

Jurnal ILMU DASAR



1. Purwatiningsih, University of Jember - **Chief Editor**
SCOPUS ID. [55341566700](#) - [Google Scholar Profile](#) - SINTA ID. [5982555](#)
2. Dwi Indarti, University of Jember
[Google Scholar Profile](#) - SINTA ID. [6648735](#)
3. Arie Srihardyastutie, University of Brawijaya, Malang
SCOPUS ID. [56549015100](#) - [Google Scholar Profile](#) - SINTA ID. [6003114](#)
4. Eva Tyas Utami, University of Jember
[Google Scholar Profile](#) - SINTA ID. [6109055](#)
5. Miftahul Ilmi, Gadjah Mada University, Yogyakarta
SCOPUS ID. [57190191276](#) - [Google Scholar Profile](#) - SINTA ID. [258133](#)
6. Hasih Pratiwi, Universitas Sebelas Maret (UNS), Surakarta
SCOPUS ID. [56233603300](#) - [Google Scholar Profile](#) - SINTA ID. [6028915](#)
7. Fiber Monado, Sriwijaya University, Palembang
SCOPUS ID. [55330195600](#) - [Google Scholar Profile](#) - SINTA ID. [53558](#)
8. Kahar Muzakhar, University of Jember
SCOPUS ID. [56737119300](#) - [Google Scholar Profile](#) - SINTA ID. [5989819](#)
9. Bambang Piluharto, University of Jember
SCOPUS ID. [37056268800](#) - [Google Scholar Profile](#) - SINTA ID. [5993961](#)
10. Siswoyo - University of Jember
SCOPUS ID. [57193830395](#) - [Google Scholar Profile](#) - SINTA ID. [257755](#)
11. Bowo Eko Cahyono, The University of Jember, Indonesia
SCOPUS ID. [57163498200](#) - [Google Scholar Profile](#) - SINTA ID. [6007108](#)
12. Abduh Riski, University of Jember
SCOPUS ID. [57213518392](#) - [Google Scholar Profile](#) - SINTA ID. [257613](#)
13. Yoyok Yulianto - University of Jember

Supriyadi Supriyadi, Misto Misto, Yulia Hartanti

97-101



PDF

Influence of the Gamma Ray towards Porosity Evaluation of the Rocks Using Well Log Measurement

Puguh Hiskiawan

103-108



PDF

Digital Image Encryption by Using a Modified Hill Code

Sochif Prasetya, Mohammad Hasan, Kiswara Agung Santoso

109-113



PDF

The Inventory of Bamboo in Antirogo Sub-district Sumbersari District Jember Regency

Ali Murtodo, Dwi Setyati

115-121



PDF

Super (a, d)-Edge Antimagic Total Labeling of Connected Ferris Wheel Graph

Djoni Budi Sumarno, D Dafik, Kiswara Agung Santoso

123-130



PDF

Penyandian Citra Digital Menggunakan Modifikasi Sandi *Hill*

Digital Image Encryption by Using a Modified Hill Code

S. Prasetya¹, M. Hasan², dan K.A. Santoso³

^{1,2,3}Jurusan Matematika Universitas Jember,
Email: hasan.fmipa@unej.ac.id

Abstract

Data security is very important data needed to stay awake in strict confidence from hacker intrusion or criminals who want to steal the data. Data security methods that are used in this paper is a digital image encryption by using a modified Hill's code which is done by changing the way of encryption. If we are using Hill's code then matrix pixel multiplied is the key matrix while on the modification Hill's code before the key matrix then the matrix is multiplied pixels must be added to the results of the main diagonal elements of the matrix times key. The results obtained in the process of digital image encoding indicating that the image is encoded with password modification results of modified Hill's code more mixed reviews when compared to the image that was encoded with password Hill so that more effective in securing data in the form of a digital image. The size of the image file using the encoding results in a modification password Hill is smaller than ordinary password Hill with a percentage decrease of 4.6 % so more ease in delivery through electronic media

Keyword: Digital image, modified Hill code, encryption, description

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. Menurut (Kromodimoeljo,2010), syarat sebuah matriks kunci agar dapat digunakan dalam proses penyandian citra digital dengan sandi *Hill* adalah matriks tersebut harus mempunyai invers (Goldberg, 1991).

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 (Menezes, 1997). 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 2 x 2 dan 3 x 3 dengan elemen bilangan bulat.

