Jurnal Teknik Informatika (JUTIF)
Vol. 5, No. 2, April 2024, pp. 405-413

DOI: https://doi.org/10.52436/1.jutif.2024.5.2.1864
p-ISSN: 2723-3863
e-ISSN: 2723-3871

IMAGE DATA SECURITY USING VERNAM CIPHER ALGORITHM

Supiyanto*[1] dan Anastasia Sri Werdhani[2]

[1]Information System faculty of Mathematics and Natural Sciences, Universitas Cenderawasih, Indonesia
[2]Mechanical Engineering, Faculty of Engineering, Universitas Cenderawasih, Indonesia
Email: [1]supi6976@gmail.com, [2]asriwerdhani@gmail.com

(Article received: February 13, 2024; Revision: March 6, 2024; Published: April 04, 2024)

Abstract

The Vernam Cipher algorithm is a symmetric key algorithm, as it uses the same key for encryption and decryption. It utilizes a binary number system with XOR operation to produce a series of bits. This study aims to implement the Vernam cipher algorithm to secure personal and confidential image data, which is at risk of misuse when shared through chat applications like Facebook, WhatsApp, and email. Therefore, developing image protection applications is crucial. The research explores whether the vernam cipher algorithm, working with single bits in block form and based on binary numbers, can effectively secure image data, specifically grey scale images with BMP and JPG extensions. The approach involves applying the Vernam cipher algorithm to programming language to create a data security application. The outcome is an image security application program, with test results indicating successful encryption with significant randomness. The decryption process with the Vernam cipher method can restore encrypted images to their original state, although some distortion may occur, especially with JPEG images. Decryption of BMP images is nearly flawless. The key for data security can vary in length and form, with encryption taking longer than decryption.

Keywords: *encryption, decryption, cryptography, Vernam cipher, XOR*

KEAMANAN DATA CITRA MENGGUNAKAN ALGORITMA VERNAM CIPHER

Abstrak

Algoritma Vernam c*ipher* termasuk algoritma *symmetric key*, karena saat proses enkripsi dan dekripsi menggunakan kunci yang sama. Algoritma ini menggunakan sistem bilangan biner dengan operasi **XOR**, hasilnya berupa rangkaian bit. Penelitian ini bertujuan mengimplementasikan algoritma Vernam *cipher* untuk pengamanan data citra. Citra digital yang bersifat personal dan confidential mudah disalahgunakan oleh pihak yang tidak bertanggung jawab, terutama saat dikirim melalui aplikasi chatting seperti facebook, whatsapp, dan email. Oleh karenanya penelitian membuat aplikasi yang dapat melindungi citra penting dilakukan. Permasalahannya apakah algoritma vernam *cipher* yang bekerja dalam bentuk blok-blok dalam bentuk bit tunggal dan berbasis bilangan biner ini dapat digunakan untuk mengamankan data citra. Citra yang digunakan ini berupa citra *gray scale* dengan ber-ektensi BMP dan JPG. Metode pada penelitian ini yakni menerapkan algoritma Vernam *cipher* ke dalam bahasa pemrograman untuk menghasilkan suatu aplikasi yang dapat digunakan untuk pengamanan data. Luaran penelitian ini, terciptanya suatu program aplikasi pengamanan citra. Hasil pengujian menunjukkan keteracakan yang cukup signifikan, hal ini menunjukkan bahwa proses enkripsi berhasil dengan baik. Selain itu, proses dekripsi dengan metode Vernam *cipher* untuk citra ter-enkripsi dapat dikembalikan seperti citra asli walaupun ada sebagian citra hasil dekripsi yang mengalami distorsi terkhusus citra yang ber-ektensi JPEG. Sedangkan untuk citra yang mempunyai ekstensi BMP dapat di-dekripsi dengan sangat baik, dengan citra hasil dekripsi hampir 100% menyerupai citra asli. Adapun kunci yang digunakan untuk pada keamanan data ini berupa string atau angka dengan panjang beragam, dengan waktu yang dibutuhkan saat proses enkripsi lebih lama daripada waktu yang dibutuhkan saat dekripsi.

Kata Kunci: enkripsi, dekripsi, kriptografi, Vernam *cipher*, XOR

1. PENDAHULUAN

Menjadi perhatian yang sangat penting ketika mengirim data yang dilakukan melalui jaringan publik untuk menjaga kerahasiaan suatu data terutama jika data tersebut bersifat rahasia yang hanya boleh diketahui isinya oleh pihak yang berhak saja [1].

Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu menyandikan isi informasi tersebut menjadi isi yang tidak dipahami, yang dikenal dengan proses enkripsi dan untuk memperoleh kembali informasi yang asli, disebut proses dekripsi, disertai dengan menggunakan kunci yang benar [2].

Salah satu algoritma persandian dalam kriptografi adalah Vernam cipher. Algoritma kriptografi ini menurut jenis kunci yang digunakan termasuk kriptografi simetris, karena kunci digunakan saat proses enkripsi sama dengan saat proses dekripsi [3] [4].

