Jurnal Informasi dan Teknologi Ilmiah (INTI)
ISSN 2301-9425 (Media Cetak)
Volume 7, No 3, Juni 2020
Hal: 242-246

Implementasi Algoritma Mars Pada Penyandian Citra Satelit

Susi Ramadhan

Prodi Tezknik Informatika, Universitas Budi Darma, Medan, Indonesia
E-mail :suciramadhan@gmail.com

Abstrak

Citra Digital adalah salah satu bentuk data digital yang banyak dipakai untuk menyimpan photo, gambar ataupun hasil karya dalam format digital, salah satunya adalah citra satelit. Citra digital sangat rentan terhadap penyadapan maupun pencurian data oleh pihak yang tidak bertanggung jawab. Demi menjaga keamanan citra satelit dapat dilakukan dengan pemanfaatan teknik kriptografi. Teknik kriptografi dapat menyandikan citra satelit dengan mengenkripsikannya ke dalam bentuk sandi-sandi yang tidak dipahami dengan menggunakan algoritma mars. Algoritma simetri ini akan menghasilkan tingkat keamanan yang lebih tinggi terhadap citra satelit karena dapat menyandikannya ke bentuk sandi dengan proses yang cukup rumit sehingga akan mempersulit kriptanalis untuk mengakses citra tersebut. Untuk membangun aplikasi yang terkomputerisasi ini menggunakan *Visual Basic* 2008 sebagai aplikasi pendukungnya. Aplikasi ini dibuat sebagai upaya untuk meminimalisir tindakan-tindakan penyalahgunaan citra *satelit.*

Kata kunci : *Kriptografi, Citra Satelit, Mars*

1. PENDAHULUAN

Kriptografi berasal dari dua suku kata yaitu kripto dan grafi. Kripto artinya menyembunyikan, sedangkan grafi artinya ilmu seni. Kriptografi (Cryptography) adalah suatu ilmu yang mempelajari sistem sandi untuk menjamin kerahasiaan dan keamanan data, yang kegiatannya dilakukan oleh seorang kriptographer. Kriptografi secara umum merupakan ilmu dan seni untuk menjaga kerahasian berita. Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data[1].

Dengan bertambahnya penggunaan teknik digital maka diperlukan pengamanan untuk melindungi kerahasiaan dan keaslian citra satelit. Aplikasi pengolah data citra satelit yang semakin canggih seiring perkembangan jaman membutuhkan data yang memuat informasi spasial yang tinggi, hal ini sulit dilaksanakan karena keterbatasan peralatan yang ada untuk menyajikan data secara bersamaan. Penggunaan data citra satelit pada prinsipnya memerlukan pengenalan obyek permukaan bumi dengan baik dan mampu membedakan satu dengan yang lain. Bidang informatika sangat perlu untuk membedakan bentuk, tekstur, batasan area maupun warna terhadap suatu objek yang mempunyai resolusi minimun.

Hal ini disebabkan pentingnya menjaga informasi yang bersifat pribadi, karena pencurian data dan serangan data berupa citra satelit akan menimbulkan berbagai masalah yang mengakibatkan dampak yang serius terhadap permasalahan ilegal, sebab tidak semua informasi dibuat bersifat umum. Rekayasa foto dan penyebaran foto yang dilakukan oleh pihak yang tidak bertanggung jawab tentunya akan merugikan pemiliknya, sehingga diperlukan suatu pengamanan citra satelit. Penyandian citra satelit dapat dilakukan menggunakan teknik kriptografi.

Citra digital adalah sebuah disiplin ilmu yang mempelajari tentang teknik-teknik mengolah citra. Citra yang dimaksud disini adalah gambar diam (foto) maupun gambar bergerak . Sedangkan digital disini mempunyai maksud bahwa pengolahan citra/gambar dilakukan secara digital menggunakan komputer[2]. Citra satelit adalah penginderaan jauh, yaitu ilmu atau seni cara merekam suatu objek tanpa kontak fisik dengan menggunakan alat pada pesawat terbang, balon udara, satelit, dan lain-lain. Dalam hal ini yang direkam adalah permukaan bumi untuk berbagai kepentingan manusia. Khususnya di Indonesia, citra satelit yang umumnya digunakan adalah citra satelit berdimensi dua.

