JURNAL INFORMASI KOMPUTER LOGIKA
Volume 2, Nomor 2, 2021
ISSN 2655-7002 (media online)
Available Online at http://ojs.logika.ac.id/index.php/jikl

Algoritma Hill Cipher Untuk Kebenaran Informasi pada Gambar dalam Media Sosial

Tomy Satria Alasi[1]
[1] Teknik Informatika, STMIK Logika, Medan
Email: [1]tomysatriaalasi@live.com

Abstrak−Permasalahan dalam sistem ini adalah mengimplementasikan kriptografi citra digital dengan menggunakan metode Hill Chiper sehingga dapat menjamin keamanan dari gambar dalam bermedia sosial, dengan gambar digital harus di validasi tersebut dari pihak-pihak yang tidak berhak untuk mengetahuinya atau melakukan perubahan dalam citra digital tersebut. Kriptografi citra digital ini dirancang menggunakan algoritma hill chiper diimplementasikan dengan bahasa pemograman visual studio. Algoritma hill cipher merupakan salah satu algoritma kriptografi kunci simetris. Algoritma hill cipher menggunakan matriks berukuran *m x m* sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill Cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks.

Kata Kunci: *Algoritma Hill Cipher, Gambar, Media Sosial.*

Abstract− *The problem in this system is to implement digital image cryptography using the Hill Ciper method so that it can ensure the security of images in social media, with digital images must be validated from parties who are not entitled to know or make changes in the digital image. This digital image cryptography is designed using hill cipher algorithm implemented with visual studio programming language. Hill cipher algorithm is a symmetric key cryptography algorithm. The hill cipher algorithm uses a matrix of size m x m as a key to perform encryption and decryption. The basis of matrix theory used in Hill Cipher, among others, is multiplication between matrices and performing inverses on matrices..*

Keywords: *Hill Cipher Algorithm, Image, Social Media.*

1. PENDAHULUAN

Media sosial sebagai alat pengolahan digital saat ini hampir dimiliki oleh setiap orang dan keluarga. Dengan perkembangan komputer serta pengetahuan dalam pengolahan sinyal digital, maka data-data dalam bentuk digital semakin banyak digunakan, hal ini dikarenakan komputer yang berkembang saat ini merupakan peralatan elektronik yang menggunakan dan mengolah data dalam bentuk digital. Penggunaan data digital baik berupa teks, suara, citra maupun video sangat pesat dengan adanya komputer apalagi ditambah dengan perkembangan teknologi jaringan antar komputer di dunia yang disebut dengan internet. Penggunaan data digital selain mudah, juga murah dalam penggandaan serta penyimpanannya untuk digunakan dilain waktu. Dengan itu disaat mengirimkan informasi gambar maka diperlukan sebuah validasi apakah gambar tersebut benar atau tidak, penulis menggunakan algoritma hill cipher agar semua itu dapat berjalan dengan baik. Pembuatan suatu perangkat lunak yang dapat melakukan penyandian citra dengan hill cipher. Matriks kunci yang dapat dipakai mencakup matriks persegi dengan ordo 2 × 2 atau 3 × 3. *File* citra hasil penyandian ini dapat dicetak dan disimpan kembali dalam format bitmap. Pada tulisan ini juga dilakukan pengujian pada file citra jenis photo dan jenis kartun agar diketahui jenis citra apa yang mampu disandikan dengan Hill Cipher

.

2. METODOLOGI PENELITIAN

2.1 Kriftografi

Dalam kriptografi ada beberapa istilah yang sering digunakan, antara lain: plaintext, ciphertext, key, enkripsi dan dekripsi . Plaintext adalah data biasa/pesan yang akan disandikan. Ciphertext adalah data/pesan tersandi. Key adalah serangkaian karakter yang bersifat rahasia. Enkripsi adalah proses untuk menyandikan suatu pesan atau proses transformasi dari plaintext menjadi ciphertext. Dengan kata lain, enkripsi adalah transformasi data kedalam bentuk yang hampir tidak dapat dibaca tanpa pengetahuan yang cukup dan sesuai[1].

