ISSN 2089-1083

EC-Council

Aptikom Wilayah 7
Asosiasi Perguruan Tinggi Informatika & Komputer

Forum Dosen Kota Malang

Co-host:

STMIK primakara

PROSIDING Volume 04

SNATIKA 2017

Seminar Nasional Teknologi Informasi, Komunikasi dan Aplikasinya

Malang, 23 November 2017

diorganisasi oleh:

Lembaga Penelitian dan Pengabdian pada Masyarakat

Sekolah Tinggi Informatika dan Komputer Indonesia

ISSN 2089 – 1083

SNATIKA 2017

Seminar Nasional Teknologi Informasi, Komunikasi dan Aplikasinya
Volume 04, Tahun 2017

SEKRETARIAT
Lembaga Penelitian dan Pengabdian Kepada Masyarakat
Sekolah Tinggi Informatika & Komputer Indonesia (STIKI) – Malang
SNATIKA 2017
Jl. Raya Tidar 100 Malang 65146, Tel. +62-341 560823, Fax. +62-341 562525
Website: snatika.stiki.ac.id
Email: snatika2017@stiki.ac.id

KATA PENGANTAR

Bapak/Ibu/Sdr. Peserta dan Pemakalah SNATIKA 2017 yang saya hormati, pertama-tama saya ucapkan selamat datang atas kehadiran Bapak/Ibu/Sdr, dan tak lupa kami mengucapkan terimakasih atas partisipasi dan peran serta Bapak/Ibu/Sdr dalam kegiatan ini.

SNATIKA 2017 adalah Seminar Nasinal Teknologi Informasi, Komunikasi dan Aplikasinya yang diselenggarakan oleh STIKI Malang bekerjasama dengan EC-COUNCIL, APTIKOM Wilayah 7 dan Forum Dosen Kota Malang serta Perguruan Tinggi selaku Co-host: Universitas Nusantara PGRI Kediri dan STMIK Primakara Denpasar-Bali. Sesuai tujuannya SNATIKA 2017 merupakan sarana bagi peneliti, akademisi dan praktisi untuk mempublikasikan hasil-hasil penelitian, ide-ide terbaru mengenai Teknologi Informasi, Komunikasi dan Aplikasinya. Selain itu sesuai dengan tema yaitu "*Keamanan Informasi untuk Ketahanan Informasi Kota Cerdas*", topik-topik yang diambil disesuaikan dengan kompetensi dasar dari APTIKOM Wilayah 7 yang diharapkan dapat mensinergikan penelitian yang dilakukan oleh para peneliti di bidang Informatika dan Komputer. Semoga acara ini bermanfaat bagi kita semua terutama bagi perkembangan ilmu dan teknologi di bidang teknologi informasi, komunikasi dan aplikasinya.

Akhir kata, kami ucapkan selamat mengikuti seminar, dan semoga kita bisa bertemu kembali pada SNATIKA yang akan datang.

Malang, 20 November 2017
Panitia SNATIKA 2017

Daniel Rudiaman S., S.T, M.Kom

SAMBUTAN KETUA
SEKOLAH TINGGI INFORMATIKA DAN KOMPUTER INDONESIA (STIKI) MALANG

Yang saya hormati peserta Seminar Nasional SNATIKA 2017,

Puji & Syukur kita panjatkan kepada Tuhan Yang Maha Esa, atas terselenggarakannya Seminar Nasional ini sebagai rangkaian kerjasama dengan EC-COUNCIL, APTIKOM Wilayah 7 dan Forum Dosen Kota Malang serta Perguruan Tinggi selaku Co-host: Universitas Nusantara PGRI Kediri dan STMIK Primakara Denpasar-Bali. Kami ucapkan selamat datang kepada peserta Seminar Nasional serta rekan-rekan perguruan tinggi maupun mahasiswa yang telah berpartisipasi aktif sebagai pemakalah maupun peserta dalam kegiatan seminar nasional ini. Konferensi ini merupakan bagian dari 10 Flag APTIKOM untuk meningkatkan kualitas SDM ICT di Indonesia, dimana anggota APTIKOM khususnya harus haus akan ilmu untuk mampu memajukan ICT di Indonesia.

