

**KRIPTOGRAFI GAMBAR MENGGUNAKAN ALGORITMA *AFFINE*
CIPHER DAN *CRYPTOGRAPHICALLY SECURE PSEUDORANDOM*
NUMBER GENERATOR BERBASIS *CHAOS***

SKRIPSI

Diajukan untuk memenuhi sebagian syarat memperoleh gelar Sarjana Matematika



Oleh:

Rajestika Faldela Ramanov

NIM 2004800

**PROGRAM STUDI MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA**

2024

LEMBAR HAK CIPTA

**KRIPTOGRAFI GAMBAR MENGGUNAKAN ALGORITMA *AFFINE*
CIPHER DAN *CRYPTOGRAPHICALLY SECURE PSEUDORANDOM*
NUMBER GENERATOR BERBASIS *CHAOS***

Oleh:

Rajestika Faldela Ramanov

2004800

Diajukan untuk memenuhi sebagian syarat memperoleh gelar Sarjana Matematika
pada Program Studi Matematika Fakultas Pendidikan Matematika dan Ilmu
Pengetahuan Alam

© Rajestika Faldela Ramanov
Universitas Pendidikan Indonesia
Agustus 2024

Hak Cipta dilindungi undang-undang
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian dengan dicetak
ulang, difotokopi, atau cara lainnya tanpa izin penulis.

LEMBAR PENGESAHAN

RAJESTIKA FALDELA RAMANOV

KRIPTOGRAFI GAMBAR MENGGUNAKAN ALGORITMA *AFFINE*
CIPHER DAN *CRYPTOGRAPHICALLY SECURE PSEUDORANDOM NUMBER*
GENERATOR BERBASIS *CHAOS*

Disetujui dan disahkan,
Pembimbing I



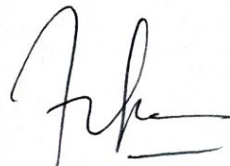
Dra. Hj. Rini Marwati, M.S.
NIP. 196606251990012001

Pembimbing II



Ririn Sispiyati, M.Si.
NIP. 198106282005012001

Mengetahui,
Ketua Program Studi Matematika



Dr. Kartika Yulianti, M.Si.
NIP. 198207282005012001

ABSTRAK

Kriptografi dapat mengamankan informasi dengan menyandikan (enkripsi) sehingga informasi menjadi tidak terbaca. Pada penelitian ini, kriptografi diterapkan pada gambar menggunakan algoritma *Affine Cipher* dengan memanfaatkan pembangkit bilangan acak *CSPRNG* berbasis *Chaos* sebagai kunci-kunci yang digunakan *Affine Cipher*. Pemanfaatan pembangkit bilangan acak diharapkan memberikan peningkatan keamanan dalam hal kualitas enkripsi. Implementasi ini dilakukan menggunakan program aplikasi yang juga digunakan untuk validasi bahwa gambar yang telah dienkripsi dapat dikembalikan seperti semula (dekripsi). Selain itu, analisis kualitas penyandian dilakukan untuk mengetahui peningkatan kualitas enkripsi *Affine Cipher* dengan dan tanpa memanfaatkan *CSPRNG* berbasis *Chaos*. Hasil dari penelitian ini menunjukkan bahwa algoritma kriptografi dapat diterapkan pada gambar, validasi berhasil dilakukan, dan pemanfaatan *CSPRNG* berbasis *Chaos* pada *Affine Cipher* secara signifikan meningkatkan kualitas enkripsi gambar.

Kata Kunci: Kriptografi, Kriptografi Gambar, *Affine Cipher*, *CSPRNG* berbasis *Chaos*

ABSTRACT

Cryptography can secure information by encrypting it so that it becomes unreadable.. In this research, cryptography is applied to images using Affine Cipher algorithm by utilizing Chaos-based CSPRNG random number generator as the keys used by Affine Cipher. The utilization of random number generator is expected to provide increased security in terms of encryption quality. This implementation is done using an application program that is also used for validation that the encrypted image can be restored to its original state (decryption). In addition, encryption quality analysis was conducted to determine the improvement of Affine Cipher encryption quality with and without utilizing Chaos-based CSPRNG. The results of this research show that the cryptographic algorithm can be applied to images, validation is successfully performed, and the utilization of Chaos-based CSPRNG on Affine Cipher significantly improves the image encryption quality.