Salah satu metode kriptografi yang dapat digunakan untuk mengimplementasikan pengamanan citra satelit adalah dengan menggunakan algoritma mars, dimana algoritma ini dapat menyelesaikan proses enkripsi dan dekripsi dengan cepat. Operasi xor pada *mars* melibatkan penjumlahan, perkalian, dan pembagian untuk mengabungkan nilai data dan nilai kunci[3]. Penelitian ini menguraikan bagaimana menerapkan algoritma *mars* pada penyandian citra satelit agar data tetap aman dan sulit terpecahkan. Maka penulis mencoba menggunakan kriptografi modern berupa algoritma *mars.* Agar proses yang dilakukan lebih mudah, maka dirancang sebuah aplikasi pengamanan citra satelit menggunakan bahasa pemrograman *visual basic* 2008.

Penelitian ini menguraikan bagaimana menerapkan algoritma *mars* pada penyandian citra satelit agar data tetap aman dan sulit terpecahkan. Maka penulis mencoba menggunakan kriptografi modern berupa algoritma *mars.*

2. TEORITIS

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa yunani, yaitu dari kata *cypto* dan *graphia* yang berarti penulisan rahasia. Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi juga merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi seperti kerahasiaan, integritas data, autentikasi dan ketiadaan penyangkalan [3].

2.2 Citra Satelit

Citra satelit merupakan citra yang dihasilkan dari pemotretan menggunakan wahana satelit. Saat ini banyak satelit mengorbit di luar angkasa dengan fingsinya yang

beragam seperti satelit militer, satelit komunikasi, satelit pengindraan jauhantaplanet, dan satelit pengindraan jauh sumber daya bumi. Oleh karna itu, perkembangan teknik pengindraan jauh sistem satelit lebih maju dibandingkan dengan air-borne (foto udara)[8].

2.3 Algoritma Mars

Algoritma mars adalah salah satu algoritma kriptografi *chiper* blok, dengan ukuran blok 128 bit dan ukuran kunci yang bervariasi dari 128 bit sampai 400 bit (Burwick et al. 1998). *Multivariate Adaptive Regression Splines* (MARS) merupakan metode dengan pendekatan regresi nonparametrik yang pertama kali diperkenalkan oleh Friedman pada tahun 1991. Data berdimensi tinggi yang dimaksud adalah data dengan ukuran $3 \leq v \leq 20$, dimana v adalah banyak variabel prediktor dan sampel data yang berukuran $50 \leq N \leq 1000$, dimana N untuk ukuran sampel (Friedman, 1991). Notasi yang digunakan dalam *chiper* adalah [4]:

a. D[ ] adalah suatu array dari 4 32 bit data word. Array ini berisikan *plaintext* dan pada akhir proses enkripsi berisikan *chipertext*.
b. K[ ] adalah array untuk *expended key*, terdiri dari 40 32 bit.
c. S[ ] adalah array yang berisikan *S-box*, terdiri dari 512 bit word.

Perluasan kunci berfungsi untuk membangkitkan sub kunci dari kunci yang diberikan yakni K[ ] terdiri dari n 32 bit dan diperluas menjadi 40 32 bit sub kunci K[ ]. Tahapan yang dilakukan pada perluasan kunci adalah:

a. Kunci disimpan pada variabel sementara T[ ] yang diset menjadi :

