kiki3

by Kiki 3

Submission date: 20-Jul-2023 05:13PM (UTC+0700)
Submission ID: 2133998595
File name: 2-Article Text-1549-1-10-20200217.pdf (379.24K)
Word count: 2838
Character count: 16077

EPOSITOR, Vol. 1, No. 1, November 2019, Pp. 1-8
ISSN : 2714-7975
E-ISSN : 2716-1382

Rancang Bangun Aplikasi Enkripsi Citra Berdasarkan Operasi Rotasi

Bagus Prasetyo Wahyudianto[*1], Diah Risqiwati[2], Denar Regata Akbi[3]
[1,2,3]Teknik Informatika/Universitas Muhammadiyah Malang
herozyko@gmail.com[*1], diah.rizqiwati@gmail.com[2], dnarregata@umm.ac.id[3]

Abstrak

Kriptografi yakni disiplin ilmu yang menggunakan persamaan matematika ketika melakukan proses dekripsi sampai enkripsi. Teknik ini memakai untuk mengubah pesan awal menjadi bentuk kode-kode tertentu, pada penelitian ini menggunakan metode rotasi, metode rotasi sendiri adalah algoritma untuk memutar citra pada porosnya pada sebagian dari citra. Yang bertujuan supaya informasi yang disimpan dan dikirim ke penerima tidak dapat dibaca atau tidak mudah di pahami oleh pihak ketiga atau pihak-pihak yang tidak berhak, keungulan dari penelitian yang dibuat adalah kecepatan proses aplikasi yang cepat serta terjadinya penurunan size file dan tidak mudah dekripsi manual dengan tools lain, Hasil percobaan aplikasi enkripsi terjadinya pemampatan size file yang terjadi sesudah proses dekripsi maupun enkripsi jika dibanding dengan ukuran awal file citra, dan tidak terjadi penurunan size file pada ektensi BMP, kecepatan waktu enkripsi terhadap file dan ukuran pixel pada citra file berektensi BMP dan PNG pada ukuran pixel 2000^{x}2000 memiliki peningkatan kecepatan terbaik yaitu sebesar 0.12x lebih cepat, serta perubahan histogram pada citra awal dengan hasil enkripsi. Penelitian ini di bangun dengan menggunakan bahasa pemprograman Python 3.4, dan ditambah dengan Library PIL-pillow, Library Time.

Kata kunci: *Kriptografi, Rotasi, Python, Rotasi Citra, Kriptografi Citra*

Abstract

Cryptography is a discipline that uses mathematical equations when doing the decryption process until encryption. This technique uses to convert the initial message into the form of certain codes, in this study using the rotation method, the rotation method itself is the algorithm to rotate the image on its axis in part of the image. Aiming that information stored and sent to the recipient can't be read or not easily understood by a third party or parties that are not eligible, advantages of the research made is the speed of fast application process and the decline in file size and not easy manual decryption With other tools, the result of encryption application encoding the occurrence of file size that occurs after the decryption process and encryption when compared with the initial size of the image file, and there is no decrease in the size of the file on BMP extension, the speed of encryption time to the file and the pixel size in the image file extension BMP And PNG on 2000x2000 pixel size has the best speed improvement that is equal to 0.12x faster, and change the histogram in the initial image with the result of encryption. This research is built using Python 3.4 programming language, and coupled with Library PIL-pillow, Library Time.

Keywords: *Cryptography, Rotate, Python, Rotate Images, Cryptography Image*

1. Pendahuluan

Kriptografi dalam disiplin ilmunya berupa seni dan ilmu yang bertujuan menjaga kerahasiaan [1]. Pesan maupun data informasi. Pesan asli biasanya disebut juga dalam *plain image.* Sedangkan pesan yang sudah diamankan disebut *chipper image* [2]. Dalam jenisnya kriptografi dibagi menjadi 2, yakni klasik dan modern [3]. Dimana dalam penerapannya, kriptografi modern biasanya digunakan sebagai teknik keamanan data, akan tetapi masih ada juga pengguna yang memakai teknik keamanan klasik dengan cara merangkap 2 algoritma klasik sehingga menghasilkan tingkat keamanan teknik klasik yang lebih tinggi.

