Turnitin Originality Report

Processed on: 12-Aug-2020 2:12 AM WIB
ID: 1368519538
Word Count: 4379
Submitted: 1

SISTEM KEAMANAN DATA TEKS DENGAN STEGANOGRAFI CITRA GAMBAR MENGGUNAKAN ALGORITMA END OF FILE By Patmi Kasih

Similarity Index	Similarity by Source	
18%	Internet Sources:	14%
	Publications:	6%
	Student Papers:	10%

1% match (publications)
Anggita Safitri Febriarini, Erna Zuni Astuti. "Penerapan Algoritma C4.5 untuk Prediksi Kepuasan Penumpang Bus Rapid Transit (BRT) Trans Semarang", Eksplora Informatika, 2019

1% match (student papers from 01-Mar-2020)
Submitted to Universitas Pancasila on 2020-03-01

1% match (publications)
Ariska Fitria Anggelin, Ardi Sanjaya, Ahmad Bagus Setiawan. "riska Fitria Anggelina Pengenalan Pola Tulisan Huruf Jepang (Hiragana) Menggunakan Partisi Citra", Generation Journal, 2018

1% match (Internet from 16-Mar-2016)
http://ejournal-s1.undip.ac.id/index.php/joint/article/download/6288/6072

1% match (Internet from 09-Jun-2020)
http://citisee.amikompurwokerto.ac.id/assets/proceedings/paper/10__AMIKOM_Purwokerto_-_Irfan_-_Implementasi_Model_Steganografi.pdf

1% match (Internet from 25-Jul-2020)
http://wehunt-project.blogspot.com/2018/10/

1% match (Internet from 15-Jan-2019)
https://adoc.site/download/sistem-penunjang-keputusan-pemilihan-perangkat-lunak-pengolah-citra-dengan-metode-multi-criteria-decision-making-mcdm-dan-analytical-hierarchy-process-ahp--a5b31ef6a7e197

1% match (Internet from 10-Apr-2018)
http://polocheater-7.blogspot.com/2012/11/kode-hex-warna.html

1% match (Internet from 16-Jun-2016)
http://eprints.dinus.ac.id/16510/1/jurnal_15452.pdf

1% match (Internet from 14-Apr-2020)
https://id.scribd.com/doc/300441201/Implementasi-dan-Analisis-Teknik-Steganografi-Menggunakan-CSS-dalam-Markup-Language-dengan-Teknik-Kriptografi-RSA

1% match (Internet from 25-Mar-2019)
http://www.g-excess.com/pengertian-mobilitas-sosial.html

1% match (Internet from 02-Jul-2018)
https://media.neliti.com/media/publications/237610-teknik-pengamanan-data-dengan-steganogra-aab8e8c2.pdf

1% match (Internet from 18-Jun-2019)
http://www.iosrjournals.org/iosr-jce/papers/Vol11-issue1/C01111519.pdf?id=114

< 1% match (Internet from 24-Jun-2015)
http://thesis.binus.ac.id/Doc/RingkasanInd/2012-1-00963-MTIF%20Ringkasan001.pdf

< 1% match (student papers from 25-May-2018)
Submitted to Universitas Jember on 2018-05-25

< 1% match (Internet from 27-May-2020)
https://es.scribd.com/document/317436017/Skripsi-pdf

< 1% match (Internet from 09-Feb-2020)
http://jti.respati.ac.id/index.php/jurnaljti/article/download/258/237

< 1% match (Internet from 13-Mar-2020)
https://es.slideshare.net/msyani/book-of-abstract-seamntik-udinus-2015

< 1% match (Internet from 08-Dec-2019)
http://ejournal.stikom-db.ac.id/index.php/processor/article/download/59/59/

< 1% match ()
http://eprints.ums.ac.id/45002/2/Surat%20Pernyataan%20Publikasi%20Ilmiah.pdf

< 1% match (Internet from 16-Sep-2017)
http://thesis.binus.ac.id/doc/Bab3/2012-1-00554-mtif%203.pdf

< 1% match (publications)
Julian Sahertian, Risa Helilintar. "Pengembangan Aplikasi Mobile Augmented Reality Sebagai Media Pembelajaran Biologi Materi Sel", Jurnal Sains dan Informatika, 2017

< 1% match (Internet from 07-Sep-2018)
http://ejournals.umn.ac.id/index.php/TI/article/download/564/494

< 1% match (Internet from 29-Apr-2020)
https://www.scribd.com/document/386606731/Buku-Knn

< 1% match (Internet from 08-Feb-2020)
http://repository.uinjkt.ac.id/dspace/bitstream/123456789/4402/1/JAMALUDIN-FST.pdf

< 1% match (Internet from 09-Jun-2020)
https://cunop.wordpress.com/category/metodologi-penelitian/page/2/

< 1% match (Internet from 08-Mar-2020)
http://simki.unpkediri.ac.id/mahasiswa/file_artikel/2017/b63e284d312525cd857bdfec4f488b9d.pdf

< 1% match (Internet from 03-Mar-2020)
https://repository.bsi.ac.id/index.php/unduh/item/217813/File_12-Bab-IV-Rancangan-Sistem-Usulan.pdf

< 1% match (Internet from 18-Mar-2019)
http://publikasi.dinus.ac.id/index.php/semantik/article/download/100/58

< 1% match (Internet from 19-Jun-2019)
http://kikiseptias.blogspot.com/2009/08/perubahan-data-menjadi-informasi_05.html

