# IMPLEMENTASI SANDI HILL UNTUK PENYANDIAN CITRA

**J. J. Siang**
Program Studi Ilmu Komputer, Fakultas MIPA, Universitas Kristen Immanuel Yogyakarta
email : j_j_siang@mail.com

**Ronald S. Lesar**
Staf PDE RS Bethesda Yogyakarta

**ABSTRAK:** Sandi Hill merupakan salah satu teknik penyandian teks. Dalam penelitian ini, pemakaian sandi Hill diperluas dari teks ke citra bertipe BMP 24 bit. Matriks yang dipakai berordo 2x2 dan 3x3. Hasil percobaan menunjukkan bahwa sandi Hill cocok untuk enkripsi citra dengan variasi nilai RGB antar piksel berdekatan yang tinggi (seperti foto), tapi tidak cocok untuk citra dengan variasi nilai RGB yang rendah (seperti gambar kartun) karena pola citra asli masih tampak dalam citra sandi.

Sandi Hill juga memiliki kelemahan dalam hal tidak tunggalnya matriks kunci yang dapat dipakai. Akan tetapi untuk pemakaian biasa, dengan pemilihan matriks kunci yang baik, sandi Hill dapat dipakai untuk penyandian karena hanya melibatkan operasi matriks biasa sehingga prosesnya relatif cepat.

**Kata kunci:** Sandi Hill, Citra, Relatif Prima.

***ABSTRACT:*** *Hill's code is one of text encoding technique. In this research, Hill's code is extended to image encoding. The image used is BMP 24 bit format. 2x2 and 3x3 matrices is used as a key. The results show that Hill's code is suitable for image whose RGB values vary highly. On the contrary, it is not suitable for less varied RGB images since its original pattern is still persisted in encrypted image.*

*Hill's code for image encoding has also disadvantage in the case that the key matrix is not unique. However, for daily application, with good key matrix, Hill's code can be applied to encode image since it's process only deals with simple matrix operation so it become fast.*

***Keywords:*** *Hill's Code, Image, Relatively Prime.*

## 1. PENDAHULUAN

Dewasa ini, kriptografi dirasakan semakin penting. Keamanan pengiriman informasi melalui komputer menjadi bagian yang tak terpisahkan dalam kehidupan sehari-hari. Seiring dengan peningkatan kepentingannya, banyak metode-metode yang ditemukan maupun diperluas penggunaannya. Diantara metode-metode tersebut terdapat metode yang hanya membutuhkan operasi matematika sederhana, tetapi juga terdapat metode yang melibatkan teori yang rumit dan sulit implementasinya.

Salah satu metode yang sangat sederhana dalam kriptografi adalah dengan melakukan penggeseran karakter dalam abjad. Jika enkripsi dilakukan dengan menggeser 3 huruf ke kanan, maka huruf A disandikan dengan D, huruf B dengan E dan seterusnya.

| | |
|---|---|
| Huruf Asli | A B C D E F G H I J K L M N O P Q R S T U V W X Y Z |
| Huruf Sandi | D E F G H I J K L M N O P Q R S T U V W X Y Z A B C |

Dekripsi dilakukan dengan membalik aturan enkripsi, yaitu dengan menggeser 3 karakter sandi ke kiri.

Meskipun metode ini sangat sederhana, tapi mudah sekali tertebak karena terdapat korespondensi satu-satu antara huruf asli dan huruf sandi. Jika sebuah huruf sandi tertebak, maka semua huruf sandi yang sama akan tertebak juga. Untuk menghindari hal ini, enkripsi teks tidak dilakukan per huruf, tapi per blok yang terdiri dari beberapa huruf sekaligus. Salah satu metode yang memungkinkan untuk hal ini adalah sandi Hill.

