An Implementation of Catmap-Rijndael (AES) Algorithm For Image Security (Case Study on A Software For Making Students Card At Universitas Jenderal Soedirman)

Bangun Wijayanto dan Retantyo Wardoyo

Abstract— The function of image encryption is to transform known have that meaning to images that cannot be read or irregular images in order to security. Storing the image data in local computer system will bring some risks on the image security.

The aim of this research is to construct an image encryption system based on Catmap-Rijndael algorithm. The system is implemented on a software form making students card at Universitas Jenderal Soedirman. The result shows that the combination of Catmap-Rijndael algorithm on bitmap image 200x200 pixel by using 3 times repetition of the Catmap algorithm (with parameter a=1 and b=1) can overcome the problem of textured of the object that caused by base colour on the image and uniform histogram of the encrypted image in short time process.

Keywords— *Rijndael, AES, Catmap, image security, students card.*

I. PENGANTAR

Kartu tanda mahasiswa adalah kartu yang digunakan sebagai identitas seorang mahasiswa, didalamnya termuat identitas seorang mahasiswa. Kartu tanda mahasiwa (KTM) digunakan didalam berbagai kepentingan akademis mahasiswa seperti peminjaman buku perpustakaan, penggunaan laboratorium, fasilitas internet dan lain sebagainya.

Pembuatan kartu tanda mahasiswa Universitas Jenderal Soedirman saat ini ditangani oleh sub bagian registrasi. Kartu tanda mahasiswa dibuat pada saat pertama kali mahasiswa melakukan registrasi, dimulai dengan proses entri data mahasiswa kemudian dilakukan pemotretan untuk mendapatkan citra dari mahasiswa tersebut, selanjutnya data citra tersebut disimpan untuk kemudian dicetak pada kartu tanda mahasiswa. Penyimpanan data citra pada komputer lokal dan bukan pada komputer server memungkinkan terjadinya celah keamanan terhadap penyalahgunaan data citra maupun penggantian terhadap citra seorang mahasiswa.

Kegunaan dari pengacakan citra adalah untuk mengubah citra yang mempunyai arti ke bentuk citra yang tidak dapat dibaca atau citra yang tidak teratur dalam rangka meningkatkan keamanan [3]. Pada algoritma Catmap citra dipermutasi dan dipetakan berdasarkan suatu perhitungan tertentu. Algoritma Catmap hanya merubah posisi pixel dari citra asli, akan tetapi nilai dari pixel tidak diubah. Citra asli dapat didapatkan kembali melalui metode *exhaustion*, sehingga pengubahan nilai pixel dengan menggunakan algoritma lainnya diperlukan untuk meningkatkan keamanan citra.

Algoritma Rijndael didesain oleh oleh Vincent Rijmen dan John Daemen asal Belgia. Algoritma ini mendukung berbagai kombinasi dari data dan kunci dari 128, 192 dan 256 bit. Biasanya Rijndael (AES) menggunakan panjang data 128 bit yang dibagi menjadi empat blok operasi dasar. Rijndael (AES) adalah algoritma blok tercepat terutama bagi implementasi pada perangkat keras. Algoritma Rijndael (AES) digunakan pada beberapa aplikasi yang membutuhkan kecepatan dalam pemrosesan seperti pada *smart card*, telepon seluler dan enkripsi gambar video. Mode operasi yang digunakan pada proses enkripsi dan dekripsi citra algoritma Rijndael adalah *electronic codebook* (ECB). Meskipun *cipher block chaining* (CBC) lebih aman akan tetapi CBC membutuhkan waktu proses yang lebih lama [1].

Berdasarkan latar belakang diatas, maka yang menjadi pembahasan utama dari penelitian ini adalah bagaimana mengimplementasi

B. Wijayanto,Computer Science Study Program, Gadjah Mada University, Yogyakarta, Indonesia 55281.

R. Wardoyo, Computer Science Study Program, Gadjah Mada University, Yogyakarta, Indonesia 55281.

algoritma Rijndael yang dikombinasikan dengan algoritma Catmap untuk keamanan citra pada perangkat lunak pembuatan kartu tanda mahasiswa Universitas Jenderal Soedirman, sehingga data citra hanya dapat dibaca oleh perangkat lunak yang ada dalam waktu yang relatif cepat.

