

IMPLEMENTASI HILL CIPHER PADA CITRA MENGGUNAKAN KOEFISIEN BINOMIAL SEBAGAI MATRIKS KUNCI

Supiyanto

Program Studi Sistem Informasi Universitas Cenderawasih
Jl. Kamp. Walker Kampus Baru Waena Jayapura
e-mail : Supi6976@gmail.com

Abstrak

Hill cipher merupakan sebuah teknik kriptografi klasik, yang menggunakan matriks sebagai kunci dalam proses meng-enkripsi dan men-dekripsi pesan dengan tipe kunci yang digunakan adalah tipe kunci simetris. Hal ini menjadi keunggulan dalam algoritma hill cipher tapi kekurangannya, tidak semua matriks kunci yang digunakan untuk mengenkripsi plaintext mempunyai invers. Menggunakan matriks kunci yang tidak mempunyai invers, akan menyebabkan pesan hasil enkripsi tidak bisa didekripsi untuk menjadi pesan asli kembali. Tujuan dari penelitian ini adalah untuk mengatasi kekurangan dari algoritma Hill Cipher yakni menentukan matriks kunci yang dijamin mempunyai invers atau dapat dibalik. Dan pada penelitian ini menggunakan Koefisien-koefisien Binomial Newton sebagai entri-entri dari matriks kunci. Hasil penelitian ini berupa program aplikasi yang dapat digunakan untuk mengenkripsi dan mendekripsi gambar menggunakan algoritma Hill Cipher dengan matriks kunci yang selalu mempunyai invers karena determinan dari matriks kunci ini sama dengan satu. Penyandian citra dengan Hill Cipher menunjukkan keteracakan warna yang cukup signifikan, hal ini menunjukkan bahwa proses enkripsi berhasil dengan baik.

Kata Kunci : Enkripsi, Dekripsi, Hill Cipher, Binomial.

1. PENDAHULUAN

Perkembangan teknologi informasi sekarang ini membuat komunikasi menjadi semakin mudah dan luas. Penyampaian pesan melalui internet merupakan sarana komunikasi yang sangat mudah dan efisien. Sejalan dengan hal itu kemunculan dari file-file multimedia yang beraneka ragam memberi pengaruh yang cukup besar dalam kemajuan teknologi informasi ini sehingga memungkinkan seseorang untuk dapat menyampaikan pesan menggunakan file-file multimedia tersebut.

Faktor keamanan dalam proses pengiriman data melalui saluran internet menjadi factor yang penting. Apabila hal ini diabaikan, maka orang yang tidak berhak akan dengan mudah memanfaatkan data tersebut untuk tujuan tertentu. Jika hal ini terjadi ada dua pihak yang dirugikan yaitu pengirim data dan penerima data. Salah satu metode untuk mengamankan data tersebut adalah dengan menyamarkan menjadi tidak bermakna.

Kriptografi adalah seni atau ilmu meliputi prinsip-prinsip dan metode mengubah pesan yang dimengerti (*plaintext*) menjadi pesan yang tidak dapat dimengerti (*ciphertext*) dan kemudian retransforming pesan yang akan kembali ke bentuk aslinya.

Substitution cipher adalah salah satu komponen dasar dari cipher klasik. Dua macam Substitution cipher pada kriptografi klasik yaitu *Polyalphabetic Substitution Cipher* dan *Monoalphabetic Substitution Cipher*. Pada *Polyalphabetic Substitution Cipher*, enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda sehingga lebih sulit untuk menemukan pola enkripsinya. Pada *monoalphabetic substitution cipher*, satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain, sehingga pola enkripsinya lebih mudah diketahui, karena satu huruf pada ciphertext pasti merepresentasikan satu huruf pada plaintext.

Dalam tulisan ini, diusulkan penggunaan matriks kunci yang entri-entrinya berasal dari koefisien binomial newton pada algoritma hill cipher. Tujuannya adalah untuk mengatasi kelemahan dari penggunaan matriks kunci secara acak dalam algoritma Hill cipher untuk enkripsi, yang mungkin tidak dapat mendekripsi pesan terenkripsi, jika matriks kunci yang digunakan tidak dapat mempunyai invers atau tidak dapat dibalik.

