LEGITIMASI INFORMASI: *WATERMARKING* DAN *STEGANOGRAPHY*

Disusun oleh:

Kelompok 3

Anita	2217020046
Muhammad Syahril Aprialsyah	2217020056
Agni Ilmi Anaya	2217020065
Hasnatul Fadillah	2217020068
Nur Aminah	2217020069

Kelas 7 SI-B Keamanan Sistem Informasi

Dosen Pengampu

Muhammad Anggun Novembra, S.Si, M.T

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI IMAM BONJOL PADANG

2025

1. *Watermarking*

1.1. Pengertian *Watermarking*

Watermarking digital merupakan salah satu teknik dalam bidang keamanan informasi yang termasuk ke dalam ranah *information hiding* bersama dengan steganografi. Secara sederhana, watermarking didefinisikan sebagai proses menyisipkan informasi tambahan (watermark) ke dalam suatu media digital baik berupa citra, audio, video, maupun dokumen tanpa menyebabkan penurunan kualitas yang signifikan dan tanpa mudah terdeteksi oleh pengamat kasat mata atau indera manusia (Steinebach, Dittmann, and Neuhold 2008), (Al-Dabbas, Azeez, and Ali 2023). Informasi yang disisipkan ini dapat berupa logo, teks, kode identifikasi, bahkan pola sinyal digital tertentu yang dirancang agar dapat diambil kembali dengan prosedur deteksi atau ekstraksi tertentu.

Contoh definisi dari *Encyclopedia of Multimedia* menyebut bahwa watermarking adalah teknik berbasis *information hiding* yang sasaran akhirnya adalah menyisipkan informasi ke dalam sinyal cover (multimedia) menggunakan algoritma embedding, dan kemudian dapat diekstraksi dengan algoritma deteksi menggunakan kunci tertentu.

Berbeda dengan steganografi, tujuan utama watermarking bukanlah untuk menyembunyikan pesan rahasia agar tidak diketahui keberadaannya, melainkan untuk memberikan perlindungan hak cipta, autentikasi, verifikasi integritas, serta pelacakan distribusi konten (Nikolaidis and Pitas 1999). Dalam konteks ini, watermarking menjadi instrumen penting dalam era digital, khususnya ketika distribusi data multimedia semakin masif melalui internet, dan kasus pelanggaran hak cipta maupun duplikasi ilegal semakin marak. Oleh karena itu, watermarking dipandang sebagai salah satu solusi teknis untuk mendukung sistem Digital Rights Management (DRM) dan perlindungan kepemilikan intelektual.

Dalam praktiknya, watermarking memiliki dua bentuk utama, yakni visible watermark dan invisible watermark. Visible watermark biasanya diwujudkan sebagai logo atau teks transparan yang tampak jelas pada gambar atau video—misalnya logo stasiun televisi yang melekat di pojok layar siaran. Sebaliknya, invisible watermark tidak dapat terlihat secara langsung oleh mata, tetapi tertanam dalam struktur sinyal digital sehingga dapat diekstraksi melalui metode komputasi. Invisible watermark inilah yang

banyak digunakan dalam bidang forensik digital, autentikasi dokumen elektronik, serta penelusuran distribusi illegal (Sarkar and Sanyal n.d.), (X. Zhong and F. Y. Shih 2019).

1.2. Klasifikasi *Watermarking*

Watermarking digital dapat diklasifikasikan ke dalam beberapa kategori berdasarkan kriteria yang berbeda, seperti tingkat visibilitas, domain penyisipan, ketahanan terhadap modifikasi, serta kebutuhan data asli dalam proses deteksi. Klasifikasi ini penting untuk memahami kelebihan, kekurangan, serta ruang lingkup aplikasi setiap teknik.

a. Berdasarkan Visibilitas

- Visible Watermark

  Watermark terlihat jelas pada media host, misalnya logo transparan pada foto digital atau tanda stasiun televisi di layar siaran. Fungsi utamanya adalah memberikan klaim kepemilikan secara langsung. Kelebihannya adalah mudah dikenali publik, tetapi kelemahannya rawan dihapus dengan teknik editing.

  Contoh:

  ➢ Situs Stok Foto: Getty Images, Shutterstock, dan Adobe Stock menempatkan logo mereka di seluruh gambar pratinjau.

Gambar 1.1 Watermarking

(Sumber : https://research.google/blog/making-visible-watermarks-more-effective/)

- Siaran Televisi: Logo stasiun TV yang muncul di sudut layar adalah bentuk *visible watermarking*.

Gambar 1.2 Logo Stasiun TV

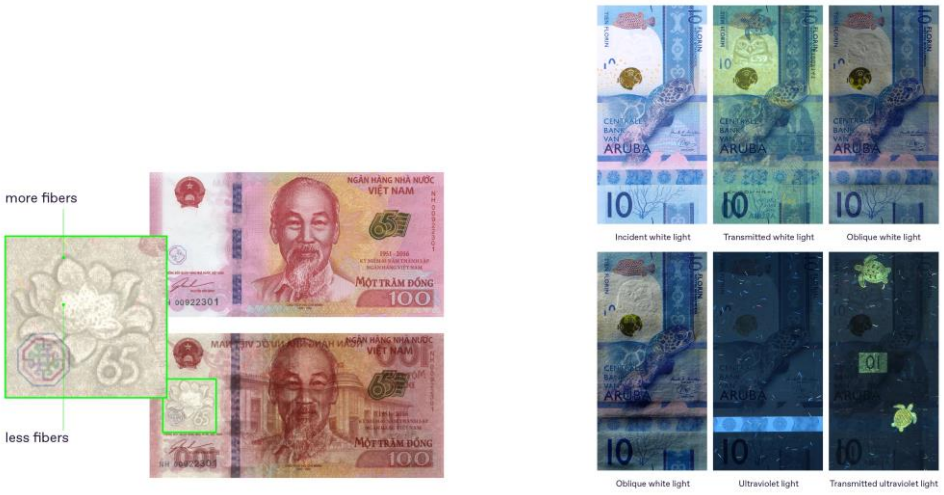
(Sumber : https://unsplash.com/id/foto/layar-televisi-dengan-logo-prime-video-di-atasnya-GgOitQkoioo)

- Fotografer Profesional: Seringkali menambahkan nama atau logo mereka di sudut foto yang mereka unggah ke media sosial.

Gambar 1.3 Logo Fotografer

Sumber : https://fixthephoto.com/id/free-photography-logo-templates

- Otentikasi Mata Uang: Beberapa negara menyematkan pola digital tak terlihat (*digital watermark*) pada desain uang kertas mereka sebagai salah satu fitur keamanan.



Gambar 1.5 otentika Mata Uang

(Sumber : https://static-content.regulaforensics.com/Blog/Vietnamese%20dong.webp)

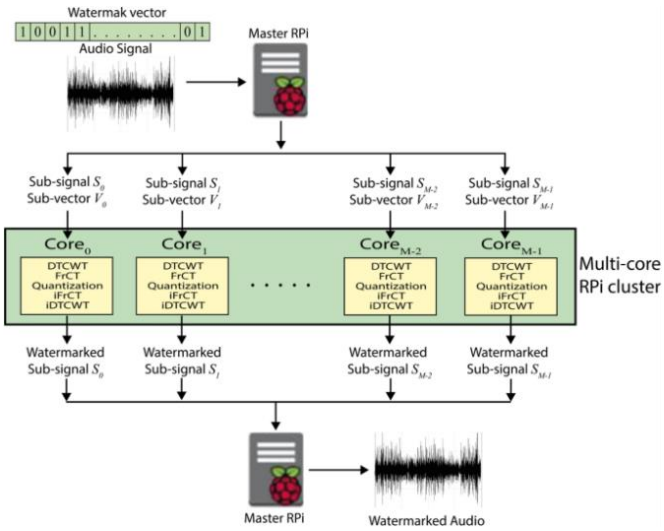
- Invisible Watermark

  Watermark disisipkan sedemikian rupa sehingga tidak dapat dilihat dengan mata manusia. Hanya bisa diekstraksi dengan algoritma khusus. Invisible watermark sering digunakan untuk autentikasi dan penelusuran distribusi ilegal. Ini bertujuan untuk Melacak sumber kebocoran, membuktikan kepemilikan, dan memverifikasi keaslian konten tanpa merusak estetika visual atau audio.

  Invisible watermark lebih populer dalam penelitian akademik karena mendukung *forensic tracking* dan *copyright protection* (Nikolaidis and Pitas 1999), (Steinebach, Dittmann, and Neuhold 2008).

  Contoh:

  - Pelacakan Dokumen Rahasia: Sebuah perusahaan dapat menyisipkan *watermark* tak terlihat yang berbeda pada setiap salinan dokumen yang dibagikan. Jika dokumen tersebut bocor, perusahaan dapat menganalisis file yang bocor untuk mengetahui dari siapa kebocoran itu berasal.
  - Monitoring Siaran: Perusahaan seperti Nielsen menggunakan *invisible audio watermarking* untuk melacak kapan dan di mana sebuah iklan atau acara TV ditayangkan.



Gambar 1.4 monitoring Siaran

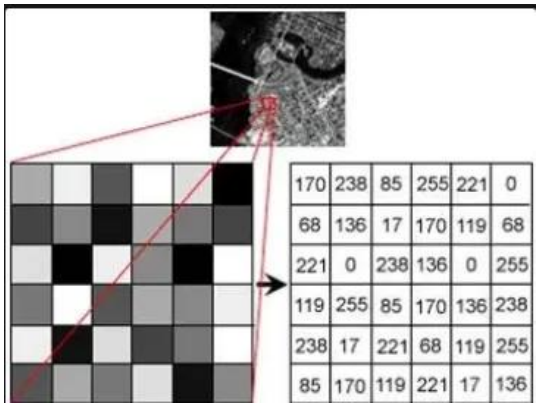
(Sumber : https://media.springernature.com/lw685/springer static/image/art%3A10.1038%2Fs41598-023-45619-w/MediaObjects/41598_2023_45619_Fig7_HTML.png)

b. Berdasarkan Domain Penyisipan

- Spatial Domain Techniques

  Penyisipan dilakukan langsung ke piksel media. Metode sederhana adalah Least Significant Bit (LSB), di mana bit paling rendah pada piksel diganti dengan bit watermark. Keuntungannya mudah diimplementasikan, namun lemah terhadap kompresi dan serangan manipulasi.

