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

Pengamanan Data Kolase Digital Menggunakan Metode Advanced Encryption Standard

I Nyoman Budhiarta Suputra[a1], I Ketut Gede Suhartana[a2]

[a]informatics Department, Faculty of Math and Science, Udayana University
Bali, Indonesia
[1]budhisuputra13@email.com
[2]ikg.suhartana@unud.ac.id

Abstract

Digital Collage is a technique of creating a work of art by sticking or combining several photos into a single unit. technological developments make everything easy, we can easily send files to each other. With the development of technology, collage art has evolved into the digital realm. However, with the ease of disseminating information, digital collage on the internet is very easy to fake or steal. Digital collage requires a digital security to maintain its authenticity and keep it away from irresponsible people. To resolve the problem, a encrypted system was created. This system will use the Advance Encryption Standard method. The encrypted digital collage will provide extra security because only the owner and recipient of the data can see it. From this test it can be concluded that the AES method can be used to encrypt a digital collage.

Keywords: *Digital security, AES, Cryptography, symmetric, digital collage*

1. Pendahuluan

Perkembangan teknologi yang sangat cepat ini memungkinkan seseorang untuk saling mengirim data dengan mudah. Namun karena kemudahan ini keamanan dari data yang di kirimkan sering kali diabaikan. Keamanan data merupakan salah satu aspek penting dalam menjaga kerahasiaan sistem informasi. Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat tidak rahasia dan data yang bersifat rahasia seperti data pribadi. Data yang harus dijaga dengan baik dan benar adalah data yang bersifat pribadi karena jika terjadi kebocoran data atau tersebarnya data tersebut akan berdampak buruk pada diri kita sendiri. Tidak hanya data pribadi saja yang menjadi incaran namun data atau file yang memiliki hak cipta. Ada banyak jenis karya yang memiliki hak cipta salah satunya adalah seni kolase.

Kolase berasal dari bahasa prancis (Collage) yang berarti merekat. Kolase adalah kreasi aplikasi yang dibuat dengan menempelkan bahan-bahan tertentu.[1] Seni kolase merupakan seni yang memerlukan tingkat kreativitas yang sangat tinggi untuk membuat suatu karya yang unik dan berbeda dengan lainnya. Oleh karena itu, kasus plagiarisme sangat susah untuk dihindari. Untuk menanggulangi masalah tersebut penulis berinisiatif membuat sebuah aplikasi enkripsi dengan mengimplementasikan algoritma AES yang dipadukan dengan library *base64.*

Algoritma AES adalah salah satu algoritma kriptografi. Kriptografi merupakan suatu metode pengamanan data yang berfungsi untuk menjaga keaslian dan kerahasiaan dari data itu sendiri. Kriptografi biasanya sering digunakan dalam aktivitas bertukar data agar tidak ada pihak ketiga yang memodifikasi ataupun merusak data yang akan di kirimkan. Didalam kriptografi terdapat proses mengacak pesan disebut dengan *encryption* dan proses untuk mengembalikan pesan yang sudah teracak disebut dengan *decryption*. [2]

2. Metode penelitian

2.1 Algoritma AES

Advanced Encryption Standard (AES) merupakan salah satu algoritma kriptografi yang digunakan untuk mengamankan data. Algoritma AES dapat mengenkripsi data menjadi sebuah *chippertext* yang tidak dapat dibaca dibaca langsung. Untuk melihat data yang terenkripsi kita perlu mendekripsi data tersebut. Proses dekripsi ini akan mengembalikan *chipertext* menjadi data awal atau *plaintext*. Algoritma AES dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. [3]

2.2 Kolase digital

Kolase merupakan sebuah teknik menciptakan sebuah karya seni dengan cara menempel atau menggabungkan beberapa bahan atau objek menjadi satu kesatuan.[4] Seiring perkembangan

teknologi, seni kolase mulai berkembang ke ranah digital. Seni kolase memerlukan kreatifitas dan imajinasi yang tinggi untuk menciptakan karya seni yang menarik dan memiliki keunikannya tersendiri. Kolase digital ini sedikit berbeda dengan kolase konvensional karena bahan yang digunakan dari kolase digital ini adalah gabungan dari beberapa foto atau gambar yang nantinya disatukan menjadi sebuah kesatuan.

2.3 Kriptografi

Kriptografi merupakan suatu metode pengamanan data yang berfungsi untuk menjaga keaslian dan kerahasiaan dari data itu sendiri. Saat pertukaran data Kriptografi memungkinkan informasi hanya diketahui oleh pengirim dan penerima. Cara kerja dari kriptografi adalah mengubah pesan atau data menjadi suatu baris kode dan membuat kunci yang hanya dimiliki oleh pemilik data, kunci inilah yang nanti akan diberikan kepada penerima pesan atau data agar si penerima dapat membaca pesan atau data yang diberikan.

