

# IMPLEMENTASI ALGORITMA CAMELLIA UNTUK KEAMANAN CITRA MEDIS PADA SISTEM RADIOLOGI BERBASIS WEB

Zaenury Dhany Wibowo<sup>1</sup>, Ipam Fuaddina Adam<sup>2</sup>, Wahyu Andi Saputra<sup>3</sup>

<sup>1,2,3</sup> Teknik Informatika, Teknologi Industri dan Informatika, Institut Teknologi Telkom Purwokerto

<sup>1</sup>15102080@st3telkom.ac.id, <sup>2</sup> ipam@ittelkom-pwt.ac.id, <sup>3</sup> andi@ittelkom-pwt.ac.id

---

## Abstrak

Dalam bidang radiologi, citra medis dikategorikan sebagai data yang sensitif dan privasi bagi pasien maupun pihak rumah sakit. Citra medis yang digunakan untuk keperluan radiologi melalui jaringan internet tidaklah sepenuhnya aman. Penelitian ini menawarkan algoritma Camellia sebagai alternatif keamanan citra medis pada sistem radiologi berbasis *web*. Penggunaan mode operasi pada *block cipher* adalah sebuah prosedur yang diperlukan untuk memproses blok agar menjadi lebih aman. Mode operasi yang dapat diaplikasikan dalam algoritma Camellia adalah ECB, CBC, CFB, dan OFB. Implementasi Camellia dengan mode operasi tersebut, memiliki hasil yang berbeda. Untuk evaluasinya, beberapa parameter analisis keamanan enkripsi yang dilakukan adalah visual, histogram, dan entropi. Sedangkan kualitas citra dekripsi diukur melalui *Peak Signal to Noise Ratio* (PSNR). Selain itu, implementasi algoritma Camellia dalam mode operasi diukur kompleksitas waktunya. Eksperimen dilakukan terhadap data citra medis berformat jpg. Pengujian sistem menggunakan *blackbox*, dimana hasil pengujian sistem radiologi dapat berjalan dengan baik. Hasil pengukuran menunjukkan mode operasi ECB dan OFB memiliki kualitas citra yang lebih baik. Sedangkan kompleksitas waktu mode operasi ECB lebih cepat dari tiga mode operasi lainnya. Namun, untuk hasil enkripsi citra dengan keamanan yang baik, perlu menghindari mode operasi ECB.

**Kata kunci : Citra medis, Algoritma Camellia, Mode Operasi, Parameter Analisis**

---

## 1. Pendahuluan

Dalam dunia medis, kebanyakan data rekam medis sudah dalam bentuk media digital. Citra medis adalah salah satu gambar, hasil dari pemeriksaan x-ray yang menyimpan informasi penyakit pasien dan dapat ditemukan dalam bidang radiologi. Pembacaan citra medis biasanya dilakukan oleh ahli radiologi yang berguna untuk analisis penyakit dari citra medis pasien dari jarak jauh. Kemajuan teknologi informasi membuat Rumah Sakit harus menyediakannya dan menerapkannya untuk layanan radiologi. Menurut Data dan Informasi dan Profil Kesehatan Indonesia tahun 2018, jumlah Dokter Spesialis Radiologi 2975 orang, masih belum memenuhi sebanyak 645 orang (kemenkes, 2018). Karena alasan ini sehingga Dokter tidak harus datang langsung ke Rumah Sakit. Dengan adanya sistem digitalisasi berbasis jaringan internet, pelayanan radiologi dapat diakses kapanpun dan dimanapun sehingga menjadi efektif dan efisien.

Keamanan menjadi masalah utama ketika melibatkan penggunaan teknologi jaringan internet. Merujuk pada data yang telah di *update* oleh *breachlevelindex.com*, dalam kurun waktu 5 tahun terakhir hingga pada tahun 2018, angka pelanggaran data yang terjadi mencapai 3 miliar (Gemalto, 2018). Hal ini menjadi perhatian bagi organisasi medis yang harus mematuhi Asuransi Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA), data rekam medis yang dikirim menyesuaikan

format standar dan keamanan yang baik (Bhagal, Li, Gale, & Chen, 2018). Informasi rahasia yang tersimpan memperkuat alasan mengapa pentingnya citra medis untuk dienkripsi dengan aman dan dapat dikembalikan sempurna setelah didekripsi. Untuk mengatasi berbagai insiden ancaman citra medis, maka dibutuhkan metode keamanan dengan menggunakan kriptografi.

Algoritma Camellia sebagai solusi alternatif untuk masalah perlindungan data. Algoritma ini berada dalam kategori algoritma simetris dan merupakan jenis *block cipher* yang beroperasi membagi blok data dengan ukuran yang sama 128 bit. Enkripsi citra medis dengan skema *block cipher*, ini bertujuan mengimplementasikan algoritma enkripsi yang mana memproses blok-blok *pixel* dengan kunci yang sama. Karena algoritma ini memproses blok data, penting untuk menggunakan mode operasi dalam mengenkripsi blok-blok *pixel* dari sebuah citra.