Konferensi ICT bertujuan untuk menjadi forum komunikasi antara peneliti, penggiat, birokrat pemerintah, pengembang sistem, kalangan industri dan seluruh komunitas ICT Indonesia yang ada didalam APTIKOM maupun diluar APTIKOM. Kegiatan ini diharapkan memberikan masukan kepada *stakeholder* ICT di Indonesia, yang meliputi masyarakat, pemerintah, industri dan lainnya, sehingga mampu sebagai penggerak dalam memajukan ICT Internasional.
Akhir kata, semoga forum seperti ini dapat terus dilaksanakan secara periodik sesuai dengan kegiatan tahunan APTIKOM. Dengan demikian kualitas makalah, maupun hasil penelitian dapat semakin meningkat sehingga mampu bersinergi dengan ilmuwan dan praktisi ICT internasional.

Sebagai Ketua STIKI Malang, kami mengucapkan terimakasih kepada semua pihak atas segala bantuan demi suksesnya acara ini.

“Mari Bersama Memajukan ICT Indonesia”

Malang, 20 November 2017
Ketua STIKI,

Dr. Eva Handriyantini, S.Kom, M.MT.

ISSN 2089-1083
SNATIKA 2017, Volume 04

DAFTAR ISI

Sistem Kriptografi pada Citra Digital Menggunakan Metode Substitusi dan Permutasi

Mety Liesdiani[1], Enny Listiawati[2]
Pendidikan Matematika
STKIP PGRI Bangkalan
[1]metylies@gmail.com, [2]ennylistiwati83@gmail.com

ABSTRAK

Keamanan merupakan salah satu hal yang sangat penting. Salah satu cara untuk mengatasi dan menambah pengamanan tersebut adalah dengan mempelajari dan mengembangkan suatu sistem dengan ilmu kriptografi. Kriptografi merupakan ilmu yang mempelajari keamanan suatu pesan sehingga pesan tersebut tidak bisa dibaca oleh orang yang tidak berhak. Pesan yang bisa diamankan dapat berbentuk suatu citra digital atau gambar. Metode yang digunakan untuk mengamankan suatu file citra digital adalah metode Substitusi dan Permutasi. Kunci yang digunakan merupakan kunci simetri yang digunakan untuk mengenkripsi dan mendekripsi citra digital tersebut.

Kata kunci*: Kriptografi, Citra Digital, Substitusi, Permutasi*

1. Pendahuluan

Keamanan merupakan salah satu bagian penting dari dunia teknologi informasi. Akses jaringan yang tidak mempunyai batas membuat keamanan dari suatu sistem semakin mudah untuk diakses oleh orang-orang yang tidak berhak. Berbagai cara dilakukan oleh ahli-ahli keamanan untuk mengamankan sistemnya sehingga tidak mengganggu kerja dari sistem tersebut. Salah satu tipe *file* yang bisa diamankan adalah tipe gambar.

Pembuatan sistem kriptografi ini didasari dengan adanya beberapa jenis gambar yang tidak dapat oleh orang-orang tertentu karena informasi yang terkandung di dalamnya sangat penting dan rahasia sehingga perlu dibuatkan suat sistem yang dapat menangani masalah tersebut.

2. Metode Penelitian

Kriptografi

Penyandian merupakan salah satu alternatif atau cara mengamankan atau menjaga suatu kerahasiaan data atau gambar. Ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain disebut kriptografi (Ariyus, 2008).

Kriptografi berasal dari bahasa Yunani, *crypto* yang berarti *secret* (rahasia) dan *graphia* yang artinya *writing* (tulisan). Informasi atau pesan adalah salah satu hal penting yang harus disampaikan dalam berkomunikasi. Pesan yang disampaikan dari satu pihak ke pihak yang lain dapat berupa *file* teks, *file* suara, maupun pesan yang berupa *file* gambar. Dalam menyampaikan sebuah informasi atau pesan ke pihak lain, kerahasiaan dan keaslian pesan perlu dijaga Sehingga pesan perlu disandikan sebelum dilakukan pengiriman.

Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentifikasi data, dengan kata lain kriptografi digunakan untuk menjamin keleluasaan pribadi dan pembuktian keaslian pesan dalam berkomunikasi.

Kriptografi terdiri dua algoritma yaitu, algoritma enkripsi dan algoritma dekripsi. Enkripsi adalah pengamanan data yang dikirimkan agar terjaga kerahasiaannya (Ariyus, 2008). Pesan asli sebelum dienkripsi disebut sebagai *plaintext*, di mana *plaintext* inilah yang akan diubah menjadi kode-kode yang tidak dimengerti yang disebut sebagai *ciphertext.* Dekripsi merupakan kebalikan dari enkripsi. Dekripsi adalah proses untuk mengembalikan *ciphertext* ke bentuk asalnya (*plaintext*) sehingga dapat terbaca kembali (Ariyus, 2008). Untuk melakukan proses enkripsi maupun dekripsi biasanya digunakan suatu kunci. Kunci terbagi menjadi dua bagian, yaitu kunci rahasia (*private key*) dan kunci umum (*public key*).

Penyandian suatu pesan atau mengenkripsi pesan, terdapat dua jenis

algoritma yang berdasarkan jenis kuncinya, yaitu:

1. Algoritma Simetri, menggunakan satu kunci untuk enkripsi dan dekripsinya.
2. Algoritma Asimetri, menggunakan kunci yang berbeda untuk enkripsi dan dekripsinya.

Penyandian Citra Digital

Kata penyandian citra digital atau gambar terdiri dari tiga buah kata yaitu pertama adalah penyandian, mempunyai kata dasar "sandi" yang menurut kamus besar Bahasa Indonesia berarti kode, sedangkan penyandian adalah sebuah bentuk kata kerja yang berarti suatu kegiatan menyandikan atau mengkodekan dengan tujuan tertentu. Kedua adalah *file* yaitu sebutan sekumpulan *byte* atau deretan karakter atau kode-kode yang membentuk sebuah dokumen yang memiliki nama yang unik, sedangkan yang ketiga adalah gambar yang dalam kamus besar bahasa Indonesia adalah "citra", citra adalah objek elemen-elemen yang dinyatakan dengan suatu besara numerik yang membentuk (*array*) sehingga penyandian file gambar dapat diartikan kegiatan menyandikan atau mengkodekan sekumpulan elemen penyusun gambar (*pixel*) dengan tujuan mengamankan informasi dari pihak yang tidak berhak mengaksesnya.

Metode Enkripsi

Metode enkripsi yang digunakan pada penelitian kali ini adalah metode substitusi dan permutasi. Aplikasi yang dibuat nantinya akan menggunakan gabungan dari kedua metode tersebut untuk menghasil gambar dengan susunan *pixel* yang tidak beraturan. Alasan digunakannya metode lebih dari satu agar menghasilkan gambar yang lebih rumit lagi sehingga informasi di dalamnya dapat lebih aman.

Metode Substitusi Pixel

Substitusi *pixel* pada suatu citra digital merupakan suatu metode untuk mengubah letak (koordinat) suatu *pixel* pada citra/gambar dan menggantikannya dengan *pixel* yang lain pada satu citra yang sama. Metode ini digunakan untuk mengamankan suatu citra, misal suatu *pixel* gambar terletak di koordinat *(x,y)* = (10,0) akan dipindahkan letaknya pada koordinat *(x,y)* = (10,10). Pengubahan letak suatu *pixel* pada citra dapat dilakukan sesuai dengan persamaan atau rumus yang telah dibuat dan ditetapkan sebelumnya. Metode substitusi yang digunakan pada penelitian kali ini dilakukan sebanyak empat kali.

