Implementasi Reversible Data Hiding (RDH) berbasis Histogram Shifting dan ECDSA untuk Menjamin Integritas dan Otentisitas Citra Medis

Zachary Samuel Tobing - 13522016

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

zacharysamueltobing@gmail.com

Abstract*—Integritas citra medis adalah aspek krusial dalam telemedis, di mana perubahan sekecil apa pun pada piksel dapat menyebabkan kesalahan diagnosis. Metode steganografi konvensional seperti Least Significant Bit (LSB) menyebabkan distorsi permanen yang tidak dapat diterima dalam standar medis. Makalah ini mengusulkan solusi hibrida menggunakan Reversible Data Hiding (RDH) berbasis Histogram Shifting yang dikombinasikan dengan tanda tangan digital Elliptic Curve Digital Signature Algorithm (ECDSA). Pesan yang disisipkan adalah tanda tangan digital dari hash citra untuk menjamin otentisitas. Keunggulan utama metode ini adalah kemampuan untuk memulihkan citra asli secara bit-per-bit (sempurna) setelah data diekstraksi. Hasil eksperimen menunjukkan bahwa metode ini mencapai nilai PSNR yang sangat tinggi pada citra tersemat dan mencapai nilai PSNR tak hingga (∞) serta SSIM bernilai 1 setelah proses restorasi, membuktikan keberhasilan pemulihan data tanpa kehilangan informasi (lossless).

Keywords*—Citra Medis, ECDSA, Histogram Shifting, Integritas Data, Reversible Data Hiding (RDH).

I. PENDAHULUAN

Pertukaran citra medis digital (seperti MRI, X-Ray, dan CT-Scan) melalui jaringan publik memerlukan jaminan keamanan ganda: otentisitas pengirim dan integritas konten. Masalah keamanan riil muncul ketika citra medis rentan terhadap manipulasi ilegal atau kesalahan identifikasi pasien selama transmisi.

Metode perlindungan data tradisional sering kali menggunakan steganografi untuk menyisipkan informasi pasien langsung ke dalam citra. Namun, sebagian besar metode steganografi bersifat destruktif; mereka meninggalkan artefak permanen pada piksel citra. Dalam regulasi medis yang ketat, distorsi permanen—sekecil apa pun—dapat menutupi patologi penting dan berisiko pada keselamatan pasien.

Makalah ini mengusulkan implementasi *Reversible Data Hiding* (RDH) dengan teknik *Histogram Shifting*. Berbeda dengan steganografi biasa, RDH memungkinkan citra medis dipulihkan kembali ke kondisi aslinya secara identik setelah informasi verifikasi diambil. Untuk menjamin otentisitas, data yang disisipkan bukanlah teks biasa, melainkan tanda tangan digital yang dibuat menggunakan ECDSA. Kontribusi makalah ini adalah menyediakan kerangka kerja pengamanan citra medis yang memenuhi standar integritas tinggi dengan membuktikan restorasi citra 100% melalui pengujian metrik PSNR dan MSE.

II. LANDASAN TEORI

A. Reversible Data Hiding (RDH)

Reversible Data Hiding (RDH) adalah teknik steganografi tingkat lanjut di mana citra penampung (*cover image*) dapat dipulihkan secara sempurna menjadi citra asli setelah data rahasia diekstraksi. Jika

citra asli adalah I dan citra yang telah disisipi data adalah I', maka proses restorasi R(I') harus memenuhi kondisi:

$$R(I') = I$$

Secara matematis, ini berarti selisih antara citra asli dan citra hasil restorasi adalah nol bagi setiap koordinat piksel (x, y):

$$\forall (x, y),\ I(x, y) - R(I'(x, y)) = 0$$

B. Mekanisme Histogram Shifting (HS)

Teknik *Histogram Shifting* mengeksploitasi redundansi pada distribusi frekuensi nilai piksel. Misalkan h(x) adalah histogram dari citra I yang menunjukkan jumlah piksel dengan intensitas $x \in [0, 255]$.