Dalam persoalan citra terdapat algoritma operasi dipakai bertujuan untuk dapat menyembunyikan data atau pesan yang nantinya ditransmisikan. Operasi rotasi adalah membalikkan dengan mengambil y atau 2πy [4]. operasi akan dikendalikan dengan memutar

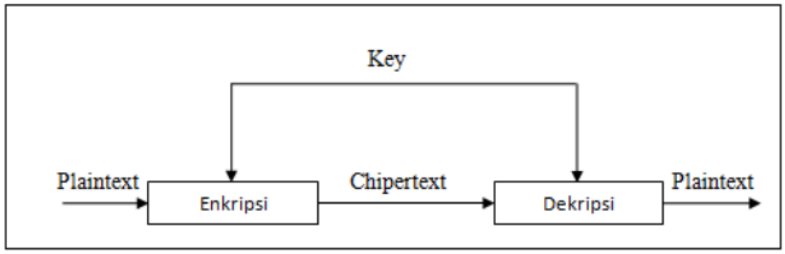
pusat, jari-jari dan sudut y. operasi akan dikendalikan dengan memutar pusat, jari-jari dan sudut y.

Python adalah bahasa pemrograman interpretatif multiguna dengan disisplin ilmu perencanaan yang berpusata pada tingkat bacaan kode [5]. Bahasa python diakui sebagai bahasa yang memadukan kemampuan, kapabilitas, dengan code pemprograman yang jelas, dan ditambahkan dengan fungsi-fungsi pustaka standar yang besar serta komprehensif [6].

Keunggulan penelitihan ini yaitu proses kecepatan enkripsi yang cepat jika perbandingan dengan *tools* manual yang lain serta terjadinya perubahan *size file* pada citra setelah *file* citra tersebut dienkripsi, dan kita dapat merubah *file* ektensi citra yang didekripsi maupun dienkripsi.

2. Metode Penelitian

Pada Gambar 1 dapat dilihat bahwa komponen sistem kriptografi yang dibangun terdiri dari proses dekripsi dan enkripsi. proses pada masing-masing bagian tetaplah sama. Setiap proses dekripsi dan enkripsi harus memasukan *key* yang sama agar dapat di buka.



Gambar 1. Proses kriptografi Simetris [6]

2.1 Operasi Rotasi

Operasi rotasi merupakan teknik pengolahan *image* dengan merubah koordinat *pixel* namun tidak mengubah nilai intensitasnya yang disebut juga sebagai salah-satu jenis transformasi geometri[7]. Prinsip operasi rotasi yakni memindahkan nilai-nilai *pixel* dari posisi awal menuju posisi akhir yang ditentukan oleh nilai batasan *pixel* yang diputar terhadap sudut(θ^o).

Cara kerja operasi rotasi yakni mentransformasikan ketetapan tiap titik pada bidang dengan memutar pada pusat titik tersebut. Titik pusat berada didalam citra dengan bentuk bangun persegi yang akan diputar. Teknik operasi rotasi menggunakan persamaan matematika berikut [4].

$$I'_o = R(I_o; x_o, y_o, r, \theta) \quad (1)$$

$$I'_o = R(I_o; x_o, y_o, r, -\theta) \quad (2)$$

Dalam teknis persamaan matematika diatas dengan konsep poros X dan Y . Sehingga mengalami perpotongan sehingga menghasilkan empat persegi. Untuk r digunakan sebagai identitas area yang dirotasi. Dalam persamaan matematika operasi rotasi Persamaan 1 digunakan untuk tahap enkripsi dan Persamaan 2 digunakan untuk tahap dekripsi. Perbedaannya yakni pada derajat rotasi (θ) pada enkripsi menggunakan nilai positif sedangkan dekripsi menggunakan nilai negatif.

