Jurnal Elektronik Ilmu Komputer Udayana
Volume 14, No 3. February 2026

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Pengamanan Data menggunakan Algoritma Enkripsi Advanced Encryption Standard (AES) dan Zigzag Cipher

I Gusti Ngurah Bagus Arimbawa [a1], I Made Widiartha [a2] , I Ketut Gede Suhartana [a3] , I Gusti Ngurah Anom Cahyadi Putra. [a4]

Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,

Universitas Udayana

Jalan Raya Kampus Udayana, Bukit Jimbaran, Kuta Selatan, Badung, Bali Indonesia

[1]dosman10m5@gmail.com

[2]madewidiartha@unud.ac.id

[3]ikg.suhartana@unud.ac.id

[4]anom.cp@unud.ac.id

Abstrak

Masalah keamanan dan kerahasiaan data merupakan aspek penting dalam komunikasi modern. Kriptografi adalah metode utama untuk mengamankan informasi dari suatu data dengan mengubahnya menjadi data yang tidak dapat dibaca menggunakan suatu algoritma enkripsi. Penelitian ini bertujuan untuk meningkatkan keamanan enkripsi data, khususnya dalam format video, dengan memodifikasi algoritma Advanced Encryption Standard (AES-256) menggunakan penambahan langkah enkripsi Zigzag Cipher. Penelitian dilakukan dengan menguji performa algoritma zigzag cipher, AES-256, AES-256 + zigzag pada input data, AES-256 + zigzag cipher pada output data, dan AES-256 + zigzag cipher pada input password, digunakan untuk memproses 30 file video yang dipotong ke durasi tertentu dari 3 video sumber dan 1 file video dengan tampilan monolitik (1 warna), dengan menggunakan 4 password per algoritma. Pengujian diterapkan menggunakan bahasa pemrograman Python 3.8.10. Hasil penelitian menunjukkan bahwa penambahan Zigzag Cipher pada AES-256 dapat meningkatkan kompleksitas dan keamanan enkripsi. Algoritma zigzag sendiri diketahui lebih cepat sekitar 20 kali dibandingkan AES atau variasinya. Meskipun penambahan zigzag cipher menyebabkan penambahan waktu pemrosesan, peningkatan ini relatif kecil. Algoritma AES Modifikasi 1 (Zigzag pada plaintext AES) secara konsisten mencapai nilai entropy yang lebih tinggi, sementara semua algoritma yang diuji mampu mencapai koefisiensi korelasi yang rendah, mendekati 0.

Kata Kunci: Kriptografi, Enkripsi, Video, Algoritma Zigzag, Algoritma AES, AES-256, Python

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah meningkatkan ancaman terhadap keamanan data, seperti kasus kebocoran data pribadi [1], [2]. Kriptografi menjadi solusi utama untuk melindungi data. Salah satu algoritma enkripsi yang unggul adalah Advanced Encryption Standard (AES) karena fleksibilitas panjang kunci dan kecepatan pemrosesan yang cukup tinggi [1], [3], [4], [5]. Namun, AES juga memiliki kelemahan, seperti ketergantungan pada keamanan penyimpanan kunci dan penggunaan sumber daya komputasi yang lebih besar untuk data yang besar [3], [6]. Untuk mengatasi kelemahan keamanan dan penggunaan suber daya komputasi ini, penelitian sebelumnya telah mengusulkan solusi berupa kombinasi algoritma, seperti

penelitian dari Fardianto dkk. yang mengusulkan kombinasi zigzag ciphere dengan vigenere cipher [7], penelitian Handoko dkk. yang mengkombinasi vigenere cipher dengan AES dan hashing [8], dan peneltian Triansyah yang mengkombinasi vigenere cipher dengan AES [9]. Pendekatan ini menginspirasi penelitian ini, yang mengusulkan penggabungan AES-256 dengan Zigzag Cipher, sebuah algoritma transposisi sederhana yang dapat meningkatkan kompleksitas ciphertext.

Penelitian ini mengembangkan hasil dan metode penelitian sebelumnya yang dilakukan oleh Al Tamimi, Mandal, dan Handoko untuk mengevaluasi performa algoritma-algoritma yang diuji, yaitu dari segi kecepatan pemrosesan data / data throughput [3], [4], dan dari segi keamanan enkripsi berdasarkan analisa statistik entropi dan koefisiensi korelasi [8]. Tujuan penelitian ini adalah untuk mengembangkan algoritma enkripsi dan dekripsi dengan memodifikasi AES-256 menggunakan Zigzag Cipher, dan menguji efektivitas modifikasi algoritma dalam mempengaruhi efisiensi proses serta entropi dan koefisien korelasi hasil enkripsi dan dekripsi [3], [4],[8], [10].

2. Metodologi Penelitian

Penelitian ini memfokuskan pada modifikasi algoritma AES-256 dengan penambahan langkah enkripsi Zigzag Cipher. Perbandingan algoritma yang dimodifikasi hanya dilakukan dengan AES-256, bukan algoritma lain. Pengujian dilakukan dengan simulasi menggunakan data video format .mp4, dan implementasi program dibuat dengan bahasa pemrograman Python. Pengujian melibatkan total 5 algoritma, 43 file plaintext, dan 4 password.