Cara kerja dari algoritma vernam cipher, setiap plainteks yang ada dibagi – bagi menjadi blok – blok dengan panjang yang sama. Plainteks dan cipherteksnya berupa *integer* (bilangan bulat) antara 1 hingga n, dimana n berukuran biasanya sebesar 1024 bit, dan panjang bloknya sendiri berukuran lebih kecil atau sama dengan log(n) +1 dengan basis 2 [5]. oleh karenanya Vernam *cipher* dapat dibuat dengan cepat bahkan lebih cepat dibandingkan dengan algoritma block *cipher* manapun [6].

Berdasarkan kemunculannya, Vernam cipher digolongkan ke dalam kriptografi modern, beroperasi dalam bentuk bit tunggal yang dalam hal kunci, plainteks dan cipherteks diproses dalam rangkaian bit. Dengan demikian algoritma ini lebih kompleks dan lebih sulit untuk dipecahkan bila dibandingkan dengan kriptografi kunci klasik [7].

Pada proses enkripsi, *plaintext* diubah ke dalam kode *ASCII* dan kemudian dikenakan operasi **XOR** terhadap kunci yang sudah diubah ke dalam kode *ASCII* [8]. Pada proses dekripsi, *ciphertext* diubah ke dalam kode *ASCII*, kemudian dikenakan operasi XOR terhadap kunci yang sudah diubah ke dalam kode *ASCII* juga. [9]

Beberapa penelitian terbaru yang berhubungan keamanan data dan algoritma Vernam cipher diantaranya; *Simulation of The Application of Intelligence in Vernam Cipher* [10], Aplikasi Enkripsi Dan Dekripsi Dengan Teknik XOR Menggunakan Metode Vernam Cipher [11], *Application of Integers in Vernam Cipher Cryptography (One Time Pad) Parasian* [12] dan *Implementation of the data encryption using caesar cipher and vernam cipher methods based on CrypTool2* [13]. Keempat penelitian ini menunjukan kalau keamanan data dengan algoritma Vernam cipher masih terus berkembang hingga saat ini. Namun penelitian yang mereka lakukan masih untuk data teks.

Citra digital yang bersifat personal dan confidential mudah disalahgunakan oleh pihak yang tidak bertanggung jawab, terutama saat dikirim melalui aplikasi chatting seperti facebook, whatsapp, dan email. Penyiaran citra melalui internet rentan diserang dan disadap, serta penyimpanan di media stroge rentan diakses oleh pihak yang tidak bertanggung jawab [14].

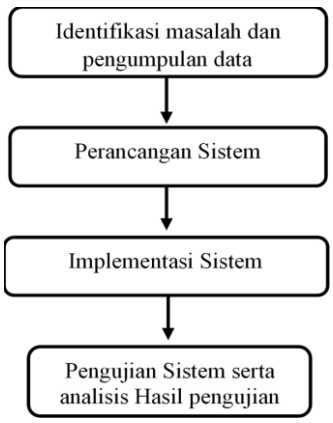
Oleh karenanya penelitian membuat aplikasi yang dapat melindungi data citra penting dilakukan. Permasalahannya apakah algoritma vernam *cipher* yang bekerja dalam bentuk blok-blok dalam bentuk bit tunggal dan berbasis bilangan biner ini dapat digunakan untuk mengamankan data citra.

Secara harafiah, citra (*image*) sendiri adalah gambar pada bidang dua dimensi. Sedangkan ditinjau dari sudut pandang matematis, citra merupakan fungsi continue dari intensitas cahaya pada bidang dua dimensi. Berdasarkan warnanya, citra terbagi atas citra biner yaitu citra yang setiap pixel bernilai 0 atau 1; citra skala keabuan (*gray scale*) yaitu citra yang nilai pixel-nya bernilai 0 sampai 255 dan citra warna (*true color*) yaitu citra yang warnanya dibentuk dari kombinasi tiga warna dasar yaitu merah hijau biru atau dikenal dengan citra RGB (*Red Green Blue*) dengan nilai pixel-nya masing-masing bernilai 0 sampai 255 [15].

2. METODE PENELITIAN

Metode penelitian ini menggunakan metode terapan, yaitu penelitian yang bertujuan untuk menerapkan suatu teori, metode atau konsep yang ada di algoritma vernam cipher ke bidang terapan yakni keamanan data citra. Citra yang digunakan berupa citra skala keabuan (*gray scale*) mempunyai ektensi BMP dan Jpeg.

Penelitian ini diselesaikan dalam empat tahapan, yaitu, (1) Tahap Identifikasi Masalah dan Pengumpulan Data, (2) Perancangan Sistem, (3) Implementasi Sistem, (4) Pengujian Sistem, serta Analisis Hasil Pengujian



Gambar 1. Tahapan Penelitian

Tahapan penelitian pada Gambar 1, dijelaskan sebagai berikut: Tahap pertama: mengidentifikasi masalah dan pengumpulan data, diantaranya bagaimana sistem kriptografi yang dibuat dapat mengenkripsi dan mendekripsi data citra dengan metode algoritma Vernam *cipher* dalam menyandikan suatu informasi. Tahap kedua: merancang proses enkripsi dan dekripsi menggunakan algoritma Vernam *Cipher*. Pada proses ini memerlukan masukan data berupa citra digital, dan kunci. Tahap ketiga: yaitu mengimplementasikan hasil perancangan. Membangun aplikasi untuk proses enkripsi dan dekripsi menggunakan algoritma vernam cipher untuk keamanan data citra. Tahap keempat: adalah melakukan pengujian sistem. Analisis dilakukan pada hasil pengujian, sehingga dapat diperoleh kesimpulan

