ENKRIPSI SELEKTIF PADA CITRA MEDIS DENGAN MENGGUNAKAN LINEAR CONGRUENTIAL GENERATOR

Aprianti Nanda[1], Trisna Gelar2[2],

[1,2] Jurusan Teknik Komputer dan Informatika, Politeknik Negeri Bandung
[1]aprianti.nanda@polban.ac.id, [2] trisna.gelar@polban.ac.id

Abstrak

Di bidang rekam medis, citra medis merupakan data yang sensitif. Akan tetapi, masih banyak sistem rekam medis di rumah sakit atau institusi kesehatan yang menyimpan citra medis pasien dalam *database* tanpa dienkripsi terlebih dahulu. Hal ini memberikan peluang terhadap pihak yang tidak berwenang untuk mengakses citra medis secara ilegal. Secara garis besar, metode enkripsi citra medis dibedakan menjadi dua yaitu enkripsi total dan enkripsi selektif. Pada enkripsi total, semua bit dan *piksel* dienkripsi secara menyeluruh menggunakan algoritma enkripsi standar sedangkan enkripsi selektif hanya sebagian bit pada citra medis yang dienkripsi. Metode enkripsi selektif dapat menghemat sumber daya seperti kecepatan transmisi, waktu komputasi dan kapasitas memori. Pada penelitian ini enkripsi selektif diimplementasikan dengan memproses sebagian bit pada setiap *piksel* yang kemudian dioperasikan dengan bilangan acak yang dibangkitkan dengan menggunakan algoritma *Linear Congruential Generator*. Citra medis yang memiliki kedalaman warna sebanyak 8-bit setiap pikselnya akan diambil sebagian bit paling kiri (*MSB*). Dari hasil pengujian, metode ini memiliki performa yang cukup baik sehingga dapat diaplikasikan pada kasus nyata. Hal ini ditandai dengan tingkat kemiripan antara citra asli dan citra terenkripsi yang mendekati nol meski hanya satu bit MSB yang dienkripsi. Namun, pada pengujian visual dan histogram, metode ini memiliki nilai optimum jika minimal empat bit MSB yang dienkripsi. Selain itu, peluang *attacker* untuk mendapatkan citra asli dengan cara *bruteforce* sebanding dengan banyaknya bit MSB yang dienkripsi.

Kata kunci : citra medis, enkripsi selektif, *linear congruential generator*, rekam medis.

1. Pendahuluan

Perkembangan teknologi informasi telah merambah ke segala bidang termasuk kesehatan. Salah satu yang menjadi perhatian penting dalam menyimpan informasi medis pasien adalah aspek keamanannya. Informasi medis pasien seperti hasil *X-ray, MRI scan, CT scan* (Larobina & Murino, 2013), diagnosa penanganan penyakit, dan data personal pasien lainnya disimpan dalam basis data. Basis data tersebut kemudian diakses oleh dokter, laboratoria, ahli radiologi, dan pihak berkepentingan lainnya menggunakan sistem rekam medis. Namun biasanya citra medis disimpan begitu saja tanpa dilakukan proteksi tambahan terlebih dahulu. Hal ini menyebabkan keamanan terhadap privasi data pasien ikut terancam (Cao et al., 2003). Untuk itu, citra medis perlu dienkripsi terlebih dahulu agar terlindung dari pihak-pihak yang tidak berkepentingan.

Berdasarkan *piksel* yang dienkripsi, terdapat dua jenis enkripsi pada citra digital di ranah spasial yaitu enkripsi total dan enkripsi selektif. Pada enkripsi total, semua bit dan *piksel* dienkripsi secara menyeluruh menggunakan algoritma enkripsi standar seperti DES, AES, Chaos (Munir, 2012), dan lain sebagainya.

Peneliti telah mengimplementasi *enkripsi* total pada citra medis dengan metode enkripsi seperti algoritma *camelia* dengan mode operasi ECB, CBC, CFB, dan OFB dapat menghasilkan kualitas citra dan kompleksitas yang baik (Zaenury et al., 2020). Selain itu kombinasi algoritma *hashing kecak* dan *rivest code 6* dapat menjaga integritas citra rekam medis, nilai *hash* citra modifikasi berbeda meskipun mirip dengan citra aslinya (Bayu Seta et al., 2020).

Dalam proses enkripsi, citra digital diperlakukan seperti teks biasa. Skema ini tidak efisien jika sumber daya seperti kecepatan transmisi, waktu komputasi, kapasitas memori, dan sumber daya lainnya tidak terpenuhi (Massoudi et al., 2008).

Untuk mengatasi kekurangan tersebut, kemudian berkembanglah metode untuk mengamankan citra dengan cara mengenkripsi sebagian *piksel* atau bit yang dinamakan enkripsi selektif. Tujuan utama dari enkripsi selektif adalah mengurangi banyaknya bit atau *piksel* yang harus dienkripsi namun masih memiliki tingkat keamanan yang cukup baik (Khashan et al., 2014).

Metode enkripsi selektif pada citra medis memerlukan ekstraksi fitur seperti area (Ou et al., 2007) dan garis (Khashan & AlShaikh, 2020) terlebih dahulu sebelum dienkripsi mengakibatkan tingginya waktu komputasi. Kontribusi peneliti adalah meniadakan proses ekstraksi fitur sehingga pemrosesan sederhana dan waktu komputasi yang singkat, alternatif yang dipilih adalah mengoperasikan bit pada citra dengan *Linear Congruential Generator*.