   T[0 . . n-1] = K[0 .. . n-1], T[n] = n, T[n+1 ...14] = 0
b. Kemudian diikuti dengan proses sebagai berikut :
   1. Transformasikan T[ ] dengan persamaan linier sebagai berikut :
      Untuk i = 0 ...14, T[i] = T[i] ((T[i-7mod 15] T[i-2 mod 15]) <<< 3) (4i+j) Dimana : j merupakan jumlah iterasi
   2. Lakukan 4 iterasi tipe-1 *feistel network* sebagai berikut :
      Untuk i = 0 ... 14, T[i] = (T[i] + S[low 9 bits dari T[i-1 mod 15]]) <<<9
   3. Ambil 10 word data dari T[ ] ke K[ ] :
      K[10j + 1] = T[4i mod 15], i = 0 ...9
c. Terakhir, nilai K5, K7 ... K35 diubah dengan ketentuan j digunakan untuk menampung dua bit terendah dari K[i], w menampung K[i] yang dua bit terendahnya diubah menjadi 1. Bit mask ke l akan diset menjadi 1 jika ml terdapat 10 bit 1 atau bit 0 yang berurutan. r digunakan untuk menyimpan lima bit terendah dari K[i-1], lalu B[ ] (tabel B[ ] = {0xa4a8d57b, 0x5b5d193b, 0xc8a8309b, 0x73f9a978}) dirotasikan sebanyak r posisi ke kiri yang hasilnya ditampung dalam p. Terakhir p di-XOR-kan dengan w dibawah kontrol M dan disimpan di dalam K[i]

3. ANALISA

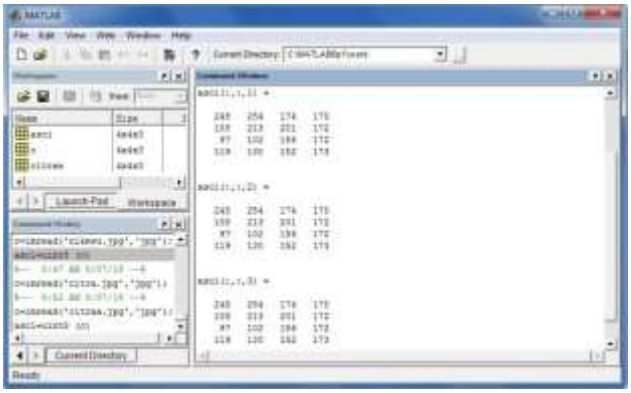
3.1 Analisa Masalah

Masalah keamanan data menjadi hal yang penting untuk dilihat, Salah satunya adalah citra satelit yang merupakan suatu informasi rahasia yang dapat digunakan dalam bentuk penyandian. Penyandian berdasarkan teknik kriptografi memberikan hasil yang signifikan untuk mengurangi penyalahgunaan dari data tersebut. Hal ini dapat dilakukan dengan menggunakan algoritma mars penyandian pada citra satelit.

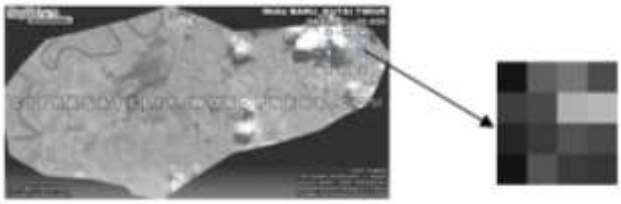
Agar algoritma dapat berjalan dengan baik terhadap enkripsi citra digital satelit, maka terlebih dahulu citra di konversi dalam bentuk biner pada setiap *pixel* citra. citra yang akan diamankan pada kasus ini adalah citra *grayscale*.

3.2 Analisa Algoritma Mars

Berikut ini adalah proses hasil nilai pixel dari matlab yang akan dipakai untuk proses enkripsi.



Gambar 1 Proses matlab



Gambar 2 *Plainimage* Sebanyak 16 piksel

Nilai elemen warna dari 16 piksel *plainimage* contoh diatas adalah = (248, 254, 174, 170, 108, 213, 201, 172, 97, 102, 156, 172, 119, 130, 152, 173).

Dari metode ini proses yang akan di jalankan terdiri dari ekspansi atau pembangkit kunci, proses enkripsi, dan proses.

