ENKRIPSI CITRA SATELIT MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* BERBASIS CCSDS

SATELLITE IMAGE ENCRYPTION USING ADVANCED ENCRYPTION STANDARD ALGORITHM BASED ON CCSDS

Patria Rachman Hakim
Pusat Teknologi Satelit, Lembaga Penerbangan dan Antariksa Nasional (LAPAN)
patriarachmanhakim@yahoo.com

Abstrak

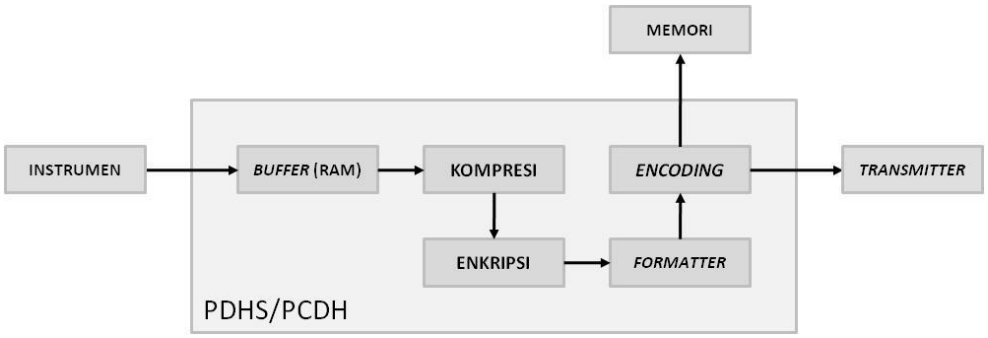
Berdasarkan rekomendasi *Concultative Committee for Space Data Systems* (CCSDS), data satelit akan melalui beberapa tahapan pengolahan sebelum ditransmisikan ke stasiun bumi, yaitu proses kompresi, enkripsi dan *encoding*. Algoritma *Advanced Encryption Standard* (AES) adalah salah satu algoritma kriptografi yang direkomendasikan CCSDS untuk proses enkripsi data satelit, yaitu suatu proses pengacakan terhadap sebuah data sehingga data tersebut terlihat acak dan tidak dapat dikenali sebagai data yang valid. Algoritma AES dapat diimplementasikan dalam beberapa mode operasi, diantaranya yaitu mode *electronic codebook* (ECB), mode *chiper block chaining* (CBC), dan mode *counter* (CTR). Makalah ini membahas perbandingan kinerja antara beberapa mode operasi algoritma AES tersebut untuk mengolah data citra satelit, terkait dengan keamanan data, resistansi terhadap *noise*, dan efisiensi mode operasi. Simulasi dan analisis dilakukan dengan menggunakan perangkat lunak MATLAB dan perangkat keras FPGA. Analisis keamanan data dengan menggunakan pendekatan histogram citra menunjukkan bahwa mode operasi ECB memiliki kinerja yang paling rendah,tetapi tidak rentan terhadap *noise* dan pengolahan dapat dilakukan dengan cepat. Mode CBC memiliki keamanan data yang cukup kuat, tetapi kurang resistan terhadap *noise* dan membutuhkan waktu pengolahan yang lebih lama. Sementara itu, mode *counter* memiliki kinerja terbaik dalam hal perimbangan keamanan data, resistansi terhadap *noise* serta kecepatan waktu pengolahan datanya. Berdasarkan analisis dan pertimbangan kelebihan dan kekurangan beberapa mode operasi tersebut, maka disarankan penggunaan algoritma enkripsi data AES dalam mode operasi *counter* pada sistem pengolah data citra satelit apabila satelit tersebut memiliki sistem *Payload Data Handling* (PDH) yang cukup handal.
Kata kunci: kriptografi, enkripsi citra, *Advanced Encryption Standard*, CCSDS, PDHS.

Abstract

Based on Consultative Committee for Space Data Systems (CCSDS) recommendation, satellite data will be processed in several processing stages before transmitted to earth ground station, which are compression, encryption and encoding process. Advanced Encryption Standard (AES) algorithm is one of cryptographic algorithm that is recommended by CCSDS for satellite data encryption process, a data scrambling process that produces random data which cannot be recognized as valid data. AES algorithm can be implemented in several modes of operation, i.e: electronic codebook mode (ECB), chiper block chaining mode (CBC), and counter mode (CTR). This paper discusses about performance comparison between these AES modes of operation, in terms of data security, noise resistance and operation mode efficiency. Simulation and analysis are done using MATLAB software as well as FPGA hardware implementation. Data security analysis based on image histogram approach shows that ECB mode has the worst performance, but it has fast processing time and resistant to noise. More common CBC mode of operation has a very good data security, but it has higher processing time and more susceptible to noise. Meanwhile, counter mode has the best trade-offs between data security performance, noise resistance and data processing efficiency. Based on advantages and disadvantages of each mode of operation, it is recommended to use AES algorithm in counter operation mode on satellite image data on-board processing, given that the satellite has a good Payload Data Handling System (PDHS).
Keywords: cryptography, image encryption, Advanced Encryption Standard, CCSDS, PDHS.

1. PENDAHULUAN

Concultative Committee for Space Data Systems (CCSDS) merupakan lembaga yang bertugas untuk melakukan penelitian dan pengembangan dalam berbagai hal terkait data satelit, baik dalam hal pengolahan data di dalam satelit ataupun proses penerimaan dan pengiriman data dari/ke stasiun bumi. Terkait pengolahan data di dalam satelit (*on-board*), CCSDS merekomendasikan beberapa tahapan pengolahan data yang sebaiknya dilakukan sebelum data tersebut disimpan atau ditransmisikan. Tahap pertama adalah proses kompresi data, yang bertujuan untuk dapat mengurangi ukuran data yang akan disimpan dalam memori satelit atau yang akan ditransmisikan melalui *transmitter* satelit. Tahap kedua adalah proses enkripsi data, yang bertujuan untuk menjaga kerahasiaan data dari pihak yang tidak berwenang, dengan cara mengacak susunan data menjadi data baru yang tidak terstruktur [1]. Tahap ketiga adalah proses *encoding* data, yang berfungsi untuk mengoreksi data yang akan disimpan atau ditransmisikan bila terganggu oleh adanya *noise* pada saat penyimpanan atau pengiriman. Dalam sistem satelit, beberapa tahapan pengolahan data tersebut dilakukan oleh *Power Control Data Handling* (PCDH) untuk data telemetri dan *Payload Data Handling* (PDH) untuk data muatan satelit. Gambar 1 berikut ini memberikan ilustrasi beberapa tahapan pengolahan data dalam sistem satelit berdasarkan rekomendasi CCSDS.