II. LANDASAN TEORI

II.I ALGORITMA CATMAP

Catmap diciptakan oleh Arnold, diberi nama demikian dikarenakan algoritma tersebut dibuat dengan percobaan sebuah citra wajah kucing. Ekspresi dari Arnold cat map ditunjukan pada persamaan berikut :

$$\begin{vmatrix} X_{n+1} \\ Y_{n+1} \end{vmatrix} = \begin{vmatrix} 1 & a \\ b & ab+1 \end{vmatrix} \begin{vmatrix} X_n \\ Y_n \end{vmatrix} \; Mod\; N$$

X_n dan Y_n adalah posisi dari pixel pada citra dengan ukuran N x N dan X_{n+1}, Y_{n+1} adalah posisi setelah ditransformasi. A dan B adalah parameter sistem dan harus bernilai bilangan bulat positif dengan nilai determinannya adalah 1.

Catmap adalah mapping satu ke satu, tiap titik dari matriks akan ditransformasikan ke titik lain secara unik. Kenyataannya Catmap adalah termasuk chaotic map. Posisi citra dapat diacak melalui iterasi atau pengulangan dari algoritma Catmap [3].

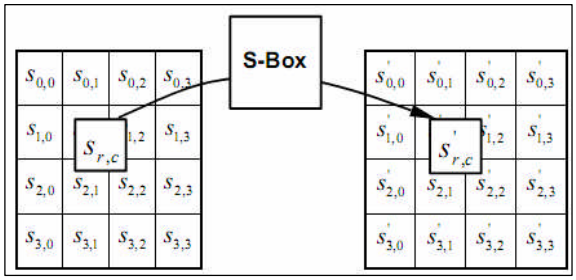
II.II ALGORITMA RIJNDAEL (AES)

Algoritma Rijndael didesain oleh oleh Vincent Rijmen dan John Daemen asal Belgia. Algoritma ini mendukung berbagai kombinasi dari data dan kunci dari 128, 192 dan 256 bit. Biasanya Rijndael(AES) menggunakan panjang data 128 bit yang dibagi menjadi empat blok operasi dasar.

Pada algoritma Rijndael(AES) panjang dari blok input, blok output adalah 128 bit. AES beroperasi pada *array* byte 4×4, yang disebut sebagai state. Adapun 4 operasi dasar pada algortima Rijndael (AES) adalah AddRoundkey, SubBytes, ShiftRow, MixColoumn.

II.II.I SUB BYTES

SubBytes adalah subtitusi byte non-linear yang beroperasi secara independen terhadap setiap byte yang terdapat pada *state* menggunakan table subtitusi (S-box) ditunjukan pada Gambar 1.



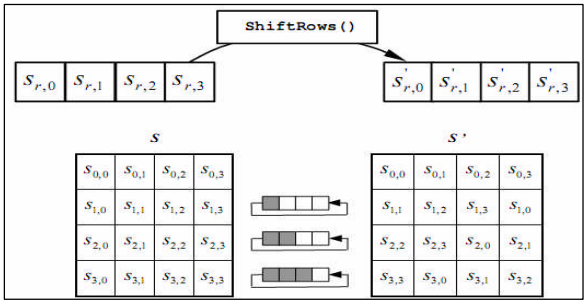
Gambar 1 Pemetaan SubBytes ke S-box (NIST, 2001)

II.II.II SHIFT ROWS

Pada ShiftRows, bytes pada tiga baris terakhir dilakukan perputaran, yaitu dengan menggeser bytes. Baris pertama, r = 0, tidak digeser. Proses transformasi ShiftRows dapat dijelaskan sebagai berikut:

$$S_{r,c}=S_{r,(c+shift(r,Nb))mod\ Nb} \text{ untuk } 0<r<4 \text{ dan } 0\leq c<Nb$$

dimana pergeseran Shift(r,Nb) bergantung pada baris r, ini mengakibatkan pergeseran bytes ke posisi yang lebih "rendah" pada suatu baris. Gambar 2 menggambarkan proses dari transformasi ShiftRows.