Tabel 1 Daftar File Plainteks

File Sumber	File Di uji
Colortest1.mp4	Colortest1.mp4
	colortest1_black.mp4
	colortest1_white.mp4
	colortest1_red.mp4
	colortest1_green.mp4
	colortest1_blue.mp4
	colortest1_grey.mp4
	colortest1_greyscale_brightness.mp4
	colortest1_greyline_horizontal.mp4
	colortest1_greyline_vertical.mp4
	colortest1_grey_checkerboard.mp4
	colortest1_rgb_brightness.mp4
	colortest1_gradient.mp4
Testvid1.mp4	testvid1_0s_to_2s_2s.mp4
	testvid1_0s_to_4s_4s.mp4
	testvid1_0s_to_6s_6s.mp4
	testvid1_0s_to_8s_8s.mp4
	testvid1_0s_to_10s_10s.mp4
	testvid1_0s_to_15s_15s.mp4
	testvid1_0s_to_20s_20s.mp4
	testvid1_0s_to_25s_25s.mp4
	testvid1_0s_to_30s_30s.mp4
	testvid1_0s_to_60s_60s.mp4
Testvid2.mp4	testvid2_0s_to_2s_2s.mp4
	testvid2_0s_to_4s_4s.mp4
	testvid2_0s_to_6s_6s.mp4
	testvid2_0s_to_8s_8s.mp4
	testvid2_0s_to_10s_10s.mp4
	testvid2_0s_to_15s_15s.mp4
	testvid2_0s_to_20s_20s.mp4

p-ISSN: 2301-5373
e-ISSN: 2654-5101

	testvid2_0s_to_25s_25s.mp4
	testvid2_0s_to_30s_30s.mp4
	testvid2_0s_to_60s_60s.mp4
Testvid3.mp4	testvid3_0s_to_2s_2s.mp4
	testvid3_0s_to_4s_4s.mp4
	testvid3_0s_to_6s_6s.mp4
	testvid3_0s_to_8s_8s.mp4
	testvid3_0s_to_10s_10s.mp4
	testvid3_0s_to_15s_15s.mp4
	testvid3_0s_to_20s_20s.mp4
	testvid3_0s_to_25s_25s.mp4
	testvid3_0s_to_30s_30s.mp4
	testvid3_0s_to_60s_60s.mp4

Tabel 2. Daftar Password

Password
password
passwoad
12345678
IlkomUdayana2025

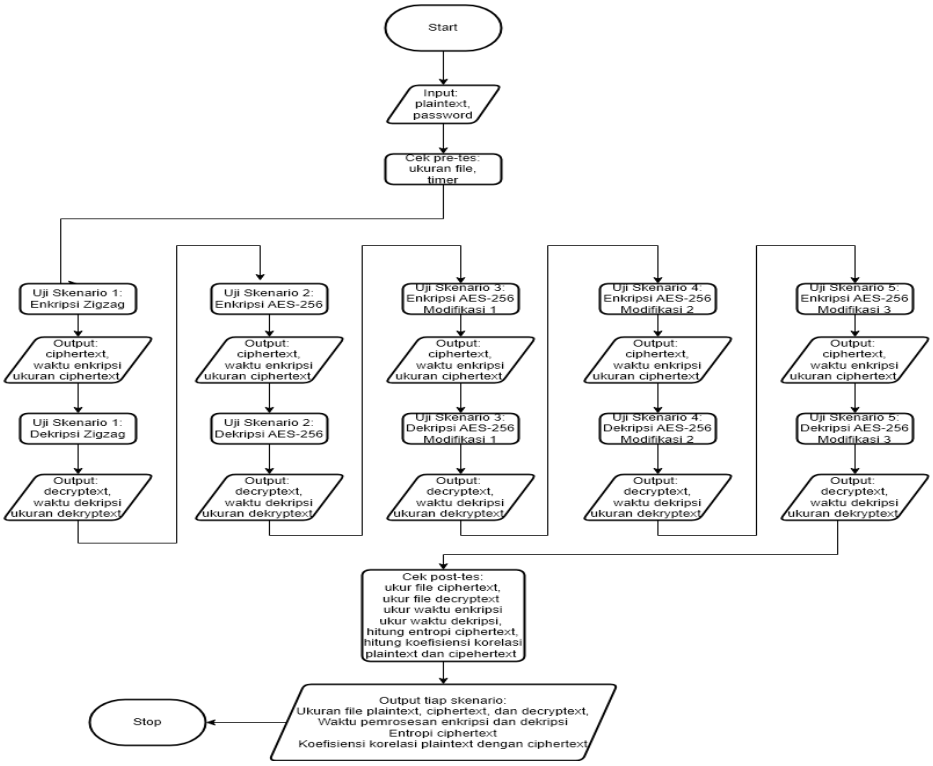
Tabel 3. Daftar Algoritma

Nama Algoritma	Penjelasan
Zigzag	Algoritma zigzag cipher dasar
AES	Algoritma AES-256 dasar
AES Mod 1	Zigzag pada input data AES-256
AES Mod 2	Zigzag pada output data AES-256
AES Mod 3	Zigzag pada input password AES-256