Gambar 1. Tahapan pengolahan data dalam sistem satelit berbasis CCSDS

Sebagai pusat unggulan teknologi satelit, Pusat Teknologi Satelit (Pusteksat-LAPAN) hingga saat ini terus melakukan penelitian dan pengembangan dalam bidang pengolahan data satelit pada sistem satelit (*on-board*). Beberapa kegiatan penelitian dan perekayasaan telah dilakukan terkait perancangan dan implementasi sistem pengolah data satelit berdasarkan rekomendasi CCSDS, di antaranya adalah mengenai perancangan dan implementasi sistem PDHS menggunakan *Field Programmable Gate Array* (FPGA) berbasis CCSDS [2], perancangan dan implementasi IP-core Reed-Solomon untuk proses encoding [3], serta analisis dan simulasi algoritma kompresi data satelit LAPAN-A3/IPB [4][5]. Walaupun demikian, satu tahapan proses lainnya yang telah direkomendasikan CCSDS yaitu proses enkripsi data belum diteliti dan dikembangkan secara mendalam. Berbeda dengan proses *encoding* yang berfungsi sebagai *forward error correction* (FEC) yang memiliki peran sangat penting dalam keberhasilan proses transmisi, atau proses kompresi yang cukup berperan penting untuk menghemat kapasitas memori penyimpanan atau *bandwidth* dalam proses transmisi, maka proses enkripsi data sering dilupakan karena fungsinya yang hanya dianggap sebagai pengaman data krusial saja. Proses enkripsi mungkin tidak terlalu diperlukan pada satelit eksperimental, tetapi untuk satelit operasional proses enkripsi sangat dibutuhkan untuk menjamin kerahasiaan data telemetri dan data muatan yang dikirimkan satelit, dan yang lebih penting adalah memastikan bahwa satelit tidak dikendalikan oleh pihak yang tidak berwenang.

Secara umum dalam proses enkripsi data, pengirim melakukan proses enkripsi yang mengubah data yang akan dikirim (*plaintext*) menjadi data yang tidak terstruktur (*chipertext*) dan tidak memiliki arti dengan menggunakan sebuah kata kunci. Penerima data kemudian melakukan proses dekripsi untuk mengubah data yang diterima menjadi data asli yang dapat dipahami dengan menggunakan kata kunci yang bersesuaian dengan kata kunci yang digunakan oleh pengirim. Berdasarkan jenis kunci yang digunakan dalam proses enkripsi dan dekripsi, algoritma enkripsi dapat dibagi menjadi dua yaitu algoritma kunci simetrik dan kunci asimetrik. Pada algoritma kunci simetrik, proses enkripsi dan dekripsi menggunakan kunci yang sama sedangkan pada algoritma kunci asimetrik, proses enkripsi dan

dekripsi menggunakan dua kunci yang berbeda. Salah satu contoh algoritma kunci simetrik adalah *Data Encryption Standard* (DES) dan AES (*Advanced Encryption Standard*) yang biasanya digunakan untuk mengolah data berukuran besar yang tidak krusial, sementara algoritma asimetrik seperti RSA (Rivest, Shamir and Adleman) dan algoritma kurva eliptik umumnya digunakan untuk mengolah data penting yang berukuran kecil.

CCSDS telah merekomendasikan algoritma *Advanced Encryption Standard* (AES) dan RSA (Rivest, Shamir dan Adleman) untuk implementasi sistem enkripsi pada sistem satelit [1]. Kedua algoritma tersebut dapat digunakan untuk proses enkripsi data baik pada PCDH maupun PDHS. Walaupun demikian, CCSDS tidak merekomendasikan secara khusus mengenai enkripsi data citra satelit. Walaupun algoritma AES dapat mengolah data citra dengan kinerja tinggi, tetapi terdapat beberapa algoritma enkripsi lain yang juga dapat digunakan untuk mengolah data citra secara efisien. Beberapa algoritma enkripsi tersebut misalnya algoritma peta *chaotic* [6], algoritma *Discrete Cosine Transform* (DCT) [7] dan beberapa algoritma lainnya [8]. Beberapa algoritma tersebut memang tidak ada dalam rekomendasi CCSDS, tetapi dengan tidak terlalu tingginya kompleksitas algoritma yang dibutuhkan, maka beberapa algoritma tersebut dapat dijadikan alternatif pada satelit mikro dengan kemampuan komputasi terbatas.

Pada dasarnya, algoritma enkripsi AES akan mentransformasi 128 bit data masukan menjadi 128 bit data keluaran berdasarkan aturan transformasi tertentu dan sebuah kata kunci, di mana kata kunci tersebut dapat berjumlah 128 bit, 192 bit atau 256 bit. Semakin besar kata kunci yang digunakan maka akan semakin tinggi tingkat keamanan data yang dihasilkan, tetapi membutuhkan pengolahan yang lebih lama. Dalam algoritma AES, aturan transformasi yang digunakan terdiri dari beberapa tahapan yang bersifat iteratif (berulang), Diana masing-masing tahapan terdiri dari empat operasi dasar, yaitu operasi substitusi, operasi transposisi, operasi perkalian dalam *Finite Field* (Galois), serta operasi penjumlahan kata kunci [9][10]. Dalam penelitian ini akan digunakan kata kunci 128 bit, sehingga algoritma AES yang digunakan akan melalui 11 tahapan, di mana tahap pertama hanya berisi operasi kata kunci, sedangkan tahap terakhir tidak memiliki operasi perkalian. Dalam sistem satelit, algoritma enkripsi umumnya diimplementasikan menggunakan perangkat keras FPGA.