Penyandian dengan sandi Hill dilakukan dengan memanfaatkan operasi matriks biasa. Penyandian dilakukan pada tiap blok teks yang berukuran sama dengan ordo matriks

yang digunakan. Sebagai perluasannya, dalam penelitian ini sandi Hill diimplementasikan untuk menyandikan sebuah citra. Ini dimungkinkan mengingat sebuah citra merupakan deretan piksel-piksel yang komponen R (Red), G (Green) dan B (Blue) nya merupakan bilangan-bilangan bulat sehingga dapat dioperasikan dalam sebuah matriks. Citra yang digunakan dalam penelitian ini dibatasi dalam format BMP 24 bit. Matriks yang dipakai adalah matriks bujur sangkar berordo 2x2 dan 3x3 dengan elemen bilangan bulat.

## 2. DASAR TEORI

### 2.1 Dasar Matematika

Matriks bujur sangkar adalah matriks dengan jumlah baris = jumlah kolom. Matriks bujur sangkar disebut matriks Identitas (= I) jika semua elemen diagonal utamanya = 1 dan elemen lainnya = 0. 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 c|d.

Sebagai contoh, faktor persekutuan 12 dan 18 adalah $\{\pm 1, \pm 2, \pm 3, \pm 6\}$, dan FPB (12,18) = 6.

Dua buah bilangan bulat a dan b dikatakan relatif prima jika FPB (a,b) = 1. Syarat ini tidak mengharuskan a dan b merupakan bilangan prima. Sebagai contoh, FPB (9,26) = 1 sehingga 9 dan 26 merupakan bilangan-bilangan yang relatif prima, meskipun masing-masing bilangannya bukan bilangan prima.

Misalkan n adalah bilangan bulat positif, a dan b adalah bilangan-bilangan bulat, a dikatakan kongruen terhadap b modulo n (ditulis $a \equiv b \pmod n$) jika n|(a-b). Bilangan-bilangan bulat modulo n (simbol $Z_n$) adalah himpunan bilangan-bilangan bulat {0, 1, 2, … , n-1}. Operasi aritmmatika pada $Z_n$ dilakukan terhadap modulo n.

Sebagai contoh, dalam $Z_{26}$, maka 13+16= 3 karena $13+16 = 29 \equiv 3 \pmod{26}$.

Misalkan $a \in Z_n$. Invers a modulo n adalah suatu bilangan bulat $x \in Z_n$. sehingga $a.x \equiv 1 \pmod n$. Jika x ada, maka x tunggal, dan a dikatakan memiliki invers, yang ditulis sebagai $a^{-1}$. $a \in Z_n$ memiliki invers bila dan hanya bila FPB (a,n) = 1.

Dalam $Z_{26}$, semua elemen ganjil kecuali 13 memiliki invers. Dalam $Z_{256}$, semua elemen ganjilnya mempunyai invers karena semua faktor 256 merupakan bilangan genap.

### 2.2 Sandi Hill

Untuk menyandikan pesan teks dengan sandi Hill, langkah-langkah yang dilakukan adalah sebagai berikut :

1. Pilih matriks bujur sangkar A yang dipakai sebagai kunci.
2. Transformasikan tiap huruf dalam teks ke bilangan bulat yang sesuai (A=1, B=2, .., Z = 26)
3. Kelompokkan barisan angka yang didapat kedalam beberapa blok vektor p yang panjangnya sama dengan ukuran matriks A.
4. Hitung $c = A.p \pmod{26}$ untuk tiap vektor p
5. Kembalikan tiap angka dalam vektor sandi c ke huruf yang sesuai untuk mendapatkan teks sandi.

Untuk mendekripsikan kembali pesan sandi, langkah-langkah yang dilakukan adalah sebagai berikut :

1. Hitung matriks $A^{-1} \pmod{26}$ sebagai kunci pembuka. $A^{-1}$ ada jika FPB (det(A), 26) = 1.
2. Lakukan langkah-langkah 2-5 pada enkripsi dengan mengganti :
   (i) Matriks A dengan matriks $A^{-1}$.
   (ii) Blok vektor teks asli p dengan blok vektor sandi c dan sebaliknya.