Tabel 4. Data Pengujian

File Plainteks	Password	Jumlah Algoritma	Total Cipherteks
31	4	5	620

Pengujian dilakukan dengan mengikuti langkah berikut:



Gambar 1. Flowchart proses pengujian

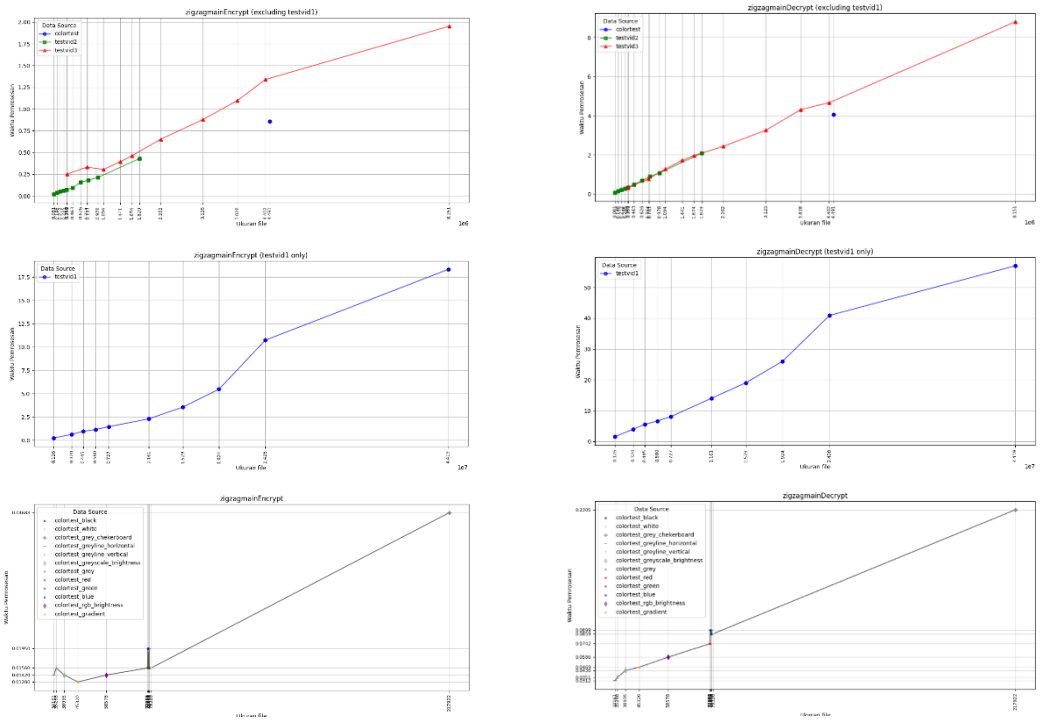
Berdasarkan flowchart di gambar 1 di atas, proses pengujian akan dilakukan dengan cara meng-iterasi setiap skenario pengujian terhadap data input. Setiap pasangan input plaintext dan password akan digunakan untuk menguji 5 skenario enkripsi dan dekripsi. Hasil setiap skenario yang disimpan meliputi ukuran file plaintext (sebelum diproses), ciphertext, dan decryptext (plaintext hasil dekripsi), waktu pemrosesan enkripsi dan dekripsi, pemakaian memory dari pemrosesan enkripsi dan dekripsi, nilai entropi ciphertext dan plaintext, nilai koefisiensi korelasi ciphertext dan plaintext.

3. Hasil dan Pembahasan

Berikut adalah graf hasil pengujian. Data dalam graf adalah nilai dari tiap titik data video yang diproses, dikelompokkan berdasarkan algoritmanya, dan di rata-ratakan berdasarkan passwordnya. Karena rentang datanya sangat berbeda dari rentag data sumber-sumber lainnya, data dari sumber testvid1 dan colortest dipisahkan.