2. Tinjauan Pustaka

Pada bagian ini akan dibahas mengenai teori-teori yang mengenai konsep citra digital dan enkripsinya, *Linear Congruential Generator*, serta beberapa metode pengujian hasil enkripsi.

2.1 Enkripsi Citra Digital

Enkripsi citra digital memiliki peran yang sangat besar dalam melindungi citra digital pengguna yang tidak berkepentingan. Enkripsi citra digital m Enkripsi citra digital memiliki teknik yang tidak jauh berbeda dengan enkripsi pada teks biasa. Secara garis besar, enkripsi citra digital dapat berupa memodifikasi nilai *piksel* atau mengacak posisi *piksel* sehingga citra yang telah dienkripsi tidak dapat dimengerti.

2.2 Linear Congruential Generator

Linear Congruential Generator merupakan algoritma yang menghasilkan deret pseudo random yang dihitung berdasarkan kongruensi linear. Kongruensi linear yang dimaksud adalah sebagai berikut (Eichenauer-Herrmann et al., 1998; MARSAGLIA, 1972).

$$X_{n+1} = (aX_n + c) \bmod m \qquad (1)$$

Di mana X adalah deret bilangan acak, m adalah *modulus*, a adalah pengali, dan c adalah *increment* atau nilai kenaikan.

Pada penelitian ini memanfaatkan algoritma *Linear Congruential Generator* sebagai algoritma pembangkit bilangan acak karena sederhana dan waktu komputasi yang singkat (James, 1990).

$$T_i = (aT_{i-1} + c) \bmod m \qquad (2)$$

Di mana $0 < i < n$, m merupakan modulus, a adalah pengali, dan c adalah nilai kenaikan. Sebagai contoh $T_0 = 5$, $a = 19$, $c = 7$, dan $m = 2^b = 2^5 = 32$. Penentuan modulo $m = 2^b$ dilakukan agar nilai hasil operasi XOR tidak melebihi bit MSB yang yang diambil.

2.3 Enkripsi Selektif State of the art

Enkripsi selektif digunakan untuk mengamankan berbagai konten multimedia seperti citra, *audio* (Abdelfatah, 2020; T et al., 2021), *video* (Cheng et al., 2020; He et al., 2020) dan *video streaming* (Shifa et al., 2020).

Beberapa penelitian sebelumnya terkait enkripsi selektif pada citra medis yang diajukan oleh memiliki kelemahan dalam hal waktu komputasi karena fitur-fitur citra medis diekstrak terlebih dahulu sebelum dienkripsi

Enkripsi citra medis berbasis fitur pada region/area gambar diusulkan oleh (Ou et al., 2007), terdapat dua skema enkripsi yaitu selang dan sesudah kompresi gambar dengan format JPEG2000. Pada skema ke-satu algoritma memilih sub-bagian fitur frekuensi pada area gambar.Pada skema ke-dua algoritma AES dioperasikan untuk mengenkripsi sebagian region/area gambar.

Enkripsi citra medis berbasis fitur garis diusulkan oleh (Khashan & AlShaikh, 2020) memanfaatkan edge map (hasil ektraksi algoritma edge detection) digabungkan chaotic map yang menghasilkan ruang kunci yang besar untuk menghasilkan gambar terenkripsi.

Kedua metode memerlukan proses ektraksi fitur pada citra yang berpengaruh pada waktu komputasi enkripsi selektif.

2.3 Uji Visual

Uji visual dilakukan dengan tujuan menganalisis citra medis yang telah terenkripsi dengan kasat mata. Pada uji ini nilai b (banyaknya bit yang dienkripsi) bervariasi antara 1 hingga 7.

2.4 Uji Histogram

Histogram adalah sebuah grafik yang merepresentasikan distribusi nilai *piksel* pada sebuah citra. Jika sebuah citra terenkripsi memiliki bentuk yang cenderung datar, maka distribusi nilai *piksel* cenderung merata sehingga sulit untuk ditebak.

2.5 Structural Similarity Index (SSIM)

Structural Similarity Index (SSIM) merupakan salah satu metode untuk membandingkan dua buah citra berdasarkan strukturnya (Wang et al., 2004). Perhitungan SSIM dari dua buah citra x dan y dihitung dengan menggunakan persamaan (3).

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{\left(\mu^2{}_x + \mu^2{}_y + C_1\right)(\sigma^2{}_x + \sigma^2{}_y + C_2)} \qquad (3)$$

Dengan μ_x adalah rata-rata nilai piksel citra x, μ_y adalah rata-rata nilai piksel citra y, ${\sigma_x}^2$ adalah varian nilai piksel citra x, ${\sigma_y}^2$ adalah varian nilai piksel citra y, σ_{xy} adalah kovarian dari x dan y, serta C_1 dan C_2 merupakan dua variabel untuk menstabilkan pembagian dengan denominator kecil.

2.6 Probabilitas Brute Force

Pengujian ini bertujuan untuk menghitung probabilitas pihak ketiga dapat mendapatkan citra medis asli dari sebuah citra medis yang telah terenkripsi. Pada pengujian ini ada dua buah asumsi. Asumsi pertama adalah ketika pihak ketiga mengetahui nilai dari b dari hasil pengamatan langsung citra terenkripsi atau dengan mengamati histogramnya. Asumsi kedua adalah Ketika pihak ketiga tidak melakukan pengamatan terlebih dahulu.