Gambar 2 Transformasi ShiftRows (NIST, 2001)

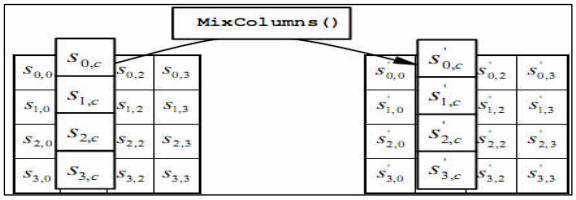
II.II.III MIX COLUMNS

MixColumns beroperasi pada *state* kolom per kolom, memperlakukan tiap kolom sebagai empat persamaan polynomial. Kolom tersebut dianggap sebagai polynomial GF(2^8)

dan perkalian modulo $x^4 + 1$ dengan polynomial tetap a(x), diberikan sebagai :

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

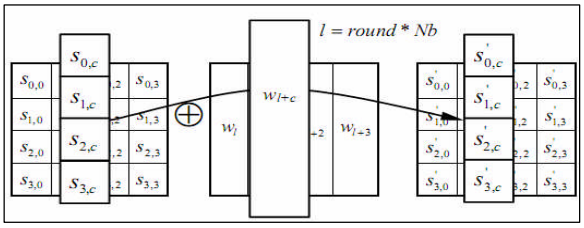
Proses Mix Columns ditunjukkan pada Gambar 3.



Gambar 3 Transformasi MixColumns (NIST, 2001)

II.II.IV AddRoundKey

Setiap byte dari array akan di lakukan operasi XOR terhadap pasangan elemen array subkey setiap ronde. Transformasi AddRoundKey sangat sederhana dan memberikan efek pada tiap bit dari state. Transformasi dari AddRoundKey ditunjukkan pada Gambar 4.



Gambar 4 Transformasi AddRoundKey (NIST, 2001)

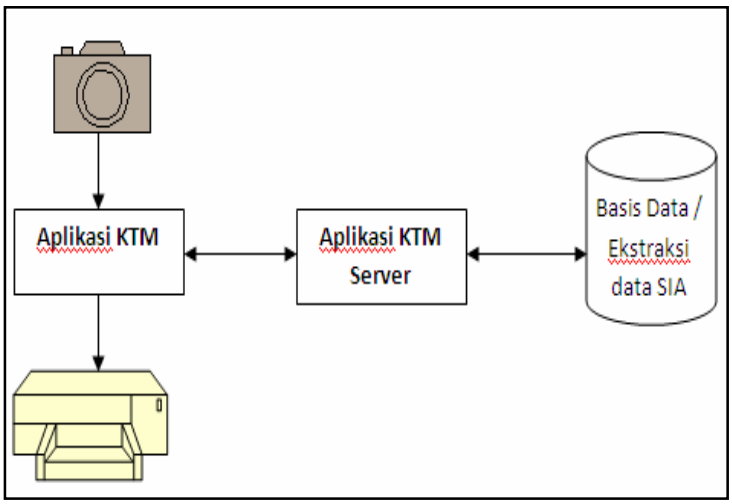
III. Analisa Dan Rancangan Sistem

Aplikasi kartu tanda mahasiswa adalah aplikasi yang digunakan untuk mengolah data citra (*image*) yang berasal dari peralatan webcam yang terhubung dengan komputer untuk kemudian data gambar diproses menggunakan algoritma Catmap dan Rijndael (AES). Pencetakan kartu tanda mahasiswa dilakukan berdasarkan informasi yang berasal dari ekstraksi sistem informasi akademik.

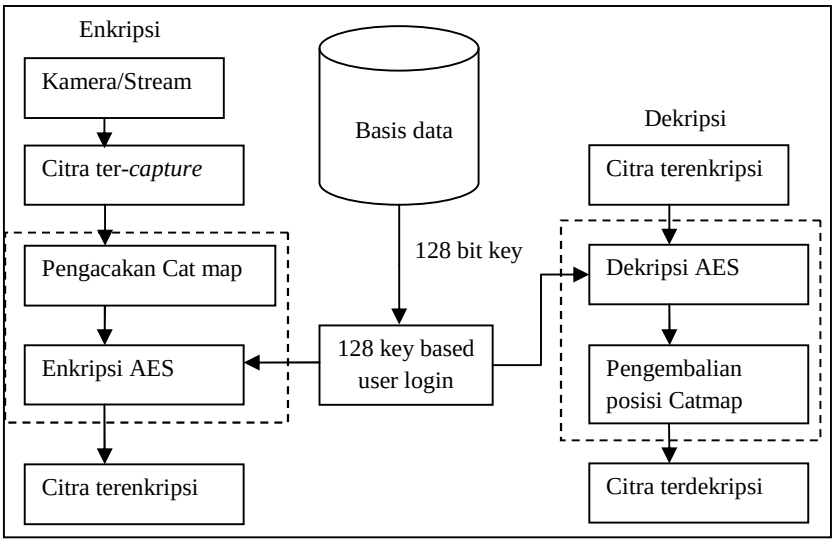
Variabel-variabel yang digunakan meliputi citra (*image*), kunci user (*user key*) sedangkan output yang dihasilkan adalah citra (*image*) yang telah terenkripsi dan aman untuk disimpan pada komputer lokal. Sebagai pembatas program dirancang agar dapat berjalan pada sistem operasi Windows.