< 1% match (Internet from 29-Apr-2020)
https://pt.scribd.com/document/209566771/IMPLEMENTASI-PENGENKRIPSIAN-DAN-PENYEMBUNYIAN-DATA-MENGGUNAKAN-TINY-ENCRYPTION-ALGORITHM-DAN-END-OF-FILE

< 1% match (Internet from 08-May-2020)
http://eprints.binadarma.ac.id/3891/1/PROSIDING%20SEMNASTIK%20X%202018.pdf

< 1% match (Internet from 29-Dec-2015)
http://repository.usu.ac.id/bitstream/123456789/52323/5/Chapter%20I.pdf

< 1% match (Internet from 09-Apr-2020)
https://dhableg.blogspot.com/2011/

< 1% match (Internet from 07-Oct-2019)
https://www.keneono.site/2018/11/alternatif-sumber-cdn-pengganti-rawgit.html

< 1% match (Internet from 07-Dec-2015)
http://www.researchgate.net/publication/279466857_PENGGUNAAN_JAVA_3D_API_UNTUK_TRANSFORMASI_DAN_PENCAHAYAAN_PADA_OBJEK_3D

< 1% match (student papers from 10-Nov-2017)
Submitted to Sriwijaya University on 2017-11-10

< 1% match (student papers from 02-Jul-2015)
Submitted to Universitas Dian Nuswantoro on 2015-07-02

< 1% match (student papers from 15-Jun-2017)
Submitted to Universiti Kebangsaan Malaysia on 2017-06-15

< 1% match (student papers from 02-Mar-2017)
Submitted to iGroup on 2017-03-02

Seminar Nasional Inovasi Teknologi ISBN : - UN PGRI Kediri, 25 Juli 2020 e-ISSN : 2549-7952 Prosiding Seminar Nasional Inovasi Teknologi (Semnasinotek) 2020 " Sain dan Teknologi Untuk Pembangunan yang Berkelanjutan " BUKU 3 Hak Cipta © 2020 pada Penulis Hak Cipta dilindungi undang – undang Artikel pada prosiding ini dapat dimodifikasi, digunakan, dan disebarluaskan secara bebas untuk tujuan non profit, dengan syarat tidak menghapus atau mengubah atribut penulis dan tidak boleh melakukan penulisan ulang tanpa seijin penulis terlebih dahulu. Diterbitkan oleh : Panitia Semnasinotek Fakultas Teknik – Universitas Nusantara PGRI Kediri Kampus 2, Mojoroto Gg 1 no. 6, Kota Kediri Telp : (0357) 771576 Website : semnasinotek.unpkediri.ac.id Email : semnasinotek@unpkdr.ac.id ii Seminar Nasional Inovasi Teknologi ISBN : - UN PGRI Kediri, 25 Juli 2020 e-ISSN : 2549-7952 Sususan Panitia Penanggung Jawab Dr. Suryo Widodo, M.Pd Ketua Umum Ahmad Bagus Setiawan, S.T., M.Kom Ketua Pelaksana Fatkur Rhohman, M.Pd Keynote Speaker Prof. Dr. Emma Utami, S.Si., M.Kom Program Committee Agus Eko Minarno, M.Kom (Universitas Muhammadiyah Malang) Renny Sari Dewi (Universitas Internasional Semen Indonesia) AM. Mufarrih, S. Pd., M.T. (Politeknik Negeri Malang) Bidang-bidang Sekertaris : Kartika Rahayu Tri P, M.Sc Bendahara : Patmi Kasih, M.Kom Sie Kesekertariatan : Umi Mahdiyah, S.Pd., M.Si M. Najibulloh Muzaki, M.Kom., M.Cs Niska Shofia, S.Si., M.Pd Sie Acara dan Keamanan : Hesti Istiqlaliyah, S.T., M.Eng Arie Nugroho, S.kom., M.M Ratih Kumalasari, S.ST, M.Kom Ary Permatadeny Nevita, S.T., M.M Rini Indriati, M.Kom Miftakhul Maulidina, S.Pd., M.Si Ah. Suhan Fauzi, M.Si Mochamad Bilal, S.Kom., M.Cs Sie Perlengkapan : Hisbulloh Ahlis Munawi, S.E., M.T Muh. Muslimin Ilham, M.T Ir. Nuryosuwito, M.Eng Pudji Slamet Mohamad Efendi Asrul Dwi Hermawan Andika Permadi, S.E Sie Makalah Review dan : Resty Wulanningrum, M.Kom Prosiding Danar Putra Pamungkas, M.Kom Sucipto, M.Kom Haris Mahmudi M.Pd vi ISBN : - e-ISSN : 2549-7952 Elsanda Merita Indrawati, M.Pd M. Dewi Manikta P, M.Pd Yasinta Sindy Pramesty, M.Pd Hermin Istiasih, S.T., M.M., M.T Kuni Nadliroh, M. Si Muhammad Zuhdi S., S.E., M.M Erna Daniati, M.Kom Siti Rochana, M.Pd Lilia Sinta Wahyuniar, M.Pd Daniel Swanjaya, M.Kom Anita Sari wardani, M.Kom Sie Promosi Dokumentasi dan : Ardi Sanjaya, M.Kom IT Teguh Andriyanto, S.T,. M.Cs Risa Helilintar, M.Kom Risky Aswi Ramadhani, M.Kom Rachmad Santoso, S.T., M.MT M. Baihaqi, S.T Abu Bakar, S.Pd Sie Humas dan Sponsor : Made Ayu Dusea Widyadara, M.Kom Rony Heri Irawan, M.Kom Julian Sahertian, S.Pd., M.Kom Aidina Ristyawan, M.Kom Sie Konsumsi : Rina Firliana, M.Kom Dwi Harini, S.Si., M.M vii Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 25 Juli 2020 ISBN : - e-ISSN : 2549-7952 Impllementasi Metode Electre Untuk Menentukan Topik Skripsi (IMEMTOPSI) Rancang Bangun Alat Pemotong Sentrifugal dan Aplikasi Sistem Pneumatik Rancang Bangun Alat Pencuci Serbaguna Tipe Silinder Pada Mesin Pembuat Keripik Perancangan Sistem Penggorengan Pada Mesin Pembuat Keripik Serbaguna Dengan Metode Deep Frying Modifikasi Alat Pencacah Daun Kering Dengan Penambahan Saringan Analisa Sudut Mata Pisau dan Jumlah Pisau pada Alat Pencacah daun Kering Terhadap hasil cacahan Analisa Perbandingan Putaran pada alat Pencacah daun kering terhadap hasil cacahan Rancang Bangun Metal Foundry Limbah Aluminium Bekas Berkapasitas 2 Kg Berbahan Bakar LPG Perancangan dan Perakitan Mesin Pencacah Bulu Ayam Sistem Rekrutmen berdasarkan

