IMPLEMENTASI ENKRIPSI CITRA DIGITAL MENGGUNAKAN SANDI HILL

M. Irwan Ukkas [1)], Reza Andrea [2)], Miftahul Huda[3)]

[1]Teknik Informatika, STMIK Widya Cipta Dharma
[2]Teknik Informatika, STMIK Widya Cipta Dharma
[3]Teknik Informatika, STMIK Widya Cipta Dharma
[1,2,3]Jl. M. Yamin No.25, Samarinda, 75123
E-mail : Irwan212@yahoo.com [1)], reza@bibirdesign.com[2)], rezafahlefi79@gmail.com[3)]

ABSTRAK

Penyandian Citra Digital dengan Sandi *Hill* dengan menggunakan Metode Sandi *Hill*, merupakan bentuk penlitian untuk membuktikan bahwa algoritma Sandi *Hill* dapat digunakan untuk pencarian solusi, khususnya pada permasalahan kerahasiaan gambar.

Tujuan dari penelitian ini adalah merancang dan membangun sebuah aplikasi yang dapat menyelesaikan masalah eknripsi gambar untuk merahasiakan sebuah gambar atau citra dengan mengacak nilai dari warna RGB yang terdapat pada gambar dengan menggunakan bahasa pemrograman Microsoft Visual Studio 2012. Dalam penelitian ini, teknik pengumpulan data yang digunakan adalah studi pustaka. Metode pengujian yang digunakan adalah dengan pengujian *White-Box.*

Adapun hasil akhir dari penelitian ini yaitu diharapkan dapat membangun sebuah aplikasi pengamanan citra yang berupa data gambar, sehingga bisa lebih mempersulit aktifitas pelaku *cyber crime*.

Kata Kunci: *Hill Cipher, Image,* Enkripsi

1. PENDAHULUAN

Penyandian citra digital merupakan salah satu metode pengamanan data yang bersifat penting dan tetap harus terjaga kerahasiaan dan keamanannya dari orang yang tidak bertanggung jawab. Seiring dengan peningkatan kepentingannya banyak metode-metode yang digunakan dalam menyandikan suatu citra digital.

Salah satu metode yang dapat digunakan adalah metode sandi *Hill*. Metode ini hanya membutuhkan sebuah matriks kunci yang akan digunakan dalam proses enkripsi dan deskripsi. Syarat sebuah matriks kunci agar dapat digunakan dalam proses penyandian citra digital dengan sandi *Hill* adalah matriks tersebut harus mempunyai invers.

Penyandian dengan sandi *Hill* dilakukan dengan memanfaatkan operasi matriks biasa. Penyandian dilakukan pada tiap blok teks yang berukuran sama dengan ordo matriks kunci yang digunakan sebagai perluasannya maka sandi *Hill* tidak hanya dilakukan pada teks tetapi juga dilakukan untuk menyandikan suatu citra digital. Matriks yang digunakan adalah matriks persegi berordo 3 x 3 dengan bilangan bulat dikarenakan kode ascii hanya mencakup bilang bulat maka penulis hanya menggunakan bilangan bulat (integer).

2. RUANG LINGKUP PENELITIAN

1. Cakupan Permasalahan

Rumusan masalah yang akan dibahas pada skripsi ini adalah : “Bagaimanakah membuat metode sandi Hill untuk mengenkripsi nilai RGB dari citra sebenarnya sehingga gambar citra asli dapat disembunyikan atau disandikan.”?

2. Batasan masalah pada penelitian ini adalah

1) Implementasi enkripsi tidak untuk gambar yang berekstensi animasi gif dan png.
2) Enkripsi dapat pula diterapkan pada gambar *grayscale*, *black and white*, dan gambar digital lainnya yang berekstensi bmp dan jpg.
3) Kunci yang digunakan adalah karakter angka bilangan bulat (integer).
4) Maksimal karakter kunci yang digunakan adalah 4 karakter, hal ini dilakukan agar proses enkripsi tidak memakan waktu yang terlalu lama.
5) Batas matriks kunci yang digunakan adalah perkalian 3 x 3 dan berupa bilangan bulat.
6) Hanya matriks yang nilai determinannya 1 yang dapat digunakan untuk proses enkripsi.
7) Program dibangun hanya untuk enkripsi, tidak untuk dekripsi.