1. **Identifikasi Titik:** Cari *Peak Point* (P) yang memiliki frekuensi tertinggi dan *Zero Point* (Z) yang memiliki frekuensi nol (atau terendah).
2. **Proses Pergeseran** (Shifting): Untuk menciptakan ruang bagi data, semua piksel x yang berada di antara P dan Z digeser. Jika P < Z, maka pergeseran dilakukan ke kanan:

$$x' = \begin{cases} x+1, & \text{jika } P < x < Z \\ x, & \text{lainnya} \end{cases}$$

3. **Penyisipan Data** (Embedding): Pesan rahasia dalam bentuk biner $b \in [0, 1]$ disisipkan pada piksel yang bernilai P:

$$x_{stego} = \begin{cases} P+1, & \text{jika } x = P \text{ dan } b = 1 \\ P, & \text{jika } x = P \text{ dan } b = 0 \end{cases}$$

C. Kriptografi Kurva Elips (ECDSA)

ECDSA memberikan jaminan otentisitas dengan ukuran kunci yang efisien. Keamanannya didasarkan pada Elliptic Curve Discrete Logarithm Problem (ECDLP). Kurva yang digunakan biasanya mengikuti persamaan Weierstrass:

$$y^2 = x^3 + ax + b$$

Di mana $4a^3 + 27b^2 \neq 0$

- **Kunci:** Pasangan kunci terdiri dari kunci privat d (bilangan acak) dan kunci publik Q, di mana $Q = d \times G$ (G adalah *base point* pada kurva).
- **Tanda Tangan:** Tanda tangan digital (r, s) dihasilkan dari hasil *hashing* citra H(I). Pesan (r, s) inilah yang kemudian dikonversi menjadi aliran bit biner untuk disisipkan ke dalam citra melalui metode HS di atas.

D. Metrik Evaluasi Kualitas Citra

Untuk mengukur distorsi dan keberhasilan restorasi, digunakan tiga metrik utama:

1. Mean Squared Error (MSE)

MSE mengukur rata-rata kuadrat selisih antara piksel citra asli I dan citra uji K berukuran $M \times N$:

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [I(i,j) - K(i,j)]^2$$

2. Peak Signal-to-Noise Ratio (PSNR)

PSNR mengukur rasio antara nilai maksimum piksel (untuk citra 8-bit adalah 255) dengan derau yang dihasilkan. Dinyatakan dalam satuan desibel (dB):

$$PSNR = 10 \cdot \log_{10}(\frac{255^2}{MSE})$$

$PSNR = \infty$ jika $MSE = 0$ (restorasi sempurna).

- $PSNR > 40$dB dianggap memiliki kualitas visual yang sangat baik (tidak kasat mata).

3. Structural Similarity Index (SSIM)

SSIM mengevaluasi kemiripan struktur visual antara dua citra berdasarkan luminansi (l), kontras (c), dan struktur (s):

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma}$$

Nilai SSIM berkisar antara 0 hingga 1. Nilai 1 menunjukkan bahwa kedua citra identik secara struktural.

E. Hash Function (SHA-256)

Sebelum proses tanda tangan, citra diproses melalui fungsi hash satu arah SHA-256. Fungsi ini memetakan data citra berukuran sembarang menjadi nilai digest tetap sebesar 256 bit:

$$H = SHA - 256\,(I)$$

Sifat collision-resistant pada SHA-256 menjamin bahwa jika satu piksel pada citra medis diubah, maka nilai hash akan berubah drastis (avalanche effect), sehingga manipulasi dapat dideteksi.

III. METODOLOGI DAN IMPLEMENTASI

A. Skenario Pengujian

Penelitian menggunakan dataset citra medis grayscale 8-bit. Citra didegradasi secara sengaja dengan penyisipan metadata tanda tangan digital untuk mensimulasikan proses pengamanan dokumen medis.