  Cocok untuk aplikasi sederhana yang tidak membutuhkan robustness tinggi (Katzenbeisser and Petitcolas 1999).



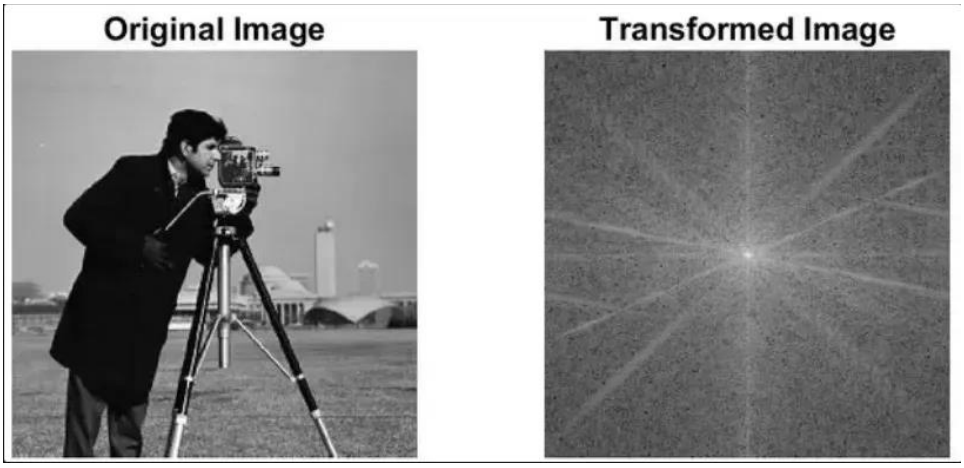
Gambar 1.7 Spatial Domain Techniques

(Sumber:(Chaw Tiri San 2024))

- Frequency/Transform Domain Techniques

  Penyisipan dilakukan pada koefisien hasil transformasi, seperti Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), atau Singular Value Decomposition (SVD). Teknik ini lebih robust terhadap kompresi JPEG, filtering, atau noise.

  Banyak sistem watermarking modern menggunakan domain frekuensi karena keseimbangan antara imperceptibility dan robustness (Sarkar and Sanyal n.d.), (Goos et al. n.d.).



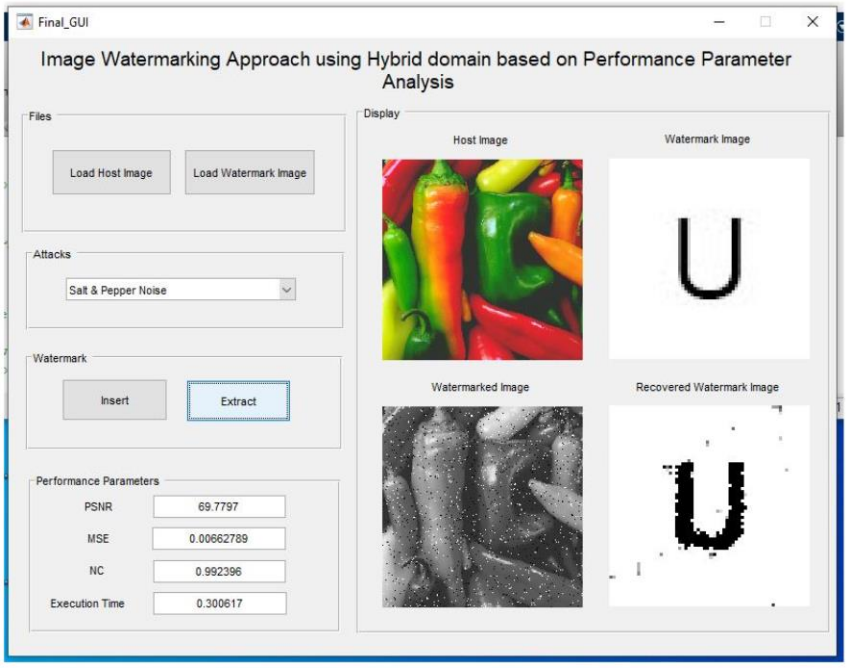
Gambar 1.8 Frequency/Transform Domain Techniques

(Sumber: (Bhat 2015))

- Hybrid Domain Techniques

  Menggabungkan metode spasial dan frekuensi untuk meningkatkan kinerja. Contoh: menyisipkan sebagian watermark dengan LSB, sebagian lain pada koefisien DWT.

  Teknik hibrid terbukti memperbaiki ketahanan terhadap serangan tanpa mengorbankan kualitas media (Chen Phin, Hidayah Ab Rahman, and Che Pa n.d.).



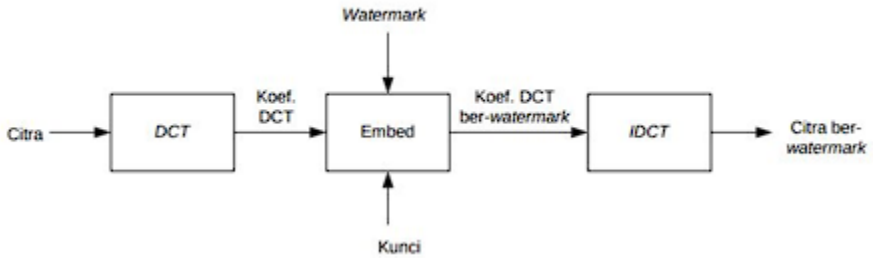
Gambar 1.9 Hybrid Domain Techniques

(Sumber: (Srivastava et al. 2021))

c. Berdasarkan Ketahanan (Robustness)

- Robust Watermarking

  Dirancang agar watermark tetap bertahan meski media host mengalami manipulasi, misalnya kompresi, rotasi, cropping, filtering, atau konversi format. Digunakan untuk hak cipta dan *ownership verification*.



Gambar 1.10 Robust Watermarking

(Sumber: (Ardian Wirasandi- n.d.))

- Fragile Watermarking

  Mudah rusak bila media dimodifikasi. Justru dipakai untuk deteksi manipulasi (tamper detection). Jika watermark hilang atau berubah, artinya

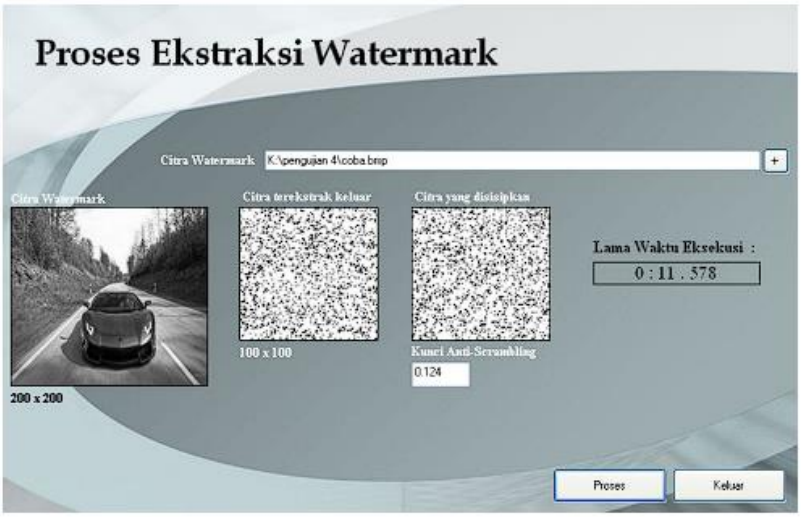
file telah dimodifikasi. Cocok untuk autentikasi dokumen digital atau rekam medis elektronik.

Gambar 1.11 Fragile Watermarking

(Sumber: (Diki Ardian Wirasandi-13515092))

- Semi-Fragile Watermarking

  Bertahan terhadap modifikasi yang tidak signifikan (misalnya kompresi JPEG ringan), tetapi rusak jika ada modifikasi berat. Banyak digunakan untuk verifikasi konten.



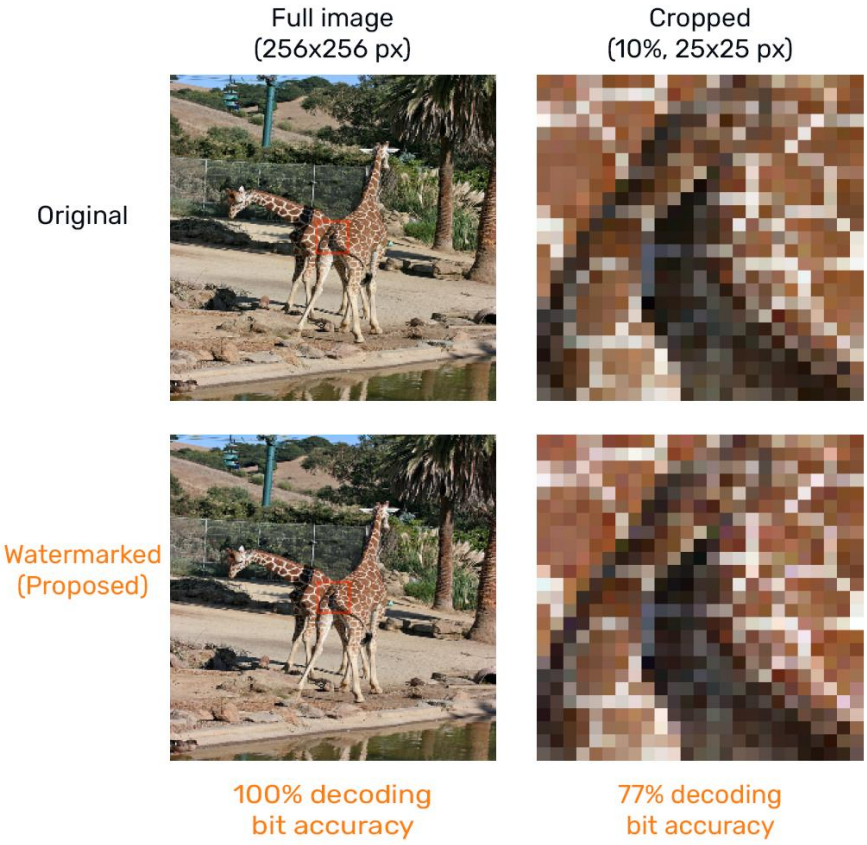
Gambar 1.12 Semi-Fragile Watermarking

(Sumber: (Andri, Ng Poi Wong, and Johnny Fransiscus 2014))

d. Berdasarkan Kebutuhan Data Asli (Detection Method)

- Blind Watermarking

  Deteksi watermark dapat dilakukan tanpa memerlukan media asli (cover image). Lebih praktis karena media asli tidak selalu tersedia. Namun tingkat akurasi deteksi kadang lebih rendah.