3. Tujuan Penelitian

Adapun tujuan penelitian yang ingin dicapai adalah sebagai berikut :

1) Mengimplementasi Enkripsi Citra
2) Hitung Estimasi Waktu

4. Manfaat Penelitian

Adapun manfaat penelitian adalah sebagai berikut :

1) Menyembunyikan informasi penting sebuah citra yang terenkripsi.
2) Metode sandi hill sebagai metode alternatif sistem pengamanan citra digital.
3) Mengetahui proses yang terjadi ketika proses enkripsi dengan menggunakan algoritma sandi hill.

3. BAHAN DAN METODE

3.1 Algoritma

Istilah algoritma berasal dari nama seorang pengarang berkebangsaan Arab bernama Ja'fat Mohammed bin Musa al Khowarizmi tahun (790 – 840), yang sangat terkenal dengan sebutan bapak Aljabar. Secara defenisi algoritma adalah alur pemikiran yang logis yang dapat dituangkan ke dalam bentuk tulisan. Sebuah algoritma dikatakan benar (*correct*) jika algoritma tersebut berhasil mengeluarkan *output* yang benar untuk semua kemungkinan *input*. (Rachmat, 2010).

3.2 Enkripsi

Enkripsi merupakan bagian dari kriptografi, dan merupakan hal yang sangat penting supaya keamanan data yang dikirimkan bisa terjaga kerahasiaannya. Enkripsi bisa diartikan dengan chiper atau kode, di mana pesan asli (*plaintext*) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan.

3.3 Kriptografi

Menurut Ariyus Dony (2008) Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata *Crypto* dan *Graphia* yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali.

Proses tranformasi dari *plaintext* menjadi *ciphertext* disebut proses Encipherment atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali *ciphertext* menjadi *plaintext* disebut proses dekripsi (*decryption*).

Untuk mengenkripsi dan mendekripsi data. Kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (*key*). Cipher adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi data. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.

Algoritma kriptografi modern tidak lagi mengandalkan keamanannya pada kerahasiaan algoritma tetapi kerahasiaan kunci. *Plaintext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *ciphertext* yang berbeda pula. Dengan demikian algoritma kriptografi dapat bersifat umum dan boleh diketahui oleh siapa saja, akan tetapi tanpa pengetahuan tentang kunci, data tersandi tetap saja tidak dapat terpecahkan.

3.4 Citra Digital

Menurut Darma Putra (2010) Citra adalah gambar pada bidang dua dimensi. Dalam tinjauan matematis, citra merupakan fungsi kontinu dari intensitas cahaya pada bidang dua dimensi. Ketika sumber cahaya menerangi objek, objek memantulkan kembal sebagian cahaya tersebut. Pantulan ini ditangkap oleh alat-alat pengindera optik, misalnya mata manusia, kamera, *scanner* dan sebagainya.

Bayangan objek tersebut akan terekam sesuai intensitas pantulan cahaya. Ketika alat optik yang merekam pantulan cahaya itu merupakan mesin digital, misalnya kamera digital, maka citra yang dihasilkan merupakan citra digital. Pada citra digital, kontinuitas intensitas cahaya dikuantisasi sesuai resolusi alat perekam.

3.2 Algoritma *Hill Cipher*

Hill cipher yang merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher*, karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula(Arya Widyanarko, 2009).

Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. *Hill Cipher* diciptakan oleh Lester S. Hill pada tahun 1929. *Hill Cipher* tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. *Hill Cipher* termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext* saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas *ciphertext* dan potongan berkas *plaintext*. Teknik kriptanalisis ini

disebut *known-plaintext attack*. (Arya Widyanarko, 2009)

Contoh kasus:

Misalkan nilai rgb yang dienkripsi adalah : "*Red* : 97, *Green* : 98 *Blue* : 99" dan kunci yang digunakan adalah matriks 3x3 sebagai berikut: $\begin{bmatrix} 1 & 0 & 0 \\ 8 & 1 & 0 \\ 7 & 2 & 1 \end{bmatrix}$

Penyelesaian:

Tahapan enkripsi
Langkah 1:
Hitung C = K x P *mod* 256
dimana C=*ciphertext*, K=*key*(matriks), dan P=*Plaintext*.

Kunci3 x 3			Nilai	Hasil Perkalian	Mod	*Ciphertext*
1	0	0	97	97	256	**97**
8	1	0	98	874	256	**106**
7	2	1	99	974	256	**206**

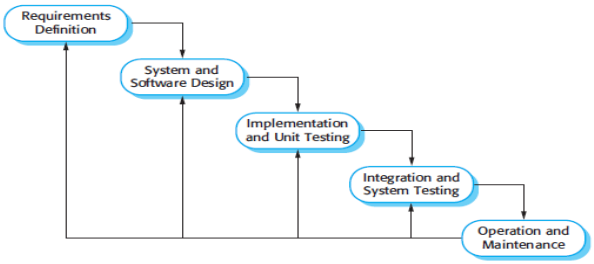
Sehingga nilai rgb yang telah ternekripsi adalah {97, 106, 206}

3.3 Aplikasi

Perangkat lunak aplikasi adalah program yang ditulis dan diterjemahkan oleh *language software* untuk menyelesaikan suatu aplikasi tertentu. Aplikasi juga merupakan program siap pakai yang digunakan manusia dalam melakukan pekerjaan dengan menggunakan komputer. (Jogiyanto,2005).

3.4 Metode Pengembangan Sistem

Dalam mengembangkan aplikasi ini, metode yang digunakan adalah model prototipe *(prototype).* Menggunakan model ini karena aplikasi yang dibuat yaitu aplikasi kamus istilah kesehatan dalam perancangannya antara *developer* dan *user* harus saling berkaitan, terlebih di dalam proses *input* istilah kosa kata dan definisinya yang dimana apabila terdapat kekurangan ataupun penambahan istilah kosa kata baru yang ingin ditambahkan, *user* dapat memberi masukkan kepada *developer* dan *developer* pun harus mendengarkan, memperbaiki dan kemudian dipresentasikan kepada pelanggan sehingga perangkat lunak yang dihasilkan nantinya sesuai dengan kebutuhan pelanggan.



Gambar 1. *Waterfall*

3.5 Teknik Pengumpulan Data Studi Pustaka

Metode-metode yang digunakan dalam pengumpulan data selama penelitian dengan mempelajari buku-buku literatur yang berhubungan dengan judul yang diambil sebagai bahan acuan atau dasar pembahasan, sehingga di dalam penulisan laporan tidak menyimpang dari teori-teori yang sebelumnya telah ada dan diakui kebenarannya.

3.6 Analisis Kebutuhan

Dari Hasil Penelitian, Kebutuhan-kebutuhan yang harus ada dalam membangun perangkat lunak ini dengan baik akan dijabarkan mengenai spsesifikasi minimun, dan juga fungsi yang terdapat dalam perangkat lunak.

3.6.1 Analisis Perangkat Keras

Pengoperasian penyandian citra ini membutuhkan seperangkat teknologi komputer dengan spesifikasi sebagai berikut:

1. ACER V3-471g
2. Processor Intel Core i5 2.5 ghz
3. Memory (DDR3) 4 GB
4. HardDisk 750 GB
5. VGA 2 GB NVIDIA GEFORCE

3.4.2 Analisis Perangkat Lunak

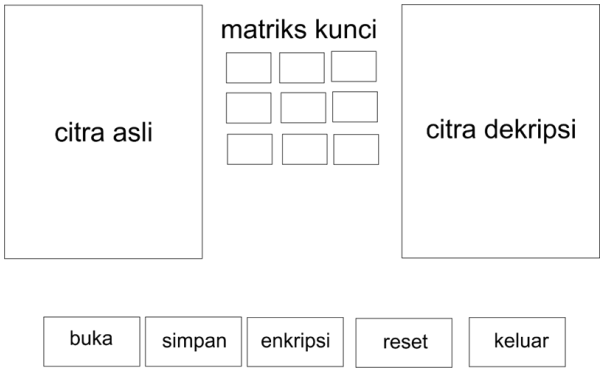
Adapun analisis perangkat lunak menggunakan perangkat sebagai berikut :

1. Sistem Operasi Windows 8.1 Enterprise 64 bit
2. Microsoft Visual Basic.NET 2012

Adobe Photoshop CC 2015

4. Rancangan Antarmuka

Berikut adalah perancangan antarmuka enkripsi citra digital menggunakan sandi hill :



Gambar 2. Rancangan Antarmuka

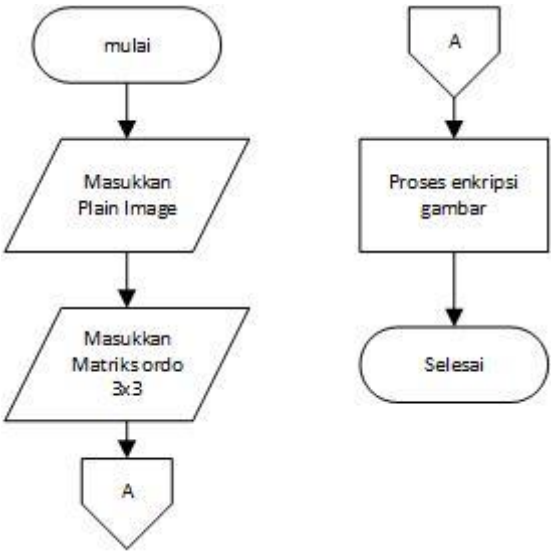
Gambar di atas adalah perancangan antarmuka enkripsi citra digital, pada *buton* reset berfungsi untuk menetralkan gambar, *button* enkrip berfungsi untuk mengenkripsi gambar asli, matriks kunci berfungsi untuk memasukkan kunci pengaman pada saat mengenkripsi gambar, *button* keluar berfungsi untuk keluar dari program, *button* open berfungsi untuk memsukan gambar yang akan di proses enkrip, *button save* berfungsi untuk menyimipan gambar yang telah selesai di enkrip.

5. IMPLEMENTASI

5.1 Implementasi Rancangan Sistem

Di dalam merancang aplikasi kamus istiah kesehatan ini, digunakan alat bantu untuk mempermudah proses perancangan sistem. Perancangan sistem ini menggunakan diagram alir *(flowchart).* Adapun *flowchat* pada aplikasi kamus istilah kesehatan digambarkan seperti berikut.

