17/S/TEKKOM-KCBR/PK.03.08/22/JULI/2024

PENERAPAN TEKNIK STEGANOGRAFI DENGAN METODE *GRAPHSTEGA* DAN KRIPTOGRAFI AES BERBASIS APLIKASI WEB

SKRIPSI

diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer

oleh

Muhammad Radya Wiguna

NIM 2005548

PROGRAM STUDI TEKNIK KOMPUTER

KAMPUS UPI CIBIRU

UNIVERSITAS PENDIDIKAN INDONESIA

2024

HALAMAN HAK CIPTA

PENERAPAN TEKNIK STEGANOGRAFI DENGAN METODE *GRAPHSTEGA* DAN KRIPTOGRAFI AES BERBASIS APLIKASI WEB

Oleh

Muhammad Radya Wiguna

Sebuah Skripsi yang Diajukan untuk Memenuhi Salah Satu Syarat Memperoleh Gelar Sarjana Teknik pada Program Studi S1 Teknik Komputer

HALAMAN PENGESAHAN SKRIPSI

MUHAMMAD RADYA WIGUNA

PENERAPAN TEKNIK STEGANOGRAFI DENGAN METODE *GRAPHSTEGA* DAN KRIPTOGRAFI AES BERBASIS APLIKASI WEB

disetujui dan disahkan oleh pembimbing:

Pembimbing I

Dr. Eng. Munawir, S.Kom., M.T.

NIP. 920200819851205101

Pembimbing II

Deden Pradeka, S.T., M.Kom.

NIP. 920200419890816101

Mengetahui,

Ketua Program Studi Teknik Komputer

Deden Pradeka, S.T., M.Kom.

NIP. 920200419890816101

PENERAPAN TEKNIK STEGANOGRAFI DENGAN METODE *GRAPHSTEGA* DAN KRIPTOGRAFI AES BERBASIS APLIKASI WEB

Muhammad Radya Wiguna

2005548

ABSTRAK

Perkembangan teknologi komputer yang semakin pesat menuntut peningkatan sistem keamanan yang berkelanjutan untuk melindungi data dari potensi ancaman. Penelitian ini mengembangkan sebuah aplikasi berbasis web yang mengintegrasikan teknik steganografi dengan metode *Graphstega* dan AES, dengan tujuan untuk mengurangi kemungkinan *file* yang dienkripsi dapat diidentifikasi dan meningkatkan keamanan *ciphertext*. Dalam penelitian ini, *Design Research Methodology* (DRM) digunakan untuk mengidentifikasi masalah secara sistematis dan mengembangkan solusi, sementara *System Development Life Cycle* (SDLC) diterapkan pada desain, implementasi, dan evaluasi aplikasi. SDLC terdiri dari tahap-tahap berikut: analisis kebutuhan, desain, implementasi, pengujian, dan pemeliharaan. Hal ini memastikan bahwa solusi yang dikembangkan tidak hanya bersifat teoritis tetapi juga praktis dan efektif. Hasilnya menunjukkan keefektifan proses enkripsi dan dekripsi, dengan sedikit perubahan pada teks sumber yang menghasilkan modifikasi yang signifikan pada *ciphertext*. Hasil eksperimen mengkonfirmasi keefektifan *Advanced Encryption Standard* (AES), yang menunjukkan bahwa satu perubahan karakter menghasilkan perubahan 77-bit, atau sekitar 60% dari total bit dan juga waktu yang sangat lama untuk pengujian *bruteforce* dengan jumlah perangkat hingga 5 milliar masih menunjukan waktu yang sangat lama yaitu 7.94×10^{19}. Indeks kepuasan pengguna menunjukkan keefektifan steganografi dalam menyembunyikan informasi tanpa menimbulkan kecurigaan, dengan skor kepuasan rata-rata 79,01%. Penelitian ini menyoroti nilai integrasi AES dan *Graphstega* dalam steganografi untuk memperkuat keamanan data di lingkungan pembelajaran *online*, serta pentingnya teknologi keamanan yang kuat dalam menjaga data di era digital.

Kata Kunci: AES; Steganografi; *Graphstega*; Aplikasi Web

APPLICATION OF STEGANOGRAPHY TECHNIQUE WITH GRAPHSTEGA METHOD AND WEB APPLICATION BASED AES CRYPTOGRAPHY

Muhammad Radya Wiguna

2005548

ABSTRACT

The fast-paced development of computer technology means that security systems need to be constantly improved to protect data from potential threats. This research develops a web-based application that combines steganography techniques with Graphstega and AES *methods. The aim is to make it harder to identify encrypted files and make ciphertext more secure. This research uses Design Research Methodology (DRM) to identify problems and develop solutions in a systematic way. The System Development Life Cycle (SDLC) is used to design, implement and evaluate the application. The SDLC has these stages: requirement analysis, design, implementation, testing, and maintenance. This means the solution we come up with is not just theoretical, but also practical and effective. The results show that the encryption and decryption process works well, even with minor changes to the source text that result in significant modifications to the ciphertext. The results show that the Advanced Encryption Standard (*AES*) is effective. A single character change affects 77 bits, which is about 60% of the total. Even with up to 5 billion devices, bruteforce testing takes a very long time: 7.94 x* 10^{19}*. The user satisfaction index shows that steganography is an effective way to hide information without raising suspicion, with an average satisfaction score of 79.01%. This research shows the value of integrating* AES *and Graphstega in steganography to strengthen data security in online learning environments, as well as the importance of strong security technologies in safeguarding data in the digital age.*