***Plainimage* :** 248 254 174 170 108 213 201 172 97 102 156 172 119 130 152 173

***Key* : SUSIRAMA**

****Plainimage*:**

Char	**248**	**254**	**174**	**170**
Bin	**11111000**	**11111110**	**10101110**	**10101010**
Char	**108**	**213**	**201**	**172**
Bin	**01101100**	**11010101**	**11001001**	**10101111**
Char	**97**	**102**	**156**	**172**
Bin	**01100001**	**01100110**	**10011100**	**10101100**
Char	**119**	**130**	**152**	**173**
Bin	**01110111**	**10000010**	**10011000**	**10101100**

Proses pembangkitan kunci karena ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu K1, K2, …, K16. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter. Lakukan Permutation Commpression (PC-1) terhadap biner kunci seseai dengan tabel PC-1.

Tabel 1 Permutation Commpression (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	45	38	30	22
14	6	61	53	45	37	29
21	13	5	20	20	12	4

Cara melakukan nya cari bit pada posisi ke-57 dan pindahkan pada posisi ke-1, cari bit ke 49 dan pindah kan pada posisi ke-2 cari posisi ke 41 dean pindah kan pada posisi ke-3, dan seterusnya.

***Key* :**

Char	S	U	S	I	R
Des	83	85	83	73	82
Bin	01010011	01010101	01010011	01001001	01010010

Char	A	M	A
Des	65	77	65
Bin	01000001	01001101	01000001

Gabungkan semua biner kunci kemudian lakukan Permutasi Compresi-1 (PC-1) untuk mendapatkan 56 bit pra kunci.

*Biner Kunci:
0101001101010101010100110100100101010010010000
010100110101000001

*Hasil PC-1
0000000011111111100000000000100010101010000100
10010000111

Hasil PC-1 di bagi menjadi 2 kelompok yang terdiri dari C_0 dan D_0 yang masing-masing terdiri dari 28 bit:

C_0 : 0000000011111111100000000001

D_0 : 0001010101000010010010000111

Proses Generate key (Pembangkitan Kunci) left shift operation sebanyak 16 iterasi

Tabel 2 Generate key (Pembangkit Kunci)

Putaran	Jumlah Putaran	C_0	D_0
		00000000111111110000000001	00010101010000100100 10000111
1	1	00000001111111100000000010	00101010100001001001 00001110
2	1	00000011111111000000000100	01010101000010010010 00011100
3	2	00001111111100000000010000	01010100001001001000 01110001
4	2	00111111110000000000001000000	01010000100100100001 11000101
5	2	11111111000000000010000000	01000010010010000111 00010101
6	2	11111100000000000100 00000011	00001001001000011100 01010101
7	2	11110000000000010000 00001111	00100100100001110001 01010100
8	2	11000000000001000000 00111111	10010010000111000101 01010000
9	1	10000000000010000000 01111111	00100100001110001010 10100001
10	2	00000000001000000001 11111110	10010000111000101010 10000100
11	2	00000000100000000111 11111000	01000011100010101010 00010010
12	2	00000010000000011111 11100000	00001110001010101000 0100101
13	2	00001000000001111111 10000000	00111000101010100001 00100100
14	2	00100000000111111110 00000000	11100010101010000100 10010000
15	2	10000000011111111000 00000000	10001010101000010010 01000011
16	1	0000000011111111 000000000001	0001010101000010 010010000111

Proses generate key (pembangkit kunci) penggabungan kembali C_0 & D_0 hasil left shift operation dan lakukan PC-2. Cara melakukan nya cari bit pada posisi ke-57 dan pindahkan pada posisi ke-1, cari bit ke 49 dan pindah kan pada posisi ke-2 cari posisi ke 41 dean pindah kan pada posisi ke-3, dan seterusnya.

