ENKRIPSI GAMBAR GRAYSCALE MENGGUNAKAN KRIPTOGRAFI RIVEST CIPHER (*RC*) *4*

Elkaf Rahmawan Pramudya*, Abdussalam dan De Rosal Ignatius Moses Setiadi
Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol 207, Kode Pos 50131, Semarang, Jawa Tengah
*Email: elkaf@dsn.dinus.ac.id

Abstrak

Algoritma Rivest Cipher (RC) 4 diktagorikan sebagai bentuk kriptografi simteris dengan fungsi XOR. RC4 menggunakan S-Box dan permutasi 256 bit sehingga tidak rentan terhadap serangan. RC4 umumnya digunakan untuk mengenkripsi teks, dalam makalah ini RC4 digunakan untuk mengenkripsi gambar dengan format grayscale. Dalam hal ini konsep kriptografi dan watermarking di hybrid. Pengukuran hasil eksperimen dengan entropy, menunjukkan hasil yang mendekati nilai tertinggi. Nilai tertinggi entropi yaitu 8, dan dalam penelitian ini menghasilkan 7.9994. Untuk membuktikan hasil tersebut, secara kasat mata kami menyajikan histogram dalam bentuk mesh, plot dan bar sehingga terlihat adanya hasil operasi kriptografi, namun hasil tersebut dapat diterima dengan mata manusia meski telah terjadi sejumlah perubahan bit pada gambar yang digunakan. Pada histogram dan mesh gambar asli dan hasil enkripsi dapat disimpulkan bahwa piksel gambar yang dienkipsi telah berubah dan pada saat dekripsi gambar dapat dikembalikan ke wujud semula.

***Kata kunci**: RC4, kriptografi, gambar, grayscale.*

1. PENDAHULUAN

Manipulasi data pada jaringan komputer telah sering dilakukan baik dengan tujuan sekedar merubah sedikit bentuk data hingga mengkamuflasekan data dalam bentuk lain. Manipulasi data merupakan topik penelitian yang banyak disorot oleh peneliti karena dinilai mempunyai banyak kesempatan untuk melakukan proses pengamanan data melalui berbagai eksperimen (Kumar and Ragupathy, 2016). Contoh manipulasi data yang paling mudah dilakukan oleh orang awam namun berbahaya yaitu melakukan manipulasi dan menempel file lain pada gambar. Untuk melakukan proteksi pada data tersebut diperlukan teknologi khusus, yakni kriptografi.

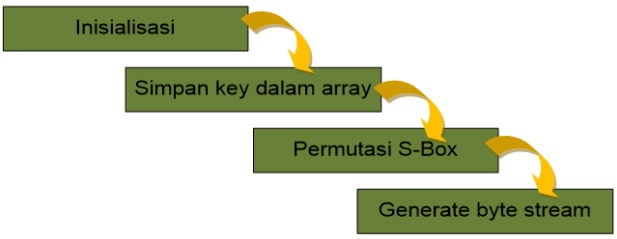
Kriptografi menjadi salah satu proses perubahan bentuk sebuah media menjadi media lain menggunakan algoritma tertentu. Penggunaan kriptografi sudah ada sejak zaman mesir kuno (Kusuma *et al.*, 2017) dengan media teks yang sangat terbatas. Saat ini, kriptografi telah merambah media gambar. Pada media gambar, kriptografi dapat dioperasikan dengan kunci simteris dan asimetris. Kunci asimetris pada beberapa media diketahui lebih handal dibanding kunci simetris karena menggunakan dua buah kunci berbeda (Sari and Rachmawanto, 2016). Terdapat algoritma kunci simteris yang tahan terhadap serangan misalnya RC4. RC4 mempunyai karakter khusus berupa stream cipher dan bilangan permutasi dari 0 sampai 255 dengan XOR, mempunyai performa enkripsi sederhana dengan hanya melibatkan beberapa operasi pada setiap byte yang digunakan.

