

ENKRIPSI GAMBAR MENGGUNAKAN ALGORITMA SECURE IMAGE PROTECTION

Tri Hariyono Reiza Hafidz¹, Isbat Uzzin Nadhori², Nana Ramadijanti²

Mahasiswa¹, Dosen²

Politeknik Elektronika Negeri Surabaya

Institut Teknologi Sepuluh Nopember

Kampus PENS-ITS Keputih Sukolilo Surabaya 60111

Telp (+62)31-5947280, 5946114, Fax. (+62)31-5946114

Email : reiza.hafidz@gmail.com

Abstrak

Citra digunakan dalam berbagai bidang seperti medis, militer, ilmu pengetahuan, teknik, seni, hiburan, iklan, pendidikan, serta pelatihan. Dengan bertambahnya penggunaan teknik digital dalam transmisi dan penyimpanan citra, masalah mendasar untuk melindungi kerahasiaan, keutuhan, dan keaslian citra memang perlu diperhatikan. Dalam tugas akhir ini dibuat suatu aplikasi untuk menyembunyikan informasi citra dengan menggunakan metode *Secure Image Protection*. Metode ini awalnya menentukan citra dan kunci kemudian melakukan proses enkripsi, bagaimana cara memetakan tiap piksel dari gambar tersebut, lalu melakukan permutasi sederhana dari lokasi piksel serta transformasi dari nilai skala abu-abu melalui operasi Boolean XOR sehingga dapat menghasilkan citra yang nilai informasinya terlindungi dan aman.

Kata Kunci : Citra, kerahasiaan, enkripsi, piksel citra

1. Pendahuluan

1.1. Latar Belakang

Dunia kriptografi modern saat ini telah menerapkan berbagai metode untuk penyandian data berupa multimedia salah satunya adalah gambar. Semakin rumit metode yang digunakan, maka tingkat keamanan yang dihasilkan pun akan semakin baik pula. Algoritma kriptografi modern telah menerapkan metode penyandian data gambar dengan metode yang lebih baik dari sebelumnya. Hal ini membuat informasi yang dirahasiakan akan semakin sulit untuk dipecahkan oleh para kriptanalisis.

Gambar digunakan dalam berbagai bidang seperti keamanan, medis, ilmu, teknik, seni, hiburan, iklan, pendidikan serta pelatihan. Dengan bertambahnya penggunaan teknik digital bagi transmisi dan penyimpanan gambar, masalah mendasar untuk melindungi kerahasiaan, keutuhan dan keaslian gambar memang perlu diperhatikan. Hal ini dikarenakan kerahasiaan suatu informasi sangatlah penting dan bersifat pribadi.

Pengolahan citra merupakan salah satu disiplin ilmu yang banyak diterapkan untuk menyelesaikan masalah diatas. Sudah banyak peneliti yang menerapkan teori pengolahan citra di berbagai terapan, seperti bidang keamanan, medis, ilmu pengetahuan, teknik, seni, hiburan, iklan. Gambar dapat menjadi hal yang penting apabila gambar tersebut memiliki informasi yang berharga, dan dapat menjadi bersifat pribadi.

Enkripsi gambar menggunakan algoritma Secure Image Protection adalah cara untuk menyembunyikan informasi gambar asli dan dibuat gambar tersebut tidak tampak seperti gambar aslinya. Menentukan gambar apa yang akan disembunyikan informasinya beserta kunci. Kemudian langkah selanjutnya melakukan proses enkripsi, bagaimana cara memetakan tiap piksel dari gambar tersebut, lalu melakukan permutasi sederhana dari lokasi piksel serta transformasi dari nilai skala abu-abu melalui operasi Boolean XOR.

1.2. Rumusan Permasalahan

Adapun permasalahan yang ada pada system ini yaitu sebagai berikut :

1. Bagaimana cara mengenkripsi gambar?
2. Bagaimana membuat kunci agar berpengaruh pada proses enkripsi dan dekripsi?
3. Bagaimana cara melakukan *permutasi piksel* terhadap gambar yang akan di enkripsi?
4. Bagaimana transformasi dari nilai skala abu-abu melalui proses XOR?

1.3. Tujuan Proyek

Tujuan dari proyek akhir ini adalah membuat sebuah aplikasi untuk enkripsi dan dekripsi gambar dengan metode SIP yang berdasarkan pada algoritma chaotic mapping. Aplikasi ini diharapkan mampu menyembunyikan informasi penting dari sebuah gambar dan mampu menjaga privasi kerahasiaan dari gambar tersebut.