Metode Substitusi Pixel Pada Baris Genap Atau Baris 0

Substitusi antar kolom digital pada baris genap atau baris 0 merupakan pertukaran letak kolom dari suatu citra yang mana *pixel* dari kolom tersebut terletak pada baris genap atau baris 0.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

Gambar 1. Citra Awal Substitusi Antar Kolom pada Baris Genap atau Baris 0

Proses substitusi dibuat dengan tujuan untuk menukar *pixel* pada kolom ke-0 dengan kolom ke-9, kolom ke-1 dengan kolom ke-8, kolom ke-2 dengan kolom ke-7, dan seterusnya pada baris genap.

10	9	8	7	6	5	4	3	2	1
11	12	13	14	15	16	17	18	19	20
30	29	28	27	26	25	24	23	22	21

Gambar 2. Citra Hasil Substitusi Antar Kolom pada Baris Genap atau Baris 0

Metode Enkripsi Substitusi Pixel Pada Kolom Ganjil

Substitusi antar baris pada kolom genap merupakan pertukaran letak baris dari suatu citra digital yang mana *pixel* dari baris tersebut terletak pada kolom ganjil.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24

Gambar 3. Citra Awal Substitusi Antar Baris Pada Kolom Ganjil

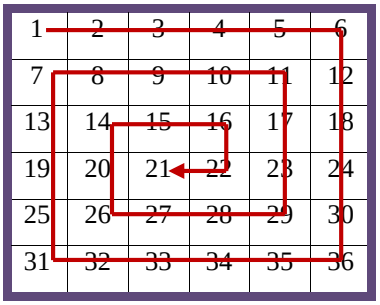
Proses substitusi dibuat dengan tujuan untuk menukar *pixel* pada baris ke-0 dengan baris ke-3, baris ke-1 dengan baris ke-2, dan seterusnya pada kolom ganjil. Hasil dari proses tersebut ditunjukkan pada gambar 4.

1	20	3	22	5	24
7	14	9	16	11	18
13	8	15	10	17	12
19	2	21	4	23	6

Gambar 4. Citra Hasil Substitusi Antar Baris Pada Kolom Ganjil

Metode Enkripsi Substitusi Pixel Spiral

Substitusi spiral merupakan substitusi dengan menggunakan metode pembacaan matriks pada citra secara spiral. Proses pembacaan secara spiral ditunjukkan pada gambar 5.



Gambar 5. Proses Pembacaan Citra secara Spiral

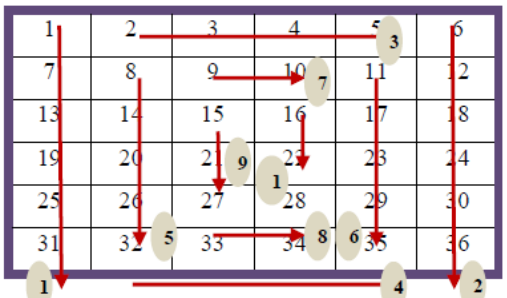
Hasil dari pembacaan secara spiral menghasilkan matriks yang ditunjukkan pada gambar 6.

1	2	3	4	5	6
12	18	24	30	36	35
34	33	32	31	25	19
13	7	8	9	10	11
17	23	29	28	27	26
20	14	15	16	22	21

Gambar 6. Citra Hasil Substitusi Spiral

Metode Enkripsi Substitusi Pixel Alur Kotak

Substitusi alur kotak merupakan substitusi dengan menggunakan metode pembacaan matriks pada citra mengikuti bentuk kotak, dimulai dengan pembacaan *pixel* kolom awal dan akhir terlebih dahulu kemudian dilanjutkan pembacaan *pixel* pada baris awal dan akhir.



Gambar 7. Pembacaan Citra secara Alur Kotak

Hasil dari pembacaan secara alur kotak menghasilkan matriks yang ditunjukkan pada gambar 8.