Kriptografi mempunyai peranan penting dalam dunia komputer. Hal ini disebabkan karena banyaknya informasi rahasia yang disimpan dan dikirimkan melalui media-media komputer. Informasi-informasi ini biasanya bersikan dokumen-dokumen penting atau bersifat rahasia dari suatu instansi yang tidak ingin dibaca oleh orang yang tidak berhak atas informasi tersebut. Dengan komputer digital, akan sangat mungkin untuk menghasilkan cipher (pesan rahasia) yang lebih kompleks dan rumit[2]. Kriptografi klasik pada umumnya dienkripsi karakter per karakter (menggunakan alfabet tradisional), sedangkan kriptografi modern beroperasi pada string biner. Kriptografi modern tidak hanya berkaitan dengan teknik menjaga kerahasiaan pesan, tetapi juga menghasilkan tanda tangan tangan digital dan sertifikat digital[3]. Dengan kata lain kriptografi modern tidak hanya memberikan aspek keamanan[4], tetapi juga kepada aspek-aspek lain dalam dunia digital[5].

JURNAL INFORMASI KOMPUTER LOGIKA
Volume 2, Nomor 2, 2021
ISSN 2655-7002 (media online)
Available Online at http://ojs.logika.ac.id/index.php/jikl

2.2 Algoritma Hill Cipher

Algoritma hill cipher menggunakan fungsi matriks didalam perhitungan. Matriks adalah susunan sekelompok bilangan dalam bentuk persegi atau persegi panjang yang diatur menurut baris dan kolom[6]. Cipher adalah kode rahasia yang dipakai untuk enkripsi pesan berupa plaintext[7]. Hill Cipher berdasarkan pada aljabar linier dan seperti sandi Vigenére, Hill Cipher merupakan block cipher[8]. Sandi ini dapat dipecahkan dengan known-plaintext attacks tetapi tahan melawan ciphertext-only attack. Cara kerja sandi ini berdasarkan atas perkalian matriks dengan menggnakan sebuah kunci K.

2.3 Citra Digital

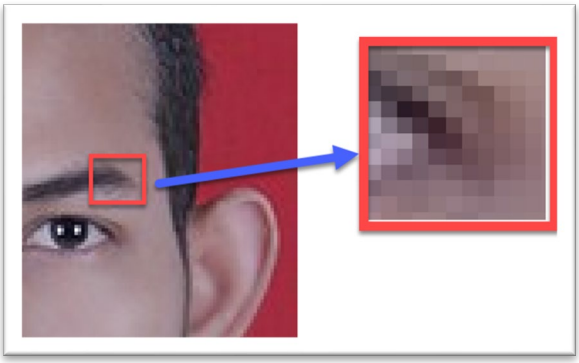
Citra adalah representasi atau deskripsi tentang suatu objek[9]. Citra juga dapat diartikan sebagai objek pada bidang dua dimensi. Citra dapat direpresentasikan ke dalam citra analog dan citra digital. Citra analog dihasilkan dari sistem optik, misalnya mata manusia, kamera, sedangkan citra digital dihasilkan dari hasil digitalisasi citra analog. Citra digital adalah representasi numerik dari objek-objek. Citra digital dibentuk oleh sekumpulan angka dalam array dua dimensi. Tiap angka menggambarkan warna dari tiap titik dalam gambar sesuai dengan mode warna yang digunakan[10].

3. HASIL DAN PEMBAHASAN

Penyandian dengan Hill Cipher pada citra seperti halnya dengan teks juga menggunakan matriks dimana ketentuannya menggunakan matriks bujur sangkar. Matriks bujur sangkar adalah matriks dengan jumlah baris = jumlah ko lom. Matriks bujur sangkar disebut matriks identitas (I) jika semua elemen diagonal utamanya sama dengan satu dan elemen lainnya sama dengan nol. Invers suatu matriks A adalah matriks B sedemikian hingga A. B = I. Invers matriks A ada jika determinan (A) $\neq 0$.