Sebagai contoh, pihak ketiga sudah mengetahui nilai $b = 5$, maka ia dapat menebak sebuah nilai *piksel* dari 0 hingga $2^5 - 1 = 31$. Sehingga probabilitas ia menebak dengan tepat nilai sebuah piksel adalah $\frac{1}{2^5} = \frac{1}{32}$. Jika sebuah citra terenkripsi memiliki ukuran $p \times q$, maka probabilitas keseluruhan citra terenkripsi dapat ditebak adalah sebagai berikut

$$p(citra) = \left(\frac{1}{2^b}\right)^{p \times q} \quad (4)$$

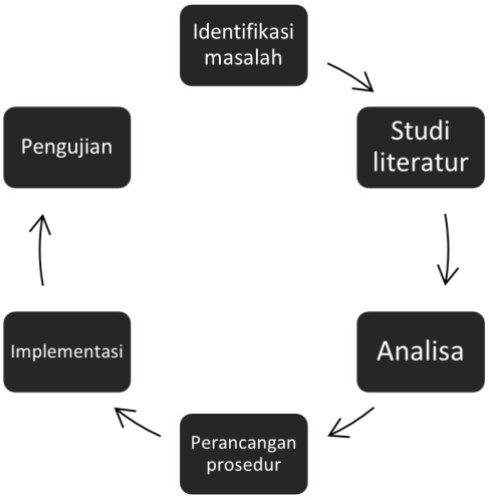
Kasus lainnya adalah ketika pihak ketiga tidak mengetahui nilai b. Sehingga ia harus mencoba menebak nilai piksel citra terenkripsi untuk semua nilai b. Sehingga probabilitasnya menjadi seperti persamaan (5).

$$p(citra) = \sum_{b=1}^{7} \left(\frac{1}{2^b}\right)^{p \times q} \quad (5)$$

Dari kedua asumsi tersebut, probabilitas sebuah *piksel* ditentukan oleh nilai b. Namun untuk keseluruhan citra, probabilitasnya bergantung pada nilai *b* dan ukuran citra itu sendiri.

3. Metode

Penelitian ini diawali dengan mengidentifikasi masalah pada metode enkripsi citra medis yang sudah ada kemudian dilanjut dengan studi literatur tentang pembangkitan angka acak. Studi literatur ini menghasilkan sejumlah informasi seputar jenis-jenis algoritma untuk membangkitkan angka acak yang dijadikan landasan dalam analisa penentuan algoritma pembangkit angka acak yang dipilih. Setelah algoritma pembangkit angka acak dipilih, tahap selanjutnya adalah merancang prosedur proses enkripsi dan dekripsi citra medis. Setelah prosedur dirancang, kemudian diimplementasikan dengan bahasa pemrograman dan dilakukan pengujian. Ilustrasi dari metode penelitian ini dapat dilihat pada *Gambar 1*

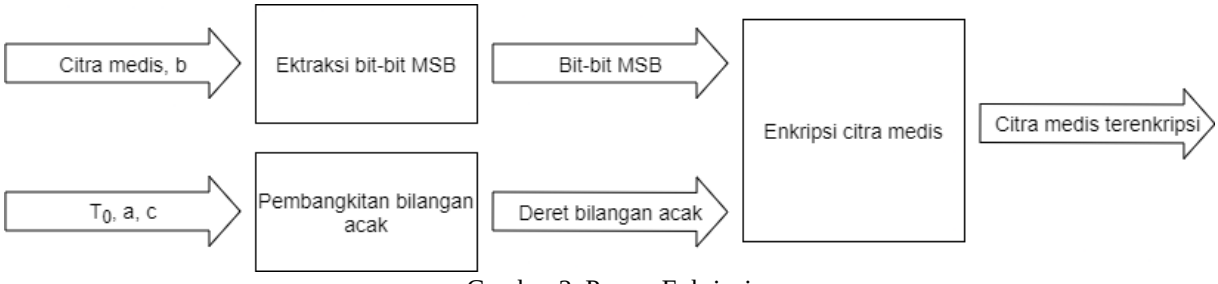


Gambar 1. Metode penelitian

Secara garis besar, metode yang diajukan memiliki dua proses utama yaitu proses enkripsi dan dekripsi yang akan dijelaskan pada sub bab berikut

3.1 Proses Enkripsi

Proses enkripsi bertujuan untuk mengubah citra medis asli menjadi citra medis yang telah terenkripsi agar sulit dimengerti oleh pihak yang tidak berwenang. *Input* dari proses enkripsi adalah sebuah citra medis berformat kedalaman warna sebesar delapan bit atau yang biasa disebut citra *greyscale* dan sebuah bilangan *b* untuk menentukan berapa bit paling kiri atau *Most Significant Bit* (MSB) yang diambil. Input lainnya yaitu nilai T_0, a dan c yang digunakan sebagai parameter untuk membangkitkan bilangan acak. Nilai MSB kemudian di-XOR-kan dengan bilangan acak sehingga output yang dihasilkan adalah sebuah citra medis yang terenkripsi. Ilustrasi proses enkripsi dapat dilihat pada *Gambar 2*.



Gambar 2. Proses Enkripsi

Detail langkah-langkah dari proses enkripsi adalah sebagai berikut.