Salah satu faktor penting dalam enkripsi citra digital adalah inspeksi visual di mana kualitas menentukan algoritma yang baik. Akan tetapi, inspeksi visual enkripsi tidak cukup untuk menilai informasi yang tersembunyi dalam sebuah citra. Mengingat citra medis bervolume data yang besar, implementasi algoritma Camellia diharapkan tidak mengompresi dan mengurangi kualitas secara signifikan. Kualitas citra yang buruk akan menghasilkan diagnosis yang salah sehingga akan berakibat fatal dalam tindakan selanjutnya. Dengan

demikian, teknik pengukuran lain dipertimbangkan untuk mengevaluasi tingkat keamanan enkripsi dan kualitas dekripsi secara kuantitatif.

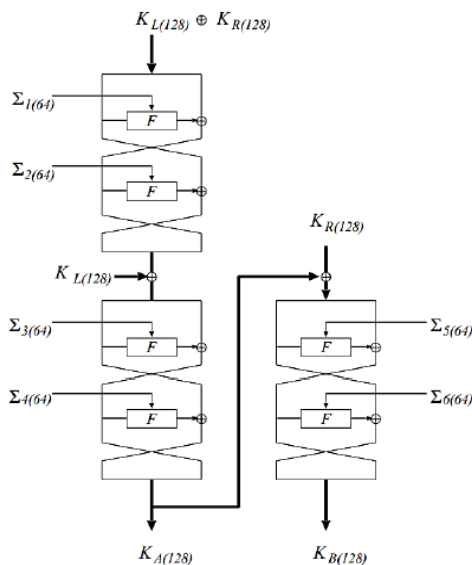
Selain inspeksi visual, tiga pengukuran untuk membandingkan antara empat mode operasi yang diaplikasikan pada algoritma Camellia adalah PSNR, Histogram dan Entropi, serta menganalisis perbandingan efisiensi kompleksitas waktu program yang diukur ketika menggunakan mode operasi tersebut.

Dalam makalah ini pengujian akan dilakukan dengan empat mode operasi *block cipher* yang diaplikasikan dalam algoritma Camellia untuk menentukan mana yang lebih baik dalam menyembunyikan informasi, kualitas yang dihasilkan dan waktu yang dibutuhkan.

2. Landasan Teori

2.1 Penjadwalan Kunci Algoritma Camellia

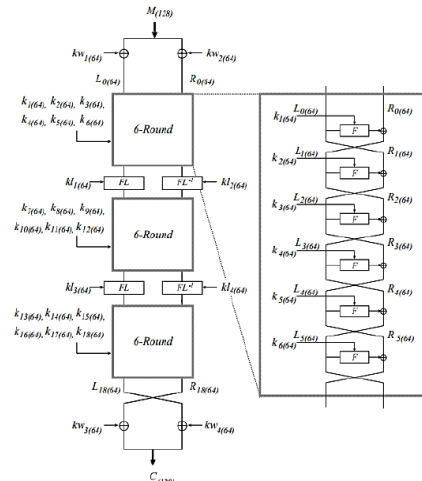
Proses penjadwalan terdapat dua buah kunci variabel 128 bit KL(128), KR(128) yang kemudian di proses dengan konstanta  $\Sigma 1, \Sigma 2, \Sigma 3$  sampai  $\Sigma 6$  sehingga menghasilkan KA(128) dan KB(128) (Kazumaro AOKI, Tetsuya ICHIKAWA, 2001).



Gambar 1 Penjadwalan Kunci Algoritma Camellia Sumber Data : (Kazumaro AOKI, Tetsuya ICHIKAWA, 2001)

2.2 Enkripsi Algoritma Camellia

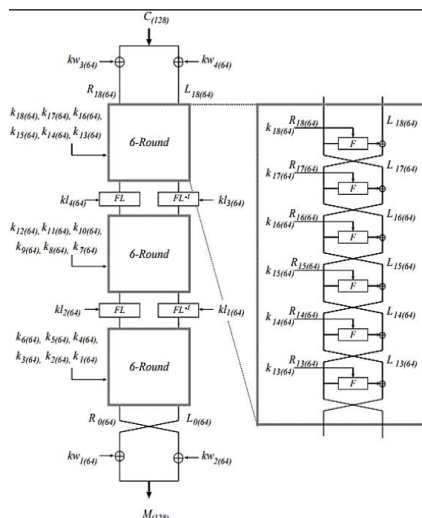
Proses enkripsi Camellia *plain image* diubah menjadi 128 bit, kemudian diproses dengan kunci substitusi k, kl, kw sehingga menghasilkan *chiper image* 128 bit. Dalam proses enkripsi terdapat 18 putaran. Fungsi utama yang akan di proses melalui perputaran tersebut adalah fungsi F yang digunakan dalam setiap 6 putaran, fungsi FL, fungsi FL<sup>-1</sup> (Kazumaro AOKI, Tetsuya ICHIKAWA, 2001).