III.I Arsitektur Sistem

Aplikasi KTM akan mengakses kamera dan melakukan pengambilan data informasi mahasiswa dengan menggunakan metode *multitier client-server* dari basis data yang berasal dari hasil ekstraksi system informasi akademik. Skema arsitektur sistem yang akan dibuat ditunjukkan pada Gambar 5.



Gambar 5 Arsitektur sistem



Gambar 5 Skema keamanan citra

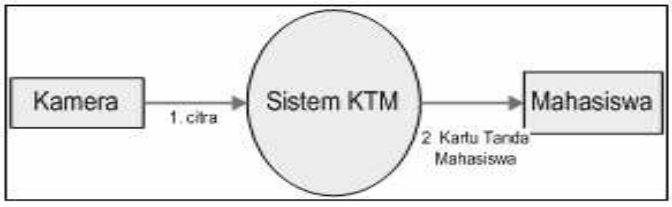
Skema pengamanan citra ditunjukkan pada Gambar 6. Pengamanan citra dilakukan dengan melakukan enkripsi terhadap data citra yang didapatkan dari hasil pengambilan gambar (*capture*) kamera, kemudian dilakukan pengacakan letak pixel gambar dengan menggunakan algoritma Catmap, pixel yang sudah teracak tersebut selanjutnya akan dienkripsi nilai warnanya menggunakan Rijndael (AES) dengan menggunakan kunci 128 bit yang berasal dari basisdata. Citra yang telah terenkripsi dapat digunakan kembali setelah melalui proses dekripsi yang merupakan kebalikan dari proses enkripsi.

III.II DIAGRAM ALIRAN DATA

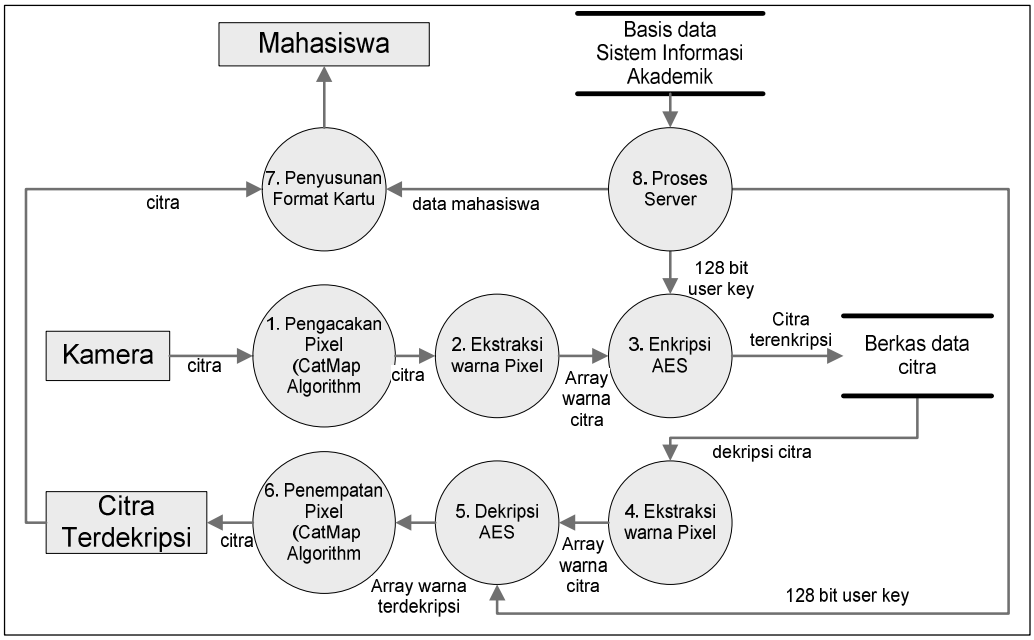
Diagram alir data adalah diagram yang digunakan untuk menggambarkan jalannya data melalui satu atau beberapa proses yang telah ditentukan.

