Implementasi *S-box Dinamis* Guna Meningkatkan Keamanan Gambar Melalui *Randomize* 8-bit Konstanta Tambahan

Rafli Hillan Yufandani[1], Alamsyah[2]

[1,2]Jurusan Ilmu Komputer, FMIPA, Universitas Negeri Semarang
Email :[1]hillan693@students.unnes.ac.id, [2]alamsyah@mail.unnes.ac.id

Abstrak

Kemajuan di bidang teknologi informasi telah memungkinkan adanya interaksi antar pengguna melalui jaringan komputer. Interaksi tersebut tidak luput dari penggunaan komunikasi gambar. Pengiriman gambar menggunakan internet melalui jaringan *wireless* terutama jika didistribusikan melalui jaringan internet aplikasi chatting seperti *whatsapp, telegram*, dan media *e-mail* rawan terhadap penyerangan dan penyadapan. Algoritma AES (*Advanced Encryption Standar*) merupakan solusi dari ancaman serangan. Namun, meskipun algoritma AES telah diakui sebagai algoritma dengan kompleksitas tinggi karena memiliki *s-box* tetapi masih memiliki kelemahan terhadap serangan *differensial cryptanalysis*. Kerentanan algortima pada AES terletak pada penggunaan *s-box* statis, sehingga perlu adanya peningkatan kekuatan *s-box* dengan memodifikasi desain dan aljabar pada konstruksi *s-box*. Pada penelitian sebelumnya sempat membahas terkait dengan peningkatan keamanan algoritma AES menggunakan modifikasi transformasi *ShiftRows* dan *s-box* dinamis. Selain itu, terdapat penelitian lain tentang *s-box* dengan memodifikasi pada konstruksi *s-box* menggunakan *Irreducible Polynomial* dan 8-bit konstanta tambahan yang dinilai mengungguli metode kontruksi *s-box* lain yang ada. Pada penelitian ini, metode yang diusulkan menggunakan modifikasi algoritma AES, algoritma AES membutuhkan dua proses yaitu penginputan multiplication inverse dan matriks affine, modifikasi algoritma terletak pada *s-box* lebih spesifiknya modifikasi pada bagian konstruksi *s-box* dengan melakukan pengacakan 8-bit konstanta tambahan untuk keamanan citra digital. Pengacakan 8-bit konstanta tambahan dilakukan dengan cara menginputkan 16 macam *s-box* dengan nilai hexa decimal bernilai 00 sampai dengan 0F atau dalam decimal dari 0 sampai dengan 15. Hasil penelitian menunjukkan bahwa metode yang digunakan berhasil diimplementasikan untuk meningkatkan keamanan enkripsi gambar.

Kata Kunci: s-box, AES, *matriks affine*

Abstract

Advances in information technology have supported the interaction between users through computer networks. This interaction does not escape the use of image communication. Sending images using the internet via wireless networks, especially if distributed through internet networks, chat applications such as whatsapp, telegram, and e-mail media are prone to attacks and eavesdropping. The AES (Advanced Encryption Standard) algorithm is a solution to the threat of attacks. However, although the AES algorithm has been recognized as an algorithm with high complexity because it has an s-box, it still has weaknesses against differential cryptanalysis attacks. The vulnerability of the AES algorithm lies in the use of static s-box, so it is necessary to increase the strength of s-box by modifying the design and algebra of the s-box construction. In a previous study, we discussed about improving the security of the AES algorithm using modified ShiftRows transformations and dynamic s-box. In addition, there are other studies on s-box by modifying the s-box construction using Irreducible Polynomial and 8-bit additional

constants which are considered to outperform other existing s-box construction methods. In this study, the proposed method uses a modified AES algorithm, the AES algorithm requires two processes, namely inputting multiplication inverse and affine matrix, the modification of the algorithm lies in the s-box, more specifically modifications to the s-box construction section by randomizing an additional 8-bit constant to digital image security. Randomization of additional 8-bit constants is done by inputting 16 kinds of s-boxes with hexa decimal values of 00 to 0F or in decimal from 0 to 15. The results showed that the method used was successfully implemented to improve the security of image encryption.

