OPTIMALISASI KEAMANAN KUNCI ENKRIPSI VIGENERE CHIPER PADA PESAN RAHASIA GAMBAR STEGANOGRAFI DENGAN MD5

Asep Suryanta[1], Yohanes Dwi Cahyono[1] dan Eko Heri Susanto[2]

[(1)]Poltekad Kodiklatad
Jl. Raya Anggrek, Desa Pendem, Kec. Junrejo, Kota Batu, Jawa Timur 65324
[(2)]Institut Teknologi Nasional
Jl. Khp Hasan Mustopa No.23, Neglasari, Kec. Cibeunying Kaler, Kota Bandung, Jawa Barat 40124
zenirakal@gmail.com, yohanes@poltekad.ac, ekoheri@gmail.com

ABSTRAK

Penelitian ini membahas pentingnya optimalisasi keamanan kunci enkripsi Vigenere Cipher pada pesan rahasia gambar steganografi dengan menggunakan algoritma MD5. Melalui kombinasi Vigenere Cipher dan MD5, tingkat keamanan pesan rahasia dapat ditingkatkan. Penggunaan algoritma MD5 sebagai fungsi hash membantu melindungi pesan rahasia dari akses tidak sah dan peretasan. Meskipun MD5 memiliki kerentanan tertentu, penggunaannya dalam konteks pengujian perangkat lunak menunjukkan efektivitas dalam memperkuat keamanan pesan rahasia. Secara keseluruhan, optimalisasi keamanan kunci enkripsi Vigenere Cipher dengan MD5 sangat penting untuk meningkatkan keamanan informasi dalam steganografi.

Kata Kunci: *Steganografy, Vigenere Cipher, algoritma MD5*

PENDAHULUAN

Steganografi adalah teknik penyembunyian pesan rahasia dalam media yang tidak mencurigakan, seperti gambar atau audio. Dalam era digital saat ini, steganografi menjadi semakin penting dalam menjaga keamanan informasi. Namun, pesan rahasia yang disembunyikan dalam media tersebut masih rentan terhadap serangan dan peretasan [1].

Oleh karena itu, diperlukan teknik enkripsi yang kuat untuk melindungi pesan rahasia tersebut. Salah satu teknik enkripsi yang kuat adalah Vigenere Cipher, yang menggunakan kunci enkripsi untuk mengacak pesan rahasia. Namun, Vigenere Cipher juga rentan terhadap serangan dan peretasan jika kunci enkripsi tidak diatur dengan baik. Artikel ini akan membahas tentang optimalisasi keamanan kunci enkripsi Vigenere Cipher pada pesan rahasia gambar steganografi dengan menggunakan algoritma MD5.

Dalam artikel ini, akan dijelaskan tentang konsep dasar steganografi, Vigenere Cipher, dan algoritma MD5.Selain itu, artikel ini juga akan membahas tentang implementasi dan pengujian dari teknik enkripsi yang diusulkan. Diharapkan artikel ini dapat memberikan wawasan dan solusi dalam meningkatkan keamanan pesan rahasia dalam media steganografi [2].

Pesan rahasia dalam gambar steganografi perlu dienkripsi untuk menjaga kerahasiaan pesan tersebut. Steganografi adalah teknik penyembunyian pesan rahasia dalam media yang tidak mencurigakan, seperti gambar atau audio. Pesan rahasia yang disembunyikan dalam media tersebut masih rentan terhadap serangan dan peretasan. Oleh karena itu, diperlukan teknik enkripsi yang kuat untuk melindungi pesan rahasia tersebut. Salah satu teknik enkripsi yang kuat adalah Vigenere Cipher, yang menggunakan kunci enkripsi untuk mengacak pesan rahasia.

