Majalah Ilmiah Matematika dan Statistika Volume 18 Nomor 1, 2018, 33 – 42
https://jurnal.unej.ac.id/index.php/MIMS/index ISSN 1411-6669

PENGAMANAN CITRA *GRAYSCALE* MENGGUNAKAN ALGORITMA AES 128 DENGAN KUNCI CITRA *GRAYSCALE*

(*Grayscale Image Security Using the AES 128 Algorithm by Image Key*)

Ahmad Khoirul Umam, Ahmad Kamsyakawuni, Abduh Riski

Jurusan Matematika, Fakultas MIPA, Universitas Jember
Jl. Kalimantan 37 Jember 68121, Indonesia
E-mail: umamkhoirul313@yahoo.com,{kamsyakawuni, riski}.fmipa@unej.ac.id

Abstract. Cryptography is the science of maintaining or securing an information by scrambling or hiding information so that it is difficult to analyze. The algorithm used in this study is the AES 128 algorithm that has been changed using the grayscale image. The AES algorithm is a modern algorithm that replaces the DES algorithm, and is an algorithm that is chosen to secure a data / message because it is efficient and has strong security. In the process, the grayscale image key is divided into 16 blocks of pixels, pixels are operated on each block with XOR operations so that one character will be obtained for each block. From the XOR process of pixels in 16 blocks, 16 characters or 128 bits long will be obtained. The data used in this study are plain images in the form of grayscale images and keys in the form of grayscale images as well. Grayscale (plain image) images will be encrypted with an image key that is also a grayscale image. Initially, the key will be taken from a grayscale image by dividing 16 blocks to get a 128-bit long key, then generating the key with the key generator in the AES algorithm so that it will get 10 sub-keys. Then encryption is done with 10 sub-keys that were obtained using the AES algorithm. The results of the encryption process will produce an encoded image or cipher image that does not contain information from the plain image. The results of this algorithm are fairly safe against attacks because they have varied and sensitive keys.

Keywords: Cryptography, AES, Rijndael Algorithm, Grayscale
MSC 2010: 68U10

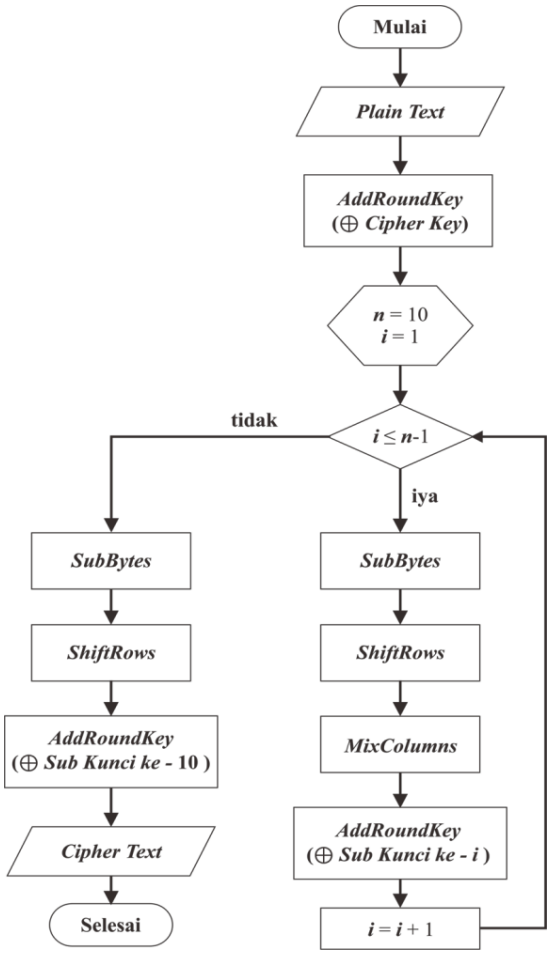
1. Pendahuluan

Perkembangan globalisasi tidak hanya memberikan dampak positif bagi lingkungan manusia, tetapi juga memberikan dampak negatif. Salah satunya yakni penyalahgunaan data privasi milik seseorang oleh pihak yang tidak berwenang. Kriptografi adalah ilmu untuk mengamankan suatu informasi/data. Rijmen dan Daemen [1] mengajukan sebuah proposal standard algoritma kriptografi baru yang dinamakan sebagai Algoritma *Rijndael*, sebagai pengganti algoritma kriptografi lama (*Data Encryption Standard* / DES). Algoritma DES dianggap sudah tidak aman lagi karena dengan perangkat keras