Gambar 1.13 Blind Watermarking

(Sumber:(IDLab-Media 2023))

- Non-Blind Watermarking

  Proses deteksi memerlukan media asli untuk membandingkan dengan hasil embedding. Akurasinya tinggi, tetapi implementasi lebih sulit karena membutuhkan akses ke file asli.

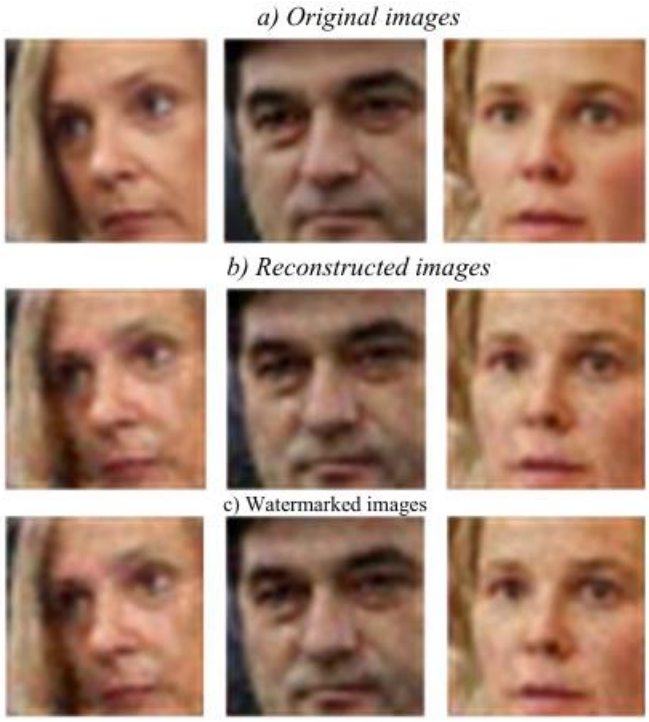
No	Citra *Host*	Citra Terwatermark
1		
	PSNR 39.1529 dB dan SSIM 0.9995 dB	
2		
	PSNR 39.1529 dB dan SSIM 0.9953 dB	
3		
	PSNR 39.1529 dB dan SSIM 0.9976 dB	
4		
	PSNR 39.1529 dB dan SSIM 0.9939 dB	
5		
	PSNR 39.1529 dB dan SSIM 0.9972 dB	

Gambar 1.14 Non-Blind Watermarking

(Sumber: (Sinaga and Jatmoko 2022))

- Semi-Blind Watermarking

  Deteksi hanya memerlukan sebagian informasi dari media asli atau kunci tertentu, sehingga menjadi kompromi antara blind dan non-blind (Al-Dabbas, Azeez, and Ali 2023) .



Gambar 1.15 Semi-Blind Watermarking

(Sumber: (Saeed Khalilidan and Zahra Moti 2020))

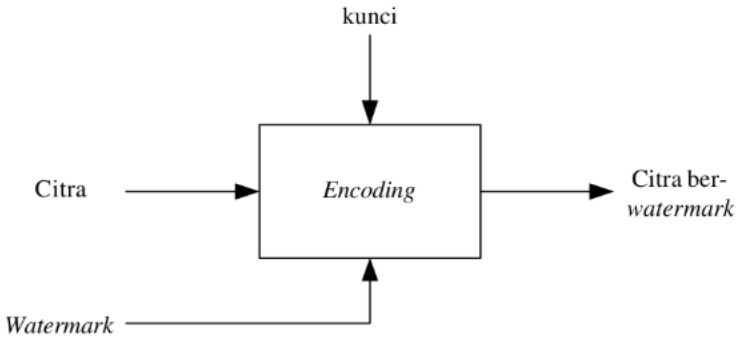
e. Berdasarkan Tujuan Aplikasi

- Copyright Protection digunakan untuk membuktikan kepemilikan karya digital.
- Authentication & Tamper Detection untuk memastikan data tidak dimodifikasi tanpa izin.
- Fingerprinting untuk memberikan watermark berbeda pada tiap salinan, sehingga bisa dilacak siapa yang membocorkan file.
- Broadcast Monitoring untuk memantau distribusi media digital di jaringan penyiaran.

1.3.Implementasi Penyisipan Watermark

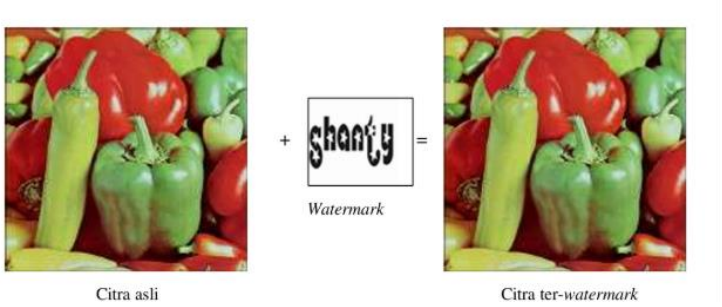
Di sini kita hanya meninjau watermarking pada citra digital. Proses penyisipan watermark ke dalam citra disebut encoding dan ditunjukkan Gambar 1.16. Encoding dapat disertai dengan pemasukan kunci atau tidak memerlukan kunci. Kunci diperlukan agar watermark hanya dapat diekstraksi oleh pihak yang sah.

Kunci juga dimaksudkan untuk mencegah watermark dihapus oleh pihak yang tidak berhak. (Garcia et al. n.d.).



Gambar 1.16 Proses penyisipan watermark pada citra digital

Sumber : (Munir 2004)



Gambar 1.17 Memberi watermark pada citra peppers

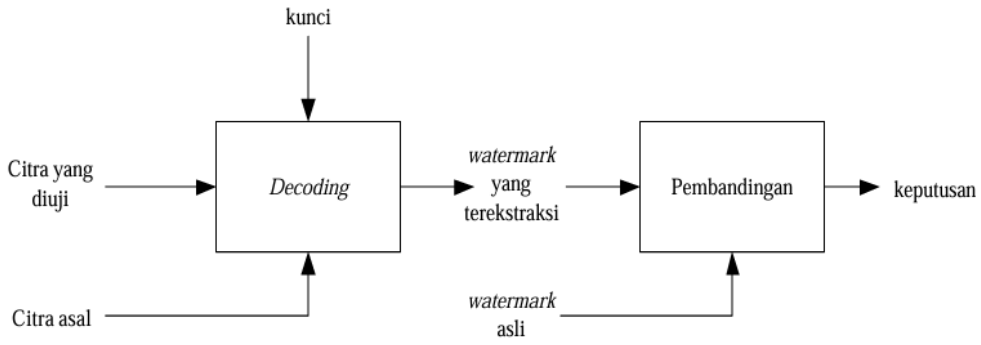
Sumber : (Munir 2004)

1.4.Verifikasi Watermarking

Verifikasi watermark dilakukan untuk membuktikan status kepemilikan citra digital yang disengketakan. Verifikasi watermark terdiri atas dua sub-proses, yaitu ekstraksi watermark dan pembandingan.

Sub-proses ekstraksi watermark disebut juga decoding, bertujuan mengungkap watermark dari dalam citra. Decoding dapat mengikutsertakan citra asal (yang belum diberi watermark) atau tidak sama sekali, karena beberapa skema watermarking memang menggunakan citra asal dalam proses decoding untuk meningkatkan unjuk kerja yang lebih baik .

Sub-proses pembandingan bertujuan membandingkan watermark yang diungkap dengan watermark asli dan memberi keputusan tentang watermark tersebut. Proses verifikasi watermark ditunjukkan pada Gambar 1.18.



Gambar 1.18 Proses verifikasi watermark pada citra digital

Sumber (Munir 2004)

2. *Steganography*

2.1. Pengertian *Steganography*

Steganografi (*steganography*) merupakan ilmu sekaligus seni dalam menyembunyikan pesan rahasia (*hiding message*) sehingga keberadaan pesan tersebut tidak dapat terdeteksi oleh indera manusia. Istilah "steganografi" sendiri berasal dari bahasa Yunani, yang secara harfiah berarti *covered writing* atau "tulisan tersembunyi" (Sion 2018). Hal ini menegaskan bahwa tujuan utama steganografi bukan hanya menyamarkan isi pesan, melainkan juga menyembunyikan eksistensinya agar tidak diketahui pihak ketiga.

