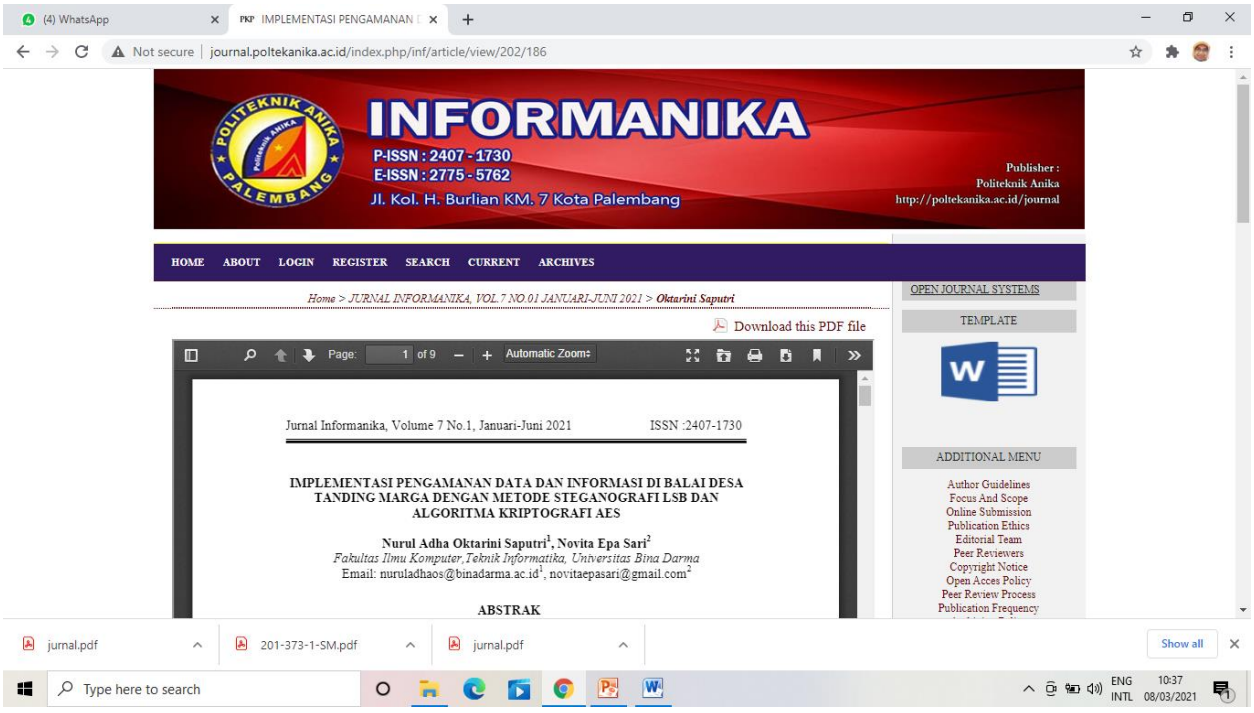
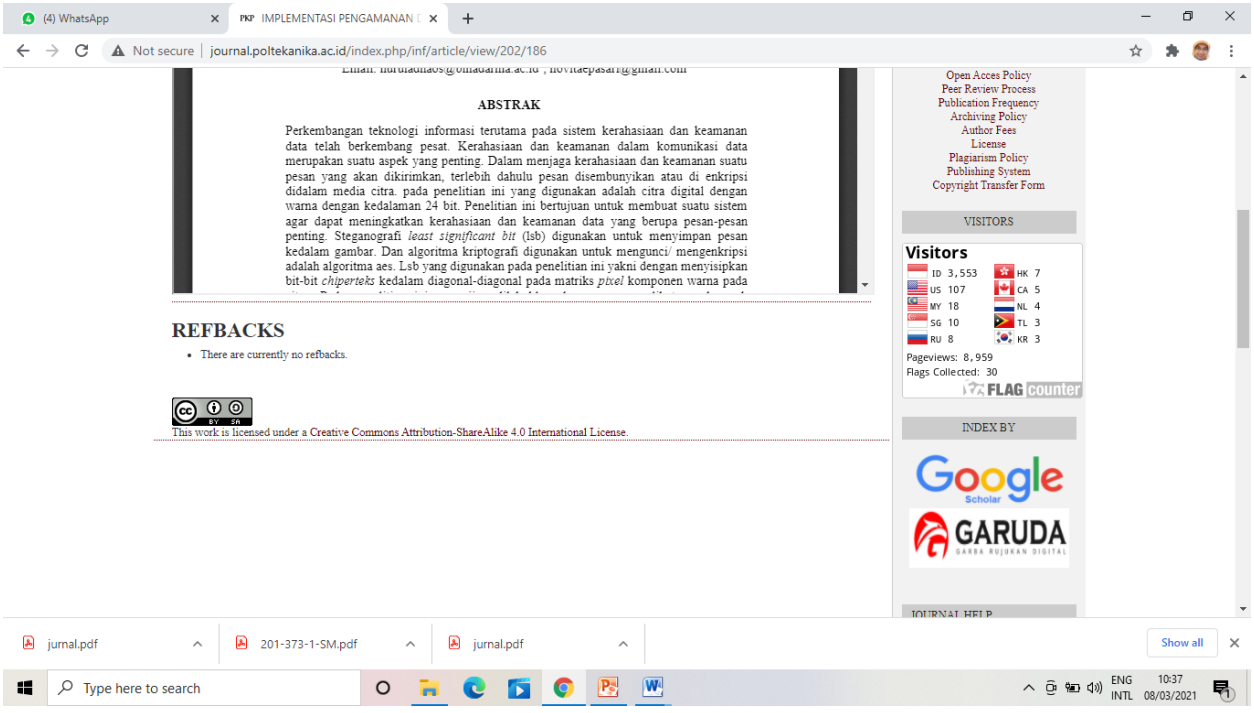
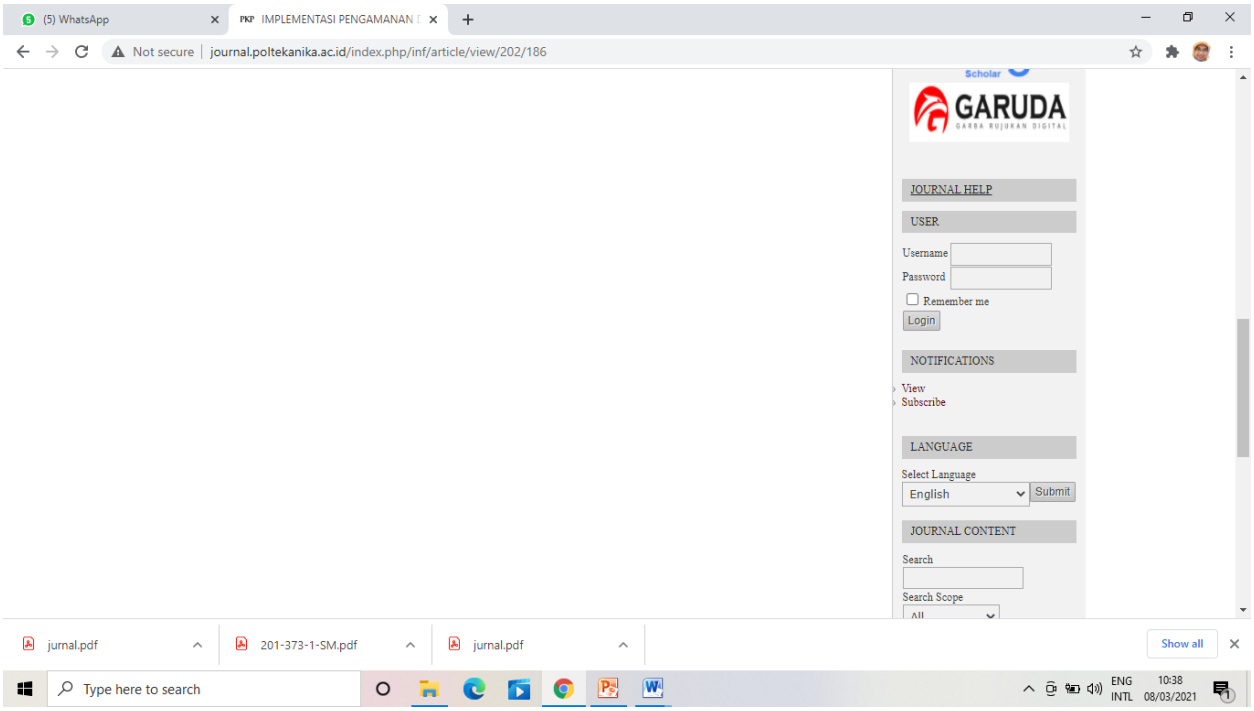