khusus kuncinya mampu ditemukan dalam beberapa hari. Algoritma *Rijndael* merupakan algoritma yang banyak dipilih untuk mengamankan suatu data/pesan karena efisien dan pengamanannya yang kuat. Pada tahun 2001, algoritma yang diajukan oleh Rijmen dan Daemen ini kemudian dipilih oleh *National Institute of Standards and Technologi* (NIST) dengan sebutan *Advanced Encryption Standart* (AES) sebagai pengganti algoritma lama (DES). Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128, 192, dan 256. Fadhillah [2] melakukan penelitian tentang algoritma AES dalam pengamanan citra digital. Penelitian tersebut menggunakan gambar sebagai plain image dan mencoba beberapa model kunci seperti huruf, angka dan symbol.Hasil dari penelitian tersebut yaitu keamanan pengamanan citra dengan algoritma AES bisa lebih optimal jika menggukanan jenis kombinasi dari angka, huruf dan symbol. Tujuan dari penelitian ini adalah memanfaatkan berbagai teknik pengamanan suatu informasi yang sudah dipaparkan. Penulis akan meneliti dan membuat suatu aplikasi untuk mengamankan suatu data berupa citra *graysacle,*dengan kunci citra *grayscale* menggunakan algoritma *AES* dengan panjang kunci 128 bit. Citra tersebut akan dibagi menjadi 16 blok dan di XOR-kan pikselnya pada tiap blok tersebut, sehingga menghasilkan 16 karakter untuk dijadikan kunci pada algoritma AES 128.

Algoritma AES

Algoritma AES merupakan algoritma modern yang bersifat simetri, *cipher block*, dan menggunakan sistem basis hexadesimal dalam proses komputasinya. Ukuran kunci pada algoritma ini sebesar 128 bit, 192 bit, dan 256 bit. Pada Umumnya ukuran kunci yang digunakan yaitu 128 bit atau AES-128. Proses enkripsi dan dekripsi pada algoritma ini dilakukan dengan dua tahapan yaitu proses pembangkitan sub-kunci dari kunci awal, kemudian proses enkripsi/dekripsi. Jumlah sub-kunci pada AES-128 adalah 10 sub-kunci, masing-masing berukuran 128 bit [1].



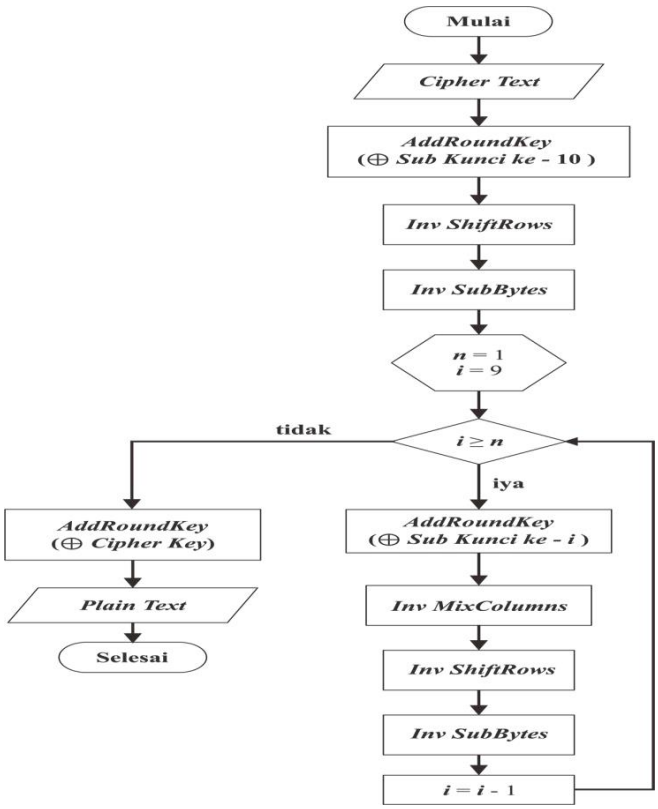
Gambar 1. Flowchart enkripsi algoritma *AES*

Proses pembangkitan sub-kunci dilakukan dengan mempartisi kunci awal menjadi 4 kolom/*words*, dilanjutkan dengan melakukan empat langkah/operasi berurutan, yaitu operasi *RotWord*, *SubWord*, Operasi XOR dengan R-*Con*, kemudian operasi XOR dengan kolom sebelumnya. Lakukan empat langkah yang sama untuk mendapatkan sub-kunci yang lain [3]. Proses enkripsi dan dekripsi membutuhkan 10 subkunci yang sudah dibangkitkan dan *plaintext* atau *ciphertext* yang sudah dipartisi menjadi *block-block* 128 bit. Gambar 1 merupakan *flowchart* enkripsi pada algoritma *AES* 128 bit (AES-128). Sedangkan Gambar 2 merupakan *flowchart* dekripsi pada algoritma *AES* 128 bit (AES-128).