1	7	14	19	25	31
6	12	18	24	30	36
2	3	4	5	32	33
34	35	8	14	20	26
11	17	23	29	9	10
27	28	15	21	16	22

Gambar 8. Citra Hasil Substitusi Alur Kotak

Metode Enkripsi Permutasi

Permutasi (transposisi) pada citra digital merupakan pertukaran berdasarkan kunci yang dimasukkan. Kunci yang dimaksud adalah kunci yang terdiri dari beberapa karakter, diurutkan berdasarkan kode ASCII (*American Standard Code for Information Interchange)* dari karakter-karakter tersebut dan dari urutan tersebut baris-baris matriks dua dimensi pada citra digital akan diurutkan. Panjang dari suatu kunci harus lebih kecil atau sama dengan dari jumlah kolom dari suatu citra atau matriks.

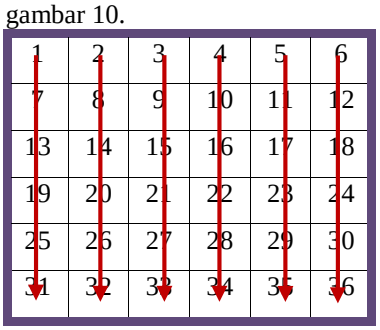
Kunci yang digunakan pada contoh ini adalah kata ENKRIP. Dari kata ENKRIP akan didapat urutan kunci yaitu 0-3-2-5-1-4. Dengan membandingkan jumlah kolom citra secara urut maka akan menghasilkan urutan dari kolom yang harus disusun, seperti yang ditunjukkan pada gambar 9.

E	N	K	R	I	P
0	3	2	5	1	4
0	1	2	3	4	5

0	4	2	1	5	3

Gambar 9. Permutasi Kunci dan Inversi Kunci

Proses dari pembacaan citra dengan urutan yang telah ditentukan ditunjukkan pada gambar 10.



Gambar 10. Proses Urutan Pembacaan Kolom Citra

Hasil dari pembacaan citra sesuai dengan urutan ditunjukkan pada gambar 11.

1	7	13	19	25	31
5	11	17	23	29	35
3	9	15	21	27	35
2	8	14	20	26	32
6	12	18	24	30	36
4	10	16	22	28	34

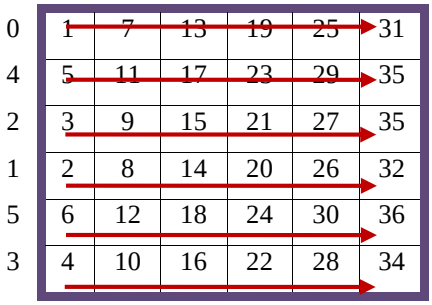
Gambar 11. Hasil Pembacaan Kolom Citra

Metode Dekripsi

Metode dekripsi yang digunakan merupakan kebalikan dari metode-metode yang digunakan pada proses pengenkripsian sebelumnya, namun dengan urutan proses yang berbeda.

Metode Dekripsi Permutasi

Proses dekripsi secara permutasi merupakan proses pengembalian dari suatu citra yang telah terenkripsi dengan menggunakan inversi dari urutan kunci yang telah dimasukkan sebelumnya. Dalam hal ini kunci yang digunakan adalah kunci yang telah dijelaskan sebelumnya (Gambar 9). Proses pengembalian suatu citra dilakukan secara berlawanan. Jika proses pembacaan enkripsi suatu citra dilakukan secara perkolom, maka untuk proses dekripsi proses pembacaan dilakukan secara perbaris dengan urutan sesuai kunci yang telah dimasukkan. Proses pembacaan dapat ditunjukkan pada gambar 12.



Gambar 12. Proses Pembacaan Dekripsi Citra

Hasil dari pembacaan citra sesuai dengan urutan ditunjukkan pada gambar 13.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36

Gambar 13. Hasil Proses Pembacaan Dekripsi Citra

Metode Dekripsi Substitusi Pixel Alur Kotak

Proses dekripsi substitusi alur kotak merupakan substitusi dengan menggunakan metode pembacaan matriks secara konvensional dan peletakan kembali *pixel-pixel* pada citra mengikuti bentuk kotak.