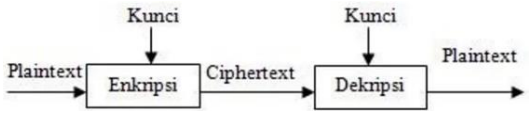
2.1. Algoritma Kriptografi

Algoritma kriptografi (*Cryptographic Algorithm*) atau sering disebut chiper merupakan fungsi matematika yang digunakan untuk proses enkripsi dan dekripsi dimana proses enkripsi dan dekripsi diatur oleh salah satu atau beberapa kunci kriptografi [16]. Secara umum, kunci-kunci yang digunakan untuk pengenkripsian dan pendekripsian tidak perlu identik, tergantung pada sistem yang digunakan. Secara matematis proses enkripsi dan dekripsi dapat ditulis:

Ek (M) = C (Proses enkripsi)
Dk (C) = M (Proses dekripsi)

dengan:

Ek = Proses enkripsi K = Kunci
M = Teks asli C = Teks terenkripsi
D = Proses dekripsi

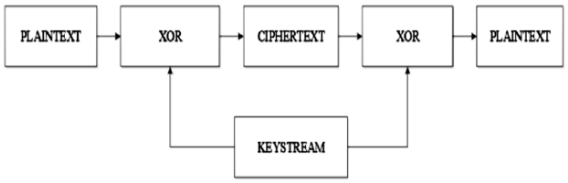


Gambar 2. Aliran Enkripsi dan Deskripsi pada Kriptografi

Pada saat proses enkripsi, pesan (M) akan di sandikan dengan menggunakan kunci enkripsi (K) menjadi sandi yang tidak dimengerti (C) sedangkan pada proses dekripsi, sandi yang tidak dimengerti (C) tersebut di uraikan dengan menggunakan kata kunci dekripsi (K) sehingga menghasilkan pesan (M) yang sama seperti pesan sebelumnya. Proses ini dapat diilustrasikan pada gambar 2.

2.2. Algoritma Vernam *Cipher*

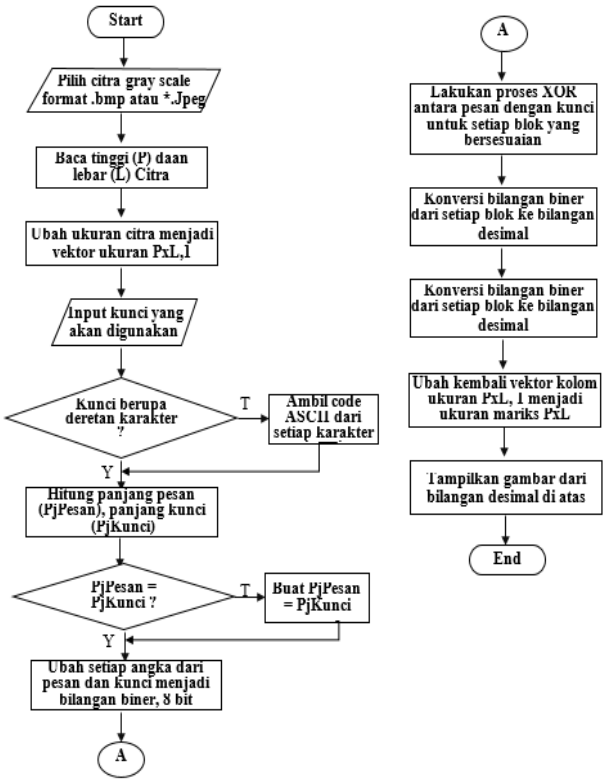
Algoritma kriptografi Vernam *Cipher* merupakan algoritma kriptografi berjenis symmetric key. Kunci yang digunakan untuk melakukan enkripsi dan dekripsi menggunakan kunci yang sama. Dalam melakukan proses enkripsi, algoritma Vernam *Cipher* menggunakan cara Vernam cipher dimana cipher berasal dari hasil operasi XOR antara bit plainteks dan bit key [17]. Secara sederhana proses enkripsi dan dekripsi algoritma Vernam *Cipher* dapat adalah pada gambar dibawah ini [18]:



Gambar 3. Proses Enkripsi dan Dekripsi Algoritma Kriptografi Vernam *Cipher*

a. Flowchart Enkripsi Vernam *Cipher*

Flowchat proses enkripsi dengan algoritma vernam cipher dapat dilihat pada Gambar 4, di bawah ini.