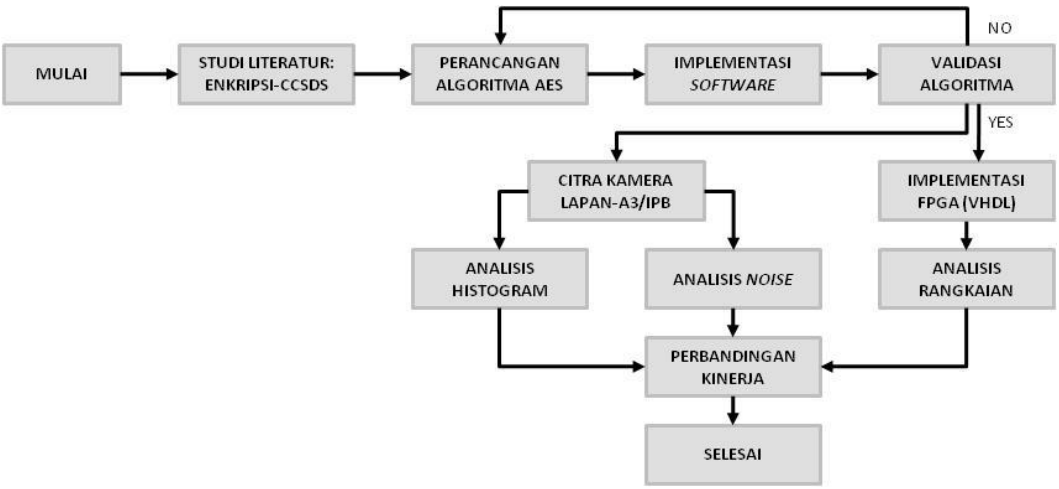
Implementasi algoritma AES pada sistem satelit perlu memperhatikan beberapa batasan yang ada, seperti kemampuan sistem PCDH dan PDHS satelit. Terdapat beberapa mode operasi algoritma AES yang memiliki karakteristik berbeda-beda terkait kekuatan keamanan data yang dihasilkan, resistansi terhadap adanya *noise* selama proses penyimpanan transmisi, serta kompleksitas implementasi pada perangkat keras FPGA. Beberapa mode operasi algoritma AES tersebut yaitu *electronic codebook* (ECB), *chiper block chaining* (CBC), *propagating* CBC (PCBC), *chiper feedback* (CFB), *output feedback* (OFB) dan *counter* (CTR) [9][10]. CCSDS merekomendasikan mode operasi CTR sebagai mode standar yang sebaiknya digunakan, tetapi tetap memperbolehkan penggunaan mode operasi lain bergantung pada keadaan dan keterbatasan yang ada [1].

Penelitian ini akan membahas mengenai langkah awal pengembangan sistem enkripsi data satelit, khususnya sebagai persiapan pengembangan dan implementasi enkripsi data citra muatan yang akan diterapkan pada PDHS satelit LAPAN-A4 yang akan datang. Sebelum melakukan perancangan dan implementasi perangkat keras menggunakan FPGA sebagai bagian dari PDHS satelit, serangkaian analisis kinerja terkait algoritma enkripsi terutama algoritma AES yang direkomendasikan CCSDS akan dibahas. Penelitian ini bertujuan untuk membandingkan kinerja untuk beberapa mode operasi algoritma AES, yaitu mode EBC, mode CBC dan mode *counter*, terkait dalam kekuatan keamanan data, resistansi terhadap *noise* dan kecepatan pengolahan data menggunakan FPGA. Hasil penelitian ini diharapkan dapat membantu proses pemilihan skema konfigurasi, perancangan dan implementasi sistem enkripsi data pada PDHS satelit LAPAN-A4.

2. METODOLOGI

Secara garis besar, penelitian dapat dibagi dalam tiga tahap, yaitu tahap studi literatur, simulasi perangkat lunak MATLAB dan implementasi perangkat keras FPGA. Dalam studi literatur,dibahas terkait rekomendasi CCSDS yaitu algoritma AES beserta beberapa mode operasinya. Kemudian pada tahap simulasi, akan dirancang dan disimulasikan algoritma AES dalam beberapa jenis mode operasi tersebut dengan menggunakan citra satelit kamera multispektral LAPAN-A3/IPB, agar analisis yang

dilakukan dapat mendekati keadaan sebenarnya. Tahap terakhir adalah implementasi algoritma AES pada perangkat keras FPGA Altera Cyclone-IVE EP4CE22F17C6, yang bertujuan untuk menunjukkan perbandingan kompleksitas rangkaian yang dibutuhkan masing-masing mode operasi. Gambar 2 berikut menunjukkan diagram alir tahapan yang dilakukan pada penelitian ini.



Gambar 2. Diagram alir penelitian yang dilakukan

Berikut ini akan diberikan penjelasan yang lebih dalam terkait algoritma AES dan beberapa mode operasi yang akan digunakan pada penelitian ini berdasarkan rekomendasi CCSDS. Algoritma AES dan mode operasi tersebut akan dijadikan dasar dalam pengembangan perangkat lunak dan perangkat keras dalam penelitian ini.