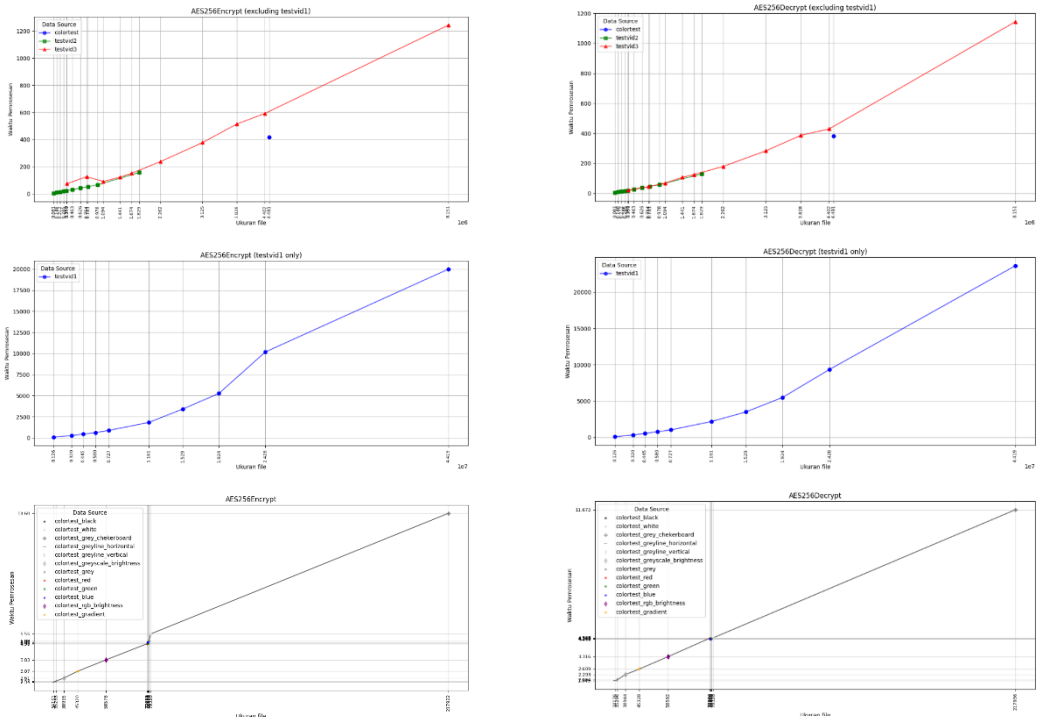
3.1 Pemrosesan Enkripsi dan Dekripsi

p-ISSN: 2301-5373
e-ISSN: 2654-5101



Gambar 2 Graf Waktu Pemrosesan zigzag

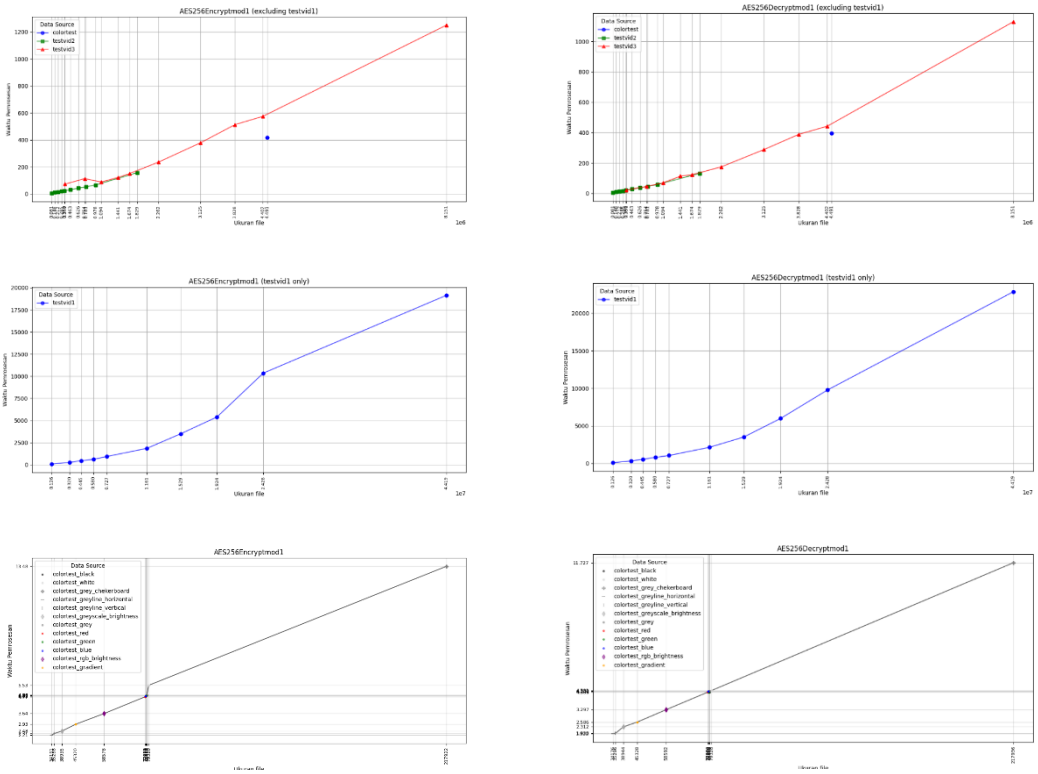
Dapat dilihat pada gambar 2 bahwa peningkatan waktu pemrosesan cenderung konsisten untuk ukuran file berbeda. Waktu pemrosesan meningkat secara linier seiring dengan meningkatnya ukuran file. Untuk video – video dari testvid1, peningkatan waktu pemrosesan sedikit melambat diantara klip 10 detik dan klip 30 detik, atau antara file berukuran 10 megabyte dan 25 megabyte, sebelum kembali ke pola linier sebelumnya.



Gambar 3 Graf Waktu Pemrosesan AES

Dapat dilihat dari gambar 3 diatas, bahwa Algoritma AES bahwa perubahan waktu pemrosesan cenderung konsisten untuk ukuran file berbeda. Waktu pemrosesan meningkat secara linier seiring dengan meningkatnya ukuran file. Untuk klip dari testvid1, peningkatan waktu pemrosesan sedikit melambat diantara klip 10 detik dan klip 30 detik, atau antara file berukuran 10 megabyte dan 25 megabyte, sebelum kembali ke pola penigkatan sebelumnya yang lebih stabil.

Kecepatan pemrosesan mulai rendah, lalu meningkat dan memuncak pada ukuran file 0,9 – 1,2 megabyte, kemudian mulai menurun. Untuk video klip yang mulai dengan ukuran file di atas 1 megabyte, kecepatan pemrosesan nampak menurun seiring dengan penigkatan ukuran file.

