Jurnal Elektronik Ilmu Komputer Udayana p-ISSN: 2301-5373
Volume 7, No 3. Februari 2019 e-ISSN: 2654-5101

Proteksi Aplikasi Pesan SMS Berbasis Mobile Android Dengan Algoritma AES 256 dan Steganografi LSB

Aan Masduki[1], I Ketut Gde Suhartana[2]
Program Studi Teknik Informatika, Jurusan Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jimbaran – Bali, Indonesia
[1]aan.masduki@gmail.com
[2]ikg.suhartana@gmail.com

Abstraksi

Perkembangan teknologi dalam beberapa tahun terakhir sangat cepat dan pesat, salah satunya adalah perkembangan smartphone. Dengan banyak nya fitur-fitur yang disediakan smartphone saat ini menjadikan hidup lebih mudah. Salah satu aplikasi dalam smartphone yang mempermudah hidup kita adalah kita sekarang tidak perlu pergi jauh-jauh lagi untuk berkomunikasi antar sesama teman atau keluarga.

Salah satu aplikasi untuk berkomunikasi adalah menggunakan aplikasi pesan atau SMS. Seiring dengan perkembangan tersebut, tingkat keamanan atau kerahasiaan data juga semakin lemah karena orang sekarang semakin pintar. Orang dapat dengan mudah melakukan pencurian data, mengubah bahkan mengganti informasi data yang disampaikan.Untuk itu diperlukan teknik untuk menyembunyikan data, dengan harapan agar data yang sifatnya rahasia tidak diketahui oleh orang yang tidak berkepentingan.

Salah satu cara untuk mengamankan pesan yang dikirim dan mencegah agar pesan kita tetap aman adalah menggunakan ilmu kriptografi atau penyandian dan steganografi. Algoritma AES merupakan salah satu ilmu kriptografi yang penulis gunakan untuk proses enkripsi dan dekripsi. Setelah pesan dienkripsi, hasil chipertext akan disisipkan kedalam gambar menggunakan salah satu metode steganografi yaitu steganografi LSB. Diharapkan dengan menggunakan kedua algortima dapat mengamankan pesan yang dikirim sehingga pesan dapat sampai tujuan dengan aman.

Keywords: *Algoritma AES, Steganografi LSB, uji recovery , uji ketahanan.*

1. Pendahuluan

Perkembangan teknologi dalam beberapa tahun terakhir sangat cepat dan pesat, salah satunya adalah perkembangan smartphone. Perkembangan smartphone diimbangi dengan perkembangan sistem operasi yang lengkap layaknya komputer seperti sistem android [1].

Salah satu fasilitas yang disediakan smartphone berbasis android untuk melakukan proses komunikasi pengiriman pesan singkat adalah dengan menggunakan aplikasi Short Message Service (SMS). Namun dengan fasilitas SMS yang ada, dalam proses pengiriman pesan terkadang ada pihak yang berbuat nakal seperti menyadap informasi pesan yang dikirimkan, melihat ataupun mengubah pesan ditengah pengiriman, sehingga pesan bisa jadi saat diterima di penerima pesan isinya berubah, tidak sesuai dengan yang dikirimkan.

Untuk mencegah kejadian yang tidak diinginkan tersebut dibutuhkan sebuah sistem keamanan pada layanan SMS. Terdapat beberapa cara untuk mengamankan pesan agar isi pesan hanya bisa dibaca maknanya oleh pengirim dan penerima salah satunya yaitu dengan ilmu kriptografi dan steganografi.

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan [2]. Dalam kriptografi terdapat proses enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awal-nya dengan menggunakan algoritma tertentu yang disebut

ciphertext [3].Proses enkripsi membuat pesan yang tersamarkan isinya namun masih berbentuk tulisan oleh karena itu walau pesan itu telah di enkripsi tetap akan menimbulkan kecurigaan sehingga dapat memicu orang yang ingin tau makna pesan untuk mencari makna sebenarnya dari pesan tersebut. Oleh karena itu penulis menggunakan steganografi LSB untuk menutupi kelemahan tersebut. Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia [4]. Diharapkan,dengan dua metode ini komunikasi melalui aplikasi pesan SMS dapat lebih aman.