Enkripsi-AES dengan Kunci Citra *Grayscale*

Enkripsi-Pembangkit Kunci Bergeser adalah metode yang bertujuan untuk memodifikasi kunci yang diambil dari sebuah citra grayscale. Proses pembangkitan kunci dari metode ini yaitu dengan membagi piksel-piksel pada gambar menjadi 16 blok, kemudian di operasikan dengan operasi XOR semua piksel tersebut pada setiap bloknya. Sehingga akan didapatkan nilai 16 karakter atau kunci dengan panjang 128 bit. Proses enkripsi pada algoritma ini yaitu seperti pada proses enkripsi AES yang sudah dijelaskan sebelumnya

dengan kunci yang didapat hasil dari pembangkitan kunci.Prosesnya dapat dilakukan dengan beberapa metode yakni *AddRoundKey, SubByte, ShiftRow* dan *MixColumns*. Ataulebih jelasnya semua langkah dapat dilihat pada gambar 1.Proses dekripsinya juga dapat dilihat langkahnya pada Bambar 2.



Gambar 2. *Flowchart* dekripsi algoritma *AES*

Analisis Keamanan

Beberapa analisis keamanan dari penelitian ini adalah sebagai berikut:

a. Analisis Diferensial

Analisis diferensial digunakan untuk menentukan perbedaan dari dua citra yaitu dengan menghitung nilai dari *number of pixels change rate* (*NPCR*). *NPCR* dengan nilai lebih besar dari 90% akan menyulitakan kriptanalisis dalam mencari hubungan statistik antara citra asli dengan citra tersandi [4].

$$NPCR = \frac{\sum_i \sum_j D(i,j)}{W \times H} \times 100\% \quad (1)$$

dimana W dan H merepresentasikan lebar citra dan tinggi citra, dan bentuk dari $D(i,j)$ dapat ditentukan seperti berikut:

$$D(i,j) = \begin{cases} 0, & C(i,j) = C'(i,j) \\ 1, & C(i,j) \neq C'(i,j) \end{cases}$$

dengan(i,j)dan $C'(i,j)$merepresentasikan nilai derajat keabuan dari baris i, dan kolom j dari citra C dan C' [5].

b. Analisis Sensitivitas Kunci

Analisis sensitivitas kunci digunakan untuk mengetahui kesensitifan kunci dari suatu algoritma. Dua hal yang menjadi tolak ukur yaitu, (i) ketika kunci yang digunakan untuk mengenkripsi citra tersebut sedikit berbeda maka akan menghasilkan *cipher image* yang sangat berbeda, (ii) jika ada perbedaan kunci antara proses enkripsi dan dekripsi maka tidak akan memperoleh *plain image* yang diinginkan. Tolak ukur tersebut didapatkan dengan menggunakan *Number of pixels change rate* (*NPCR)* [6].

c. Analisis *Brute Force Attak*

Proses Analisis kemanan suatu metode atau algoritma sangat penting untuk dilakuakan untuk mengetahui seberapa aman ketika algoritma itu digunakan. *Brute force attack* adalah metode untuk menemukan skema kriptografi dengan mencoba semua kemungkinan *password* atau kunci. *Brute force attack* adalah metode untuk menemukan skema kriptografi dengan jumlah besar kemungkinan kunci. *Brute force attack* memungkinkan dapat menyerang kunci privat dihampir semua skema kriptografi, tipe serangan ini bergantung pada ukuran kunci dan mekanisme pada enkripsi yang digunakan. Dalam bidang kriptografi, *brute force attack* merupakan teknik yang digunakan penyerang untuk menemukan kunci enkripsi dengan cara mencoba semua kemungkinan kunci.

