OPTIMASI ALGORITMA SUPER ENKRIPSI UNTUK MENINGKATKAN PENGAMANAN DATA CITRA DIGITALDALAM PENGIRIMAN MMS PADA PIRANTI CERDAS

Emy Setyaningsih[1], Catur Iswahyudi [2], Naniek Widyastuti [3]

[1.]Program Studi Sistem Komputer, [2,3] Program Studi Teknik Informatika,
Intitut Sains & Teknologi AKPRIND Yogyakarta.

Masuk: 9 Oktober 2012, revisi masuk: 18 Desember 2012, diterima: 3 Januari 2013

ABSTRACT

Advances in technology have made communication and information technology functions into convergent and known as ICT (Information and Communication Technology). Internet and smart devices have an important role as a medium for multimedia convergence at this time. Mobile communications technology also developed rapidly, as well as the development of features that support services in the GSM system, among others, is MMS (Multimedia Messaging Service) that allows data transmission such as images, audio, and video.Computational complexity becomes an important concern in the development of cryptographic techniques on smart devices in the limited of bandwidth on wireless networks, also limited processing, memory, and time. This paper will discuss the security of image message using the concept of super encryption to optimize security of encryption key that adopts the concept of steganography method called End Of File (EOF). Applications built able to combine the speed, security, and flexibility so as to produce a good combination of speed, high security, complexity, reasonable computational overhead, and computational power.Image encryption algorithm is successfully implemented on a smart device with Android based operating system. Application also has the fastprocess and efficient computing resource. These are evidenced by the average time of encryption for image size of 256 x 256 pixels at 0.75 seconds and the image with a size of 480 x 640 pixels at 2.09 seconds. Average time decryption to image size of 256 x 256 pixels by 0.58 seconds and the image with a size of 480 x 640 pixels of 1.66 seconds.

Keywords : *smart device, Multimedia Messaging Service (MMS), cryptographic, super encryption, steganography.*

INTISARI

Kemajuan teknologi telah menjadikan fungsi teknologi informasi dan komunikasi menjadi konvergen sehingga kini muncul istilah ICT (*Information and Communication Technology*). Internet dan piranti cerdas memiliki peran penting sebagai medium untuk konvergensi multimedia saat ini. Teknologi komunikasi bergerak juga berkembang pesat, begitu juga perkembangan fitur-fitur layanan yang mendukung dalam sistem GSM, antara lain adalah MMS (*Multimedia Messaging Service*) yang memungkinkan melakukan pengiriman data berupa citra, audio, dan video. Kompleksitas komputasi menjadi perhatian penting dalam pengembangan teknik kriptografi pada piranti cerdas di tengah keterbatasan *bandwidth* pada jaringan nirkabel, keterbatasan pemroses, memory, dan waktu. Pada makalah ini akan dibahas keamanan pesan citra menggunakan konsep super enkripsi dengan mengoptimalkan keamanan kunci enkripsi yang mengadopsi konsep steganografi yaitu metode End Of File (EOF). Aplikasi yang dibangun mampu memadukan antara kecepatan, keamanan, dan fleksibilitas sehingga menghasilkan kombinasi yang baik antara kecepatan, pengamanan yang tinggi, kompleksitas, *reasonable computational overhead*, dan *computational power.*Dari hasil pengujian berhasil didapatkan algoritma enkripsi citra yang dapat diimplementasikan pada piranti cerdas dengan basis sistem operasi Android, yang hemat sumberdaya komputasi serta

[1] catur@akprind.ac.id,
[2] emypurnomo@akprind.ac.id, [3)]
[3] naniek_wid@yahoo.com

proses yang cepat. Hal tersebut dibuktikan dengan rata-rata waktu enkripsi untuk citra ukuran 256 x 256 piksel sebesar 0,75 detik dan citra dengan ukuran 480 x 640 piksel 2,09 detik. Rata-rata waktu dekripsi untuk citra ukuran 256 x 256 piksel sebesar 0,58 detik dan citra dengan ukuran 480 x 640 piksel sebesar 1,66 detik.

Kata Kunci : piranti cerdas, *Multimedia Messaging Service* (MMS), kriptografi, super enkripsi, steganografi.

PENDAHULUAN

Teknologi komunikasi bergerak saat ini berkembang dengan sangat cepat, begitu juga perkembangan fitur-fitur layanan yang mendukung dalam sistem GSM. Salah satu layanan yang ditawarkan adalah MMS (*Multimedia Messaging Service*) yang merupakan perkembangan dari SMS (*Short Message Service*) yang memungkinkan untuk melakukan pengiriman data berupa citra digital.

Keamanan informasi menjadi isu penting dalam penyimpanan dan transmisi data. Penggunaan data citra pun semakin luas dalam berbagai bidang. Untuk itu diperlukan sistem pengamanan untuk melindungi data yang ditransmisikan melalui suatu jaringan komunikasi, antara lain dengan menggunakan teknik kriptografi. Namun demikian enkripsi tidak dapat mencegah intersepsi dan modifikasi data pada saluran komunikasi. Enkripsi tidak mampu melindungi komunikasi dari para pendengar rahasia *(eavesdropper)* untuk mengekstrak data rahasia (Chang Lo, 2007).