Namun, Vigenere Cipher juga rentan terhadap serangan dan peretasan jika kunci enkripsi tidak diatur dengan baik. Oleh karena itu, perlu dilakukan optimalisasi keamanan kunci enkripsi Vigenere Cipher untuk meningkatkan keamanan pesan rahasia. Pesan rahasia algoritma Vigenere Cipher perlu dienkripsi untuk menjaga kerahasiaan pesan tersebut. Vigenere Cipher adalah salah satu teknik enkripsi yang kuat dan populer dalam kriptografi. Teknik ini menggunakan kunci enkripsi untuk mengacak pesan rahasia sehingga tidak dapat dibaca oleh orang yang tidak

berwenang [3].

Dalam Vigenere Cipher, pesan rahasia dienkripsi dengan menggunakan kunci yang sama panjangnya dengan pesan rahasia. Kunci ini digunakan untuk mengacak pesan rahasia dengan cara menggeser setiap karakter pesan rahasia sebanyak nilai kunci yang sesuai. Dengan demikian, pesan rahasia yang dienkripsi dengan Vigenere Cipher akan sulit dibaca oleh orang yang tidak memiliki kunci enkripsi yang tepat. Namun, jika kunci enkripsi tidak diatur dengan baik, Vigenere Cipher dapat rentan terhadap serangan dan peretasan. Oleh karena itu, perlu dilakukan optimalisasi keamanan kunci enkripsi Vigenere Cipher untuk meningkatkan keamanan pesan rahasia. Salah satu cara untuk melakukan optimalisasi keamanan kunci enkripsi Vigenere Cipher adalah dengan menggunakan algoritma MD5. Algoritma MD5 dapat digunakan untuk menghasilkan kunci enkripsi yang lebih kuat dan sulit ditebak oleh penyerang [4].

Dengan demikian, pesan rahasia yang dienkripsi dengan Vigenere Cipher dan kunci enkripsi yang dihasilkan oleh algoritma MD5 akan lebih sulit dibaca oleh penyerang. Salah satu cara untuk melakukan optimalisasi keamanan kunci enkripsi Vigenere Cipher adalah dengan menggunakan algoritma MD5. Algoritma MD5 dapat digunakan untuk menghasilkan kunci enkripsi yang lebih kuat dan sulit ditebak oleh penyerang. Dengan demikian, pesan rahasia yang dienkripsi dengan Vigenere Cipher dan kunci enkripsi yang dihasilkan oleh algoritma MD5 akan lebih sulit dibaca oleh penyerang. Oleh karena itu, penelitian tentang optimalisasi keamanan kunci enkripsi Vigenere Cipher pada pesan rahasia gambar steganografi dengan menggunakan algoritma MD5 sangat penting untuk meningkatkan keamanan informasi [5].

Optimasi keamanan kunci enkripsi sangat penting untuk menjaga kerahasiaan dan keamanan data. Dengan mengoptimalkan keamanan kunci enkripsi, data sensitif dan informasi pribadi dapat dienkripsi dan hanya dapat dibuka oleh orang yang memiliki kunci yang tepat. Hal ini membantu melindungi data dari akses tidak sah dan peretasan, privasi pengguna dapat terjaga. Data yang dienkripsi tidak dapat dibaca oleh orang yang tidak berwenang, sehingga privasi pengguna tetap terjaga [6].

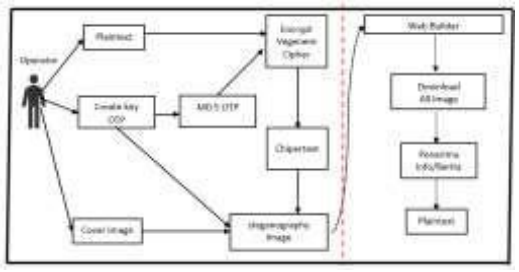
Banyak peraturan industri dan pemerintah yang menjabarkan perlindungan khusus mengenai perlindungan data dan persyaratan enkripsi. Dengan mengoptimalkan keamanan kunci enkripsi, organisasi dapat memenuhi persyaratan kepatuhan tersebut dapat mencegah akses tidak sah pada informasi yang tersimpan di perangkat atau sistem mereka."Optimalisasi Keamanan Kunci Enkripsi Vigenere Cipher pada Pesan Rahasia Gambar Steganografi dengan MD5", optimasi keamanan kunci enkripsi VigenereCipher pada pesan rahasia gambar steganografi dengan menggunakan algoritma MD5 sangat penting untuk meningkatkan keamanan informasi.

