Versi Online: https://journal.ubm.ac.id/index.php/alu
Jurnal ALU

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 2) : 61 - 67. Th. 2018
p-ISSN: 2620-620X
e-ISSN: 2621-9840

PENGAMANAN DATA MELALUI *CLOUD COMPUTING* DENGAN INTEGRASI STEGANOGRAFI LSB DAN KRIPTOGRAFI VIGENERE KEY BERBASIS ANDROID

Data Safety Through Cloud Computing With Integration Of Android-Based LSB Steganography And Cryptography Of Vigenere Key

Chyquitha Danuputri, M.Kom, chyquitha@gmail.com [1)]
[1)]Teknik Informatika / Fakultas Teknologi dan Desain, Universitas Bunda Mulia

ABSTRACT

*Data exchange today is mostly done using cloud computing systems. There are still many message delivery service features that do not have good security standards, because the implementation of the service provider as the service provider of these features can still find out the contents of the message sent by the customer. In this research using Cryptographic Key Vigenere method and LSB Steganography which are integrated into one in a data security system. With these techniques put together into a system that helps the user in terms of exchanging confidential data through online share media without being known of their existence by irresponsible parties. The cover object used in this research is a digital image with * .gif, * .jpeg, * .png and * .bmp types of images. Data that can be inserted into the cover image is in the form of plaintext and document files format * .txt, * .doc, * .xls, * .pdf. This research produces stego image quality that does not look different from the original image visible and requires an encryption key to store into the cover image and decryption to open data from the stego image. This system prototype generates the process of exchanging confidential data through online share media, especially Android smartphone is more secure because the unauthorized party of confidential data will not know that the message contains confidential data.*

***Keywords**: Android, Kriptografi, Steganografi, LSB-Insertion, Enkripsi, Cloud Computing*

ABSTRAK

Pertukaran data pada jaman sekarang sudah banyak dilakukukan dengan menggunakan sistem *cloud computing*. Saat ini masih banyak fitur layanan penyampaian pesan belum memiliki standar keamanan yang baik, karena pada implementasinya pihak operator *provider* selaku penyedia layanan fitur-fitur ini masih dapat mengetahui isi pesan yang dikirimkan oleh pelanggan. Pada penelitian ini menggunakan metode *Vigenere Key* Kriptografi dan LSB Steganografi yang diintegrasikan menjadi satu dalam sebuah sistem pengamanan data. Dengan teknik-teknik tersebut disatukan menjadi suatu sistem yang membantu user dalam hal petukaran data rahasia melalui media *share online* tanpa diketahui keberadaannya oleh pihak yang tidak bertanggung jawab. *Cover object* yang digunakan di penilitian ini adalah *image digital* dengan jenis gambar *.gif, *.jpeg, *.png dan *.bmp. Data yang dapat disisipkan ke dalam *cover image* adalah berupa *plaintext* dan *file* dokumen yang berformat *.txt, *.doc, *.xls, *.pdf. Penelitian ini menghasilkan kualitas hasil gambar stego yang tidak terlihat perbedaannya dengan gambar aslinya terlihat kasat mata dan dibutuhkan kunci enkripsi untuk menyimpan ke dalam *cover image* dan dekripsi untuk membuka data dari *stego image*. Prototipe sistem ini menghasilkan proses pertukaran data rahasia melalui media *online share smartphone* khususnya android lebih terjamin karena pihak yang tidak berwenang atas data rahasia tersebut tidak akan mengetahui bahwa pesan tersebut mengandung data rahasia.

Kata kunci: *Android, Kriptografi, Steganografi, LSB-Insertion, Enkripsi, Cloud Computing*

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 2) : 61 - 67. Th. 2018
p-ISSN: 2620-620X
e-ISSN: 2621-9840

PENDAHULUAN

Perkembangan teknologi informasi sudah semakin pesat termasuk yang menggunakan sistem *cloud computing*. Dalam hal pertukaran data informasi tentunya pada jaman sekarang sudah menggunakan sistem *cloud computing* ini untuk menghemat biaya.

Android adalah salah satu sistem operasi berbasis linux untuk perangkat mobile. Banyak gadget media pertukaran data digital menggunakan sistem operasi *android* dengan memiliki berbagai fitur yang menarik.

Dengan segala kemudahan dalam pertukaran data digital *online* ini diperlukan metode untuk mengamankan bebarapa data informasi yang sifatnya rahasia yang akan dipertukarkan, terlebih tentang data rahasia negara karena jika pesan itu tersebar maka akan mengancam persatuan dan keamanan negara.

