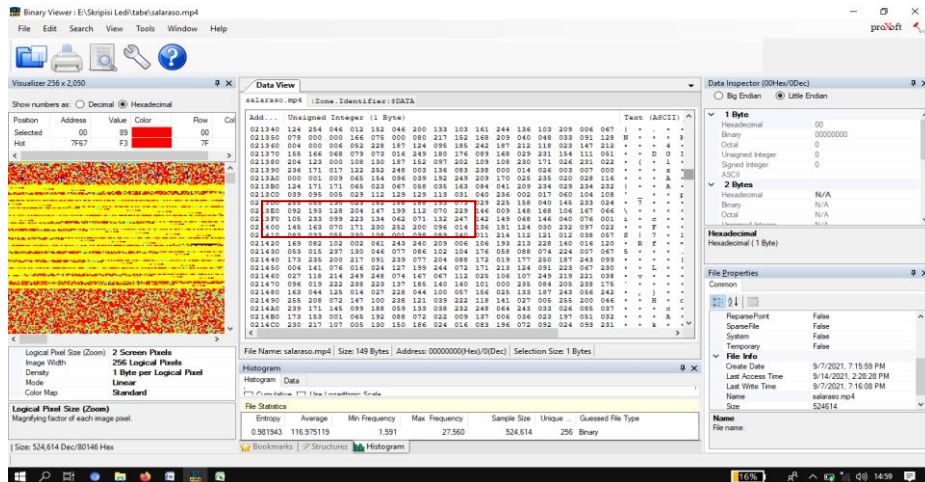
**Gambar 1.** Alur Proses Penyisipan Dan Ekstraksi

Penerapan metode *Two Sided Side Match* merupakan analisa penyisipan gambar pada file video. Dalam melakukan penyisipan pesan gambar sebagai sampel file gambar pada file video, pengguna menggunakan *Tools Binnary Viewer* dengan memperoleh nilai decimal dari file sampel firman.jpg dengan stego salaraso.mp4 yang tertera sebagai berikut ini :



**Gambar 2.** Nilai Sampel Biner pesan Gambar

Hasil nilai sampel gambar diatas berhasil didapatkan dengan menggunakan bantuan dari *tools viewer* sehingga nilai binernya menjadi 10001001, yang akan disisipkan kedalam file video.



**Gambar 3.** Nilai Sampel Desimal *File* Video

**Tabel 1.** Hasil Desimal *File* Video

124	171	171	65	23	67	58	35	163	84
39	95	5	29	112	129	129	113	31	40
255	55	130	23	182	188	188	193	73	29

1. Proses *Embedding* (Penyisipan)

Dalam melakukan penyisipan dengan metode *two sided side match* terlebih dahulu menghitung nilai *d* antara nilai *pixel* tetangga. Selanjutnya menghitung banyak bit pesan *n* yang akan disisipkan pada *pixel*. Penyisipan Tahap 1

Dalam tahap penyisipan harus dimulai dari koordinat  $xy = (2,2)$ , dimana  $P_x$  diasumsikan sebagai *pixel* yang memiliki nilai  $g^x = 95$ , kemudian nilai  $P_u$  yang memiliki nilai *pixel* tetangga atas yang diasumsikan sebagai  $g^u = 171$  dan nilai  $P^{ur}$  yang memiliki nilai *pixel* tetangga kanan atas diasumsikan sebagai  $g^{ur} = 171$ . Kemudian hasil perhitungan yang diperoleh sebelumnya *d* akan dilakukan perhitungan nilai  $n = \log_2 |d|$  lalu dibulatkan nilai *n*, di konversikan ke bilangan ingger *b* dan diperoleh nilai *b*. Maka akan dilakukan proses penyisipan sebagai berikut :