Gambar 4. Flowchart Enkripsi dengan Algoritma Vernam *Cipher*

b. Proses Enkripsi Vernam *Cipher*

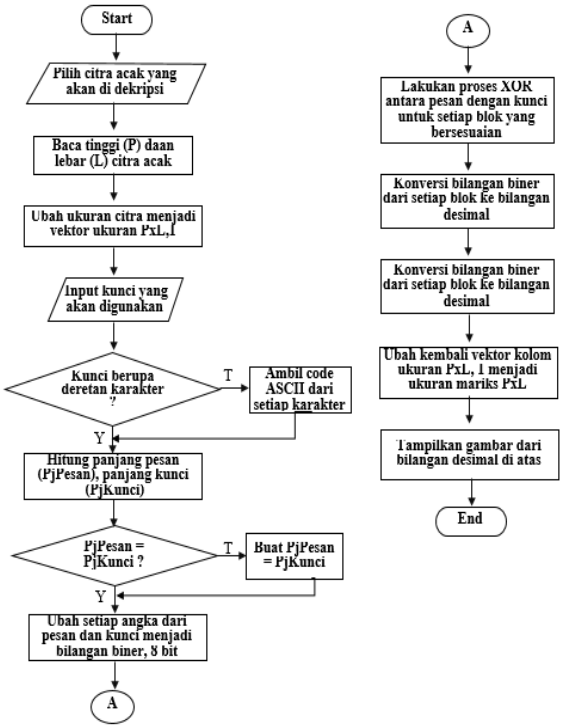
Berikut proses enkripsi dengan algoritma Vernam cipher pada data citra, mulai dari *Plaintext* hingga Ciphertext sebagaimana Gambar 3:

1. Input citra
2. Baca ukuran citra m x n
3. Ubah ukuran citra menjadi vektor baris, $m*n\ x\ 1$
4. Hitung panjang yang berupa vektor baris
5. Inputkan kunci yang akan digunakan.
6. Jika kunci berupa kumpulan karakter maka ubah setiap karakter pada kunci ke dalam bentuk kode ASCII; jika berupa deretan angka-angka lanjut ke langkah berikutnya.
7. Hitung panjang kunci

8. Buat panjang kunci sama dengan panjang pesan
9. Ubah nilai pixel pesan dan kode ASCII dari kunci yang dalam bentuk desimal ke dalam bilangan biner dengan format panjang bilangan biner 8 digit.
10. Lakukan operasi XOR setiap bilangan biner dari pesan dan kunci yang bersesuaian
11. Ubah hasil operasi XOR yang dalam bentuk bilangan biner ke dalam bentuk desimal
12. Ubah kembali vektor kolom menjadi sebuah matrik berukuran m x n sebagaimana citra awal
13. Konversi ke dalam citra, hasilnya sebuah citra yang ter-enkrip

c. *Flowchart* Dekripsi Vernam Cipher

Flowchart proses dekripsi dengan algoritma vernam cipher dapat dilihat pada Gambar 5, di bawah ini.



Gambar 5. *Flowchart* Dekripsi dengan Algoritma Vernam *Cipher*

d. Proses Dekripsi Vernam *Cipher*

Sedangkan berikut proses dekripsi dengan algoritma Vernam cipher pada data citra. Proses Ciphertext hingga Plaintex, sebagaimana yang digambarkan pada Gambar 3

1. Input citra ter-enkrip hasil proses enkripsi sebelumnya
2. Baca ukuran citra ter-enkrip misalnya m x n
3. Ubah ukuran citra ter-enkrip menjadi vektor baris dengan uuran $m*n\ x\ 1$
4. Hitung panjang citra ter-enkrip yang berupa vektor baris
5. Inputkan kunci yang akan digunakan.
6. Sebagaimana Langkah 6 pada proses enkripsi, jika kunci berupa kumpulan karakter maka ubah setiap karakter ke dalam bentuk kode ASCII jika berupa deretan angka-angka lanjut ke langkah berikutnya.
7. Hitung panjang kunci
8. Buat panjang kunci sama dengan panjang citra ter-enkrip
9. Ubah nilai *pixel* citra ter-enkrip dan ASCII kode dari kunci yang dalam bentuk desimal ke dalam bilangan biner dengan format panjang bilangan biner 8 digit.
10. Lakukan operasi XOR setiap bilangan biner dari citra ter-enkrip dengan kunci yang bersesuaian
11. Ubah hasil operasi XOR yang dalam bentuk bilangan biner ke dalam bentuk desimal
12. Ubah kembali vektor kolom menjadi sebuah matrik sesuai ukuran citra.
13. Hasilnya adalah berupa berupa citra yang ter-dekripsi yang seharusnya kembali sebagaimana citra asli.

3. HASIL DAN PEMBAHASAN

Pada bagian ini diuraikan mengenai hasil dari penelitian beserta pengujian yang telah dilakukan. Selain itu, disampaikan juga mengenai pembahasan dari penelitian maupun pengujian yang telah dilakukan.

3.1. Data Penelitian

Data citra yang digunakan pada penelitian ini adalah data citra *grayscale* yang mempunyai ektensi *.BMP dan *.Jpg. Selanjutnya data citra ini pada hasil pengujian sistem diberi nama citra asli.

Lena.bmp Anak.bmp Bunga.bmp Kamera.jpg

Gambar 6. Sample Data Penelitian

Data citra pada gambar 6, selanjutkan diamankan dengan cara diacak menggunakan algoritma Vernam *cipher*. Data citra hasil proses acak selanjutnya disebut citra acak. Kunci yang digunakan dapat berupa sebuah kalimat atau deretan angka-angka.