Tabel 3 Permutation Commpression (PC-2)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

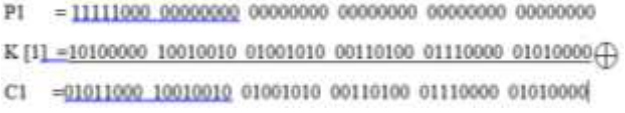
Setelah di lakukan Generate key maka di hasilkan kunci internal untuk proses Enkripsi:

Tabel 4 Kunci Internal

Round	Biner Kunci
K[1]	101000001001001001001010001101000111000001010000
K[2]	101000000011001011011011001010000010011000010
K[3]	001101000101001001010000010000101100001110011001
K[4]	000001100101000101010000000100110001010100001001
K[5]	000011100100000101010111001010000100010010000
K[6]	000011110100000100001101010000100110101100101100
K[7]	000010110000000110101001011100000001100010011000
K[8]	100110010000100010001001110000010001100000111011
K[9]	000110010000100010001010111010111100011110000000
K[10]	001100000010100010001100000110000100011000000011
K[11]	000100000010110000000100110111100100000000000100
K[12]	010000000010110000110100100000000110001111001000
K[13]	110001000101100001001001011000000110010000000001
K[14]	110000100000110001000101111001000100110001000010
K[15]	111010001001001000100010001111000010101100001010
K[16]	101000011001001000100010000001000000010110100101

Proses Enkripsi :

Langkah 1



Langkah 2

P2 =11111110 00000000 00000000 00000000 00000000 00000000

K[2] =10100000 00110010 11011010 11001010 00001000 11000101 ⊕

C2 =01011110 00110010 11011010 11001010 00001000 11000101

Lakukan dengan cara yang sama seoerti langkah 1 dan 2 sampai langkah 16.

Setelah proses enkripsi di lakukan maka mendapatkan hasil ciphertext dari algoritma, dan pembentukan ciphertext di ambil dari setiap hasil 8 bit pertama pada setiap putaran, maka cipertext yang di hasilkan adalah :

***Cipherimage* :**

Bin	01011000	01011110	10011010	10101100
Des	88	94	154	172
Char	X	ʌ	Š	¬
Bin	01100110	11011010	11000010	00110110
Des	102	218	194	54
Char	f	Ú	Â	6
Bin	01010110	01111000	10001100	11101100
Des	86	120	140	236
Char	V	x	Œ	Í
Bin	10110011	01000000	01110000	00001100
Des	179	64	112	12
Char	3	@	p	♀

***Cipherimage*:** X ʌ Š ¬ f Ú Â 6 V x Œ Í 3 @ p ♀

Proses Dekripsi:

Untuk mendapatkan hasil plaintext dari proses dekripsi ini maka di lakukan langkah seperti pada proses enkripsi :

Langkah 1

C1 = 01011000 00000000 00000000 00000000 00000000 00000000

K[1] = 10100000 10010010 01001010 00110100 01110000 01010000 ⊕

P1 = 11111000 10010010 01001010 00110100 01110000 01010000

Lakukan dengan cara yang sama seperti langkah 1 sampai langkah 16.

Setelah proses dekripsi di lakukan maka mendapatkan hasil plaintext dari algoritma kedua, dan pembentukan plaintext di ambil dari setiap hasil 8 bit pertama pada setiap putaran, maka plaintext nya adalah :

Bin	11111000	11111110	10101110	10101010
Char	248	254	174	170
Des	Ø	Þ	®	ã
Bin	01101100	11010101	11001001	10101111
Char	108	213	201	175
Des	l	Õ	Ě	-
Bin	01100001	01100110	10011100	10101100
Char	97	102	156	172
Des	a	f	œ	¬
Bin	01110111	10000010	10011000	10101101
Char	119	130	152	173
Des	w	,	˜	-