kualifikasi Sistem Pemilihan Bahan Baku Tempe berkualitas Sistem Seleksi Atlet Sepak Takraw Krawnjang Alat Pemanas Tambal Ban Otomatis Rancang Bangun Alat Perontok Kacang Tanah Perancangan alat penyikat kamar mandi dan kloset otmatis bertenaga dinamo Optimasi Penyimpanan Fotorontgen Pada Sistem Informasi Rekam Medis Klinik Decision Suport System Pemilihan Bibit Unggul Tanaman Kelengkeng Menggunakan Metode SAW (Simple Additive weighting) Sistem Keamanan Data Teks Dengan Steganografi Citra Gambar Menggunakan Algoritma End Of File Pembuatan Special Effect dalam Film Pendek Menggunakan Muzzle Flare dan Sound Effect dengan Aplikasi Camtasia 8 Pengaruh Quenching Baja ST 60 Dengan Media Hot Oil terhadap Nilai kekerasan Analisa Teknik dan Biaya Pembuatan Elektric Furnace Berkapasitas 7000 Watt Alat Pemanas Ban Otomatis Sistem Otomasi Mikrocontroller untuk Furnace dengan Kapasitas 7000 watt x SISTEM KEAMANAN DATA TEKS DENGAN STEGANOGRAFI CITRA GAMBAR MENGGUNAKAN ALGORITMA END OF FILE Arvin Argananta Gilbijatno 1, Patmi Kasih2, 1,2 ,Teknik Informatika, Fakultas Teknik, Universitas Nusantara PGRI Kediri E-mail: *1aargananta @gmail.com, 2 fatkasih @gmail.com Abstrak- Steganografi merupakan ilmu dan seni yang mempelajari cara penyembunyian informasi pada suatu media sedemikian rupa sehingga keberadaannya tidak terdeteksi oleh pihak lain yang tidak berhak atas informasi tersebut. Pengguna pertama (pengirim pesan) dapat mengirim media yang telah disisipi informasi rahasia tersebut melalui jalur komunikasi publik, hingga dapat diterima oleh pengguna kedua (penerima pesan). Penerima pesan dapat mengekstraksi informasi rahasia yang ada di dalamnya. Pada penelitian ini sistem dibuaat dengan menggunakan metode End of File untuk proses penyisipan dan ekstraksi pesan. Sistem keamanan data dibuat bekerja dengan cara melakukan enkripsi teks ASCII dan citra gambar. Lalu menggabungkan keduanya dalam suatu media dengan menggunakan metode end of file. Pesan yang berupa plaintext (data teks) akan di ubah ke ASCII kemudian disisipkan pada akhir dari media citra yang digunakan. Dengan adanya metode ini memungkinkan kita bisa saling bertukar informasi tanpa adanya rasa khawatir pesan rahasia yang kita kirim diketahui oleh orang yang tidak berhak menerimanya. Pada pengujian dihasilkan karakteristik metode end of file adalah mampu menampung lebih banyak data atau pesan sehingga memungkinkan dapat menyisipkan lebih banyak pesan yang akan disisipkan. Tapi tetap ditentukan oleh ukuran panjang pesan ynag akan disisipkan agar tidak mempengaruhi citra penampung yaitu image. Kata Kunci : Steganografi, Data Teks, Gambar, End Of File (EOF) 1. PENDAHULUAN Perkembangan teknologi informasi dan komunikasi berperan penting dalam mempermudah masyarakat untuk saling bertukar informasi. Namun informasi yang bersifat rahasia saat ini rentan dicuri oleh orang yang tidak bertanggung jawab. Karena pada dasarnya pengiriman informasi dilakukan tanpa adanya pengamanan terhadap konten yang dikirim. Ketika terkena penyadapan, maka data dapat langsung dibaca oleh penyadap. Pengamanan informasi bisa dilakukan dengan berbagai cara, salah satunya adalah penyandian pesan menggunakan kode kode yang rumit ataupun acak. Oleh sebab itu diperlukan ilmu yang mempelajari keamanan informasi. Dan ilmu yang mempelajari sistem keamanan informasi tersebut adalah kriptografi. Kriptografi berasal dari dua kata, yaitu cryptos dan graphein. Cryptos berarti rahasia dan graphein berarti tulisan, sehingga menurut bahasa, kriptologi adalah tulisan rahasia. Menurut (Eko Arryawan, 2010) kriptografi adalah "ilmu untuk menyembunyikan isi pesan yang disandikan sehingga tidak diketahui apa isi pesan tersebut". Pada kriptografi terdapat dua proses utama yakni encoding dan decoding. "Proses encoding dan decoding diatur oleh satu atau lebih kunci kriptografi" (Wirdasari, 2008). Dalam kriptografi pesan asli yang akan dikirim terlebih dahulu dikodekan, proses ini disesbut Enkripsi. Sementara itu, untuk mengembalikan ke bentuk pesan asli disebut Dekripsi. Pesan asli disebut Plaintext dan pesan yang sudah dirahasiakan di sebut chipertext. Namun disisi lain kriptografi dapat menimbulkan kecurigaan pada orang yang membaca data terenkripsi. Teknik lain sebagai upaya pengamanan data adalah Steganografi. Cara kerja dari steganografi adalah menyamarkan pesan rahasia pada suatu media digital dengan teknik penyisipan. Penelitian ini terinspirasi keinginan untuk membuat suatu sistem keamanan data teks dengan menerapkan metode End Of File dengan teknik steganografi berbasis web. Selain itu peneliti ingin mengetahui bagaimana membuat sistem keamanan data berupa teks yang nantinya akan disisipkan pada citra gambar. Dalam penelitian ini digunakan data awal atau pesan rahasia yang di sembunyikan berformat teks yang berupa citra gambar. Tujuan dari penelitian pembuatan sistem keamanan data ini adalah merancang dan membangun aplikasi sistem keamanan data dengan implementasi metode End Of File dalam teknik steganografi. Menganalisis perbedaan besar ukuran file citra sebelum dan sesudah disisipkan pesan. Manfaat yang diinginkan peneliti dengan dibangunnya aplikasi ini adalah menjaga keamanan pesan rahasia yang ingin disampaikan, mengkombinasikan