- **Langkah 1**. Sebuah citra medis berukuran $p \times q$ dibaca nilai pikselnya kemudian disimpan ke dalam sebuah matriks R dengan ukuran sama. Sebagai contoh, matriks R yang dihasilkan adalah sebagai berikut.
- **Langkah 2.** Tentukan berapa bit MSB yang akan diambil, disimbolkan dengan *b* dengan ketentuan $1 \leq b < 8$, karena delapan adalah kedalaman warna sebuah citra *greyscale*. Sebagai contoh, $b = 5$, sehingga akan diambil 5 bit MSB dari setiap piksel citra

$$R = \begin{bmatrix} 4 & 4 & 4 & 5 & 5 & 5 & 5 & \dots & 4 \\ 35 & 33 & 34 & 35 & 35 & 35 & 36 & \dots & 34 \\ 37 & 37 & 37 & 38 & 37 & 40 & 39 & \dots & 40 \\ 36 & 35 & 35 & 33 & 35 & 36 & 36 & \dots & 40 \\ 33 & 32 & 35 & 32 & 32 & 32 & 34 & \dots & 42 \\ 31 & 31 & 33 & 32 & 32 & 32 & 32 & \dots & 40 \\ 28 & 31 & 31 & 33 & 33 & 31 & 32 & \dots & 40 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 57 & 57 & 57 & 55 & 56 & 54 & 54 & \dots & 18 \end{bmatrix}$$

- **Langkah 3.** Buat sebuah *array* T dengan entri sebanyak $n = p \times q$ yang merupakan representasi deret bilangan acak. Bilangan acak tersebut dibangkitkan oleh algoritma *Linear Congruential Generator* dengan persamaan (2). Dengan nilai awal $T_0 = 5$, maka deret selanjutnya $T_1 = (19 \times 5 + 7) \bmod 32 = 6$, $T_2 = (19 \times 6 + 7) \bmod 32 = 25$, dan seterusnya hingga menghasilkan *array* T sebagai berikut.

$$T = [5, 6, 25, 2, 30, 1, \dots, 17\ ]$$

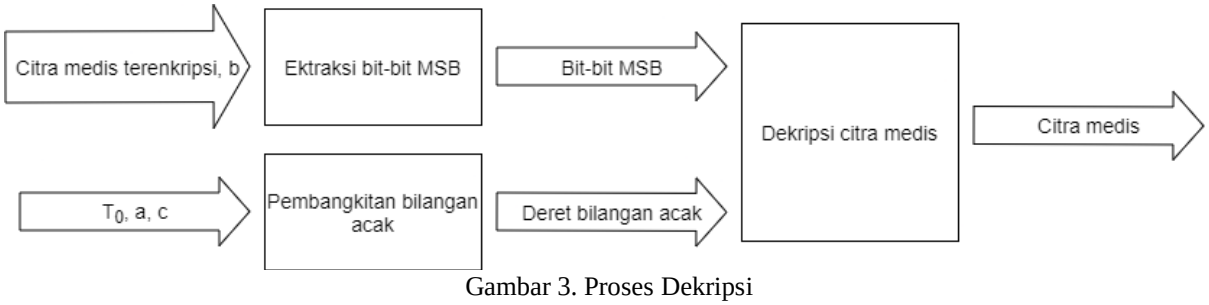
- **Langkah 4.** Setiap entri matriks R diubah menjadi bilangan biner dengan panjang 8 bit dan diambil b bit MSB. Sebagai contoh, $R[0,0] = 4$ sehingga representasi 8-bit biner dari 4 adalah 00000100. Kemudian ambil 5 bit MSB yaitu 00000.
- **Langkah 5.** Setiap entri *array* T diubah menjadi bilangan biner dengan panjang b bit. Sebagai contoh, $T_0 = 5$ sehingga representasi 5-bit biner dari 5 adalah 00101.
- **Langkah 6.** Operasikan XOR bit pada langkah 4 dengan bit pada langkah 5. Sehingga didapat $00000 \oplus 00101 = 00101$. Hasil ini kemudian digabungkan dengan $8 - b = 8 - 5 = 3$ bit yang tidak diambil pada langkah 4 (3 bit paling kanan). Sehingga didapat 00101100 atau 44 dalam desimal. Lakukan hal yang sama untuk semua *piksel*. Nilai tersebut lalu disimpan hasilnya pada sebuah matriks S sebagai berikut.

$$S = \begin{bmatrix} 44 & 52 & 204 & 20 & 245 & 13 & 213 & \dots & 180 \\ 107 & 177 & 202 & 83 & 171 & 115 & 12 & \dots & 234 \\ 53 & 77 & 213 & 46 & 245 & 128 & 151 & \dots & 184 \\ 204 & 83 & 171 & 113 & 11 & 20 & 236 & \dots & 64 \\ 209 & 40 & 243 & 136 & 144 & 104 & 178 & \dots & 193 \\ 151 & 79 & 9 & 16 & 232 & 48 & 72 & \dots & 32 \\ 204 & 183 & 175 & 105 & 177 & 247 & 80 & \dots & 120 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 145 & 137 & 113 & 167 & 208 & 70 & 190 & \dots & 58 \end{bmatrix}$$

- **Langkah 7**. Simpanlah matriks S sebagai sebuah citra yang telah terenkripsi dan proses selesai.

3.2 Proses Dekripsi

Proses dekripsi bertujuan mengubah citra yang telah terenkripsi menjadi citra medis asli. *Input* dari proses ini adalah sebuah citra medis terenkripsi dan variabel b untuk mendapatkan bit MSB dari piksel. Selain itu dibutuhkan parameter-parameter untuk membangkitkan bilangan acak yaitu $T_0, a,$ dan c seperti yang terlihat pada *Gambar 3*.