Dalam implementasinya, steganografi membutuhkan dua komponen utama, yaitu wadah penampung (cover media) dan data rahasia yang akan disembunyikan. Pada era digital, perkembangan teknologi informasi telah memperluas penerapan steganografi, di mana media digital seperti citra, suara, teks, dan video berfungsi sebagai wadah penampung. Sementara itu, data rahasia yang disisipkan juga bersifat fleksibel karena dapat berupa citra, suara, teks, maupun video. Dengan demikian, teknik steganografi memiliki ruang lingkup yang sangat luas dalam hal variasi media dan jenis data yang dapat disembunyikan (Davidson and Martiscia 2024).

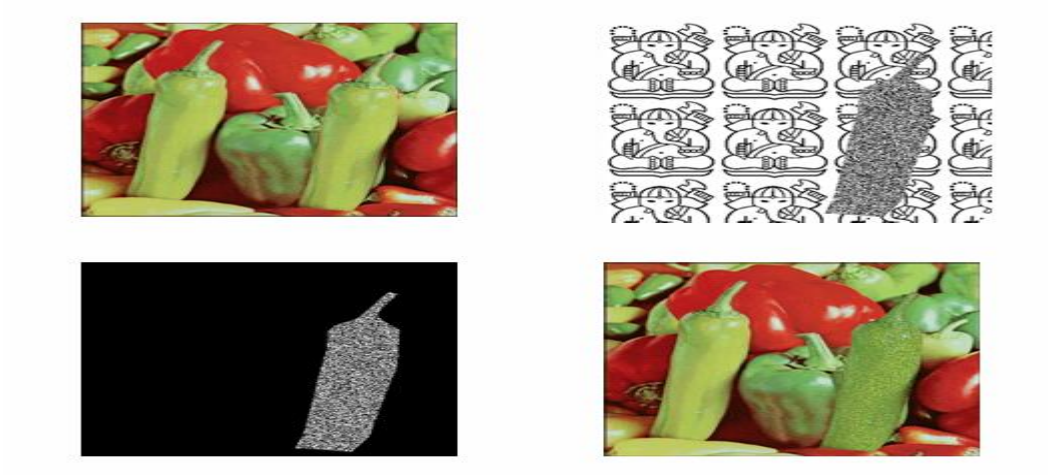
Lebih lanjut, steganografi dapat dipandang sebagai kelanjutan dari kriptografi. Pada kriptografi, pesan asli terlebih dahulu diubah menjadi bentuk tersandi (*ciphertext*) sehingga isinya tidak dapat dipahami tanpa kunci tertentu. Namun, keberadaan ciphertext tersebut tetap terlihat dan dapat memunculkan kecurigaan. Sebaliknya, steganografi berupaya menyembunyikan ciphertext di dalam media penampung sehingga pihak ketiga bahkan tidak menyadari adanya pesan rahasia di dalamnya. Dengan cara ini, keamanan komunikasi dapat ditingkatkan melalui kombinasi antara kerahasiaan isi dan penyembunyian eksistensi pesan.

Konteks penerapan steganografi menjadi semakin relevan di negara-negara yang memberlakukan penyensoran informasi. Dalam situasi semacam ini, steganografi sering dimanfaatkan untuk menyelundupkan pesan-pesan rahasia tanpa memunculkan kecurigaan, misalnya dengan menyisipkan informasi ke dalam gambar (*images*), video, maupun file suara (*audio*)(Margie Semilof 2023). Fakta ini menunjukkan bahwa steganografi tidak hanya berfungsi sebagai teknologi keamanan informasi, tetapi juga memiliki dimensi sosial dan politik yang erat kaitannya dengan kebebasan berekspresi dan distribusi informasi di masyarakat.

2.2.Kriteria Steganografi

data yang disembunyikan tidak hanya berupa teks, tetapi juga berupa citra, audio, atau video. Selain citra digita, media penampung data rahasia juga bisa berupa teks, audio, atau video (Munir 2004). Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah:

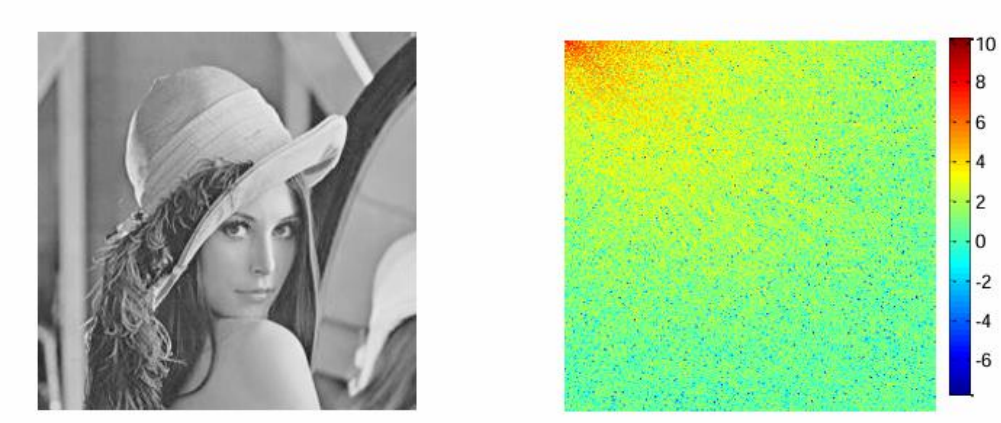
a) **Fidelity**. Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.



Gambar 2.1 Fidelity
(Sumber: (Diki Ardian Wirasandi-13515092))

Gambar di atas merupakan Contoh penampung citra dimana hasil dari gambar yang dimasukkan data rahasia namun citra masih terlihat baik tanpa kerusakan pada gambar .

b) **Robustness.** Data yang disembunyikan harus tahan (robust) terhadap berbagai operasi manipulasi yang dilakukan pada citra penampung, seperti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (cropping), enkripsi, dan sebagainya. Bila pada citra penampung dilakukan operasi-operasi pengolahan citra tersebut, maka data yang disembunyikan seharusnya tidak rusak (tetap valid jika diekstraksi kembali)



Gambar 2.2 Robustness
(Sumber: (Ma et al. 2023))

c) **Recovery.** Data yang disembunyikan harus dapat diungkapkan kembali (reveal). Karena tujuan steganografi adalah data hiding, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

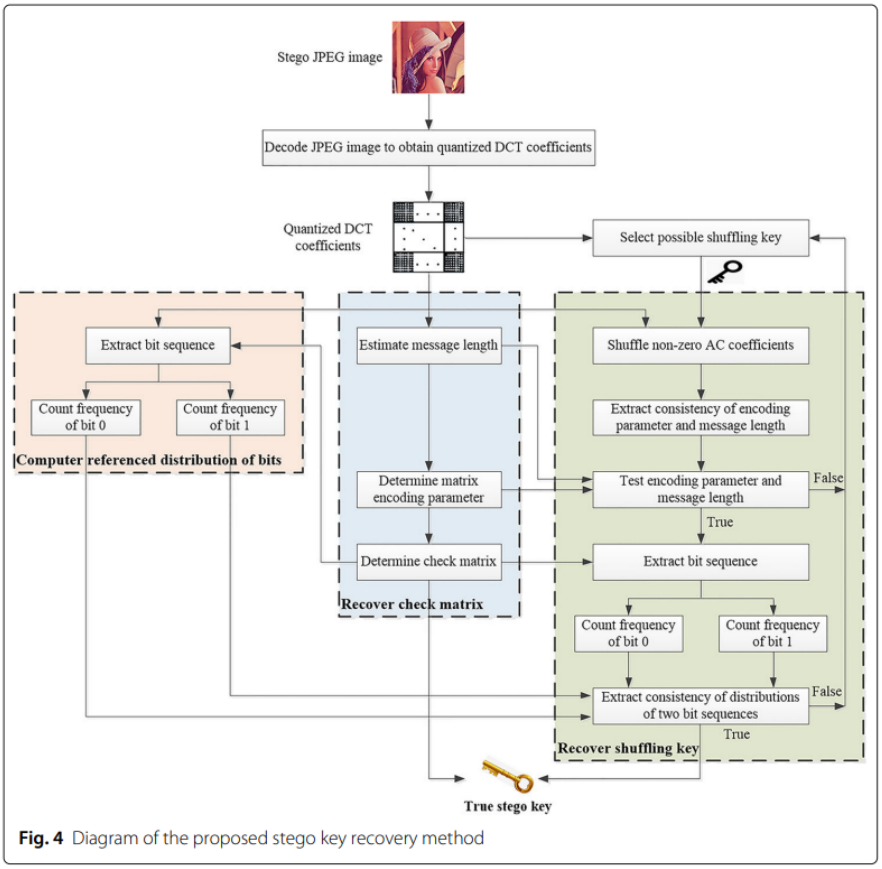


Fig. 4 Diagram of the proposed stego key recovery method

Gambar 2.3 Proses r*ecovery pada sebuah citra*

(Sumber: (Diki Ardian Wirasandi-13515092))

2.3.Klasifikasi *Steganography*

Steganografi adalah seni dan ilmu menyembunyikan informasi dalam suatu media digital sehingga keberadaannya tidak mudah terdeteksi. Untuk memahami ruang lingkupnya, steganografi dapat diklasifikasikan berdasarkan media penampung, domain penyisipan, robustness, kebutuhan kunci, serta strategi penyisipan.

a. Berdasarkan Media Penampung

- Image Steganography

  Media host berupa citra digital. Teknik paling populer adalah Least Significant Bit (LSB), yang mengganti bit paling rendah pada piksel dengan

bit pesan rahasia. Citra sering dipilih karena memiliki redundansi tinggi dan toleransi manusia terhadap perubahan warna kecil.

Contoh: penyisipan teks dalam format BMP atau PNG (Fridrich 2010).