Contoh :
Kunci yang digunakan pada penulisan ini yaitu kunci dengan panjang 128 bit. Maka jumlah kunci yang harus dievaluasi oleh pihak lawan adalah sebanyak $(2)(2)(2)...(2)(2) = 2128 = 3{,}4028e + 38$.
Artinya ada $3{,}4028\ x\ 10^{38}$ kemungkinan kunci yang harus dicoba. Jika tahun ada 31.536.000 detik dan 1 komputer untuk menganalisis 1 kunci membutuhkan 1 detik, maka ada $1{,}0790\ x\ 10^{31}$ tahun. Meskipun algoritma *brute force* tidak cocok karena membutuhkan waktu yang cukup lama, namun sebagaimana ciri algoritma *brute force* pada umumnya nilai plusnya terletak pada keberhasilannya yang selalu menemukan solusi (jika diberikan waktu yang cukup) [7].

2. Metodologi

Metode penelitian yang dilakukan mengunakan algoritma AES dengan kunci sebuah citra *grayscale.* Pertama, membangkitkan kunci dari gambar dengan mengkonversinya menjadi 16 karakter. Kemudian dilakukan enkripsi AES dengan kunci yang sudah didapat dari sebuah citra. Gambar 3 adalah proses enkripsi AES dengan kunci citra *grayscale*. Proses Enkripsi AES dengan kunci citra *grayscale* pada Gambar 3 dijelaskan sebagai berikut,

a) Konversi karakter *plain image* menjadi bilangan biner Setiap karakter dalam *plain image* dikonversi menjadi bilagan desimal sesuai kode ASCII kemudian dikonversi menjadi bilangan biner.

b) Membagi pixel menjadi 16 blok dan di XOR setiap pixelnya Membagi 16 blok dari jumlah pixel yang ada dengan mengurutkan baris pertama sampai baris terakhir. Kemudian mengoperasikan setiap pixel yang ada pada setiap blok dengan operasi XOR sehingga didapatkan 16 karakter atau 128 bit untuk dijadikan kunci pada algoritma AES 128.

c) Kunci yang didapat hasil dari proses pembagian gambar menjadi 16 blok yang nantinya akan mendapat 16 karakter atau 128 bit untuk digunakan dalam enkripsi algoritma AES.

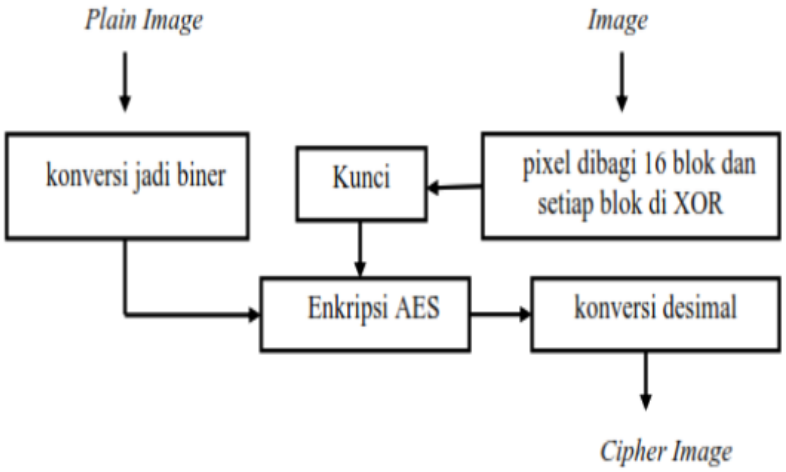
d) Enkripsi AES

Proses enkripsi dari *plain image* dan kunci yang sudah didapatkan dengan langkah sebagai beikut

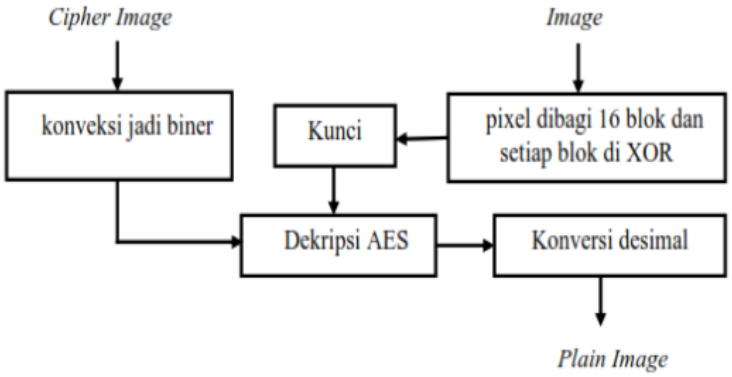
1) *AddRoundKey*
2) *SubByte*
3) *Shiftrows*
4) *MixColumns*

e) Konversi desimal

Setiap bilangan biner dari hasil enkripsi tersebut dikembalikan lagi dalam bentuk desimal dan dirangkai menjadi sebuah citra. Hasil konversi ini akan menjadi *cipher image.* Kedua, proses dekripsi *cipher image* menjadi *plain image* kembali dengan membalik dari proses enkripsi, diuraikan pada Gambar 4.