Gambar 3. Proses Dekripsi

Detail langkah-langkah untuk mendekripsi citra medis adalah sebagai berikut.

- **Langkah 1**. Sebuah citra medis yang telah terenkripsi berukuran $p \times q$ dan memiliki kedalaman warna 8 bit dibaca nilai pikselnya dan disimpan ke dalam sebuah matriks S. Matriks S tersebut sama seperti yang terlihat pada proses enkripsi.
- **Langkah 2.** *Input* nilai dari b untuk menentukan berapa bit MSB yang akan diambil. Nilai dari b pada proses dekripsi haruslah sama dengan nilai b pada proses enkripsi. Dari proses enkripsi

diketahui $b = 5$, maka pada proses dekripsi akan diekstrak 5-bit MSB untuk setiap piksel.

- **Langkah 3.** Sebuah *array* berisi angka acak dibuat dengan cara yang sama seperti pada proses enkripsi. Untuk itu, parameter-parameter yang digunakan haruslah sama.
- **Langkah 4.** Setiap entri pada matriks S diubah ke dalam bilangan biner dengan panjang 8 bit. Sebagai contoh $S[0,0] = 44$ dalam biner menjadi 00101100. Kemudian ambil $b = 5$ bit MSB, sehingga menjadi 00101.
- **Langkah 5.** Setiap entri pada *array* T diubah ke dalam bilangan biner dengan panjang b bit. Sebagai contoh $T_0 = 5$ dalam biner menjadi 00101.
- **Langkah 6.** Operasikan XOR bit pada langkah 4 dan langkah 5. Sehingga didapat $00101 \oplus 00101 = 00000$. Hasil ini kemudian digabungkan dengan $8 - b = 8 - 5 = 3$ bit yang tidak diambil pada langkah 4 (3 bit paling kanan). Sehingga didapat 00000100 atau 4 dalam desimal. Lakukan hal yang sama untuk semua piksel. Nilai tersebut lalu disimpan hasilnya pada sebuah matriks R yang identik dengan nilai piksel citra medis sebelum dienkripsi.
- **Langkah 7.** Simpanlah matriks R sebagai sebuah citra yang berhasil didekripsi dan proses selesai.

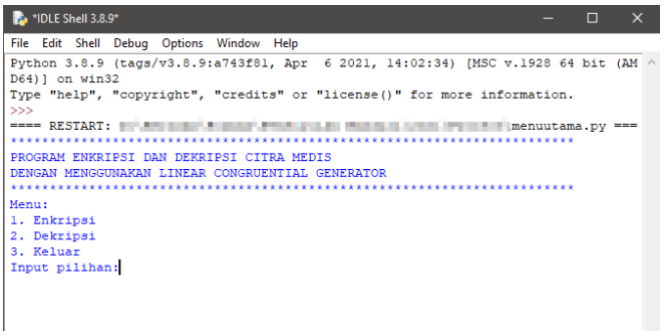
3.3 Implementasi

Prosedur enkripsi dan dekripsi yang sudah dirancang kemudian diimplementasikan menjadi sebuah program. Bahasa pemrograman yang digunakan adalah *Python* dengan bantuan beberapa *library* seperti *Skimage* untuk mengolah citra medis dan *Matplotlib* untuk membuat grafik histogram.

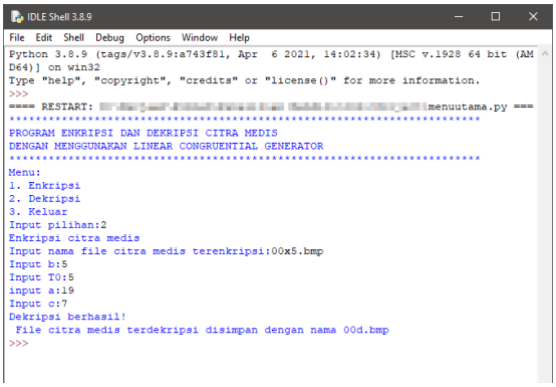
Menu utama dari program ini dapat dilihat pada Gambar 4a. Untuk mengenkripsi citra medis, user dapat memilih menu Enkripsi pada menu utama dan input nama file citra medis asli dan banyaknya bit MSB yang akan dioperasikan (b). Untuk membangkitkan bilangan acak, user input bilangan acak awal (T_0) , pengali (a) dan nilai kenaikan (c). Implementasi proses enkripsi tersebut dapat dilihat pada **Error! Reference source not found.**4b. Sedangkan untuk proses dekripsi, user input nama file citra medis yang terenkripsi, b, T_0, a, dan c. Agar dapat menghasilkan citra medis terdekripsi yang identik dengan citra asli, maka nilai b, T_0, a, dan c harus sama seperti pada proses enkripsi. Implementasi proses dekripsi dapat dilihat pada **Error! Reference source not found.**4c.