2.2 Alur Sistem

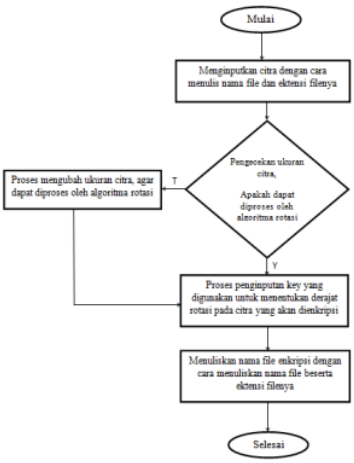
Alur sistem enkripsi Gambar 2 yakni dengan menginputan citra, dengan menginputkan nama *file* dan ektensi *file* dalam aplikasi enkripsi, dengan ukuran pixel minimal 40x40 dan maksimal 2000x2000. Dengan citra yang sudah diinputkan, citra akan dicek ukuran pixelnya. Ketika ukuran pixel tidak dapat dibagi oleh modulus 8, citra akan melalui proses normalisasi. Proses normalisasi adalah proses *resize* citra agar bisa diproses oleh algoritma rotasi agar dapat dimodulus 8. Dengan ukuran yang sudah dinormalisasi, citra akan dirotasi dengan key yang akan diinputkan. Dimana pada proses ini pengimputan *key* menggunakan 7 digit angka, huruf, maupun simbol.

Dengan inputan setiap digit pada *key* yang sudah ditetapkan perwakilan berapa derajat rotasi pada setiap *pixel*nya. Beberapa *pixel* yang berada dalam citra akan berotasi sesuai dengan ketetapan nilainya sesuai dengan inputan *key,* membuat citra akan teracak dengan berbagai variasi putaran. Tahap akhir dalam proses enkripsi yakni pemberian nama pada citra hasil enkripsi dengan menuliskan nama *file* dan ektensi *file* sehingga keluaran citra hasil enkripsi dapat dilihat hasilnya.

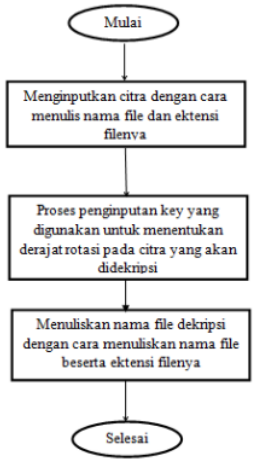
Alur sistem dekripsi Gambar 3 yakni dengan menginputan citra, dengan menginputkan nama *file* dan ektensi *file* dalam aplikasi dekripsi, Citra akan dirotasi sesuai *key* yang diinputkan. Dimana pada proses ini *key* mengguakan 7 digit angka, huruf, maupun simbol.

Dengan inputan setiap digit pada *key* yang sudah ditetapkan perwakilan berapa derajatnya. Beberapa *pixel* yang berada dalam citra akan berotasi sesuai dengan ketetapan nilainya sesuai dengan inputan *key,* membuat citra yang awalnya teracak menjadi citra awal. Setelah proses rotasi selesai, citra hasil dekripsi inilah yang disebut dengan *plaintext.*

Berbeda dengan proses enkripsi, proses deskripsi berkebalikan proses enkripsi. Artiannya, secara proses menginputan citra sama dengan proses enkripsi namun pada proses perotasian *pixel*nya berbeda.



Gambar 2. Alur Sistem Enkripsi



Gambar 3. Alur Sistem Dekripsi

ISSN: 2714-7975; E-ISSN: 2716-1382

3. Hasil Penelitian dan Pembahasan

Pengujian Aplikasi Enkripsi dieksekusi dengan melakukan beberapa percobaan pada aplikasi. Data hasil uji pada aplikasi akan dianalisis sehingga menyimpulkan analisis dari aplikasi ini. Pengujian yang akan dilakukan pada aplikasi :

1. Perubahan size file saat proses enkripsi
2. Perubahan size file saat proses dekripsi
3. Kecepatan enkripsi
4. Analisis ruang kunci
5. Analisis histogram

3.1 Perubahan Size File Saat Proses Enkripsi

Tujuan pengujian ini untuk mengetahui perubahan *size file* sebelum dienkripsi dan setelah dienkripsi.

Skenario pada pengujian penelitihan akan dilakukan dengan beberapa percobaan ektensi *file* awal dan di rubah saat selesai proses enkripsi.