3.2. Implementasi Sistem

Implementasi sistem pada penelitian ini dituangkan dalam suatu bahasa pemogramaman MATLAB R2012b. Aplikasi dirancang dengan membuat dua bagian coding sesuai proses yang ada di algoritma vernam cipher yakni untuk proses enkripsi dan untuk proses dekripsi yang kemudin dilanjukan dengan pengujian sistem yang dibuat.

a. Listing untuk Proses Enkripsi

Berikut ini adalah penggalan koding yang digunakan untuk meng-enkripsi pesan berupa citra dengan menggunkan bahasa pemogrman Matlab.

```
A=imread([pathname jns]);
[n m] = size(A);
warning off all
if (ndims(A)~=3)
A = im2double(A);
pesan=A;
```

Gambar 7. Code ini digunakan memanggil citra

Perintah pada Gambar 7, digunakan membaca citra, selanjutnya melihat ukuran citra serta merubah tipe datanya ke format double.

```
[n m] = size(pesan);
pesan = reshape(pesan,[n*m 1]);
kunci = abs(kunci);
```

Gambar 8. Code ini digunakan memanggil citra

Perintah pada Gambar 8, digunakan melihat ukuran citra, lalu mengubah ukuran yang semula dalam bentuk matriks n x m menjadi vektor kolom dengan n x m. Selanjutnya jika kunci berupa kumpulan karakter maka kunci diubah menjadi numerik dengan perintah abs.

```
pp=length(pesan);
pk=length(kunci);
% membuat panjang kunci=panjang pesan
pjkunci=[];
k=floor(pp/pk);
for x=1:k;  %round utk pembulatan ke integer terdekat
pjkunci=[pjkunci kunci];
end;
```

Gambar 9. Code ini digunakan mengetahui panjang pesan dan kunci.

Perintah pada Gambar 9 digunakan untuk membuat panjang kunci sama dengan panjang pesan dalam hal vektor kolom citra.

```
pb=dec2bin(pesan);
pb2=pb(1:pp,1:8);
for i=1:pp
  for j=1:8
   hasil2=mod((pb2(1:pp,1:j)+pk2(1:pp,1:j)),2);
  end
end
hasil2;
```

Gambar 10. Code ini digunakan proses XOR pada algoritma Vernam cipher.

Perintah pada Gambar 10, berfungsi untuk melakukan proses XOR antara pesan dengan kunci yang diberikan. Sebelum proses XOR dieksekusi, terlebih dahulu nilai pesan yang berupa numerik dikonversi ke bilangan biner dengan panjang 8 bit. Pada program ini Operasi XOR saya ganti dengan operasi Modulo 2.

```
for i=1:pp
  for j=1:8
    nk= hasil2(i:i,1:j);
  end
  nk;
 db(i)=bin2dec(num2str(nk));
end
k=db(1:pp);
Se=reshape(k,[n m]);
```

Gambar 11. Code ini digunakan mengkonversi bilangan biner menjadi bilagan desimal

Perintah pada Gambar 11 dipergunakan untuk mendapatkan citra hasil proses XOR antara pesan dan kunci. Hasil proses XOR antara pesan dan kunci semula berupa deretan bit-bit dalam bentuk blok-blok dengan per-blok terdiri dari 8 bit. Selanjutnya bit-bit yang merupakan bilangan biner dikonversi ke bilangan desimal sebagai nilai pixel dari citra yang diperoleh.

3.3. Pengujian Sistem

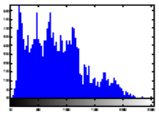
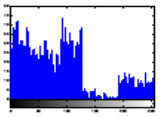
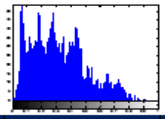
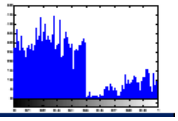
Pengujian sistem terhadap pesan berupa citra grayscale yang ber-ektensi ".bmp" dan .jpg. Selanjutnya di-enkrip dan di-dekrip menggunakan algoritma Vernam cipher dan kunci tertentu.

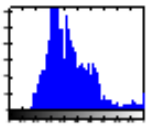
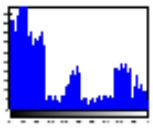
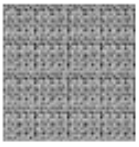
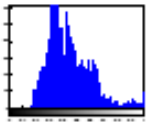
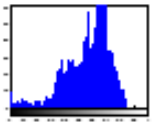
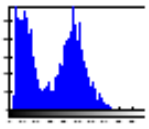
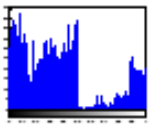
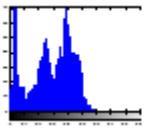
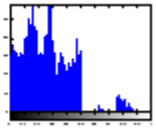
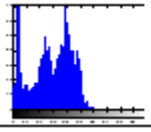
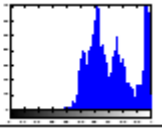
Tabel berikut ini hasil pengujian sistem terhadap beberapa citra dengan menggunakan beberapa kunci yang berbeda.

a. Proses Enkripsi

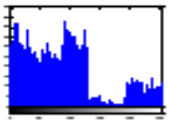
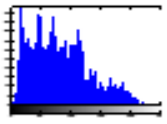
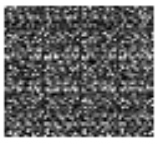
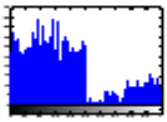
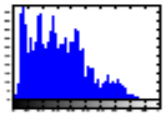
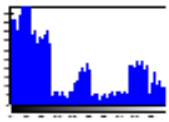
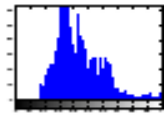
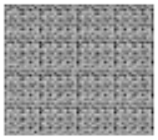
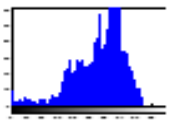
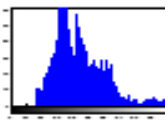
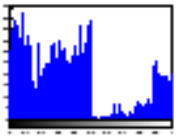
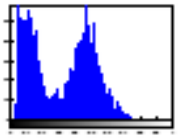
Hasil pengujian sistem untuk proses enkripsi atau proses mengacak pesan citra dapat dilihat pada Tabel 1.