   Misalkan matriks $A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ dipakai untuk menyandikan teks “KOMPUTER”. Mula-mula, teks “KOMPUTER” diubah ke bilangan bulat yang sesuai dengan urutan abjadnya. Didapat : 11 15 13 16 21 20 5 18. Barisan angka tersebut dikelompokkan dalam blok dengan panjang 2.

$p = \begin{pmatrix} 11 & 13 & 21 & 5 \\ 15 & 16 & 20 & 18 \end{pmatrix}$.

$c = A.p = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 11 & 13 & 21 & 5 \\ 15 & 16 & 20 & 18 \end{pmatrix} = \begin{pmatrix} 41 & 45 & 61 & 41 \\ 45 & 48 & 60 & 54 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 15 & 19 & 9 & 15 \\ 19 & 22 & 8 & 2 \end{pmatrix}$

Jika c dikembalikan ke huruf yang sesuai didapatkan teks sandi "OSSVIHOB".

Untuk mendekripsi teks sandi, mula-mula dihitung $A^{-1}$

det (A) = 3 sehingga $A^{-1}$ ada. $3^{-1}(\text{mod } 26) = 9$.

$A^{-1} = 3^{-1}\begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix} = 9\begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 27 & -18 \\ 0 & 9 \end{pmatrix}$

$p = A^{-1}.c = \begin{pmatrix} 27 & -18 \\ 0 & 9 \end{pmatrix}\begin{pmatrix} 15 & 19 & 9 & 15 \\ 19 & 22 & 8 & 2 \end{pmatrix} = \begin{pmatrix} 63 & 117 & 99 & 369 \\ 171 & 198 & 72 & 18 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 11 & 13 & 21 & 5 \\ 15 & 16 & 20 & 18 \end{pmatrix}$

Jika dikembalikan ke huruf akan didapatkan teks asli "KOMPUTER" seperti teks semula.

## 3. IMPLEMENTASI

Dalam penelitian ini penggunaan sandi Hill diperluas pemakaiannya pada citra bertipe BMP 24 bit. Karena tiap-tiap komponen RGB piksel memiliki panjang 8 bit, maka sistem modulo yang dipakai dalam penyandian adalah $Z_n = Z_{256}$. Program dibuat dengan bahasa Delphi.

Untuk mengenkripsi citra dengan sandi Hill, mula-mula nilai RGB tiap piksel diambil. Berikutnya, algoritma enkripsi sandi Hill pada teks diterapkan pada barisan nilai RGB piksel dengan mengambil n = 256. Dekripsi juga dilakukan dengan cara yang sama.

Misalkan matriks kunci A berordo 2x2 dipakai untuk mengenkripsi potongan citra yang komponennya adalah :

| | | |
|---|---|---|
| $R_{11} = 200$<br>$G_{11} = 150$<br>$B_{11} = 200$ | $R_{12} = 200$<br>$G_{12} = 150$<br>$B_{12} = 150$ | $R_{13} = 100$<br>$G_{13} = 120$<br>$B_{13} = 10$ |
| $R_{21} = 100$<br>$G_{21} = 10$<br>$B_{21} = 70$ | $R_{22} = 40$<br>$G_{22} = 20$<br>$B_{22} = 30$ | $R_{23} = 0$<br>$G_{23} = 100$<br>$B_{23} = 20$ |

Nilai-nilai RGB tersebut dibagi menjadi blok dengan panjang 2 sehingga didapatkan

$p = \begin{pmatrix} 200 & 200 & 150 & 100 & 10 & 10 & 40 & 30 & 100 \\ 150 & 200 & 150 & 120 & 100 & 70 & 20 & 0 & 20 \end{pmatrix}$

Berikutnya, proses enkripsi dilakukan dengan cara yang sama dengan enkripsi teks tapi pada $Z_{256}$. Vektor hasil enkripsi dikembalikan sebagai nilai RGB citra sandi.