antara Kriptografi dan Steganografi untuk mengamankan pesan yang disisipkan di dalam citra, menghindari kecurigaan publik pada sebuah kata ataupun kalimat acak. 2. METODE PENELITIAN 2.1 Steganografi Kata Steganografi berasal dari bahasa Yunani "steganos", yang artinya tersembunyi atau terselubung dan "graphein" artinya menulis. Menurut (Munir, 2009) Steganografi adalah ilmuuntuk menyembunyikan suatu pesan rahasia sehingga keberadaan pesan tersebut menjadi tidak dapat dideteksi oleh indra manusia. Jadisteganografi adalah sebuah teknik yang digunakan untuk menyisipkan data ke dalam sebuah media yang bertujuan untuk menyembunyikan keberadaan data rahasia dari pihak-pihak yang tidak berkepentingan. Gambar 1. Konsep dasar Steganografi Beberapa hal yang harus diperhatikan dalam penyembunyian data, adalah : 1. Tidak dapat dipersepsi (Impercepbility) 2. Ketepatan (Fidelity) 3. Ketahanan (Robustness) 4. Kapasitas (Capacity) 5. Pemulihan (Recovery) 2.2 Data Text dan Citra Digital Text merupakan sekumpulan karakter terdiri dari huruf-huruf, angka-angka (A-Z, a-z, 0-9) dan simbol-simbol lainya seperti %, &, ^, =, @, $, !, * dan lain-lain, dengan menggunakan kode ASCII setiap karakter dari text berjumlah 8-bit atau 1 byte. Citra digital adalah gambar dua dimensi yang bisa ditampilkan pada layar komputer sebagai himpunan atau diskrit nilai digital yang disebut pixel atau picture elements. Dalam tinjauan matematis, citra merupakan fungsi kontinu dari intensitas cahaya pada bidang dua dimensi. Jenis-jenis warna pada citra digital adalah hitam putih (monochrome), Hitam Putih dan abu abu (Grayscale), dan citra digital berwarna (RGB). 2.3 Perencanaan Sistem Sistem ini dirancang dengan user satu adalah pengirim sebagai pembuat dan pengelola pesan rahasia sebelum data tersebut dienkripsi, dikirim dan disisipkan dalam media gambar. Selanjutnya user dua sebagai penerima pesan yaitu orang tertentu yang bisa membuka pesan rahasia setelah data yang di terima di ekstraksi atau didekripsi terlebih dahulu. a. Data Input Dalam penelitian ini yang dijadikan data input adalah data berupa teks dan citra gambar b. Gambaran Proses Data Input yang akan akan diproses, yaitu penyisipan pesan rahasia ke dalam citra digital sebagai pengirim (enkripsi end of file), dan proses ekstraksi pesan (dekripsi stego image) sebagai pihak penerima. 1. Penyisipan pesan teks sebagai enkripsi pihak pengirim : a) Masukan pertama yaitu media penampung berupa citra gambar b) Masukan kedua yaitu pesan rahasia berupa pesan teks c) Proses steganografi enkripsi dengan metode End Of File d) Menghasilkan citra digital berupa gambar yang telah disisipi dengan data berupa teks atau biasa disebut stego image 2. Proses Ekstraksi Pesansebagai dekripsi pihakpenerima : a) Masukkan stego image yaitu hasil dari enkripsi awal b) Proses ekstraksi pesan c) Menghasilkan Pesan rahasia dan Gambar awal c. Data Output Data yang dihasilkan setelah proses stenografi adalah data berupa sebuah file gambar yang berisi pesan asli (teks) yang sebelumnya telah dienkripsi dan disisipkan pada citra gambar. 2.4 Arsitektur dan Desain Sistem Secara umum program steganografi ini mempunyai fungsi untuk menyembunyikan informasi berupa pesan teks dibalik data citra, Dalam hal ini media yang digunakan adalah citra digital. Dan harus diperhatikan bahwa perubahan pada citra penampung yang telah termodifikasi tidak boleh terlalu terlihat, agar suatu kerahasian dari informasi yang ada dalam file citra digital tetap terjaga (integrity). Perencanaan dalam sistem keamanan data steganografi ini dibagi beberapa subsistem yaitu : a. Use Case Diagram Pemodelan sistem menggunakan Use Case Diagram antara pengirim dan penerima pesan dapat dilihat pada gambar 2. Gambar 2. Use Case Diagram Pengirim dan Penerima Dari Use Case Diagram gambar dapat kita simpulkan bahwa user (Pengirim/Penerima) dapat melakukan 6 hal: 1. Login ke sistem 2. Masukkan key antar Pengirim dan Pernerima 3. Menentukan pesan rahasia yang akan dibuat 4. Menentukan Citra Masukan. 5. Melakukan proses penyisipan pesan (berlaku jika user sebagai pengirim pesan) 6. Melakukan proses ekstraksi pesan (berlaku jika user sebagai penerima pesan) b. Activity Diagram Proses sistem yang dilakukan untuk menyisipkan pesan digambarkan pada diagram gambar 3. Pada proses ini masukkan input file berupa pesan teks dan citra penampung berupa gambar. Saat proses enkripsi penyisipan, sistem akan merubah file file masukan tadi terlebih dahulu menjadi biner lalu hexadesimal. Dan tahap selanjutnya adalah menyisipkan pesan yang terenkripsi tadi pada akhir nilai hexadesimal citra gambar. Gambar 3. Activity Diagram Penyisipan Teks Selanjutnya pada gambar 4, dari diagram proses ekstraksi, citra masukan pesan tersebut adalah berupa citra yang mengandung pesan didalamnya yaitu Stegoimage. Lalu user hanya perlu memilih pilihan menu dekripsi untuk mengubah dan membalik stegoimage menjadi file file masukan pertama. Terakhir, sistem akan menampilkan gambar awal dan isi dari pesan awal yang di rahasiakan. Gambar 4. Activity Diagram Ekstraksi Pesan c. Flowchart Progam Secara keselurhan alur aplikasi yang dibuat dalam penelitian ini digambarkan dalam bentuk flowchart diagram pada gambar 5 dan gambar 6. Gambar 5. Flowchart Proses Penyisipan teks Dari gambar 5, dapat dijelaskan bahwa langkah awal pada tahap