Keywords: *Cryptography, Image Cryptography, Affine Cipher, Chaos-based CSPRNG*

DAFTAR ISI

LEMBAR HAK CIPTA	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN	iii
KATA PENGANTAR.....	iv
UCAPAN TERIMA KASIH	v
ABSTRAK	vi
<i>ABSTRACT</i>	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL.....	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian	3
BAB II KAJIAN TEORI	4
2.1 Teori Dasar Matematika.....	4
2.1.1 Algoritma Pembagian.....	4
2.1.2 Faktor Persekutuan Terbesar	4
2.1.3 Relatif Prima	4
2.1.4 Kongruen Modulo	4
2.1.5 Invers Modulo	4
2.2 Teori Dasar Kriptografi	5
2.2.1 Terminologi Istilah	5
2.2.2 Kriptografi.....	5
2.2.3 Kriptosistem Kunci-Simetri	6

2.2.4 Cipher Substitusi	6
2.2.5 <i>Affine Cipher</i>	6
2.2.6 Pembangkit Bilangan Acak.....	7
2.2.7 <i>CSPRNG</i> Berbasis <i>Chaos</i>	7
2.3 Kriptografi Gambar	10
2.4 Analisis Histogram.....	11
2.5 Autokorelasi Piksel Bertetangga	11
2.6 Entropi Informasi	12
2.7 <i>Python</i>	13
BAB III METODE PENELITIAN.....	14
3.1 Identifikasi Masalah.....	14
3.2 Model Dasar	14
3.2.1 <i>Affine Cipher</i>	14
3.2.2 <i>CSPRNG</i> Berbasis <i>Chaos</i>	15
3.3 Pengembangan Model Dasar.....	17
3.4 Konstruksi Program Aplikasi	23
3.4.1 <i>Input</i> dan <i>Output</i>	23
3.4.2 Algoritma Deskriptif	23
3.4.3 Desain Tampilan.....	24
3.4.4 <i>Library</i> Program.....	25
3.5 Proses Validasi.....	26
3.6 Penarikan Kesimpulan.....	26
BAB IV HASIL DAN PEMBAHASAN.....	27
4.1 Skema Kriptografi Gambar Menggunakan <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	27
4.2 Konstruksi Program Aplikasi Kriptografi Gambar Menggunakan <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	30
4.2.1 <i>Pseudocode</i> Program Aplikasi Kriptografi Gambar Menggunakan <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	30

4.2.2 Program Aplikasi Kriptografi Gambar Menggunakan <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	35
4.2.3 Validasi.....	37
4.3 Analisis Kualitas Enkripsi.....	41
4.3.1 Analisis Histogram.....	42
4.3.2 Autokorelasi Piksel Bertetangga.....	45
4.3.3 Entropi Informasi.....	48
BAB V KESIMPULAN DAN SARAN.....	50
5.1 Kesimpulan	50
5.2 Saran.....	51
DAFTAR PUSTAKA	52
LAMPIRAN	53

DAFTAR GAMBAR

Gambar 2.1 Diagram <i>Bifurcation</i> Persamaan Logistik	9
Gambar 2.2 Contoh Sederhana Gambar RGB dan <i>Grayscale</i>	11
Gambar 3.1 Skema Enkripsi <i>Affine Cipher</i> pada Nilai Piksel Gambar.....	15
Gambar 3.2 Skema Dekripsi <i>Affine Cipher</i> pada Nilai Piksel Gambar	15
Gambar 3.3 Skema Pembangkitan Barisan Bilangan Acak dengan <i>CSPRNG</i> Berbasis <i>Chaos Logistic Map</i>	17
Gambar 3.4 Skema Enkripsi Pengembangan Model Dasar <i>Affine Cipher</i> dan <i>CSPRNG</i> Berbasis <i>Chaos</i> pada Gambar RGB.....	19
Gambar 3.5 Skema Dekripsi Pengembangan Model Dasar <i>Affine Cipher</i> dan <i>CSPRNG</i> Berbasis <i>Chaos</i> pada Gambar RGB.....	20
Gambar 3.6 Skema Enkripsi Pengembangan Model Dasar <i>Affine Cipher</i> dan <i>CSPRNG</i> Berbasis <i>Chaos</i> pada Gambar <i>Grayscale</i>	21
Gambar 3.7 Skema Dekripsi Pengembangan Model Dasar <i>Affine Cipher</i> dan <i>CSPRNG</i> Berbasis <i>Chaos</i> pada Gambar <i>Grayscale</i>	22
Gambar 3.8 Rancangan Tampilan Program Enkripsi dan Dekripsi	25
Gambar 4.1 Skema Enkripsi Kriptografi Gambar menggunakan <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	27
Gambar 4.2 Skema Dekripsi Kriptografi Gambar menggunakan <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	28
Gambar 4.3 Berkas Program Aplikasi Kriptografi Gambar Menggunakan <i>Affine</i> <i>Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	35
Gambar 4.4 Tampilan Utama Program Aplikasi Kriptografi Gambar Menggunakan <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	36
Gambar 4.5 Plain Gambar RGB Berukuran 256×256 dengan Cipher Gambar dan Hasil Dekripsi dari Cipher Gambar.....	38
Gambar 4.6 Kode dan Hasil Perbandingan Larik Gambar 4.5 (a) dan (c)	39
Gambar 4.7 Kode dan Hasil Perbandingan Larik Gambar 4.5 (d) dan (f)	39
Gambar 4.8 Plain Gambar <i>Grayscale</i> Berukuran 256×256 dengan Cipher Gambar dan Hasil Dekripsi dari Cipher Gambar.....	39
Gambar 4.9 Kode dan Hasil Perbandingan Larik Gambar 4.8 (a) dan (c)	40