Menurut Mousa dan Hamad, RC4 dapat ditingkatkan keamanannya dengan mengacak kunci yang digunakan melalui metode peseudo-random bit pada piksel (Irfianti, 2007). Berdasarkan pernyataan dan hasil eksperimen yang telah dilakukan oleh peneliti sebelumnya, maka penulis mencoba untuk mengimplementasikan ide tersebut dan bermaksut untuk mengevaluasi hasil proses enkripsi dan dekripsi. Adapun perbedaan penelitian yang telah kami lakukan, RC4 telah diimplementasikan dalam media gambar grayscale dengan objek berupa teks huruf dan angka 512x512 piksel.

2. RIVEST CODE 4 (RC4)

RC4 diktegorikan sebagai kriptografi simteris dalam bentuk stream cipher yang muncul tahun 1987 dengan model permutasi (Irfianti, 2007). Tahapan RC4 dibedakan menjadi insialisasi dan operasi. Panjang kunci yang digunakan pada RC4 yaitu 1 sampai 256 byte, dimana elemen vektor adalah S[0], S[1], .., S[255] dengan permutasi bilangan 8 bit antara 0 sampai 255 baik pada proses

enkripsi maupun dekripsi. Proses perhitungan permutasi pada RC4 berlangsung secara berkesinambungan seperti pada Gambar 1 berikut.



Gambar 1. Tahapan Umum Enkripsi pada Algoritma RC4

Berdasarkan Gambar 1, proses inisialisasi yang dilakukan dapat diilustrasikan seperti pada pseudo-code dibawah ini.

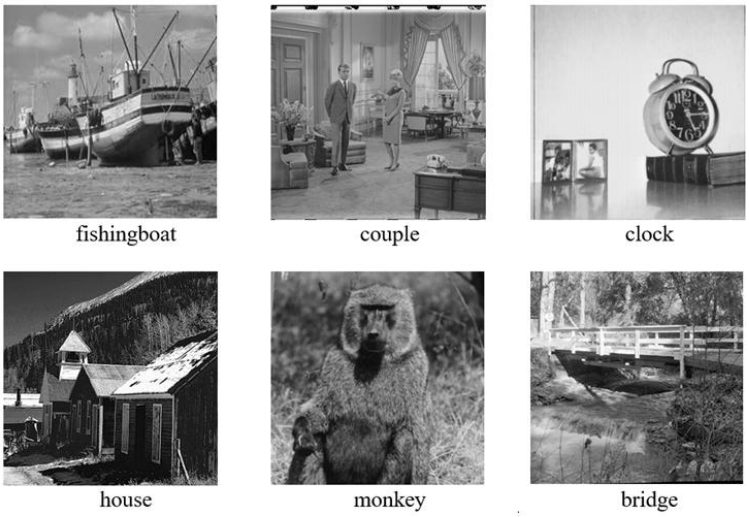
```
j = 0;
for i = 0 to 255:
S[i] = i;
for i = 0 to 255:
j = (j + S[i] + K[i]) mod 256;
swap S[i] and S[j];
```

Sedangkan proses swapping sebagai berikut.

```
i = ( i + 1 ) mod 256
j = ( j + Si ) mod 256
swap Si dan Sj
t = (Si + Sj) mod 256
K = St
```