Hingga bulan Agustus 2011, berdasarkan penelitian oleh AC Nielsen terhadap pengguna piranti cerdas di Amerika Serikat seperti yang dilansir oleh situs www.dailytech.com dan http:// www.netmarketshare.com/, Google Android memiliki *market share* 43%, diikuti oleh iPhone (28%), RIM (18%), dan Microsoft (11%). Sedangkan untuk pengguna di seluruh dunia, Microsoft Windows Mobile memiliki market share 4,9%, dan Google Android sebesar 18,9%. Sementara Apple dengan iOS sebesar 61,5%, Java ME (12,8%), dan Symbian (3,5%).

Jumlah pengguna ponsel BlackBerry di Indonesia hampir mencapai 9 juta pengguna (Juli 2012). Fakta tersebut membuat Indonesia dijuluki sebagai Negara blackBerry, pasalnya angka 9 juta juga menempatkan Indonesia sebagai pengguna ponsel Ber-OS BlackBerry terbanyak di dunia. Namun, semakin gencar munculnya ponsel Android membuat pengguna ponsel BlackBerry beralih ke sistem operasi lain. Berdasar-kan hasil penelitian firma Analis IDC, jumlah pengguna Android di Indonesia selama tahun 2012 meningkat dan menguasai 52% smartphone yang beredar di pasar Indonesia (republika. co.id, 2012).

Kriptografi pada piranti cerdas memunculkan tantangan baru, karena keterbatasan sumberdaya komputasi pada perangkat. Kompleksitas komputasi menjadi perhatian penting dalam pengembangan teknik kriptografi di tengah keterbatasan *bandwidth* pada jaringan nirkabel, keterbatasan pemroses, memory, dan waktu. Oleh sebab itu, diperlukan *tradeoff* antara kecepatan, keamanan, dan fleksibilitas sehingga menghasilkan kombinasi yang baik antara kecepatan, pengamanan yang tinggi, kompleksitas, *reasonable computational overhead*, dan *computational power* (Jolfaei dan Mirghadri, 2011).

Beberapa penelitian yang telah dilakukan untuk mendapatkan algoritma yang handal untuk mengamankan data citra telah pula dilakukan oleh beberapa peneliti diantaranya Abrihama(2008), Stinson(1995), dan Younes (2008). Penelitian untuk mendapatkan algoritma enkripsi citra yang sederhana namun aman dengan proses yang cepat dan hemat sumber daya komputasi yang menggabungkan dua buah cipher yaitu Playfair cipher dan Vigenere cipher telah dilakukan oleh Setyaningsih, dkk (2012). Pemilihan algoritma ini karena Super Enkripsi tidak membutuhkan resource yang banyak, sehingga cocok untuk diterapkan pada telepon seluler yang memiliki kapasitas memori yang terbatas. Kendala yang dijumpai pada kunci Super Enkripsi adalah ukurannya yang cukup besar yaitu 16 x 16 piksel sehingga sangat sulit untuk diingat. Hal tersebut menyebabkan pertukaran kunci yang dilakukan melalui email, atau pesan sms

menjadi tidak aman. Fridrich dan Goljan (2002) melakukan pengujian kehandalan steganografi berdasarkan serangan yang terjadi pada steganografi. Pengujian dilakukan menggunakan RS Analisis pada tool Steganos, S-Tools, Hide4PGP. Manglem dkk. (2007) menggabungkan kriptografi dan steganografi. Metode steganografi yang digunakan adalah Sequential LSB, Random LSB, Edge LSB, dan Random Edge LSB. Enkripsi dilakukan terhadap pesan yang akan disisipkan, sedangkan algoritma enkripsi yang digunakan adalah S-DES. Pengujian untuk mengetahui kehandalan steganografi dilakukan dengan cara mendeteksi menggunakan Gradient Energy, selain itu membandingkan juga hasil dari masing-masing steganografi yang diuji dengan gradient energy. Hasil yang didapat dari perbandingan gambar steganografi yaitu gambar steganografi dapat dideteksi kecuali Random Edge LSB. Anneria (2008) melakukan pendeteksian gambar steganografi yang dihasilkan oleh beberapa tool yaitu InPlainView, S-Tool dan The Thrid Eyes. Metode steganalisis yang digunakan yaitu RS-Analysis. Pendeteksian dengan RS-Analisis dapat mengetahui prosentase noise pada RGB dalam pixel. Dalam penelitian ini diketahui bahwa gambar yang disisipi pesan dengan ukuran pesan yang kecil akan sulit untuk dideteksi.

Penelitian ini bertujuan untuk mengoptimalkan keamanan pada kunci yang digunakan. Teknik yang diusulkan adalah mengadopsi dari konsep steganografi menggunakan metode End Of File (EOF), yaitu menyisipkan/ menyebunyikan kunci yang digunakan untuk proses enkripsi dan dekripsi pada citra hasil enkripsi sebelum dikirimkan. Metode EOF mempunyai kelebihan mampu menyisipkan kunci yang sangat besar, sehingga cocok untuk menyisipkan kunci playfair yang berukuran cukup panjang.

METODE

Teknik enkripsi citra bertujuan untuk mengkonversi citra ke bentuk lain sehingga sulit dipahami. Sedangkan teknik dekripsi digunakan untuk mengembalikan citra terenkripsi menjadi citra asli. Terdapat banyak sistem enkripsi citra untuk melakukan enkripsi dan dekripsi, namun tidak ada algoritma enkripsi tunggal yang memuaskan untuk berbagai tipe citra (Gupta, 2009).