ini adalah memilih citra. Citra yang dipilih merupakan citra gambar RGB yang mana dalam citra tersebut akan diubah menjadi citra biner Inputan selanjutnya adalah pesan berupa teks yang nantinya akan disisipkan. Karakter pesan yang akan disisipkan kedalam citra harus sudah dalam bentuk sekumpulan kode ASCII, sebab letak kode ASCII tersebut akan ditempatkan pada akhir baris citra cover. Dan masukkan juga key password sebagai ketentuan proteksi yang hanya diketahui oleh pengirim dan penerima pesan nantinya. Terdapat keterangan jika gambar bukan merupakan stegoimage maka proses tidak bisa dijalankan. Namun jika gambar belum pernah disisipi pesan apapun maka proses enkripsi bisa dijalankan. Gambar 6. Flowchart Proses Ekstraksi pesan Proses ekstraksi pesan (dekripsi) bisa dilihat pada gambar 6. dan dapat dijelaskan bagaimana proses ekstraksi pesan yaitu tahap diungkapkannya kembali pesan yang telah disisipkan, sehingga penerima dapat memahami pesan yang terkandung didalam citra stego. Pada tahap ini terdapat beberapa tahapan yaitu memilih citra stego image dan memasukkan password. Jika password salah, progam akan mengarahkan user pada pilihan "kembali" memilih stegoimage dan memasukkan password sekali lagi. Jika password sudah benar, maka proses bisa dijalankan dan menghasilkan outputan berupa pesan teks yang dirahasiakan dan gambar awal sebelum disisipi. 2.5 Metode End Of File Metode End Of File merupakan salah satu metode yang digunakan dalam steganografi. Metode ini menggunakan cara dengan menyisipkan data pada akhir file (Sejati, 2007). Metode End of File merupakan salah satu teknik yang menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan kedalam file tersebut. Dalam teknik End Of File, data yang disisipkan pada akhir file diberi tanda khusus sebagai pengenal start dari data tersebut dan sekaligus sebagai tanda pengenal akhir dari data tersebut. Prinsip kerja End Of File menggunakan karakter atau simbol khusus ctrl-z yang diberikan pada setiap akhir file (Anggraini dan Dolly, 2014). Misalkan pada sebuah citra berukuran 5x5 pixel disisipkan pesan yakni "gajah". Nilai desimal ASCII dari pesan diberikan sebagai berikut : 103 97 106 97 104 Misalkan matrik nilai desimaldari pixel citra adalah sebagai berikut : Gambar 7. Matrik Decimal Pixel Citra Sebelum Disisipi Nilai desimal pesan disisipkan pada akhir citra menjadikan nilai berikut : Gambar 8. Matrik Decimal Pixel Citra Setelah Disisipi Kelebihan dari metode end of file adalah tidak ada batasan dalam menambahkan informasi yang ingin disembunyikan, bahkan jika ukuran informasi itu melebihi ukuran citra penampung. Data informasi akan disembunyikan atau disisipkan diakhir file sehingga file image mungkin akan tampak ada perubahan dengan aslinya. Jika dapat dilihat mata maka perubahan ini akan tampak di baris bawah dari image. a. Encode Data Teks Proses encoding dimulai dengan pesan yang akan disisipkan. Pesan diubah kedalam bentuk biner dengan representasi 1 atau 0. Selanjutnya rangkaian biner tersebut dikonversikan menjadi bilangan decimal dan menghasilkan sebuah bilangan yang dinamakan dengan m. Algoritma yang dilakukan dalam data teks adalah proses perubahan kalimat ke dalam bentuk ASCII. Sebagai contoh pesan yang akan disisipkan adalah "#aku". Maka kode ASCII dari pesan tersebut adalah :35 97 107 117 b. Encode Data Gambar Proses Encode gambar adalah sebagai berikut : 1. Menghitung jumlah warna yang terdapat pada berkas RGB yang menjadi objek steganografi dan akan menghasilkan sebuah bilangan. Bilangan tesebut dinamakan dengan n, maka apabila m>n!-1 maka pesan yang akan disisipkan berukuran terlalu besar sehingga proses penyisipan tidak dapat dilakukan. 2. Warna dalam palet warna diurutkan sesuai dengan urutan yang "natural". Setiap warna dengan format RGB dikonversikan kedalam bilangan integer dengan aturan (Merah * 65536 + Hijau * 256 + Biru). Kemudian diurutkan berdasarkan besar bilangan integer yang mewakili warna tersebut. 3. Setelah itu proses iterasi terhadap variable i dengan nilai i adalah dari 1 sampai n. Setiap warna dengan urutan n-i dipindahkan ke posisi baru yaitu m mod i, kemudian m dibagi dengan i. 4. Kemudian palet warna yang baru hasil iterasi pada langkah ke-4 dimasukkan kedalm palet warna berkas RGB. 5. Apabila ternyata besar dari palet warna yang baru lebih kecil dari 256 maka palet warna akan diisi dengan warna terakhir dari palet warna sebelumnya. Kemudian berkas RGB akan dikompresi ulang dengan palet warna baru, untuk menghasilkan berkas yang baru dengan ukuran dan gambar yang sama, namun telah disisipi pesan. Gambar 9. Tabel warna RGB c. Kode Warna Dalam sebuah gambar digital sering melihat kode warna yang terdiri dari tanda '#' dan 6 angka atau huruf di belakang tanda tersebut, kode warna tersebut dapat diterjemahkan menjadi kode warna RGB. Misalkan kita mempunyai kode warna "#0088FF", kita akan mencari beberapa porsi untuk warna merah (red), hijau (green), dan biru (blue). Gambar 10. Tabel graysacale d. Proses Decode Adapun langkah-langkah proses decode atau mengekstrak pesan dari citra RGB yang telah disisipi pesan dengan metode End Of File adalah sebagai berikut: 1. Masukkan nomor sesuai dengan posisi