Tabel 1. Hasil Pengujian Size File

No.	Ektensi awal	Size file (KB)	Ektensi Setelah Proses	Size file (KB)	Perubahan Size file (KB)	Perbandingan size file
1.	JPG	275	JPG	74	-201	-0,73091
2.	PNG	515	PNG	527	13	0,025243
3.	BMP	1876	BMP	1876	0	0
4.	GIF	133	GIF	87	-46	-0,34586
5.	TIFF	1450	TIFF	2321	871	0,60069

Hasil dari analisis Tabel 1 yang didapat dari pengujian perubahan *size file* sebelum dienkripsi dan setelah dienkripsi. Terjadi penurunan *size file* pada ektensi JPG dan GIF. Untuk ektensi PNG dan TIFF terjadi peningkatan *size file* dan tidak ada perubahan *size file* pada ektensi BMP.

3.2 Perubahan Size File Saat Proses Dekripsi

Tujuan pengujian penetilihan untuk mengetahui perubahan *size file* setelah dienkripsi dan setelah didekripsi.

Skenario pada pengujian ini akan dilakukan dengan beberapa percobaan ektensi *file* awal dan di rubah saat selesai proses enkripsi.

Pengujian ini menggunakan hasil dari ektensi awal TIF yang di ubah menjadi JPG, PNG, MBP, dan GIF.

Tabel 2. Hasil Pengujian Ukuran Data

No.	Ektensi awal	Size file (KB)	Ektensi Setelah Proses	Size file (KB)	Perubahan Size file (KB)	Perbandingan size file
1.	JPG	74	JPG	71	-3	-0,040541
2.	PNG	527	PNG	519	-8	-0,015181
3.	BMP	1876	BMP	1876	0	0
4.	GIF	86	GIF	84	-2	-0,023256
5.	TIFF	2321	TIFF	2299	-22	-0,009479

Hasil dari analisis Tabel 2 yang didapat dari pengujian perubahan *size file* sebelum dienkripsi dan setelah dienkripsi, Terjadi penurunan *size file* pada ektensi JPG, PNG, GIF, dan TIFF. tetapi tidak ada penurunan *size file* pada ektensi BMP.

Kesimpulan dari percobaan perubahan *size file* adalah hanya file berektensi BMP mempunyai aspek layanan keamanan data yaitu keutuhan data (*Data Integrity*), dikarenakan hanya file berektensi BMP yang mempunyai *size file* yang sama dengan file asli, sedangkan untuk ektensi yang lainnya, mengalami penurunan *size file* sehingga berbeda dengan *file* awal.

3.3 Kecepatan Proses Enkripsi

Tujuan pengujian ini untuk mengetahui kecepatan enkripsi citra, skenario pada pengujian penelitihan akan dilakukan dengan beberapa percobaan ektensi dan ukuran pixel yang berbeda.

Tabel 3. Hasil Pengujian Kecepatan Enkripsi

No.	Ektensi *File*	Ukuran *pixel*	Kecepatan percobaan 1 (s)	Kecepatan percobaan 2 (s)	Kecepatan percobaan 3 (s)	Perbandingan waktu percobaan 3 dan 1
1.	BMP	2000x2000	1,30208333	0,171875	0,15625	0,12
2.	BMP	1500x1500	0,109375	0,09375	0,109375	1
3.	BMP	1000x1000	0,03125	0,046875	0,046875	1,5
4.	BMP	500x500	0,015625	0,015625	0,015625	1
5.	BMP	250x250	0,015625	0,015625	0,015625	1
6.	GIF	2000x2000	0,078125	0,078125	0,078125	1
7.	GIF	1500x1500	0,03125	0,03125	0,046875	1,5
8.	GIF	1000x1000	0,015625	0,03125	0,015625	1
9.	GIF	500x500	0,015625	0,015625	0,015625	1
10.	GIF	250x250	0,015625	0,00965	0,00965	0,6176
11.	JPG	2000x2000	0,171875	0,171875	0,171875	1
12.	JPG	1500x1500	0,109375	0,109375	0,09375	0,857143
13.	JPG	1000x1000	0,03125	0,046875	0,046875	1,5
14.	JPG	500x500	0,015625	0,015625	0,015625	1
15.	JPG	250x250	0,00955	0,00955	0,00955	1
16.	PNG	2000x2000	1,30208333	1,302083	0,15625	0,12
17.	PNG	1500x1500	0,09375	0,09375	0,109375	1,166667
18.	PNG	1000x1000	0,046875	0,046875	0,015625	0,333333
19.	PNG	500x500	0,015625	0,015625	0,00978	0,62592
20.	PNG	250x250	0,00955	0,00955	0,00955	1
21.	TIF	2000x2000	1,30208333	1,302083	0,171875	0,132
22.	TIF	1500x1500	0,09375	0,109375	0,109375	1,166667
23.	TIF	1000x1000	0,03125	0,03125	0,046875	1,5
24.	TIF	500x500	0,015625	0,015625	0,00955	0,6112
25.	TIF	250x250	0,00955	0,00955	0,00955	1