2.1. Algoritma *Advanced Encryption Standard* (AES)

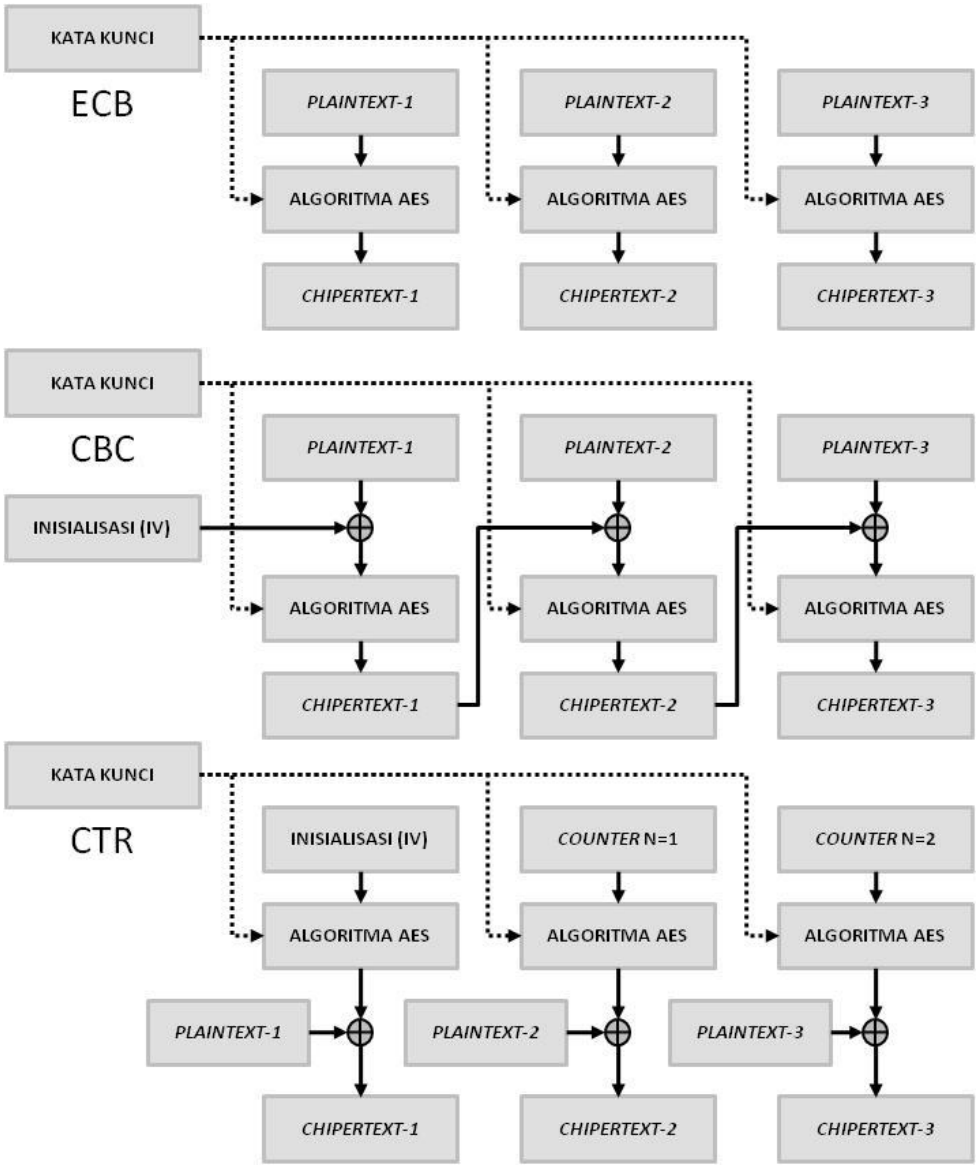
Seperti yang telah dijelaskan sebelumnya, algoritma AES terdiri dari beberapa tahapan di mana dalam tiap tahapan tersebut terdapat empat proses utama. Proses pertama yaitu proses substitusi, merupakan proses transformasi sebuah *byte* data masukan menjadi *byte* lain berdasarkan sejumlah operasi nonlinear dalam *Finite Field*. Walaupun proses substitusi dapat diimplementasikan dengan menggunakan kombinasi gerbang logika pada FPGA, tetapi pada umumnya operasi ini direalisasikan dengan menggunakan *Look-up Table* (LUT) berukuran 256 byte, baik dalam implementasi perangkat lunak maupun perangkat keras. LUT berukuran 256 *byte* tersebut umum dikenal sebagai S-box [9]. Karakteristik transformasi operasi substitusi yang bersifat nonlinear ini menjadi dasar kekuatan utama algoritma AES untuk menghasilkan data yang bersifat acak. Proses kedua yaitu proses transposisi atau proses permutasi, merupakan proses transformasi seluruh 16 *byte* data hasil keluaran proses substitusi menjadi 16 *byte* data baru dengan nilai yang sama tetapi dengan posisi yang berbeda. Proses ini sangat sederhana dan dapat direalisasikan dalam perangkat lunak dan perangkat keras secara efisien, yaitu dengan menggunakan rangkaian *shift-register*.

Sementara itu, proses ketiga yaitu proses perkalian dalam *Finite Field* (Galois) merupakan proses transformasi yang akan merubah 16 *byte* data keluaran hasil proses transposisi menjadi 16 *byte* data baru berdasarkan persamaan perkalian matrik Galois dengan polinomial $x^8+x^4+x^3+x^1+1$. Walaupun secara matematis operasi perkalian ini sangat kompleks, tetapi operasi ini dapat direalisasikan dengan menggunakan beberapa persamaan gerbang logika XOR secara sederhana. Proses terakhir yaitu proses penjumlahan kata kunci merupakan operasi penjumlahan modulo dua antara 16 *byte* data keluaran proses perkalian Galois dengan 16 *byte* kata kunci pada tahapan tersebut, yang dalam implementasinya direalisasikan menggunakan operasi XOR. Kata kunci yang digunakan untuk setiap tahap memiliki nilai yang berbeda, yang dapat diturunkan secara sistematis dari kata kunci 128 bit awal melalui proses *key-expansion* [9]. Secara umum, untuk sebuah kata kunci 128 bit maka dapat diturunkan kata kunci sebanyak 11x128=1408 *byte* yang akan digunakan untuk masing-masing tahapan.

2.2. Mode Operasi AES

Pada dasarnya sebuah algoritma enkripsi akan menghasilkan *N-byte* data keluaran (*chipertext*) berdasarkan *N-byte* data masukan (*plaintext*) dan *M-byte* kata kunci (*keyword*). Terlepas dari berbagai algoritma enkripsi yang digunakan, apakah algoritma AES atau algoritma lainnya, terdapat beberapa

mode operasi yang dapat digunakan untuk meningkatkan keamanan data atau untuk menyederhanakan implementasi perangkat keras algoritma enkripsi tersebut. Berdasarkan konfigurasi data masukan dan data keluaran yang dihasilkan, mode operasi algoritma enkripsi dapat dibedakan menjadi beberapa jenis, diantaranya yaitu mode *electronic codebook* (ECB), mode *chiper block chaining* (CBC), dan mode *counter* (CTR). Gambar 3 berikut menjelaskan ketiga konfigurasi mode operasi tersebut, untuk proses enkripsi data (sisi pengirim data).