Gambar 7 memperlihatkan diagram aliran data (*Data Flow Diagram*/DFD) level 0 dari sistem yang akan dibuat. Data citra yang diambil oleh kamera masuk ke dalam sistem untuk kemudian dilakukan proses enkripsi maupun dekripsi, luaran dari proses tersebut adalah hasil cetakan kartu mahasiswa yang diperoleh oleh seorang mahasiswa.

Gambar 8 memperlihatkan diagram alir data level 1, data citra yang dihasilkan oleh kamera akan dilakukan pengacakan posisi pixel dengan algoritma Catmap seperti dijelaskan pada bagian 2.1, kemudian dilakukan ekstraksi warna pixel untuk mendapatkan komposisi warna RGB (*Red Green Blue*) dari tiap pixel yang ada. Mengacu pada arsitektur sistem Gambar 6, data warna per-pixel tersebut dienkripsi dengan algoritma Rijndael (AES) dengan menggunakan 128 bit kunci yang didapatkan dari hasil basisdata sistem informasi akademik yang sudah ada sebelumnya.

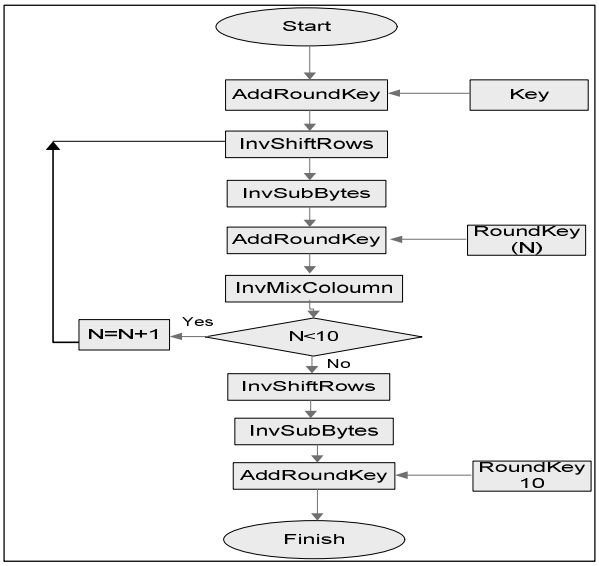


Gambar 6 Diagram alir data level 0



Gambar 7 Diagram alir data level 1

Gambar 9 memperlihatkan diagram alir (*flowchart*) dari proses enkripsi Rijndael.



Gambar 8 Diagram alir enkripsi Rijndael

Proses enkripsi dimulai dari N=0 sampai dengan N=10. Pada N=1 sampai dengan N=9 terjadi proses perulangan (*looping*) terhadap proses SubBytes, ShiftRows, MixColoumns, AddRoundkey yang melibatkan kunci pada tiap ronde (RoundKey) seperti telah dipaparkan pada bagian II.II.

Proses pencetakan kartu dimulai dengan mengambil citra mahasiswa yang telah terenkripsi kemudian dilakukan ekstraksi warna pixel untuk mendapatkan komposisi warna RGB (*Red Green Blue*), data warna per-pixel tersebut didekripsi dengan algoritma Rijndael (AES). Data citra yang telah didekripsi lalu disusun urutan pixel-nya dengan algoritma Catmap. Citra tersebut diproses dengan data mahasiswa untuk kemudian diformat dan dicetak sebagai kartu tanda mahasiswa.

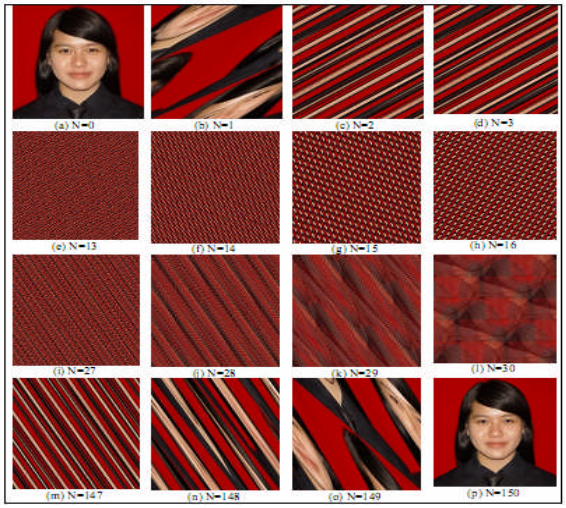
IV. Hasil Penelitian Dan Pembahasan

Dari hasil implementasi dilakukan beberapa pengujian untuk menentukan skema keamanan yang sesuai dengan sistem yang akan dibuat. Pengujian dilakukan pada masing masing algoritma yakni Catmap, Rijndael serta kombinasi Catmap-Rijndael. Berikut adalah hasil penelitian daan pembahasan terhadap pengujian yang telah dilakukan