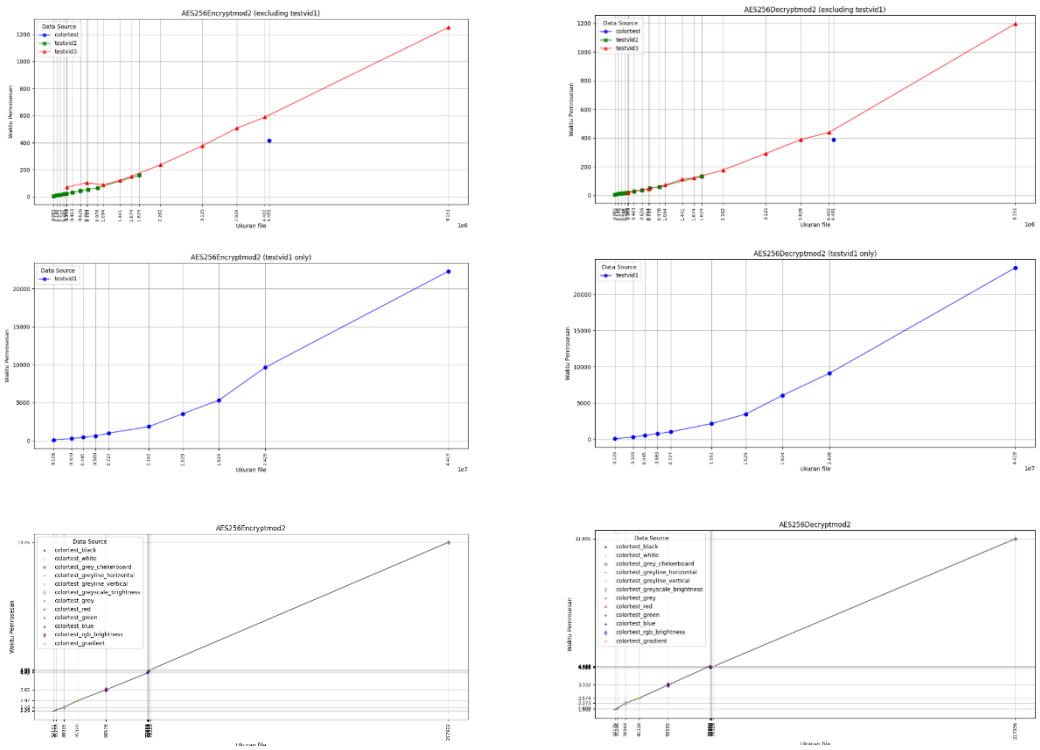


Gambar 4 Graf Waktu Pemrosesan AES Mod 1

Dapat dilihat dari Gambar 4 diatas, bahwa waktu pemrosesan cenderung konsisten untuk ukuran file berbeda. Waktu pemrosesan meningkat secara linier seiring dengan meningkatnya ukuran file. Untuk klip dari testvid1, peningkatan waktu pemrosesan sedikit melambat diantara klip 10 detik dan klip 30 detik, atau antara file berukuran 10 megabyte dan 25 megabyte, sebelum kembali ke pola penigkatan sebelumnya yang lebih stabil.

Kecepatan pemrosesan mulai rendah, lalu meningkat dan memuncak pada ukuran file 0,9 – 1,2 megabyte, kemudian mulai menurun. Untuk video klip yang mulai dengan ukuran file di atas 1 megabyte, kecepatan pemrosesan nampak menurun seiring dengan penigkatan ukuran file.