***Plainimage* :** Ø Þ ® ã l Õ Ě – a f œ ¬ w , ˜ -

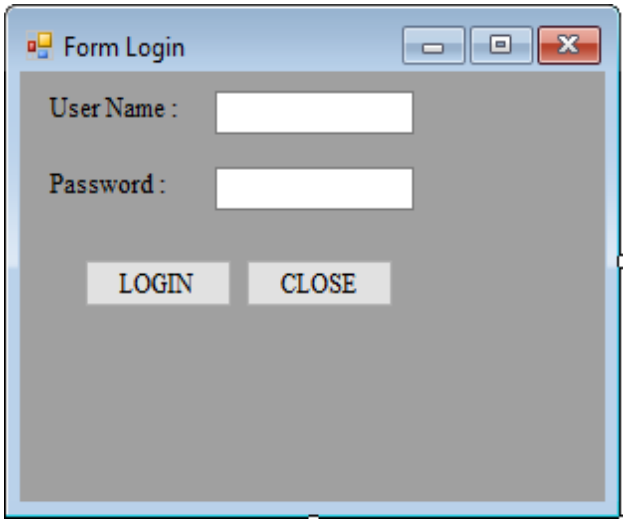
4. IMPLEMENTASI

Implementasi merupakan langkah yang digunakan untuk mengoperasikan rancangan yang dibangun. Dalam bab ini dijelaskan bagaimana menjalankan sistem tersebut. Sistem pengolahan program merupakan suatu kesatuan pengolahan yang terdiri prosedur dan pelaksanaan data. Komputer sebagai sarana pengolahan program haruslah menyediakan fasilitas-fasilitas pendukung dalam pengolahan nantinya. Secara proposional haruslah memenuhi akses yaitu Perangkat Keras (*Hardware*) dan Perangkat Lunak (*Software*)

4.1 Tampilan Program

Bentuk tampilan *form Login* yang di desain untuk masuk kedalam akses program dengan mengunakan *username* dan *password.* Dan bentuk tampilan *form* penyandian citra satelit saat di jalankan akan menampilkan menu utama yang terdiri dari menu untuk memilih *image*, *textbox* untuk pengimputan kunci, kotak *plainimage* untuk memasukan image yang akan di enkripsi dengan *button* enkripsi, kotak *cipherimage* untuk menampilkan hasil dekripsi dari proses enkripsi dengan *button* dekripsi.

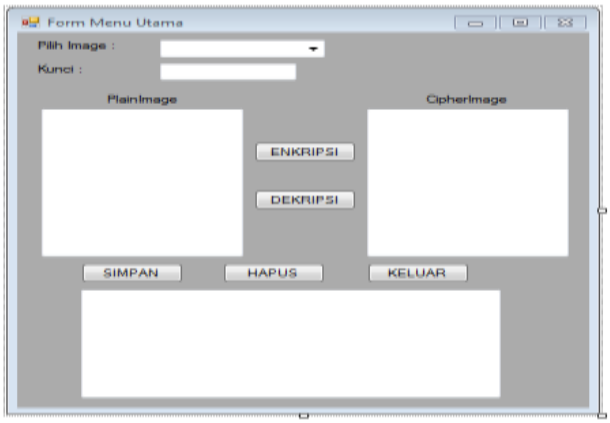
a. Tampilan *form login* dapat dilihat pada gambar 3.



Gambar 3 *Interface* Tampilan *Form Login*

Pada Gambar 3, tampilan *form login* ini didesain minimalis agar pengguna aplikasi tidak sulit untuk memahami cara masuk atau *login* ke dalam program tersebut.

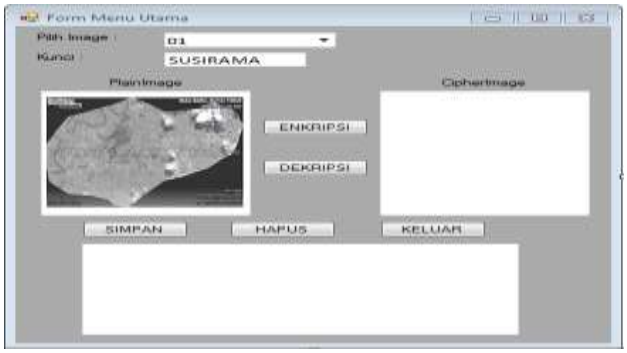
b. Tampilan *form* menu utama dapat dilihat pada gambar 4



Gambar 4 *Interface* Tampilan *Form* Menu Utama

Pada Gambar 4, tampilan *form* menu utama ini didesain minimalis agar pengguna aplikasi penyandian citra satelit tidak sulit memahami bagaimana cara menggunakan maupun mengoperasikan aplikasi ini.