Gambar 14. Pembacaan Citra secara Alur Kotak

Hasil dari pembacaan secara alur kotak menghasilkan matriks yang ditunjukkan pada gambar 15.

Gambar 14. Citra Hasil Substitusi Alur Kotak

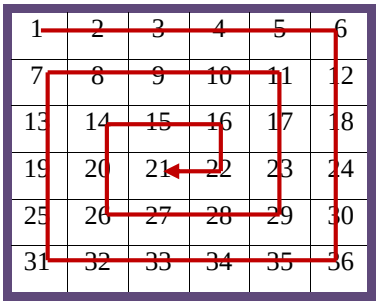
Metode Dekripsi Substitusi Pixel Spiral

Proses dekripsi substitusi spiral merupakan substitusi dengan menggunakan metode pembacaan matriks pada citra secara konvensional dan diletakkan kembali secara spiral. Proses pembacaan secara spiral ditunjukkan pada gambar 16.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36

Gambar 16. Proses Pembacaan Citra secara Spiral

Hasil dari pembacaan secara konvensional dan diletakkan secara spiral menghasilkan matriks yang ditunjukkan pada gambar 17.



Gambar 17. Citra Hasil Substitusi Spiral

Metode Dekripsi Substitusi Pixel Pada Kolom Ganjil

Proses dekripsi substitusi antar baris pada kolom genap merupakan proses pengembalian suatu citra denan menukar letak baris dari suatu citra digital yang mana *pixel* dari baris tersebut terletak pada kolom ganjil.

1	20	3	22	5	24
7	14	9	16	11	18
13	8	15	10	17	12
19	2	21	4	23	6

Gambar 18. Citra Awal Substitusi Antar Baris Pada Kolom Ganjil

Hasil dekripsi dari matriks sebelumnya ditunjukkan pada gambar 19.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24

Gambar 19. Citra Hasil Substitusi Antar Baris Pada Kolom Ganjil

Metode Dekripsi Substitusi Pixel Pada Baris Genap Atau Baris 0

Proses dekripsi Substitusi antar kolom digital pada baris genap atau baris 0 merupakan proses pengembalian sutau citra dengan menukar letak kolom dari suatu citra yang mana *pixel* dari kolom tersebut terletak pada baris genap atau baris 0.

10	9	8	7	6	5	4	3	2	1
11	12	13	14	15	16	17	18	19	20
30	29	28	27	26	25	24	23	22	21

Gambar 20. Citra Awal Dekripsi Substitusi Antar Kolom pada Baris Genap atau Baris 0

Hasil Pengembalian atau dekripsi dari suatu matriks citra ditunjukkan pada gambar.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

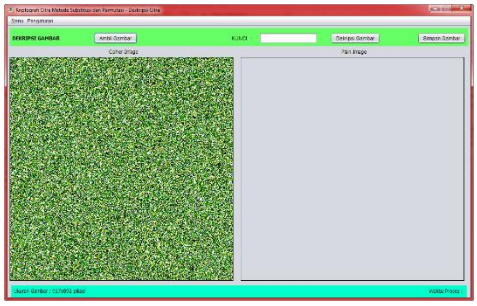
Gambar 21. Citra Hasil Dekripsi Substitusi Antar Kolom pada Baris Genap atau Baris 0