Berdasarkan latar belakang ini, maka pada penelitian ini dibuat sistem pengamanan pertukaran data dengan metode LSB Steganografi untuk penyisipan data ke dalam gambar digital yang diintegrasikan dengan metode *Vigenere key* Kriptografi.

Penelitian ini bertujuan untuk membuat suatu sistem keamanan dalam pertukaran data digital dalam *cloud computing* berbasis *android* agar kerahasiaan data dapat dilindungi dari pihak ketiga yang tidak berhak atas data tersebut.

METODE PENELITIAN

Penelitian ini bertujuan untuk mengembangkan teori dalam metode keamanan penyampaian informasi yang dilakukan melalui smartphone dan hasilnya dapat langsung diterapkan untuk memecahkan permasalahan-permasalahan yang dihadapi. Berdasarkan tujuan dan ruang lingkup penelitian yang telah dibahas sebelumnya, penelitian ini merupakan jenis penelitian murni dan penelitian terapan . Penelitian murni adalah penelitian yang diperuntukan bagi pengembangan ilmu pengetahuan, bertujuan untuk mengembangkan teori atau menemukan teori baru, sedagkan penelitian terapan adalah penelitian yang hasilnya dapat langsung diterapkan untuk memecahkan permasalahan-permasalahan yang dihadapi (Moedjiono 2012).

Penerapan konsep penelitian ini akan diimplementasikan pada sebuah aplikasi yang nantinya dikembangkan menggunakan metode pengembangan sistem model prototipe, analisis dan perancangan sistem dengan pendekatan berorientasi objek.

Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah:

1. Metode observasi

Observasi adalah kegiatan pengamatan yang direncanakan, sistematis dan hasilnya dicatat serta diinterpretasikan dalam rangka memperoleh pemahaman tentang objek yang diamati[Sugiyono 2012]. Observasi yang dilakukan adalah pengamatan terhadap system android, fitur-fitur android khususnya yang berfungsi untuk media penyampaian pesan, mencatat dan mengamati proses pengambilan *cover image,* menyisipkan file soal dan hasil *stego image* guna dilakukan analisis lebih lanjut Sumber Data.

2. Metode Studi Pustaka

Metode pengumpulan data yang diperoleh dengan mempelajari, meneliti, dan membaca buku, jurnal, skripsi, tesis baik hardcopy maupun softcopy yang terdapat di internet yang berhubungan dengan android, citra digital, steganografi, kompresi, hash.

Instrumentasi

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 2) : 61 - 67. Th. 2018
p-ISSN: 2620-620X
e-ISSN: 2621-9840

Instrumen yang digunakan untuk mendukung proses penelitan ini adalah sebagai berikut :

Teknik analisis yang diterapkankan dalam penelitian ini adalah analisis data kuantitatif dengan cara menganilisis proses penyisipan pesan atau file rahasia ke dalam citra yang akan menjadi *cover object* dan menganalisis perubahan perbedaan warna pada citra setelah dilakukan *LSB Steganography*.

Langkah-Langkah Penelitian

Penelitian ini melalui beberapa tahap langkah sehingga mencapai hasil yang diinginkan, dimana langkah-langkah penelitian ini adalah sebagai berikut :

Pemilihan Obyek

Memilih obyek sistem berdasarkan perkembangan zaman di dalam tekhnologi di bidang ilmu komputer yaitu dalam hal penelitian ini dipilih Kriptografi dan Steganografi.

Studi Pustaka

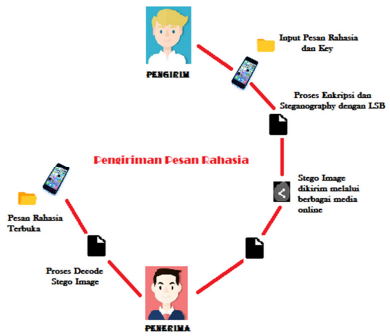
Melakukan penelitian terhadap kepustakaan tentang objek-objek penelitian yaitu teknik *LSB Steganography* dan *Vigenere Key Cryptography*. Bahan-bahan studi pustaka yang digunakan diperoleh dari publikasi *paper* local dan internasional, jurnal local dan internasional, tesis-tesis dan sumber-sumber lain dari internet.

Formulasi Hipotesis

Formulasi Hipotesis dalam penelitian ini adalah meningkatkan keamanan dalam pengiriman pesan rahasia dengan teknik *Vigenere Key Cryptography*, *LSB Steganography* dan *Stego Image* yang dihasilkan sulit diketahui keberadaan pesan rahasia. Metode ini diharapkan agar para pihak yang tidak bertanggung jawab tidak akan mudah membuka atau mengambil informasi rahasia dari atau yang dilakukan prosesnya pada *smartphone* berbasis *android*.