3.4 Pengujian

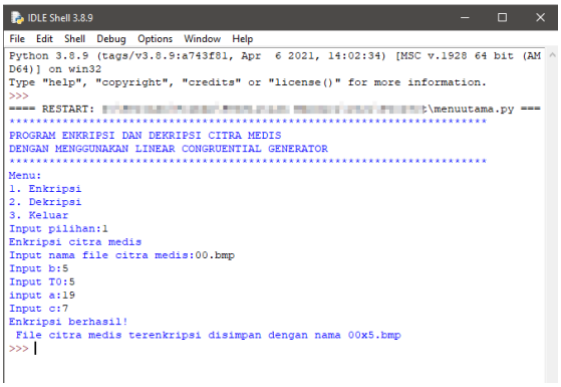
Untuk menguji apakah metode yang diajukan memiliki performa yang baik, beberapa skenario pengujian dilakukan. Pengujian tersebut meliputi uji visual, uji histogram, menghitung Structural Similarity Index (SSIM), serta uji probabilitas mendapatkan citra medis asli dengan cara brute force.



a Menu Utama



b Proses Enkripsi



c. Proses Dekripsi

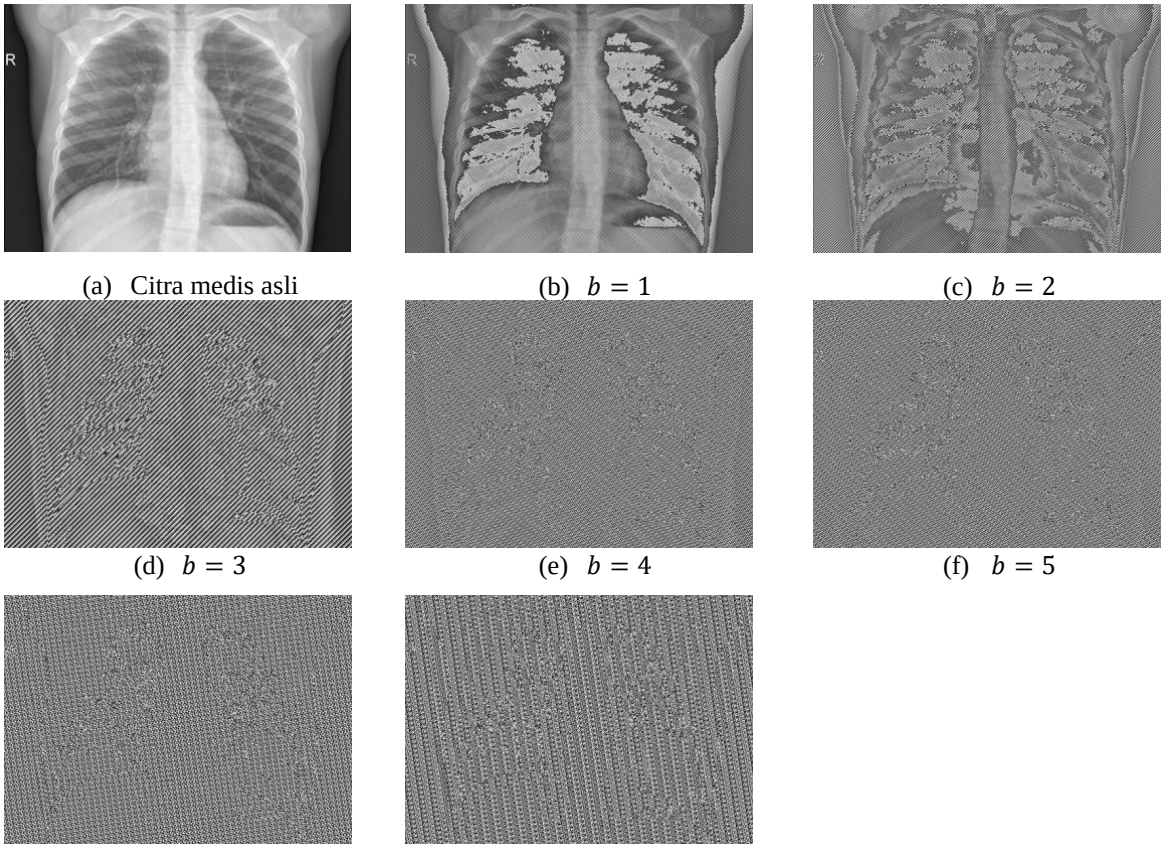
Gambar 4. Implementasi proses enkripsi dan dekripsi.

4. Hasil dan Pembahasan

Hasil dari penelitian ini adalah sebuah metode baru untuk mengenkripsi sebagian bit citra medis pada ranah spasial. Berikut adalah hasil metode tersebut setelah dilakukan berbagai skenario pengujian. *Sample* data merupakan citra paru-paru pasien *Covid -19* diambil dari (Cohen et al., 2020)

4.1 Uji Visual

Hasil enkripsi citra medis tersebut dapat dilihat pada Gambar 5. Dari hasil pengamatan, nilai $b > 3$ menghasilkan citra terenkripsi yang terlihat acak sehingga sulit ditebak. Lain halnya jika $b < 4$, citra terenkripsi masih dapat dikenali karena memiliki kemiripan dengan citra asli.



