

## **PENERAPAN ALGORITMA VERNAM CIPHER DALAM PENGAMANAN CITRA DIGITAL**

Sartika dewi

STMIK Kristen Neumann Indonesia Jl. Letjen Jamin Ginting KM.10,5 Medan

[Sartikadewi18111996@gmail.com](mailto:Sartikadewi18111996@gmail.com)

Program Studi Teknik Informatika

### **ABSTRAK**

*Kriptografi atau yang sering dikenal dengan sebutan ilmu penyandian data adalah suatu bidang ilmu dan seni yang bertujuan untuk menjaga kerahasiaan suatu pesan yang berupa data-data dari pihak lain yang tidak berhak sehingga tidak menimbulkan kerugian. Pada masa sekarang ini, kriptografi atau ilmu penyandian data sering diklasifikasikan menjadi dua jenis yaitu kriptografi klasik dan kriptografi modern. Penerapan Algoritma Vernam Cipher dalam Pengamanan Citra Digital untuk proses menyandikan suatu gambar. Penyandian gambar dapat membantu kerahasiaan gambar yang akan dirahasiakan dari siapa pun*

**Kata Kunci:** citra digital, vernam cipher, kriptografi, gambar, kerahasiaan

### **PENDAHULUAN**

Seiring dengan sangat pesatnya kemajuan teknologi jaringan informasi khususnya di bidang komputer, seseorang memungkinkan untuk bertukar informasi secara jarak dekat maupun jauh. Informasi ada yang bersifat umum dan ada yang bersifat rahasia. Bentuk informasi pun sangat banyak seperti teks, gambar, suara, video, dan lain sebagainya. Di era modern ini pertukaran informasi jarak jauh bukan merupakan suatu masalah lagi, dikarenakan adanya jalur transmisi informasi jarak jauh. Jalur transmisi informasi jarak jauh sangat

beragam bentuknya salah satunya dengan internet. Tetapi informasi yang melalui internet tidak terjamin kerahasiaannya. Dikarenakan internet adalah media transmisi informasi yang bisa di akses siapa saja, kapan saja, dan dimana saja. Dengan demikian semakin banyak pengguna maka semakin banyak serangan yang mungkin terjadi dalam proses pertukaran informasi di internet.

Kriptografi atau yang sering dikenal dengan sebutan ilmu penyandian data adalah suatu bidang ilmu dan seni yang bertujuan untuk menjaga kerahasiaan suatu pesan yang berupa data-data dari pihak lain yang tidak berhak sehingga

tidak menimbulkan kerugian. Pada masa sekarang ini, kriptografi atau ilmu penyandian data sering diklasifikasikan menjadi dua jenis yaitu kriptografi klasik dan kriptografi modern.

Kriptografi dan enkripsi sangat dibutuhkan dalam pengamanan gambar dengan menggunakan citra digital, data atau informasi yang dikirim dapat terhindar dari pembajakan, pengapusan yang dilakukan oleh user yang tidak berhak.

Berdasarkan latar belakan yang telah diuraikan, maka rumusan masalah penulis adalah :

1. Bagaimana membangun aplikasi yang dapat digunakan untuk menyandikan gambar melalui proses kriptografi.
2. Bagaimana penerapan algoritma vernam cipher dalam pengamanan Citra Digital.  
Tujuan dari penelitian adalah :
  - a. Menjaga kerahasiaan gambar
  - b. Menerapkan ilmu-ilmu dalam merancang sebuah sistem yang telah diperoleh selama kuliah.

### **Definisi Kriptografi**

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pengertian ilmu yang mengajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan

data, intergrasi data. Menurut buku yang berjudul “Applied Cryptography” karangan Bruce Schneider (John Wiley & Sons, 1996), kriptografi merupakan suatu seni atau ilmu untuk menjaga kerahasiaan dari sebuah tulisan agar tetap aman, tanpa diketahui pihak yang tidak berkepentingan. Pakar ilmu kriptografi dikenal sebagai kriptografer. Selain kriptografi, ada kriptanalisis yang merupakan kebalikan dari proses kriptografi dalam kriptologi. Kriptologi ini termasuk kedalam salah satu cabang ilmu algoritma dibidang matematika. Para pelaku kriptologi dikenal sebagai kriptologis. Pada kriptanalisis, penganalisan dan pemecah kode ciphertext menjadi plaintext tanpe melalui proses dekripsi yang wajar disebut kriptanalisis. Algoritma kriptografi dan seluruh kemungkinan *ciphertext*, *plaintext* dan kunci yang disebut kriptosystem. *Plaintext* adalah pesan/data asli yang dapat dibaca. *Ciphertext* adalah pesan data yang di acak, yang sulit diartikan. Kunci adalah nilai yang digunakan untuk mengubah *plaintext* menjadi *ciphertext*.