Gambar 2 Diagram Alir Enkripsi Camellia 128 bit Sumber Data : (Kazumaro AOKI, Tetsuya ICHIKAWA, 2001)

2.3 Dekripsi Algoritma Camellia

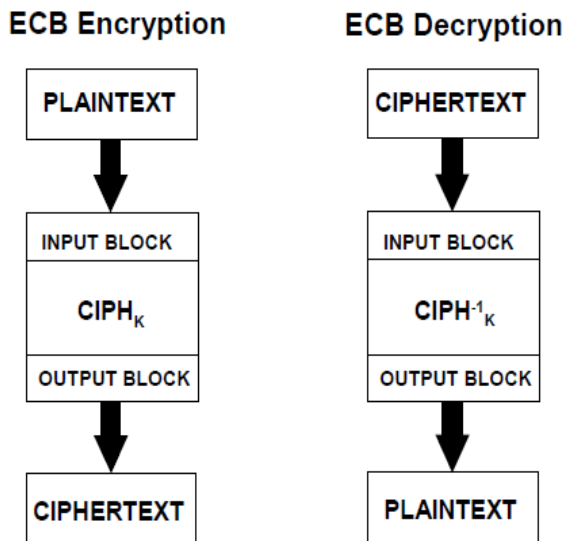
Proses dekripsi Camellia *chiper image* diubah menjadi 128 bit, kemudian diproses dengan kunci substitusi k, kl, kw sehingga menghasilkan *chiper image* 128 bit. Dalam proses enkripsi terdapat 18 putaran. Fungsi utama yang akan di proses melalui perputaran tersebut adalah fungsi F yang digunakan dalam setiap 6 putaran, fungsi FL, fungsi FL<sup>-1</sup> (Kazumaro AOKI, Tetsuya ICHIKAWA, 2001).



Gambar 3 Diagram Alir Dekripsi Camellia 128 bit Sumber Data : (Kazumaro AOKI, Tetsuya ICHIKAWA, 2001)

2.4 Electronic Code Book

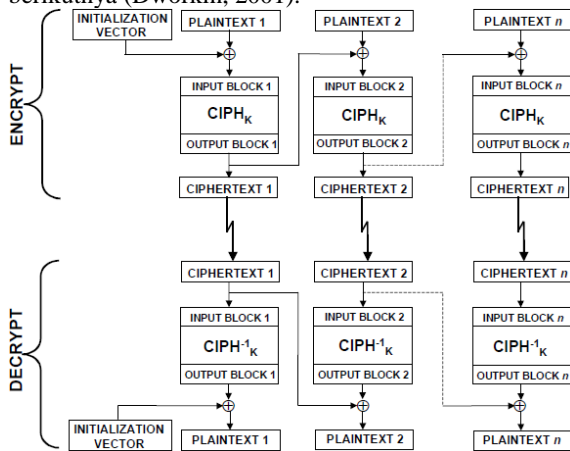
Mode ECB merupakan skema yang paling sederhana. *Plain image* akan di pecah terpisah menjadi blok dengan ukuran sama dan setiap blok dapat di proses langsung dengan kunci masukan tanpa ada operasi tambahan (*feedback*) dan inputan tambahan (*initialization vector*) (Dworkin, 2001).



Gambar 4 Skema Mode Operasi ECB  
Sumber Data : NIST Special Publication 800-38A

2.5 Chiper Block Chaining

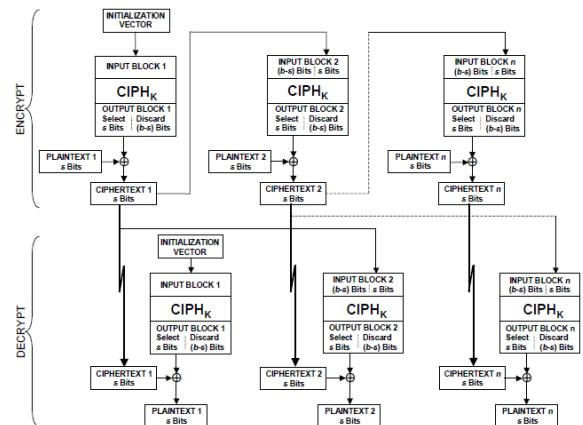
Mode CBC menerapkan operasi berantai (*chaining*). Blok pertama *plain image*, memerlukan tambahan *initialization vector* sebagai data acak ( $C_0$ ) untuk menghasilkan *chiper image* ( $C_1$ ). Hasil dari blok sebelumnya menjadi *feedback* pada blok berikutnya (Dworkin, 2001).