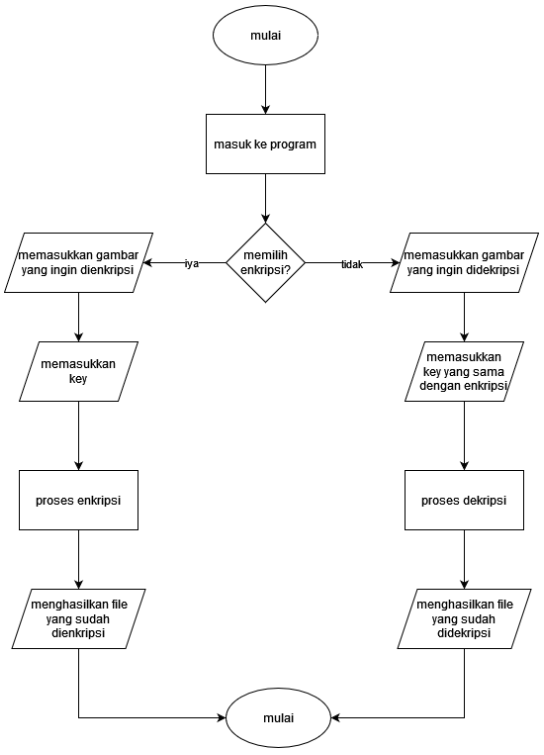
2.4 CFB

Data dienkripsikan dalam unit yang lebih kecil daripada ukuran blok. Unit yang dienkripsikan dapat berupa bit per bit, 2 bit, 3 bit, dan seterusnya. Bila unit yang dienkripsikan satu karakter setiap kalinya, maka mode CFB-nya disebut CFB 8-bit. Secara umum CFB n-bit mengenkripsi *plaintext* sebanyak n bit setiap kalinya, yang mana n = m (m = ukuran blok).[5] Mode CFB memerlukan antrian yang memiliki ukuran yang sama dengan blok input. Algoritma enkripsi dengan mode CFB adalah sebagai berikut:

1. Antrian diisi dengan IV atau *initialization vector.*
2. Enkripsikan antrian dengan kunci K. n bit paling kiri dari hasil enkripsi berlaku sebagai keystream (k_i) yang kemudian diXOR-kan dengan n-bit dari plainteks menjadi n-bit pertama dari *ciphertext*. Salinan (copy) n-bit dari *ciphertext* ini dimasukkan ke dalam antrian (menempati n posisi bit paling kanan antrian), dan semua m-n bit lainnya di dalam antrian digeser ke kiri menggantikan n bit pertama yang sudah digunakan.
3. Lalu terapkan langkah 2 pada bit plainteks.

2.5 Desain system

a. Flowchart system



Gambar 1. alur program

b. Penjelasan

Pada gambar 1 dijelaskan mengenai alur dari program enkripsi menggunakan algoritma AES. Proses enkripsi dan dekripsi dapat dilakukan dengan langkah-langkah berikut:

1. Pertama-tama user memasuki program.
2. User diminta untuk memilih menu yaitu enkripsi atau dekripsi.

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

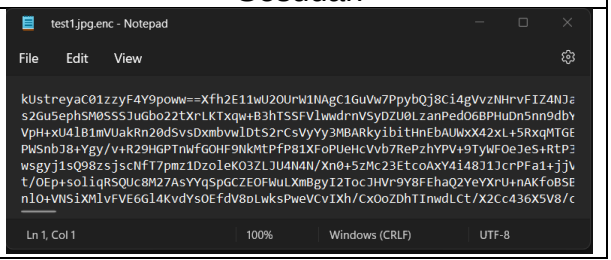
3. Jika user memilih enkripsi maka user akan diminta untuk memasukkan file yang ingin dienkripsi.
4. Lalu user memasukkan key atau password untuk proses enkripsi.
5. Setelah memasukkan key atau password maka proses ekripsi akan dijalan.
6. Setelah berhasil akan dihasilkan file yang sudah di enkripsi.
7. Jika user memilih menu dekripsi user akan diminta memasukkan file yang sudah dienkripsi.
8. Lalu user akan memasukkan key atau password yang sama dengan yang tersematkan di dalam file enkripsi tersebut.
9. Setelah memasukkan password maka file tersebut akan didekripsi.
10. Setelah berhasil akan dihasilkan file yang sudah didekripsi.