IV.I Percobaan Algoritma Catmap

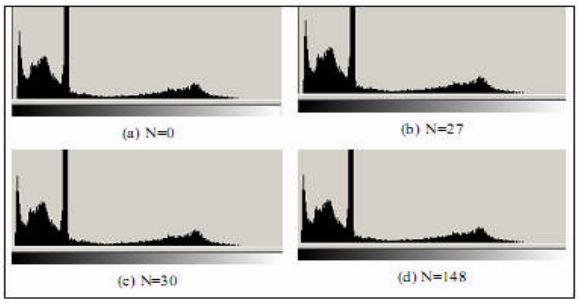
Pengacakan posisi koordinat pixel dilakukan terhadap berkas citra E1A002131.bmp dengan parameter a=1 dan b=1 pada algoritma catmap. Hasil pengujian berkas tersebut diperlihatkan pada Gambar 10 dengan N adalah banyaknya putaran algoritma Catmap yang dilakukan.

Penggunaan algoritma Catmap secara berulang untuk melakukan pengacakan posisi koordinat pixel akan mengembalikan posisi koordinat pixel ke posisi semula, pada berkas citra E1A002131.bmp yang berukuran 200x200 pixel dengan parameter a=1 dan b=1 secara visual bentuk citra kembali setelah 150 kali pengacakan. Dari 150 kali putaran algoritma Catmap didapatkan rerata waktu pengacakan koordinat posisi pixel sebesar 781,1409 mili detik. Secara visual objek dari citra sudah tidak dapat dikenali setelah 3 putaran.



Gambar 9 Pengacakan koordinat pixel E1A002131.bmp a=1 b=1

Pengacakan posisi pixel tanpa melakukan perubahan terhadap nilai atau isi pixel menyebabkan histogram yang terbentuk tidak mengalami perubahan seperti ditunjukkan pada Gambar 11.



Gambar 10 Histogram E1A002131.bmp

IV.II PERCOBAAN ALGORITMA RIJNDAEL

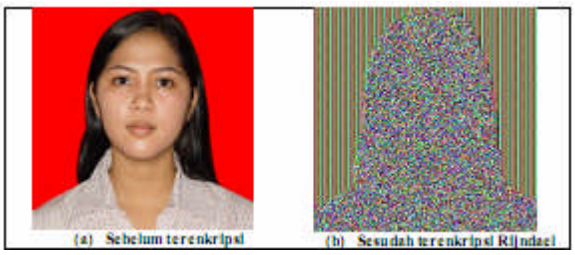
Algoritma Rijndael (AES) diterapkan pada berkas citra E1A002092.bmp dengan menggunakan kunci 16 byte (128 bit):

```
2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
```

Kunci tersebut lalu diekspansi menjadi 176 byte dan didapatkan kunci hasil ekspansi sebagai berikut:

```
2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
a0 fa fe 17 88 54 2c b1 23 a3 39 39 2a 6c 76 05
f2 c2 95 f2 7a 96 b9 43 59 35 80 7a 73 59 f6 7f
3d 80 47 7d 47 16 fe 3e 1e 23 7e 44 6d 7a 88 3b
ef 44 a5 41 a8 52 5b 7f b6 71 25 3b db 0b ad 00
d4 d1 c6 f8 7c 83 9d 87 ca f2 b8 bc 11 f9 15 bc
6d 88 a3 7a 11 0b 3e fd db f9 86 41 ca 00 93 fd
4e 54 f7 0e 5f 5f c9 f3 84 a6 4f b2 4e a6 dc 4f
d2 73 21 b5 8d ba d2 31 2b f5 60 7f 8d 29 2f ac
77 66 f3 19 fa dc 21 28 d1 29 41 57 5c 00 6e d0
14 f9 a8 c9 ee 25 89 e1 3f 0c c8 b6 63 0c a6
```

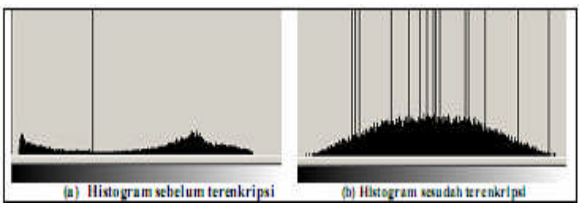
Gambar 12.a dan 12.b memperlihatkan citra sebelum dan sesudah enkripsi.