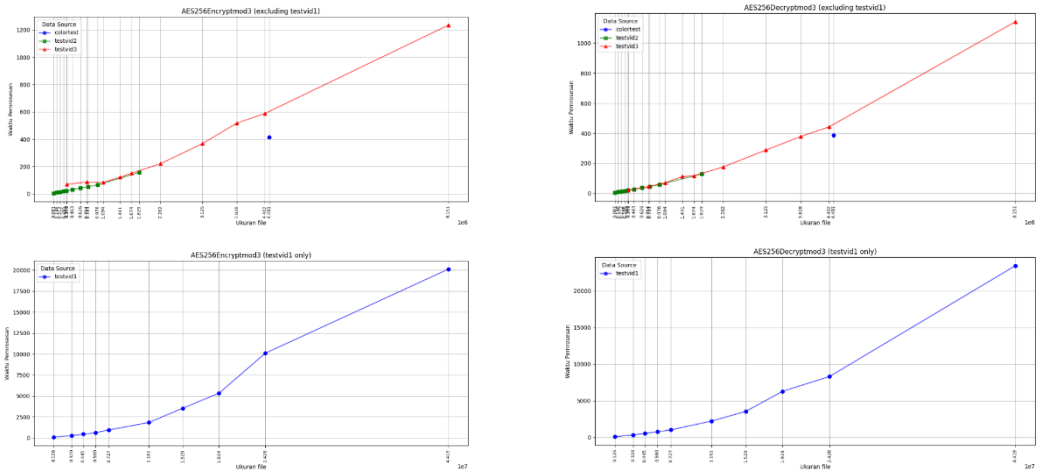
p-ISSN: 2301-5373
e-ISSN: 2654-5101

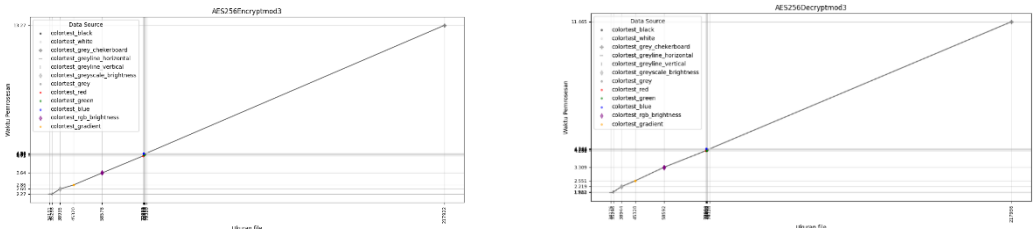


Gambar 5 Graf Waktu Pemrosesan AES Mod 2

Dapat dilihat pada Gambar 5 diatas bahwa waktu pemrosesan cenderung konsisten untuk ukuran file berbeda. Waktu pemrosesan meningkat secara linier seiring dengan meningkatnya ukuran file. Untuk klip dari testvid1, peningkatan waktu pemrosesan sedikit melambat diantara klip 10 detik dan klip 30 detik, atau antara file berukuran 10 megabyte dan 25 megabyte, sebelum kembali ke pola penigkatan sebelumnya yang lebih stabil.

Kecepatan pemrosesan mulai rendah, lalu meningkat dan memuncak pada ukuran file 0,9 – 1,2 megabyte, kemudian mulai menurun. Untuk video klip yang mulai dengan ukuran file di atas 1 megabyte, kecepatan pemrosesan nampak menurun seiring dengan penigkatan ukuran file.





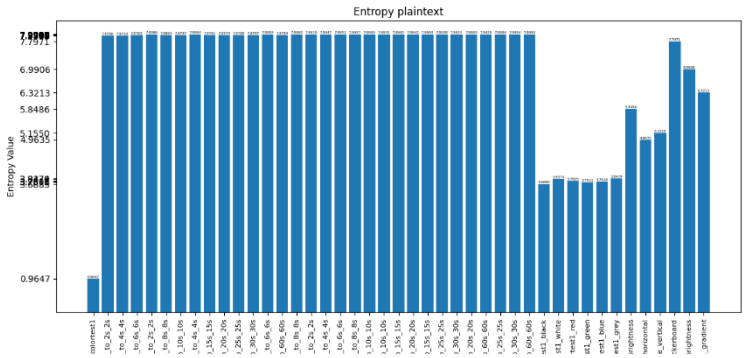
Gambar 6 Graf Waktu Pemrosesan AES Mod 3

Dapat dilihat pada gambar 6 diatas bahwa waktu pemrosesan cenderung konsisten untuk ukuran file berbeda. Waktu pemrosesan meningkat secara linier seiring dengan meningkatnya ukuran file. Untuk klip dari testvid1, peningkatan waktu pemrosesan sedikit melambat diantara klip 10 detik dan klip 30 detik, atau antara file berukuran 10 megabyte dan 25 megabyte, sebelum kembali ke pola penigkatan sebelumnya yang lebih stabil.

Kecepatan pemrosesan mulai rendah, lalu meningkat dan memuncak pada ukuran file 0,9 – 1,2 megabyte, kemudian mulai menurun. Untuk video klip yang mulai dengan ukuran file di atas 1 megabyte, kecepatan pemrosesan nampak menurun seiring dengan penigkatan ukuran file.

3.2 Entropi.

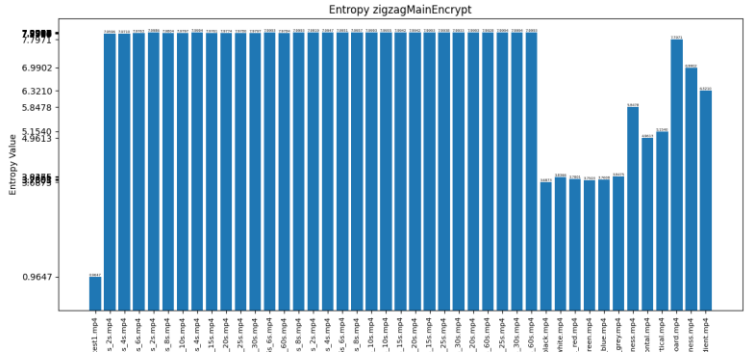
Berikut adalah graf data entropi dari semua plainteks dan cipherteks.