(4) WhatsApp
IMPLEMENTASI PENGAMANAN
Not secure | journal.poltekanika.ac.id/index.php/inf/article/view/202/186
INFORMANIKA
P-ISSN : 2407 - 1730
E-ISSN : 2775 - 5762
Jl. Kol. H. Burlian KM. 7 Kota Palembang
Publisher :
Politeknik Anika
http://poltekanika.ac.id/journal
HOME ABOUT LOGIN REGISTER SEARCH CURRENT ARCHIVES
Home > JURNAL INFORMANIKA, VOL 7 NO.01 JANUARI-JUNI 2021 > Oktarini Saputri
Download this PDF file
Page: 1 of 9
Automatic Zoom
Jurnal Informanika, Volume 7 No.1, Januari-Juni 2021 ISSN :2407-1730
IMPLEMENTASI PENGAMANAN DATA DAN INFORMASI DI BALAI DESA TANDING MARGA DENGAN METODE STEGANOGRAFI LSB DAN ALGORITMA KRIPTOGRAFI AES
Nurul Adha Oktarini Saputri[1], Novita Epa Sari[2]
Fakultas Ilmu Komputer, Teknik Informatika, Universitas Bina Darma
Email: nuruladhaos@binadarma.ac.id[1], novitaepasari@gmail.com[2]
ABSTRAK
OPEN JOURNAL SYSTEMS
TEMPLATE
ADDITIONAL MENU
Author Guidelines
Focus And Scope
Online Submission
Publication Ethics
Editorial Team
Peer Reviewers
Copyright Notice
Open Acces Policy
Peer Review Process
Publication Frequency
jurnal.pdf
201-373-1-SM.pdf
jurnal.pdf
Show all
Type here to search
ENG INTL 10:37 08/03/2021