Bayangkan sebuah piksel dengan nilai warna biru 11010101 (desimal 213). Jika kita ingin menyisipkan bit '0' dari pesan rahasia, nilainya menjadi 11010100 (desimal 212). Perbedaan warna antara 213 dan 212 sangatlah tipis dan tidak akan terlihat. Teknik yang paling umum untuk adalah **Least Significant Bit (LSB)**. Setiap piksel dalam sebuah gambar digital terdiri dari nilai warna Merah, Hijau, dan Biru (RGB). Setiap nilai warna ini direpresentasikan oleh 8 bit angka (misalnya, 11010101). Metode LSB mengubah bit *terakhir* (yang paling tidak signifikan) dari setiap nilai warna untuk menyisipkan data dari pesan rahasia. Perubahan ini sangat kecil sehingga tidak dapat dideteksi oleh mata manusia

Gambar 2.4 Image Steganography

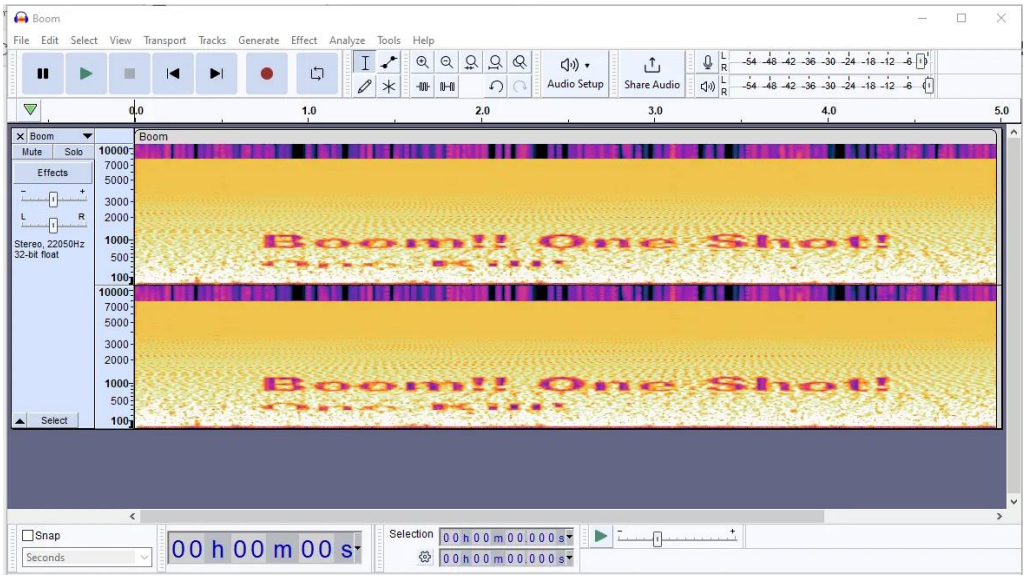
(Sumber: (Image steganography: Concealing secrets within pixels 2023))

- Audio Steganography

Informasi disembunyikan di dalam file audio. Teknik umum meliputi LSB coding, phase coding, echo hiding, dan spread spectrum. Audio memiliki kapasitas cukup besar dan modifikasi kecil sulit dideteksi oleh telinga manusia [2].

Contoh: Sebuah pesan teks diubah menjadi bit, lalu bit-bit ini disisipkan ke dalam bit terakhir dari setiap sampel data dalam file WAV atau MP3. Saat file audio diputar, suara terdengar normal. Metode yang digunakan Sama seperti gambar, metode **LSB** dapat digunakan pada setiap *sampel* audio

digital. Cara lain adalah dengan menyembunyikan data pada frekuensi suara yang tidak dapat didengar oleh telinga manusia (sangat tinggi atau sangat rendah).

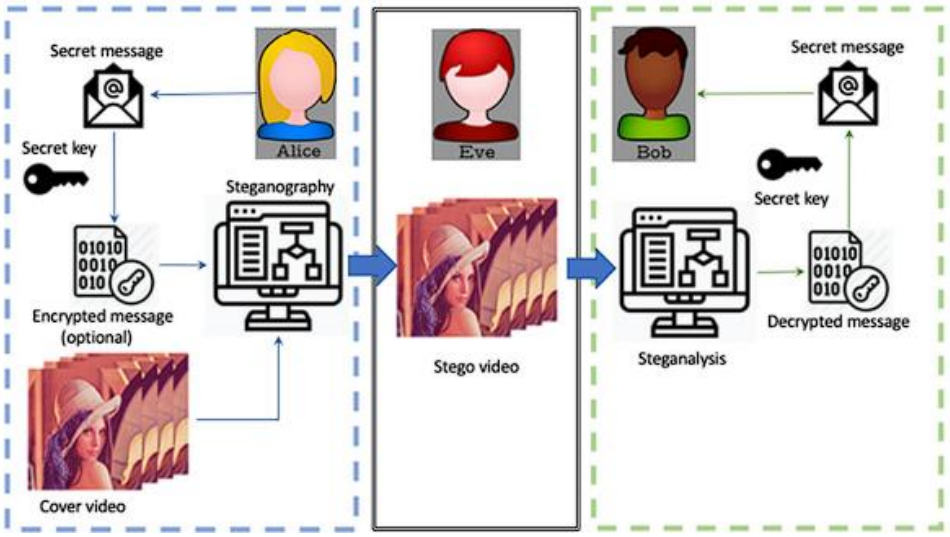


Gambar 2.5 Audio Steganography

(Sumber: (Aung Kyaw Zall 2023))

- Video Steganography

Menggunakan file video sebagai wadah. Data dapat disisipkan pada frame individu atau pada transformasi frekuensi. Keunggulannya adalah kapasitas tinggi, namun kompleksitas juga lebih besar.



Gambar 2.6 Video Steganography

(Sumber: (Kunhoth et al. 2023))

- Text Steganography

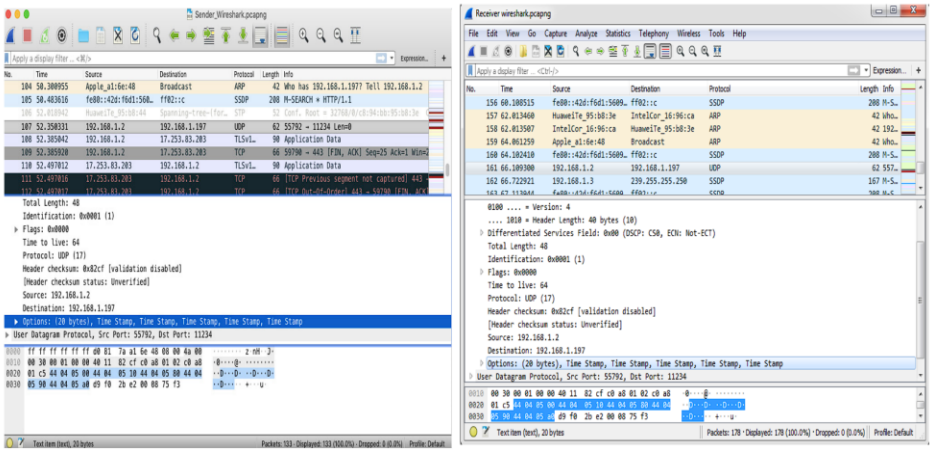
  Data disisipkan dalam teks, misalnya dengan manipulasi spasi, tanda baca, atau sinonim. Kapasitas terbatas dan lebih mudah terdeteksi, tetapi masih digunakan dalam aplikasi ringan (H. Shirali-Shahreza and M. Shirali-Shahreza 2007).

  Contoh: **“S**elalu **e**ling **l**akukan **a**turan **m**enjaga **a**manah **t**ersebut.”

  Jika kita ambil huruf pertama dari setiap kata, kita akan mendapatkan pesan tersembunyi: "SELAMAT"**.** Metode yang digunakan bisa sangat kreatif. Misalnya contoh diatas dengan menggunakan huruf pertama dari setiap kata untuk membentuk pesan rahasia (akrostik), atau dengan menggunakan spasi ganda setelah tanda baca tertentu, atau bahkan menggunakan karakter spasi tak terlihat (zero-width characters).

- Network Steganography

  Informasi rahasia disisipkan dalam lalu lintas jaringan, misalnya header TCP/IP atau pola pengiriman paket. Metode ini sering digunakan dalam konteks keamanan jaringan (Zander, Armitage, and Branch 2007).



Gambar 2.7 Network Steganography

(Sumber: Bedi and Dua 2020)

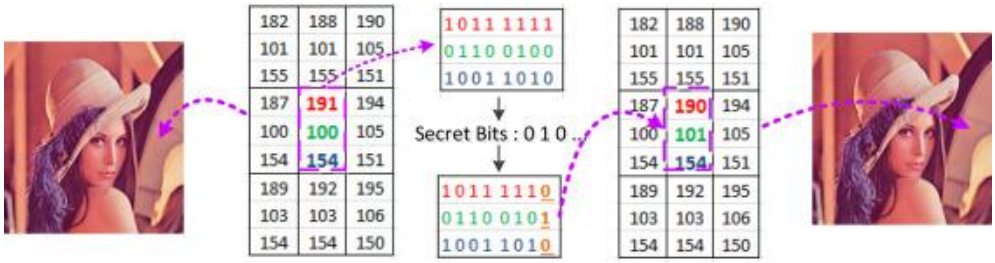
b. Berdasarkan Domain Penyisipan

- Spatial Domain Techniques

  Pesan rahasia disisipkan langsung ke media host (misalnya piksel citra atau sampel audio).

  ➢ Kelebihan: sederhana, kapasitas relatif besar.

- Kekurangan: rentan terhadap kompresi dan manipulasi.



Gambar 2.7 Spatial Domain Techniques

(Sumber: https://ars.els-cdn.com/content/image/1-s2.0-S092359651830256X-gr5.jpg)

- Transform Domain Techniques

  Data disisipkan pada koefisien hasil transformasi seperti Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), atau Fourier Transform.