Gambar 5 Skema Mode Operasi CBC  
Sumber Data : NIST Special Publication 800-38A

2.6 Chiper Feedback

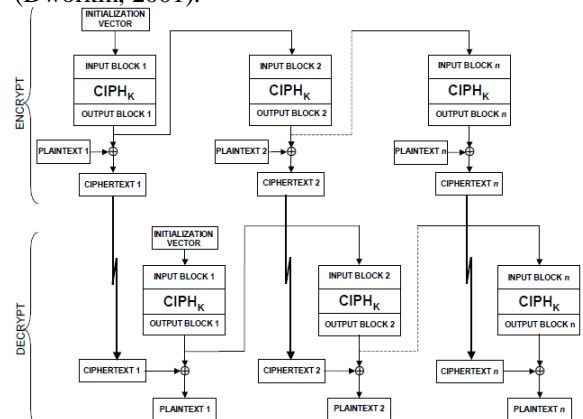
Mode CFB mirip dengan mode CBC yaitu hasil *chiper image*  $C_1$  menjadi *feedback* pada blok berikutnya. Hanya saja perbedaan terletak pada proses awal setiap blok. *Initialization vector* ( $C_0$ ) akan dimasukkan dalam *register* geser dalam blok *plain image* pertama. Untuk lebih selengkapnya Gambar 3 menjelaskan skema enkripsi dan dekripsi mode CFB (Dworkin, 2001).



Gambar 6 Skema Mode Operasi CFB  
Sumber Data : NIST Special Publication 800-38A

2.7 Output Feedback

Mode OFB mirip dengan mode CFB yaitu Blok *plain image* pertama, *initialization vector* ( $C_0$ ) akan dimasukkan dalam *register* geser. Perbedaannya terletak pada hasil keluaran blok proses enkripsi yang kemudian akan dilakukan operasi *feedback* untuk proses blok berikutnya (Dworkin, 2001).



Gambar 7 Diagram Mode Operasi OFB  
Sumber Data : NIST Special Publication 800-38A

3. Metode Penelitian

Metode penelitian yang akan diterapkan terdiri dari dua yaitu melakukan pengumpulan data dengan mempelajari, mengamati, studi literatur serta didukung dengan implementasi untuk menguji fungsional aplikasi berdasarkan perancangan sistem, dan analisis deskriptif hasil pengukuran dari keempat mode operasi yang diaplikasikan dalam algoritma Camelia.

3.1 Sumber Data

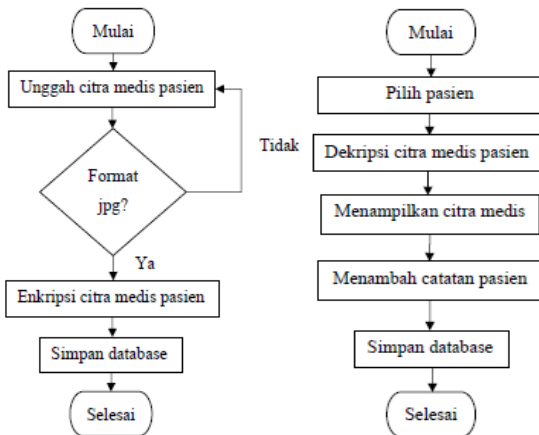
Sumber data yang dikumpulkan penulis melalui observasi dan wawancara langsung pada bagian teknologi informasi, Radiolog dan Dokter Spesialis Radiologi di Rumah Sakit Siaga Medika Banyumas. Data yang diambil dan digunakan untuk

penelitian ini adalah citra medis hasil pemeriksaan x-ray dengan format jpg.

### 3.2 Perancangan Sistem

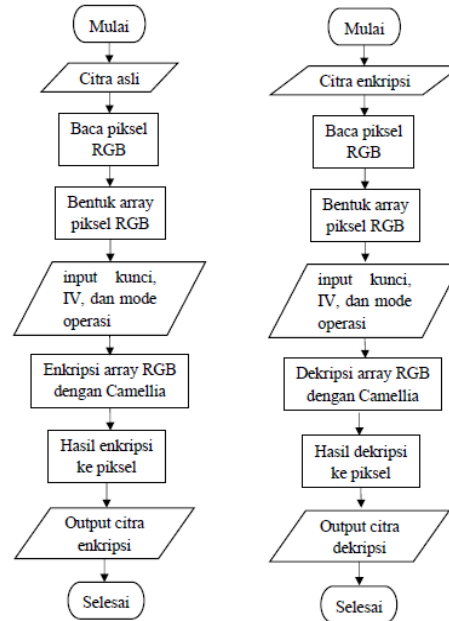
Metode pengembangan sistem aplikasi yang dibuat menggunakan *prototype*. Perancangan dibagi menjadi dua bagian yaitu perancangan desain *Unified Modeling Language* (UML) dan perancangan alur pembentukan keamanan citra medis menggunakan algoritma Camellia. Implementasi interaktif aplikasi menggunakan *framework CodeIgniter*. Sedangkan untuk keamanan menggunakan bahasa pemrograman Python 3.