2. Teori Penunjang

2.1. Kriptografi

2.1.1. Sejarah

Kriptografi mempunyai sejarah yang sangat panjang. Sejarah kriptografi dimulai pertama sekali dengan menggunakan metode pertukaran posisi untuk mengenkripsi suatu pesan. Dalam sejarah perkembangannya, Julius Caesar dalam mengirimkan pesan yang dibawa oleh hulubalangannya, sengaja mengacak pesan tersebut sebelum diberikan kepada kurir. Hal ini dilakukan untuk menjaga kerahasiaan pesan baik bagi kurir maupun bagi musuh jika kurir tertangkap di tengah jalan oleh musuh



Gambar. Kriptografi zaman dahulu

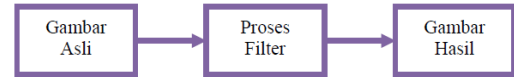
2.1.2. Definisi Kriptografi

Kriptografi (*cryptography*) berasal dari kata 'kryptos' yang artinya tersembunyi dan 'grafia' yang artinya sesuatu yang tertulis (bahasa Yunani) sehingga kriptografi dapat juga disebut sebagai sesuatu yang tertulis secara rahasia (tersembunyi). Kriptografi merupakan seni dan ilmu menyembunyikan informasi dari penerima yang tidak berhak. Enkripsi adalah transformasi data kedalam bentuk yang tidak dapat terbaca tanpa sebuah kunci tertentu. Tujuannya adalah untuk meyakinkan privasi dengan menyembunyikan informasi dari orang-orang yang tidak ditujukan, bahkan mereka mereka yang memiliki akses ke data terenkripsi. Dekripsi merupakan kebalikan dari enkripsi, yaitu transformasi data terenkripsi kembali ke bentuknya semula. Plainimage merupakan data/pesan sebelum dilakukan proses enkripsi atau data sesudah dilakukan proses dekripsi. Chypertext merupakan data setelah dilakukan proses enkripsi.

2.2. Pengolahan Citra

Sebuah citra diubah ke bentuk digital agar dapat disimpan dalam memori komputer atau media lain. Proses mengubah citra ke bentuk digital bisa dilakukan dengan beberapa perangkat, misalnya *scanner*, kamera digital, dan *handycam*. Ketika

sebuah citra sudah diubah ke dalam bentuk digital (selanjutnya disebut citra digital), bermacam-macam proses pengolahan citra dapat diperlakukan terhadap citra tersebut. *Image processing* atau sering disebut dengan pengolahan citra digital merupakan suatu proses dari gambar asli menjadi gambar lain yang sesuai dengan keinginan kita. Misal suatu gambar yang kita dapatkan terlalu gelap maka dengan *image processing* gambar tersebut bisa kita proses sehingga mendapat gambar yang jelas Secara garis besar dapat diilustrasikan seperti tampak pada gambar 2.6 dibawah ini.



Gambar. Blok diagram pengolahan citra

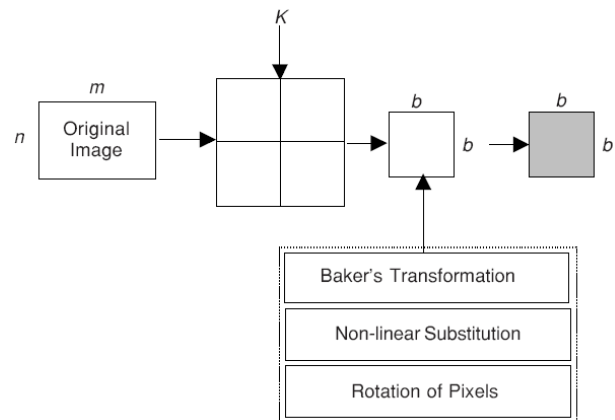
Pengolahan citra adalah pemrosesan citra, khususnya dengan menggunakan komputer, menjadi citra yang kualitasnya lebih baik.

3. Perancangan Sistem

3.1 Secure Image Protection

Secure Image Protection (SIP) secara umum terdiri dari input sistem yang tersiri dari gambar yang akan dienkripsi atau didekripsi dan kunci kemudian dilakukan proses enkripsi atau dekripsi kemudian menghasilkan output gambar yang sudah disembunyikan informasinya. Untuk proses dekripsi dilakukan dengan modus kebalikan dari proses enkripsi. Secara garis besar sistem untuk mendapatkan gambar yang telah di enkripsi.

3.1.1 Input Sistem



Gambar. Blok diagram SIP

Input untuk sistem ini adalah gambar yang akan dienkripsi dan nilai kunci. Dalam tugas akhir ini terdapat fungsi f dimana fungsi f ini digunakan untuk menunjukkan gambar ukuran $m \times n$ dimana m dan n mewakili baris dan kolom gambar masing-masing. $f(x, y)$ adalah nilai skala keabuan piksel pada posisi x dan y

di mana $0 < x \leq m - 1$ dan $0 < y \leq n - 1$. Sebelum melanjutkan ke proses enkripsi, maka gambar akan menjalani konfigurasi awal.