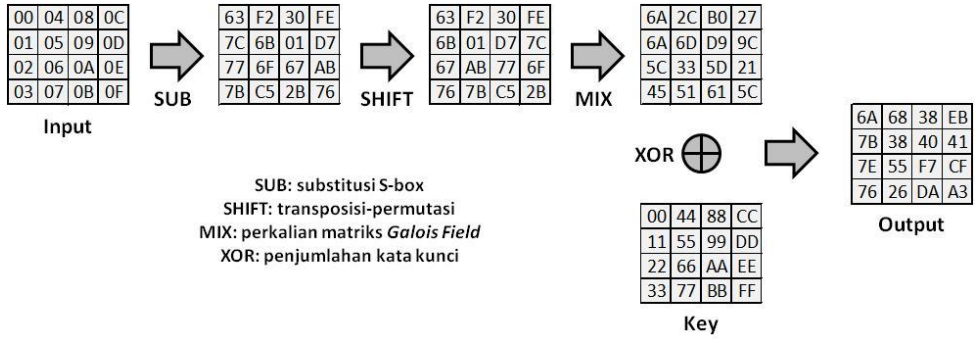
Gambar 3. Konfigurasi mode operasi ECB, CBC dan CTR [9]

Ketiga mode tersebut memiliki kelebihan dan kekurangan masing-masing dalam hal kekuatan keamanan data, sensitivitas terhadap adanya gangguan data (*noise*), maupun fleksibilitas operasi dan implementasi rangkaiannya [9]. CCSDS telah merekomendasikan penggunaan mode *counter* (CTR), tetapi tetap memperbolehkan penggunaan mode lainnya disesuaikan dengan kebutuhan aplikasi dan kemampuan sistem pengolah data *on-board* yang dimiliki satelit [1].

3. HASIL DAN PEMBAHASAN

Algoritma AES berhasil diimplementasikan menggunakan perangkat lunak MATLAB dan bahasa pemrograman VHDL pada perangkat keras FPGA. Gambar 4 menunjukkan hasil validasi algoritma AES pada perangkat lunak MATLAB. Implementasi algoritma pada perangkat lunak dilakukan untuk

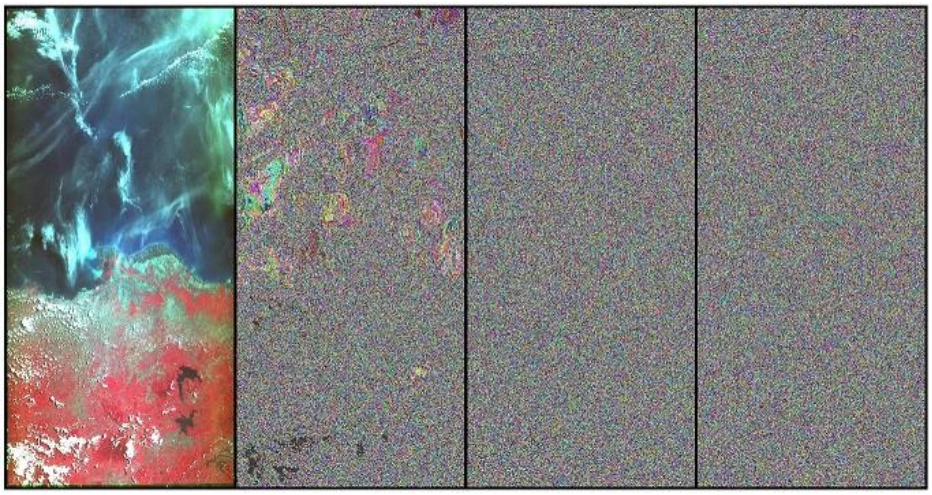
mengenkripsi data citra kamera multispektral satelit LAPAN-A3/IPB menggunakan beberapa mode operasi. Tingkat kinerja keamanan data untuk masing-masing mode operasi tersebut akan ditentukan dengan pendekatan histogram citra, sedangkan tingkat sensitivitas terhadap *noise* ditentukan dengan cara menambahkan data *noise* acak pada citra sebelum proses dekripsi. Sementara itu, implementasi algoritma AES pada FPGA dilakukan untuk mengetahui perbandingan kompleksitas rangkaian dan lamanya waktu pemrosesan yang dibutuhkan masing-masing mode operasi tersebut.



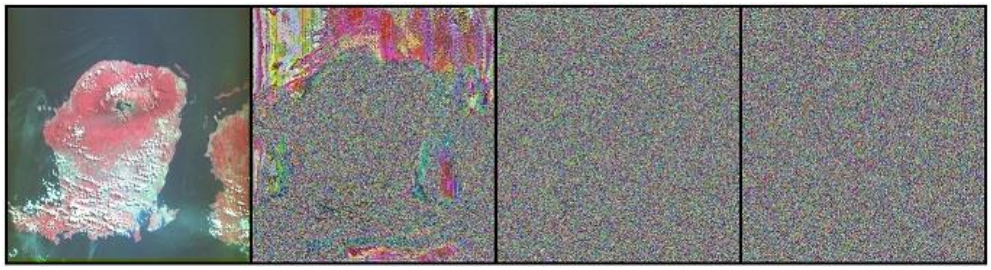
Gambar 4. Validasi algoritma AES pada perangkat lunak MATLAB untuk satu tahapan

3.1.Simulasi Algoritma AES pada Citra Satelit LAPAN-A3/IPB

Citra yang digunakan dalam simulasi ini adalah citra kamera multispektral empat kanal satelit LAPAN-A3/IPB dengan kanal warna NRG (inframerah dekat-merah-hijau). Citra kamera ini memiliki resolusi spasial 15 meter dengan lebar sapuan sekitar 120 km dan resolusi radiometrik 16-bit. Gambar 5 menunjukkan hasil enkripsi algoritma AES untuk citra wilayah DKI Jakarta dan sekitarnya, dengan menggunakan mode operasi ECB, CBC dan CTR (*counter*). Sementara itu, Gambar 6 menunjukkan hasil enkripsi untuk citra wilayah Lombok dan sekitarnya. Untuk menyederhanakan simulasi yang dilakukan, digunakan citra 8-bit yang telah dikontraskan.