Penyandian citra digital menggunakan sandi *Hill* memiliki kelemahan yaitu citra hasil penyandian tidak teracak dengan bagus jika menggunakan matriks kunci yang memiliki unsure matriks bernilai kecil (Forouzan, 2007) Oleh karena itu perlu dilakukan suatu terobosan dalam menggunakan sandi *Hill* agar hasil enkripsi sesuai dengan yang diharapkan.

Modifikasi sandi *Hill* diharapkan menjadi solusi dalam mengatasi permasalahan yang muncul jika

penyandian citra digital menggunakan sandi *Hill*. Modifikasi sandi *Hill* dilakukan pada cara pengkodeannya. Dalam paper ini peneliti akan memodifikasi sandi *Hill* dan mengaplikasikan hasil modifikasi tersebut kedalam citra digital. Setelah itu hasil modifikasi dibandingkan dengan sandi *Hill* biasa ditinjau dari segi hasil pengkodean dan ukuran file citra digital.

METODE

Metode penelitian yang digunakan yaitu 1) melakukankuantisasi citra digital yang akan disandikan. 2) membuat algoritma penyandian citra digital menggunakan modifikasi sandi *Hill*. 3) menentukanmatriks kunci yang berupa matriks persegi berordo 2 x 2 dan 3 x 3. 4) melakukan perhitungan enkripsi dan deskripsi secara manual dengan menggunakan modifikasi sandi *Hill*. 5) membuat program modifikasi sandi *Hill* dengan menggunakan bahasa pemrograman *visual basic*. 6) melakukan analisa data hasil penelitian. Disini hasil modifikasi dikatakan lebih baik jika ukuran file citra digital hasil pengkodean lebih kecil daripada tanpa modifikasi. 7) apabila ternyata hasil modifikasi tidak lebih baik, maka point 2 akan diulang dan elemen matriks kunci pada point ke 3, diubah sehingga menghasilkan pengkodean citra yang mempunyai ukuran file lebih kecil.

HASIL DAN PEMBAHASAN

Modifikasi sandi *Hill* dilakukan dengan cara merubah cara pengkodeannya. Jika pada sandi *Hill* dalam pengkodeannya matriks piksel dikalikan dengan matriks kunci sedangkan pada modifikasi sandi *Hill*

matriks piksel ditambah dengan hasil perkalian unsur-unsur matriks ke arah diagonal utama.

Besarnya nilai penjumlahan ditentukan oleh matriks itu sendiri. Jika matriks berordo 2 dengan matriks kunci $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ maka nilai penjumlahannya adalah $ad + bc$. Sedangkan jika matriks kunci yang digunakan berordo 3 dengan matriks kunci $\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ maka nilai penjumlahannya adalah $aei + bfg + cdh + gec + hfa + idb$.

Untuk mengenkripsi citra dengan sandi Hill dan modifikasi sandi Hill, mula-mula nilai RGB tiap piksel diambil. Misalkan potongan citra memiliki komponen sebagai berikut :

Tabell Komponen piksel mula-mula

Piksel ke	Red	Green	Blue
1	100	150	200
2	150	200	150
3	250	100	120
4	200	150	115
5	117	235	78
6	119	215	46

Perhitungan enkripsi citra dengan sandi Hill pada piksel 1 dan 2 dengan menggunakan matriks kunci $\begin{bmatrix} 8 & 11 \\ 5 & 7 \end{bmatrix}$ dapat dilakukan dengan menggunakan persamaan berikut:

$$C = (K.P) \text{ mod } 256 \quad (1)$$

Keterangan :

C = Piksel hasil enkripsi

K = Matriks kunci

P = Matriks piksel citra mula-mula

Sehingga proses enkripsi dengan sandi Hill adalah sebagai berikut :

$$C = (K.P) \text{ mod } 256$$

$$C = \left(\begin{bmatrix} 8 & 11 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 100 & 150 & 200 \\ 150 & 200 & 150 \end{bmatrix} \right) \text{ mod } 256$$

$$C = \begin{bmatrix} 2450 & 3400 & 3250 \\ 1550 & 2150 & 2050 \end{bmatrix} \text{ mod } 256$$

$$C = \begin{bmatrix} 146 & 72 & 178 \\ 14 & 102 & 2 \end{bmatrix}$$

Sedangkan jika citra dienkripsi dengan menggunakan modifikasi sandi Hill maka terlebih dahulu menentukan besar nilai penjumlahan yang akan digunakan untuk modifikasi. Jika matriks kunci yang digunakan adalah matriks $\begin{bmatrix} 8 & 11 \\ 5 & 7 \end{bmatrix}$ maka besar nilai penjumlahannya adalah $8 \times 7 + 5 \times 11 = 111$.