3. Implementasi Sistem

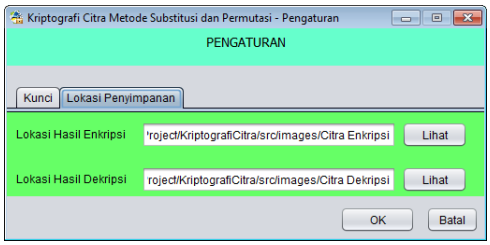
1. **Menu Utama**
   Menu Utama (Gambar 21)merupakan bagian utama dari sistem yang menyediakan fasilitas untuk mengakses langsung menu-menu lainnya, seperti menu enkripsi citra, menu dekripsi citra dan sebagainya.
2. **Menu Enkripsi Citra**
   Menu Enkripsi Citra (Gambar 22) merupakan menu yang dibuat untuk mengenkripsi suatu *file* citra digital atau gambar
3. **Menu Dekripsi Citra**
   Menu Dekripsi Citra (Gambar 23) merupakan menu yang dibuat untuk mendekripsi suatu *file* citra digital atau gambar
4. **Menu Pengaturan**
   Menu pengaturan (Gambar 24) digunakan untuk mengatur beberapa aturan, seperti minimal panjang dari kunci, lokasi penyimpanan gambar hasil enkripsi dan lokasi penyimpanan gambar hasil dekripsi

Gambar 22. Menu Utama

Gambar 23. Menu Enkripsi Citra



Gambar 24. Menu Dekrispi Citra



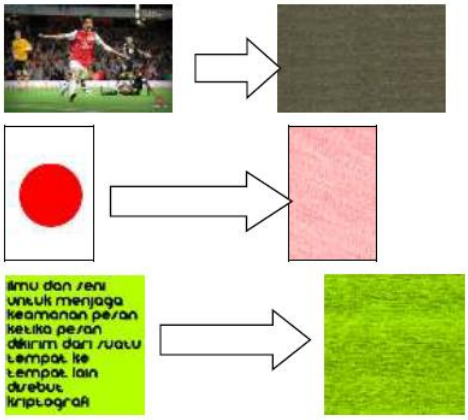
Gambar 25. Menu Pengaturan

Pengujian Sistem dan Analisa Hasil

Pengujian pada sistem difokuskan pada tahapan enkripsi citra dan dekripsi citra Pengujian pada enkripsi dan dekripsi dilakukan untuk menguji tingkat keberhasilan, apakah suatu citra dapat dienkripsi dengan menggunakan kunci atau kata sandi, dan citra dapat dideskripsi atau dikembalikan kembali sehingga informasi yang terkandung di dalamnya terbaca kembali. Pada bagian dekripsi citra juga akan diuji hasil dari dekripsi citra-citra terenkripsi yang mempunyai format JPG dan PNG untuk dibandingkan mana yang menghasilkan kualitas yang lebih baik.

Pengujian Proses Enkripsi

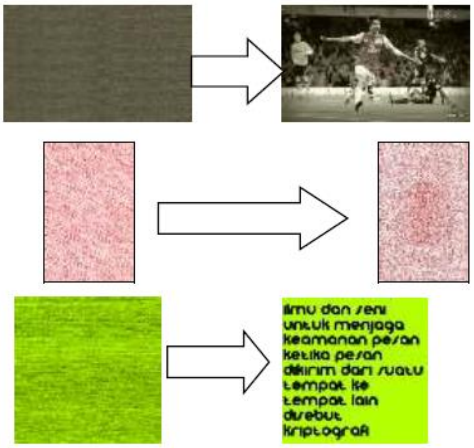
Pengujian pada proses enkripsi menggunakan citra sebagai media ujinya. Setiap citra akan disertai masing-masing kunci untuk enkripsinya. Gambar di bawah ini menunjukkan hasil proses enkripsi dari beberapa gambar yang dijadikan bahan uji dari sistem ini.



Gambar 26.`Hasil Enkripsi Beberapa Citra

Hasil percobaan menunjukkan semua gambar/citra, baik yang berupa JPG maupun PNG berhasil diproses untuk dienkripsi. Yang membedakan terletak pada ukuran *pixel* dari suatu gambar. Semakin besar ukuran *pixel* suatu gambar, maka semakin lama pula enkripsi memakan waktu. Hasil Percobaan juga menunjukkan bahwa jika kunci yang dimasukkan berbeda, maka akan menghasilkan gambar enkripsi yang berbeda pula bentuknya.