setiap warna pada palet warna citra RGB yang telah disisipkan pesan 2. Warna diurutkan berdasarkan konversi RGB ke nilai integer dengan rumus: (Merah * 65536 + Hijau * 256 + Biru). 3. m diberi nilai 0 4. Iterasi variabel i dari i+1 sampai n-1. a) m=m*(n-1) + posisi warna ke i b) iterasi variabel j dari i +1 sampai n-1 c) jika posisi warna ke j > nilai posisi warna ke-i, maka posisi warna ke i dikurangkan 1 5. Setelah nilai m diperoleh, maka nilai m dikonversikan kebilangan binari utuk memperoleh pesan asli kembali e. Proses End Of File Contoh penyisipan pesan "T" kedalam berkas RGB dengan jumlah warna pada palet warna sebanyak 6 buah, adalah sebagai berikut: 1. Pesan yang disisipkan adalah "T" yang diubah kebentuk binary dengan pengkodean ASCII menghasilkan bilangan biner : 01010100. Untuk mendapatkan nilai M disisipkan angka 1 pada rangkaian biner maka: m = 1 + 01010100 2 = 101010100 2 = 340 10 2. Jumlah warna pada palet warna citra tesebut adalah 6, maka apabila 340 >6!-1 cara menghitungnya yaitu sebagia berikut: C ("T") = ("T" + "U") mod 256 = L T = 51 dan U = 52 (51+52) % 96 = 7 C ("E") = ("E" + "K") mod 96 = p 3. Urutan warna pada palet warna citra tersebut sacara "natural"ditunjukkan dari beberapa warna yang didapat dari besar nilai RGB. Contoh pada warna A, nilai Red dalam hexadecimal adalah f7, dan di konversikan kedalam decimal menjadi 247, nilai Green pada hexadecimal adalah 47 dan nilai Blue dalam hexadecimal adalah 47 dan dikonversikan kedalam decimal menjadi 71. Berdasarkan nilai-nilai tersebut didapat nilai "natural" dengan rumus sebagai berikut: (Red 65536 + Green 256 + Blue) sehingga didapat nilai integer yaitu: 16205639. 4. Iterasi variabel i mulai dari 1 sampai n: Warna indeks ke- (n-1) dipindahkan ke- (m mod i), m = 1) a) Untuk i = 1 m = 340, m =340/1 = 340 maka warna indeks ke-5 dipindahkan ke indeks ke-0 pada susunan palet warna yang baru. b) Untuk i = 2 m = 340, m =340/2 = 170 maka warna indeks ke-4 dipindahkan ke indeks ke-0 pada susunan palet warna yang baru. c) Untuk i = 3 m = 170, m =170/3 = 56 maka warna indeks ke-3 dipindahkan ke indeks ke-2 pada susunan palet warna yang baru. d) Untuk i = 4 m = 56, m =56/4 = 14, maka warna indeks ke-2 dipindahkan ke indeks ke-0 pada susunan palet warna yang baru. e) Untuk i = 5 m = 14, m = 14/5= 2 maka warna indeks ke-1 dipindahkan ke indeks ke-3 pada susunan palet warna yang baru. f) Untuk i = 6 m = 2, m = 2/6= 0 maka warna indeks ke-0 dipindahkan ke indeks ke-1 pada susunan palet warna yang baru. 5. Pada tahap berikutnya, apabila ada beberapa warna indeks yang menempati indeks yang sama, maka setiap warna yang menempati indeks tersebut akan bergeser sekali ke indeks berikutnya. Gambar 11. Palet Index 6. Urutan palet warna ini kemudian dimasukkan kedalam berkas citra RGB untuk menghasilkan citra yang telah disisipi pesan. 3. HASIL DAN PEMBAHASAN Sistem keamanan data pesan dengan Steganografi End of File, terdapat 3 komponen penting menu utama yang mendasari. Adalah sebagai berikut : 1. Menu Enkripsi Merupakan interface yang memungkinkan user untuk membuat (button tambah), analisa dan hapus pesan rahasia yang akan dibuat maupun yang telah dibuat. a) Button Tambah dalam form Enkripsi Tombol menu yang di gunakan user untuk membuat baru sebuah pesan rahasia b) Button Analisa dalam form Enkripsi Tombol Menu yang di gunakan user untuk memastikan atau mengecek pesan yang di buat telah berhasil di sisipkan di media gamabar atau belum c) Button Hapus dalam form Enkripsi Tombol menu yang di gunakan user untuk menghapus pesan rahasia beserta media gambarnya. d) Button Pencarian Memungkinkan user untuk mencari file file enkripsi yang diinginkan 2. Menu Dekripsi Interface yang memungkinkan user untuk membuka (decrypt), analisa dan hapus pesan rahasia yang akan telah di enkripsi sebelumnya. a) Button Tambah dalam Menu Dekripsi Menu yang di gunakan user untuk memilih lalu membuka pesan rahasia dalam gambar b) Button Analisa dalam form Dekripsi Menu yang di gunakan user untuk memastikan dan membuktikan bahwa pesan rahasia sudah bisa di lepas dari media gambar. c) Button Hapus dalam form Dekripsi Menu yang di gunakan user untuk menghapus pesan rahasia beserta media gambar yang telah dibuka. 3. Menu Gallery Interface yang menyediakan tampilan pesan berupa gambar baik enkripsi maupun dekripsi beserta tanggal penyimpanan. Dan memungkinkan user untuk melihat langsung pesan rahasia yang ada di dalamnya dengan mengklik button buka pesan. a) Button Buka Pesn Menu yang di gunakan user untuk membuka secara langsung isi pesan rahasia yang ada di dalam gambar. b) Button Buka Pesan Memungkinkan user untuk mencari file file enkripsi dan dekripsi yang tersimpan di gallery. Pada sistem terdapat dua form/ layar kerja utama, pertama adalah hasil enkripsi berupa file gambar yang sudah tersisipi pesan teks rahasia di dalamnya, dan yang kedua adalah hasil dekripsi berupa pesan rahasia (awal) berbentuk teks dengan format ASCII dan citra gambar (awal) berformat JPEG maupun PNG. Secera rinci layar kerja yang ada dalam sistem adalah: 1. Form Enkripsi Gambar 12. Menu Enkripsi dengan Submenu Tambah Proses Enkripsi Layar kerja ini digunakan untuk menambah maupun membuat pesan teks yang ingin di

