ANALISIS ALGORITMA CATMAP UNTUK KEAMANAN DATA CITRA SATELIT-NANO PADA *LOW EARTH ORBIT*

Halim Futu Wijaya[1)], Budi Syihabudin[2)], Efa Maydhona Saputra[3)]

[1,2,3)]School of Electrical Engineering, Telkom University
Jl Telekomunikasi, Bandung, Jawa Barat 40257
Email : halimfutuwijaya@gmail.com[1)], budisyihab@telkomuniversity.ac.id[2)], maydhona@telkomuniversity.ac.id[3)]

Abstrak

Satelit-nano merupakan jenis satelit yang memiliki masa dibawah 10 kg, dan berada dalam orbit LEO (Low Earth Orbit). Saat ini riset tentang satelit-nano menjadi suatu hal yang menarik bagi mahasiswa maupun dosen karena memiliki ciri low cost, dan sistem yang tidak rumit. Salah satu misi yang sering dikembangkan saat ini adalah penginderaan jarak jauh. Salah satu blok penting dalamn misi ini adalah masalah pengenkripsian data gambar. Pengenkripsian disini bertujuan untuk memastikan data gambar yang ditransmisikan oleh satelit hanya dapat digunakan oleh pihak-pihak yang memiliki wewenang saja. Dalam paper ini akan disimulasikan enkripsi dekripsi data gambar menggunakan algoritma Cat Map untuk aplikasi satelit-nano. Algoritma Cat Map sendiri memiliki kelebihan dalam hal kecepatan enkripsi data gambar, karena satelit-nano sendiri hanya memiliki waktu yang sangat singkat ketika melewati stasiun bumi. Hal yang dikaji lainnya adalah masalah ketahanan dari algoritma Cat Map sendiri terhadap serangan hacker ,salah satunya dengan menggunakan brute force attack. Hasil dari simulasi algoritma Cat Map untuk berbagai ukuran citra dari penelitian ini membuktikan bahwa metode Cat Map memiliki waktu enkripsi yang cukup cepat, dengan waktu tracking stasiun bumi selama 11 menit yang didapat dari simulai menggunakan software orbit STK 10 , algoritma ini dapat mengenkripsi data gambar paling lama 5 menit untuk ukuran citra sebesar 1600x1200 pixel, dengan 10 kali iterasi. Ukuran citra tersebut termasuk besar untuk aplikasi satelit nano pada umumnya, kecepatan akan meningkat jika resolusi makin rendah dari ukuran pixel diatas. Ketahanan algoritma Cat Map terhadap brute force attack untuk ukuran image sebesar 1600x1200 pixel adalah 18,201 tahun dan untuk resolusi yang lebih rendah waktu peretasan jauh lebih cepat.

Kata kunci: *Enkripsi-Dekripsi, Satelit-nano, Cat Map*

1. Pendahuluan

Indonesia merupakan negara yang memiliki wilayah darat dan perairan yang sangat luas, wilayahnya terbentang dari barat ke timur sejauh 6400 km, oleh karena itu untuk dapat mengawasi seluruh wilayahnya akan sangat sulit jika dilakukan hanya menggunakan pesawat atau kapal saja. Satelit merupakan alternatif yang efektif dan efisien untuk pengawasan wilayah, di negara maju teknologi satelit sudah dijadikan kelengkapan dalam pertahanan. Dari ketinggian minimum satelit yaitu pada orbit LEO dibutuhkan 1-2 satelit yang saling terhubung untuk dapat mencakup seluruh wilayah Indonesia, satelit-nano bisa menjadi salah satu alternatif jika ingin mengembangkan sistem pengawasan yang low cost dan dapat dikembangkan oleh kaum akademisi.

Salah satu misi satelit-nano yang dibahas pada paper ini adalah penginderaan jarak jauh. Pada misi tersebut selalu ada data berupa gambar atau video yang akan diambil oleh satelit untuk di transmisikan di stasiun bumi agar dapat diamati, data citra merupakan data yang sangat berharga, bisa saja data tersebut memperlihatkan kekayaan alam, basis markas militer, maupun jumlah armada tempur di suatu negara, hal tersebut dapat disalahgunakan oleh pihak-pihak yang tak bertanggung jawab.