Gambar 5. Hasil enkripsi algoritma AES pada citra kamera multispektral satelit LAPAN-A3/IPB wilayah DKI Jakarta, (a) Citra awal, (b) Mode ECB, (c) Mode CBC, (d) Mode CTR

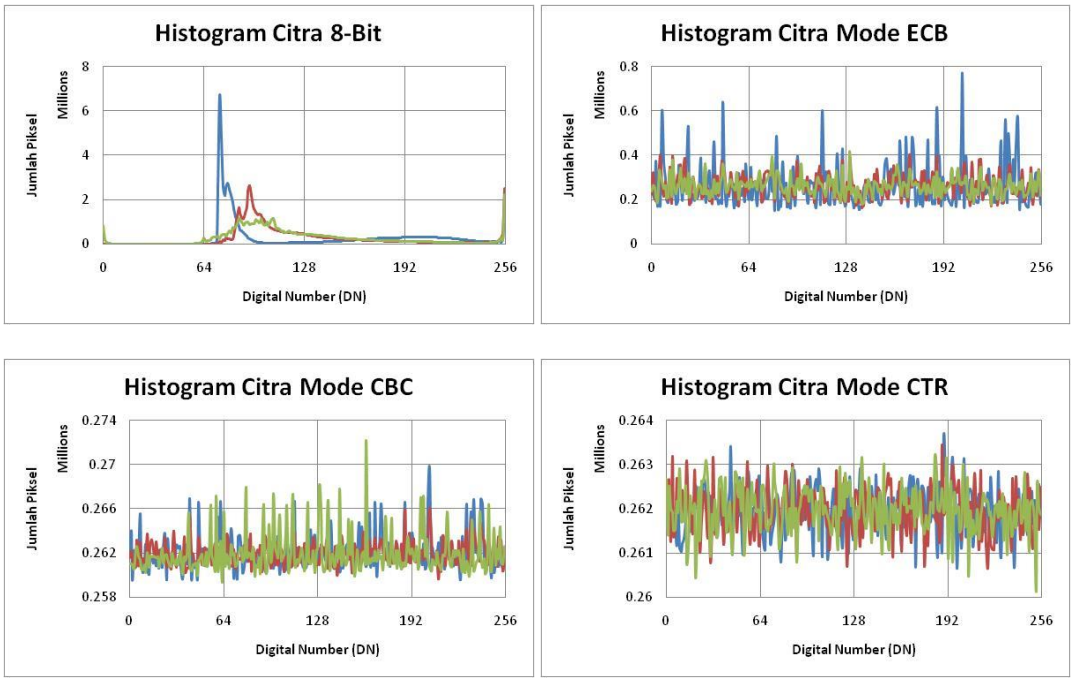


Gambar 6. Hasil enkripsi algoritma AES pada citra kamera multispektral satelit LAPAN-A3/IPB wilayah Lombok, (a) Citra awal, (b) Mode ECB, (c) Mode CBC, (d) Mode CTR

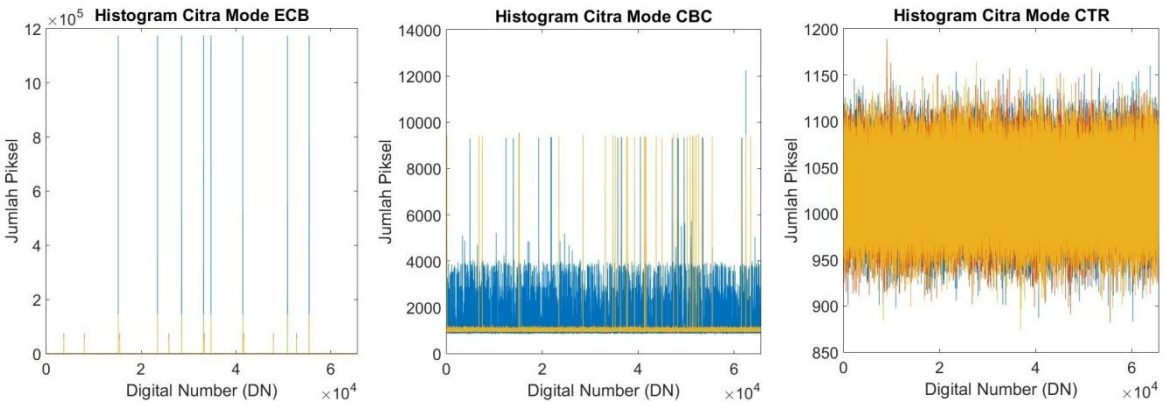
Secara visual, tampak jelas bahwa citra hasil enkripsi dalam mode EBC (kedua dari kiri) memiliki kualitas paling rendah dibandingkan mode CBC (ketiga dari kiri) dan mode CTR (paling kanan). Hal ini dapat dilihat dari kedua hasil simulasi tersebut, di mana citra hasil enkripsi dalam mode ECB belum sepenuhnya bersifat acak dan masih menunjukkan pola seperti citra aslinya, seperti masih terlihatnya sebagian garis pantai pada pulau Lombok pada Gambar 6. Sementara itu, hasil enkripsi dalam mode CBC dan CTR menghasilkan citra dengan tingkat keacakan yang cukup tinggi, sehingga kedua mode ini dapat dikatakan memiliki tingkat keamanan data yang sangat baik. Semakin acak suatu data hasil enkripsi maka semakin sulit bagi pihak lain untuk mengembalikan data tersebut menjadi data aslinya, baik menggunakan teknik *brute-force attack* maupun teknik *dictionary* (kamus data).

3.2. Analisis Keamanan Data Menggunakan Pendekatan Histogram

Untuk dapat lebih menggambarkan tingkat kinerja keamanan data untuk masing-masing mode operasi, metode pendekatan histogram merupakan metode yang umum digunakan untuk menunjukkan kualitas sebuah algoritma enkripsi secara kuantitatif. Secara umum, semakin konvergen histogram citra hasil enkripsi menuju nilai tertentu, maka semakin tinggi tingkat keamanan data tersebut. Gambar 7 berikut menunjukkan histogram citra untuk hasil simulasi pada Gambar 6, sedangkan Gambar 8 menunjukkan histogram untuk citra 16-bit sebelum dikontraskan.