2. Metode Penelitian

2.1. Analisis Kebutuhan

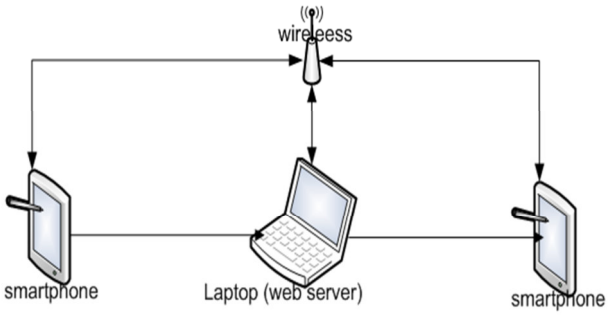
a. Kebutuhan masukan
   1. Pesan dan kunci yang dienkripsi berupa huruf alfabet dan angka.
   2. Kunci digunakan untuk enkripsi dan dekripsi file pesan rahasia.
   3. File chiperteks hasil enkripsi disisipkan ke dalam gambar.
   4. Media yang digunakan dalam penyisipan adalah citra gambar bitmap (.bmp) .
   5. File bmp digunakan untuk pengujian hasil stegoimagenya.
   6. File stegoimage berisi pesan rahasia hasil ekstraksi.

b. Kebutuhan keluaran
   1. File gambar bertipe bitmap (.bmp) .
   2. Chipertext hasil enkripsi yang berada di dalam gambar.
   3. Pesan asli atau plaintext yang dihasilkan dari proses dekripsi pesan yang ada di dalam gambar yang sebelumnya sudah diestrak.

c. Kebutuhan proses
   1. Saat pesan dikirim akan disandikan menggunakan algoritma AES.
   2. Pada sisi pengirim pesan teks dienkripsi untuk mendapatkan *ciphertext* kemudian *ciphertext* tersebut disisipkan ke dalam citra gambar yang diambil secara langsung dan berformat BMP dengan metode *Least Significant Bit* (LSB).
   3. Pada sisi penerima citra gambar hasil enkripsi dan penyisipan diekstrak dan hasilnya didekripsikan untuk mendapatkan *plaintext* atau pesan asli.

2.2. Desain Sistem

Pertama pengirim dan pengguna harus saling terkoneksi dengan jaringan yang sama. Setelah terkoneksi pengirim akan melakukan request ke webserver. Selanjutnya webserver akan memproses request dari pengirim dan mengirimkan jawaban ke pengirim. Setelah terhubung maka pengguna dapat melakukan pengiriman dan penerimaan pesan dari dan ke pengguna lain. Saat proses pengiriman pesan, idpenerima dan pesan yang disandikan akan dikirim. Pesan yang dikirim akan masuk ke webserver, kemudian disimpan ke webbase dan di Forward ke penerima. Penerima yang telah terhubung ke webserver dapat mengakses dan mengupdate pesan yang diterima.

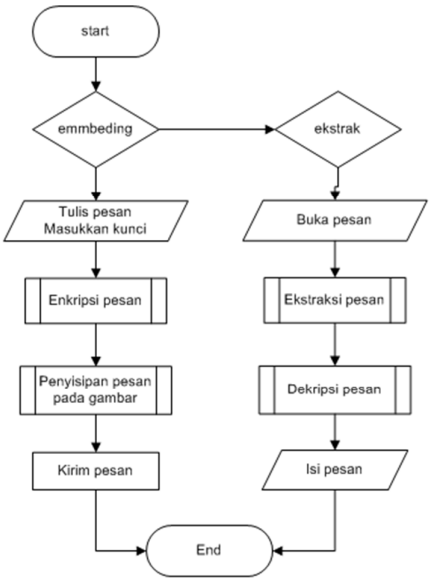


Gambar 1 Desain sistem pengiriman pesan sms menggunakan webserver

Pesan yang dikirim akan dienkripsi terlebih dahulu. Setelah terenkripsi kemudian disisipkan pada gambar untuk menyembunyikan pesan dan kemudian dikirimkan. Untuk proses dekripsi,

p-ISSN: 2301-5373
e-ISSN: 2654-5101

penerima akan menerima pesan dalam bentuk stegoimage yang perlu terlebih dahulu diekstraksi dan didekripsi untuk melihat isi pesan.