**Tabel 2.** Desimal *File* video

124	171	171	65	23	67	58	35	163	84
39	95	5	29	112	129	129	113	31	40
255	55	130	23	182	188	188	193	73	29

a. Hitung nilai *d* dengan rumus  $d = \frac{g^u + g^{ur}}{2} - g^x$

$$d = \frac{171 + 171}{2} - 95$$

$$d = 76$$

b. Hitung nilai *n* dengan rumus  $n = \log_2 |d|$

$$n = \log_2 |76| = 6,24 \text{ dibulatkan menjadi } 6$$

c. Karena nilai  $n = 6$ , maka diambil 6 bit pesan pertama dari "10001001", sehingga mempunyai sisa pesan "01"

d. Koneversikan 6 bit pesan yang akan disisipkan kedalam integer, mka hasil dari biner 100010 = 34

e. Hitung nilai *d'* yang baru dengan rumus  $d' = 2^n + b$

$$2^6 + 34 = 98$$

f. Hitung nilai  $g^x$  yang baru dengan rumus  $g^x = \frac{g^u + g^{ur}}{2} - d'$

$$d = \frac{171 + 171}{2} - 98$$

$$d = 73$$

Pada perhitungan yang awalnya nilai  $g^x = 95$ , telah mengalami penkoveresian menjadi nilai  $g^x = 73$ , yang tertera sebagai berikut :

**Tabel 3.** Hasil Nilai *Pixel* Stego Koordinat 2.2

124	171	171	65	23	67	58	35	163	84
39	73	5	29	112	129	129	113	31	40
255	55	130	23	182	188	188	193	73	29

2. Proses *Extraction* (Ekstraksi)

Dalam melakukan penyisipan dengan metode *two sided side match* terlebih dahulu menghitung nilai *d\** antara nilai *pixel* tetangga. Selanjutnya menghitung banyak bit pesan *n* yang akan disisipkan pada *pixel*. Ekstraksi tahap 1



dalam tahap ekstraksi ke dua akan dilakukan pergeseran koordinatnya kes sebelah kanan sebanyak satu kali pergeseran dengan koordinatnya  $xy = (2,3)$ , dimana  $P_{x^*}$  diasumsikan sebagai *pixel* yang memiliki nilai  $g^x = 95$  sebelumnya yang akan digantikan dengan hasil  $d = 73$  menjadi  $g^x = 73$ . Kemudian nilai  $P_{u^*}$  yang memiliki nilai *pixel* tetangga atas yang diasumsikan sebagai  $g^{u^*} = 171$  dan nilai  $P^{ur}$  yang memiliki nilai *pixel* tetangga kanan atas diasumsikan sebagai  $g^{ur^*} = 171$ . Kemudian hasil perhitungan yang diperoleh sebelumnya  $d$  akan dilakukan perhitungan nilai  $n = \log_2 |d^*|$  lalu dibulatkan nilai  $n$ , di koveresikan ke bilangan ingger  $b$  dan diperoleh nilai  $b$ . Maka akan dilakukan proses penyisipan sebagi berikut :

**Tabel 4.** Nilai *Pixel* Stego Koordinat 2.2

124	171	171	65	23	67	58	35	163	84
39	73	5	29	112	129	129	113	31	40
255	55	130	23	182	188	188	193	73	29

a. Hitung nilai  $d$  dengan rumus  $d^* = \frac{g^{u^*} + g^{ur}}{2} - g^x$

$$d^* = \frac{171 + 171}{2} - 73$$

$$d^* = 98$$

b. Hitung nilai  $n$  dengan rumus  $n = \log_2 |d^*|$

$$n = \log_2 |98| = 6,6 \text{ dibulatkan menjadi } 6$$

c. Hitung nilai  $b^*$  yang baru dengan rumus  $b^* = 2^n$

$$98 - 2^6 = 6$$
$$= 34$$

d. Hasil konversi nilai  $d^* = 34$  diubah ke biner menjadi  $b = 100010$

e. Dari hasil ekstraksi yang dilakukan maka diperoleh bit yang akan disisipkan yaitu "100010"

Dari hasil pengujian yang dilakukan pada dua *file* yang ada pada sampel data sebelumnya, maka hasil yang didapatkan dalam pengujian penyisipan (*embedding*) dan ekstraksi pada sampel data tersebut maka dapat dilihat pada tabel berikut ini :

**Tabel 5.** Hasil Pengujian

No	Nama <i>File</i>	Proses <i>Embedding</i>	Hasil Proses Ekstraksi
1.	Firman.JPG	√	√
2.	Salaraso.MP4	√	√

Dari hasil pengujian diatas, maka dapat disimpulkan bahwa penyisipan *file* gambar dengan menerapkan metode *Two Sided Side Match* dapat dilakukan dan memperoleh hasil gambar ekstraksi yang sam dengan gambar yang telah disisipkan ke dalam *file* video. Metode *Two Sided Side Match* merupakan metode yang bisa menjadi solusi untuk penyisipan gambar pada *file* video.