Algoritma MD5 digunakan dalam penelitian "Optimalisasi Keamanan Kunci Enkripsi Vigenere Cipher pada Pesan Rahasia Gambar Steganografi denganMD5" untuk menghasilkan kunci enkripsi yang lebih kuat dan sulit ditebak oleh penyerang. Hal ini membantu meningkatkan keamanan pesan rahasia dan melindungi data dari akses tidak sah dan peretasan yang memungkinkan penggunaanalgoritma MD5 dalam aplikasi membutuhkan waktu respons yang cepat, Hal ini membuat algoritma MD5 lebih mudah diimplementasikan dan didukung oleh banyak platform dan bahasa pemrograman. Dalam konteks penelitian "Optimalisasi Keamanan Kunci Enkripsi Vigenere Cipher pada Pesan Rahasia Gambar Steganografi dengan MD5", penggunaan algoritma MD5 untuk menghasilkan kunci enkripsi yang lebih kuat dan sulit ditebak oleh penyerang sangat penting untuk meningkatkan keamanan pesan rahasia dalam media steganografi.

METODE PENELITIAN

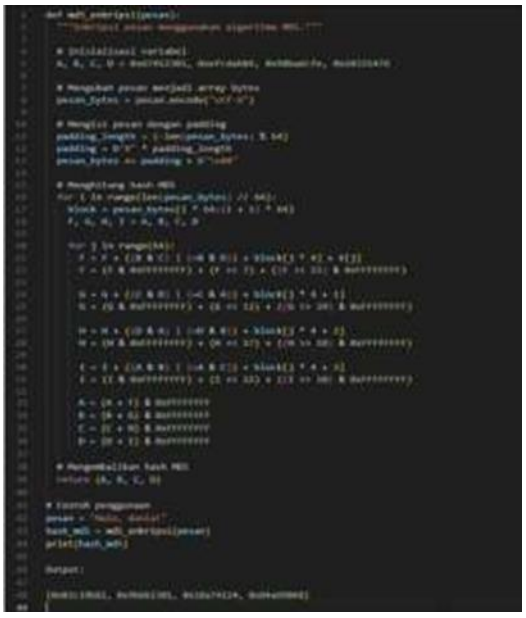
Dalam penelitian ini, fokus utama adalah pada optimalisasi keamanan kunci enkripsi Vigenere Cipher dalam konteks pesan rahasia gambar steganografi dengan memanfaatkan algoritma MD5. Vigenere Cipher, sebuah teknik enkripsi kuat, digunakan untuk mengacak pesan rahasia,

Langkah pertama melibatkan pemahaman mendalam tentang konsep dasar steganografi, Vigenere Cipher, dan algoritma MD5. Pengujian dilakukan untuk mengevaluasi keefektifan dan kinerja optimalisasi ini. Dapat melihat pada Gambar 1 di bawah ini.



Gambar 1.

Algoritma MD5 menggunakan fungsi hash satu arah, sehingga tidak mungkin untuk mengenkripsi kembali hash MD5 menjadi pesan aslinya. Algoritma MD5 terdiri dari 64 langkah, masing-masing langkahnya menggunakan operasi XOR, AND, OR, OT,dan shift. Dan Hash MD5 dari pesan terdiri dari 128 bit, yang dibagi menjadi 4 bagian, masing-masing bagian berukuran 32 bit. Algoritma Vigenere Cipher MD5 [7]:



Gambar 2.

Keamanan MD5 :

Algoritma MD5 dianggap aman untuk digunakan pada aplikasi yang tidak membutuhkan keamanan tingkat tinggi. Namun, algoritma MD5 telah terbuktirentan terhadap serangan brute force, sehingga tidak disarankan untuk digunakan pada aplikasi yang membutuhkan keamanan tingkat tinggi [8].