Gambar 7. Histogram citra asli 8-bit dan hasil enkripsi mode ECB, CBC, dan CTR



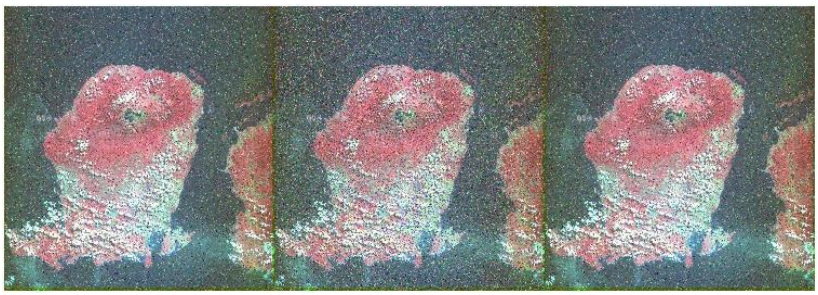
Gambar 8. Perbandingan histogram citra hasil enkripsi citra 16-bit

Dari kedua histogram tersebut, baik untuk citra 8-bit maupun 16-bit, tampak bahwa mode operasi counter (CTR) menghasilkan histogram citra yang paling konvergen, dengan nilai standar deviasi

terendah sebesar 521 piksel untuk citra 8-bit, dibandingkan dengan mode CBC yang memiliki standar deviasi sebesar 1467 piksel dan mode ECB sebesar 64918 piksel. Hasil ini dipertegas pada citra 16-bit, di mana mode CTR memiliki standar deviasi 32 piksel, mode CBC 213 piksel dan mode ECB 5161 piksel. Berdasarkan analisis kualitatif menggunakan citra hasil enkripsi pada Gambar 5 dan 6 serta analisis kuantitatif menggunakan pendekatan histogram tersebut, maka dapat dikatakan bahwa algoritma AES dalam mode operasi *counter* memiliki tingkat keamanan data yang terbaik.

3.3. Analisis Sensitivitas Terhadap *Noise*

Setelah menganalisis tingkat kinerja utama dari sebuah algoritma enkripsi berupa keamanan data, selanjutnya dianalisis beberapa tingkat kinerja lain yang dapat digunakan sebagai pertimbangan dalam pemilihan mode operasi yang optimal untuk sistem dan aplikasi tertentu. Gambar 9 menunjukkan hasil dekripsi citra pada Gambar 6, dengan menambahkan *noise* yang bersifat acak. Tampak bahwa citra hasil dekripsi dalam mode CBC (kedua dari kiri) memiliki kualitas citra yang paling rendah, karena dalam mode CBC, sebuah blok data yang terkena gangguan pada saat proses transmisi atau saat proses penyimpanan akan menyebabkan satu blok data setelahnya mengalami gangguan juga pada saat proses dekripsi data citra tersebut. Secara kuantitatif, mode operasi CBC akan menghasilkan *noise* dua kali lebih besar pada saat proses dekripsi dibandingkan kedua mode operasi lainnya tersebut.



Gambar 9. Hasil dekripsi algoritma AES untuk citra wilayah Lombok dengan adanya gangguan *noise* acak, (a) Mode ECB, (b) Mode CBC, (c) Mode CTR

3.4. Implementasi Algoritma AES pada FPGA: Analisis Kompleksitas Rangkaian

Algoritma AES dapat diimplementasikan dalam FPGA dengan sangat efisien karena sebagian besar operasi yang dibutuhkan adalah operasi XOR, termasuk operasi perkalian dalam *Galois Field*. Walaupun demikian pada penelitian ini, terdapat beberapa operasi yang menggunakan LUT seperti proses substitusi S-box dan proses ekspansi kata kunci. Beberapa elemen memori juga dibutuhkan untuk menyimpan data transisi yang dihasilkan setiap tahapan algoritma. Tabel 1 berikut menunjukkan gerbang logika primitif yang dibutuhkan untuk merealisasikan algoritma enkripsi AES pada FPGA dengan menggunakan bahasa pemrograman VHDL, dan perbandingannya terhadap hasil perancangan modul PDHS lain beserta modul IP-Core komersial yang disediakan oleh FPGA Altera.

Tabel 1. Kebutuhan gerbang logika primitif untuk modul algoritma enkripsi AES

Elemen Rangkaian	Hasil Perancangan			Altera IP-Core		
	AES	RS[3]	PDHS	RSenc	RSdec	Vitterbi
Gerbang Logika	4062	422	31882	301	689	1052
Register	401	273	22080	203	462	654
Memori Bit	0	0	0	0	640	5696

Tampak bahwa rangkaian yang dibutuhkan untuk mengimplementasikan algoritma AES jauh lebih kompleks dibandingkan dengan algoritma *encoding* Reed-Solomon [3]. Hal ini disebabkan karena implementasi algoritma AES ini belum mempertimbangkan optimasi dan efisiensi penggunaan gerbang logika dan register untuk merealisasikan beberapa operasi seperti operasi substitusi S-box, operasi perkalian *Galois Field* dan proses ekspansi kata kunci. Perancangan yang dilakukan baru ditekankan pada keakuratan data yang dihasilkan proses enkripsi, di mana modul enkripsi AES yang dirancang telah dapat menghasilkan keluaran sesuai dengan simulasi yang dilakukan pada perangkat lunak. Terkait kompleksitas rangkaian, secara umum modul enkripsi data memang membutuhkan implementasi FPGA yang lebih kompleks dibandingkan dengan modul *encoding* dan modul kompresi data pada sistem *Payload Data Handling* (PDHS).

Sementara itu, Tabel 2 menunjukkan perbandingan kebutuhan rangkaian untuk beberapa mode operasi enkripsi yaitu mode ECB, mode CBC dan mode CTR. Karena dalam mode operasi CBC, hasil *chipertetxt* blok data sebelumnya mempengaruhi proses enkripsi data selanjutnya maka algoritma AES dalam mode CBC ini harus diimplementasikan secara serial, yang berarti seluruh data masukan akan diproses oleh sebuah modul algoritma enkripsi AES. Sementara itu, karena dalam mode operasi ECB dan mode CTR setiap proses enkripsi sebuah blok data terpisah satu sama lainnya, maka pengolahan dapat dilakukan secara paralel di mana beberapa modul enkripsi AES mengenkripsi beberapa blok data secara bersamaan. Dengan demikian pengolahan paralel dalam mode ECB dan mode *counter* dapat mempercepat proses pengolahan data tetapi membutuhkan implementasi rangkaian FPGA yang lebih kompleks. Dengan demikian, tingkat keparalelan mode ECB/CTR dibatasi oleh kemampuan perangkat keras FPGA yang digunakan. Pada Tabel 2 tersebut, algoritma enkripsi AES diimplementasikan menggunakan FPGA Altera tipe Cyclone-IVE EP4CE22F17C6dengan kapasitas gerbang logika dan register sebanyak 22320 unit. Dalam contoh kasus tersebut, mode operasi ECB dan mode CTR dapat mengolah data lima kali lebih cepat dibandingkan mode CBC, dengan asumsi bahwa data yang diolah, memori tempat penyimpanan atau instrumen *transmitter* dapat diakses secara paralel.