Tabel 1. Hasil pengujian aplikasi untuk proses enkripsi

No	Citra Asli	Kunci	Citra Acak
1.		FAKULTAS MATEMATIKA DAN ILMU ALAM	
			
2.		Tujuan penelitian ini, membuat sebu-ah aplikasi atau perangkat lunak.	
			

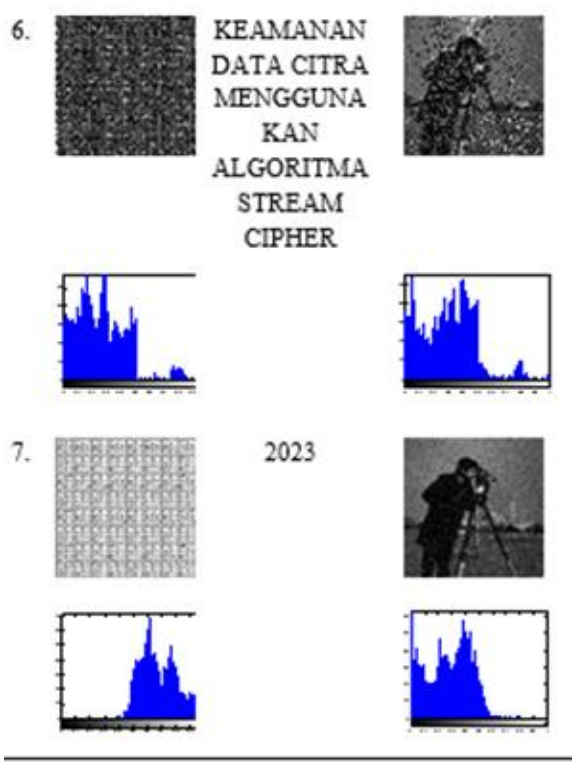
No	Citra Asli	Kunci	Citra Acak
3.		PROGRAM STUDI SISTEM INFORMASI UNCEN	
			
4.		2023	
			
5.		Program Studi Sistem Informasi jayapura Papua	
			
6.		KEAMANAN DATA CITRA MENGGUNA KAN ALGORITMA STREAM CIPHER	
			
7.		2023	
			

Tabel 2 Hasil pengujian aplikasi untuk proses dekripsi

No	Citra Acak	Kunci	Citra dekripsi
1.		FAKULTAS MATEMATIKA DAN ILMU ALAM	
			
2.		Tujuan penelitian ini, membuat sebu-ah aplikasi atau perangkat lunak.	
			
3.		PROGRAM STUDI SISTEM INFORMASI UNCEN	
			
4.		2023	
			
5.		Program Studi Sistem Informasi jayapura Papua	
			

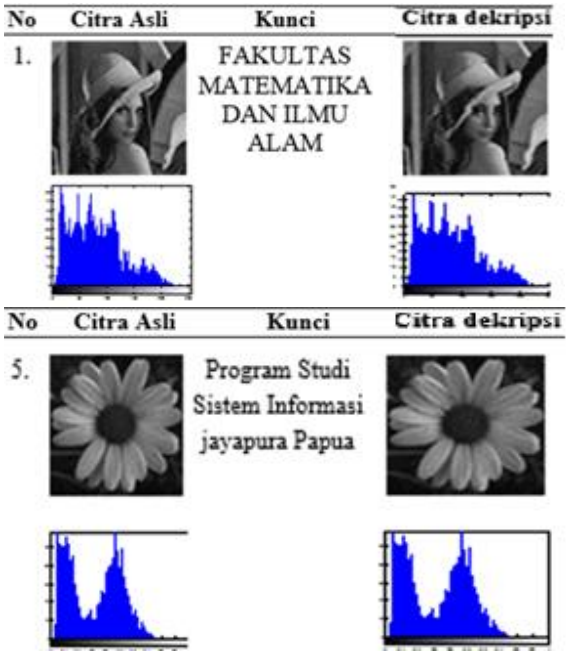
b. Proses Dkripsi

Hasil pengujian sistem untuk proses dekripsi atau proses mengembalikan pesan acak menjadi pesan awal (citra dekripsi) dapat dilihat pada Tabel 2.