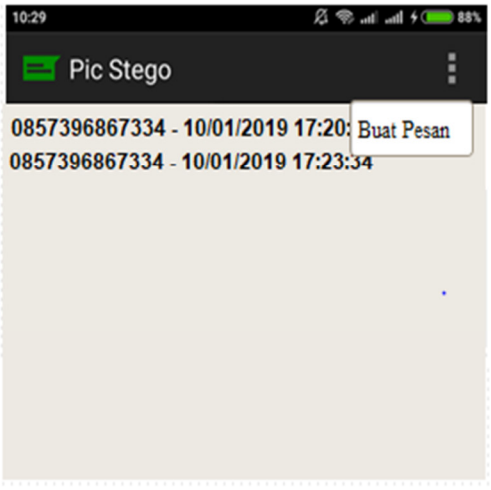


Gambar 2 Flowchart utama sistem

Flowchart diatas menggambarkan main sistem dari program yang dibuat dimana terdapat dua proses yaitu proses pengiriman dan proses penerimaan pesan. Proses pengiriman pesan, dimulai dengan menulis pesan dan password untuk enkripsi kemudian sistem akan melakukan proses enkripsi. Hasil enkripsi yang berupa chipertekt akan disisipkan pada gambar yang diambil secara langsung melalui smartphone. Sistem akan melakukan proses penyisipan setelah pengambilan gambar kemudian dikirim ke nomor penerima pesan dalam bentuk gambar yang sudah disisipi pesan. Untuk penerima, apabila ingin membuka pesan maka gambar yang diterima terlebih dahulu di ekstraksi dan didekripsi sehingga pesan yang disisipkan dke dalam gambar dapat dibaca.

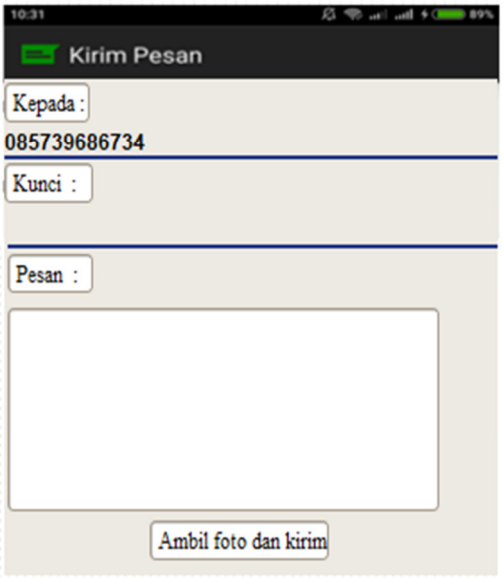
3. Hasil dan Pembahasan

3.1. Tampilan Program Aplikasi SMS



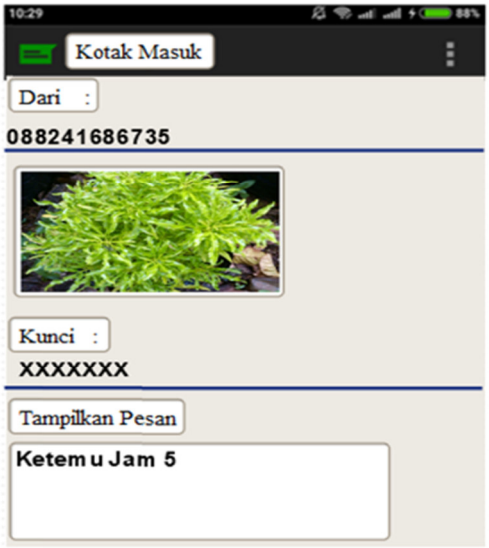
Gambar 3 Tampilan antarmuka pesan (kotak masuk)

Gambar 3 merupakan tampilan antarmuka pesan sms dimana berisi tampilan pesan masuk seperti aplikasi sms yang brada di smartphone. Pada tampilan antarmuka pesan terdapat tombol buat pesan baru dimana berada di kanan atas tampilan antarmuka. Untuk pesan masuk berisi nomor pengirim, tanggal, bulan, tahun dan jam pesan dikirim.