Pada Gambar 8, skenario penggunaan aplikasi dimulai dari radiolog yang mengunggah citra medis. Apabila citra medis yang di unggah bukan merupakan format jpg, maka sistem akan menampilkan *bad request error* yang berarti format file harus sesuai dengan jpg. Setelah mengecek format file yang diunggah valid, citra medis dienkripsi menggunakan algoritma Camellia dengan kunci 128 bit. Radiolog melanjutkan dengan mengisi formulir data pasien dan mengirimkannya pada Dokter Spesialis Radiologi. Proses dekripsi citra medis dimulai saat Dokter Spesialis Radiologi membuka salah satu pasien masuk. Dokter Spesialis Radiologi dapat menambah catatan pasien sebagai hasil pemeriksaan citra medis. Untuk lebih selengkapnya digambarkan dalam diagram alir berikut.



Gambar 8 Diagram Alir Aplikasi Web Secara Umum

Diagram alir berikut memperlihatkan bagaimana proses citra medis menjadi terenkripsi.



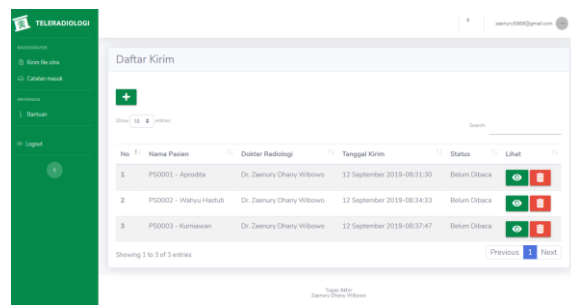
Gambar 9 Tahapan Proses

Dalam Gambar 9 diatas dijelaskan tahapan berjalannya proses secara runtut. Berikut penjelasan dari gambar diatas.

1. Proses dimulai dengan memasukkan file citra asli.
2. Selanjutnya adalah proses membaca *pixel* citra (panjang dan lebar) setiap *red*, *green* dan *blue*.
3. Bentuk array untuk menampung masing-masing *red*, *green*, dan *blue*.
4. Deklarasi variabel untuk menyimpan konfigurasi kunci 128 bit, *initialization vector*, dan mode operasi yang digunakan.
5. Proses dilakukan menggunakan algoritma Camellia pada array setiap *red*, *green*, dan *blue*.
6. Kembalikan dari proses array sebelumnya ke bentuk *pixel* setiap *red*, *green*, dan *blue*.
7. Hasil keluaran menjadi citra yang terenkripsi dan terdekripsi.

## 4. Pengujian dan Analisis

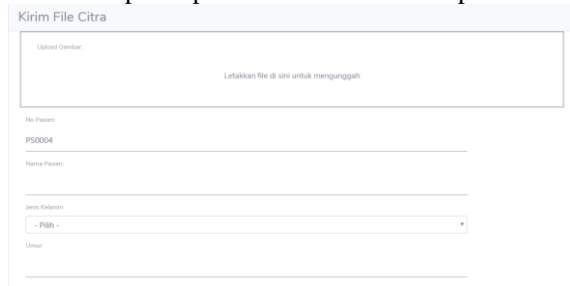
### 4.1 Tampilan Antarmuka



Gambar 10 Daftar Kirim Citra Medis Pasien

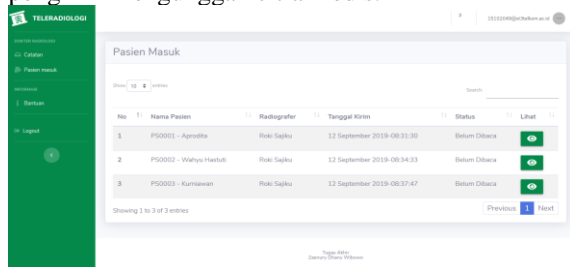
Halaman ini menampilkan daftar pengiriman citra medis pasien dari menu “kirim file citra”.

Sedangkan untuk menu “catatan masuk” merupakan halaman laporan pemeriksaan citra medis pasien.



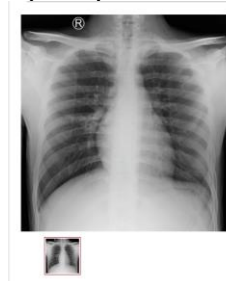
Gambar 11 Mengunggah Citra Medis Pasien

Halaman ini digunakan untuk mengunggah citra medis pasien. Proses enkripsi dimulai pada saat pengirim mengunggah citra medis.



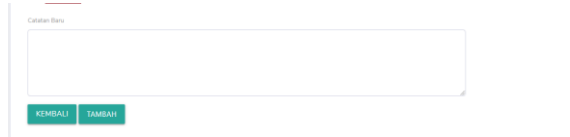
Gambar 12 Daftar Pasien Masuk

Halaman ini menampilkan daftar pasien masuk dari menu “pasien masuk”. Sedangkan untuk menu “catatan” merupakan halaman daftar pengiriman laporan pemeriksaan citra medis pasien.