Penggunaan koefisien binomial newton sebagai entri-entri pada matriks kunci, memastikan pesan dapat dideskripsi, karena matriks kunci ini selalu mempunyai invers. Suatu matriks akan selalu mempunyai invers apabila nilai determinan dari matriks tersebut tidak sama dengan nol.

2. METODE PENELITIAN

2.1 Hill Cipher

Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. *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. Oleh karena itu Hill Cipher termasuk dalam salah satu kriptosistem polialfabetik. Cipher ini ditemukan pada tahun 1929 oleh Lester S. Hill.

Berdasar jenis kunci yang dipakai, kriptografi Hill Cipher termasuk ke dalam Algoritma Simetrik (*Symmetric Algorithms*), karena algoritma ini menggunakan suatu kunci yang sama untuk proses enkripsi dan dekripsi pesan.

Dalam melakukan proses enkripsi dan dekripsi, algoritma ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan dan menerapkan aritmatika modulo.

Untuk enkripsi, algoritma ini mengambil m plaintext berurutan dan setiap karakter diberi nilai numerik seperti $a = 0, b = 1, \dots, z = 25$. Untuk $m = 3$, sistem persamaan dapat dijelaskan sebagai berikut:

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \text{ mod } 26 \\ C_2 &= (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \text{ mod } 26 \\ C_3 &= (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \text{ mod } 26 \end{aligned} \quad (1)$$

Persamaan di atas menggunakan modulo 26 dikarenakan alphabet yang digunakan pada proses enkripsi dan dekripsi sebanyak 26 karakter. Jika Persamaan di atas kita gunakan pada citra Grayscale atau Citra Warna (8 bit) maka Pers (1) menggunakan modul 256, sehingga Pers (1) menjadi :

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \text{ mod } 256 \\ C_2 &= (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \text{ mod } 256 \\ C_3 &= (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \text{ mod } 256 \end{aligned} \quad (1a)$$

Per (1) tanpa modular-nya dapat diekpresikan dalam bentuk vektor kolom dan matriks sebagai berikut :

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \quad (2)$$

atau sederhananya kita dapat menulis sebagai $\mathbf{C} = \mathbf{K}\mathbf{P}$, di mana \mathbf{P} dan \mathbf{C} adalah vektor kolom dengan panjang 3, masing-masing mewakili plaintext dan ciphertext, dan \mathbf{K} adalah matriks 3×3 , yang merupakan matriks kunci untuk enkripsi. Pada proses dekripsi membutuhkan invers dari matriks \mathbf{K} . Invers matriks \mathbf{K} (\mathbf{K}^{-1}) didefinisikan oleh persamaan $\mathbf{K}\mathbf{K}^{-1} = \mathbf{K}^{-1}\mathbf{K} = \mathbf{I}$, dimana \mathbf{I} adalah matriks identitas. secara umum kita dapat menulis sebagai berikut:

Untuk enkripsi:

$$\mathbf{C} = E_k(\mathbf{P}) = \mathbf{K}_p \mathbf{P} \quad (3)$$

Untuk Deskripsi:

$$\mathbf{P} = D_k(\mathbf{C}) = \mathbf{K}^{-1}\mathbf{C} = \mathbf{K}^{-1}\mathbf{K}_p \mathbf{P} \quad (4)$$

2.2 Aritmetika Modular

Operasi aritmatika yang disajikan di sini adalah penambahan, pengurangan, perkalian dan pembagian [9]. Berdasarkan ini, matriks kunci untuk algoritma Hill cipher ditentukan. Operator kongruensi modulo memiliki sifat sebagai berikut:

1. $a \equiv a \pmod{p}$
2. $a \equiv b \pmod{p}$ if $p|(a - b)$
3. $a \equiv b \pmod{p} \Rightarrow b \equiv a \pmod{p}$
4. $a \equiv b \pmod{p}$ and $b \equiv c \pmod{p} \Rightarrow a \equiv c \pmod{p}$