Dalam enkripsi citra digital, terdapat dua level enkripsi yaitu *low-level* dan *high-level*. Dalam enkripsi *low-level*, citra yang terenkripsi mengalami penurunan kualitas visual dibandingkan dengan citra asli. Namun citra tersebut tetap dapat terlihat dan dipahami oleh orang yang melihat. Dalam enkripsi *high-level*, isi citra benar-benar teracak dan hanya nampak seperti derau (*noise*). Dengan demikian citra menjadi tidak dapat dipahami oleh orang yang melihatnya (Krikor dkk., 2009). Sementara itu Puech (2005) mengatakan bahwa karakteristik visual yang paling penting dari citra terletak pada frekuensi rendah, sedangkan informasi detil tersimpan di frekuensi yang lebih tinggi. Penglihatan manusia (HVS-*Human Visual System*) lebih sensitif pada frekuensi rendah dibandingkan dengan frekuensi tinggi. Younes (2008) mengatakan bahwa semua cipher image yang hanya berbasis permutasi tidak aman dari serangan *known-plaintext*. Ia menyarankan agar permutasi rahasia harus digabungkan dengan teknik enkripsi lain untuk menghasilkan citra yang benar-benar aman.

Super enkripsi merupakan salah satu kriptografi berbasis karakter yang menggabungkan cipher substitusi dan cipher transposisi. Hal tersebut bertujuan untuk mendapatkan cipher yang lebih kuat daripada hanya menggunakan satu cipher saja, sehingga tidak mudah untuk dipecahkan. Enkripsi dan dekripsi dapat dilakukan dengan urutan cipher substitusi kemudian cipher transposisi, atau sebaliknya. Konsep super enkripsi dapat diperluas penggunaannya dari teks ke citra warna. Ini dimungkinkan mengingat sebuah citra merupakan deretan piksel-piksel yang terdiri atas komponen R (Red), G (Green), B (Blue) yang merupakan bilangan-bilangan bulat sehingga dapat dioperasikan dalam sebuah matrik. Super enkripsi juga tidak membutuhkan sumberdaya yang besar, sehingga cocok untuk diterapkan pada telepon seluler

yang memiliki kapasitas memori yang terbatas.

Algoritma superenkripsi yang dikembangkan pada penelitian ini menggunakan konsep *symmetric cryptosystem. Symmetric cryptosystem* sangat menekankan pada kerahasiaan kunci yang digunakan untuk proses enkripsi dan dekripsi. Oleh karena itulah sistem ini sering disebut sebagai *secret-key ciphersystem*. *Secret-key cryptography* merupakan bentuk kryptografi yang lebih tradisional, dimana sebuah kunci tunggal dapat digunakan untuk mengenkrip dan mendekrip pesan. Kriptografi kunci-simetrik mengarah kepada metode enkripsi yang mana baik pengirim maupun yang dikirim saling memiliki kunci yang sama. Masalah utama yang dihadapi *secret-key cryptosystems* adalah membuat pengirim dan penerima menyetujui kunci rahasia tanpa ada orang lain yang mengetahuinya. Ini membutuhkan metode dimana dua pihak dapat berkomunikasi tanpa takut akan disadap.

Untuk menghadapi serangan semacam ini kriptografer harus menggunakan kunci yang lebih panjang dan tidak mudah ditebak. Semakin panjang kunci maka waktu *exhaustive search* menjadi makin sulit dan bahkan tidak mungkin dilakukan karena waktu yang dibutuhkan semakin lama. Namun cara ini mempunyai kelemahan dimana untuk mengingat kunci yang sangat panjang tentulah tidak mudah. Misalkan untuk kunci playfair yang digunakan pada penelitian ini ukurannya adalah 16 x 16 piksel atau 256 piksel warna. Apabila setiap piksel warna diwakili dengan 3 digit angka maka panjang kunci yang harus diingat sepanjang 256 x 3 = 768 digit angka. Hal ini tentu saja sangat menyulitkan baik bagi penerima apabila ingin melakukan proses dekripsi. Oleh karena itu pada penelitian ini diusulkan sebuah cara untuk mengoptimalkan keamanan pada kunci yang digunakan. Teknik yang diusulkan adalah mengadop dari konsep steganografi menggunakan metode *End Of File* (EOF), yaitu menyisipkan/ menyembunyikan kunci yang digunakan untuk proses enkripsi dan dekripsi pada image hasil enkripsi sebelum dikirimkan. Metode *End Of File* (EOF) mempunyai kelebihan mampu menyisipkan kunci yang sangat besar, sehingga cocok untuk menyisipkan kunci playfair yang berukuran cukup panjang.

Dengan menggunakan konsep ini maka pengirim maupun penerima pesan cukup hanya mengingat 6 digit angka yang mewakili intensitas dari warna citra dan tidak perlu mengingat 768 digit angka. Dimana 6 digit angka ini nanti sebagai kunci untuk bisa melakukan proses dekripsi. Penerima harus menginputkan 6 digit angka dengan benar sebelum bisa melakukan proses dekripsi. Untuk mengamankan dari penysup, maka nantinya proses untuk mencoba proses dekripsi hanya diijinkan 3 kali. Selain itu proses penginputan kunci sepanjang 6 digit juga dibatasi oleh waktu yang ditentukan oleh pengirim. Dimana waktu maksimal yang diijinkan adalah 255 detik. Apabila lebih dari 3 kali atau waktu penginputan kunci yang dicobakan melebihi dari waktu yang ditentukan maka image sudah tidak dapat dibuka lagi untuk dilakukan proses dekripsi. Sehingga apabila menginginkan informasi kembali harus meminta pengirim melakukan pengiriman kembali citra tersebut (Iswahyudi dkk, 2012).