(4) WhatsApp
IMPLEMENTASI PENGAMANAN
Not secure | journal.poltekanika.ac.id/index.php/inf/article/view/202/186
ABSTRAK
Perkembangan teknologi informasi terutama pada sistem kerahasiaan dan keamanan data telah berkembang pesat. Kerahasiaan dan keamanan dalam komunikasi data merupakan suatu aspek yang penting. Dalam menjaga kerahasiaan dan keamanan suatu pesan yang akan dikirimkan, terlebih dahulu pesan disembunyikan atau di enkripsi didalam media citra. pada penelitian ini yang digunakan adalah citra digital dengan warna dengan kedalaman 24 bit. Penelitian ini bertujuan untuk membuat suatu sistem agar dapat meningkatkan kerahasiaan dan keamanan data yang berupa pesan-pesan penting. Steganografi least significant bit (lsb) digunakan untuk menyimpan pesan kedalam gambar. Dan algoritma kriptografi digunakan untuk mengunci/ mengenkripsi adalah algoritma aes. Lsb yang digunakan pada penelitian ini yakni dengan menyisipkan bit-bit chiperteks kedalam diagonal-diagonal pada matriks pixel komponen warna pada
REFBACKS
There are currently no refbacks.
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Open Acces Policy
Peer Review Process
Publication Frequency
Archiving Policy
Author Fees
License
Plagiarism Policy
Publishing System
Copyright Transfer Form
VISITORS
Visitors
ID 3,553 HK 7
US 107 CA 5
MY 18 NL 4
SG 10 TL 3
RU 8 KR 3
Pageviews: 8,959
Flags Collected: 30
FLAG counter
INDEX BY
Google Scholar
GARUDA
JOURNAL HELP
jurnal.pdf
201-373-1-SM.pdf
jurnal.pdf
Show all
Type here to search
ENG INTL 10:37 08/03/2021