Hasil analisis Tabel 3 yang didapat dari pengujian kecepatan enkripsi adalah semakin rendah *pixel* suatu ektensi semakin cepat pula kecepatan enkripsi, *pixel* suatu extensi juga mempengaruhi *size file* sebuah citra, di saat ukuran citra tersebut rendah atau sedikit kecepatan enkripsi juga semakin cepat, begitu juga sebaliknya.

3.4 Analisis ruang kunci

Serangan *Brute-Force* digunakan untuk mencoba kemungkinan *key* untuk dilakukan dekripsi. Ruang kunci dibuatcukup besar yang bertujuan agar serangan hacker dengan *Brute Force* kurang efektik atau tidak efektif, ruang kunci merupakan jumlah total *key* yang dapat diinputkan saat melakukan dekripsi[8].

Parameter kunci rahasia yang digunakan di dalam algoritma enkripsi ini memiliki satu buah key, yakni *p*. Dalam rancangan penelitihan ini satu key menggunakan 7 karakter, dimana 1 karakter mempunyai 8 bit dalam pegkodean ASCII. Sehingga 1 key memiliki 56 bit, maka nilai kemungkinan ruang kunci adalah sekitar $2^{56} = 7.2 \times 10^{16}$.

$$H = 2^p \quad (3)$$

Dengan menggunakan Persamaan 3, Ruang kunci seluruhnya adalah

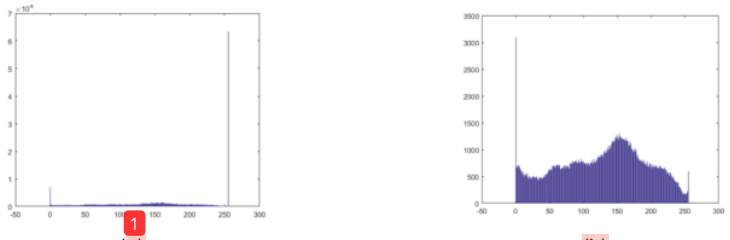
$H = 2^{56}$

$H = 7.2 \times 10^{16}$

Ukuran Ruang Kunci ini cukup besar, sehingga algoritma dapat bertahan terhadap serangan *Brute-Force Attack*.