(a) Citra medis asli (b) $b = 1$ (c) $b = 2$

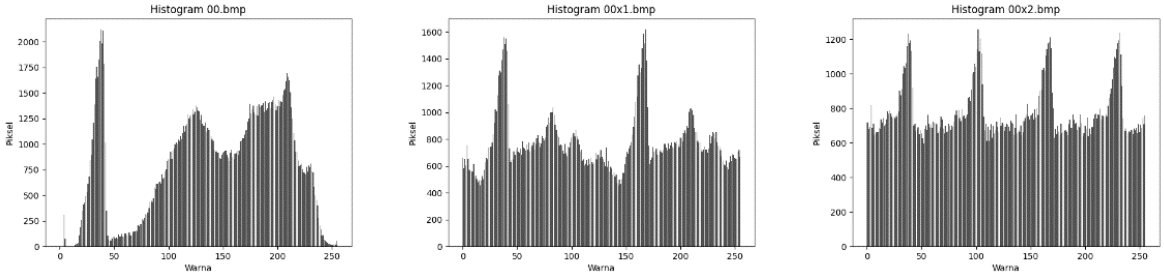
(d) $b = 3$ (e) $b = 4$ (f) $b = 5$

(g) $b = 6$ (h) $b = 7$

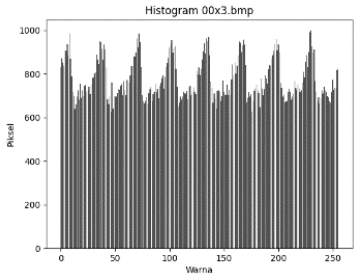
Gambar 5. Hasil enkripsi citra medis

4.2 Uji Histogram

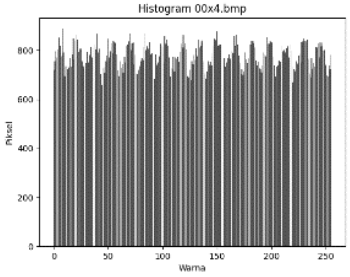
Histogram citra medis asli dan hasil enkripsi dengan nilai b yang berbeda dapat dilihat pada Gambar 6. Dari hasil pengamatan, terlihat bahwa jika nilai $b < 4$ distribusi nilai pikselnya masih tidak merata. Sedangkan jika $b \geq 4$ distribusi nilai *piksel* cenderung seragam.



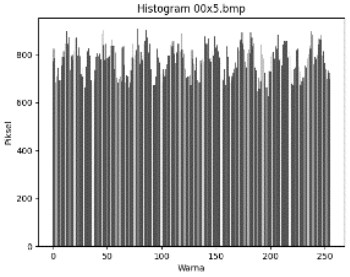
(a) Histogram Citra medis asli (b) $b = 1$ (c) $b = 2$



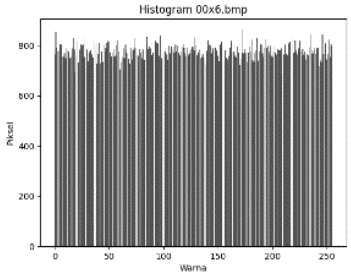
(d) $b = 3$



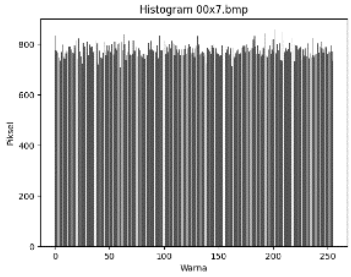
(e) $b = 4$



(f) $b = 5$



(g) $b = 6$



(h) $b = 7$

Gambar 6. Hasil enkripsi citra medis

4.3 SSIM

Dari persamaan (3) didapati bahwa SSIM memiliki nilai antara 0 dan 1. Semakin mirip dua buah gambar, maka nilai SSIM akan semakin mendekati 1.

Tabel 1 Hasil perhitungan SSIM

b	**SSIM**
1	0.0166
2	0.0086
3	0.0086
4	0.0094
5	0.0093
6	0.0090
7	0.0091

Pada penelitian ini, citra asli dibandingkan dengan citra terenkripsi dengan nilai $b = 1$ hingga $b = 7$ seperti yang terlihat pada Tabel 1. Dari hasil tersebut, semua nilai *b* menghasilkan skor SSIM yang mendekati 0 sehingga citra terenkripsi cenderung berbeda dari citra aslinya.

4.4 Probabilitas Brute Force

Pada pengujian ini, dilakukan dua asumsi yaitu asumsi bahwa pihak ketiga mengetahui banyaknya bit MSB yang diganti (nilai dari *b*) dan asumsi bahwa pihak ketiga tidak mengetahui banyaknya bit MSB yang diganti.

Perhitungan probabilitas pada asumsi pertama dengan ukuran citra 528×377 piksel dengan menggunakan persamaan (4) dapat dilihat pada Tabel 2.

Tabel 2 Probabilitas brute force asumsi pertama

b	**P(citra)**
1	$\left(\frac{1}{2^1}\right)^{528\times377} = (1.14 \times 10^{-169})^{377}$
2	$\left(\frac{1}{2^2}\right)^{528\times377} = (1.29 \times 10^{-318})^{377}$
3	$\left(\frac{1}{2^3}\right)^{528\times377} \approx 0$
4	$\left(\frac{1}{2^4}\right)^{528\times377} \approx 0$
5	$\left(\frac{1}{2^5}\right)^{528\times377} \approx 0$
6	$\left(\frac{1}{2^6}\right)^{528\times377} \approx 0$
7	$\left(\frac{1}{2^7}\right)^{528\times377} \approx 0$

Sedangkan untuk asumsi kedua, probabilitas pihak ketiga mendapatkan citra medis asli dengan ukuran citra 528×377 menggunakan persamaan (5) adalah $p(citra) = \sum_{b=1}^{7} \left(\frac{1}{2^b}\right)^{528\times377} \approx 0$.