Sebelum melakukan perkalian dengan matriks kunci maka matriks piksel citra mula-mula terlebih dahulu dilakukan penjumlahan dengan nilai penjumlahan dari perkalian matriks piksel ke arah diagonal. Misalkan piksel yang digunakan adalah

piksel 1 dan piksel 2 pada tabel 1, maka besar nilai penjumlahannya adalah sebagai berikut :

$$P = \begin{bmatrix} 100 & 150 & 200 \\ 150 & 200 & 150 \end{bmatrix} + \begin{bmatrix} 111 & 111 & 111 \\ 111 & 111 & 111 \end{bmatrix}$$

$$P = \begin{bmatrix} 211 & 261 & 311 \\ 261 & 311 & 261 \end{bmatrix}$$

Hasil penjumlahan dengan matriks piksel mula-mula kemudian dilakukan perkalian dengan matriks kunci seperti pada proses enkripsi dengan menggunakan sandi Hill. Adapun proses enkripsi dengan modifikasi sandi Hill adalah sebagai berikut:

$$C = (K.P) \text{ mod } 256$$

$$C = \left(\begin{bmatrix} 8 & 11 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 211 & 261 & 311 \\ 261 & 311 & 261 \end{bmatrix} \right) \text{ mod } 256$$

$$C = \begin{bmatrix} 4559 & 5509 & 5359 \\ 2882 & 3482 & 3382 \end{bmatrix} \text{ mod } 256$$

$$C = \begin{bmatrix} 207 & 133 & 239 \\ 66 & 154 & 54 \end{bmatrix}$$

Jika penyandian citra digital menggunakan matriks kunci yang digunakan adalah $\begin{bmatrix} 8 & 11 \\ 5 & 7 \end{bmatrix}$ maka hasil perbandingan antara sandi Hill dan modifikasi sandi Hill adalah sebagai berikut:

Tabel 2 Perbandingan antara sandi Hill dan modifikasi sandi Hill

Piksel	Sandi Hill			Modifikasi Sandi Hill		
	R	G	B	R	G	B
1	146	72	178	207	133	239
2	14	102	2	66	154	54
3	104	146	117	165	207	238
4	90	14	125	142	66	177
5	197	149	106	2	210	167
6	138	120	200	190	172	252

Jika penyandian citra menggunakan matriks kunci $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ maka proses enkripsi piksel 1,2, dan 3 pada tabel 1 dengan menggunakan sandi Hill adalah sebagai berikut:

$$C = (K.P) \text{ mod } 256$$

$$C = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 100 & 150 \\ 150 & 200 \\ 250 & 100 \end{pmatrix} \text{ mod } 256$$

$$C = \begin{pmatrix} 500 \\ 400 \\ 350 \end{pmatrix} \text{ mod } 256$$

$$C = \begin{pmatrix} 244 \\ 144 \\ 94 \end{pmatrix}$$

Sedangkan jika citra enkripsi dengan menggunakan modifikasi sandi Hill maka terlebih dahulu menentukan besar nilai penjumlahan yang akan digunakan untuk modifikasi. Jika matriks kunci yang digunakan adalah matriks maka besar nilai penjumlahannya adalah sebagai berikut $1.1.1 + 1.1.1 + 1.0.0 + 1.1.1 + 0.1.1 + 1.0.1 = 3$.

Sebelum melakukan perkalian dengan matriks kunci maka matriks piksel citra mula – mula terlebih dahulu dilakukan penjumlahan dengan nilai penjumlahan dari perkalian matriks kunci ke arah diagonal utama. Misalkan piksel yang digunakan adalah piksel 1, 2, dan 3 pada tabel 1 maka besar nilai penjumlahannya adalah sebagai berikut :

$$P = \begin{pmatrix} 100 & 150 & 200 \\ 150 & 200 & 150 \\ 250 & 100 & 120 \end{pmatrix} + \begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix}$$

$$P = \begin{pmatrix} 103 \\ 153 \\ 253 \end{pmatrix}$$

Hasil penjumlahan dengan piksel mula-mula kemudian dilakukan perkalian dengan matriks kunci seperti pada proses enkripsi dengan menggunakan sandi Hill. Adapun proses enkripsi dengan modifikasi sandi Hill adalah sebagai berikut:

$$C = (K.P) \text{ mod } 256$$

$$C = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 103 & 153 \\ 153 & 203 \\ 253 & 103 \end{pmatrix} \text{ mod } 256$$

$$C = \begin{pmatrix} 509 \\ 406 \\ 356 \end{pmatrix} \text{ mod } 256$$

$$C = \begin{pmatrix} 244 \\ 144 \\ 94 \end{pmatrix}$$

Jika penyandian citra digital menggunakan matriks kunci maka hasil perbandingan antara

sandi Hill dan modifikasi sandi Hill adalah sebagai berikut :

Tabel 3 Perbandingan antara sandi Hill dan modifikasi sandi Hill

Piksel	Sandi Hill			Modifikasi Sandi Hill		
	R	G	B	R	G	B
1	244	194	214	253	203	223
2	144	44	14	150	50	20
3	94	250	64	100	0	70
4	180	88	239	189	97	248
5	236	194	124	242	200	130
6	63	109	161	69	115	167

Perhitungan secara manual menggunakan sandi Hill dan modifikasi sandi Hill menunjukkan perbedaan nilai RGB pada piksel hasil enkripsi. Perbedaan itu akan diuji coba dengan menggunakan program yang dibuat kemudian dibandingkan antara penyandian dengan menggunakan sandi Hill dan menggunakan modifikasi sandi Hill. Percobaan dilakukan dengan menggunakan matriks kunci yang berbeda. Jika matriks kunci yang digunakan adalah matriks $A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$, matriks $B = \begin{pmatrix} 19 & 20 \\ 18 & 19 \end{pmatrix}$, dan matriks $C = \begin{pmatrix} 1 & 1 & 1 \\ 5 & 1 & 4 \\ 4 & 5 & 4 \end{pmatrix}$. Citra yang akan dienkripsi adalah citra pada Gambar 1.

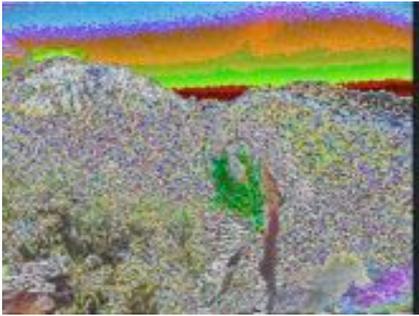


Gambar 1. Citra yang akan dienkripsi

Hasil enkripsi citra menggunakan sandi Hill (Gambar 2a) dan modifikasi sandi Hill (Gambar 2b) dengan menggunakan matriks A adalah sebagai berikut:

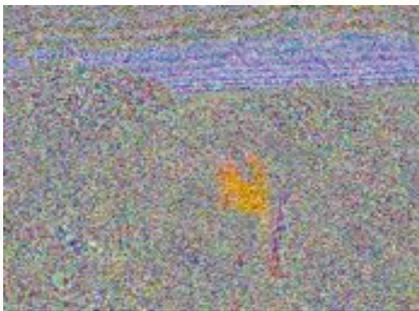


Gambar 2a. Citra enkripsi dengan sandi Hill.

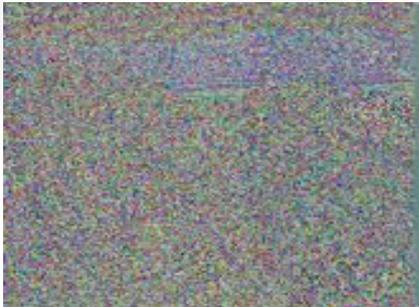


Gambar 2b. Citra enkripsi dengan modifikasi sandi Hill.

Hasil enkripsi citra menggunakan sandi Hill (Gambar 3a) dan modifikasi sandi Hill (Gambar 3b) dengan menggunakan matriks B adalah sebagai berikut:



Gambar 3a. Citra enkripsi dengan sandi Hill.

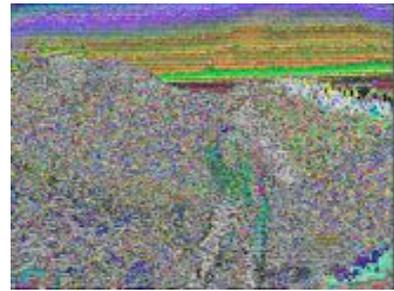


Gambar 3b. Citra enkripsi dengan modifikasi sandi Hill.