Misalnya $Z_p = [0, 1, \dots, p - 1]$ himpunan residu modulo p . Jika aritmatika modular dilakukan dalam himpunan Z_p ini, persamaan berikut menyajikan operasi aritmatika:

- a. Penjumlahan
 $(a + b) \pmod{p} = [(a \pmod{p}) + (b \pmod{p})] \pmod{p}$
- b. Negasi:
 $-a \pmod{p} = p - (a \pmod{p})$
- c. Pengurangan
 $(a - b) \pmod{p} = [(a \pmod{p}) - (b \pmod{p})] \pmod{p}$
- d. Perkalian
 $(a * b) \pmod{p} = [(a \pmod{p}) * (b \pmod{p})] \pmod{p}$
- e. Pembagian
 $(a / b) \pmod{p} = c$ when $a = (b * c) \pmod{p}$

2.3 Binomial Newton

Untuk Membuat pesan rahasia tetap aman tidak mudah diketahui orang lain yang tidak berhak, maka untuk menghadapi serangan semacam ini kriptografer harus menggunakan kunci yang lebih kompleks dan tidak mudah ditebak. Semakin kompleks kunci maka untuk waktu *exhaustive search* menjadi makin sulit dan bahkan tidak mungkin dilakukan karena waktu yang dibutuhkan semakin lama. Namun cara ini mempunyai kelemahan dimana untuk mengingat kunci yang sangat kompleks tentulah tidak mudah dalam proses operasinya yakni operasi perkalian matriks, penentuan invers dari matriks kunci yang digunakan dan harus juga dipastikan matriks yang digunakan selalu mempunyai invers.

Dalam penelitian ini, untuk memastikan bahwa matriks kunci yang digunakan selalu mempunyai invers maka kami gunakan matriks yang entri-entrinya diambil dari **koefisien-koefisien binomial**, ini karena nilai determinan dari ini sama dengan satu. Dengan demikian inversnya ada.

Teorema binomial memberikan bentuk ekspansi dari pangkat binomial $(x + y)^n$, untuk setiap n bilangan bulat tidak negatif dan semua bilangan real a dan b yang hasil penjabaran dari $(x + y)^n$ bergantung pada nilai n .

Sebagai contoh :

$$n = 1 \text{ maka } (x + y) = (1)x + (1)y$$

$$n = 2 \text{ maka } (x + y)^2 = (1)x^2 + (2)xy + (1)y^2$$

$$n = 3 \text{ maka } (x + y)^3 = (1)x^3 + (3)x^2y + (3)xy^2 + (1)y^3$$

$$n = 4 \text{ maka } (x + y)^4 = (1)x^4 + (4)x^3y + (6)x^2y^2 + (4)xy^3 + (1)y^4$$

dan seterusnya.

Koefisien a pada suku $ax^b y^c$ yang berupa angka yang diberi tanda kurung dikenal sebagai **koefisien binomial**.

Koefisien - koefisien binomial di atas memperlihatkan adanya suatu aturan yang dikenal dengan Segitiga Pascal, yang bentuknya sebagai berikut :

$$\begin{array}{cccc}
 & & 1 & 1 \\
 & & 1 & 2 & 1 \\
 & & 1 & 3 & 3 & 1 \\
 & & 1 & 4 & 6 & 4 & 1 \\
 & & 1 & 5 & 10 & 10 & 5 & 1
 \end{array}$$

dan seterusnya.

Berikut ini contoh cara menggunakan koefisien binomial sebagai entri-entri untuk matriks kunci pada keamanan data menggunakan hill cipher.

- Untuk matriks ukuran 2 x 2 maka matriksnya $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$
- Untuk matriks ukuran 3 x 3 maka matriksnya $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & 3 & 3 \end{pmatrix}$
- Untuk matriks ukuran 4 x 4 maka matriksnya $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \\ 1 & 4 & 6 & 3 \end{pmatrix}$

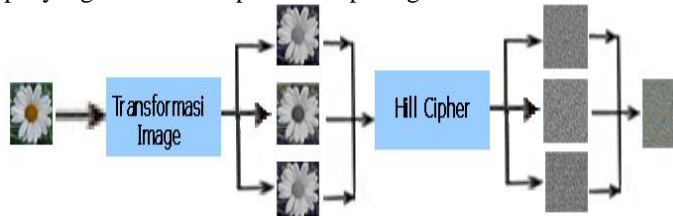
dan seterusnya.

dimana nilai determinan dari matriks-matriks di atas tidak sama dengan nol tetapi sama dengan satu.