Pengamanan data citra menjadi sangatlah penting untuk misi penginderaan jarak jauh. Saat ini banyak algoritma-algoritma yang sangat baik dari sisi keamanan, permasalahannya tidak semua algoritma sesuai diimplementasikan untuk mengenkripsi data citra. Data citra memiliki kapasitas volume yang lebih besar dari pada text, jika diterapkan algoritma-algoritma konvesional seperti DES, dan RSA maka akan membutuhkan waktu komputasi yang lama saat enkripsi [1]. Satelit-nano hanya memiliki waktu yang singkat untuk mentransmisikan data diatas stasiun bumi. Selain alasan volume, karakteristik data teks dan data citra pun berbeda, jika teks hanya memiliki hubungan dengan tetangga sebelumnya dan setelahnya saja, pixel dalam citra memiliki hubungan dengan pixel lain yang lain di delapan arah mata angin . Salah satu algoritma citra yang dipilih untuk diteliti dalam paper ini adalah algoritma arnold's Cat Map. Algoritma Cat Map termasuk dalam algoritma enkripsi citra digital, jenisnya adalah algoritma selektif, dimana ia hanya akan mengenkripsi sebagian elemen dari citra tapi efeknya membuat seluruh citra terenkripsi, hal tersebut dapat mengurangi waktu komputasi [1], dan otomatis dapat mempercepat pengenkripsian data citra.

Dalam paper ini akan dilakukan percobaan pada beberapa ukuran citra yang berbeda dengan menggunakan

algoritma Cat Map, dan diamati performansi kecepatan enkripsi dan dekripsinya. Lalu akan dianalisis juga kekuatan enkripsinya menggunakan brute force attack.

2. Analisis Orbit

Satelit-nano berada pada orbit LEO , Tabel 1 adalah hasil simulasi menggunakan software simulasi orbit satelit yaitu STK 10.

Tabel 1. *Simulasi orbit dalam software STK 10*

Properties	Value
Jenis Orbit	Polar Sun-syncronous
Apogee/Perigee Radius	700 Km
Inklinasi	98.2°
Periode Orbit	5926.38 s
Jumlah Melintasi stasiun bumi	2 kali
Perioda saat melintasi target	8-11 menit

Tujuan simulasi ini adalah menemukan rentang waktu tracking stasiun bumi terhadap satelit-nano. Diasumsikan stasiun bumi berada di wilayah Indonesia , orbit satelit-nano yaitu polar dengan ketinggian 700 km, dan inklinasi 98,2°. Dalam simulasi, orbit dirancang berbentuk circular yang menyebabkan radius apogee dan perigee sama.dari hasil simulasi dalam satu hari satelit-nano melintas diatas stasiun bumi sebanyak dua kali dengan periode setiap melintas sekitar 11 menit. Waktu ini lah yang dijadikan parameter untuk waktu enkripsi.

3. Algoritma Cat Map

Konsep dari enkripsi algoritma Cat Map sendiri adalah mentransformasikan posisi seluruh pixel pada suatu matriks gambar menggunakan persamaan matematis sebagai berikut [2]:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \ mod\ N \quad \text{..... (1)}$$

Dimana :

1. (x_n , y_n) adalah posisi pixel dalam N × N citra dan $x_n , y_n \in \{0, 1, 2, 3, \dots, N-1\}$
2. (x_{n+1} , y_{n+1}) adalah hasil dari transformasi posisi berdasarkan metode Cat Map.
3. a dan b adalah dua parameter kontrol dan keduanya integer positif.

Satu iterasi dalam algoritma Cat Map dihitung setelah seluruh pixel selesai ditransformasi dengan persamaan diatas. Algoritma Cat Map senantiasa merubah ukuran pixel gambar dengan ukuran M x N menjadi N x N dengan menambahkan matriks kosong atau menambahkan potongan citra asli yang di replikasi ke sisi yang lebih pendek. Ada tiga buah kunci utama dalam algoritma Cat Map yaitu jumlah iterasi, a ,dan b.

4. Analisis Algoritma Cat Map

Misi penginderaan jarak jauh membutuhkan payload berupa kamera. Dalam penelitian ini digunakan kamera LSY-201 yang beresolusi 2 MP. Kamera LSY-201 memiliki spesifikasi sebagai berikut [3] :

1. 1600*1200/1280*960/1024*768/800*600/VGA/ QVGA/160*120 resolution
2. Support capture JPEG from serial port
3. Default baud rate of serial port is 38400
4. DC 3.3V or 5V power supply
5. Size 32mm X 32mm
6. Current consumption: 80-100mA
7. Rasio kompresi 36:1

Pada paper ini variasi resolusi kamera diambil dari datasheet output LSY-201 dapat dilihat pada Tabel 2 untuk variasi resolusinya dan waktu enkripsi berdasarkan jumlah iterasi dengan algoritma Cat Map.