Hasil enkripsi citra menggunakan sandi Hill (Gambar 4a) dan modifikasi sandi Hill (Gambar 4b) dengan menggunakan matriks C adalah sebagai berikut:



Gambar 4a. Citra enkripsi dengan sandi Hill.



Gambar 4b. Citra enkripsi dengan modifikasi sandi Hill.

Hasil enkripsi citra menggunakan matriks A dengan menggunakan sandi Hill pada Gambar 2a dan modifikasi sandi Hill pada Gambar 2b ternyata menghasilkan suatu citra enkripsi yang kurang begitu bagus hasil penyandiannya atau citra masih belum teracak. Tetapi hasil penyandian citra menggunakan modifikasi sandi Hill lebih bagus hasil pengacakannya bila dibandingkan dengan yang disandikan dengan sandi Hill.

Hasil enkripsi citra menggunakan matriks B dengan menggunakan sandi Hill pada Gambar 3a dan modifikasi sandi Hill pada Gambar 3b ternyata menghasilkan enkripsi citra yang baik tetapi citra enkripsi dengan menggunakan modifikasi sandi Hill memiliki hasil yang lebih baik bila dibandingkan dengan sandi Hill. Perbedaan citra enkripsi dengan menggunakan sandi Hill dan modifikasi sandi Hill ditentukan oleh perbedaan nilai elemen matriks. Semakin besar nilai elemen matriks yang digunakan maka citra hasil enkripsi akan semakin teracak dengan bagus.

Penyandian citra digital menggunakan matriks C dengan menggunakan sandi Hill pada Gambar 4a dan modifikasi sandi Hill pada Gambar 4b ternyata menghasilkan citra enkripsi yang kurang begitu bagus karena citra asli masih dapat ditebak. Hasil enkripsi yang kurang begitu bagus karena nilai elemen matriks kunci bernilai kecil.

Citra enkripsi hasil modifikasi sandi Hill juga lebih baik bila dibandingkan dengan citra enkripsi dengan sandi Hill karena pada proses modifikasi sandi Hill terjadi proses penambahan nilai RGB pada piksel matriks mula – mula. Besar penambahan tergantung dari elemen matriks yang digunakan. Semakin besar elemen matriks yang digunakan maka semakin besar penambahan nilai RGB pada masing – masing piksel.

Besar ukuran file enkripsi juga lebih kecil bila dibandingkan dengan ukuran file citra mula – mula. Pada Gambar 1 citra yang akan dienkripsi memiliki ukuran 4.40 Mb, setelah dilakukan enkripsi dengan menggunakan sandi Hill maka file enkripsi menjadi 284 Kb. Jika enkripsi dilakukan dengan menggunakan modifikasi sandi Hill maka file enkripsi menjadi 271 kb sehingga terjadi penurunan ukuran file sebesar 4,6 % bila dibandingkan dengan ukuran file enkripsi dengan menggunakan sandi Hill. Kecilnya ukuran file hasil enkripsi dengan modifikasi

sandi *Hill* memudahkan dalam pengiriman lewat media elektronik seperti email.

KESIMPULAN

Perbedaan sandi *Hill* dengan modifikasi sandi *Hill* terletak pada cara pengkodeannya. Jika pada sandi *Hill* biasa dalam pengkodeannya matriks piksel dikalikan dengan matriks kunci, sedangkan dalam modifikasi sandi *Hill* sebelum dikalikan dengan matriks kunci, matriks piksel ditambah dengan hasil kali elemen diagonal utama matriks kunci. Hasil enkripsi sandi *Hill* yang dimodifikasi lebih sulit dikenali daripada sandi *Hill* biasa. Ukuran file hasil

enkripsi citra modifikasi sandi *Hill* lebih kecil bila dibandingkan dengan file hasil enkripsi dengan sandi *Hill* biasa dengan persentase sebesar 4,6 %.

DAFTAR PUSTAKA

- Forouzan, B. 2007. *Cryptography and Network Security*. Tata Mc Graw – Hill Inc, New Delhi.
- Goldberg, J. 1991. *Matrix Theory with Applications*. Mc Graw – Hill Inc, New York.
- Kromodimoeljo, S. 2010. Teori dan Aplikasi Kriptografi. Jakarta : SPK IT Consulting
- Menezes, A. 1997. *Handbook of Applied Cryptography*. CRC Press Inc, New York.