Gambar 3. Proses enkripsi AES kunci citra *grayscale*



Gambar 4. Proses dekripsi

3. Hasil dan Pembahasan

Data penelitian yang digunakan sebagai *plain image* yaitu citra *grayscale* berukuran 128x128 (lena.jpg), dan kunci citra *grayscale* berukuran 256x256 (cameraman.tif), ditunjukkan pada Gambar 5(a) dan 5(b). Proses enkripsi menggunakan satu buah kunci awal yaitu berupa citra *grayscale* (cameraman.tif). Kunci tersebut dimodifikasi dengan membagi seluruh pixel menjadi 16 blok kemudian setiap blok tersebut di operasikan dengan operasi XOR, sehingga akan memperoleh 16 nilai derajat keabuan dan di konversi kedalam bentuk desimal.Gambar 6 menunjukkan gambar awal kunci dan hasil konversi menjadi 16 derajat keabuan yang akan digunakan dalam tahap enkripsi. Proses selanjutnya yaitu proses enkripsi algoritma AES dengan kunci yang sudah dibangkitkan dari citra *grayscale*. Proses enkripsi bias dilihat langkah langkahnya seperti pada Gambar 1. Enkripsi dilakukan mulai dengan 16 data awal yang ada pada *plain image* hingga pada data akhir. Hasilnya dapat dilihat pada Gambar 7.

(a) *Plain Image* (b) *Key*

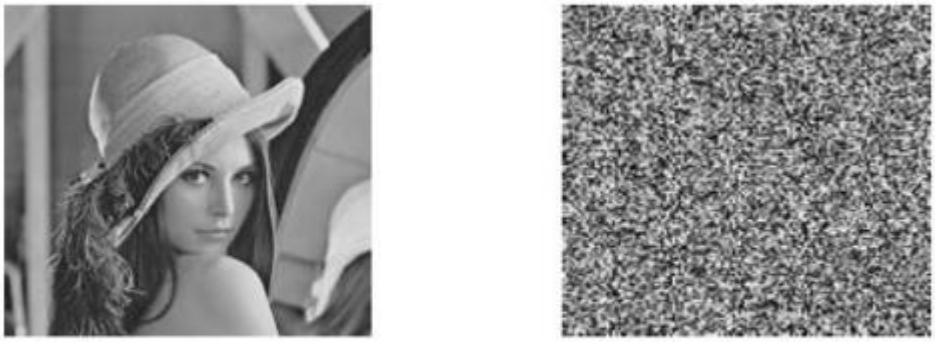
Gambar 5. Data penelitian

$$\begin{bmatrix} 76 & 186 & 18 & 190 \\ 126 & 153 & 35 & 86 \\ 27 & 228 & 143 & 242 \\ 129 & 170 & 53 & 214 \end{bmatrix}$$

(a) (b)

(a) Kunci ; (b) perubahan kunci

Gambar 6. Kunci dan hasil konversi (*cipher key*)



(a) (b)

(a) *Plain Image;* (b) *Cipher Image*

Gambar 7. Hasil proses enkripsi

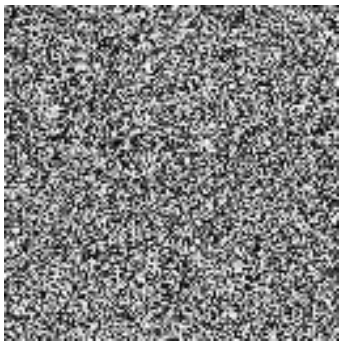
Nilai *NPCR* lebih besar dari 90% menunjukkan algoritma tersebut baik digunakan untuk enkripsi data. Nilai *NPCR* yang didapatkan antara *cipher image* akhir dengan *plain image* adalah 99,6582%. Sehingga metode ini aman untuk digunakan.

Analisis Sensitivitas Kunci

Kunci yang digunakan untuk enkripsi *plain image* pada tahap ini yaitu cameraman.tif berdimensi 256x256, cameraman.jpg berdimenasi 256x256 piksel dan cameraman.jpg berdimensi 255x255 piksel.