Tabel 2. *Tabel Waktu Enkripsi Menggunakan Algoritma Cat Map*

Resolusi	Ukuran Citra (KB)	Waktu Enkripsi berdasar jumlah iterasi (detik)				
		2	4	6	8	10
160x160	7,02	0,62	1,14	1,59	2,14	2,5
640x640	85,1	8,2	15,99	24,50	33,85	40,09
800x800	141	13,99	25,93	37,23	51,47	65,16
1024x1024	169	22,07	43,81	61,50	83,18	103,20
1280x1280	322	33,07	64,56	94,99	131,54	162,09
1600x1600	171	56,28	101,50	150,82	207,67	254,99

Resolusi kamera 2 MP dipilih dengan pertimbangan volume gambar, semakin besar volumenya maka akan memperlama waktu pengiriman data dan waktu enkripsi, maka dari itu untuk aplikasi satelit nano pada umumnya hanya membawa kamera beresolusi VGA sampai 2 MP.

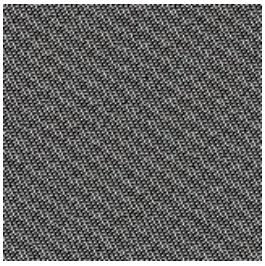
Gambar 1. *Kamera LSY-201[3]*

Proses pengujian algoritma Cat Map dilakukan dalam beberapa iterasi, maksimal 10 iterasi dengan mempertimbangkan periode satelit di atas stasiun bumi selama 8-11 menit. Dengan asumsi waktu kirim citra selama 2 menit untuk ukuran citra terbesar 1600x1200

piksel. Proses pengiriman juga mempertimbangkan ACK dan NACK sehingga diestimasi terjadi dua kali pengiriman data dan satu kali waktu tunggu dari stasiun bumi. Dengan skema tersebut, proses enkripsi pada satelit dialokasikan 2-5 menit sehingga jumlah iterasi yang diuji merujuk pada waktu proses tersebut. Waktu proses enkrip dapat dilihat pada Tabel 2. Untuk jumlah iterasi lainnya (2,4,6,8) ditampilkan untuk memperlihatkan performansi enkripsi algoritma Cat Map jika disimulasikan kurang dari 10 iterasi. Tidak ada aturan khusus untuk menampilkan hanya kelipatan dua saja, hal tersebut dilakukan hanya untuk mempercepat menemukan jumlah iterasi maksimum untuk enkripsi pada skema diatas.

Hasil enkripsi gambar pada algoritma Cat Map untuk setiap iterasi berbeda-beda, berikut akan ditampilkan beberapa contoh hasil simulasi pengenkripsian citra dengan resolusi 160x120 pixel, dan jumlah iterasi 10 :

(a)



(b)

(c)

Gambar 2. *(a) citra awal, (b)citra hasil enkripsi, (c) citra hasil dekripsi*

Dalam paper ini tidak memperhatikan aspek transmisi, diasumsikan kondisi transmisi ideal dan bitrate komunikasi 9600bps, waktu transmisi (t) didapatkan dengan pesamaan [**4**] :

$$t = \frac{jumlah\ bit\ data}{bitrate\ transmisi} \quad \text{.....(2)}$$

Untuk contoh data citra diatas adalah data yang telah melalui proses kompresi, sehingga untuk volume data terbesar yaitu 322 KB, resolusi 1280x1280 piksel, dan jumlah bit per pixel 8 bit memerlukan waktu transmisi 322x1000x8/9600 = 4,47 menit dengan asumsi waktu tracking satelit nano oleh stasiun bumi 11 menit [5] dan waktu enkripsi terlama untuk ukuran tersebut dengan 10 kali iterasi adalah 162,09 detik atau sekitar 2,7015 menit, maka dengan menggunakan algoritma Cat Map masih dapat mengirimkan 2 buah citra. Pada kamera LSY-201 rasio kompresi citra adalah 36:1, jika ingin mendapatkan jumlah bit data dari suatu citra 1280x960 piksel keluaran LSY-201, maka jumlah bit data = 1280x1280x3x8/36=1092266 bit, dikalikan 3 karena data RGB, data tersebut setara dengan 136,53 KB, lalu jumlah bit dibagi bitrate 9600 menghasilkan 14,2 detik untuk waktu transmisi, jika di iterasi 10 kali waktu enkripsi akan tetap sama dengan gambar yang memiliki ukuran volume lebih besar maupun lebih kecil asalkan ukuran piksel citranya sama, karena konsep dari Cat Map sendiri adalah mentransformasikan matriks gambar per piksel bukan per bit. Tentu saja dengan ukuran pixel atau dengan jumlah iterasi lebih kecil, akan didapatkan waktu enkripsi lebih cepat dan dapat mentransmisikan data citra lebih dari sebelumnya. Waktu enkripsi algoritma Cat Map untuk ukuran citra terbesar keluaran kamera LSY-201 sendiri dengan ukuran 1600x1200 piksel adalah 254,99 detik, waktu transmisinya jika dihitung secara ideal adalah (171x1000x8)/9600= 142,5 detik, dari hasil tersebut algoritma ini masih mampu untuk memenuhi kebutuhan dari satelit-nano sendiri.