(5) WhatsApp
IMPLEMENTASI PENGAMANAN
Not secure | journal.poltekanika.ac.id/index.php/inf/article/view/202/186
Scholar
GARUDA
GARBA RUJUKAN DIGITAL
JOURNAL HELP
USER
Username
Password
Remember me
Login
NOTIFICATIONS
View
Subscribe
LANGUAGE
Select Language
English
Submit
JOURNAL CONTENT
Search
Search Scope
All
jurnal.pdf
201-373-1-SM.pdf
jurnal.pdf
Show all
Type here to search
ENG
INTL
10:38
08/03/2021

IMPLEMENTASI PENGAMANAN DATA DAN INFORMASI DI BALAI DESA TANDING MARGA DENGAN METODE STEGANOGRAFI LSB DAN ALGORITMA KRIPTOGRAFI AES

Nurul Adha Oktarini Saputri[1], Novita Epa Sari[2]
Fakultas Ilmu Komputer,Teknik Informatika, Universitas Bina Darma
Email: nuruladhaos@binadarma.ac.id[1], novitaepasari@gmail.com[2]

ABSTRAK

Perkembangan teknologi informasi terutama pada sistem kerahasiaan dan keamanan data telah berkembang pesat. Kerahasiaan dan keamanan dalam komunikasi data merupakan suatu aspek yang penting. Dalam menjaga kerahasiaan dan keamanan suatu pesan yang akan dikirimkan, terlebih dahulu pesan disembunyikan atau di enkripsi didalam media citra. pada penelitian ini yang digunakan adalah citra digital dengan warna dengan kedalaman 24 bit. Penelitian ini bertujuan untuk membuat suatu sistem agar dapat meningkatkan kerahasiaan dan keamanan data yang berupa pesan-pesan penting. Steganografi *least significant bit* (lsb) digunakan untuk menyimpan pesan kedalam gambar. Dan algoritma kriptografi digunakan untuk mengunci/ mengenkripsi adalah algoritma aes. Lsb yang digunakan pada penelitian ini yakni dengan menyisipkan bit-bit *chiperteks* kedalam diagonal-diagonal pada matriks *pixel* komponen warna pada citra. Pada penelitian ini pengujian dilakuklan dengan cara melihat aspek-aspek *recorvery* pada metode *modified* Lsb danAES

Kata Kunci : steganografi, modified LSB, kriptografi, AES

I. PENDAHULUAN

Dalam penerapan sistem keamanan dan kerahasiaan suatu data pada Desa Tanding Marga masih terkendala oleh kurangnya pengetahuan mengenai betapa pentingnya menjaga kerahasiaan data yang dianggap penting, adapun permasalahan lainnya yaitu kurangnya fasilitas sistem untuk menjaga data ataupun informasi dari desa tersebut. Berdasarkan permasalahan yang ada peneliti akan membuat suatu sistem untuk mengamankan data penting yang ada pada Desa tanding Marga dengan menerapkan metode pengembangan sistem *Prototype* yaitu dengan melibatkan penggunanya langsung untuk ikut serta merancang sistem tersebut, dengan cara melakukan perancangan secara berualang hingga mencapai kesepakatan yang diinginkan, dan yang terakhir yaitu menggunakan sistem.