HASIL DAN PEMBAHASAN

Dalam pengujian perangkat lunak enkripsi Vigenere Cipher dengan metode MD5, hasil yang diperoleh menunjukkan bahwa kombinasi algoritma enkripsi Vigenere Cipher dengan fungsi hash MD5 menghasilkan tingkat keamanan yangcukup tinggi. Data yang dienkripsi dengan Vigenere Cipher dan kemudian di-hash dengan MD5 tidak dapat dengan mudah diretas oleh pihak yang tidak memiliki kunci dekripsi yang benar. Menginput data menggunakan kata kunci rahasia dan memberikan isi pesan rahasia dalam gambar Steganography.

Gambar 3.

Memproses Enkripsi kunci rahasia pada gambar menggunakan MD5.

Gambar 4.

Hasil Enkripsi Plaintext tang sudah di sisipkan ke *Image Steganography*.

Gambar 5.

Hasil mendeskripsi gambar Steganographyyang berisi kunci rahasia dan pesan rahasia menggunakan enkripsi MD5.

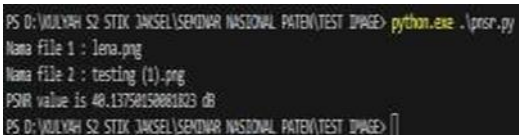
Gambar 6.

Memproses Deskripsi kunci rahasia pada *Image Steganography* menggunakan MD5.

Gambar 7.

Dari hasil pengujian enskripsi dan deskripsi, di dapatkan hasil bahwasanya pesan yang di enskripsi kemudian di sisipkan kedalam steganografi berhasil di deskripsi tanpa mengalami error ataupun kerusakan pada pesan yang di kirim.

Langkah selanjutnya adalah melakukan analisa *Peak Signal-to-Noise Ratio* (PNSR) dan histogram, untuk menganalisa apakah gambar yang belum disisipi berita dengan gambar yang sudah disisipi berita terjadi perubahan maupun kerusakan pixel yang signifikan. Menganalisa gambar dengan menggunakan metode Peak Signal-to-Noise Ratio (PNSR).



Gambar 8.

Dari hasil pengujian menggunakan metode *Peak Signal-to-Noise Ratio* (PNSR) di dapatkan nilai rasio frekuensi pixel yakni 40.13750150081823 dB. Sehingga mutudari *stego-image* yang dihasilkan baik [9].

Selanjutnya dilaksanakan pengujian kualitas gambar dengan metode histogram, sehingga didapat hasil berupa grafik.

Gambar 9.

Gambar diatas menunjukan grafik histogram dari image yang belum disisipi pesan dalam steganografi. Selanjutnya dilaksanakan pengujian histogram dengan gambar yang sudah disisipi pesan dalam steganografi.

Gambar 10.

Dari pengujian dengan metode histogram yang telah dilaksanakan terlihat bahwa grafik yang ditampilkan menunjukan kemiripan atau kesamaan tanpa ada perubahan yang mencolok, dengan ini dapat

disimpulkan bahwasanya gambar yang sudah disisipi pesan dalam steganografi memiliki kesamaan dengan gambar asli, sehingga pesan yang dikirm melalui steganografi dapat tersamar dengan baik.

Penggunaan metode MD5 dalam pengujian perangkat lunak enkripsi Vigenere Cipher membawa beberapa keuntungan. Pertama, MD5 adalah salah satu fungsi hash yang cepat dan efisien, sehingga tidak memerlukan banyak sumber daya komputasi. Kedua, MD5 menghasilkan hash yang unik untuk setiap input yang berbeda, sehingga memungkinkan untuk memverifikasi integritas data dengan baik. Namun, perlu diingat bahwa MD5 bukan lagi pilihan yang aman untuk penggunaan kriptografi yang sangat sensitif, karena terdapat kerentanannya terhadap serangan hash collision. Meskipun demikian, dalam konteks pengujian perangkat lunak, MD5 masih dapat memberikan lapisan keamanan yang baik saat digunakan bersama dengan Vigenere Cipher.