Gambar 7 Entropi Plainteks

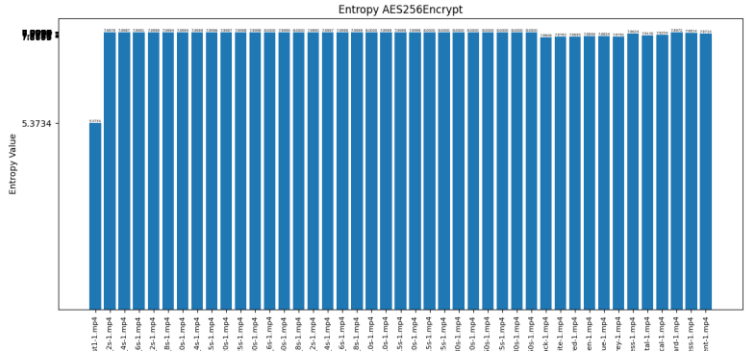
Sebagaimana dapat pada gambar 7, nilai entropi plainteks bervariasi sesuai dengan kompleksitas vide plainteks yang digunakan. Colortest dan variasinya memiliki nilai entropi yang cenderung lebih rendah (>7), sedangakan testvid dan variasinya memiliki entropi yang dekat dengan maksimal (7,99)

p-ISSN: 2301-5373
e-ISSN: 2654-5101



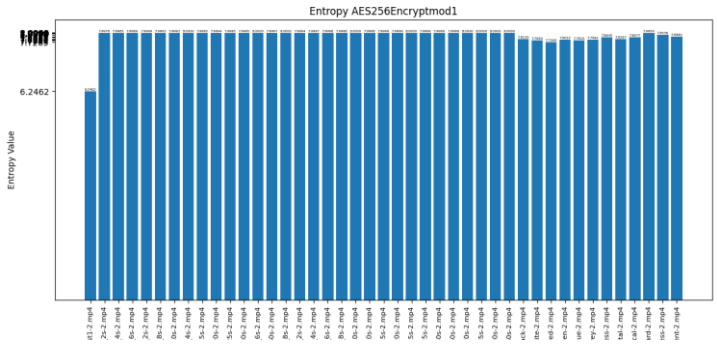
Gambar 8 Entropi Zigzag

Sebagaimana dapat dilihat pada gambar 8, nilai entropi cipherteks hasil enkripsi zigzag adalah sama dengan entropi plainteks.



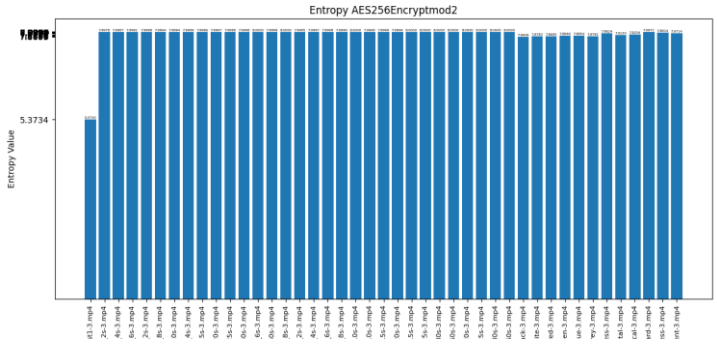
Gambar 9 Entropi AES

Dapat dilihat pada gambar 9, bahwa nilai entropi semua cipherteks meningkat mendekati nilai maksimal, kecuali cipherteks colortest1. Untuk colortest1, nilai entropinya menigkat secara signifikan dari 0,96 menjadi 5,37.



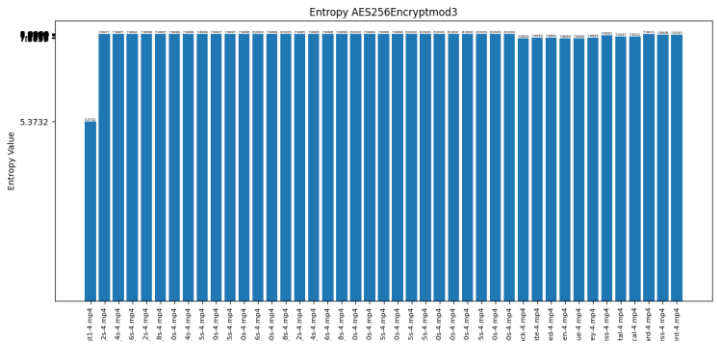
Gambar 10 Entropi AES Mod 1

Dapat dilihat bahwa pada gambar 10, nilai entropi semua cipherteks meningkat mendekati nilai maksimal, kecuali cipherteks colortest1. Untuk colortest1, nilai entropinya menigkat secara signifikan dari 0,96 menjadi 6,24.



Gambar 11 Entropi AES Mod 2

Dapat dilihat pada gambar 11, bahwa nilai entropi semua cipherteks meningkat mendekati nilai maksimal, kecuali cipherteks colortest1. Untuk colortest1, nilai entropinya menigkat secara signifikan dari 0,96 menjadi 5,37.



Gambar 12 Entropi AES Mod 3

Dapat dilihat pada gambar 12, bahwa nilai entropi semua cipherteks meningkat mendekati nilai maksimal, kecuali cipherteks colortest1. Untuk colortest1, nilai entropinya menigkat secara signifikan dari 0,96 menjadi 5,37.

3.3. Koefisien Korelasi.

Berikut adalah tabel rekapitulasi rata rata nilai koefisiensi dari semua sumber dan algoritma.