Padding piksel yang ditambahkan pada gambar sehingga gambar dapat dipartisi menjadi blok-blok persegi ukuran $b \times b$. Kondisi padding piksel sebagai berikut

- jika ukuran gambar $m < n$, gambar dibagi menjadi a blok dimana $a = (n + \text{padding piksel}) / m$ dan $b = m$,
- jika ukuran gambar $m > n$, gambar dibagi menjadi a blok dimana $a = (m + \text{padding piksel}) / n$ dan $b = n$.
- $\text{Padding piksel} = n - (m \% n)$

Sedangkan kunci K (Kr) terdiri dari parameter jumlah iterasi dilambangkan dengan Kr.

3.1.2 Proses Enkripsi

Proses enkripsi terdiri dari tiga fungsi utama.

- Fungsi 1: Melakukan permutasi piksel
- Fungsi 2: Nonlinear substitusi umpan balik. Fungsi ini akan mengubah level skala keabuan dari piksel dengan melakukan bitwise sederhana operasi umpan balik nonlinier, yaitu $f'(x_{l+1}, y_k) = f(x_l, y_k) \text{ XOR } f(x_{l+1}, y_k)$ untuk $k = 0 - (b-1)$ dan $l = 0 - (b-1)$.
- Fungsi 3: Pergeseran piksel dalam baris. Untuk lebih mengacak transposisi dari piksel, piksel pada tiap baris akan diputar ke kiri dengan 0, 1, 2, 3 atau 5 shift tergantung pada nilai modulus (nomor baris).

3.2 Perancangan Aplikasi

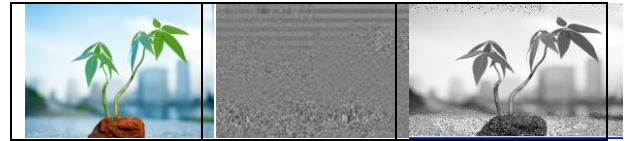
Perangkat lunak enkripsi gambar ini dirancang dengan menggunakan beberapa *user interface*, tamak seperti gambar dibawah



Gambar. User interface aplikasi

4. Hasil dan Kesimpulan

Citra dapat dibedakan dan dapat dilihat pada gambar tabel di bawah ini.



Gambar .a) citra asal b) citra hasil enkripsi c) citra hasil dekripsi

Dari uji coba yang telah dilakukan dengan parameter resolusi cira, jumlah iterasi, dan waktu seperti tampak pada tabel dibawah ini.

Tabel Uji coba aplikasi pada proses enkripsi

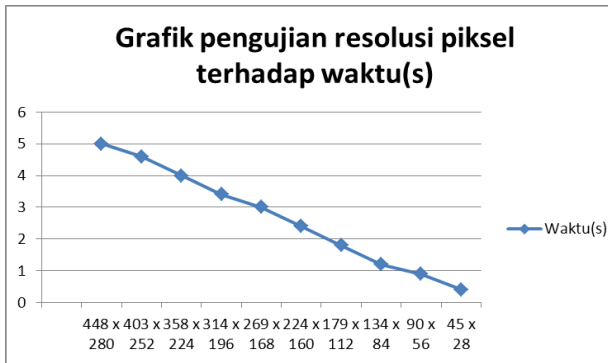
No.	Resolusi	waktu (s) pada iterasi ke-									
		1	2	3	4	5	6	7	8	9	10
1	448 x 280	5	6	7	8	9	10	11	12	13	15
2	403 x 252	4.6	5	5.2	5.8	6.4	7	7.8	8.5	9	10
3	358 x 224	4	4.3	4.7	5.1	5.6	6	6.6	7.3	7.9	8.3
4	314 x 196	3.4	3.7	3.9	4.3	4.7	5.3	6	6.3	6.8	7.3
5	269 x 168	3	3.2	3.4	3.6	4	4.4	4.7	5.2	5.7	6.2
6	224 x 160	2.4	2.5	2.6	2.9	3.2	3.5	3.8	4.3	4.6	5.1
7	179 x 112	1.8	1.8	1.9	2.2	2.5	2.8	3.2	3.5	3.9	4.6
8	134 x 84	1.2	1.3	1.3	1.5	1.6	1.7	2	2.4	2.9	3.5
9	90 x 56	0.9	1.1	1.1	1.2	1.2	1.4	1.7	1.8	2	2.3
10	45 x 28	0.4	0.4	0.5	0.5	0.6	0.6	0.7	0.8	0.8	0.9

Jika diambil beberapa data diatas, kemudian dilakukan uji coba pengaruh ukuran resolusi piksel terhadap waktu maka dapat dilihat pada tabel dibawah ini