  - Kelebihan: lebih robust terhadap kompresi (misalnya JPEG).
  - Kekurangan: lebih kompleks dalam implementasi (Provos and Honeyman 2003).

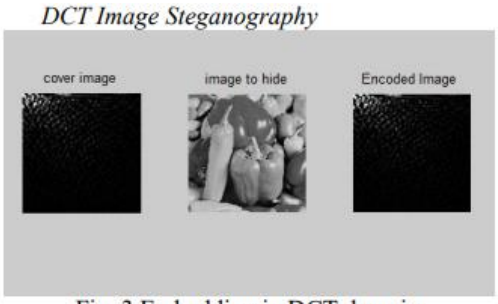


Fig. 3 Embedding in DCT domain

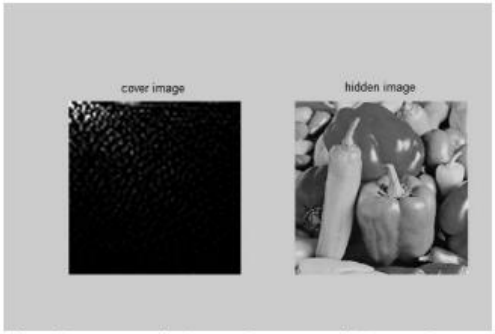


Fig. 4 Recovered Cover Image and Secret Image

Gambar 2.8 Discrete Cosine Transform

(Sumber: (Bhat 2015))

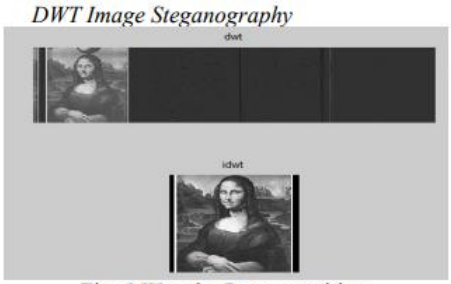


Fig. 5 Wavelet Decomposition

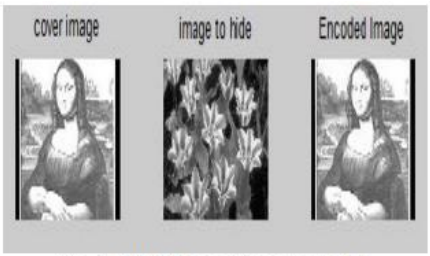


Fig. 6 DWT Image Steganography

Fig. 7 Recovered Cover Image and Hidden Image

Gambar 2.9 Discrete Wavelet Transform
(Sumber:(Bhat 2015))

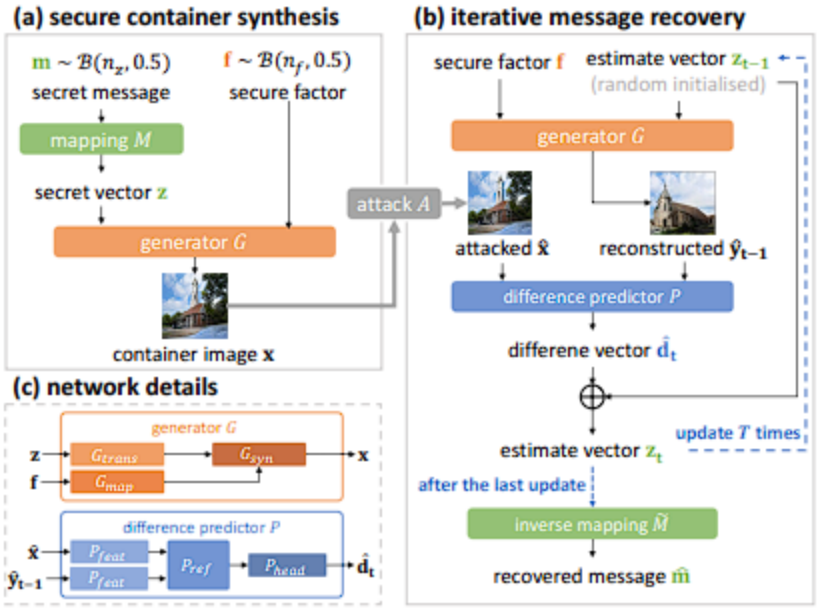
c. Berdasarkan Robustness

- Fragile Steganography

  Mudah rusak jika media host dimodifikasi. Biasanya dipakai untuk content authentication.

- Robust Steganography

  Tetap dapat bertahan walaupun terjadi kompresi atau manipulasi ringan. Cocok untuk komunikasi rahasia yang harus melewati banyak tahap transmisi.



Gambar 2.10 Proses robust steganography

(Sumber: Ma et al. 2023)

- Semi-Fragile Steganography

  Bertahan terhadap perubahan minor (misalnya kompresi ringan), namun hilang bila terjadi perubahan besar (Cheddad et al. 2010).

d. Berdasarkan Kebutuhan Kunci

- Pure Steganography

  Tidak memerlukan kunci khusus, hanya mengandalkan kerahasiaan metode penyisipan.

- Secret-Key Steganography

  Menggunakan kunci rahasia bersama untuk proses embedding dan ekstraksi. Tingkat keamanannya lebih tinggi.

- Public-Key Steganography

  Mengadaptasi prinsip kriptografi asimetris: kunci publik digunakan untuk embedding, sementara kunci privat dipakai untuk ekstraksi (Hameed et al. 2019).

e. Berdasarkan Strategi Penyisipan

- Static Steganography

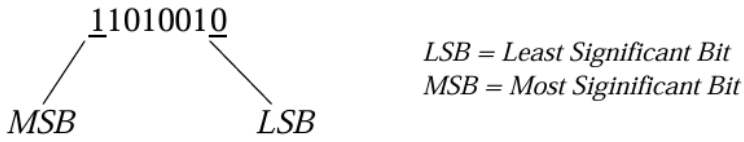
  Algoritma embedding tidak berubah, tidak memperhatikan karakteristik media host.

- Adaptive Steganography

  Algoritma disesuaikan dengan karakteristik media. Misalnya, penyisipan dilakukan pada area gambar dengan tekstur tinggi agar lebih sulit dideteksi. Adaptive techniques terbukti meningkatkan imperceptibility (Katzenbeisser and Petitcolas 1999).

2.4.Implentasi Teknik penyembunyian data pada steganografi

Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Hingga saat ini sudah banyak dikemukakan oleh para ilmuwan metode-metode penyembunyian data. Metode yang paling sederhana adalah metode modifikasi LSB (Least Significant Bit Modification). Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB). Sebagai ilustrasi, di bawah ini dijelaskan metode modifikasi LSB untuk menyisipkan watermark pada citra (gambar) digital.perhatikan contoh sebuah susunan bit pada sebuah byte:

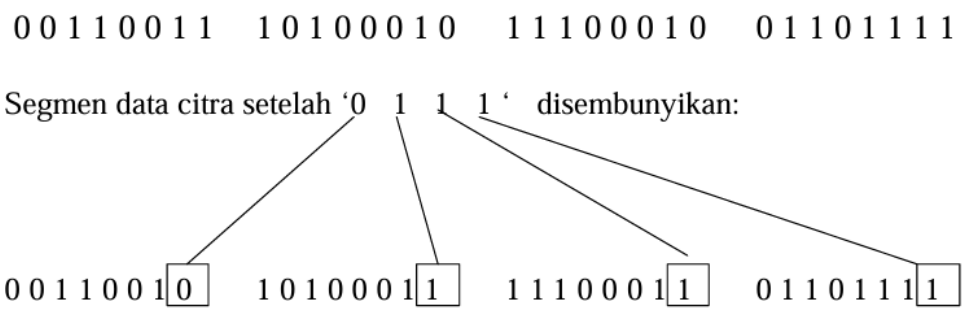


Gambar 2.11 susunan bit

Sumber :(Watermarking and Steganografi 2004)

Bit yang cocok untuk diganti adalah bit LSB, sebab penggantian hanya mengubah nilai byte tersebut satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut di dalam gambar menyatakan warna tertentu, maka perubahan satu bit LSB tidak mengubah warna tersebut secara berarti. Lagi pula, dan ini keuntungan yang dimanfaatkan, mata manusia tidak dapat membedakan perubahan yang kecil.

Misalnya Segmen data citra sebelum perubahan :



Gambar 2.12 segmen data citra

Sumber:(Watermarking and Steganografi 2004)

Untuk memperkuat penyembunyian data, bit-bit data tidak digunakan untuk mengganti byte-byte yang berurutan, namun dipilih susunan byte secara acak. Misalnya jika terdapat 50 byte dan 6 bit data yang akan disembunyikan, maka byte yang diganti bit LSB-nya dipilih secara acak, misalkan byte nomor 36, 5, 21, 10, 18, 49.

Bilangan acak dibangkitkan dengan pseudo-random-number-generator (PRNG). PRNG menggunakan kunci rahasia untuk membangkitkan posisi pixel yang akan digunakan untuk menyembunyikan bit-bit. PRNG dibagun dalams ejumlah cara, salah satunya dengan menggunakan algoritma kriptografi DES (Data Encryption Standard), algoritma hash MD5, dan mode kriptografi CFB (Chiper-Feedback Mode). Tujuan dari enkripsi adalah menghasilkan sekumpulan bilangan acak yang sama untuk setiap kunci enkripsi yang sama. Bilangan acak dihasilkan dengan cara memilih bit-bit dari sebuah blok data hasil enkripsi (Munir 2004).

Contoh ilustrasi , gambar 2.13 dibawah ini adalah citra lada (peppers. bmp) yang akan digunakan sebagai media untuk pemnyimpan sebuah data nantinya dalam bentuk word (hendro . Doc) pada gambar 2.14

Gambar 2.13 peppers . Bmp

Sumber : (Watermarking and Steganografi 2004)

LETTER OF RECOMMENDATION

To Whom It May Concern,

Herewith I highly recommend **Mr. R. Hendro Wicaksono** continue his postgradu
study at your university. My recommendation is based on my experience as
lecturer in several courses for the past four years.