Tabel 5 Rerata Koefisien Korelasi per Sumber dan Algoritma

Sumber file	Zigzag	AES	AESMod1	AESMod2	AESMod3
Colortest	0,02039739	-0,00640786	0,00757968	0,00016432	0,00444395
Testvid1	0,00020646	-0,00015818	-0,00002606	-0,00003165	0,00004864
Testvid2	0,00117669	0,00114971	0,00026359	-0,00068181	-0,00004546
Testvid3	0,00159160	0,00025032	-0,00032084	-0,00009882	0,00028400
Rata rata	0,00130971	-0,00315938	0,00343016	-0,00007300	0,00207219

Dari tabel diatas, dapat dilihat bahwa AESMod2 mengahsilkan cipherteks dengan nilai korelasi paling dekat dengan nol, artinya paling jauh korelasinya dengan plainteks.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

3.4. Pembahasan

Hasil penelitian yang sudah dilakukan menunjukkan bahwa:

a. Waktu pemrosesan file meningkat secara linier seiring dengan meningkatnya ukuran file.

b. Zigzag Cipher memiliki waktu pemrosesan yang jauh lebih cepat (sekitar 20 kali) dibandingkan AES dan variasinya. Penambahan proses enkripsi Zigzag pada AES, dari AES Mod 1, hingga Mod 3, hanya menambahkan waktu pemrosesan yang relatif kecil (± 0,05% – 2%).

c. Algoritma Zigzag tidak mengubah distribusi frekuensi nilai byte (nilai Shannon Entropy sama dengan plaintext), namun AES dapat menghasilkan nilai entropy lebih tinggi dibandingkan plainteks.

d. Semua algoritma yang diuji berhasil mengubah korelasi antara plaintext dan ciphertext mendekati nilai 0, hingga tiga digit pecahan desimal (0,00x).

e. Algoritma AES Mod 1 adalah algoritma yang menghasilkan peningkatan entropi terbesar (rata rata +1,18%, peningkatan terbesar +67,01%), dan dapat menghasilkan koefisien korelasi dan waktu pemrosesan yang setara dengan algoritma AES dan Modifikasi AES lainnya.

4. Kesimpulan

Penelitian ini menunjukkan bahwa salah satu metode modifikasi algoritma AES yang diusulkan, yaitu AES Mod 1, berhasil meningkatkan nilai Shannon Entropy dari cipherteks dibandingkan algoritma AES dasar, dengan rata rata peningkatan sebesar 1,18% lebih besar dari entropi AES dasar. Semua algoritma AES dan modifikasinya memiliki waktu pemrosesan dan koefisien korelasi yang mirip (variasi waktu pemrosesan ± 0,05% – 2%, dan koefisien korelasi dibawah tiga digit pecahan desimal (0,00x))

Untuk penelitian selanjutnya, disarankan untuk melakukan penelitian lebih dalam mengenai integrasi algoritma AES dan Zigazg, serta meneliti kombinasi algoritma-algoritma lainnya. Penelitian berikutnya juga dapat menambah jumlah dan jenis data yang diuji, tidak hanya video, dan menggunakan metode atau algoritma-algoritma khusus untuk memproses jenis data tertentu. Penelitian berikutnya juga dapat meneliti dampak modifikasi algoritma dengan cara menggabungkan dua atau lebih algortima yang sudah ada dengan menggunakan metode evaluasi yang lebih lengkap, tidak hanya terbatas pada entropi dan koefisien korelasi.

References

[1] Almadira, A., Pratama, Y., & Purwani, F. (2024). Melindungi data di dunia digital: Peran strategis enkripsi dalam keamanan data. Journal of Scientech Research and Development, 6(2), 540–549.
[2] Cyberlands. (2022). Top security breaches in Indonesia. Diakses dari https://www.cyberlands.io
[3] Al Tamimi, A. K. (2006). Performance analysis of data encryption algorithms (Master's thesis). Washington University in St. Louis.
[4] Mandal, P. C. (2012). Evaluation of performance of the symmetric key algorithms: DES, 3DES, AES and Blowfish. Journal of Global Research in Computer Science (JGRCS), 3(8), 67–70.
[5] Sharma, N., Prabhjot, & Kaur, H. (2017). A review of information security using cryptography technique. International Journal of Advanced Research in Computer Science, 8(4), 323–326.
[6] Wiharto, Y., & Irawan, A. (2018). Enkripsi data menggunakan Advanced Encryption Standard 256. Jurnal Kilat, 7(2), 91–98.

[7] Fardianto, F. A. E., Yanto, F., Iskandar, I., & Pizaini. (2023). Kombinasi algoritma kriptografi Vigenere Cipher dengan metode Zig-Zag dalam pengamanan pesan teks. Jurnal Computer Science and Information Technology (CoSciTech), 4(1), 182–192.
[8] Handoko, L. B., & Umam, C. (2022). Kombinasi Vigenere-AES256 dan fungsi hash dalam kriptografi aplikasi chatting. Prosiding Seminar Nasional Sains dan Teknologi, 12(1), 390–397.
[9] Triansyah, H., Pratama, A., Syahputra, F., & Gunawan, I. (2019). Kombinasi kriptografi algoritma Vigenere Cipher dan algoritma AES untuk pengamanan pesan teks. TECHSI, 11(3), 409–418.
[10] Wahyudi, E. N., Ardhianto, E., Handoko, W. T., Murti, H., Supriyanto, E., Lestariningsih, E., & Redjeki, R. S. (2024). Peningkatan keamanan data melalui teknik super enkripsi menggunakan algoritma Vigenere dan Caesar. Jurnal Informatika Polinema, 10(3), 315.