Proses enkripsi yang digunakan adalah menggabungkan metode vigenere cipher dan playfair cipher selanjutnya kunci playfair yang digunakan untuk mengenkripsi citra disisipkan kedalam cipher image seperti terlihat pada Gambar 1 (Iswahyudi dkk, 2012)

Sedangkan proses dekripsi yang digunakan adalah dengan cara memasukkan pin yang digunakan untuk untuk mengestrak kunci nantinya digunakan untuk melakukan proses dekripsi, selanjutnya dilakukan proses dekripsi menggunakan algoritma playfair cipher yang dilanjutkan dengan algoritma vigenere cipher seperti terlihat pada Gambar 2 (Iswahyudi dkk, 2012).

Pengembangan dari metode *Vigenere Cipher* untuk penyandian citra dilakukan dengan menggunakan Formula *Vigenere Cipher* dengan menggunakan nilai basis modulo 256 sesuai dengan intensitas warna pada citra.

Rumus enkripsi yang digunakan untuk menghitung nilai cipher image tiap pixel adalah sebagai berikut:

$$E_{ki}(a) = (a + ki) mod\ 256 \quad \text{.....(1)}$$

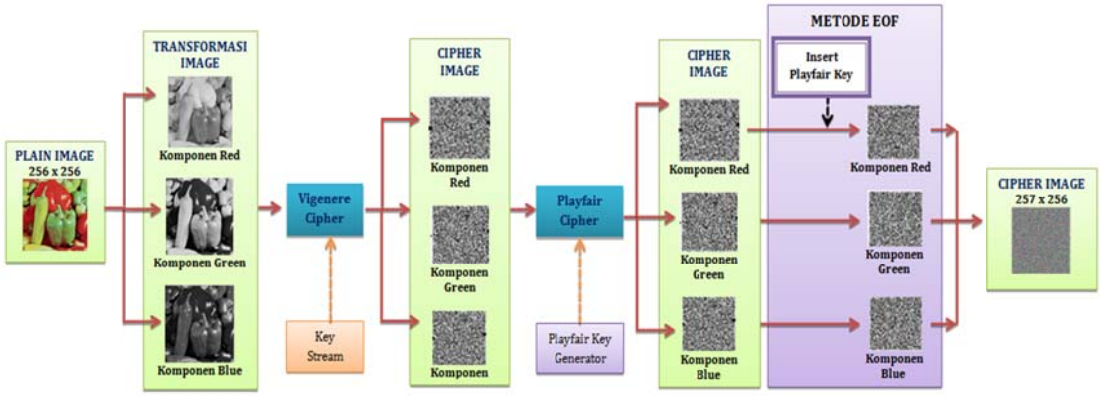
Dengan : a : Intensitas ke-i,j citra asli
Ki: kunci ke-i

Sedangkan rumus yang digunakan untuk mendapatkan kembali plainteks yang berupa image tiap pixel yang telah terenkripsi (dekripsi) adalah:

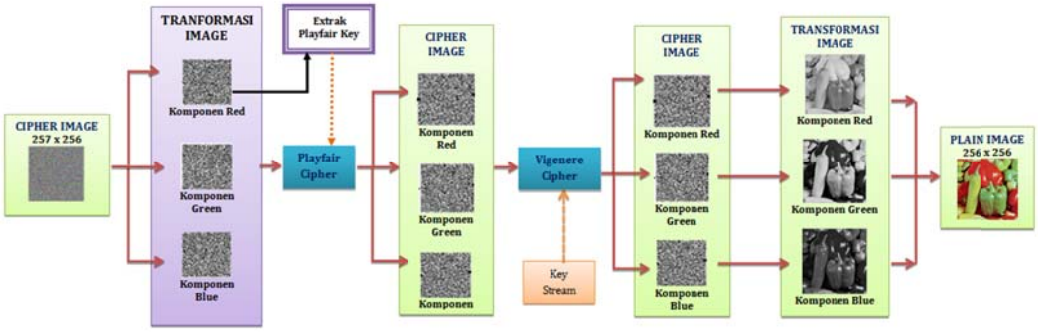
$$D_{ki}(a) = (a - ki) mod\ 256 \quad \text{..... (2)}$$

Dengan : a: Intensitas citra pixel ke-i,j yang terenkripsi, ki: kunci ke-i

.



Gambar 1. Skema Proses Enkripsi



Gambar 2. Skema Proses Dekripsi

Sedangkan algoritma enkripsi menggunakan metode *Playfair Cipher* yang dikembangkan untuk data citra adalah sebagai berikut : 1) membentuk matrik bujur sangkar yang akan menjadi kunci dengan jumlah disesuaikan dengan semesta pembicaraan yang digunakan sebagai dasar. Misalkan pada citra yang mempunyai derajad keabuan 256 maka kunci yang akan digunakan untuk menyandikan citra adalah matrik bujur sangkar dengan ukuran 16 x 16 dengan nilai elemennya adalah bilangan bulat acak antara 0 sampai dengan 255. 2) *Cipher*ing menggunakan setiap pasangan intensitas citra dalam plainteks untuk masing-masing kanal warna. Plainteks dibagi dalam blok-blok dimana setiap blok berisi 2 pixel (m1 dan m2) pada masing-masing baris untuk setiap kanal warna. 3) Proses *cipher*ing pada masng-masing kanal warna dilakukan dengan cara: a) jika m1 dan m2 terdapat pada baris yang sama dalam matrik kunci maka c1 diambil dari 1 pixel sebelah kanan m1, c2 diambil dari 1 pixel sebelah kanan m2 pada matrik kunci. b) jika m1 dan m2 terdapat pada kolom yang sama dalam matrik maka c1 dan c2 masing-masing diambil dari 1 pixel dibawah m1