3. HASIL IMPLEMENTASI

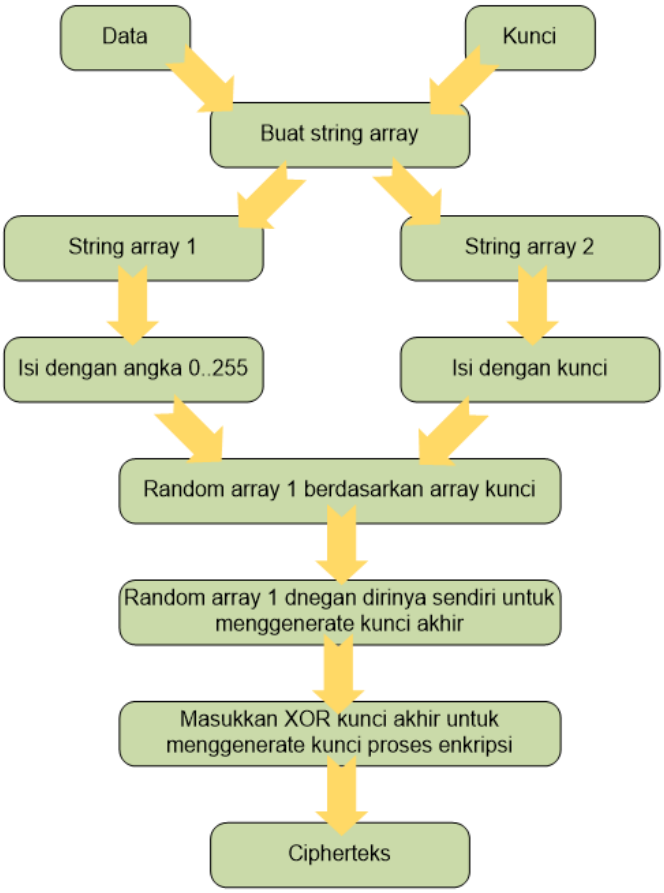
Dalam penelitian ini telah diuji coba sejumlah gambar yang diilustrasikan pada Gambar 3 dengan ukuran 512x512 piksel dan berjenis *grayscale*.



Gambar 3. Dataset Penelitian

Pada makalah ini, kami menggunakan model pengacakan kunci untuk menghasilkan cipherteks sesuai Gambar 2.

ISBN 978-602-99334-9-9



Gambar 2. Tahapan Percobaan yang Dilaksanakan

Dalam proses evaluasi kriptografi simteris dengan RC4 kami telah melakukan beberapa pengujian pada entropi, waktu tempuh enkripsi dan dekripsi, histogram gambar hasil dan gambar asli, serta mesh gambar yang telah dirangkum pada Gambar 4. Menurut Zhang (Li *et al.*, 2014), nilai entropy mencerminakan pengukuran kuantitatif pada sinyal yang dihasilkan oleh gambar sehingga diketahui nilai probabilitas keteracakan gambar. Sedangkan menurut Zahmoul (Zahmoul and Zaied, 2016), rumus entropy pada gambar *grayscale* dapat dilihat pada Persamaan (1) dan Persamaan (2).

$$H(A) = \sum_{i=1}^{n} Yr(A_i)\, Log_2 Yr(A_i) \quad (1)$$

$$Yr(Z = A_i) = \frac{1}{G} \quad (2)$$

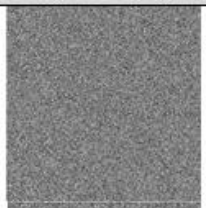
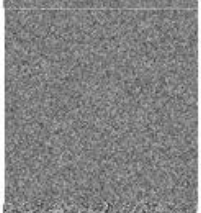
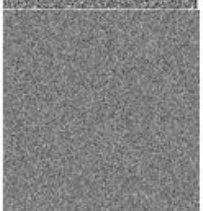
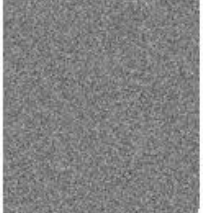
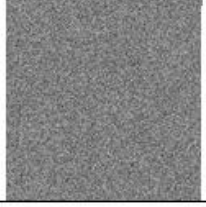
Sesuai Persamaan (1) dan Persamaan (2), rumus *entropy* telah kami sederhanakan sesuai dengan potongan *pseudo-code* berikut.

```
function H = Entropy(X)
n m] = size(X);
H = zeros(1,m);
for Column = 1:m,
    Alphabet = unique(X(:,Column));
    Frequency = zeros(size(Alphabet));
    for symbol = 1:length(Alphabet)
        Frequency(symbol) = sum(X(:,Column) == Alphabet(symbol));
    end
```

```
    P = Frequency / sum(Frequency);
    H(Column) = -sum(P .* log2(P));
end
```

Hasil enksperimen pada sejumlah dataset pada proses enkripsi atau penyandian gambar telah diilustrasikan pada Tabel 1, Tabel 2 dan Tabel 3, dimana kunci yang digunakan untuk enkripsi dan dekipsi adalah `key='kriptografimemangtepatuntukmelakukanproteksidata';`