Selain aspek kecepatan enkripsi hal lain yang diteliti dalam paper ini adalah ketahanann agoritma Cat Map terhadap serangan brute force attack. Brute force attack adalah upaya peretasan data dengan cara mencoba- coba semua kemungkinan kunci yang ada. Berikut persamaan untuk menemukan waktu yang dibutuhkan brute force attack untuk memecahkan algoritma Cat Map[5] :

$$t_{br} = \frac{0{,}5\ x\ waktu\ dekripsi\ x\ N^2}{365\ x\ 24\ x\ 3600} \quad \text{.....(3)}$$

Pada Tabel 3 akan diperlihatkan hasil simulasi untuk waktu dekripsi data, lalu pada Tabel 4 akan diperlihatkan kekuatan algoritma Cat Map jika diserang dengan brute force attack. Pada dasarnya brute force attack akan mencoba seluruh kemungkinan kunci untuk membongkar suatu algoritma, dalam penelitian ini akan diuji seberapa kuat algoritma Cat Map dalam menghadapi serangan tersebut. Pertama akan disimulasikan waktu dekripsi citra dengan jumlah iterasi yang telah dirancang, Setelah waktu dekripsi didapatkan, dapat dihitung ketahanan algoritma Cat Map sendiri dari serangan brute force attack dengan memasukan waktu dekripsi kedalam persamaan (3) diatas. Pengujian kekuatan algoritma penting untuk dilakukan agar dapat mengevaluasi hasil kinerja sistem pengamanan data citra.

Tabel 3. *Tabel kecepatan dekripsi algoritma Cat Map*

Resolusi	Ukuran Citra (KB)	Waktu Dekripsi berdasar jumlah iterasi (detik)				
		2	4	6	8	10
160x160	7,02	0,5	1,07	1,53	2,05	2,53
640x640	85,1	7,7	15,42	23	30,93	38,57
800x800	141	12,36	23,99	36,47	47,6	60,48
1024x1024	169	18,47	39,11	55,86	74,89	91,21
1280x1280	322	56,92	57,33	94,59	114,17	142,77
1600x1600	171	52,02	92,31	138,31	358,06	448,43

Untuk mendapatkan waktu enkripsi maupun dekripsi menggunakan counter pada software simulasi, yang mulai menghitung dari awal proses enkripsi sampai akhir proses, sehingga didapatkan waktu enkripsi. Begitu pula dengan proses dekripsi, counter mulai menghitung dari awal proses dekripsi hingga akhir proses. Dari Tabel 3 dapat dilihat bahwa waktu dekripsi tidak jauh berbeda dengan waktu enkripsi, hal itu terjadi akibat algoritma Cat Map sendiri tergolong algoritma simetris yang memiliki kunci yang sama dengan enkripsi, oleh karena itu untuk pengujian jumlah iterasi dekripsi disamakan dengan jumlah iterasi enkripsi. Waktu dekripsi tidak ada batasan karena dilakukan setelah data diterima di stasiun bumi, data tersebut digunakan untuk menghitung kekuatan algoritma jika diuji dengan brute force attack. Seluruh simulasi waktu baik enkripsi dan dekripsi tergantung dari kecepatan komputasi komputer yang digunakan. Dalam paper ini spesifikasi komputer akan ditampilkan dalam Tabel 5.