dan m2 pada matrik kunci. c) jika m1 dan m2 berbeda baris dan kolom dalam matrik kunci maka c1 diambil dari pertemuan baris pixel m1 dan kolom m2, dan c2 diambil dari pertemuan baris m2 dan kolom m1 pada matrik kunci. d) Jika m1 = m2 maka cipherteks adalah c1=m1 dan c2=m2.

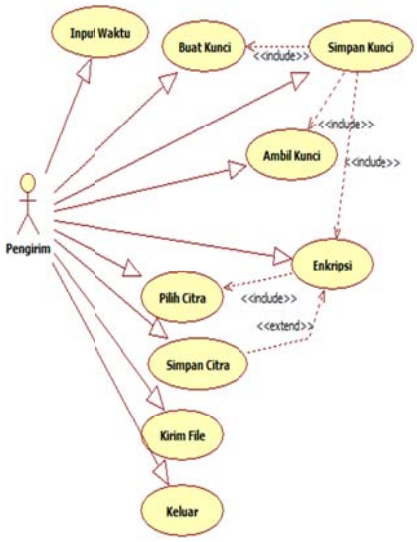
Sedangkan algoritma dekripsi untuk menggunakan metode *Playfair Cipher* adalah sebagai berikut : 1) Sama dengan proses enkripsi yaitu menggunakan matrik kunci yang sama untuk proses enkripsi. 2) Proses *cipher*ing dilakukan dengan cara : a) jika c1 dan c2 terdapat pada baris yang sama dalam matrik kunci maka m1 diambil dari 1 pixel sebelah kiri c1, m2 diambil dari 1 pixel sebelah kiri c2 pada matrik kunci. b) jika c1 dan c2 terdapat pada kolom yang sama dalam matrik maka m1 dan m2 masing-masing diambil dari 1 pixel diatas m1 dan m2 pada matrik kunci. c) jika c1 dan c2 berbeda baris dan kolom dalam matrik kunci maka m1 diambil dari pertemuan baris c1 dan kolom c2, dan m2 diambil dari pertemuan baris c2 dan kolom c1 pada matrik kunci. d) jika c1 = c2 maka plainteks adalah adalah m1=c1 dan m2=c2.

Untuk menyembunyikan kunci digunakan teknik EOF atau End Of File yang merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut. Dalam teknik ini, data disisipkan pada akhir file dengan diberi tanda khusus sebagai pengenal start dari data tersebut dan pengenal akhir dari data tersebut. Dengan demikian ukuran file setelah disisipkan pesan rahasia akan bertambah. Sebab, ukuran file yang telah disisipkan pesan rahasia sama dengan ukuran file sebelum disisipkan pesan rahasia ditambah dengan ukuran pesan rahasia yang disisipkan. Contoh hasil penyisipan pesan rahasia dengan menggunakan metode End of File.

Untuk menggambarkan kebutuhan sistem sebelum diimplementasikan pada piranti bergerak (handphone) ataupun smart phone menggunakan bahasa pemrograman Android dilakukan proses perancangan sistem. Dalam perancangan sistem ini menggunakan tool UML (Unified Modelling Language), yang mencakup perancangan use case diagram, sequence diagram, class diagram, dan activity diagram.

Use Case enkripsi mempunyai langkah – langkah: 1) Pengirim dapat memilih untuk membuat kunci baru atau memanggil kunci yang telah tersimpan dengan memilih *Buat Kunci* atau *Panggil Kunci*. 2) Pemngirim dapat memilih untuk menyimpan kunci enkripsi dengan memilih *Simpan Kunci*. 3) Pengirim diharuskan memilih citra yang akan dienkripsi dengan memilih *Pilih Citra*. 4) Pengirim dapat memulai melakukan proses enkripsi dengan memilih *Enkripsi Citra*. 5) Pengirim dapat mengirimkan file hasil enkripsi dengan memilih *Kirim MMS*. 6) Pengirim dapat keluar dari program dengan memilih *keluar*.

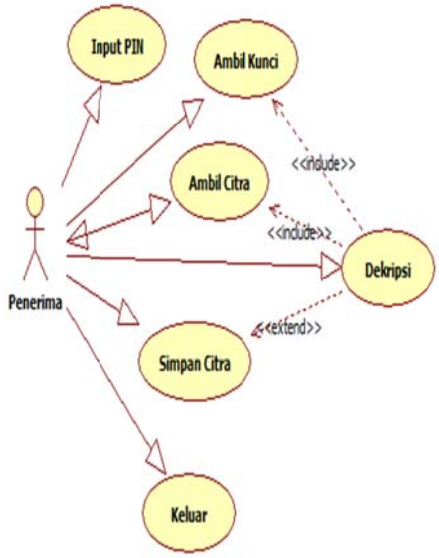
Gambar 3 menggambarkan use case diagram enkripsi. Pengirim dapat melakukan enkripsi mulai dari membuat atau memilih kunci enkripsi, melakukan proses enkripsi hingga mengirimkan citra hasil enkripsi melalui fasilitas pengiriman MMS.