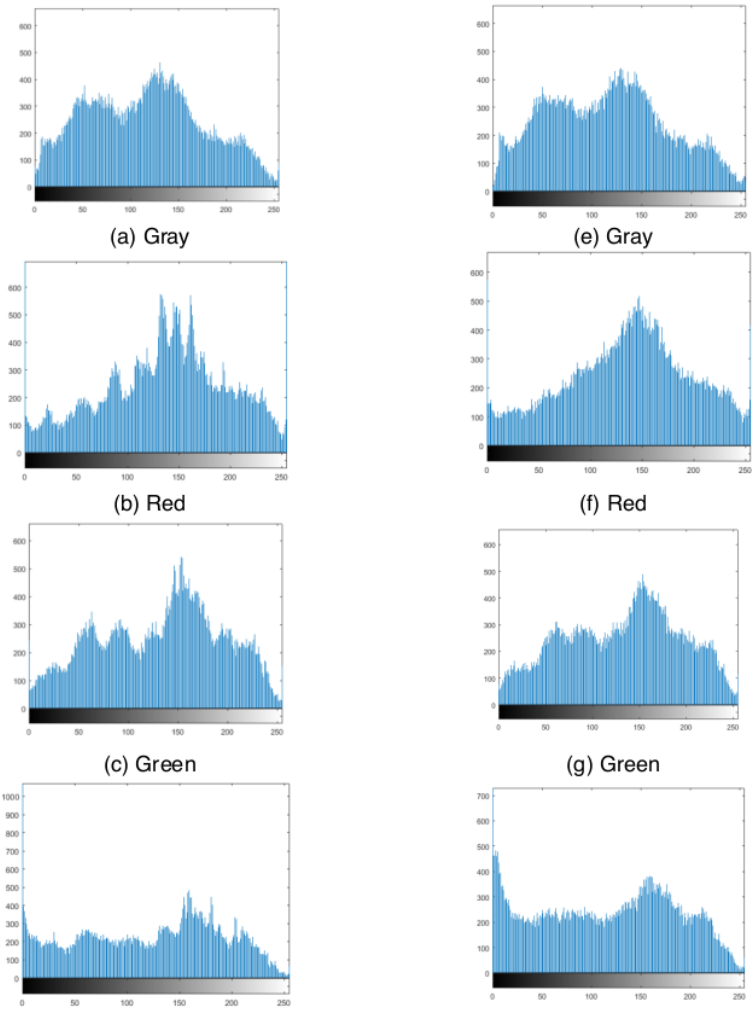
ISSN: 2714-7975; E-ISSN: 2716-1382

3.5 Analisis histogram



(a) (b)

Gambar 4. (a) Histogram Citra Awal, (b) Histogram Enkripsi JPG



(a) Gray (e) Gray

(b) Red (f) Red

(c) Green (g) Green

(d) Blue (h) Blue

Gambar 5. (A)-(D) Histogram Citra Awal Untuk Masing-Masing Kanal, Dan (E)-(H) Histogram Chiper-Image Untuk Setiap Kanal

Pengolahan citra histogram menunjukan penyeberan nilai *pixel* dalam sebuah citra. Pada saat peretas (*hacker*) memakai teknik histogram agar dapat melakukan kriptanalisis dengan memanfaatkan frekuensi kemunculan *pixel* pada histogram. Dengan menganalisa frekuensi nilai *pixel*, peretas memperkirakan *key* atau *pixel-pixel* di dalam *plain-image* [9].

Agar tidak dapat memakai teknik histogram agar dapat memakai analisis frekuensi, sehingga histogram plain-image dan histogram cipher-image seharusnya berbeda secara signifikan atau secara statistik tidak memiliki kemiripan. Peretas (hacker) berharap nilai pixel yang sering muncul didalam plain-image berkorelasi dengan nilai pixel yang sering muncul di dalam cipher-image [10]. Oleh karena itu, harusnya histogram cipher-image datar (flat) atau berbeda dengan citra awal.

Gambar 4(a) menunjukkan histogram citra awal sebelum dienkripsi, dan Gambar 4(b) menunjukan histogram dari hasil enkripsi. Histogram dari Gambar 4(a) dan Gambar 4(b) terjadi perubahan setelah dienkripsi.

Gambar 5(a) sampai Gambar 5(d) memperlihatkan histogram citra awal sebelum dienkripsi (*plain image*) untuk setiap karnal warna *Gray* dan RGB, Gambar 5(e) sampai Gambar 5(h) adalah histogram masing-masing karnal warna pada *cipher image*. Sama seperti citra awal pada Gambar 4(a) dan Gambar 4(b) histogram *chiper image* pada setiap karnal *Gray* dan RGB juga terlihat berbeda dengan histogram *plain image*.

Kesimpulan dari analisis histogram adalah dengan menggunakan algoritma operasi rotasi dapat menunjukan histogram yang berbeda dengan citra awal, tetapi histogram yang baik harusnya berbeda secara signifikan atau secara statistik tidak memiliki kemiripan dan harusnya histogram chiper-image datar (flat) atau secara statistik memiliki distribusi (relatif) uniform, sehingga dapat disimpulkan algoritma operasi rotasi saja kurang efektif untuk enkripsi.