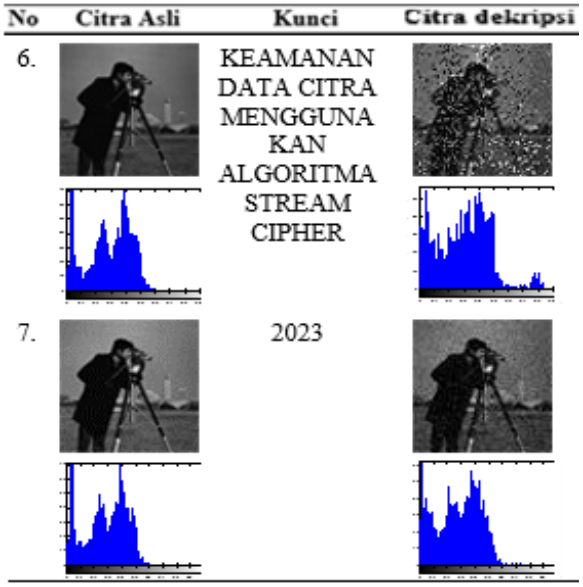
Tabel 1 merupakan tabel hasil pengujian sistem untuk proses enkripsi yakni mengacak pesan citra menjadi pesan citra yang teracak. Untuk Nomor 1 sampai dengan 5 menggunakan pesan citra yang digunakan untuk pengujian ber-ekstensi *.bmp sedangkan untuk Nomor 6 dan 7 citra ber-ektensi .jpg. Hasil pengujian menunjukkan proses enkripsi berhasil dengan baik, citra teracak dengan baik. Algoritma Vernam cipher dapat meyembunyikan citra aslinya. Sedangkan dilihat dari grafik sebaran nilai pixel (*histogram*) hasil enkripsi, citra ter-enkripsi kurang baik, karena nilai pixel yang terendah sampai yang terbesar tidak tersebar secara merata.

Tabel 2 merupaka proses dekripsi, proses yang digunakan untuk mengembalikan pesan ter-acak pada Tabel 1 menjadi pesan citra asli atau pesan citra semula. Untuk Nomor 1 sampai 5, pesan citra ter-acak berhasil dikembalikan dengan sangat baik, mirip dengan citra awal. Kemiripan antara pesan citra awal dengan citra dekripsi bisa lihat dari sebaran nilai pixel (*histogram*) antara citra asli dengan citra dekripsi dari masing-masing citra, sebagaimana pada Gambar 12, di bawahini



Gambar 12. Citra dan histogram citra asli dan citra

Sedangkan untuk proses dekripsi untuk Nomor 6 dan 7 Pada Tabel 2, citra acak dapat dikembalikan namun terjadi destorsi karena adanya noise.lebih jelas bisa dilihat pada Gambar 13, di bawah ini.



Gambar 13. Citra acak dikembalikan seperti citra asli namun mengalami destroy karena noise.

4. DISKUSI

Hasil penelitian keamanan data citra menggunakan algoritma Vernam cipher menunjukkan bahwa proses enkripsi dan dekripsi berjalan dengan baik. Dalam penelitian ini algoritma Vernam *cipher* yang digunakan beroperasi dalam bentuk bit tunggal. penelitian sebelumnya yang berhubungan keamanan data citra diantaranya dilakukan oleh Furqan, dkk dengan judul *digital Image Security System Using Spritz Algorithm* [14].

kesimpulan yang diperoleh diantaranya pengmanan citra digital menggunakan algoritma Spritz berhasil menyamarkan citra digital yang informasinya dapat dilihat menjadi citra digital yang tidak dapat dikenali oleh mata manusia.

Supiyanto dan Mandowen, melakukan penelitian tentang pengamanan data citra dengan judul penelitiannya : *Advanced Hill Cipher Algorithm For Security Image Data With The Involutory Key Matrix* [19]. hasil penelitin ini menyimpulkan algoritma advanced hill cipher dapat mengamankan data citra dengan sangat baik. Ini dapat dilihat dari grafik sebaran nilai pixel (histogram), dari nilai pixel yang terendah sampai yang terbesar tersebar secara merata. Ini menandakan bahwa citra hasil enkripsi, ter-enkripsi dengan sangat baik.

Adapun pengamanan data citra dengan algoritma vernam cipher, sebaran nilai pixel belum merata, ini dapat dilihat pada histogram hasil enkripsi setiap citra. Namun demikian algoritma ini tetap dapat digunakan untuk pengamanan data citra. Hasil proses enkripsi menggunakan algoritma vernam cipher sudah dapat meyembunyikan citra aslinya.

5. KESIMPULAN

Berdasarkan hasil dan pembahasan hasil pengujian aplikasi dengan menggunakan algoritma Vernam cipher untuk pengamanan data citra, maka dapat diambil kesimpulan bahwa metode Vernam cipher yang diimplementasikan menggunakan bahasa pemrograman Matlab dapat melakukan enkripsi dan dekripsi pada citra digital dengan baik. Proses penyandian citra dengan metode Vernam cipher menunjukkan keteracakan yang cukup signifikan, hal ini menunjukkan bahwa proses enkripsi berhasil dengan baik.

Proses Dekripsi dengan metode Vernam cipher dari citra yang telah ter-enkripsi .Jpg dapat dikembalikan seperti citra semula atau citra asli walaupun ada citra hasil dekripsi yang mengalami destorsi. Namun demikian, proses dekripsi berhasil dengan baik. Sedangkan untuk citra yang ber-ektensi .bmp, citra enkripsi dapat dikembalikan dengan sangat baik. Citra hasil dekripsi hampir 100% menyerupai citra aslinya.