Tabel Uji coba untuk iterasi = 1

No.	Ukuran Resolusi	Waktu(s)
1	448 x 280	5
2	403 x 252	4.6
3	358 x 224	4
4	314 x 196	3.4
5	269 x 168	3
6	224 x 160	2.4
7	179 x 112	1.8
8	134 x 84	1.2
9	90 x 56	0.9
10	45 x 28	0.4

Data tabel diatas diperoleh dari hasil iterasi = 1 dan grafik dibawah ini merupakan hasil dari data tabel diatas



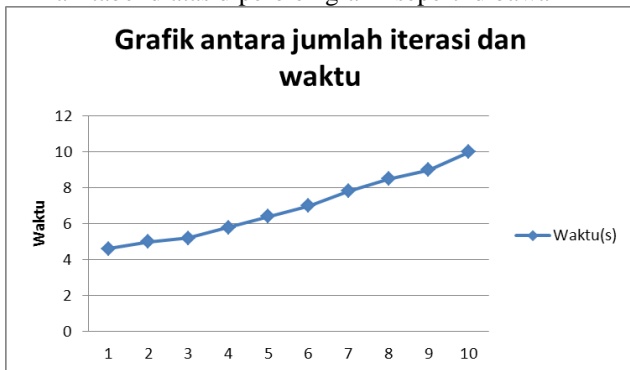
Gambar Grafik pengujian ukuran resolusi – waktu

Kemudian dilakukan uji coba kembali namun kali ini melakukan pengujian jumlah iterasi terhadap waktu dengan citra resolusi 403 x 252 piksel dapat dilihat pada tabel dibawah ini.

Tabel Uji coba untuk resolusi citra 403 x 252 piksel

No.	Jumlah Iterasi	Waktu(s)
1	1	4.6
2	2	5.0
3	3	5.2
4	4	5.8
5	5	6.4
6	6	7.0
7	7	7.8
8	8	8.5
9	9	9.0
10	10	10.0

Dari tabel diatas diperoleh grafik seperti dibawah ini



Gambar Grafik jumlah iterasi – waktu 1

Berdasarkan hasil pengujian sistem yang telah dilakukan didapatkan beberapa kesimpulan :

1. Perangkat lunak enkripsi gambar ini memberikan sebuah metode baru dimana gambar yang diproses adalah piksel-piksel bukan binernya.
2. Keunggulan dari algoritma SIP ini adalah penggunaan fungsi-fungsi yang beragam serta memiliki kemampuan untuk mengenkripsi ukuran gambar, persegi atau persegi panjang sehingga cukup sulit untuk dapat diserang oleh kriptanalisis.
3. Jumlah iterasi dan resolusi citra memiliki nilai yang berbanding lurus terhadap waktu eksekusi program. Semakin bertambah jumlah iterasi dan juga resolusi citra dapat membuat waktu eksekusi bertambah. Dan sebaliknya semakin berkurang jumlah iterasi dan resolusi citra maka semakin berkurang pula waktu eksekusi programnya

DAFTAR PUSTAKA

- [1]Mazleena Salleh, Subariah Ibrahim & Ismail Fauzi Isnin. *Image Encryption Algorithm Based On Chaotic Mapping*. Jurnal Teknologi Universitas Teknologi Malaysia. 2003
- [2]Basuki ,Achmad & Nana Ramadijanti. *Pengantar Grafika Komputer*. Laboratorium Computer Vision – (PENS-ITS).
- [3]Nana Ramadijanti. *Image Processing*. Laboratorium Computer Vision – (PENS-ITS). 2009
- [4]Basuki ,Achmad & Nana Ramadijanti. *Transformasi Gray Scale, Statistik dalam Image Enhancement*. Surabaya. 2009
- [5]Nadhori, Isbat Uzzin. *Introduction of Cryptography*. (PENS-ITS)
- [6]Rinaldi Munir. *Bahan Kuliah IF5054 Kriptografi*. IF-ITB
- [7]Mazleena Salleh, Subariah Ibrahim. *ENHANCED CHAOTIC IMAGE ENCRYPTION ALGORITHM BASED ON BAKER'S MAP*. UTM. 2003
- [8]A Darto Iwan S. *Pengenalan Kriptografi*. Buletindo. 2009
- [9]<http://id.shvoong.com/exact-sciences/physics/1803933-citra-image/>. Diakses pada tanggal 25 Januari 2011

- [10] <http://wasista-eeepis.blogspot.com/2009/03/format-citra.html/>. Diakses pada tanggal 25 Januari 2011
- [11] <http://windupurnomo.wordpress.com/2009/10/18/menghitung-waktu-eksekusi-program-di-java-dan-c/>
Diakses pada tanggal 5 Juli 2011
- [12] Ahmad, Musheer & M. Shamseer Alam. *A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping*. IJCSE. 2009