### 4. KESIMPULAN

Berdasarkan hasil dan penelitian yang dilakukan oleh peneliti dari bab-bab sebelumnya maka dapat diambil kesimpulan, kiranya kesimpulan tersebut dapat berguna bagi pembaca. Adapun kesimpulan yang dapat diambil dimana Metode *Two Sided Side Match* dapat digunakan untuk menyisipkan sebuah gambar kedalam video atau media- media lainnya dengan menggunakan teknik steganografi. Penerapan metode *Two Sided Side Match* dapat dilakukan dalam dua proses yaitu proses penyisipan (*embedding*) dan proses ekstraksi dengan menggunakan teknik steganografi. Pengujian yang dilakukan dengan menerapkan aplikasi *visual studio* 2010 sehingga dapat mempermudah proses penyisipan dan proses ekstraksi.

### REFERENCES

Andika, D., & Darwis, D. (2020). Modifikasi Algoritma Gifshuffle Untuk Peningkatan Kualitas Citra Pada Steganografi. *Jurnal Ilmiah Infrastruktur Teknologi Informasi*, 1(2), 19–23.

Azarianpour, S., & Sadri, A. R. (2019). A generalized ghost detection and segmentation method for double-joint photographic experts group compression. *Journal of Medical Signals and Sensors*, 9(4), 211.

Bross, B., Chen, J., Ohm, J.-R., Sullivan, G. J., & Wang, Y.-K. (2021). Developments in international video coding standardization after avc, with an overview of versatile video coding (vvc). *Proceedings of the IEEE*, 109(9), 1463–1493.

Darwis, D., & Pasaribu, A. F. O. (2020). Komparasi Metode Dwt Dan Svd Untuk Mengukur Kualitas Citra Steganografi. *Network Engineering Research Operation*, 5(2), 100–108.

Hafiz, A. (2019). Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB). *Jurnal Cendikia*, 17(1 April), 194–198.



- Ii, B. A. B. (2001). *Universitas Sumatera Utara* 6. 1(2), 6–38.
- Khairina, N. (2016). Analisis Steganografi Metode Two Sided Side Match. *CESS (Journal of Computer Engineering, System and Science)*, 1(2), 7–11.
- Kusrini, 2006:25. (2012). Issn 2252-9063. *Universitas Stuttgart*, 1(5), 444–456.
- Manullang, D. E. P. (2019). Penyisipan Pesan Ke Dalam File Video Menerapkan Metode Chinese Remainder Theorem. *KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer)*, 3(1), 108–117. <https://doi.org/10.30865/komik.v3i1.1576>
- Pamungkas, N. B., Darwis, D., Nurjayanti, D., & Prastowo, A. T. (2020). Perbandingan Algoritma Pixel Value Differencing dan Modulus Function pada Steganografi untuk Mengukur Kualitas Citra dan Kapasitas Penyimpanan. *Jurnal Informatika*, 20(1), 67–77.
- Ratnasari, A. P., & Dwiyanto, F. A. (2020). Metode Steganografi Citra Digital. *Sains, Aplikasi, Komputasi Dan Teknologi Informasi*, 2(2), 52–56.
- Rulin, R. (2007). *PERANCANGAN PROGRAM APLIKASI SEKURITI SOAL UJIAN MENGGUNAKAN TWO-SIDED SIDE MATCH PADA CITRA DIGITAL STUDI KASUS: FMIPA UNIVERSITAS BINA NUSANTARA*. BINUS.
- Swain, G., & Lenka, S. K. (2013). Steganography using two sided, three sided, and four sided side match methods. *CSI Transactions on ICT*, 1(2), 127–133.
- Tarigan, R. S., & Dwiatma, G. (2022). *ANALISA STEGANOGRAFI DENGAN METODE BPCS (Bit-Plane Complexity Segmentation) DAN LSB (Least Significant Bit) PADA PENGOLAHAN CITRA*.
- Winanti, W. (2009). Penyembunyian Pesan pada Citra Terkompresi JPEG Menggunakan Metode Spread Spectrum. *Communications*, 13505017.