(a) *Cipher Image;* (b) *Plain Image*

Gambar 8. Hasil proses dekripsi



Gambar 9. Hasil dekripsi (kunci cameraman.jpg)

Seperti yang ditunjukkan pada tabel 3, no 1 adalah nilai *NPCR* dengan kunci AES yang digunakan dalam tahap enkripsi pada penulisan ini. No 2 yaitu perbedaan hasil enkripsi dengan nilai *NPCR* 99,5483% yang dibandingkan dengan hasil enkripsi no 1. Sedangkan pada no 3, nilai *NPCR* 99,6643% yang dibandingkan hasil enkripsinya dengan no 1. Gambar 9 merupakan gambar hasil dekripsi yang kunci aslinya cameraman.tif akan tetapi diinput dengan kunci cameraman.jpg, sehingga tidak mampu mengembalikan gambar menjadi *plain image.*

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan pada penelitian ini, maka didapatkan beberapa kesimpulan sebagai berikut:

a. Proses pembangkitan kunci algoritma *AES* dari citra *grayscale* dengan mengkonversi menjadi 16 blok dan mengoperasikan setiap pikselnya pada setiap blok menggunakan operasi XOR. Hasil operasi tersebut akan mendapatkan 16 karatkter atau bilangan

biner sepanjang 128 bit dan akan digunakan pada tahapan enkripsi maupun dekripsi terhadap algoritma AES.

b. Proses enkripsi dengan kunci citra *grayscale* yaitu dengan membangkitkan sebuah kunci dari citra *grayscale* tersebut menjadi 128 bit. Kemudian dilakukan tahapan-tahapan pada algoritma AES yakni pembangkitan 10 sub kunci, *AddRounKey*, *SubBytes*, *Shiftrows*, *MixColumns*. Sedangkan pada proses dekripsi yaitu caranya sama dengan mengkonversi kunci *grayscale* dan membangkitkan menjadi 10 sub kunci, kemudian melakukan tahapan algoritma AES dengan kunci kunci ke-10 sampai ke-1. Tahapan tersebut meliputi *AddRoundKey*, *InvShiftRows*, *InvSubBytes* dan *InvMixColumns*. Proses enkripsi maupun dekripsi memiliki putaran tahapan yang sama, yakni 10 putaran.

c. Analisis keamanan pada penelitian ini menunjukkan bahwa metode yang diajukan oleh penulis dengan menerapkan kunci citra *grayscale* untuk enkripsi algoritma AES 128 merupakan metode yang aman dalam penyandian informasi. Dibuktikan d dengan *cipher image* yang memiliki nilai $NPCR = 90\%$ dari semua data penelitian. Dilakukan juga percobaan enkripsi dengan kunci yang mirip dan semuanya mendapatkan nilai $NPCR > 90\%$ yang dapat diartikan bahwa algoritma ini memiliki kunci yang sensitif.

Datar Pustaka

[1] Atani, R. E., Rad, R. M. dan Attar, A. (2013). A new fast and simple image encryption algorithm using scan patterns and xor. *International Journal of Signal Processing, Image Processing and Pattern Recognition*. Vol.6(5): 275-290.

[2] Dharmaadi, I. P. A., Barmawi, A. M. dan Bayu, G. (2013). *Enkripsi Gambar Parsial dengan Kombinasi Metode Stream Cipher RC4 dan Chaotic Function*. Bandung: Institut Teknologi Telkom.

[3] Hanifah, F. (2012). Tugas Akhir: *Aplikasi Algoritma Rijndael dalam Pengamanan Citra Digital*. Depok: Universitas Indonesia.

[4] Patel, A. dan Padate, R. (2015). Image encryption and decryption using aes algorithm. *International Journal of Electronics and Communication Engineering &Technology* (*IJECET*). Vol. 6(1). 23-29.

[5] Rijmen, V. dan Daemen, J. (1999). AES Proposal: Rijndael. http://csrc.nist.gov/archive/aes/rijndael/Rijn dael-ammended.pdf.

[6] Song, C., dan Qiao, Y. (2015). A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal.Chaos. www.mdpi.com/journal/entropy.

[7] Wicaksono, L. (2013). Tugas Akhir : Ketahanan Algoritma RSA Terhadap *Brute Force Attack*. Malang: Universitas Islam Negeri Maulana Malik Ibrahim.