Desain Sistem Steganografi

Perancangan sistem keamanan dalam pengiriman pesan rahasia yang berbasis *android* ini dibuat dengan teknik LSB (*Least Significant Bit*) pada metode Steganografi, digunakan juga teknik *Vigenere Key* pada metode Kriptografi, Teknik-teknik akan digabung menjadi satu sistem keamanan pengiriman pesan rahasia, Gambaran sistemnya akan ditunjukkan pada Gambar 5. Perancangan teknik-teknik ini akan diimplementasikan pada *smartphone* berbasis *android.*



Gambar 1 : Skema Sistem Keamanan Pengiriman Pesan Rahasia

Algoritma Sistem Steganografi

Dalam penelitian ini dilakukan desain sistem Steganografi terdiri dari dua, yaitu fungsi utama *encode* dan *decode*.

Algoritma *Encode* adalah sebagai berikut :

a) Enkripsi pesan dengan menggunakan *Vigenere Key*.
b) Pesan rahasia yang sudah di encrypt disisipkan ke dalam *cover image* menggunakan LSB dan menghasilkan *stego image.*

Sedangkan algoritma *Decode* sebagai berikut :

a) Proses baca isi *Stego Image* dengan metode LSB.
b) Dekripsi dilakukan terhadap pesan rahasia tersebut dengan LSB.

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 2) : 61 - 67. Th. 2018
p-ISSN: 2620-620X
e-ISSN: 2621-9840

Vigenere Key Yang Diusulkan

Pada penelitian ini di coba mengembangkan rumus di mana dapat diterapkan terhadap karakter-karakter.

Rumus yang diterapkan di penelitian ini

Rumus Enkripsi :

Pertama kali dilakukan penjumlahan *plaintext (*Pi) dengan kunci (Ki).

- Jika hasil penjumlahan Pi dan Ki kurang dari 127, maka :
  Ci = (Pi + Ki) mod 127
- Jika hasil penjumlahan Pi dan Ki lebih dari 127, maka :
  Ci = (Pi + Ki) -127

Rumus Dekripsi :

Pi = (Ci – Ki) mod 127

Diketahui *Plaintext* (P) ”fath” dan *Keyword (*K) ”pass”, maka dilakukan perhitungan per karakter *plaintext* dan *keyword*;

Enkripsi :

P(i) = f → kode Ascii = 102

K(i) = p → kode Ascii = 112

Karena hasil P(1)+K(1) > 127, maka
C(1) = (P(1)+K(1)) -127

C(i) = (102+112)-127

= 87 → W

Chipertext yang diperoleh : WCh&

Dekripsi :

C(i) = f → kode Ascii = 87

K(i) = p → kode Ascii = 112

C(1) = (C(1)-K(1)) mod 127

C(i) = (87-112) mod 127

= 102 → f

Karakter yang diperoleh : fath (*plaintext*)

HASIL DAN PEMBAHASAN

Pengujian *Black Box* yang dilakukan di dalam penelitian ini diawali dengan penentuan beberapa file Gambar yang digunakan untuk data set *cover image* yang akan ditampilkan di tabel 1

Selain Gambar-Gambar, disediakan juga data-data yang akan digunakan sebagai pesan rahasia. Tabel 2 menunjukkan data-data pesan rahasia. Disediakan lima file dengan tipe *.txt, *.pdf, *.xls dan *.docx, pesan dengan tipe *plain text* juga disediakan untuk bahan pengujian.

Data-data diatas diuji dalam hal kecepatan enkripsi. Pada tabel 3 menunjukkan waktu yang dibutuhkan dalam proses enkripsi yang dihasilkan dengan teknik *Vigenere Key*.

Tabel 1 : Cover Image

Gambar	Resolusi	Ukuran (Byte)
 Bridge.jpg	1960x2560	151552
 panda.png	1020 x 510	666735
 tiger.bmp	259 x 157	155557
 Husky.gif	249 x 503	116736
 Jasmine.jpeg	800 x 600	323584

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 2) : 61 - 67. Th. 2018
p-ISSN: 2620-620X
e-ISSN: 2621-9840

Tabel 2 : Data Pesan Rahasia

Pesan	Jenis Pesan	Ukuran (Byte)
Pesan rahasianya terkirim	Plain Text	25
Profile.ppt	File	44505
Data.xlsx	File	87050
Report.doc	File	169785
IMG_20180522_0001.pdf	File	19574

Tabel 3: Kecepatan Enkripsi

Pesan	Jenis Pesan	Ukuran (Byte)	Kec (det)
Pesan rahasianya terkirim	Plain Text	25	0.00000
Profile.ppt	File	44505	0.00200
Data.xlsx	File	87050	0.00500
Report.doc	File	169785	0.00800
IMG_20180522_0001.pdf	File	19574	0.00100

Semakin besar ukuran pesan maka waktu yang dibutuhkan dalam proses enkripsi makin lama.