4. Kesimpulan

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan dari tugas akhir yang berjudul "Rancang Bangun Aplikasi Enkripsi Citra berdasarkan Operasi Rotasi" dapat disimpulkan sebagai berikut:

1. Pesan yang berupa citra dapat dikonversi menjadi pesan enkripsi dan dekripsi, hasil proses enkripsi citra terjadi perubahan *size file* dan histogramnya, sedangkan hasil proses dekripsi mengalami perubahan *size file* namun memiliki histogram yang sama dengan citra awal.
2. Dari analisis perubahan *size file* proses enkripsi dan dekripsi, hanya *file* yang berektensi BMP yang memiliki *size file* yang tetap seperti *file* awal, sedangkan untuk ektensi JPG, BMP, PNG, dan TIF mengalami penurunan size file.
3. Dari analisis kecepatan proses enkripsi berpengaruh terhadap *size file* dan ektensi *file* pada citra. dari percobaan yang dilakukan, *file* berektensi BMP dan PNG pada ukuran *pixel* 2000X2000 memiliki pengkatan kecepatan terbaik yaitu sebesar 0.12x lebih cepat.

Daftar Notasi

H = Hasil dari kombinasi karakter *key*
p = Jumlah bit pada key

Referensi

[1] Rizqi Firmansyah and W. Suadi, "Pada Media Gambar Dengan Menggunakan Metode Des Dan Region-Embed Data Density .," *Byte*, pp. 1–7, 2011.
[2] B. S. W. Poetro, P. Studi, T. Informatika, and U. Diponegoro, "Prosiding seminar nasional ilmu komputer universitas diponegoro 2010 semarang, 7 agustus 2010," pp. 175–178, 2010.
[3] D. Abrihama, "Keystream Vigenere Cipher: Modifikasi Vigenere Cipher dengan Pendekatan Keystream Generator," *Progr. Stud. Inform. ITB. Bandung*, 2008.
[4] Z. Liu, S. Li, M. Yang, W. Liu, and S. Liu, "Image encryption based on the random rotation operation in the fractional Fourier transform domains," *Opt. Lasers Eng.*, vol. 50, no. 10, pp. 1352–1358, 2012.
[5] B. Santoso, "Bahasa Pemrograman Python di Platform GNU/LINUX," pp. 1–9, 2016.
[6] T. Heriyanto, "Pengenalan Kriptografi," p. 60, 1999.
[7] D. Putra, *Pengolahan Citra Digital*, 1st ed. Yogyakarta: ANDI OFFSET, 2010.
[8] R. Munir, "Digital Menggunakan Kombinasi Dua Chaos Map Dan Penerapan Teknik Selektif."

[9] P. Ronsen, A. Halim, and I. Syahputra, "Enkripsi Citra Digital Menggunakan Arnold's Cat Map dan Nonlinear Chaotic Algorithm," *JSM STMIK Mikroskil*, vol. 15, no. 2, pp. 61–71, 2014.
[10] V. Yuniati, G. Indriyanta, and A. R. C, "Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk Semua Jensis File," *J. Inform.*, vol. 5, no. 1, pp. 22–31, 2009.

kiki3

ORIGINALITY REPORT

15%	15%	2%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	juti.if.its.ac.id Internet Source	6%
2	journal.unipdu.ac.id Internet Source	2%
3	Submitted to Universitas Terbuka Student Paper	1%
4	catatankriptografi.wordpress.com Internet Source	1%
5	123dok.com Internet Source	1%
6	Submitted to University of Nottingham Student Paper	1%
7	core.ac.uk Internet Source	1%
8	hm2.heubach-media.de Internet Source	1%
9	Muhammad Yunus, A. Arifin. "Karakterisasi Sensor Kekentalan Oli Berbasis Serat Optik	1%

Plastik Menggunakan Metode Back Scattering", POSITRON, 2018

Publication

Exclude quotes	Off	Exclude matches	< 1%
Exclude bibliography	On		