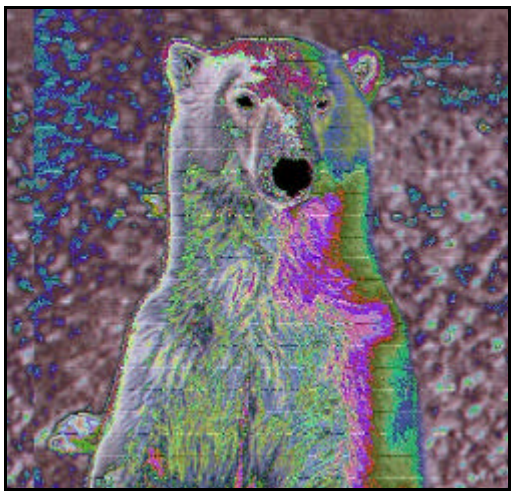
Sebenarnya enkripsi bisa dilakukan untuk sembarang matriks bujur sangkar A. Tapi citra sandi hanya bisa didekripsi kembali jika $A^{-1}$ ada. Untuk itu, jika $A^{-1}$ tidak ada, maka program akan memberikan peringatan pada pemakai karena jika enkripsi tetap dilanjutkan, citra sandi tidak bisa dikembalikan ke citra aslinya.

$A^{-1}$ ada jika det (A) mempunyai invers pada $Z_{256}$, atau FPB (det(A),256) = 1. Untuk lebih memudahkan, harga-harga $a^{-1}$ untuk $a \in Z_{256}$ diringkas dalam suatu tabel, dan tidak dihitung langsung dalam program.

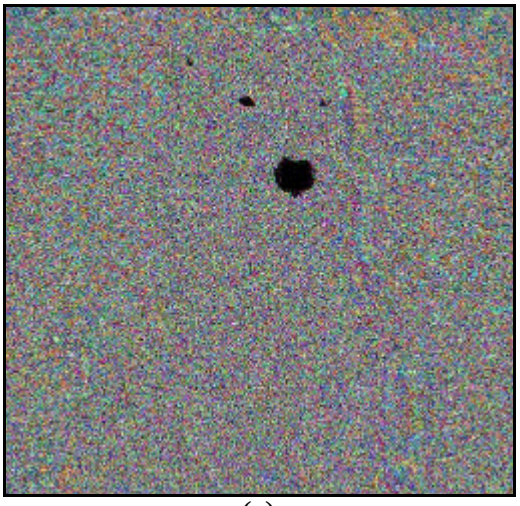
## 4. HASIL DAN PEMBAHASAN

Program yang dibuat diuji coba dengan mengenkripsi citra dengan variasi nilai RBG antar piksel berdekatan yang tinggi (foto), serta citra dengan variasi nilai RGB yang rendah (gambar kartun). Untuk melihat pengaruh pemakaian matriks kunci yang berbeda-beda, maka pada tiap citra, digunakan beberapa matriks 2x2 ($\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}, \begin{pmatrix} 19 & 5 \\ 12 & 23 \end{pmatrix}$) dan matriks 3x3 ($\begin{pmatrix} 12 & 34 & 51 \\ 3 & 48 & 27 \\ 17 & 5 & 13 \end{pmatrix}$). Hasilnya tampak pada gambar 1 dan 2.

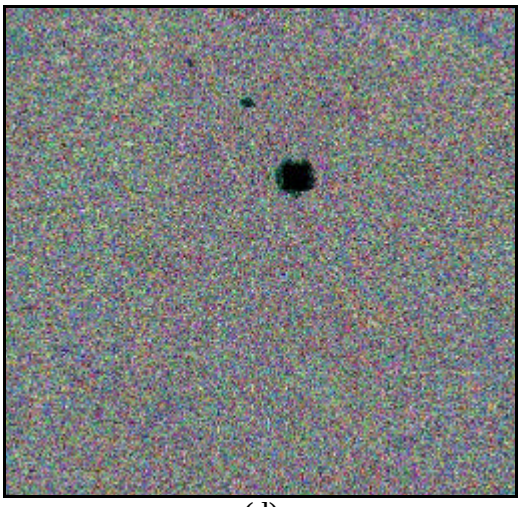
(a)