Tabel 2. Perbandingan kompleksitas implementasi antar mode operasi algoritma AES

Elemen Rangkaian	Mode CBC (Serial)	Mode ECB/CTR (Paralel 5-blok)
Gerbang Logika	4062 (18%)	20310 (90%)
Register	401 (2%)	2005 (10%)
Memori Bit	0	0

4. KESIMPULAN

Salah satu pengolahan data yang dilakukan sistem PCDH dan PDHS satelit adalah proses enkripsi data yang berfungsi untuk mentransformasikan data telemetri atau data muatan menjadi data yang tidak terstruktur sehingga tidak disalahgunakan oleh pihak lain. CCSDS merekomendasikan algoritma *Advanced Encryption Standard* (AES) untuk keperluan enkripsi data satelit tersebut. Penelitian ini telah berhasil mengimplementasikan algoritma AES dalam perangkat lunak MATLAB dan perangkat keras FPGA yang telah divalidasi keakuratan hasilnya. Berdasarkan beberapa hasil simulasi yang telah dilakukan, algoritma AES yang diimplementasikan dalam mode operasi *counter* memiliki tingkat kinerja terbaik, terutama terkait keamanan data yang dihasilkan dan fleksibilitas pengolahan yang dapat dilakukan secara paralel. Mode operasi CBC juga dapat menghasilkan tingkat keamanan data yang cukup baik tetapi lebih rentan terhadap adanya gangguan *noise* dan pengolahannya hanya dapat dilakukan secara serial. Sementara itu mode operasi ECB dapat digunakan sebagai alternatif untuk sistem pengolah data dengan kemampuan rendah, karena mode operasi ini dapat dilakukan dengan cepat dan tidak terlalu rentan terhadap gangguan transmisi, walaupun tingkat keamanan data yang dihasilkan lebih rendah dibandingkan mode operasi lainnya. Dengan demikian, berdasarkan beberapa hasil penelitian tersebut maka algoritma enkripsi data AES sebaiknya diimplementasikan dalam mode operasi *counter*. Hasil penelitian ini diharapkan dapat membantu proses pemilihan skema enkripsi data satelit yang akan digunakan pada PDHS satelit LAPAN-A4

UCAPAN TERIMA KASIH

Penulis mengucapkan rasa terima kasih kami kepada Bapak Abdul Karim sebagai Plt. Kepala Pusat Teknologi Satelit (Pusteksat-LAPAN) dan Bapak Wahyudi Hasbi sebagai *Chief Engineer* satelit LAPAN-A3/IPB atas arahan dan bimbingannya sehingga karya tulis ilmiah ini dapat terselesaikan dengan baik.

PERNYATAAN PENULIS

Penulis dengan ini menyatakan bahwa seluruh isi menjadi tanggung jawab penulis.

DAFTAR PUSTAKA

[1] The Consultative Committee for Space Data Systems. *CCSDS Cryptographic Algorithms, Blue Book, CCSDS 352.0-B-1*, 2012.

[2] W. Rosa, D.E. Amin, dan E.N. Nasser. "Design and Implementation of *Payload* Data Handling Based on Field Programmable Gate Array," *ICARES*, hal. 48-54, Yogyakarta, 2014.

[3] P.R. Hakim, et.al. "Implementasi Encoder Reed-Solomon pada FPGA Berbasis CCSDS," *Jurnal Teknologi Dirgantara*, vol. 12 no. 2, hal. 116-127, 2014.

[4] P.R. Hakim, dan R. Permala. "Compression Algorithm Performance Analysis of LAPAN-A3 Satellite Image using Fast-Fourier Transform," *ISAST*, Bali, 2015.

[5] P.R. Hakim, dan R. Permala. "Analysis of LAPAN-IPB Image Lossless Compression using Differential Pulse Code Modulation and Huffman Coding," *Earth and Environmental Science*, vol. 54, 2017.

[6] L. Zhang, X. Liao, dan X. Wang. "An Image Encryption Approach Based on Chaotic Maps," *Chaos, Solitons and Fractals*, vol. 24, hal. 759-765, 2005.

[7] L. Krikor, S. Baba, T. Arif, dan Z. Shaaban. "Image Encryption using DCT and Stream Chiper," *European Journal of Scientific Research*, vol. 32 no. 1, hal. 47-57, 2009.

[8] K.D. Patel, dan S. Belani. "Image Encryption using Different Techniques: A Review," *International Journal of Emerging Technology and Advanced Engineering*, vol. 1, 2011.

[9] B.A. Forouzan.*Cryptography and Network Security*, McGraw-Hill, New York, 2008.

[10] H. Delfs, dan H. Knebl.*Introduction to Cryptography: Principles and Applications*, Second Edition, Springer, Berlin, 2007.

DAFTAR RIWAYAT HIDUP PENULIS

DATA UMUM

Nama Lengkap	: Patria Rachman Hakim, ST, MT.
Tempat & Tgl. Lahir	: Jakarta, 30 April 1982
Jenis Kelamin	: Pria
Instansi Pekerjaan	: LAPAN
NIP. / NIM.	: 19820430 201012 1 002

DATA PENDIDIKAN

SLTA	: SMUN 8 Jakarta	Tahun: 1997-2000
STRATA 1 (S.1)	: Teknik Elektro ITB	Tahun: 2000-2004
STRATA 2 (S.2)	: Teknik Elektro ITB	Tahun: 2005-2008

ALAMAT

Alamat Kantor / Instansi	: Jl. Cagak Satelit Km 04, Rancabungur, Bogor
Telp.	: 0251-8343333
Email	: patriarachmanhakim@yahoo.com