Gambar 13 Lihat Citra Medis Pasien

Halaman ini adalah untuk melihat citra medis. Proses dekripsi dimulai saat membuka daftar pasien masuk.



Gambar 14 Pemeriksaan Citra Medis Pasien

Halaman ini digunakan untuk menafsirkan pemeriksaan, melaporkan citra medis dan merekomendasikan tindakan.

4.2 Pengujian Blackbox

Pengujian blackbox merupakan pengujian yang didasarkan pada detail sistem fokusnya untuk

mengamati dan memeriksa fungsional dari perangkat lunak.

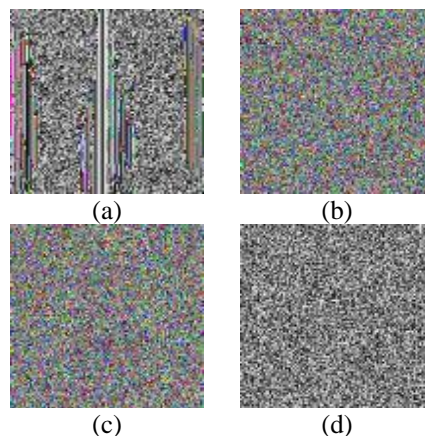
Tabel 1 Pengujian Blackbox Radiolog

No	Pengujian	Hasil
1	Mengunggah citra medis	Berhasil
2	Mengenkripsi citra medis	Berhasil
3	Mengisi form data pasien	Berhasil
4	Menampilkan daftar kirim citra medis pasien	Berhasil
5	Menghapus citra medis pasien	Berhasil
6	Menampilkan daftar laporan pemeriksaan citra medis pasien	Berhasil
7	Mengunduh laporan citra medis pasien	Berhasil
8	Menghapus laporan citra medis pasien	Berhasil

Tabel 2 Pengujian Blackbox Dokter Spesialis Radiologi

No	Pengujian	Hasil
1	Menampilkan daftar pasien masuk	Berhasil
2	Melihat citra medis pasien	Berhasil
3	Mendekripsi citra medis	Berhasil
4	Mengisi form pemeriksaan citra medis	Berhasil
5	Menampilkan daftar laporan pemeriksaan citra medis pasien	Berhasil
6	Mengunduh laporan citra medis pasien	Berhasil
7	Menghapus laporan citra medis pasien	Berhasil

4.3 Analisis Visual



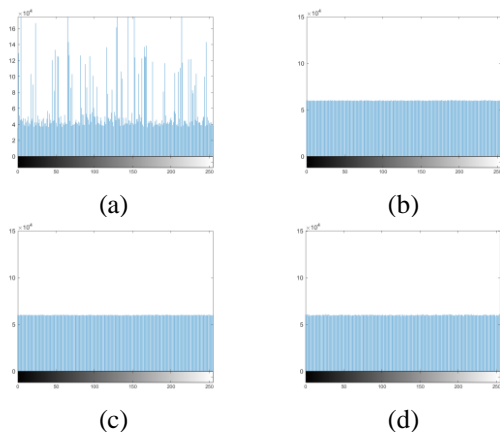
Gambar 15 Perbandingan Visual Enkripsi (a) Mode ECB, (b) Mode CBC, (c) Mode CFB, (d) Mode OFB

Analisa visual berdasarkan pengujian enkripsi disetiap mode operasi menunjukkan bahwa algoritma Camellia dalam mode ECB memiliki perbedaan dibandingkan dengan lain. Secara teori, ini karena mode ECB memproses setiap blok plain image secara independen dan tanpa ada operasi feedback ke blok berikutnya. Jika pada titik-titik pixel plain image tertentu memiliki intensitas warna

yang sama, maka akan menghasilkan *chiper image* yang sama. Sehingga akan terlihat jelas bahwa citra yang terenkripsi masih membentuk pola dari citra aslinya.

**4.4 Analisis Histogram**

Menurut (Kaur & Sharma, 2013), histogram adalah representasi grafis dari nilai intensitas warna sehubungan dengan jumlah *pixel* pada suatu citra. Histogram pada citra dapat digunakan untuk menganalisis jumlah piksel yang terdistribusi pada intensitas warna tertentu. Histogram citra terenkripsi memiliki perbedaan dengan citra asli. Sehingga histogram tersebut secara statistik tidak sama. Semakin merata bentuk histogram citra, maka semakin tersebar pula intensitas warna pada *pixel*.



Gambar 16 Perbandingan Visual Enkripsi (a) Mode ECB, (b) Mode CBC, (c) Mode CFB, (d) Mode OFB

Histogram citra asli dengan citra terenkripsi terlihat sangat berbeda jauh. Histogram citra enkripsi dalam mode ECB menunjukkan distribusi nilai *pixel* tidak merata. Intensitas warna citra enkripsi dalam mode CBC, CFB dan OFB menunjukkan distribusi nilai *pixel* yang merata.