Data yang sudah di enkrip ke dalam stego image. Pada saat proses perolehan data rahasia kembali, akan dilakukan proses dan dekripsi, dan jika hasilnya berbeda, maka sistem akan memberikan error messege.

Tabel 4 : Hasil Waktu Proses Encode dan Decode

Gambar	Pesan	Lama Encode (dt)	Lama Decode (mnt)
Bridge.jpg	Pesan rahasianya terkirim	0.978	1.25_{10}
Panda.png	Profile.ppt	9.953	0.73_{90}
Tiger.bmp	Data.xlsx	18.755	0.35_{87}
Husky.gif	Report.doc	0.7573	0.19_{95}
Jasmine.jpeg	IMG_20180522_0001.pdf	19.357	0.00_{45}

Sistem keamanan pengiriman data dengan melalui proses penggabungan metode kriptografi, dan steganografi secara keseluruhan proses total akan ditampilkan waktu hasil proses encode dan decode pada Tabel 5. Waktu yang dibutuhkan dalam proses decode lebih lama dibanding dengan waktu proses encode, ini dikarenakan pada saat proses pemrolehan data rahasia, sistem akan melakukan proses pembongkaran stego image, yang telah disisipkan di stego image dan dekripsi. Dengan metode ini keaslian data akan lebih terjamin.

SIMPULAN DAN SARAN

Simpulan

Dari rumusan masalah Bagaimana menerapakan teknik Steganografi dan Kriptografi untuk meningkatkan keamanan proses penyampaian data rahasia, maka dalam penelitian ini dilakukan penerepan beberapa metode dan teknik untuk mengatasi masalah tersebut dan dicapai beberapa kesimpulan :

1. *Cover image* berupa *image digital* jenis *.gif, *.jpeg, *.png, *.bmp
2. Data rahasia yang dapat disisipkan ke *cover image* adalah file *.doc, *.docx, *.xs, *.xlsx, *.txt, *.pdf dan *plaintext*.
3. Dengan sistem ini dapat mengirimkan pesan rahasia melaui semua media *share online* (yang tidak tersedia fasilitas *encrypt)* dan *bluetooth* yang ada di *android* tersebut.
4. Prototipe perangkat lunak ini sebaiknya dijalankan di android dengan mikroprosesor memiliki kecepatan minimal 1.2 GHz, Internal memori minimal 2 GB dan RAM minimal 1 GB karena sistem ini dalam menjalankan proses enkripsi, kompresi, dekompres, checksum dan steganografi membutuhkan waktu dan memori yang ekstra.
5. Kecepatan dalam melakukan setiap atau bahkan semua proses teknik di dalam sistem ini secara bersamaan tergantung pada RAM yang dimiliki *android* tempat menjalankan sistem ini dan aktifitas yang sedang berlangsung di *android* tersebut.

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 2) : 61 - 67. Th. 2018
p-ISSN: 2620-620X
e-ISSN: 2621-9840

6. Menghasilkan *stego image* yang tidak terlihat perbedaan yang *significant* dengan kasat mata.
7. Perbedaan yang terlihat dari *image* asli dan *stego image* adalah ukuran *image* (ini tidak akan diketahui oleh pihak ketiga).
8. Setelah mealalui proses *decrypt* dan pembukaan *stego image*, data atau pesan tidak mengalami perubahan dari proses sebelum penyisipan ke *cover image*.

Saran

Adapun saran guna dilakukan di penelitian lebih lanjut adalah sebagai berikut :

1. Mencoba untuk dibuat sistem yang dapat menyampaikan pesan rahasia untuk semua jenis pesan termasuk tipe data audio dan video.
2. Perlu mencoba menggunakan teknik-teknik lain dalam kriptografi, steganografi, kompresi dan checksum guna validasi, contohnya RSA dalam metode kriptografi, BPCS steganografi, LZW dalam kompresi dan SHA512 untuk *checksum.*

Mencari teknik-teknik yang lebih baik untuk pengamanan dalam pertukaran pesan rahasia lewat media *online* dengan basis semua OS *smartphone* tidak hanya *android*

DAFTAR PUSTAKA

[1] Adnan Abdul-Aziz Gutub,2010, "Pixel Indicator Technique for RGB Image Steganography", Journal Of Emerging Technologies In Web Intelligence, Vol.2, No.1.