***Keyword**: s-box, AES, affine matrics*

1. PENDAHULUAN

Kemajuan di bidang teknologi informasi telah memungkinkan institusi-institusi pendidikan atau lainnya melakukan interaksi dengan pengguna melalui jaringan komputer. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak, oleh karena itu dibutuhkan suatu keamanan data untuk membantu menjaga informasi. Aspek keamanan data sebenarnya meliputi banyak hal yang saling berkaitan. Pada 2019, Badan Siber dan Sandi Negara (BSSN) melaporkan 290 juta kasus serangan siber. Jumlah tersebut 25% lebih banyak jika dibandingkan tahun sebelumnya ketika kejahatan siber menyebabkan kerugian sebesar US$ 34,2 miliar di Indonesia [1]. Hal yang didapatkan dari serangan siber yaitu segala bentuk informasi baik berupa teks maupun visual seperti audio dan gambar.

Gambar atau citra melengkapi bahasa lisan dan tulisan dalam menjelaskan keberadaan suatu obyek, sehingga citra memiliki peran yang sangat besar dalam dunia modern [2]. Interaksi antar pengguna melalui jaringan komputer tidak luput dari penggunaan komunikasi gambar. Pengiriman gambar menggunakan internet melalui jaringan *wireless* terutama jika didistribusikan melalui jaringan internet aplikasi chatting seperti *whatsapp, telegram,* dan media *e-mail* rawan terhadap penyerangan dan penyadapan. Maka dari itu, diperlukan sebuah tindakan peningkatan keamanan data untuk melindungi informasi pada citra digital dengan menggunakan penerapan ilmu penyandian atau kriptografi.

Paar dan Pelzl dalam bukunya berujudul *"Understanding Cryptography"*, kriptografi adalah ilmu penulisan rahasia dengan tujuan menyembunyikan arti dari pesan [3]. Salah satu teknik kriptografi modern adalah algoritma AES (*Advanced Encryption Standar*) yang telah diakui sebagai algoritma dengan kompleksitas tinggi karena memiliki s-box tetapi masih memiliki kelemahan terhadap serangan *differensial cryptanalysis*. Kerentanan algortima pada AES terletak pada penggunaan *s-box statis*, sehingga perlu adanya peningkatan kekuatan *s-box* dengan memodifikasi desain aljabar pada konstruksi *s-box* dan menggunakan metode s-box dinamis.

2. METODE

2.1. Metode Penelitian

Penelitian-penelitian ini mendasari dari penyusunan algoritma AES, penerapan algoritma AES dalam keamanan citra digital dengan menggunakan *affine mapping* [4–6] dan metode *S-box dinamis* yang digunakan [7].

Menurut Parthebann dan kavitha dalam penelitiannya menjelaskan bahwa metode cipher blok pada AES menyediakan blok dan panjang kunci 128, 192 dan 256. Di AES, pada dasarnya ada empat transformasi untuk setiap putaran, tidak termasuk transformasi MixColumns untuk putaran terakhir. Mode operasi dasar adalah *SubBytes, ShiftRows, MixColumns,* dan *AddRoundkeys* [8].

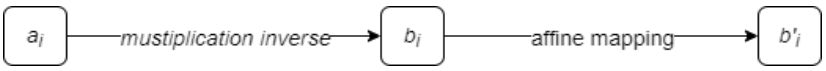
Dalam beberapa tahun terakhir, beberapa teknik baru untuk desain konstruksi *s-box* telah dikembangkan pada sistem keamanan data pesan teks berbasis perangkat seluler android menggunakan standar enkripsi lanjutan dengan *s-box dinamis*, dalam penelitiannya Akhmad dan Alamsyah menggunakan operasi XOR dari transformasi affine dengan matriks elemen biner 8-bit yang disusun dan secara acak menghasilkan sebanyak 256 s-box dan hasil dari penelitian tersebut menghasilkan bahwa *s-box* dinamis dari aplikasi *chat* AES dapat berjalan dengan baik dan dapat mengenkripsi teks pesan menjadi *ciphertext* dan mendekripsi *ciphertext* menjadi pesan asli [9].

2.1.1 Kriptografi

Kriptografi merupakan keahlian dan ilmu dari cara-cara untuk komunikasi aman pada kehadirannya di pihak ketiga. Dalam buku Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi [9] kriptografi dibedakan menjadi dua jenis yaitu kriptografi klasik dan kriptografi modern. AES merupakan kriptografi modern. Penjelasan tentang AES secara detail pada bagian selanjutnya.