**4.5 Analisis Entropi**

Entropi memainkan peranan penting dimana citra medis harus di enkripsi secara benar sehingga tidak ada kebocoran informasi. Secara spesifik, entropi digunakan untuk mengukur kemungkinan informasi yang terkandung pada sebuah citra. Jika *m* merupakan sekumpulan citra acak, maka nilai entropi *H(m)* dihitung dengan rumus berikut:

$$H(m) = \sum_{i=0}^{2^m-1} P(M_i) \log_2 \frac{1}{P(m_i)}$$

Menurut (Munir, 2012), *cipher image* (citra acak) yang dihasilkan memiliki nilai ideal 8. Entropi *chiper image* yang kurang dari nilai ini, menyatakan kemungkinan informasi yang terkandung didalamnya dapat diketahui. Untuk melihat tingkat keamanannya dengan cara menghitung nilai entropi

sehingga dapat diketahui keacakan dari *chiper image*.

Analisis keamanan dan metode pengukuran menggunakan aplikasi MATLAB R2018b. Berikut adalah data uji yang digunakan dalam penelitian ini.

Tabel 3 Data Uji

No	Ukuran Dimensi	Ukuran File (byte)	Format
1	2048x2048	274,262	JPG
2	3020x2400	560,431	JPG
3	2048x2048	257,507	JPG
4	2048x2048	209,257	JPG
5	2048x2500	309.117	JPG

Tabel 4 Analisa Entropi

No	Entropi			
	ECB	CBC	CFB	OFB
1	7,9939	8	8	8
2	7,9419	8	8	8
3	7,9969	8	8	8
4	7,9957	8	8	8
5	7,9868	8	8	8
Rata-rata	7,98304	8	8	8

Berdasarkan data pengujian pada Tabel 3, pengukuran pada Tabel 4 menunjukkan nilai entropi algoritma Camellia dalam mode ECB tidak lebih baik daripada yang lain. Intensitas warna yang belum sepenuhnya seragam dan transisi tingkat keabuan yang belum sepenuhnya merata, maka kualitas enkripsi rendah. Sehingga informasi yang terkandung dalam citra medis dapat diketahui.

**4.3.4 Analisis Kualitas Citra**

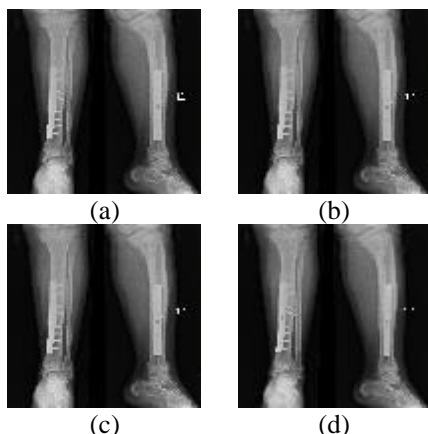
Untuk mengukur kualitas citra, *Mean Square to Error* (MSE) digunakan untuk mengukur kualitas algoritma yang diusulkan dengan memeriksa antara citra asli dengan citra dekripsi. Secara matematis dapat dihitung dengan rumus berikut.

$$MSE = \frac{1}{M * N} \sum_{y=1}^{M-1} \sum_{x=1}^{N-1} [I(x, y) - K(x, y)]$$

PSNR merupakan hasil perhitungan rasio tingkat warna maksimum dengan kuantitas nilai MSE (*noise*) dari citra didekripsi. Dalam kasus sebuah citra, semakin tinggi nilai PSNR berarti semakin baik kualitasnya. Secara matematis dapat dihitung dengan rumus berikut.

$$PSNR = 10 \log_{10} \frac{255}{\sqrt{MSE}}$$

Menurut (Sulaiman & Agoes, 2017), kualitas citra dikatakan baik jika PSNR diatas 40 dB (desibel). Sementara kualitas citra yang buruk kurang dari 40 dB.



Gambar 17 Perbandingan Visual Dekripsi (a) Mode ECB, (b) Mode CBC, (c) Mode CFB, (d) Mode OFB

Tabel 5 Analisa PSNR

No	PSNR (dB)			
	ECB	CBC	CFB	OFB
1	67,88	57,48	60,11	67,88
2	68,3	61,63	60,83	68,3
3	69,22	60,14	58,91	69,22
4	69,64	60,34	59,9	69,64
5	69,65	58,52	58,18	69,65
Rata-rata	68,94	59,62	59,59	68,94

Pengukuran PSNR menggunakan data uji yang tertera pada Tabel 3. Hasil pada Tabel 5 menunjukkan algoritma Camellia dalam mode ECB dan OFB memiliki kualitas yang sama daripada mode CBC dan CFB.