(b)



(c)

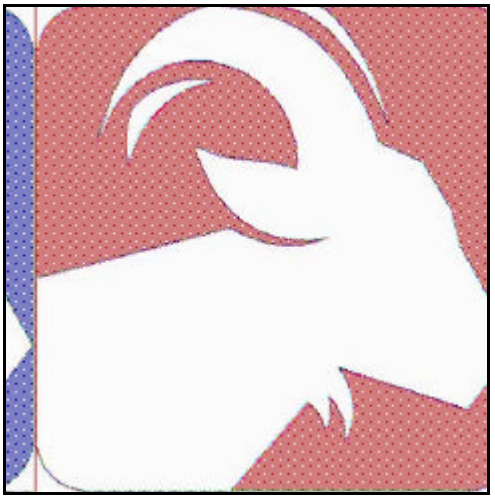


(d)

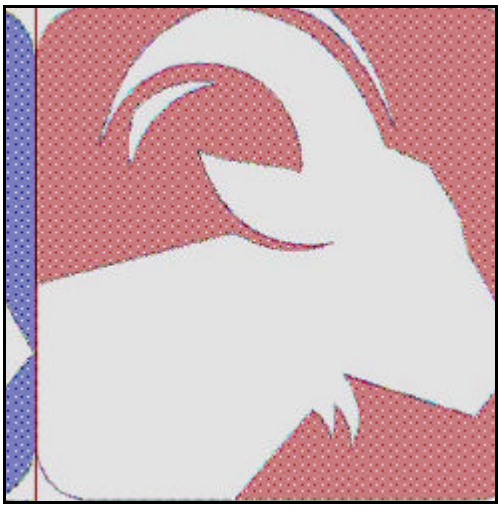
**Gambar 1. (a) Citra asli dengan variasi nilai RGB yang tinggi ; (b)-(d) citra hasil enkripsi dengan matriks** $\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}, \begin{pmatrix} 19 & 5 \\ 12 & 23 \end{pmatrix}$ **dan** $\begin{pmatrix} 12 & 34 & 51 \\ 3 & 48 & 27 \\ 17 & 5 & 13 \end{pmatrix}$

Tiap-tiap citra hasil enkripsi juga telah dicoba didekripsi dan didapatkan citra aslinya. Ini berarti proses enkripsi dan dekripsi sudah berjalan dengan benar.

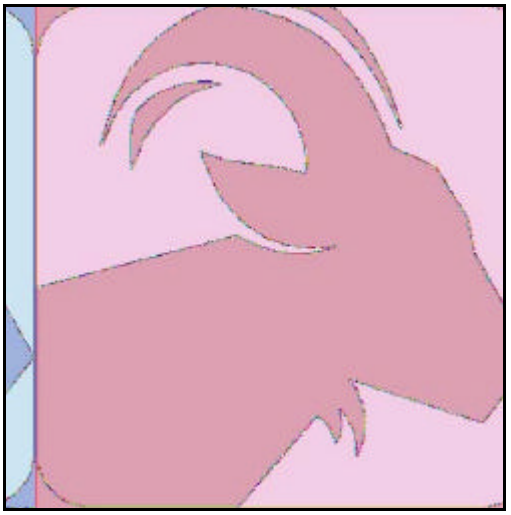
(a)



(b)



(c)



(d)

**Gambar 2. (a) Citra asli dengan variasi nilai RGB rendah; (b)-(d) citra hasil enkripsi dengan matriks** $\begin{pmatrix}2 & 1\\ 5 & 3\end{pmatrix}, \begin{pmatrix}19 & 5\\ 12 & 23\end{pmatrix}$ **dan** $\begin{pmatrix}12 & 34 & 51\\ 3 & 48 & 27\\ 17 & 5 & 13\end{pmatrix}$