Tabel 1. Komparasi Enkripsi dan Dekripsi

Nama	Gambar Asli	Cipher Image	Decrypted Image	Entropy
Fishingboat				7.9993
Couple				7.9993
Clock				7.9969
House				7.9994
Monkey				7.9994
Bridge				7.9993

Berdasarkan Tabel 1, telah dipaparkan mengenai hasil enkripsi secara visual dengan tujuan memenuhi aspek ketidaknampakan proses oleh mata manusia. Cipher image akan berbentuk sepeti noise hitam dan putih yang pekat, dimana gambar telah dioperasikan dengan kriptografi. Hasil dekripsi pesan secara kasat mata tidak mengalami perubahan. Demikian hasil dekripsi yang diperoleh telah dihitung dengan *entropy*. Nilai *entropy* tertinggi yaitu 8 (Shukla and Kumar, 2016), sedangkan pada metode yang diterapkan menghasilkan entropy tertinggi 7,9994. Pengujian lain yang dilakukan adalah menganalisa waktu tempuh untuk masing-masing proses enkripsi dan

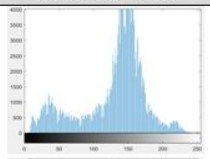
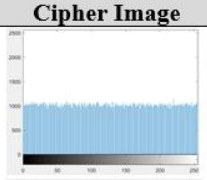
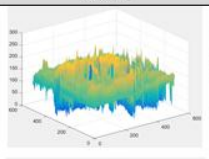
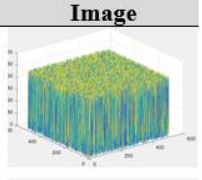
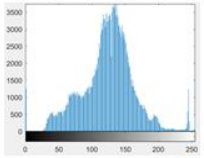
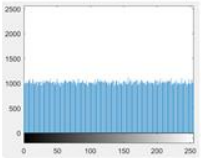
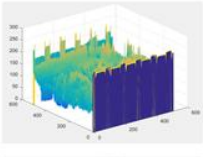
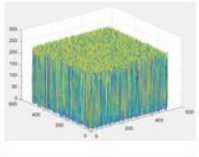
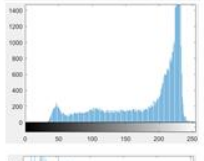
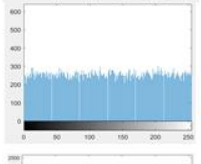
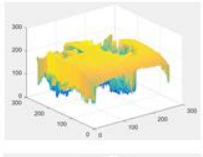
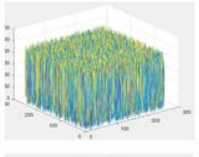
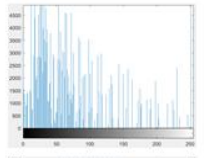
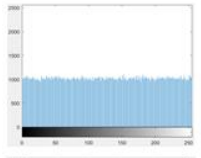
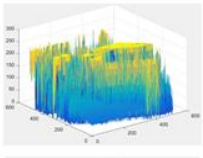
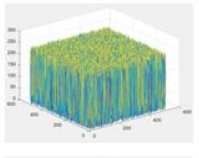
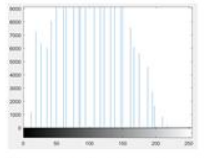
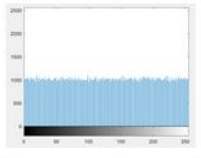
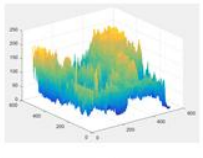
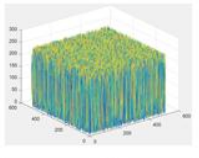
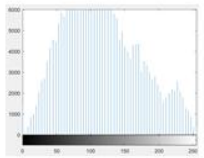
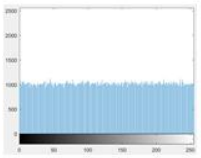
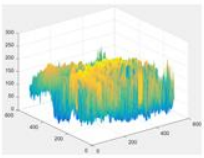
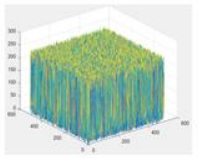
ISBN 978-602-99334-9-9

dekripsi. Dari Tabel 2, dapat disiplukan bahwa waktu enkripsi semua gambar lebih cepat dibanding waktu dekripsinya karena perlu pencocokan kunci terlebih dahulu pada proses dekripsi.s