2.4 Enkripsi Citra Menggunakan Teknik Hill

a. Proses Enkripsi Citra

Proses enkripsi yang diusulkan dapat dilihat pada gambar berikut.



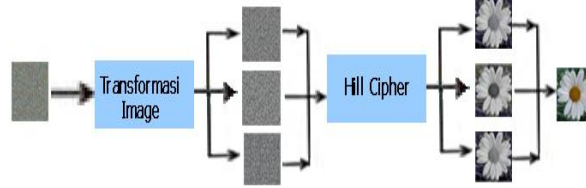
Gambar 1. Skema Proses Enkripsi

Algoritmanya diberikan di bawah ini

1. Tentukan matriks kunci yang berukuran $m \times m$ yang disepakati oleh Pengirim dan Penerima.
2. Ambil citra yang akan dienkripsi
3. Lakukan transformasi citra untuk citra berwarna sehingga menjadi citra grayscale.
4. Ambil nilai komponen warna (pixel) dari citra kemudian ubah ukurannya menjadi vektor baris dengan ukuran $[1 \dots m \times m]$
5. Bagi nilai pixel atau citra dalam block-block yang bila dinyatakan dalam bentuk matriks, ukuran barisnya sebanyak m .
6. Lakukan enkripsi menggunakan kunci hill cipher untuk masing-masing matriks dari setiap komponen warna menggunakan Pers (2)
7. Ubah kembali ukuran matriks hasil enkripsi ke ukuran citra semula.
8. Matriks hasil enkripsi dikembalikan sebagai nilai intensitas menggunakan transformasi warna sehingga menghasilkan citra baru yang sudah tersandikan seperti terlihat pada Gambar 1.

b. Proses Dekripsi Citra

Proses dekripsi yang dilakukan pada penelitian ini dapat dilihat pada gambar berikut :



Gambar 2. Skema Proses Dekripsi

Algoritmanya diberikan di bawah ini

1. Ambil citra yang akan didekripsi
2. Gunakan matriks kunci yang disepakati sebelumnya untuk menentukan matriks invers yang akan digunakan untuk mendekripsi citra menggunakan metode hill cipher.
3. Transformasi warna sehingga komponen warna RGB dari citra yang telah tersandikan terpisahkan seperti pada proses enkripsi
4. Proses dekripsi menggunakan metode hill cipher prosesnya sama dengan langkah pada proses enkripsi untuk tiap matrik warna. Proses decipher dilakukan dengan menggunakan Pers (4).
5. Vektor hasil dekripsi dikembalikan sebagai sebagai nilai intensitas warna menggunakan transformasi warna balik sehingga menghasilkan citra yang sama dengan citra aslinya.


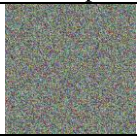

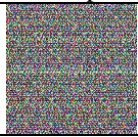

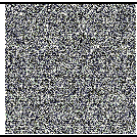
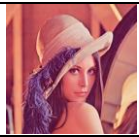
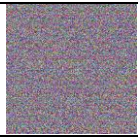
3. HASIL DAN PEMBAHASAN

Untuk menguji Hill Cipher menggunakan koefisien binomial sebagai matriks kunci-nya merupakan sebuah teknik kriptografi, proses enkripsi-dekripsi berikut ini akan dilakukan pengujian dari algoritma Hill Cipher di atas.

Pengujian keamanan kunci enkripsi dilakukan pada beberapa citra berwarna dengan ukuran 256 x 256 piksel dengan tipe JPG dan 128 x 128 piksel dengan tipe BMP. Analisis histogram warna dilakukan untuk mengetahui adanya perbedaan antara *plain image* dengan *cipher image*. Untuk mengakomodir konsep yang diusulkan, maka pada saat membangkitkan kunci Hill Cipher digunakan matriks dengan ordo 4 x 4 dan 6 x 6.