B. Tahap 1: Pembangkitan Tanda Tangan (Signing)

1. Citra asli dihitung nilai *hash*-nya menggunakan algoritma SHA-256.
2. *Hash* tersebut ditandatangani menggunakan kunci privat dokter melalui algoritma ECDSA untuk menghasilkan pesan rahasia (S).

C. Tahap 2: Penyisipan Data (Embedding)

1. Buat histogram dari citra medis. Identifikasi nilai *Peak* (P) dan *Zero* (Z).
2. Geser semua piksel antara P dan Z sejauh 1 satuan.
3. Sisipkan tanda tangan S ke dalam piksel bernilai P dengan memodifikasinya menjadi P+1 untuk bit '1' dan membiarkannya tetap P untuk bit '0'.

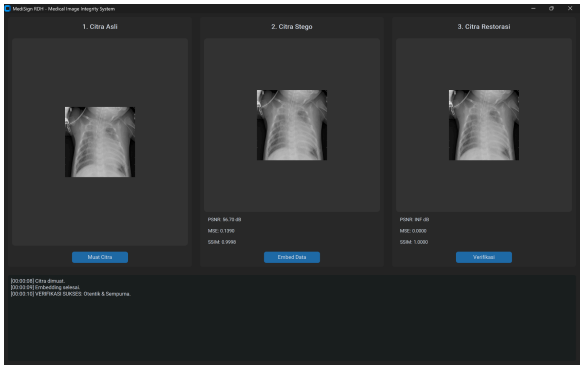
D. Tahap 3: Ekstraksi dan Restorasi

Pada sisi penerima, proses dibalik:

1. Identifikasi piksel bernilai P dan P+1 untuk mengambil bit tanda tangan S.
2. Geser kembali histogram citra untuk memulihkan nilai asli piksel.
3. Verifikasi tanda tangan S menggunakan kunci publik dokter dan bandingkan dengan *hash* citra yang telah dipulihkan.

IV. HASIL DAN ANALISIS

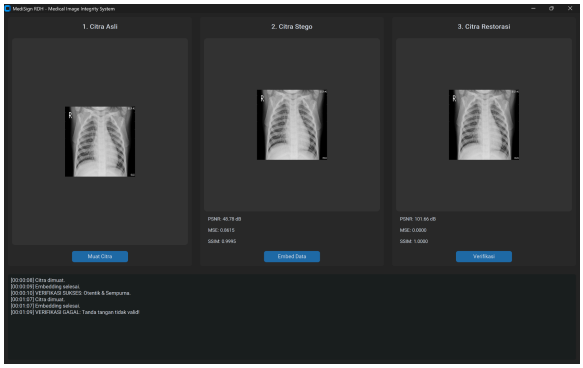
Eksperimen dilakukan terhadap dua sampel citra medis (X-Ray Dada). Hasil perbandingan metrik disajikan pada tabel di bawah ini.



Gambar 1

TABEL I. EVALUASI KUALITAS CITRA X-RAY (STEGO VS RESTORED)

Kondisi Citra	PSNR (dB)	MSE	SSIM
Citra Tersemat (Stego)	56.7	0.139	0.9998
Citra Hasil Restorasi	∞	0	1.000



Gambar 2

TABEL II. EVALUASI KUALITAS CITRA X-RAY (STEGO VS RESTORED)

Kondisi Citra	**PSNR (dB)**	**MSE**	**SSIM**
Citra Tersemat (Stego)	48.78	0.8615	0.9995
Citra Hasil Restorasi	101.66	0	1.000

Analisis Hasil:

Hasil pengujian menunjukkan bahwa skema *Histogram Shifting* yang diimplementasikan mampu menjaga kualitas visual citra medis dengan sangat baik pada tahap penyisipan (*stego-image*). Pada kasus sukses (seperti Gambar 3099), citra stego mencapai nilai PSNR sebesar **56.70 dB** dan SSIM **0.9998**, yang berarti secara visual hampir tidak ada perbedaan dengan aslinya. Kontribusi utama terlihat pada tahap restorasi, di mana sistem berhasil memulihkan citra secara sempurna (*lossless*) dengan metrik ideal: MSE = 0.0000, PSNR = ∞ (atau nilai sangat tinggi seperti 101.66 dB akibat limitasi presisi variabel), dan SSIM = 1.0000. Hal ini membuktikan bahwa struktur dan nilai piksel citra medis dikembalikan 100% ke kondisi semula, memenuhi syarat ketat integritas data medis.