Keywords: AES*; Steganography; Graphstega; Web Application*

DAFTAR ISI

DAFTAR PUSTAKA

Arif, M. (2022, Juni). Profil Internet Indonesia 2022. *SRA Consulting. https://online.fliphtml5.com/rmpye/ztxb/#p=1*

Ashari, I. F., & Munir, R. (2018). Graph Steganography Based on Multimedia Cover to Improve Security and Capacity. *2018 International Conference on Applied Information Technology and Innovation (ICAITI)*, 194–201. https://doi.org/10.1109/ICAITI.2018.8686741

Desoky, A. (2016). *Noiseless Steganography: The Key to Covert Communications*. https://doi.org/10.1201/b11575

Handoyo, J., & Subakti, Y. M. (2020). Keamanan dokumen menggunakan algoritma *Advanced Encryption Standard* (AES). *SITECH*, 3(2), Desember 2020. P-ISSN: 2615-8531, E-ISSN: 2622-2973. http://www.jurnal.umk.ac.id/sitech

Hermansa, H., Umar, R., & Yudhana, A. (2020). Pangamanan pesan menggunakan kriptografi CAESar Cipher dan steganografi EOF pada citra. Jurnal Sains Komputer & Informatika (J-SAKTI), 4(1), 157-169. ISSN: 2548-9771, E-ISSN: 2549-7200. http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Hendarsih, I. (2016). Analisis perubahan harga saham dengan menggunakan grafik candlestick (Nomor 2). MONETER, 3(2), Oktober 2016.

Karuppiah, M., Ramanujam, S., & Professor, A. (2011). Designing an algorithm with high *Avalanche Effect*. Dalam *IJCSNS International Journal of Computer Science and Network Security* (Vol. 11, Nomor 1). https://www.researchgate.net/publication/266468045

Kumar, A. (2012). Effective Implementation and *Avalanche Effect* of AES. *International Journal of Security, Privacy and Trust Management*, *1*(3), 31–35. https://doi.org/10.5121/ijsptm.2012.1303

Kurnia Nurhareza, I., & Siswanto, S. (2022). Penerapan algoritma kriptografi AES 256 untuk mengamankan dokumen berbasis web pada Kelurahan Belendung. In *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*. Jakarta, Indonesia, 06 September 2022.

Muttaqin, K., & Rahmadoni, J. (2020). ANALYSIS AND DESIGN OF FILE SECURITY SYSTEM AES (ADVANCED ENCRYPTION STANDARD) CRYPTOGRAPHY BASED. Dalam *Journal of Applied Engineering and Technological Science* (Vol. 1, Nomor 2).

Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma *Advanced Encryption Standard* (AES) 128 Untuk Enkripsi dan Dekripsi *File*

Dokumen. *Eksplora Informatika*, *8*(1), 52. https://doi.org/10.30864/eksplora.v8i1.139

Pujianto, Y. R. (2016). Perancangan dan implementasi aplikasi kriptografi algoritma AES-128 pada *file* dokumen. Program Studi Teknik Informatika FTI-UKSW. http://repository.uksw.edu/handle/123456789/11377

Sulfikar, S., & Qammaddin, Q. (2020). Keamanan data pembelajaran *online* jaringan komputer di perguruan tinggi. *Jurnal Instruksional*, 2(1), 35-40. https://doi.org/10.24853/instruksional.2.1.35-40

Munir, R. (2019). *Kriptografi* (2nd ed.). Bandung: Informatika.

Munir, R. I. (2020). Kripto 20: *Advanced Encryption Standard* (AES) [Video]. YouTube. https://youtu.be/4q3bA0W7UHg?si=0LYyzdmIu2fniv3U

Hossen, M., Islam, M., & Rahman, M. (2020, October). A new approach to hiding data in the images using steganography techniques based on AES and RC5 algorithm cryptosystem. In *Proceedings of the 2020 International Conference on Smart Electronics and Communication (ICOSEC)*. Trichy, India.

Verma, A., Khatana, A., & Chaudhary, S. (2017). A Comparative Study of Black Box Testing and White Box Testing. *International Journal of Computer Sciences and Engineering*, *5*(12), 301–304. https://doi.org/10.26438/ijcse/v5i12.301304

Verma, R., & Sharma, A. K. (2020). Cryptography: Avalanche effect of AES and RSA. *International Journal of Scientific and Research Publications (IJSRP)*, *10*(4), p10013. https://doi.org/10.29322/ijsrp.10.04.2020.p10013

Widodo, B. E., & Purnomo, A. S. (2020). IMPLEMENTASI ADVANCED ENCRYPTION STANDARD PADA ENKRIPSI DAN DEKRIPSI DOKUMEN RAHASIA DITINTELKAM POLDA DIY. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69–77. https://doi.org/10.20884/1.jutif.2020.1.2.21