Gambar 4.10 Kode dan Hasil Perbandingan Larik Gambar 4.8 (d) dan (f)	40
Gambar 4.11 Perbandingan Hasil Enkripsi Gambar RGB Menggunakan <i>Affine Cipher</i> dengan <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	41
Gambar 4.12 Perbandingan Hasil Enkripsi Gambar <i>Grayscale</i> Menggunakan <i>Affine Cipher</i> dengan <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	42
Gambar 4.13 Perbandingan Histogram Distribusi Nilai Pixel pada Plain Gambar RGB 1, Hasil Enkripsi <i>Affine Cipher</i> Gambar RGB 1, dan Hasil Enkripsi <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i> Gambar RGB 1	43
Gambar 4.14 Perbandingan Histogram Distribusi Nilai Pixel pada Plain Gambar RGB 2, Hasil Enkripsi <i>Affine Cipher</i> Gambar RGB 2, dan Hasil Enkripsi <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i> Gambar RGB 2	44
Gambar 4.15 Perbandingan Histogram Distribusi Nilai Pixel pada Plain Gambar <i>Grayscale</i> 1, Hasil Enkripsi <i>Affine Cipher</i> Gambar <i>Grayscale</i> 1, dan Hasil Enkripsi <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i> Gambar <i>Grayscale</i> 1.....	44
Gambar 4.16 Perbandingan Histogram Distribusi Nilai Pixel pada Plain Gambar <i>Grayscale</i> 2, Hasil Enkripsi <i>Affine Cipher</i> Gambar <i>Grayscale</i> 2, dan Hasil Enkripsi <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i> Gambar <i>Grayscale</i> 2.....	45
Gambar 4.17 Visualisasi Korelasi Pixel Bertetangga pada Gambar RGB	47
Gambar 4.18 Visualisasi Korelasi Pixel Bertetangga pada Gambar <i>Grayscale</i> ...	47

DAFTAR TABEL

Tabel 4.1 Perbandingan Nilai Autokorelasi Piksel Bertetangga	46
Tabel 4.2 Perbandingan Nilai Entropi Gambar RGB	48
Tabel 4.3 Perbandingan Nilai Entropi Gambar <i>Grayscale</i>	48

DAFTAR LAMPIRAN

Lampiran 1. Kode Python Pembangkitan Kunci.....	53
Lampiran 2. Kode Python Pembangkitan Larik Bilangan Relatif Prima.....	53
Lampiran 3. Kode Python Enkripsi dan Dekripsi <i>Affine Cipher</i> dan <i>CSPRNG</i> berbasis <i>Chaos</i>	54

DAFTAR PUSTAKA

- Burton, D. M (2010). *Elementary Number Theory*. New York: McGraw-Hill.
- Dhruv, A. J., Patel, R., & Doshi, N. (2021). Python: The Most Advanced Programming Language for Computer Science Applications. *Science and Technology Publications, Lda*, 292-299. doi: 10.5220/0010307900003051
- Irwansyah, E. & Moniaga, J. V. (2014). *Pengantar Teknologi Informasi*. Yogyakarta: Deepublish.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2001). *Handbook of Applied Cryptography*. Amerika Serikat: CRC Press.
- Munir, R. (2019). *Kriptografi Edisi Kedua*. Bandung: Penerbit INFORMATIKA.
- Naufal, M. F., Marwati, R., & Sispiyati, R. (2021). Kriptografi Audio Menggunakan Transposisi dan Affine Cipher yang Dikembangkan dengan Algoritma Blum Blum Shub. *Jurnal EurekaMatika*, 9(1), 1-14.
- Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review SIM). *Jurnal Ekonomi Manajemen Sistem Informasi*, 3(5), 564—573. doi: <https://doi.org/10.31933/jemsi.v3i5>
- Stinson, D. R. (2006). *Cryptography Theory and Practice Third Edition*. Boca Raton: Chapman & Hall/CRC.
- Sulistiyanti, S. R., Setyawan FX. A., & Komarudin, M. (2016). *Pengolahan Citra Dasar dan Contoh Penerapannya*. Yogyakarta: Teknosain.
- Wu, Y., Yang, G., Jin, H., & Noonan, J. P. (2012). Image Encryption using the Two-dimensional Logistic Chaos Map. *Journal of Electronic Imaging*. 21(1). 1—29 doi: 10.1117/1.JEI.21.1.013014
- Zelvian, M. R. (2023). *Kriptografi Gambar dengan Menggunakan Algoritma Blowfish*. Universitas Pendidikan Indonesia, Bandung