3. Hasil dan Pembahasan

3.1 Implementasi Algoritma AES

Metode yang digunakan pada implementasi ini adalah AES yang bersifat simetris untuk melakukan enkripsi terhadap kolase digital atau gambar. Kolase digital yang diinputkan akan dirubah terlebih dahulu ke bentuk text agar dapat dienkripsi. Pengubahan bentuk ini dapat dilakukan dengan mengimport *library base64*, lalu setelah dirubah menjadi text maka akan masuk ke proses enkripsi menggunakan algoritma AES dengan mode CFB. Algoritma ini juga diimport dari *library pycryptodome* yang memiliki banyak fungsi dari enkripsi itu sendiri. alur program adalah sebagai berikut:

a. Enkripsi
   1. Memasukkan nama file (test1.jpg) yang sudah berada pada satu folder.
   2. Jalankan program.
   3. Memasukkan key yang ingin digunakan dalam proses enkripsi.
   4. File berhasil dienkripsi

Sebelum	Sesudah
	

b. Dekripsi
   1. Memasukkan nama file(test1.jpg.enc) yang berada pada satu folder.
   2. Jalankan program.
   3. Memasukkan key yang sudah dibuat pada saat enkripsi.
   4. File berhasil didekripsi

3.2 Pengujian

Dalam pengujian implementasi ini penulis menggunakan data gambar kolase digital sebanyak 8 buah dengan ukuran yang berbeda dan format jpg. Berikut merupakan hasil yang didapatkan:

Nama	Ukuran Awal	Waktu	Hasil
test1.jpg	3mb	0,2sec	4mb
test2.jpg	6mb	0,2sec	8mb
test3.jpg	42mb	2sec	56mb
test4.jpg	41mb	1,4sec	55mb
test5.jpg	7mb	0,4sec	9mb
test6.jpg	8mb	0,4sec	11mb
test7.jpg	4mb	0,2sec	5mb
test8.jpg	5mb	0,2sec	6mb

Table 1. Pengujian Enkripsi

Dari tabel 1 dapat dilihat bahwa ukuran file yang dienkripsi akan bertambah dan waktu enkripsi dari

masing masing file berskala dengan ukuran filenya. Waktu yang tertera pada tabel 1 memperoleh rata-rata 0,62 second. Dilanjutkan dengan pengujian dekripsi dapat dilihat pada tabel berikut:

Nama	Ukuran Awal	Waktu	Hasil
Test1.jpg	4mb	0,1sec	3mb
test2.jpg	8mb	0,2sec	6mb
test3.jpg	56mb	1,2sec	42mb
test6.jpg	55mb	1,2sec	41mb
test7.jpg	9mb	0,2sec	7mb
Test8.jpg	11mb	0,2sec	8mb
Test9.jpg	5mb	0,1sec	4mb
Test10.jpg	6mb	0,2sec	5mb

Tabel 2. Pengujian Dekripsi

Dari data yang ditampilkan pada tabel 2 terlihat bahwa ukuran file setelah dekripsi sama dengan ukuran file sebelum dilakukannya proses enkripsi, namun terdapat sedikit perbedaan dari segi waktu yang diperlukan untuk mendekripsi file yang sudah di enkripsi. Waktu yang diperlukan untuk dekripsi relatif lebih singkat yaitu didapatkan rata-rata 0,42 second.

4. Kesimpulan

Dari penjelasan yang telah dibuat pada bab-bab sebelumnya, dapat disimpulkan bahwa karya seni kolase digital merupakan karya seni dengan tinggat kesulitan yang tinggi karena untuk membuat sebuah karya seni kolase diperlukannya imajinasi dan kreativitas yang sangat tinggi. Data kolase digital bisa disimpan dan dienkripsi menggunakan sistem keamanan kriptografi, yaitu *Advance Encryption Standard*. Pada sistem ini, dilakukan pengujian .enkripsi dan dekripsi dengan masing-masing 8 buah data. Yang diuji adalah waktu yang diperlukan untuk proses enkripsi maupun dekripsi dan ukuran file setelah enkripsi dan dekripsi. Dari hasil pengujian didapatkan waktu rata-rata yang diperlukan untuk mengenkripsi file adalah 0,62 second dan waktu rata-rata yang diperlukan untuk dekripsi adalah 0,42 second. Dari ukuran file terlihat bahwa ukuran file yang dienkripsi mengalami penambahan dan ukuran file setelah didekripsi akan kembali lagi ke ukuran semula sebelum file tersebut mengalami proses enkripsi.

References

[1] N. R. Puspitasari and I. Zultiar, “Penggunaan teknik kolase terhadap kemampuan motorik halus anak usia 5-6 tahun PAUD Warci Jaya tahun ajaran 2017-2018,” *Utile J. Kependidikan*, vol. 4, no. 1, pp. 48–53, 2018.

[2] H. Mukthar, “Kriptografi untuk Keamanan Data,” *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2018.

[3] J. Handoyo and Y. M. Subakti, “Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (Aes),” *J. SITECH Sist. Inf. dan Teknol.*, vol. 3, no. 2, pp. 143–152, 2020, doi: 10.24176/sitech.v3i2.5865.

[4] Y. R. K. Wati, “Digital Repository Repository Universitas Universitas Jember Jember Digital Digital Repository Repository Universitas Universitas Jember Jember,” *Digit. Repos. Univ. Jember*, no. September 2019, pp. 2019–2022, 2017.

[5] C. Lung and R. Munir, “Studi Dan Implementasi Advanced Encryption Standard Dengan Empat Mode Operasi Block Cipher,” pp. 1–10, 1997.