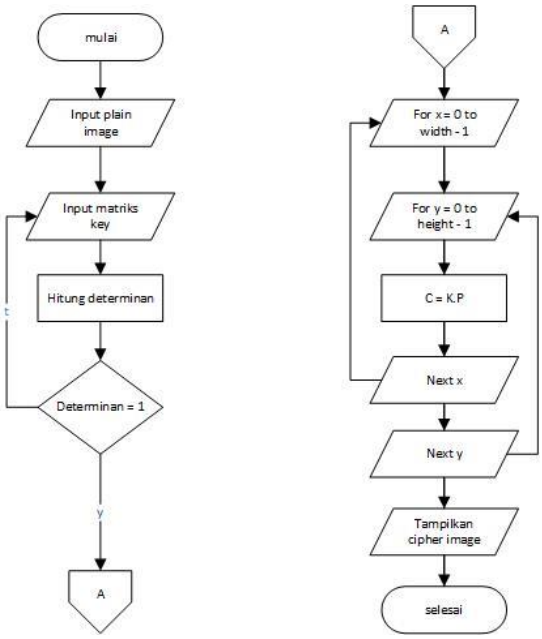
5.1.1 *Flowchart* Enkripsi Pesan



Gambar 3. *Flowchart* Enkripsi Pesan

Pada gambar 3. terlihat bagaimana diagram alir bagaimana cara mengenkripsi pesan. Di mulai dengan masuk memasukkan *plain image*. Dilanjutkan dengan memasukkan kunci matriks yang berordo 3x3 setelah itu lanjut ke proses enkripsi gambar dan selesai.

5.1.2 *Flowchart* Prosedur Enkripsi



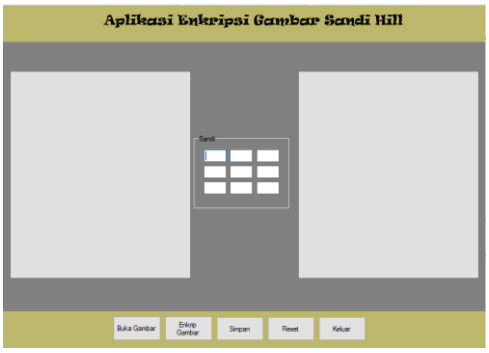
Gambar 4. *Flowchart* Prosedur Enkripsi

Pertama kita mulai, masukan gambar, masukan matriks kunci, hitung determinan, jika determinan = 1 maka lanjut ke tahap selanjutnya jika tidak maka masukkan lagi matriks kunci *for* x = 0 to *width* -1 artinya perulangan sebanyak lebar gambar, for y = 0 to *height* -1 artinya perulangan sebanyak tinggi gambar, C = K.P mod 256 adalah rumus dari perkalian matriks Sandi *Hill*, *next* y artinya pixel y selanjutnya, *next* x artinya pixel x selanjutnya, tampilkan *chiper image* artinya gambar telah terenkripsi dan ditampilkan, dan selesai.

5.2 Implementasi Program

Implementasi merupakan tahapan yang bertujuan mengubah hasil dari rancangan sistem menjadi bentuk nyata. Pada saat pertama kali aplikasi dijalankan maka akan muncul sebuah tampilan.

5.2.1 *Form* Utama Program



Gambar 6. Tampilan *Menu* Utama

Gambar 6 merupakan tampilan menu utama. Di dalam *form* menu utama terdapat beberapa menu, yaitu buka gambar, enkrip gambar, save, reset, keluar.

5.2.2 Pengujian Citra

Dibawah ini adalah pengujian terhadap berupa jenis tipe gambar :

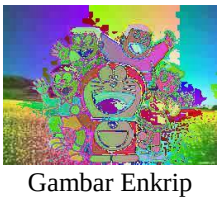
1. Gambar foto berwarna :

Gambar Asli

Gambar Enkrip

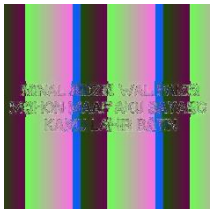
2. Gambar kartun berwarna :

Gambar Asli



Gambar Enkrip

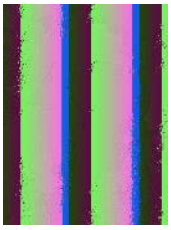
3. Gambar Tulisan



Gambar Asli Gambar Enkrip

4. Foto grayscale :


Gambar Asli Gambar Enkrip

5. Gambar *black and white*

Gambar Asli Gambar Enkrip

6. Gambar *invert*

Gambar asli Gambar enkrip

5.2.3 Penujian Perhitungan Waktu Estimasi Enkripsi Gambar

Dibawah ini adalah perhitungan waktu lama enkripsi gambar sesuai dengan resolusi gambar:

No	Ukuran Skala Gambar	Waktu Estimasi (*Second*)
1	1240 x 775	13.6250
2	1024 x 678	11.6250
3	3645 x 2364	110.9375
4	1600 x 675	12.9675
5	1198 x 805	15.3750
6	729 x 456	5.4687
7	670 x 335	2.5672
8	640 x 640	4.5691
9	500 x 360	1.8750
10	1080 x 807	8.9218

6. KESIMPULAN

Dengan adanya hasil penelitian yang dilakukan dan berdasarkan uraian uraian yang dibahas dalam bab-bab sebelumnya, maka dapat ditarik kesimpulan bahwa :

1. Metode Sandi Hill yang diaplikasikan dengan membuat kunci matriks 3x3 yang determinannya 1, pembuatan program dengan VB.Net 2012, sampai dengan pengujian menggunakan *white box*, perhitungan estimasi waktu dalam proses enkripsi.
2. Enkripsi dapat berfungsi pada semua jenis tipe gambar seperti gambar foto RGB, gambar kartun RGB, gambar tulisan, gambar *grayscale*, gambar *black and white*, dan gambar *invert*.
3. Semakin besar ukuran skala gambar, maka semakin lama waktu estimasi proses enkripsi, hal ini dikarenakan lamanya proses perhitungan setiap piksel gambar.
4. Dari hasil pengujian menggunakan *white box*, didapat pengujian terhadap tombol buka gambar, enkrip gambar, dan simpan semuanya bekerja dan berfungsi sebagaimana mestinya.

7. SARAN

Adapun saran-saran yang dapat dikemukakan yaitu sebagai berikut :

1. Dalam Pemrosesan enkripsi dan dekripsi kunci yang digunakan masih tergolong biasa maka lebih baik lagi untuk kunci di enkripsikan menggunakan metode yang berbeda dan metode yang lebih rumit.
2. Aplikasi dapat di kembangkan ke operasi sistem *handphone* seperti android dan windows phone.
3. Kunci yang digunakan dalam implementasi masih tergolong lemah karena sedikitnya jumlah kunci matriks, maka diharapkan untuk penelitian yang lebih lanjut terdapat ordo matriks yang dinamis.
4. Penelitian lebih lanjut diharapkan dapat mengenkripsi gambar sekaligus dalam jumlah yang besar.
5. Penelitian ini tidak sampai proses dekripsi, diharapkan diharapkan penelitian lebih lanjut dapat di implementasi lebih baik.

8. DAFTAR PUSTAKA

Dony, Ariyus. 2008. *Pengantar Ilmu Kriptografi.* Yogyakarta : ANDI.

Putra, Darma. 2010. *Pengolahan Citra Digital*. Yogyakarta : ANDI.

Daryanto. 2004, *Keterampilan Dasar Pengoprasian Komputer*. Bandung : Yrama Widya. Kadir,

Abdul. 2009. *Dasar Perancangan dan Implementasi Database Relasional. Yogyakarta : Andi Offset.*

Hariyono, Tri. 2009. *Enkripsi Gambar Menggunakan Algoritma Secure Imge Protection*. Surbaya.

Kurniawan, Agus. 2008, *Konsep dan Implementasi Cryptography Dengan .NET*. Jakarta: PC Media.

Lumbangaol, Rini Wati. 2012. *Aplikasi Pengamanan Gambar Dengan Algoritma Rivest-Shamir Adleman (RSA)*

Munir, Rinaldi, 2006, *Pengantar Kriptografi*, Bandung: Informatika.

Romdhoni, M. Arif. 2008, *Kriptografi visual pada biner dan citra berwarna serta pengembangannya dengan steganografi dan fungsi XOR. Sekolah Teknik Elektro dan informatika*, ITS. Surabaya.

Tjiharjadi Semuil. 2009, *Pengaman data menggunakan metode enkripsi Einstein. Sistem Komputer, Fakultas Teknik, Universitas Kristen Maranatha*. Bandung.

Hasim Ahmad 2014, *Enkripsi citra digital rgb dengan menggunakan metode vigenere*, STMIK Widya Cipta Dharma. Samarinda