### **Vernam cipher**

Vernam cipher merupakan salah satu algoritma kriptografi klasik untuk menyandikan suatu plaintext dengan menggunakan teknik substitusi. Vernam cipher yang juga

merupakan system kerahasiaan yang sempurna dimana plaintext dikombinasikan dengan key yang sama panjang untuk menghasilkan ciphertext

Vernam cipher merupakan algoritma kriptografi yang ditemukan oleh Mayor J. Maugborne dan G. Vernam. Algoritma Vernam cipher diadopsi dari one time pad cipher, dimana dalam hal ini karakter diganti dengan bit (0 atau 1). Dengan kata lain, vernam cipher merupakan versi lain dari one-time pad 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 stream cipher dimana cipher berasal dari hasil operasi XOR antara bit plainteks dan bit key . Pada cipher aliran, bit hanya mempunyai dua buah nilai, sehingga proses enkripsi hanya menyebabkan dua keadaan pada bit tersebut, yaitu berubah atau tidak berubah. Dua keadaan tersebut ditentukan oleh kunci enkripsi yang disebut dengan aliran-bit-kunci (keystream). Secara sederhana proses enkripsi dan dekripsi algoritma vernam cipher dapat adalah pada Gambar . Gambar .Proses Enkripsi dan Dekripsi Algoritma Kriptografi Vernam Cipher

### Citra Digital

Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra terbagi 2 yaitu ada citra yang bersifat analog dan ada citra yang bersifat digital. Citra analog adalah citra yang bersifat kontinu seperti gambar pada monitor televisi, foto sinar X, hasil CT Scan dll. Sedangkan pada citra digital adalah citra yang dapat diolah oleh komputer( T,Sutoyo *et al.* 2009: 9). Sebuah citra digital dapat mewakili oleh sebuah matriks

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M-1) \\ f(1,0) & \dots & \dots & f(1,M-1) \\ \dots & \dots & \dots & \dots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,M-1) \end{bmatrix}$$

### METODE PENELITIAN

Masalah yang diselesaikan dalam skripsi ini antara lain adalah menerapkan algoritma *vernam cipher* digunakan untuk enkripsi dan dekripsi dalam gambar. Pada subbab ini dilakukan beberapa analisis yaitu enkripsi dan dekripsi sistem dan perancangan proses sistem yang akan dibangun.

a. Proses Citra

Proses citra yaitu mengambil nilai perpixel pada gambar yang akan diproses pada gambar yang akan di sandikan yang akan diubah menuju ke vernam cipher.

b. Menu Enkripsi / Dekripsi

Di menu ini akan mengubah RGB perpixel pada gambar menjadi bilangan biner. Jika gambar yang telah disandikan maka menggunakan dekripsi. Dan sebaliknya jika gambar yang mau disandikan maka menggunakan enkripsi.

c. Masukan kunci

Kunci yang dimasukkan menggunakan kunci vernam cipher untuk mengubah gambar citra.

d. Plaintext

Plaintext merupakan gambar yang belum disandikan yang harus diubah menjadi ciphertext plaintext akan digunakan dahulu jika diketahui enkripsi, dan sebaliknya jika diketahui dekripsinya maka menggunakan ciphertext.

e. Program keluar

Jika program selesai maka akan keluar jika ingin lanjut maka akan kembali ke menu awal diproses citra.

## HASIL DAN PEMBAHASAN

### Hasil Pembahasan

#### Form Utama

Program ini menggunakan aplikasi Visual Studio. Ada dua form didalam form utama yaitu : form enkripsi dan form dekripsi.