PENUTUP

Kesimpulan

Dari hasil pengujian sistem yang dilakukan pada bab sebelumnya, maka dapat disimpulkan beberapa hal antara lain:

1. Dalam konteks pengujian perangkat lunak enkripsi Vigenere Cipher dengan metode MD5, hasil penelitian menunjukkan bahwa penggunaan kombinasi algoritma Vigenere Cipher dengan fungsi hash MD5 dapat meningkatkan tingkat keamanan pesan rahasia dalam media steganografi.
2. Penggunaan MD5 sebagai alat untuk menghasilkan kunci enkripsi yang kuat membantu melindungi pesan rahasiadari akses tidak sah dan peretasan yang mungkin terjadi, Meskipun MD5 memiliki beberapa kerentanan, penggunaannya dalamkonteks pengujian perangkat lunak menunjukkan keefektifan dalam memperkuat lapisan keamanan pesan rahasia.
3. Penelitian ini menggarisbawahi pentingnya optimalisasi keamanan 3 kunci enkripsi Vigenere Cipher dalam konteks pesan rahasia gambar steganografi dengan menggunakan algoritma MD5 untuk meningkatkan keamanan informasi secarakeseluruhan, Penggunaan algoritma MD5 dalam penelitian tersebut memberikan lapisan keamanan yang baik saat digunakan bersama dengan Vigenere Cipher dalam konteks pengujian perangkat lunak.

Saran

Berdasarkan artikel tersebut, berikut adalah beberapa saran yang dapat diambil:

1. Perlu dilakukan optimalisasi agar representasi 1 huruf yang sebelumnya menggunakan 2 pixel dapat dikurangi menjadi 1 huruf 1 pixel. Hal ini bertujuan untuk mengurangi jumlah piksel yang digunakan, sehingga kerusakan pada gambar steganografi yang dihasilkan dapat diminimalisir.
2. Diperlukan metode lain untuk memastikan kunci OTP tetap aman dan tidak terbuka, serta mekanisme tambahan untuk menyamarkan kunci guna meningkatkan keamanan
3. Kunci privat pada MD5 masih dianggap terlalu pendek, sehingga diperlukan mekanisme lain untuk memperpanjang kunci demi meningkatkan keamanan.
4. Dengan menerapkan saran-saran ini, kita dapat memastikan bahwa keamanan pesan rahasia dalam steganografi tetap menjadi prioritas dan terlindungi dengan baik dalam lingkungan yang terus berubah dan berpotensi berbahaya.

DAFTAR PUSTAKA

[1] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, “A Good Performance OTP encryption image based on DCT-DWT steganography,” Telkomnika (Telecommunication Computing Electronics and Control), vol. 15, no. 4, pp. 1987–1995, Dec. 2017, doi: 10.12928/TELKOMNIKA.v15i4.5883.

[2] S. Hajar, “Analisa Metode Message Digest 5 (Md5) Untuk Mendeteksi Orisinalitas Citra Digital,” 2021.

[3] Ibezato Zalukhu, Z. Sitorus, and N. Septiani, “Enhancing Text Messages with a Combination of Vigenère Cipher and One Time Pad Using Random Key

LFSR," Jurnal Sains dan Teknologi, vol. 6, no. 1, pp. 52–57, doi: 10.55338/saintek.v6i1.3190.

[4] M. Musrini, B. Rahardjo, and R. Krisnadi, Implementation Of Vigenere Cipher With Euler Key Generator To Secure Text Document.

[5] L. Budi Handoko, "Sekuriti Teks Menggunakan Vigenere Cipher Dan Hill Cipher," 2022.

[6] F. Meneses Et Al., "Rsa Encryption Algorithm Optimization To Improve Performance And Security Level Of Network Messages," 2016.

[7] V. Klíma, "Finding Md5 Collisions- A Toy For A Notebook," 2005. [Online]. Available: Http://Cryptography.Hyperlink.Cz

[8] Muhidin And R. Alfianto, "Kelemahan Metode Enkripsi Message Digest 5 Terhadap Kriptanalisis MODERN," vol. 11, no. 3, pp. 2407–3903, 2020.