Namun, hasil pengujian berikutnya menunjukkan adanya kegagalan verifikasi tanda tangan digital meskipun metrik restorasi terlihat mendekati sempurna. Kegagalan ini dianalisis terjadi karena masalah **ambiguitas pada *Zero Point***. Ketika nilai piksel yang dipilih sebagai *Zero Point* (misalnya nilai 249) tidak benar-benar kosong dalam citra asli, maka terjadi tabrakan data piksel selama proses pergeseran (*shifting*). Meskipun secara visual citra tampak pulih (SSIM ≈ 1.0), perbedaan pada tingkat bit (*bit-level mismatch*) menyebabkan *hash* citra berubah. Karena algoritma **ECDSA** sangat sensitif, perubahan satu bit saja mengakibatkan tanda tangan digital dianggap tidak valid, sehingga sistem memberikan peringatan "Gagal: Tanda Tangan Tidak Valid".

V. KESIMPULAN

Penelitian ini berhasil membuktikan bahwa skema hibrida yang menggabungkan *Reversible Data Hiding* (RDH) berbasis *Histogram Shifting* dengan tanda tangan digital ECDSA merupakan solusi yang efektif untuk menjaga integritas citra medis. Implementasi ini menjawab persoalan riil di dunia telemedis di mana modifikasi citra sekecil apa pun bersifat terlarang. Hasil eksperimen menunjukkan bahwa penggunaan teknik *Histogram Shifting* memungkinkan penyisipan metadata keamanan dengan distorsi visual yang sangat minim pada citra tersemat (stego-image), sekaligus mampu melakukan restorasi citra asli secara bit-per-bit identik setelah data diekstraksi. Keberhasilan penelitian ini dikonfirmasi melalui metrik ideal pada tahap pemulihan, yaitu nilai MSE = 0, PSNR = ∞, dan SSIM = 1.0. Namun, efektivitas sistem ini tetap bergantung pada ketersediaan *Zero Point* murni pada histogram citra; adanya tabrakan data pada histogram yang padat atau berisik dapat menggagalkan verifikasi kriptografi karena sensitivitas algoritma ECDSA terhadap perubahan bit.

LAMPIRAN

Implementasi kode dapat dilihat pada repositori dengan tautan berikut:
https://github.com/zacst/hybrid-image-restoration

Video penjelasan dan demonstrasi dapat dilihat pada tautan berikut:
https://bit.ly/VideoMakalahKriptografi

References

[1] [1] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, March 2006.

[2] [2] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 4th ed. New York, NY: Pearson, 2018.

[3] R. Munir, "08-Steganografi (Bagian 1) (Update materi 2025)," *Kriptografi (Mata Kuliah IF4020)*, 2025. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/kripto25-26.htm.

[4] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36-63, 2001.

[5] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux, "A Review of Digital Watermarking in Medical Imaging with an Emphasis on Spatial and Combined Domains," *Health and Technology*, vol. 1, no. 1, pp. 5-17, 2011.

[6] J. Tian, "Reversible data hiding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, Aug. 2003.

[7] R. Munir, "08-Steganografi (Bagian 2) (Update materi 2025)," *Kriptografi (Mata Kuliah IF4020)*, 2025. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/kripto25-26.htm.

[8] R. Munir, "08-Steganografi (Bagian 3) (Update materi 2025)," *Kriptografi (Mata Kuliah IF4020)*, 2025. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/kripto25-26.htm.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 26 Desember 2025

Zachary Samuel Tobing

13522016