Tabel 4. *Tabel ketahanan algoritma catmap terhadap serangan brute force attack*

Resolusi	Ukuran Citra (KB)	Ketahanan algoritma (dalam tahun)				
		2	4	6	8	10
160x160	7,02	0,00015	0,0002	0,0003	0,0005	0,000657
640x640	85,1	0,008	0,016	0,023	0,032	0,04
800x800	141	0,051	0,099	0,152	0,198	0,251
1024x1024	169	0,307	0,65	0,928	1,245	1,516
1280x1280	322	1,478	1,48	2,457	2,966	3,709
1600x1600	171	2,11	3,74	5,614	14,53	18,201

Tabel 5. *Spesifikasi komputer*

Ram	Vga	Hardisk	OS	Prosesor
8192 MB	1792 MB	500 GB	win 8.1	2.50 GHz

Pada Tabel 4 dapat diamati bahwa kekuatan keamanan algoritma Cat Map dari hasil simulasi tidak sebaik algoritma-algoritma konvensional pada umumnya, jika dilakukan brute force attack menggunakan teknologi super komputer mungkin akan dapat terbongkar dengan mudah, hal ini tidak terlepas dari sifat dari algoritma Cat Map sendiri yaitu jika terus-terusan dilakukan iterasi maka pada periode iterasi tertentu gambar akan kembali seperti citra awal, jika periodenya adalah T maka algoritma Cat Map akan kembali ke citra awal dalam rentang $T < 3N$ [2].

5. Kesimpulan

Di dalam paper telah dipaparkan hasil simulasi Algoritma Cat Map. Dari hasil simulasi Resolusi citralah yang mempengaruhi kecepatan enkripsi bukan volume data citra, volume data citra berpengaruh terhadap waktu transmisi data citra. Untuk ukuran resolusi tertinggi keluaran LSY-201 yaitu 1600x1200 piksel algoritma ini dapat menghasilkan waktu enkripsi 254,99 detik dan waktu transmisi 142,5 detik, jika waktu tracking stasiun bumi terhadap satelit adalah 11 menit maka algoritma ini memungkinkan untuk diimplementasikan dalam aplikasi satelit-nano. Hasil enkripsi citra dari Cat Map pun baik, hasilnya dapat dilihat dari gambar yang acak dan tidak dapat dikenali lagi.

Ketahanan algoritma Cat Map terhadap serangan brute force attack dari hasil simulasi didapatkan untuk waktu terlama meretas citra dengan ukuran resolusi terbesar adalah 18,201 tahun, waktu peretasan semakin cepat jika ukuran resolusi atau jumlah iterasi dikurangi. Jika dilihat dari hasil simulasi tingkat keamanan algoritma Cat Map kurang baik. Sebaiknya untuk menutupi kekurangan tersebut algoritma Cat Map harus digabung atau ditambahkan algoritma lain,untuk selanjutnya sebaiknya efek transmisi juga diperhitungkan agar hasil yang diperoleh lebih nyata.

Daftar Pustaka

[1] Munir.Rinaldi, *"Algoritma Enkripsi Citra Digital Berbasis Chaos Dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map Dan Logistic Map," in Prosiding Seminar Nasional Pendidikan Informatika 2012,*pp.108, September 22,2012.

[2] Struss,K. (2009): *A Chaotic Image Encryption*, Mathematic Senior Seminar, 4901, University Of Minnesota, Morris

[3] www.linksprite.com diakses pada 29 November 2014

[4] Gulzar Kashf, Camera Design for Pico and Nano Satellite Applications, 2009

[5] Hafsahtiarni. Rifa.2009, *Desain dan Implementasi Metode Gabungan Cat Map dan Baker Map Untuk Peningkatan Sekuritas Pada Enkripsi Citra Digital,*Tugas Akhir, Jurusan Teknik Telekomunikasi ITTelkom, Bandung

ISSN : 2302-3805

Biodata Penulis

Halim Futu Wijaya, Jurusan Teknik Telekomunikasi Universitas Telkom Bandung.Saat ini menjadi mahasiswa di Universitas Telkom Bandung.

Budi Syihabuddin ,memperoleh gelar Sarjana Teknik (S.T), Jurusan Teknik Telekomunikasi ITTelkom Bandung, lulus tahun 2008. Memperoleh gelar Magister Teknik (M.T) Program Pasca Sarjana Magister Teknik Telekomunikasi ITTelkom Bandung lulus tahun 2012. Saat ini menjadi Dosen di Universitas Telkom Bandung.

Efa Maydhona Saputra, memperoleh gelar Sarjana Teknik (S.T), Jurusan Teknik Telekomunikasi ITTelkom Bandung, lulus tahun 2010. Memperoleh gelar Magister Teknik (M.T) Program Pasca Sarjana Magister Teknik Telekomunikasi ITTelkom Bandung lulus tahun 2013. Saat ini menjadi Dosen di Universitas Telkom Bandung.

ISSN : 2302-3805