#### 4.3.5 Analisis Kompleksitas Waktu

Kompleksitas diukur waktu keseluruhan implementasi dalam bahasa pemrograman Python. Dalam penelitian ini, Lingkungan implementasi dan pengujian dengan Prosesor : Intel(R) Core (TM) i3-5005U CPU 2.00GHz (4 CPUs), dan memori RAM 4 GB.

Tabel 6 Analisa Kompleksitas Waktu Enkripsi

No	Kompleksitas Waktu Enkripsi (detik)			
	ECB	CBC	CFB	OFB
1	33	33	145	52
2	73	57	260	76
3	39	34	144	44
4	43	33	143	44
5	43	41	174	51
Rata-rata	46	40	173	53

Tabel 7 Analisa Kompleksitas Waktu Dekripsi

No	Kompleksitas Waktu Dekripsi (detik)			
	ECB	CBC	CFB	OFB
1	32	34	142	43
2	69	57	257	73
3	38	33	144	43
4	37	33	144	42

5	43	40	174	51
Rata-rata	44	39	172	50

Berdasarkan Tabel 6 dan Tabel 7, memperlihatkan algoritma Camellia dalam mode ECB memiliki waktu komputasi yang lebih cepat daripada tiga mode lainnya. Secara teori, hal ini disebabkan algoritma Camellia dalam mode ECB memproses setiap blok *plain image* tanpa menunggu blok-blok sebelumnya. Sedangkan pada mode operasi lain bergantung pada blok sebelumnya selesai terlebih dahulu dan terdapat masukan tambahan yaitu *initialization vector*.

## 5. Kesimpulan dan Saran

### 5.1 Kesimpulan

Adapun hasil kesimpulan dari penelitian ini sebagai berikut:

1. Implementasi algoritma Camellia pada sistem radiologi berbasis *web* berhasil dilakukan dengan cara enkripsi dan dekripsi ketika mengunggah dan melihat citra medis.
2. Algoritma Camellia memberikan hasil yang sangat baik dalam mengenkripsi citra medis dalam tiga mode operasi kecuali mode ECB. Keamanan pada mode ECB kurang memenuhi syarat dan tidak disarankan. Hal ini ditunjukkan dari hasil analisa visual enkripsi, data pengukuran entropi dan analisa histogram enkripsi.
3. Membandingkan hasil pengujian citra medis dengan ukuran yang berbeda dalam mode ECB, terlihat bahwa meskipun kualitas enkripsi sangat buruk, ini memberikan hasil kualitas dekripsi tertinggi bersama dengan mode OFB.
4. Kompleksitas waktu yang dibutuhkan masih relatif lama. Meskipun mode ECB memiliki waktu komputasi lebih cepat, implementasi mempengaruhi hasil tersebut. Hal ini disebabkan proses pembentukan array RGB, enkripsi dan dekripsi array RGB hingga mengembalikan hasil enkripsi ke *pixel* lebih lama. Selain faktor tersebut, ukuran resolusi citra medis mempengaruhi. Semakin besar volume citra, maka akan semakin lama waktunya.

### 5.2 Saran

Penulis mempunyai saran untuk pengembangan selanjutnya yaitu

1. Penulis dalam mengembangkan aplikasi hanya sebatas *prototype*. Untuk pengembangan selanjutnya aplikasi radiologi dibuat menggunakan metode pengembangan sistem yang lebih kompleks dan menyesuaikan Standar Pelayanan Radiologi Diagnostik .
2. Teknik dalam Implementasi algoritma khususnya citra digital dalam bahasa

pemrograman tertentu, diharapkan tidak menghambat waktu selama proses enkripsi maupun dekripsi.

**Daftar Pustaka:**

- Bhagal, R. S., Li, B., Gale, A., & Chen, Y. (2018). Medical Image Encryption using Chaotic Map Improved Advanced Encryption Standard. *International Journal of Information Technology and Computer Science*, 10(8), 1–10. <https://doi.org/10.5815/ijitcs.2018.08.01>
- Dworkin, M. (2001). *Recommendation for block cipher modes of operation : National Institute of Standards and Technology*. <https://doi.org/10.6028/NIST.SP.800-38d>
- Gemalto. (2018). *Breach Level Index 2018 First Half Review*.
- Kaur, T., & Sharma, R. (2013). Security Definitive Parameters for Image Encryption Techniques. *International Journal of Emerging Technology and Advanced Engineering*, 3(5), 109–112.
- Kazumaro AOKI, Tetsuya ICHIKAWA, M. K. (2001). *Specification of Camellia / a 128-bit Block Cipher*.
- Kemenkes. (2018). *Data dan Informasi Profil Kesehatan Indonesia 2018*.
- Munir, R. (2012). Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map Dan Penerapan Teknik Selektif. *Juti*, 10(2), 89–95. <https://doi.org/http://dx.doi.org/10.12962/j24068535.v10i2.a310>
- Sulaiman, S., & Agoes, S. (2017). Analisis Reduksi Data Citra Menggunakan Metode Dekomposisi Nilai Singular. *CITEE*, 21–25.