Gambar 11 Enkripsi Rijndael citra E1A002092.bmp

Pada Gambar 12.b terlihat bahwa citra hasil enkripsi algoritma Rijndael (AES) membentuk pola siluet dari objek citra yang ada, hal ini disebabkan karena warna latar (background) dari objek citra berwarna murni (R, G atau B). Pola atau siluet objek ini biasa terjadi pada enkripsi citra yang merubah nilai pixel saja tanpa melakukan pengubahan koordinat posisi pixel.

Histogram dari citra E1A002092.bmp sebelum dan sesudah pengubahan nilai pixel ditampilkan pada Gambar 13.a dan 13.b.



Gambar 12 Histogram sebelum dan sesudah enkripsi E1A002092.bmp

Gambar 13.b memperlihatkan bahwa bentuk histogram setelah dilakukan pengubahan nilai pixel menggunakan algoritma Rijndael (AES) lebih seragam (*uniform*) dan berbeda dengan histogram dari berkas citra sebelum dilakukan pengubahan nilai pixel (Gambar 13.a). Waktu yang dibutuhkan untuk proses enkripsi adalah 109 ms, sedangkan waktu untuk proses dekripsi 718 ms.

IV.III PERCOBAAN ALGORITMA CATMAP-RIJNDAEL

Catmap-Rijndael adalah skema keamanan citra yang terbentuk dari 2 algoritma yakni Catmap dan Rijndael (AES). Catmap digunakan untuk melakukan pengacakan koordinat posisi pixel sedangkan Rijndael (AES) digunakan untuk mengenkripsi nilai dari pixel. Catmap yang digunakan akan di set parameter a=1 dan b=1. Kunci yang digunakan dalam percobaan adalah kunci 16 byte (128 bit):

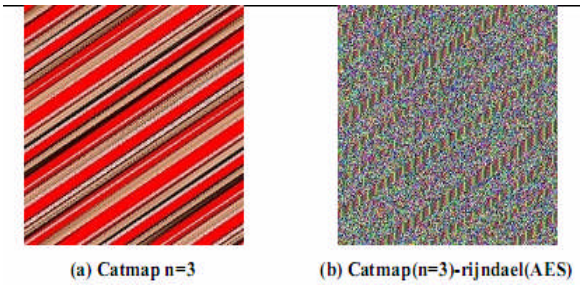
8a 9b 1c 1a 28 ae d2 a6 ab f7 15 99 09 cf 4f 3c

Kunci tersebut lalu diekspansi menjadi 176 byte dan didapatkan kunci hasil ekspansi sebagai berikut:

8a 9b 1c 1a 28 ae d2 a6 ab f7 15 99 09 cf 4f 3c 01 1f f7 1b 29 b1 25 bd 82 46 30 24 8b 89 7f 18 a4 cd 5a 26 8d 7c 7f 9b 0f 3a 4f bf 84 b3 30 a7 cd c9 06 79 40 b5 79 e2 4f 8f 36 5d cb 3c 06 fa 2e a6 2b 66 6e 13 52 84 21 9c 64 d9 ea a0 62 23 de 0c 0d e1 b0 1f 5f 65 91 83 3b bc 7b 23 59 9f d8 c7 d6 c0 68 d8 89 a5 f9 5b b2 19 82 78 eb 86 24 2e 92 d3 4c f6 1b 76 b5 ad a9 6f 37 d5 42 e9 a7 02 8c 49 eb f4 97 3f 5e 59 3e 50 69 8c 7c b9 d8 12 da b0 33 e6 4d 8f 6d bf 73 df 04 33 0f 66 2d 64 e9 42 1e 82 a4 cd 73 3d d7 12 77 0e d8 74

Percobaan akan mengamati tiap konfigurasi Catmap (n)-Rijndael (AES) secara visual, histogram maupun kecepatannya.