3.1. Hasil Enkripsi dan Analisis Histogram

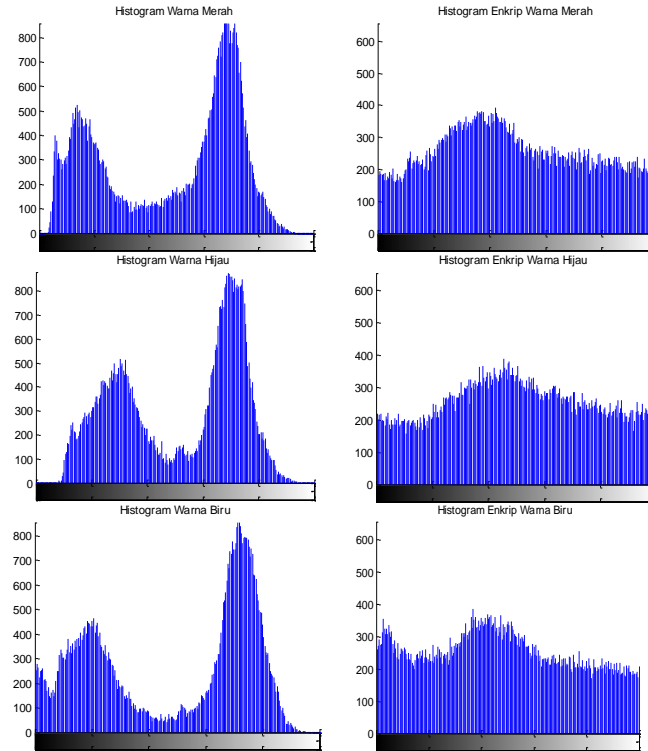
Pengujian dilakukan kepada 4 jenis citra yang berbeda, format dan ukurannya dengan menggunakan kunci yang sama, maka berdasarkan uji secara visual dapat dilihat hasilnya pada gambar 3 berikut.

Citra			
Asli	Enkripsi	Asli	Enkripsi
			
a		b	
			
c		d	

Gambar 3. Hasil proses enkripsi dari 3 citra warna dan sebuah citra gray scale

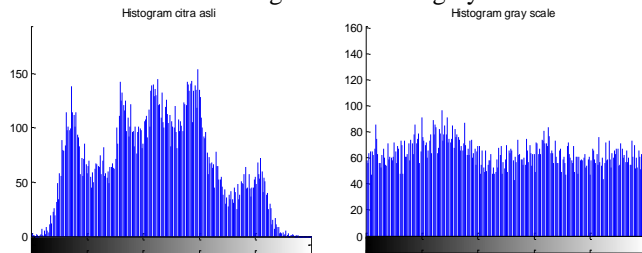
Gambar 3. menunjukkan bahwa citra asli tidak dapat terlihat setelah dilakukan proses enkripsi. Hasil penyandian citra menunjukkan keteracakan warna dan perubahan intensitas warna yang cukup signifikan, hal ini menunjukkan bahwa proses enkripsi berhasil dengan baik.

Berikut ini adalah salah satu contoh histogram dari citra warna.



Gambar 4. Histogram citra asli dan citra hasil enkripsi dari citra (a)

Sedangkan berikut adalah contoh histogram dari citra gray scale.



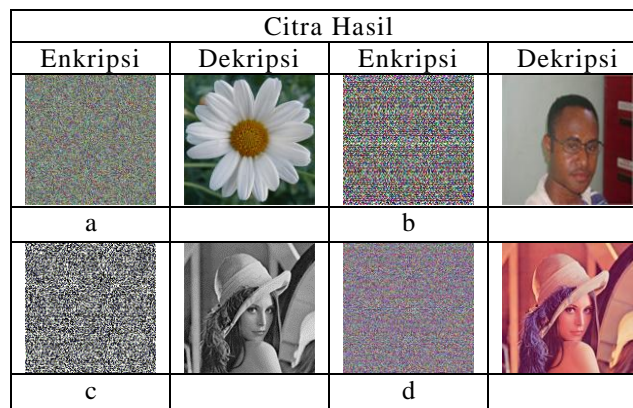
Gambar 5. Histogram citra asli dan citra hasil enkripsi dari citra (c)