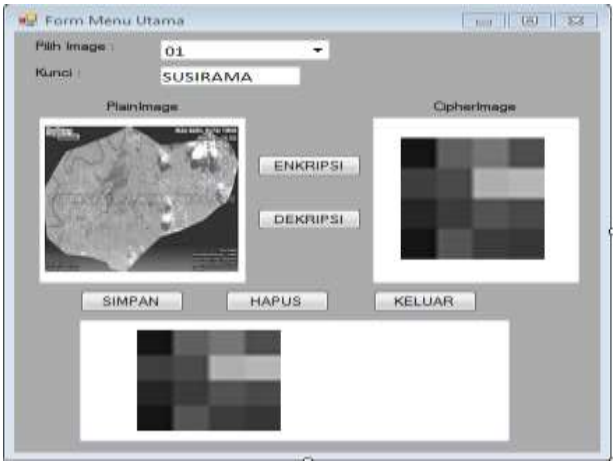
c. Tampilan Input Penyandian Citra Satelit
Bentuk tampilan *input* penyandian citra satelit yang akan tampil pada menu utama yang akan dijalankan proses enkripsi dan dekripsi setelah disandikan dapat dilihat pada gambar 5.



Gambar 5 Tampilan *Input Plainimage satelit*

Pada gambar 5, untuk pertama pengguna harus memilih file *image* mana yang akan di enkripsikan kemudian pengguna mengisi kotak kunci lalu menekan tombol enkripsi agar image dapat tersandikan.

d. Tampilan Output Penyandian Citra Satelit



Gambar 6 Tampilan *Output Cipherimage* satelit

Pada gambar 6 pada proses ini *image* yang sudah terenkripsi yang berbentuk kode-kode dapat di simpan ke dalam kotak *listview*, dan jika ingin mengembalikan *image* ke bentuk semula dapat mengunakan tombol dekripsi.

5. KESIMPULAN

Berdasarkan uraian dari bab-bab sebelumnya, maka penulis dapat memberikan kesimpulan sebagai berikut:

a. Proses penyandian citra satelit dapat dilakukan dengan algoritma Mars sehingga gambar asli atau informasi tidak dapat dibaca dan dimengerti oleh sembarang pihak.
b. Implementasi Algoritma *Mars* dalam proses penyandian citra satelit dapat disandian dan menggunakan penyisipan kunci yang ingin disisipkan agar tidak sesuai dengan gambar aslinya.
c. Menerapkan aplikasi dengan menggunakan *Visual Basic* 2008 yang telah selesai dirancang dengan desain minimalis diharapkan dapat berguna dalam penyandian c*itra satelit.*

Daftar Pustaka

[1] J. A. H. N. N. F-medan, "PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI SIMETRI IDEA Iskandar Zulkarnain , Ramenra Sinaga , Saniman Program Studi Sistem Komputer , STMIK Triguna Dharma PENDAHULUAN Sistem keamanan pengiriman data (komunikasi d," 1978.

[2] R. D. Kusumanto and A. N. Tompunu, "Pengolahan Citra Digital Untuk Mendeteksi Obyek Menggunakan Pengolahan Warna Model Normalisasi RGB," *Semin. Nas. Teknol. Inf. Komun. Terap. 2011*, vol. 2011, no. Semantik, pp. 1–7, 2011.

[3] E. Setyaningsih, S.Si., M.Kom, *Kriptografi & Inplementasinya menggunakan MATLAB*. Yogyakarta: Andi Publisher.com, 2015.

[4] C. Algoritma, "Ketepatan Klasifikasi Status Pemberian Air Susu Ibu (ASI) Menggunakan Multivariate Adaptive Regression Splines (MARS) dan," vol. 5, pp. 229–238, 2016.