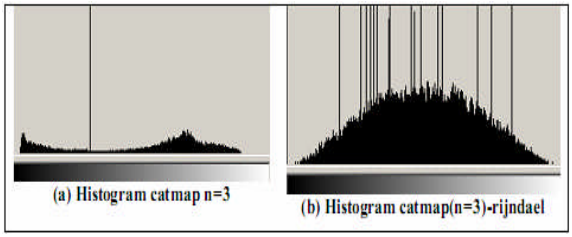
Berkas citra E1A002092.bmp diacak posisi pixelnya sebanyak 3 kali dengan menggunakan algoritma Catmap, 3 kali pengacakan dipilih karena pada pengacakan ke 3 objek pada citra udah tidak dapat dikenali lagi. Gambar 14.a dan 14.b masing-masing memperlihatkan citra yang telah teracak algoritma catmap n=3, serta enkripsi Catmap-Rijndael (AES).



Gambar 13 Citra E1A002092.bmp dengan Catmap(n=3)-Rijndael

Gambar 14.a menunjukan secara visual objek citra tidak dapat dikenali lagi, pada Gambar 14.b terdapat garis-garis yang merupakan representasi dari warna dasar, akan tetapi garis tersebut sudah tidak menunjukkan pola-pola objek citra aslinya seperti pada Gambar 12.b.

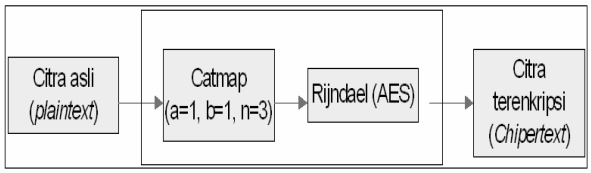
Histogram dari Gambar 14.a dan 14.b diperlihatkan pada Gambar 15.a dan 15.b.



Gambar 14 Histogram enkripsi Catmap(n=3) dan Catmap(n=3)–Rijndael

IV.IV PERANGKAT LUNAK PEMBUATAN KARTU TANDA MAHASISWA

Dari hasil percobaan algoritma Catmap-Rijndael pada bagian 4.3 maka perangkat lunak pembuatan kartu tanda mahasiswa mengimplementasikan skema keamanan citra seperti digambarkan pada Gambar 16.



Gambar 15 Skema keamanan citra yang digunakan

Nilai parameter di set a=1, b=1 serta pengacakan posisi pixel sebanyak 3 kali, hal ini mengacu pada percobaan pada bagian 4.1 dimana pada pengacakan ke 3, objek citra sudah tidak dapat dikenali lagi.

V. KESIMPULAN DAN SARAN

Kombinasi algoritma Catmap-Rijndael (AES) dapat mengatasi terbentuknya pola atau siluet dari objek yang disebabkan karena adanya warna dasar citra yang terjadi pada enkripsi Rijndael dengan mode operasi ECB (*electronic codebook*), serta menyeragamkan bentuk histogram dari citra yang terenkripsi.

Skema keamanan citra yang diterapkan pada perangkat lunak pembuatan kartu tanda mahasiswa universitas Jenderal Soedirman menggunakan algoritma Catmap-Rijndael (AES) dengan menggunakan pengacakan Catmap sebanyak 3 kali serta menset parameter a=1, b=1.

Waktu yang digunakan untuk melakukan enkripsi dengan algoritma Catmap-Rijndael dengan pengacakan posisi pixel sebanyak 3 kali adalah 360 ms, sedangkan waktu dekripsinya adalah 3781 ms.

VI. DAFTAR PUSTAKA

[1] Al-Tamimi, A., 2006, Performance Analysis of Data Encryption Algorithms, *http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html*, diakses tanggal 18/12/2009

[2] Cheranov, A.G., 2007, AES Cipher, *http://cmpe.emu.edu.tr/chefranov*, diakses tanggal 25/12/2009

[3] Liehuang, Z., Wenzhuo, L., Lejian, L., dan Hong, L., 2006, A Novel Image Scrambling Algorithm for Digital Watermarking Based on Chaotic Sequences, *Journal Computer Science and Network Security*, VOL.6 No.8B, 125

[4] Menezes, A.J., Van Oorschot, P.C., dan Vanstone, S.A., 1997, *Handbook of applied cryptography*, CRC Press, Florida

[5] National Institute of Standards and Technology (NIST), 2001, Advanced Encryption Standard (AES), *Federal Information Processing Standards Publication 197*, NIST, Springfield

[6] Yu, X Y., Zhang, J., Ren, H.E., Xu, G.S., dan Luo, X Y., 2006, Chaotic Image Scrambling Algorithm Based on S-DES, *Journal of Physics:International Symposium on Instrumentation Science and Technology*, Series 48, 349–353