Hasil analisis histogram warna diperlihatkan pada Gambar 4 dan Gambar 5. Apabila dilihat secara visual dari histogram plain image dengan histogram dari *cipher image*-nya, maka terlihat perbedaan yang signifikan antara keduanya. Pada histogram hasil enkripsi terlihat rata untuk setiap intensitas warna, hal ini menunjukkan bahwa algoritma enkripsi yang digunakan tidak dapat memberikan petunjuk apa-apa untuk dilakukan *statistical attack* oleh *kriptanalis* karena tidak ada intensitas yang menonjol seperti yang terlihat pada histogram citra asli.

3.2. Hasil Dekripsi

Untuk mengetahui algoritma dekripsi yang digunakan pada penelitian ini berjalan dengan baik maka citra yang telah ter-enkripsi akan di dekripsi kembali sehingga menghasilkan citra semula.

Karena menurut jenis kuncinya, Hill Cipher termasuk didalam kriptografi yang simetris maka dalam proses dekripsi citra yang telah di-enkripsi sebagaimana pada gambar 3. maka kunci yang digunakan pada proses dekripsi adalah kunci yang sama pada proses enkripsi.



Gambar 6. Hasil proses dekripsi

Gambar 6 menunjukkan bahwa citra yang telah enkripsi dapat dikembalikan seperti citra semula atau citra asli, hal ini menunjukkan bahwa proses dekripsi berhasil dengan baik.

4. KESIMPULAN

Berdasarkan pembahasan di atas maka kesimpulan yang dapat diambil adalah :

1. Koefisien-koefisien binomial dapat dijadikan sebagai entri-entri dari matrik kunci
2. Matriks kunci hill cipher yang entri-entri dibentuk dari koefisien-koefisien binomial selalu mempunyai matriks invers karena determinan dari matriks kuncinya selalu sama dengan satu.
3. Proses penyandian citra dengan Hill Cipher menunjukkan keteracakan warna yang cukup signifikan, hal ini menunjukkan bahwa proses enkripsi berhasil dengan baik.
4. Proses Dekripsi dengan teknik Hill Cipher dari citra yang telah ter-enkripsi dapat dikembalikan seperti citra semula atau citra asli. Hal ini menunjukkan bahwa proses dekripsi berhasil dengan baik.

5. DAFTAR PUSTAKA

- Acharya, B. dkk, 2009. *Image Encryption Using Advanced Hill Cipher Algorithm*, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009
- Anton, H. & Rorres, C., 2005, *Elementary Linear Algebra, Applications Version*, 9th Edition, New York: John Wiley & Sons.
- Acharya B., dkk, 2007. *Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm*, International Journal of Security, Vol 1, Issue 1, 2007, pp. 14-21.
- Biggs, L. N, 2008. *Codes: An Introduction to Information Communication and Cryptography*, Springer Undergraduate Mathematics Series ISSN 1615-2085.
- Imai H., dkk, 2002. *Cyptography with Information Theoretic Security*. Information Theory Workshop, 2002, Proceedings of the IEEE, 20-25 Oct 2002.
- Ragab, A. H. M, dkk, 2014. *Encryption Quality Evaluation of Robust Chaotic Block Cipher for Digital Imaging*, International Journal of Recent Technology and Engineering (IJRTE) 6 January 2014.
- Rojali , 2011. *Studi dan Implementasi Hill Cipher menggunakan binomial newton berbasis komputer*. Prosiding pada Seminar Nasional Matematika dan Pendidikan Matematika, Yogyakarta, 3 Desember 2011.

Setyaningsih, E. dkk, 2011. *Konsep Super Enkripsi Untuk Meningkatkan Keamanan Data Citra*, SNASTI 2011, ISLP-7.

Stinson, D.R., 1995, *Cryptography Theory and Practice*, Florida: CRC Press, Inc.

University of Florida, "How to Encipher and Decipher Codes using the Hill 2-Cipher," Web. 8 Apr. 2013.