Gambar 4 Tampilan antarmuka kirim pesan

Gambar 4 merupakan tampilan antarmuka kirim pesan dimana terdapat beberapa kolom diantaranya kolom kepada yang digunakan untuk menulis nomor tujuan pesan, kolom kunci yang digunakan untuk mengisi password proses enkripsi, kolom pesan untuk menulis pesan yang akan dikirim ke penerima pesan. Pada menu pesan baru terdapat button ambil gambar dan kirim dimana pada tombol ini akan dilakukan proses enkripsi dan pengambilan gambar secara langsung untuk disisipi pesan yang telah terenkrisi yang kemudian akan langsung dikirimkan ke penerima pesan.



Gambar 5 Tampilan pesan masuk

Gambar 5 merupakan tampilan antarmuka pesan masuk dimana didalamnya terdapat nomor si pengirim pesan, gambar.bmp, kunci pesan dan tombol tampilkan pesan. Untuk menampilkan pesan teks harus memasukkan kunci terlebih dahulu untuk mengekstrak dan

p-ISSN: 2301-5373
e-ISSN: 2654-5101

mendekripsi isi pesan yang terdapat pada gambar. Kemudian tekan tombol tampilkan pesan untuk pross ekstraksi dan proses dekripsi sehingga pesan teks yang trsembunyi dapat dibaca.

3.2. Hasil Pengujian

a. Hasil Penyisipan

Gambar 6 Photo sebelum proses penyisipan

Gambar 7 Photo setelah penyisipan

Gambar 6 merupakan photo sebelum proses penyisipan dimana photo diambil langsung menggunakan kamera smartphone saat proses pengiriman. Gambar 7 merupakan photo yang sudah disisipi pesan hasil enkripsi. Dari kedua photo dapat dilihat bahwa tidak ada perbedaan sama sekali pada gambar sebelum dan setelah pesan disisipkan. Gambar tetap sama layaknya tidak ada penyisipan pesan sama sekali. Begitu pula ukuran dan resolusi photo setelah dan sebelum disisipi pesan juga tetap sama.

Tabel 1 hasil penyisipan

No	Nama foto	Ukuran
1	Bunga.bmp	11,2 kb
2	Bunga1.bmp	11,5 kb
3	kaktus.bmp	14,2 kb
4	kaktus1.bmp	15,1 kb
5	mawar.bmp	18, 6 kb
6	mawar1.bmp	19.9 kb
7	brokoli.bmp	25,8 kb
8	brokoli1.bmp	27,1 kb
9	rombusa.bmp	35,1 kb
10	rombusa1.bmp	38,8 kb

b. Pengujian Recovery

pengujian recovery diperlukan untuk membuktikan apakah pesan yang telah tersandikan dan tersisipkan deengan metode algoritma AES dan steganografi LSB bisa kembali utuh pesannya tanpa ada yang rusak.

Tabel 2 Pengujian Recovery

No	Jumlah karakter sisip	Jumlah pngujian	Hasil sha-1 gambar sisip sebelum dan sesudah steganografi	isi pesan
1	20	10	hasil sha antara kedua gambar sama	20
2	40	10	hasil sha antara kedua gambar sama	40
3	60	10	hasil sha antara kedua gambar sama	60
4	80	10	hasil sha antara kedua gambar sama	80
5	100	10	hasil sha antara kedua gambar sama	100

Pada hasil uji Recovery yang ditunjukan pada Tabel 2 dapat dilihat bahwa sistem mampu menyisipkan dan mengekstrak kembali informasi yang sama pada citra yang digunakan dengan menggunakan panjang pesan yang bervariasi. Pengujian dilakukan secara berulang sebanyak 10 kali pada tiap citra uji. Dengan kata lain pesan yang dienkripsi dan disisipkan ke dalam gambar dapat diekstraksi dan didekripsi dengan sempurna sehingga aplikasi yang dibuat dapat berjalan dengan benar. Selain itu gambar hasil asli dan gambar hasil penyisipan terlihat sama jelas sehingga tidak terasa disisipi pesan sama sekali dan juga ukuran gambar asli dan disisipi sama besar.

c. Pengujian Ketahanan

Terdapat 3 pengujian Uji ketahanan yang diujikan pada sistem antara lain rotate gambar, resize gambar, dan penambahan brightness dan contrast pada gambar yang berformat bmp.