#### Form Enkripsi

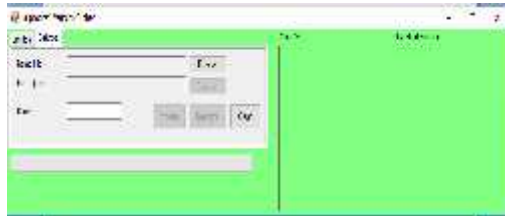
Form enkripsi dimana bagian dari form ini yaitu *text field file* input untuk menginputkan gambar yang akan di enkripsi, *button* load citra untuk mencari gambar di file yang akan di enkripsi, *button* proses adalah tombol untuk mengetahui hasil per pixel citra, *button* enkripsi untuk mengubah gambar dan mengitung hasil *vernem cipher*, *button* clear untuk menghapus semua inputan dan keluaran dari enkripsi.



#### Form Dekripsi

Form dekripsi bagian dari form ini yaitu *text field file* input untuk menginputkan gambar yang telah disandikan di dekripsi, *button* browse untuk mencari gambar yang telah disandikan di file penyimpanan, *button* proses adalah tombol untuk mengetahui hasil per pixel citra,

*button* dekripsi untuk mengubah gambar yang telah disandikan kembali ke gambar sempurna dan mengitung hasil *vernam cipher*, *button* clear untuk menghapus semua inputan dan keluaran dari dekripsi



### Proses Enkripsi

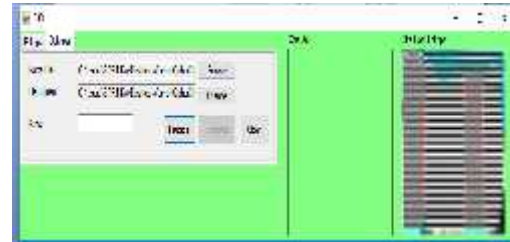
Pada proses Enkripsi ini pertama penulis, contohnya gambar yang telah di ubah pikselnya menjadi 50x50 setelah itu akan otomatis masuk ke dalam *textbox* tersebut

Setelah itu di input kunci yang akan sama digunakan untuk dekripsi. Kunci yang digunakan tergantung pada berapa kunci yang di berikan



### Proses Dekripsi

Sebelumnya sudah dijelaskan bahwa dekripsi disini mengubah hasil enkripsi atau mengembalikan gambar seperti semula. Dekripsi menggunakan kunci yang sama dengan enkripsi agar gambar dapat di buka



### Kesimpulan

Kesimpulan yang didapatkan dari perancangan penyandian gambar dengan menggunakan system pemograman visual basic adalah sebagai berikut:

1. Program aplikasi ini dirancang untuk menjaga kerahasiaan gambar sehingga gambar terjaga kerahasiaannya.
2. Pada aplikasi ini penyandian gambar memiliki kunci dekripsi untuk membuka sehingga keamanan nya terjaga.
3. Perangkat lunak ini hanya menyandikan gambar bukan teks.

### Daftar Pustaka

- 1 Aria Rahajoeningroem, (2011), "Studi dan Implementasi Algoritma Vernam Cipher untuk Pengamanan Data Transkrip Akademik Mahasiswa".
2. Ariyus, D. 2008. *Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi*. ANDI: Yogyakarta.
3. Debbie W. Leung, Quantum Vernam Cipher, Quantum Information and Computation, Vol. 1, 2001, Rinton Press.
- 4.
5. Madcoms, Madiun, Visual Basic, Penerbit Andi

6. Purnomo Mauridhi Hery, Muntasa Arif, “ *Konsep Pengolahan Citra Digital dan Ekstraksi Fitur* “, Graha Ilmu Yogyakarta, 2010.
7. Sholeh, M., & Hamokwarong, J. V. (2011). Aplikasi Kriptografi Dengan Metode Vernam *Cipher* Dan Metode Permutasi Biner. Momentum, Vol. 7, No. 2, 8-13.
8. Sholeh, & Hamokwarong, (2011), “Aplikasi Kriptografi dengan Metode *Vernam Cipher* dan Metode Permutasi Biner”.
9. Sutoyo. T, Mulyanto. Edy, Suhartono. Vincent, Dwi Nurhayati Oky, Wijanarto, “ *Teori Pengolahan Citra Digital* ”, Andi Yogyakarta dan UDINUS Semarang,