Gambar 3. Use case diagram proses enkripsi

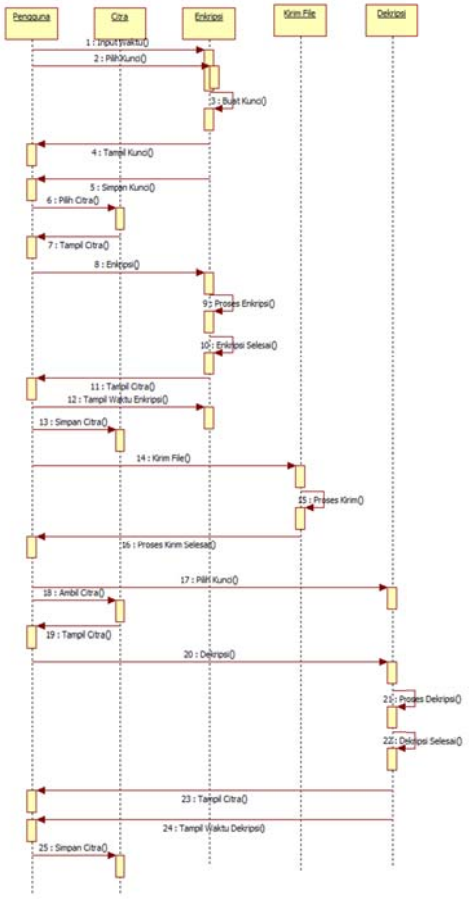
Use Case dekripsi mempunyai langkah – langkah: 1) Penerima harus memilih kunci untuk memulai proses dekripsi dengan memilih *Pilih Kunci*. 2) Penerima diharuskan memilih citra yang akan di-dekripsi dengan memilih *Pilih Citra*. 3) Penerima dapat memulai melakukan proses dekripsi dengan memilih *Dekripsi.* 4) Penerima dapat memilih untuk menyimpan citra hasil dekripsi dengan memilih *Simpan Citra*. 5) Penerima dapat keluar dari program dengan memilih *keluar*.

Gambar 4 menggambarkan use case diagram proses dekripsi. Penerima yang telah menerima kiriman citra terenkripsi dapat melakukan proses dekripsi dengan memilih kunci enkripsi. Selanjutnya mengambil citra dan secara otomatis sistem akan melakukan proses dekripsi. Kemudian, penerima dapat menyimpan citra yang telah didekripsi.



Gambar 4. Use case diagram proses dekripsi

Dalam aplikasi ini terdapat kelas-kelas yang saling berkomunikasi dalam penggunaannya. Komunikasi antar kelas tersebut dimodelkan oleh diagram runtun keseluruhan program. Gambar 5 merupakan diagram runtun keseluruhan program, yang meliputi enkripsi, dekripsi, dan pengiriman citra yang dilakukan oleh obyek Citra, Enkripsi, Dekripsi, dan Kirim file. Obyek Citra akan menangani pemilihan citra dan mengirimkan citra tersebut kepada enkripsi atau dekrisi. Untuk memulai proses enkripsi seorang pengguna harus memilih pilihan enkripsi dan membuat/memilih kunci, memilih citra hingga kemudian runtutan proses enkripsi dapat dimulai, proses dekripsi juga memiliki aturan yang sama.



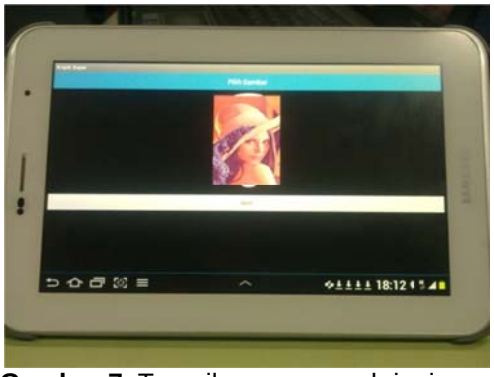
Gambar 5. Diagram runtun keseluruhan sistem

PEMBAHASAN

Pengujian keamanan kunci enkripsi dilakukan pada beberapa citra berwarna dengan ukuran 256 x 256 piksel dan 480 x 640 piksel dengan tipe BMP dan JPG. Pada pengujian aplikasi menggunakan smart phone dengan sistem operasi Android, aplikasi pengamanan data image dapat dilihat pada Gambar 6.

Gambar 6. Tampilan icon pada SAM-SUNG Galaxy Tab2

Proses enkripsi diawali dengan memilih citra yang akan dilakukan proses enkripsi seperti terlihat pada Gambar 7.

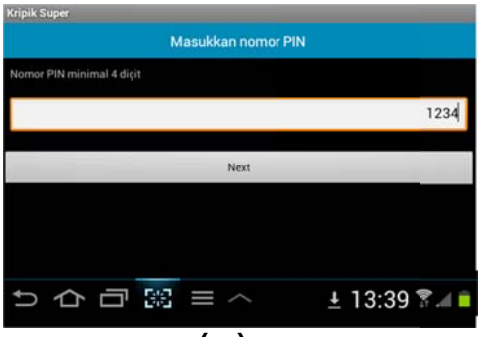


Gambar 7. Tampilan proses enkripsi pada smart phone

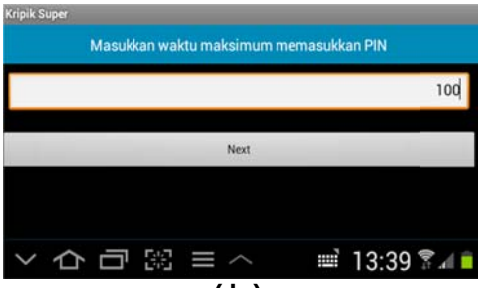
Selanjutnya diinputkan kunci sandi yang berupa bilangan antara 0-9 minimal 4 digit serta waktu proses yang diijinkan untuk melakukan proses dekripsi seperti terlihat pada gambar 8a dan 8b.