He has shown me his excellent attitude and personality. He is a hard working pers
and he has a lot of creative ideas. He is also a very intelligent student and
cooperates very well with his peers whenever they had to work together.

During his study, he showed diligence and eagerness to achieve his goal. He sets v
high standard for himself and organizes himself very well to achieve the standard
am confident that if he can maintain his goal work, he should be able to complete
postgraduate program well within the stipulated time.

I am sure that his abilities and his personal qualities along with his acade
capabilities will help his to obtain his Master's degree at your university, which w
be very useful for our country.

Bandung, November 15, 2002
Yours Sincerely,

Ir. Rinaldi Munir, M.Sc.
Senior Lecturer
Informatics Engineering Department,
Institute Technology of Bandung (ITB)
Jl. Ganesha No. 10, Bandung 40132
Email : rinaldi@informatika.org
Phone +62-22-2508135
Indonesia

Gambar 2. 14 hendro. Doc

Sumber : (Watermarking and Steganografi 2004)

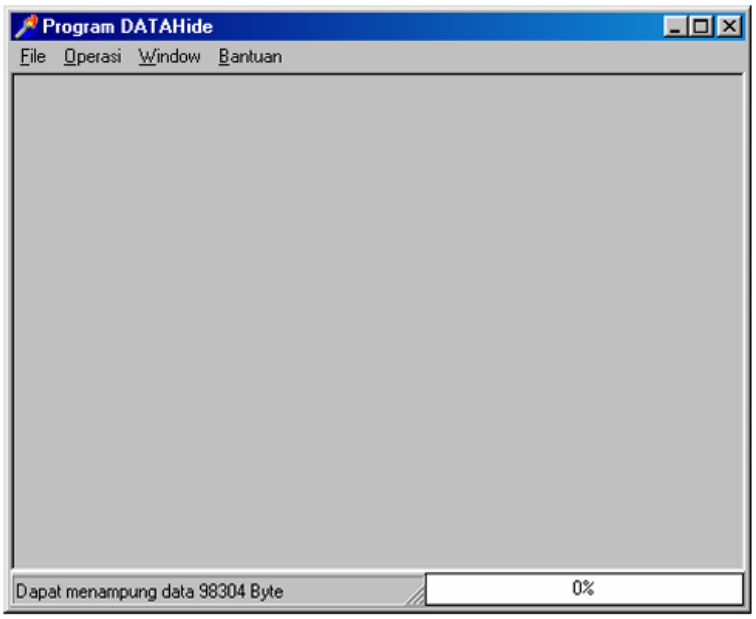
Hasil penyembunyian data pada file *peppers.bmp* dengan file *hendro.doc* ditunjukkan pada Gambar 2.15 di bawah ini. Terlihat bahwa gambar masih tampak sama dan tidak menunjukkan adanya perubahan meskipun data telah disisipkan.

Gambar 2.15 citra lada seteaah diisii dengan data teks

2.5.Teknik pengungkapan data pada steganografi

Data yang disembunyikan di dalam citra dapat dibaca kembali dengan cara pengungkapan (reveal atau extraction). Posisi byte yang menyimpan bit data dapat diketahui dari bilangan acak yang dibangkitkan oleh PRNG. Karena algoritma kriptografi yang digunakan menggunakan kunci pada proses enkripsi, maka kunci yang sama digunakan untuk membangkitkan bilangan acak. Bilangan acak yang dihasilkan sama dengan bilangan acak yang dipakai pada waktu penyembunyian data. Dengan demikian, bit-bit data rahasia yang bertaburan di dalam citra dapat dikumpulkan kembali.

Contoh steganografi berikut diadaptasi dari program Tugas Akhir Lazarus Poli [POL98] yang diberi nama *DATAhide*. Pada setiap contoh digunakan kunci yang sama, yaitu *informatika*. Gambar 2.16 memperlihatkan tampilan awal program. Pada menu Operasi terdapat dua sub-menu, yaitu Penyembunyian Data dan Pengungkapan Data.



Gambar 2.16 Upa-menu pada Operasi: penyembunyian data dan pengungkapan data

Sumber : (Watermarking and Steganografi 2004)

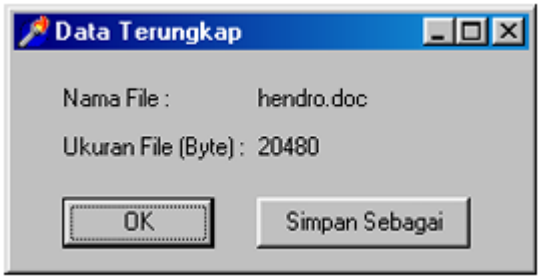
Citra penampung : peppers. Bmp (512 x 512 pixel) yang ada pada gambar 2.13

Data yang akan di sembunyikan: dalam bentuk dokumnet word yang ada pada gambar 2.14 yaitu hendro. Doc (20 KB)

Hasil dari penyembunyian data (peppers. Bmp + hendro. Doc)

Gambar 2. 17 Hasil dari penyembunyian data

Hasil dari ekstraksi data menggunakan DATAhide:



Sumber:

Gambar 2. 18 Hasil ektraksi data menggunakan DATAhide

Berkas hendro-stega. Doc yang sudah di ekstraksi dari citra peppers.bmp sebelumnya.

LETTER OF RECOMMENDATION

To Whom It May Concern,

Herewith I highly recommend **Mr. R. Hendro Wicaksono** continue his postgradua study at your university. My recommendation is based on my experience as his lecturer several courses for the past four years.

He has shown me his excellent attitude and personality. He is a hard working person a he has a lot of creative ideas. He is also a very intelligent student and he cooperates ve well with his peers whenever they had to work together.

During his study, he showed diligence and eagerness to achieve his goal. He sets ve high standard for himself and organizes himself very well to achieve the standard. I a confident that if he can maintain his goal work, he should be able to complete t postgraduate program well within the stipulated time.

I am sure that his abilities and his personal qualities along with his academic capabilit will help his to obtain his Master's degree at your university, which will be very use for our country.

Bandung, November 15, 2002
Yours Sincerely,

Ir. Rinaldi Munir, M.Sc.
Senior Lecturer
Informatics Engineering Department,
Institute Technology of Bandung (ITB)
Jl. Ganesha No. 10, Bandung 40132
Email : rinaldi@informatika.org
Phone +62-22-2508135
Indonesia

Gambar 2. 19 Berkas hendro-stega

2.6.Metode penyisipan

Metode steganografi dan watermarking digunakan untuk menyembunyikan informasi dalam media digital (gambar, audio, video teks), namun steganografi bertujuan untuk menyembunyikan pesan rahasia agar tidak terdekteksi keberdaannya yang di letakkan di dlam media,sedangkan watermarking bertujuan untuk menyisipkan informasi (misalnya logo, kode identitas,metadat) untuk melindungi hak cipta atau otentika.bebrapa metode memang sama secara teknis, namun untuk melindungi hak cipta atau otentika beberapa metode memang sama secara teknis, namun pengguanaannya berbeda konteks yang terdiri dari

1. *Least Significant Bit Insertion (LSB)*. menyisipkan bit watermark pada bit paling rendah (bit ke-8) dari nilai intensitas piksel. Karena perubahan hanya terjadi pada bit terakhir, maka dampak terhadap kualitas visual gambar sangat kecil.. Contohnya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap pixel berkas bitmap 24 bit kita dapat menyisipkan 3 bit data. Kekurangan dari LSB Insertion: Dapat diambil kesimpulan dari contoh 8 bit pixel, menggunakan LSB Insertion dapat secara drastis mengubah unsur pokok warna dari pixel. Ini dapat menunjukkan perbedaan yang nyata dari cover image menjadi stego image, sehingga tanda tersebut menunjukkan keadaan dari steganografi. Variasi warna kurang jelas dengan 24 bit image, bagaimanapun file tersebut sangatlah besar. Antara 8 bit dan 24 bit image mudah diserang dalam pemrosesan image, seperti cropping (kegagalan) dan compression (pemampatan). Keuntungan dari LSB Insertion : Keuntungan yang paling besar dari algoritma LSB ini adalah cepat dan mudah. Dan juga algoritma tersebut memiliki software steganografi yang mendukung dengan bekerja di antara unsur pokok warna LSB melalui manipulasi pallete (lukisan).

2. Discrete Cosine Transform (DCT)

   Discrete Cosine Transform (DCT) membagi gambar menjadi blok-blok (biasanya 8x8 piksel), lalu setiap blok diubah ke domain frekuensi menggunakan DCT. *Menyisipkan* dengan mengubah nilai koefisien DCT pada frekuensi menengah, yang relatif tahan terhadap kompresi (seperti JPEG) namun tidak terlalu memengaruhi kualitas visual.

3. Discrete Wavelet Transform (DWT)

   DWT memecah gambar menjadi beberapa level sub-pita frekuensi (LL, LH, HL, HH). Ini memungkinkan penyisipan pada area yang paling sesuai dengan persepsi mata manusia, sehingga menjadi lebih tidak terlihat dan lebih tangguh. Biasanya disisipkan pada koefisien di sub-pita frekuensi rendah atau menengah, yang menyimpan sebagian besar energi dan informasi visual gambar.