1. Rotasi

Tabel 3 Pengujian rotasi

No	Jumlah karakter sisip	Jumlah Pengujian	Hasil deskripsi isi pesan stelah mengalami rotasi
1	20	10	Pesan rusak/tidak terbaca
2	40	10	Pesan rusak/tidak terbaca
3	60	10	Pesan rusak/tidak terbaca
4	80	10	Pesan rusak/tidak terbaca
5	100	10	Pesan rusak/tidak terbaca

2. Resize

Tabel 4 Pengujian resize

No	Jumlah karakter sisip	Jumlah Pengujian	Hasil deskripsi isi pesan stelah mengalami resize
1	20	10	Pesan rusak/tidak terbaca
2	40	10	Pesan rusak/tidak terbaca
3	60	10	Pesan rusak/tidak terbaca
4	80	10	Pesan rusak/tidak terbaca
5	100	10	Pesan rusak/tidak terbaca

p-ISSN: 2301-5373
e-ISSN: 2654-5101

3. Brightness dan contrast

Tabel 5 Pengujian brightness dan contrast

No	Jumlah karakter sisip	Jumlah Pengujian	Hasil deskripsi isi pesan stelah mengalami penambahan brightness dan contrast
1	20	10	Pesan rusak/tidak terbaca
2	40	10	Pesan rusak/tidak terbaca
3	60	10	Pesan rusak/tidak terbaca
4	80	10	Pesan rusak/tidak terbaca
5	100	10	Pesan rusak/tidak terbaca

Dari ketiga pengujian ketahanan yang dilakukan pada sistem, semua nya mengalami kegagalan setelah dilakukan proses ekstraksi dan dekripsi. Sistem tidak mampu menjaga keutuhan pesan ketika diberikan serangan rotasi, resize, dan penambahan brightness dan contrast. Saat proses dekripsi pesan rusak atau tidak terbaca sama sekali. Dapat dikatakan bahwa sistem sangat rentan terhadap serangan yang ditujukan pada gambar karena setelah diberikan serangan data yang disisipkan berubah hampir secara menyeluruh sehingga informasi awal yang disisipkan menjadi hilang atau tidak utuh seperti sedia kala.

4. Kesimpulan

Aplikasi dapat berjalan dengan lancar dan dapat mengembalikan pesan seperti sedia kala sehingga proses komunikasi menggunakan aplikasi sms sedikit lebih aman. Pada proses penyembunyian dengan metode steganografi LSB terlihat pada gambar tidak ada pesan yang tersisipkan sama sekali karena gambar yang disisipi pesan enkripsi tidak berubah sama sekali.

Namun terdapat kelemahan pada program yang dibuat. Dimana disini kelemahan program yang dibuat adalah sangat rentan terhadap serangan yang ditujukan secara langsung ke pada objek gambar yang disisipi seperti merotasi gambar, meresize dan menambah kan brightness dan contras. Dengan sedikit perubahan pada gambar maka pesan yang disisipkan akan rusak dan tidak bisa terbaca. Sehingga diperlukan metode yang lebih baru agar bisa lebih aman lagi.

References

[1] D. M. Fajar," Aplikasi Data Keamanan SMS Menggunakan Metode Enkripsi Berbasis Android" LPT Y .A.I, 2014.

[2] F.N. Pabokory, I. F. Astuti and A.H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard " *Jurnal Informatika Mulawarman,* Vol. 10, no. 1, Februari 2015.

[3] I.A. Ilyas and S.Widodo, "Kriptografi File Menggunakan Metode Aes Dual Password" *Prosiding Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2014),* Depok, 2014, Vol. 8. Page 263.`

[4] M. Tezar, R. Magdalena and N. Andini, "Implementasi Dan Analisis Keamanan Pesan Menggunakan Teknik Steganografi Lsb Dan Algoritma Kriptografi Relative Displacement Cipher" *e-Proceding of Engineering,* Bandung, 2015, Vol. 2, no. 3, Page 7190.