Proses dekripsi dilakukan proses yang sama, yaitu dengan memilih cipher image yang akan dilakukan proses dekripsi. selanjutnya diinputkan kunci sandi yang terdiri dari 6 digit. Apabila kunci sesuai dengan kunci yang digunakan untuk enkripsi maka proses dekripsi dapat dilanjutkan sehingga akan tampil waktu proses dekripsi dan citra hasil dekripsi yang sama dengan citra asli.

Hasil pengujian proses enkripsi serta waktu proses enkripsi ditampilkan pada Gambar 9.

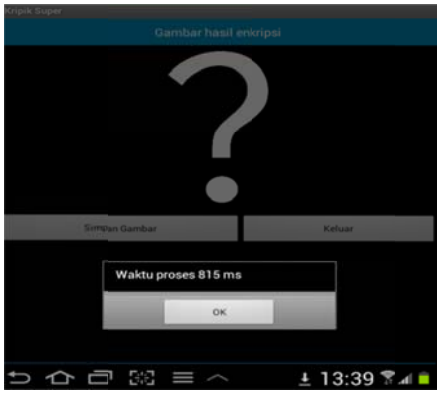


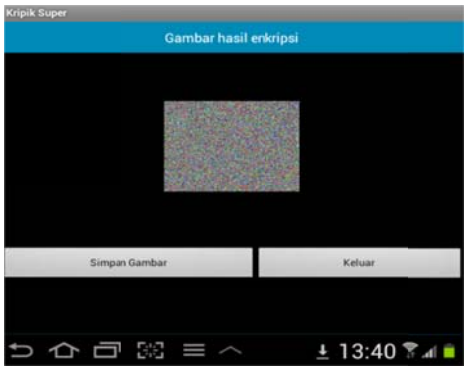
(a)



(b)

Gambar 8a. Tampilan untuk menginput-kan kunci dan 8b. Tampilan untuk menginputkan batas waktu proses untuk menginputkan kunci yang valid

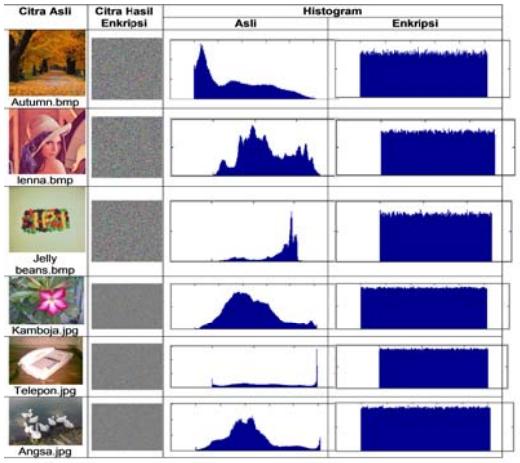




Gambar 9. Tampilan hasil enkripsi dan waktu proses enkripsi pada smart phone

Hasil analisis histogram warna diperlihatkan pada Tabel 1.

Tabel 1. Analisis histogram warna



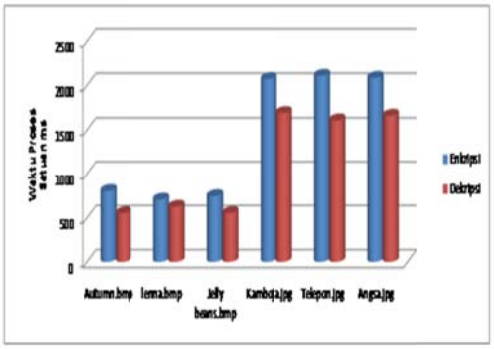
Apabila dilihat secara visual dari histogram plain image dengan histogram dari cipher image-nya, maka terlihat perbedaan yang signifikan antara keduanya. Pada historam hasil enkripsi terlihat rata untuk setiap intensitas warna, hal ini menunjukkan bahwa algoritma enkripsi yang digunakan tidak dapat memberikan petunjuk apa-apa untuk dilakukan statistical attack oleh kriptanalis karena tidak ada intensitas yang menonjol seperti yang terlihat pada citra asli. Dari Tabel 1 juga terlihat bahwa citra asli tidak dapat terlihat setelah dilakukan proses enkripsi. Hasil penyandian citra menunjukkan keteracakan warna dan perubahan intensitas warna yang cukup signifikan, hal ini menunjukkan bahwa proses enkripsi berhasil dengan baik.

Analisis waktu proses enkripsi dan dekripsi hasil pengujian disajikan pada tabel 2. Rata-rata waktu enkripsi untuk 3 buah gambar uji dengan ukuran 256 x 256 sebesar 754 miliseconds (0,75 detik) dan rata-rata waktu dekripsi sebesar 579 (0,58 detik). Sedangkan rata-rata waktu enkripsi untuk 3 buah gambar uji dengan ukuran 480 x 640 sebesar 2091 miliseconds (2,09 detik) dan rata-rata waktu dekripsi sebesar 1657 (1,66 detik). Dari hasil tersebut dapat dinyatakan bahwa algoritma ini cukup efektif untuk penyandian data citra warna dan dapat diimplementasikan pada telepon seluler dengan sistem operasi Android karena tidak membutuhkan waktu proses yang lama.