Misal a dan b adalah bilangan-bilangan bulat. Bilangan bulat c disebut faktor persekutuan a dan b jika c|a dan c|b. Bilangan bulat tak negatif d disebut faktor persekutuan terbesar (FPB) a dan b jika d adalah faktor persekutuan a dan b dan untuk setiap c, jika c|a dan c|b maka d|c. Penyandian dengan Hill Cipher dilakukan dengan memanfaatkan operasi matriks biasa. Penyandian dilakukan pada tiap blok teks yang berukuran sama dengan ordo matriks yang digunakan. Sebagai perluasannya, dalam tulisan ini Hill Cipher diimplementasikan untuk menyandikan sebuah citra. Ini dimungkinkan mengingat sebuah citra merupakan deretan piksel-piksel yang mempunyai komponen R (Red), G (Green) dan B (Blue).

Komponen-komponen ini merupakan bilangan-bilangan bulat sehingga dapat dioperasikan dalam sebuah matriks. Citra yang digunakan dalam tulisan ini dibatasi dalam format BMP, GIF, JPG atau JPEG. Sedangkan matriks yang dipakai adalah matriks bujur sangkar atau persegi berordo 2 × 2 atau 3 × 3 dengan elemen bilangan bulat. Implementasi akhir dari tulisan ini adalah perancangan suatu program yang dapat berfungsi untuk menyandikan atau mengekripsi citra sehingga tiap komponen warna pada citra tersebut menjadi tidak teratur dan citra menjadi sulit untuk dikenali.



Gambar 3.1 Ilustrasi RGB pada pixel

3.1 Enkripsi Hill Cipher pada Citra Digital

Adapun tahapan didalam enkripsi hill cipher adalah sebagai berikut :

1. Tentukan ukuran dan nilai RGB tiap piksel citra digital.
2. Pilih suatu matriks kunci K yang berupa matriks bujur sangkar yang dipakai sebagai kunci.
3. Transformasikan tiap piksel dalam citra digital ke bilangan bulat yang sesuai dengan nilai RGB (0-255)
4. Kelompokkan barisan angka yang didapat ke dalam beberapa blok vektor P yang panjangnya sama dengan ukuran matriks K.
5. Hitung C = K . P (mod 256) untuk tiap vektor P.

JURNAL INFORMASI KOMPUTER LOGIKA
Volume 2, Nomor 2, 2021
ISSN 2655-7002 (media online)
Available Online at http://ojs.logika.ac.id/index.php/jikl

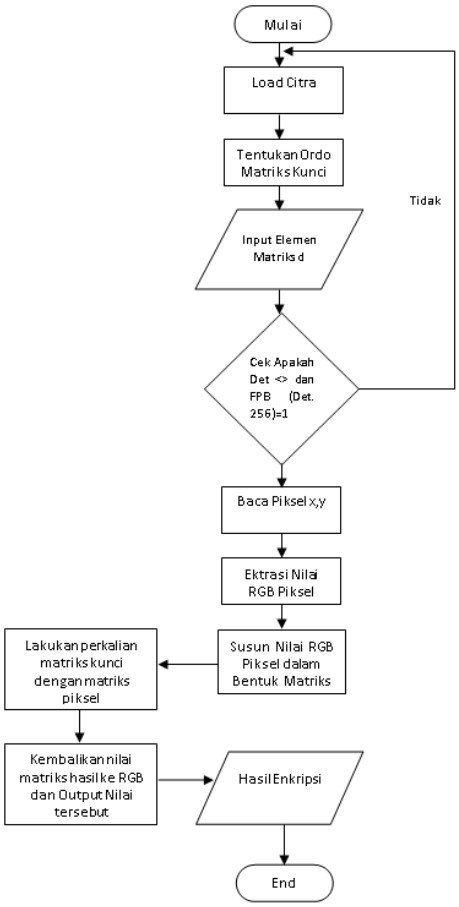
6. Kembalikan tiap angka dalam vektor sandi C ke piksel yang sesuai untuk mendapatkan piksel sandi.

3.2 Deskripsi Algoritma Hill Chiper pada Citra Digital

Algoritma proses pendekripsian Hill Cipher dapat diuraikan dalam bentuk langkah-langkah sebagai berikut:

1. Hitung matriks K^{-1} (mod 256) sebagai kunci pembuka. K^{-1} ada jika FPB ((det(K), 256)=1.
2. Lakukan langkah-langkah 2–5 pada enkripsi dengan mengganti:
   (i) Matriks K dengan matriks K^{-1}
   (ii) Blok vektor piksel asli P dengan blok vektor sandi C dan sebaliknya.