Tabel 2. Komparasi Waktu Enkripsi dan Dekripsi

Nama	Encrypt Time	Decrypt Time
Fishingboat	**0.622567**	**0.320523**
Couple	**0.110220**	**0.094481**
Clock	**0.334711**	**0.307316**
House	**0.308630**	**0.357645**
Monkey	**0.336850**	**0.332381**
Bridge	**0.345699**	**0.327564**

Tabel 3. Komparasi Histogram dan Mesh Gambar

Nama	Gambar Asli	Histogram Gambar Asli	Histogram Cipher Image	Mesh Gambar Asli	Mesh Cipher Image
Fishingboat					
Couple					
Clock					
House					
Monkey					
Bridge					

Melalui Tabel 3, histogram gambar asli dan gambar hasil telah menandakan terjadinya perubahan bentuk gambar setelah proses enkripsi. Begitu pula dengan bentuk mesh yang dihasilkan, antara mesh gambar asli dan mesh hasil enkripsi terlihat berbeda. Perbedaan disebabkan oleh pengacakan bit pada saat enkripsi.

4. KESIMPULAN

Kriptografi sangat penting dilakukan dengan tujuan proteksi data. Penggunaan algoritma tertentu dalam kriptografi kunci simteris dapat digunakan untuk meningkatkan keamanan dan ketidaknampakan penggunaan teknik kriptografi tersebut. Melalui RC4, makalah ini mengimplementasikan penyandian data gambar untuk mencapai aspek visual. Hasil eksperimen dapat disimpulkan bahwa RC4 berhasil dalam mengenkripsi dan mendekripsi data gambar dengan

nilai entropy mendekati 8 yaitu 7,994. Pengujian secara visual juga dilakukan dengan histogram dan mesh gambar. Dapat dilihat pola pengacakan bit yang terjadi, ditandai dengan model histogram dan mesh pada pola intensitas piksel yang seragam.

DAFTAR PUSTAKA

Irfianti, A. D. (2007) 'METODE PENGAMANAN ENSKRIPSI RC4 STREAM CIPHER UNTUK APLIKASI', *Seminar Nasional Aplikasi Teknologi Informasi 2007 (SNATI 2007)*, 2007(Snati), p. 4.

Kumar, M. G. V. and Ragupathy, U. S. (2016) 'A Survey on current key issues and status in cryptography', in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, pp. 205–210. doi: 10.1109/WiSPNET.2016.7566121.

Kusuma, E. J. *et al.* (2017) 'An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption', in *International Conference on Innovative and Creative Information Technology (ICITech)*, pp. 1–5.

Li, X. *et al.* (2014) 'A brief review on reversible data hiding: Current techniques and future prospects', in *2IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP)*. IEEE, pp. 426–430. doi: 10.1109/ChinaSIP.2014.6889278.

Sari, C. A. and Rachmawanto, E. H. (2016) 'Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting', *Journal of Applied Intelligent System (JAIS)*, 1(3), pp. 179–190. Available at: https://scholar.google.co.id/citations?view_op=view_citation&hl=id&user=RG2Im6cAAAAJ&citation_for_view=RG2Im6cAAAAJ:5nxA0vEk-isC.

Shukla, A. and Kumar, S. (2016) 'Analysis of secure watermarking based on DWT-SVD technique for piracy', in *2016 International Conference on Computing, Communication and Automation (ICCCA)*. IEEE, pp. 1110–1115. doi: 10.1109/CCAA.2016.7813882.

Zahmoul, R. and Zaied, M. (2016) 'Toward new family beta maps for chaotic image encryption', in *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, pp. 004052–004057. doi: 10.1109/SMC.2016.7844867.

ISBN 978-602-99334-9-9