rahasiakan keberadaannya melalui media citra gambar sebagai penampungnya. 2. Form Analisa Enkripsi File Gambar 13. Analisa Enkripsi Menggunakan Size Gambar, Hexadesimal dan Opcode. Form ini digunakan untuk melakukan analisa atau cek pesan teks yang telah di sisipkan pada gambar apakah sudah berhasil atau belum. Tanda proses enkripsi berhasil adalah size gambar yang bertambah besar, jika format hexadecimal pada akhiran media gambar terlihat bertambah banyak di akhiran. Pengamatan lebih lanjut juga bisa di analisa pada akhiran simbol opcode progam. 3. Form hapus file terenkripsi dan dekripsi Gambar 14. Menu Hapus File Enkripsi Dekripsi Menu yang di gunakan user untuk menghapus pesan rahasia beserta media gambar di dalamnya baik file enkripsi ataupun file dekripsi. 4. Form Tambah Dekripsi File Gambar 15. Tambah File Dekripsi Form ini digunakan untuk membuka pesan teks rahasia yang telah terenkripsi sebelumnya dalam media gambar. Jadi dekripsi ini adalah kebalikan dari enkripsi. 5. Form Analisa File Dekripsi Gambar 16. Analisa Dekripsi Menggunakan Size Gambar, Hexadecimal, dan Opcode Form ini duganakan oleh user untuk menganalisa file enkripsi yang sudah bisa dibuka atau dibalikkan dengan dekripsi. Tanda jika berhasilnya proses Dekripsi adalah ukuruan atau size gambar yang mengecil dan juga jika format hexadecimal pada akhiran media gambar terlihat berkurang di akhir hexadecimal. 6. Form Gallery Layar kerja yang menyediakan tampilan pesan berupa gambar baik enkripsi maupun dekripsi beserta tanggal penyimpanan. Dan memungkinkan user untuk melihat langsung pesan rahasia yang ada di dalamnya dengan mengklik button buka pesan. Gambar 17. Gallery Enkripsi dan Dekripsi 4. KESIMPULAN Berdasarkan rangkaian kegiatan yang dilakukan dalam penelitian ini, mulai dari perencanaan, analisa permasalahan, perancangan, development sistem, uji coba dan analisa hasil, maka diperoleh beberapa kesimpulan sebagai berikut: 1. Penelitian ini berhasil membuat suatu sistem keamanan data pesan dalam gambar dengan menerapkan steganografi dengan metode End Of File, dimana sebuah pesan tek akan disisipkan ke dalam media penampung berupa gambar. Teks dan gambar harus sama sama di jadikan format hexadecimal terlebih dahulu agar bisa disisipkan di akhir penanda citra. 2. Sistem keamanan data yang diterapkan adalah dengan cara melakukan enkripsi teks ASCII dan citra gambar. Lalu menggabungkan keduanya dalam suatu media dengan menggunakan metode end of file. Dengan konsep seperti ini, maka pesan yang dibuat bisa terjaga kerahasiaannya di dalam file. 3. Ukuran pixel citra dan jumlah karakter yang digunakan berpengaruh terhadap lamanya waktu proses embedding dan extracting. Semakin besar ukuran pixel citra dan jumlah karakter, maka akan semakin lama proses penyisipan dan ekstraksinya. 5. SARAN Dalam pelaksanaan penelitian ini, peneliti menemukan beberapa pemikiran yang akhirnya tertuang dalam saran dan harapan yang dititipkan untuk peneliti selanjutnya, yaitu: 1. Aplikasi dapat dikembangkan lebih lanjut dengan menambahkan format gambar lain seperti bitmap (bmp) dan format penampung lain, seperti teks, audio, dan video. 2. Untuk Pengembangan lebih lanjut diharapkan dapat menambahkan sistem keamanan yang lebih baik pada perangkat lunak dalam meningkatkan keamanan sistem data yang seringkali dianggap sepele. DAFTAR PUSTAKA