Program adalah serangkaian instruksi yang disusun untuk menyelesaikan suatu pekerjaan dengan menggunakan komputer. Sedangkan program *flowchart* adalah suatu bagan dengan simbol-simbol tertentu yang menggmbarkan urutan-urutan proses secara mendetail dan hubungan antara suatu proses dengan proses lainnya dalam suatu program.



Gambar 3.2 Flowchart Enkripsi dan Deskripsi

Kriptografi citra digital ini menghasilakn sebuah citra digital yang kabur dan tidak dapat dilihat dengan kasat mata tanpa bantuan perangkat lunak yang penulis rancang, serta mengubah besar ukuran file citra digital tersebut dengan cara memetakan nilai RGB pada masing-masing pixel citra digital tersebut menjadi bentuk sebuah geometri. Namun, sistem ini hanya dapat mengenkripsi citra digital dengan format JPG, BMP, dan GIF sehingga masih membutuhkan pengembangan lebih lanjut.

4. KESIMPULAN

Algoritma Hill Chiper mampu mendeteksi nilai piksel dari suatu citra digital. Proses enkripsi citra digital menggunakan algoritma Hill Chiper ini dilakukan dengan cara mengambil nilai RGB, lalu di XOR kan antara nilai RGB dengan nilai ASCII kata sandi, lalu disusun kembali menjadi sebuah citra digital yang terenkripsi Algoritma Hil Chiper dapat mendeteksi suatu citra digital walaupun memiliki tingkat piksel yang tinggi. Hasil enkripsi citra digital dengan menggunakan algoritma Hill Chiper dapat digunakan sebagai output menjadi teknik pengolahan kriptograpi citra digital yang baik.

REFERENCES

[1] H. Mukhtar, *Kriptografi untuk Keamanan Data*. Deepublish, 2018.
[2] Jamaludin and Romindo, "Rancang Bangun Pengamanan Teks Menggunakan Kombinasi Vigenere Cipher dan RSA dalam Hybrid Cryptosystem," *Pros. Semin. Nas. Ris. Dan Inf. Sci.*, vol. 2, no. 0, pp. 105–116, 2020.
[3] T. S. Alasi, "IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITMA CEASAR CIPHER UNTUK KEAMANAN DATA MICROSOFT OFFICE WORD DAN EXCEL," *J. Inf. Komput. Log.*, vol. 1, no. 2, 2019.
[4] M. C. Sinaga, *Kriptografi Python*. Matius Celcius Sinaga, 2017.
[5] M. K. Ridwan, W. F. Pattipeilohy, S. Sanwani, and others, "Aplikasi Keamanan Document Digital Menggunakan Algoritma Steganografi Discrete Cosine Transform (Dct) Pada Perusahan Alat Berat," *JITK (Jurnal Ilmu Pengetah. Dan Teknol. Komputer)*, vol. 5, no. 2, pp. 177–182, 2020.
[6] T. S. Alasi, "Penerapan Algoritma Algoritma Boyer Moore untuk Penyaringan Pesan dan Algoritma Hill Cipher dalam Keamanan Pesan Teks Berbasis Web Chat," *KAKIFIKOM Kumpul. Artik. Karya Ilm. Fak. Ilmu Komput.*, vol. 1, no. 2, pp. 73–79, 2019.
[7] V. S. Ginting, "Penerapan Algoritma Vigenere Cipher dan Hill Cipher Menggunakan Satuan Massa," *JurTI (Jurnal Teknol. Informasi)*, vol. 4, no. 2, pp. 241–246, 2020.
[8] T. S. Alasi and A. T. A. A. Siahaan, "Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database," *J. Inf. Komput. Log.*, vol. 1, no. 4, 2020.
[9] P. Fitriani and T. S. Alasi, "Pengamanan Pesan Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit Pada Citra Digital," *J. Inf. Komput. Log.*, vol. 1, no. 2, 2019.
[10] G. R. Safri, "PENERAPAN LIVENESS SEBAGAI ANTI-SPOOFING CITRA DIGITAL PADA SISTEM KEAMANAN AKSES KONTROL RUANG SERVER BERBASIS RASPBERRY PI," Universitas Muhammadiyah Gresik, 2021.