[2] Basuki Rakhmat1 Muhammad Fairuzabadi, M.Kom.2, 2010, "Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenère Dan Rc4", Jurnal Dinamika Informatika Volume 5, Nomor 2.

[3] Hasbian Saputra[1], M. Zen Samsono Hadi[2], Nanang Syahroni[3], 2011, "Implementasi Algoritma Steganografi Embedding Dengan Metode Least Significant Bit (Lsb) Insertion Dan Huffman Coding Pada Pengiriman Pesan Menggunakan Media Mms Berbasis J2ME", Teknik Telekomunkasi - Politeknik Elektronika Negeri Surabaya Institut Teknologi Sepuluh Nopember (ITS) Surabaya.

[4] Kevin Chandra Irwanto, 2011, "Aplikasi Teori Bilangan Dalam Sandi Vigenere Dan Caesar", Bandung.

[5] Ary Budi Warsito1, Lusi Fajarita2, Nazori AZ3, 2012," Proteksi Keamanan Dokumen Sertifikat File Jpeg Pada Perguruan Tinggi Dengan Menggunakan Steganografi Dan Kriptografi ",Jurnal TELEMATIKA MKOM Vol.4 No.1.

[6] Tri Prasetyo Utomo, 2012, "Steganografi Gambar Dengan Metode *Least Significant Bit* Untuk Proteksi Komunikasi Pada Media Online", Fakultas Sains dan Teknologi UIN Sunan Gunung Djati Bandung.

[7] Sushil Kumar[1], S.K.Muttoo[2], 2013, "A Comperative Study Of Image Steganography In Wavalet Domain", ISSN 2320-088X IJCSMC, Vol.2, Issue.2, pg.91-101

[8] Pu, I.M., 2006, Fundamental Data Compression, Elsevier, Britain.

[9] Putu H. Arjana, Tri Puji Rahayu ,Yakub, Hariyanto, 2012, "Implementasi Enkripsi Data dengan Algoritma Vigenere Cipher", Yogyakarta.

[10] Agnes Aryasanti[#1], Mardi Hardjianto[*2], 2014, "Model Pengamanan Berkas Bank Soal dengan Metode Steganografi LSB Dan Kompresi", Jurnal TICOM Vol.2 No.2.

[11] Tri Cahyadi, 2012, "Implementasi Steganography dengan enkripsi

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 2) : 61 - 67. Th. 2018
p-ISSN: 2620-620X
e-ISSN: 2621-9840

Vigener Cipher pada Citra JPEG", Semarang.

[12] Muharram Huda W, 2009, "Perkembangan Enkripsi Fungsi Hash pada SHA (Secure Hash Algorithm)", MAKALAH IF2091 STRATEGI ALGORITMIK, Bandung.

[13] Quist-Aphetsi Kester, Digital Forensics Department, Faculty of Informatics, Ghana Technology University College. Accra, Ghana, 2012, "A cryptosystem based on Vigenère cipher withvarying key", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1.

[14] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, 2012, "Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp. 338-341

[15] Nurhasanah1dan Raden Sulaiman2, 2013, "Pembuatan Tanda Tangan Digital Menggunakan Digital Signature Algorithm".

[16] Sugiyono, 2012,"Metode Penelitian Kuantitatif, Kualitatif dan R&D", Bandung: Alfabeta.

[17] Ms.E.Suneetha[1], Smt. D.Swetha[2], Ms.E.Sumalatha[3], Ms.P.Sridevi[4] & Ms.Sk.Rajeena Sulthana[5] Bapatla, Guntur, 2012, "Steganography Using LSB Algorithm And RGB Decomposition", ISSN: 0975-6779 NOV 11 TO OCT 12 VOLUME -02, ISSUE – 01

[18] Virginia L. Clark, Teaching with aSpecialization in the Teaching of Middle Level Mathematics in the Department of Mathematics., 2012,"The Vigenére Cipher Expository Paper", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10.

[19] Sanjeev Kumar Mandal[1], A.R Deept[2], 2012, "Steganography Using LSB Algorithm And RGB Decomposition", ISSN: 0975-9646 (IJCSIT) International Journal of Computer Science and Information Technologies , Vol 7 (4), 2016, 2096-2099