[1] Arifin, R., dan Oktaviana, L. T. 2013, Implementasi Kriptografi dan Steganografi Menggunakan Algoritma RSA dan Metode LSB, Universitas Malang. [2] Ariyus, Dony. 2008, Pengantar Ilmu Kriptografi. Yogyakarta: CV. ANDI OFFSET. [3] K. P. Adhiya dan S. A. Patil, "Hiding Text in Audio Using LSB Based Steganography, "Information and Knowledge Management, vol. 2, no. 3, 2012. [4] Rifki Sadikin, 2012, Kriptografi Untuk Keamanan dan Implementasi Dalam Bahasa Java. Yogyakarta: Andi Offset. [5] Saputra, Joko. 2017, Steganografi penyisipan teks pada citra menggunakan end of file, Institut Teknologi Sepuluh November Surabaya. [6] Sembiring, Sandro. 2013, Perancangan Aplikasi Steganografi untuk menyisipkan pesan teks pada gambar dengan metode End Of File STMIK Budi Darma Medan [7] Munir Rinaldi, 2004, "Diktat Kuliah IF5054 Kriptografi : Steganografi dan Watermarking", Teknik Informatika ITB, Bandung, diakses dari http://informatika. stei. itb. ac. id/~rinaldi. munir/ Kriptografi/Steganografi dan Watermarking. pdf, akses 17 September 2019, pukul 13. 14 WIB. Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 25 Juli 2020 Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 25 Juli 2020 e-ISSN: 2549- 7952 p-ISSN: 2580- 3336 Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 25 Juli 2020 e-ISSN: 2549- 7952 p-ISSN: 2580- 3336 Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 25 Juli 2020 e-ISSN: 2549- 7952 p-ISSN: 2580- 3336 Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 25 Juli 2020 e-ISSN: 2549- 7952 p-ISSN: 2580- 3336 Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 25 Juli 2020 e-ISSN: 2549- 7952 p-ISSN: 2580- 3336 Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 25 Juli 2020 e-ISSN: 2549- 7952 p-ISSN: 2580- 3336 Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 25 Juli 2020 e-ISSN: 2549- 7952 p-ISSN: 2580- 3336 Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 25 Juli 2020

e-ISSN: 2549- 7952 p-ISSN: 2580- 3336