4. Singular Value Decomposition (SVD)

   Prinsip dasar dari SVD adalah memecah matriks citra menjadi tiga komponen, yaitu matriks ortogonal *U*, matriks diagonal berisi nilai singular *S*, dan matriks ortogonal transpos V^T. penyisipan informasi rahasia biasanya dilakukan pada bagian nilai singular karena sifatnya yang relatif stabil terhadap berbagai manipulasi seperti kompresi, penambahan noise, atau rotasi. Dengan demikian, pesan atau watermark yang ditanamkan tetap dapat dipertahankan tanpa merusak kualitas visual citra asli secara signifikan (R. Liu and Tan 2002)

5. Hybrid

   Tujuan utama penggunaan hybrid adalah meningkatkan **robustness** (ketahanan terhadap serangan manipulasi), **imperceptibility** (ketidakterlihatan pesan bagi indera manusia), serta **kapasitas** (jumlah data yang dapat disisipkan). Contoh penerapan hybrid adalah kombinasi DWT-SVD atau DCT-SVD, di mana pesan disisipkan pada domain transformasi gelombang diskrit (DWT) atau kosinus diskrit (DCT), lalu diperkuat melalui nilai singular (SVD). Teknik ini terbukti mampu menghasilkan sistem watermarking yang lebih kuat dan tahan terhadap berbagai bentuk modifikasi citra (Al-Haj 2007)

Metode LSB, DCT, DWT, SVD, Hybrid, diatas merupakan metode penyisipan untuk watermarking dan stagnografi tapi . Bedanya pada steganografi dipakai untuk kerahasiaan, sedangkan watermarking dipakai untuk perlindungan/identitas

3. Perbedaan Steganografi dengan Watermarking

Watermarking merupakan aplikasi dari steganografi, namun ada perbedaan antara keduanya. Jika pada steganografi informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak berarti apa-apa, maka pada watermarking justru media digital tersebut yang akan dilindungi kepemilikannya dengan pemberian label hak cipta (watermark). Meskipun steganografi dan watermarking tidak sama, namun secara prinsip proses penyisipan informasi ke dalam data digital tidak jauh berbeda. Beberapa metode yang sudah ditemukan untuk penyisipan watermark adalah metdoe LSB (seperti pada penjelasan steganografi di atas), metode adaptif, metode spread spectrum, dan sebagainya (Munir 2004).

No		watermarking	steganografi
1	Tujuan	perlindungan copyright, pembuktian kepemilikan (ownership), keaslian/autentikasi	mengirim pesan rahasia apapun tanpa menimbulkan kecurigaan
2	Persyaratan	sulit dihapus (remove)	aman, sulit dideteksi, sebanyak mungkin menampung pesan (large capacity)
3	Komunikasi	one-to-many	point-to-point
4	Komentar lain	media penampung justru yang diberi proteksi, tidak	Media penampung tidak punya arti apa-apa (meaningless)

		mementingkan kapasitas watermark	

REFERENSI

Al-Dabbas, Hind, Raghad Azeez, and Akbas Ali. 2023. "Digital Watermarking, Methodology, Techniques, and Attacks: A Review." *Iraqi Journal of Science* 64: 5069–86. doi:10.24996/ijs.2023.64.8.37.

Al-Haj, Ali. 2007. "Combined DWT-DCT Digital Image Watermarking." *Journal of Computer Science* 3(9): 740–46. doi:10.3844/jcssp.2007.740.746.

Andri, Ng Poi Wong, and Johnny Fransiscus. 2014. "APLIKASI ALGORITMA SEMI-FRAGILE IMAGE WATERMARKING BERDASARKAN PADA REGION SEGMENTATION." 15.

Ardian Wirasandi-, Diki. *Implementasi Robust Video Watermarking Berbasis DCT Pada Video Copyright Media Sosial*.

Aung Kyaw Zall. 2023. "Audio Steganography." *Medium*.

Bedi, Punam, and Arti Dua. 2020. "Network Steganography Using the Overflow Field of Timestamp Option in an IPv4 Packet." In *Procedia Computer Science*, Elsevier B.V., 1810–18. doi:10.1016/j.procs.2020.04.194.

Bhat, Pradyumna. 2015. "Transform Domain Techniques for Image Steganography." *INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL* 3(1): 2321–5526. doi:10.17148/IJIREEICE.

Chaw Tiri San. 2024. "Spatial Vs Frequency Domain: A Guide to Image Interpretation." *Medium*. https://medium.com/@chawthirisan/spatial-vs-frequency-domain-a-guide-to-image-interpretation-d9c16b129b3f (September 30, 2025).

Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. 2010. “Digital Image Steganography: Survey and Analysis of Current Methods.” *Signal Processing* 90(3): 727–52. doi:https://doi.org/10.1016/j.sigpro.2009.08.010.

Chen Phin, ng, Nurul Hidayah Ab Rahman, and Noraini Che Pa. *A Digital Image Watermarking System: An Application Of Dual Layer Watermarking Technique*.

Davidson, and A.M. Martiscia. 2024. “Steganography.” *EBSCO Research Starters*. https://www.ebsco.com/research-starters/communication-and-mass-media/steganography?utm_source=chatgpt.com (September 22, 2025).

Fridrich, Jessica. 2010. *Steganography in Digital Media : Principles, Algorithms, and Applications*. Cambridge University Press.

Garcia, Ana Rita, Sara Brito Filipe, Cristina Fernandes, Cristina Estevão, and George Ramos. *No*

Goos, Gerhard, Juris Hartmanis, Jan Van, Leeuwen Editorial Board, David Hutchison, Takeo Kanade, Josef Kittler, et al. Lecture Notes in *LNCS 3710 - Digital Watermarking*.

H. Shirali-Shahreza, and M. Shirali-Shahreza. 2007. *Internet, 2007. ICI 2007. 3rd IEEE/IFIP International Conference in Central Asia On*. IEEE.

Hameed, Mohamed Abdel, M. Hassaballah, Saleh Aly, and Ali Ismail Awad. 2019. “An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques.” *IEEE Access* 7: 185189–204. doi:10.1109/ACCESS.2019.2960254.

IDLab-Media. 2023. “IEEE ICCE 24 - Blind Image Watermarking Robust Against Geometric Transformations.” *IDLab-Media*. https://media.idlab.ugent.be/watermarking-blind-icce (September 30, 2025).

Image steganography: Concealing secrets within pixels. 2023. “Image Steganography: Concealing Secrets within Pixels.” *LevelBlue*.

Katzenbeisser, Stephan, and Fabien Petitcolas. 1999. 28 Edpacs *Information Hiding Techniques for Steganography and Digital Watermaking*. doi:10.1201/1079/43263.28.6.20001201/30373.5.

Kunhoth, Jayakanth, Nandhini Subramanian, Somaya Al-Maadeed, and Ahmed Bouridane. 2023. “Video Steganography: Recent Advances and Challenges.” *Multimedia Tools and Applications* 82(27): 41943–85. doi:10.1007/s11042-023-14844-w.

Liu, Ruizhen, and Tieniu Tan. 2002. “An SVD-Based Watermarking Scheme for Protecting Rightful Ownership.” *IEEE Transactions on Multimedia* 4(1): 121–28. doi:10.1109/6046.985560.

Ma, Ziping, Yuesheng Zhu, Guibo Luo, Xiyao Liu, Gerald Schaefer, and Hui Fang. 2023. *Robust Steganography without Embedding Based on Secure Container Synthesis and Iterative Message Recovery*. https://github.com/Lemok00/.

Margie Semilof. 2023. "Steganography." *Tech Target*. https://www.techtarget.com/searchsecurity/definition/steganography?utm_source=chatgpt.com (September 22, 2025).

Munir, Rinaldi. 2004. "Steganografi Dan Watermarking Pada Citra Digital." *Pengolahan Citra Digital dengan Pendekatan Algoritmik*: 197–212.

Nikolaidis, N, and I Pitas. 1999. "Digital Image Watermarking: An Overview." In *Proceedings IEEE International Conference on Multimedia Computing and Systems*, , 1–6 vol.1. doi:10.1109/MMCS.1999.779111.

Provos, N, and P Honeyman. 2003. "Hide and Seek: An Introduction to Steganography." *IEEE Security & Privacy* 1(3): 32–44. doi:10.1109/MSECP.2003.1203220.

Saeed Khalilidan, and Zahra Moti. 2020. *2020 6th International Conference on Web Research (ICWR)*. IEEE.

Sarkar, Tanmoy, and Sugata Sanyal. *DIGITAL WATERMARKING TECHNIQUES IN SPATIAL AND FREQUENCY DOMAIN*.

Sinaga, Daurat, and Cahaya Jatmoko. 2022. 13 *Non-Blind Watermarking Menggunakan Discrete Dan Wavelet Transform*.

Sion, Radu. 2018. "Steganography." In *Encyclopedia of Database Systems*, eds. Ling Liu and M Tamer Özsu. New York, NY: Springer New York, 3714–15. doi:10.1007/978-1-4614-8265-9_1487.

Srivastava, Rohit, Ravi Tomar, Maanak Gupta, Anuj Kumar Yadav, and Jaehong Park. 2021. "Image Watermarking Approach Using a Hybrid Domain Based on Performance Parameter Analysis." *Information (Switzerland)* 12(8). doi:10.3390/info12080310.

Steinebach, Martin, Jana Dittmann, and Erich Neuhold. 2008. "Digital Watermarking." In *Encyclopedia of Multimedia*, ed. Borko Furht. Boston, MA: Springer US, 181–86. doi:10.1007/978-0-387-78414-4_303.

Watermarking, Steganografi, and Definisi Steganografi. 2004. "Steganografi Dan Watermarking Departemen Teknik Informatika Institut Teknologi Bandung."

X. Zhong, and F. Y. Shih. 2019. "A Robust Image Watermarking System Based on Deep Neural Networks."

Zander, S, G Armitage, and P Branch. 2007. “A Survey of Covert Channels and Countermeasures in Computer Network Protocols.” *IEEE Communications Surveys & Tutorials* 9(3): 44–57. doi:10.1109/COMST.2007.4317620.

Watermarking, Steganografi, and Definisi Steganografi. 2004. “Steganografi Dan Watermarking Departemen Teknik Informatika Institut Teknologi Bandung.”