5. Kesimpulan dan Saran

Pada penelitian ini, telah diajukan sebuah metode enkripsi selektif untuk citra medis yang bertujuan untuk menghemat waktu komputasi dan sumber daya namun masih memiliki performa yang baik. Dari hasil pengujian, nilai SSIM untuk setiap nilai *b* mendekati 0. Namun untuk hasil yang optimal berdasarkan hasil pengamatan langsung pada citra terenkripsi dan histogram, banyaknya bit minimal yang yang dienkripsi adalah 4. Selain itu, metode

yang diajukan memiliki probabilitas yang kecil untuk citra terenkripsi dapat ditebak oleh pihak ketiga sehingga layak untuk diimplementasikan pada kasus nyata. Metode enkripsi ini dapat dikembangkan dengan menggunakan algoritma pembangkit bilangan acak seperti Lehmer dan Park-Miller-Carta pseudo-random number generators.

Ucapan Terima kasih

Program Penelitian Mandiri (PM) bersumber dari DIPA Politeknik Negeri Bandung dengan surat perjanjian Pelaksanaan Kegiatan Nomor : 105.91/PL1.R7/PG.00.03/2021. Kami ucapkan terima kasih atas partisipasi semua pihak atas terlaksananya penelitian ini.

Daftar Pustaka:

Abdelfatah, R. I. (2020). Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi Chaotic-Based Dynamic DNA Computations. *IEEE Access*, *8*, 69894–69907. https://doi.org/10.1109/ACCESS.2020.2987197

Bayu Seta, H., Yulistiani, R., Universitas Pembangunan Nasional Veteran Jakarta, D., Universitas Pembangunan Nasional Veteran Jakarta, M., & Fatmawati Jakarta Selatan, J. R. (2020). Pengamanan Citra Digital Rekam Medis Menggunakan Perpaduan Hashing Algoritma Keccak Dan Rivest Code 6. *Jurnal Ilmiah Matrik*, *22*(3), 257–269. https://doi.org/10.33557/JURNALMATRIK.V22I3.1077

Cao, F., Huang, H. ., & Zhou, X. . (2003). Medical image security in a HIPAA mandated PACS environment. *Computerized Medical Imaging and Graphics*, *27*(2–3), 185–196. https://doi.org/10.1016/S0895-6111(02)00073-3

Cheng, S., Wang, L., Ao, N., & Han, Q. (2020). A Selective Video Encryption Scheme Based on Coding Characteristics. *Symmetry*, *12*(3), 332. https://doi.org/10.3390/sym12030332

Eichenauer-Herrmann, J., Herrmann, E., & Wegenkittl, S. (1998). *A survey of quadratic and inversive congruential pseudorandom numbers* (hal. 66–97). https://doi.org/10.1007/978-1-4612-1690-2_4

He, J., Xu, Y., Luo, W., Tang, S., & Huang, J. (2020). A novel selective encryption scheme for H.264/AVC video with improved visual security. *Signal Processing: Image Communication*, *89*, 115994. https://doi.org/10.1016/j.image.2020.115994

James, F. (1990). A review of pseudorandom number generators. *Computer Physics Communications*, *60*(3), 329–344. https://doi.org/10.1016/0010-4655(90)90032-V

Khashan, O. A., & AlShaikh, M. (2020). Edge-based lightweight selective encryption scheme for digital medical images. *Multimedia Tools and Applications*, *79*(35–36), 26369–26388. https://doi.org/10.1007/s11042-020-09264-z

Khashan, O. A., Zin, A. M., & Sundararajan, E. A. (2014). Performance study of selective encryption in comparison to full encryption for still visual images. *Journal of Zhejiang University SCIENCE C*, *15*(6), 435–444. https://doi.org/10.1631/jzus.C1300262

Larobina, M., & Murino, L. (2013). Medical Image File Formats. *Journal of Digital Imaging 2013 27:2*, *27*(2), 200–206. https://doi.org/10.1007/S10278-013-9657-9

MARSAGLIA, G. (1972). The Structure of Linear Congruential Sequences. In *Applications of Number Theory to Numerical Analysis* (hal. 249–285). Elsevier. https://doi.org/10.1016/B978-0-12-775950-0.50013-3

Massoudi, A., Lefebvre, F., De Vleeschouwer, C., Macq, B., & Quisquater, J.-J. (2008). Overview on Selective Encryption of Image and Video: Challenges and Perspectives. *EURASIP Journal on Information Security*, *2008*, 1–18. https://doi.org/10.1155/2008/179290

Munir, R. (2012). Algoritma Enkripsi Citra Digital Berbasis Chaos dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map. *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, *1*(3), 166. https://doi.org/10.23887/janapati.v1i3.9814

Ou, Y., Sur, C., & Rhee, K. H. (2007). Region-Based Selective Encryption for Medical Imaging. In *Frontiers in Algorithmics* (hal. 62–73). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-73814-5_6

Shifa, A., Naveed Asghar, M., Ahmed, A., & Fleury, M. (2020). Fuzzy-logic threat classification for multi-level selective encryption over real-time video streams. *Journal of Ambient Intelligence and Humanized Computing*, *11*(11), 5369–5397. https://doi.org/10.1007/s12652-020-01895-2

T, V. M., C, R. K., & M E, R. (2021). Selective Encryption of the Audio Extracted from the Video Streamed Over the CDN. *2021 IEEE Mysore Sub Section International Conference (MysuruCon)*, 98–102. https://doi.org/10.1109/MysuruCon52639.2021.9641548

Zaenury, Z. D. W., ipam, I. F. A., & wahyu, W. A. S. (2020). Implementasi Algoritma Camellia Untuk Keamanan Citra Medis Pada Sistem Radiologi Berbasis Web. *Jurnal Informatika Polinema*, *6*(4), 1–8. https://doi.org/10.33795/JIP.V6I4.296