2.1.2 Advanced Encryption Standar (AES)

Advanced Encryption Standard (AES) adalah jenis algoritma kriptografi yang berciri simetris dan *cipher block*, algoritma ini menggunakan kunci yang sama pada saat enkripsi dan dekripsi serta input dan output berupa blok dengan jumlah sama. AES memiliki empat konversi data: *Substitusi Bytes (SubBytes) / Inverse SubBytes (Inv SubBytes), ShiftRow / Inverse ShiftRow (Inv ShiftRow), MixColumn / Inverse MixColumn (Inv MixColumn),* dan *AddRoundkey* [10]. Algoritma AES memerlukan s-box untuk melakukan proses pengacakan. Proses pembentukan s-box pada AES meliputi dua proses yaitu multlipication inverse dalam GF (2^8) dan proses affine mapping sebagaimana tercantum pada Gambar 2.1.



Gambar 1. Proses Pembentukan s-box

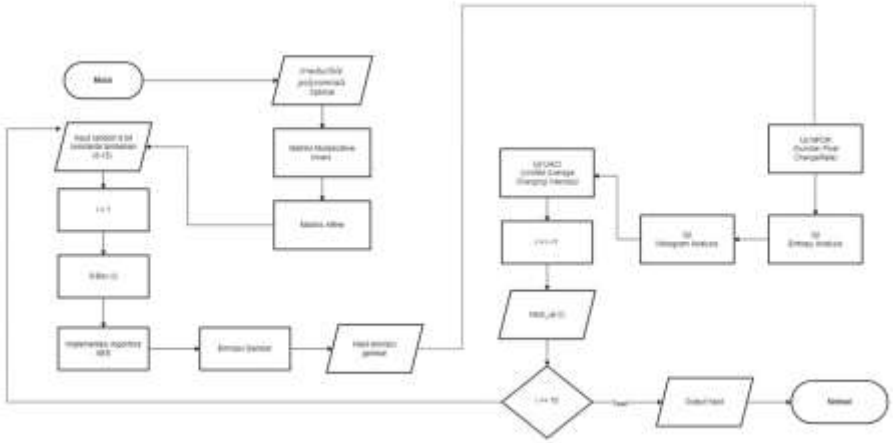
ISSN: 2614-1205

2.1.3 S-box Dinamis

S-box dinamis adalah matriks yang berisi substitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit lainnya. variabel matriks affine dan konstanta bit tambahan selama proses affine mapping dilakukan secara acak dari 0 – 255. Pada S-box dinamis menggunakan *irreducible polynomial* yaitu $x^8 + x^6 + x^5 + x + 1$.

3. HASIL DAN PEMBAHASAN

Metode yang digunakan pada modifikasi s-box dinamis pada dengan melakukan pengacakan 8-bit konstanta tambahan sebagaimana yang tercantum pada Gambar 2.



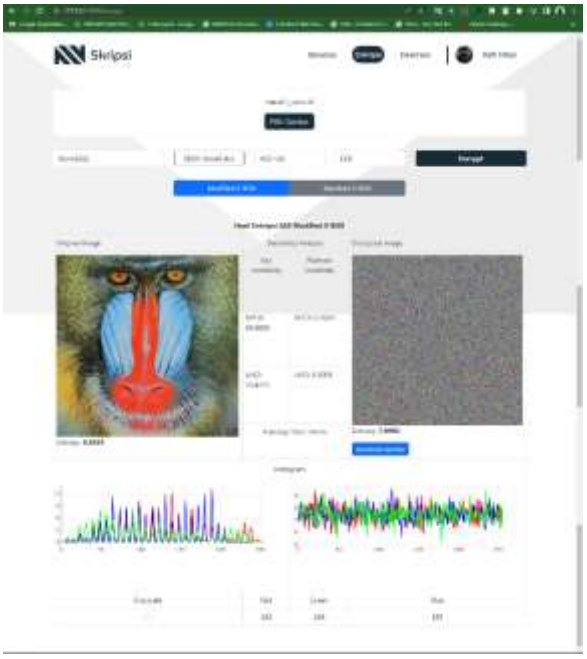
Gambar 2. Diagram alur algoritma S-Box pada AES