Pengujian Proses Dekripsi



Gambar 27. Hasil Dekripsi Beberapa Citra

Hasil percobaan proses dekripsi, dapat diketahui bahwa jika gambar didekripsi menggunakan kunci yang benar, maka gambar akan kembali menjadi bentuk asalnya. Sebaliknya jika citra didekripsi menggunakan kunci yang salah maka keadaan gambar tidak akan kembali menjadi seperti semula. Dari hasil percobaan dapat dilihat pula perbedaan yang dihasilkan pada gambar terenkripsi yang disimpan dalam format JPG dan PNG. Dekripsi gambar yang awalnya berformat JPG menghasilkan gambar yang kualitasnya berkurang, dalam hal ini ada perubahan dalam warna citra tersebut. Sedangkan dekripsi gambar dengan format PNG menghasilkan citra yang hampir sama persis dengan citra asli sebelum dienkripsi. Hal ini sesuai dengan yang telah dijelaskan bahwa citra dengan format JPG akan mengkompresi gambar dengan sedikit menurunkan kualitas gambar (*lossy compression*). Sebaliknya, citra yang disimpan dalam format PNG tidak akan mengkompresi gambar/citra aslinya (*loss-less compression*) sehingga kualitas dari suatu citra tidak berkurang.

4. Kesimpulan

Berdasarkan hasil penelitian dan implementasi sistem, maka dapat diambil kesimpulan bahwa:

1. Sistem Kriptografi pada Citra Digital menggunakan metode Substitusi dan Permutasi telah dibangun.
2. Sistem Kriptografi pada citra digital (gambar) dengan metode substitusi dan permutasi dapat menghasilkan gambar yang tidak dapat dikenali seperti gambar semula.
3. Metode penyandian dengan substitusi dan permutasi yang diterapkan dalam mengakses *pixel-pixel* dari suatu gambar berhasil memanipulasi posisi dan mengacak susunan *pixel* pada gambar atau citra digital.
4. Gambar yang sudah disandikan dan tidak dapat dikenali dapat dikembalikan lagi oleh sistem yang telah dibuat, sehingga gambar dapat kembali dikenali.
5. Gambar yang dienkripsi dengan kunci yang berbeda akan menghasilkan gambar yang berbeda pula.
6. Gambar yang mempunyai ukuran *pixel* kecil menghasilkan waktu proses yang lebih singkat, sedangkan gambar yang mempunyai ukuran *pixel* yang besar menghasilkan waktu proses yang lebih lama. Semakin besar *pixel* warna maka semakin besar pula waktu proses yang diperlukan.
7. Gambar hasil enkripsi jika disimpan dalam bentuk JPG akan mengubah warna asli dari gambar asli tersebut. Sebaliknya jika disimpan dalam bentuk PNG maka tidak ada perubahan warna dari gambar aslinya.

8. Enkripsi suatu citra digital menggunakan kunci yang terurut dan didekripsi menggunakan kunci yang berbeda tetapi berurut masih dapat mengembalikan citra enkripsi menjadi seperti semula.
9. Jika hasil citra enkripsi diubah ukurannya, maka gambar tersebut tidak dapat didekripsikan kembali karena ada perubahan jumlah *pixel.*

5. Referensi

[1] Ariyus, D. 2008. *Keamanan Multimedia*. Yogyakarta: C.V Andi Offset.

[2] Ariyus, D. 2008. *Pengantar Ilmu Kriptografi.* Yogyakarta: C.V Andi Offset.

[3] González R.C. dan Woods, R.E. 2008, *Digital Image Processing*. New Jersey: Prentice Hall.

[4] Knudsen, J. 1999. *Java 2D Graphics.* California: OReilly Media.

[5] Kristanto, A. 2004. *Rekayasa Perangkat Lunak (Konsep Dasar).*Yogyakarta: Penerbit Gava Media.

[6] Kurniawan, Y. 2004, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung: Informatika.

[7] Putra, D. 2010. *Pengolahan Citra Digital.* Yogyakarta: C.V Andi Offset.