Tampak pada gambar (1) dan (2) bahwa dengan pemakaian matriks yang sama, hasil enkripsi jauh berbeda. Pada citra gambar (1), hasil enkripsi sulit dikenali. Sebaliknya pada gambar (2), pola citra hasil enkripsi masih menyerupai citra aslinya, hanya warnanya saja yang berubah. Bahkan pemakaian beberapa matriks berbeda tidak menghasilkan perubahan yang berarti. Pola yang masih kelihatan tersebut disebabkan karena nilai-nilai RGB piksel yang berdekatan sama sehingga ketika dikalikan dengan matriks kuncinya, nilai RGB piksel citra sandi juga sama. Disimpulkan bahwa pemakaian sandi Hill untuk enkripsi gambar yang variasi warnanya tidak banyak (seperti gambar kartun) tidaklah tepat.

Terlihat juga pada gambar 1 bahwa untuk memperoleh hasil enkripsi yang baik, elemen-elemen matriks enkripsi haruslah cukup besar sehingga jika dikalikan dengan nilai RGB citra akan menghasilkan perubahan nilai RGB yang cukup signifikan. Ini juga berlaku pada ordo matriks yang digunakan. Semakin besar ordo matriksnya, semakin besar pula pengaruh perubahan nilai RGB citra sandi sehingga hasil enkripsi menjadi lebih baik. Pemakaian matriks dengan elemen kecil seperti gambar 1(b) masih menampakkan pola citra asli. Sebaliknya dengan elemen yang cukup besar (gambar 1c) atau ordo matriks yang lebih tinggi (gambar 1d) akan menghilangkan pola citra asli.

Dengan melihat proses enkripsi, ada kelemahan lain yang tampak yaitu tidak tunggalnya matriks kunci A. Hasil enkripsi yang dilakukan dengan matriks $A = (a_{ij})$ akan sama dengan matriks $A' = (a_{ij} \pm 256\, k_{ij})$ dengan $k_{ij}$ bulat. Hal yang sama berlaku juga pada dekripsi. Jika A adalah matriks yang dipakai untuk enkripsi, maka $A^{-1}$ tidaklah tunggal.

Terlepas dari beberapa kelemahan yang timbul, sandi Hill masih dapat diterapkan pada citra yang warnanya bervariatif. Keuntungan utama pemakaian sandi Hill adalah dalam hal kecepatan yang tinggi karena perhitungan yang dilakukan sederhana.

## 5. KESIMPULAN

Beberapa kesimpulan yang dapat diambil dari penelitian ini adalah sebagai berikut :

1 Sandi Hill merupakan metode penyandian sederhana yang cocok diterapkan pada citra dengan variasi warna tinggi (seperti foto), dan tidak cocok diterapkan pada citra yang warnanya tidak terlalu bervariatif.
2. Keuntungan utama pemakaian sandi Hill untuk penyandian citra adalah metodenya yang sederhana sehingga prosesnya cepat. Kerugian yang terjadi adalah tidak tunggalnya matriks kunci A (dan $A^{-1}$) yang menyebabkan tingkat keamanannya berkurang.
3. Hanya matriks bujur sangkar yang nilai determinannya relatif prima dengan 256 saja yang dapat dipakai untuk proses penyandian. Dekripsi tidak bisa dilakukan jika nilai determinanya tidak relatif prima dengan 256.

## DAFTAR PUSTAKA

1. Anton, H, Rorres, C., P. Silaban (terj), *Penerapan Aljabar Linear*, Erlangga, Jakarta, 1988.
2. Cullen, C.G., Bambang Sumantri (terj), *Aljabar Linear Dengan Penerapannya*, PT Gramedia Pustaka Utama, Jakarta, 1993.
3. Djoko Pramono, *Mudah Menguasai Delphi 4.0*, PT Elex Media Komputindo, Jakarta, 2000.
4. Menezes, A., P.van Oorschot, Vanstone, S., *A Handbook of Applied Cryptography*, CRC Press, 1997.