Langkah awal yang dilakukan dengan menginputkan nilai input *irreducible polinomial* optimal. Setelah *irreducible polynomial* optimal berhasil dimasukkan, maka dibuatlah matriks *multiplicative inverse*. Selanjutnya dilakukan proses input matriks affine, dan terakhir dilakukan pengacakan atau randomize 8-bit konstanta tambahan. Pengacakan dilakukan 16 macam *s-box* dengan nilai *hexa decimal* bernilai 00 sampai dengan 0F atau dalam decimal dari 0 sampai dengan 15 dan diubah ke dalam biner, kemudian dimasukkan konstruksi s-box bersifat dinamis kemudian diimplementasikan ke dalam algorima AES dan lakukan analisis pengujian.

Implementasi hasil enkripsi gambar ini menggunakan bahasa pemrograman python dan library flask untuk enrkipsi gambar.

Gambar 3.2 User Interface Enkripsi Gambar

Diberikan dua buah alur dalam kriptografi yaitu enkripsi dan deskripsi, Proses penyandian pesan asli (plaintext) menjadi berkas teks tersandi yang dirahasiakan (chippertext) disebut proses enkripsi, sedangkan proses mengembalikan pesan tersandi yang dirahasikan (chippertext) menjadi teks asli (plaintext) disebut deskripsi.



Gambar 3.3 Hasil Enkripsi Gambar

Dengan melakukan modifikasi pada 16 s-box yang berbeda maka diperoleh nilai enkripty, UACI, NPCR, dan histogram analisis pada setiap citra sama dan responsive timenya berbeda beda karena s-box akan mempengaruhi hasil *runnig time* dalam proses enkripsi gambar tersebut.

4. SIMPULAN

Dengan diterapkannya modifikasi s-box dinamis pada AES dengan melakukan pengacakan 8-bit konstanta tambahan dapat meningkatkan keamanan algoritma AES sehingga keamanan suatu citra akan terjaga. Keberhasilan suatu citra dinilai dari uji metode analisis nilai NPCR (number pixelchange rate), UACI, entropy, dan histogram analisis, hasil uji citra menunjukan bahwa nilai metode analisis di nilai yang optimal sehingga dapat dikatakan citra akan semakin aman dan sulit untuk dilakukan serangan *differensial cryptanalysis*.

5. REFERENSI

[1] Anjani, Noor H. "Perlindungan Keamanan Siber di Indonesia." Center for Indonesian Policy Studies, 2021.
[2] Istanto, F. H. Gambar Sebagai Alat Komunikasi Visual. *Nirmana*, 2, 23–35, 2000.
[3] Paar, C., & Pelzl, J. *Cryptography*, *Understanding* (Second Edi). Germany: Springer, 2009. https://doi.org/10.1007/978-3-642-04101-3
[4] Alamsyah, A Bejo, dan T B Adji. "*Enhancement strict avalanche criterion value in robust S-boxes construction using selected irreducible polynomial and affine matrixes*", J. Phys.: Conf. Ser. 1321 032020, 2019.
[5] D. Topanto dan A. Alamsyah, "*Security Improvement Of Aes Algorithm Using S-Box Modification Based On Strict Avalanche Criterion On Image Encryption*", J. Soft Comput. Explor., vol. 3, no. 1, pp. 55-61, 2022.
[6] Alamsyah, Alamsyah. "*A Novel Construction of Perfect Strict Avalanche Criterion S-box using Simple Irreducible Polynomials*." Scientific Journal of Informatics, 2020
[7] Alamsyah, B Prasetiyo, dan M N Ardian." *Enhancement security AES algorithm using a modification of transformation ShiftRows and dynamic S-box*", J. Phys.: Conf. Ser. 1567 032025, 2020.
[8] Partheeban, P., & Kavitha, V. *Dynamic key dependent AES S-box generation with optimized quality analysis.* Cluster Computing, 22(s6), 14731–14741, 2019. https://doi.org/10.1007/s10586-018-2386-6.
[9] Arius D. "Pengantar ilmu kriptografi : Teori, analisis dan implementasi", Yogyakarta : Penerbit Andi, 2008
[10] Daemen J dan dan Rijmen V. "*The Design of Rijndael: AES - The Advanced Encryption Standard* ", Springer, 2012.