Proses pengamanan data citra pada aplikasi ini dapat menggunakan kunci yang berupa string atau angka dengan panjang beragam.

UCAPAN TERIMA KASIH

Tim peneliti menyampaikan terima kasih kepada Rektor UNCEN untuk dana penelitian dari PNBP UNCEN tahun 2023.

DAFTAR PUSTAKA

[1] Supiyanto and T. Suparwati, “Penerapan Matriks Invers Tergeneralisasi (MIT) Untuk Keamanan Data Pada Sandi Hill,” Indonesia, 2020.

[2] A. Hermansyah and K. M. Helma widya, Syafrawali Pasaribu, “No Title,” in *Prosiding Seminar Nasional Teknik UISU (SEMNASTEK)*, 2019, pp. 200–2006.

[3] N. R. Reddy, C. Aravind Kumar, P. Rajkumar, and V. Velde, “Public key authentication schemes in asymmetric cryptography,” *Mater. Today Proc.*, no. xxxx, pp. 1–5, 2021, doi: 10.1016/j.matpr.2021.02.172.

[4] C. Y. Milian and Sulistyo W., “Model Pengembangan Keamanan Data dengan Algoritma ROT 13 Extended Vernam Cipher dan Stream Cipher,” *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 7, no. 2, pp. 208–216, 2023, doi: 10.35870/jtik.v7i2.716.

[5] Z. Shabrizqi, “Penerapan Algoritma Vegenere Cipher Dan Vernam Cipher Dalam Penggamanan File Text,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 6, no. 3, pp. 326–332, 2019.

[6] Supiyanto, A. D. Saputro, and M. Asghar, “Text Data Security Using Stream Cipher Algorithm,” vol. 6, no. 158, pp. 613–617, 2023.

[7] M. Sutikno, K. Dibiyo, and Aisyatul, “IMPLEMENTASI VERNAM CIPHER DAN STEGANOGRAFI END OF FILE (EOF) UNTUK ENKRIPSI PESAN PDF,” *Techno.COM*, vol. Vol. 15, 2016.

[8] Y. Irnanda, “Enkripsi dan Dekripsi Dengan Menggunakan Metode Kriptografi Vernam Cipher (XOR),” *Kumpul. Karya Ilm. Mhs. Fak. sains dan Tekhnologi*, vol. 1, no. 1, p. 47, 2019.

[9] S. M. Bellovin, “Inventor of the One-Time Pad,” in *Cryptologia*, 2011, pp. 203–222.

[10] A. Simangunsong and R. M. Simanjorang, “Simulation of The Application of Intelligence in Vernam Cipher Cryptography (One Time Pad),” vol. 15, no. 1, pp. 2723–8695, 2021.

[11] M. H. D. Firmansyah, “Aplikasi Enkripsi Dan Dekripsi Dengan Teknik XOR Menggunakan Metode Vernam Cipher,” *Kumpul. Karya Ilm. Mhs. Fak. sains dan Tekhnologi*, vol. 2, no. 2, p. 8, 2021.

[12] P. D. . Silitonga and S. Pakpahan, “Application of Integers in Vernam Cipher Cryptography (One Time Pad),” vol. 9, no. 2, pp. 350–353, 2021.

[13] G. N. Salmi and F. Siagian, "Implementation of the data encryption using caesar cipher and vernam cipher methods based on CrypTool2," *J. Soft Comput. Explor.*, vol. 3, no. 2, pp. 99–104, 2022, doi: 10.52465/joscex.v3i2.86.

[14] M. Furqan, R. R. Kurniawan, Hasugian A H, and N. I. Z. H, "Digital Image Security System Using Spritz Algorithm," *Infokum*, vol. 10, no. 1, pp. 392–397, 2021.

[15] Supiyanto and T. Suparwati, "Perbaikan Kualitas Citra Menggunakan Metode Contrast Stretching," *J. Siger Mat.*, vol. 02, no. 2, p. 13, 2021, doi: 10.26623/transformatika.v8i2.48.

[16] G. Miftakhul Fahmi, K. N. Isnaini, and D. Suhartono, "Implementation of Steganography on Digital Image With Modified Vigenere Cipher Algorithm and Least Significant Bit (Lsb) Method," *J. Tek. Inform.*, vol. 4, no. 2, pp. 333–344, 2023, doi: 10.52436/1.jutif.2023.4.2.340.

[17] M. H. D. Firmansyah, "Aplikasi Enkripsi Dan Dekripsi Dengan Teknik XOR Menggunakan Metode Vernam Cipher," 2021. [Online]. Available: https://jurnal.pancabudi.ac.id/.

[18] M. Jumeidi, D. Triyanto, and Y Brianorman, "Implementasi Algoritma Kriptografi Vernam Cipher Berbasis Fpga," *Coding J. Komput. dan Apl.*, vol. 4, no. 1, 2016, doi: http://dx.doi.org/10.26418/coding.v4i1.13329.

[19] Supiyanto and S. A. Mandowen, "Advanced hill cipher algorithm for security image data with the involutory key matrix," *J. Phys. Conf. Ser.*, vol. 1899, no. 1, pp. 1–8, 2021, doi: 10.1088/1742-6596/1899/1/012116.