Tabel 2. Analisis waktu pada pengujian di ponsel

No.	Nama File	Size		Waktu Proses (ms)	
		Plain	Cipher	Enkripsi	Dekripsi
1	Autumn.bmp	256 x 256	257 x 256	807	554
2	lenna.bmp	256 x 256	257 x 256	708	627
3	Jelly beans.bmp	256 x 256	257 x 256	747	555
Rata-rata				**754**	**579**
1	Kamboja.jpg	480 x 640	481 x 640	2075	1695
2	Telepon.jpg	480 x 640	481 x 640	2111	1612
3	Angsa.jpg	480 x 640	481 x 640	2087	1665
Rata-rata				**2091**	**1657**

Grafik perbandingan waktu enkripsi dan dekripsi diperlihatkan oleh Gambar 9.



Gambar 9. Grafik perbandingan waktu enkripsi dan dekripsi

KESIMPULAN

Berdasarkan hasil penelitian dapat diambil beberapa kesimpulan antara lain: 1) Algoritma enkripsi citra yang diusulkan dapat diimplementasikan pada telepon seluler yang hemat sumberdaya komputasi serta proses yang cepat. Hal tersebut dibuktikan dengan rata-rata waktu enkripsi untuk citra dengan ukuran 256 x 256 sebesar

0,75 detik, dan rata-rata waktu dekripsi sebesar 0,58 detik, sedangkan citra dengan ukuran 480 x 640 rata-rata waktu enkripsi 2,09 detik dan rata-rata waktu dekripsi sebesar 1,66 detik. 2) Hasil pengujian pengamanan kunci algoritma super enkripsi dengan teknik penyisipan kunci menggunakan metode end-of-file menunjukkan secara visual citra hasil enkripsi tidak terlihat lagi disebabkan oleh keteracakan warna dan perubahan intensitas warna yang cukup signifikan. Dari histogram plain image dan cipher image-nya terlihat perbedaan yang signifikan antara keduanya. Ukuran citra juga tidak mengalami perubahan yang signifikan, sehingga tidak menimbulkan kecurigaan bagi yang melihatnya. 3) Metode EOF mempunyai kelebihan mampu menyisipkan kunci yang sangat besar, sehingga cocok untuk menyisipkan kunci playfair yang berukuran cukup panjang.

UCAPAN TERIMA KASIH

Ucapan terima kasih kami sampaikan kepada Direktorat Jenderal Pendidikan Tinggi, Kementrian Pendidikan Nasional yang telah mendanai kegiatan penelitian ini sesuai dengan Surat Perjanjian Penugasan Penelitian Nomor: 560.14/K5/KL/ 2012, Tanggal 10 Februari 2012, melalui dana Penelitian Hibah Bersaing.

DAFTAR PUSTAKA

Abrihama, D. (2008). *Keystream Vigenere Cipher : Modifikasi Vigenere Cipher dengan Pendekatan Keystream Generator*. Program Studi Informatika ITB. Bandung.

Anneria, Y.S, (2008). *Program Stegonalis Metode LSB pada Citra dengan Enhanced LSB, Uji Chi-Square, dan RS-Analysis*. Tugas Akhir. Program Studi Teknik Informatika ITB, Bandung.

Iswahyudi, C. Setyaningsih, E. Widyastuti, N. (2012). "Pengamanan Kunci Enkripsi Citra pada Algoritma Super Enkripsi Menggunakan Metode End of File". *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) Periode III. ISSN: 1979-911X.*

Fridrich. J., dan Goljan. M. (2002). *Practical Steganalysis of Digital Images*. State of The Art, Department of Electrical Engineering. Binghamton.

Gupta K, Silakari S. (2009). "Choase Based Image Encryption Using Block-Based Transformation Algorithm". *International Journal of Computer and Network Security. 1(3).*

Jolfaei A, Mirghadri A. (2011). "Image Encryption Using Chaos and Block Cipher". *Computer and Information Science. 4(1).*

Krikor L, Baba S, Arif T, Shaaban Z. (2009). "Image Encryption Using DCT and Stream Cipher". *European Journal of Scientific Research.* http://www.eurojournals.com/ejsr.htm. ISSN 1450-216X ; 32(1): 47-57.

Manglem, Kh. S., Birendra, S. S., Shyam, L. S. S. (2007). *Hiding Encrypted Message in Features Image*. IJCSNS. Vol. 7 No. 4. India.

Puech, W. dan Rodrigues, J. (2005), *Crypto-compression of Medical Images by Aelective Encryption of DCT*. 13th European Signal Processing Conference. Turkey.

Setyaningsih E, Iswahyudi C, Widyastuti N. (2012). "Image Encryption on Mobile Phone Using Super Encryption Algorithm". *Jurnal Ilmiah Nasional Terakreditasi TELKOMNIKA.* ISSN : 1693-6930. 10(4): 599-608.

Stinson R Douglas. (1005). *Cryptography Theory and Practice*. London: CRC Press. Inc.

Younes, M A B , Jantan A. (2008). "Image Encryption Using Block-Based Transformation Algorithm" . *IAENG International Journal of Computer Science*. *35(1).*