Penggunaan sistem tersebut terbagi menjadi dua yaitu satu untuk pengirim pesan agar dapat mengenkripsi pesan terlebih dahulu sebelum dikirimkan kepada penerima pesan dan yang kedua yaitu untuk penerima pesan agar bisa membaca pesan tersebut terlebih dahulu untuk mengekstrak pesan tersebut supaya bisa dibaca oleh penerima pesan. Dengan menggunakan metode steganografi LSB(Least Significant Bit) dan kriptografi AES(*Advanced Encryption Standard*).

Selain itu, sistem ini menggunakan citra (gambar) sebagai wadah penampung yang digunakan untuk menyisipkan pesan rahasia dengan cara pesan terlebih dahulu dienkripsi dan menjadi sebuah *chiperteks* dengan begitu tidak ada yang bisa membaca pesan tersebut kecuali penerima pesan, dengan cara mendeskripsikan pesan tersebut dengan *key* yang hanya diketahui oleh pengirim dan penerimanya saja.

Steganografi pada dasarnya berasal dari bahasa Yunani, dan terdiri dari 2 suku kata yaitu *steganos* yang berarti tersembunyi sedangkan *graphia* artinya tulisan. Dengan demikian, steganografi ialah ilmu atau seni yang digunakan untuk menyembunyikan pesan. adapun tujuan penyembunyian pesan tersebut yakni agar tidak diketahui oleh orang lain. Dan yang bisa mengetahuinya hanyalah pemilik pesan dan orang yang di percaya. Pada steganografi lsb ini akan membahas bagaimana cara untuk menyisipkan atau menyamarkan pesan[1].

Metode *least significant bit* (lsb) adalah salah satu teknik substitusi pada metodesteganografi. Pada lsb ini tiap bit yang terendah pada byte-byte citra digital akan segera digantikan dengan bit yang akan disisipkan pesan. Secara umum, pada steganografi terdapat dua proses yaitu penyisipan (*embeding*) pesan dan pengungkapan pesan (ekstraksi) [6].

Sejak tahun 1976, algoritma DES (*Data Encryption Standard*) telah dipilih sebagai standar kriptografi ole pemerintah Amerika Serikat. Namun pada tahun 1990 , kunci pada DES dianggap masih terlalu pendek, dan kemudian pada tahun 1998 dalam waktu 96 hari DES berhasil dipecahkan., dan pada tahun 1999 dalam waktu 22 hari dapat dipecahkan kembali. Oleh karena itu maka NIST (*National of Standard and Technology*) mengadakan kompetisi agar mencari pengganti des. Peserta yang berpartisipasi berasal dari seluruh dunia yang digunakan oleh Nist.[1].

Kriptografy berasal daribahasa Yunani yaitu *cryptos* (*secret*) dan juga *graphia (writing)*. Dengan demikian kriptografi artinya *secret writing* atau tulisan rahasia[1].

Dengan dikombinasikannya algoritma steganografi LSB dan kriptografi AES akan meningkatkan kualitas keamanan data. Dari penjelasan diatas peneliti bertujuan agar menerapkan kedua metode steganografi dan kriptografi pada pesan yang nantinya akan menjadi target keamanan.

II. TINJAUAN PUSTAKA

2.1 Steganografi LSB (*Least Significant Bit*)

Ilmu atau seni yang digunakan untuk menyembunyikan pesan di sebut steganografi. Adapun tujuan yang ingin dicapai dengan menerapkan steganografi ialah agar pesan yang rahasia tidak diketahui oleh orang lain. Adapun yang dapat mengetahuinya adalah pemilik pesan dan orang yang diinginkannya.[1]

Teknik substiusi yang digunakan pada metode steganografi ialah metode LSB. tiap bit yang terendah pada byte-byte citra digital, akan segera digantikan dengan bitpesan yang akan disisipkan. Pada citra memiliki susunan tiga warna yaitu merah, hijau dan biru (RGB) yang didalamnya terdapat susunan 8 bit (1 byte) dari 0 sampai 255 atau dalam

format binner 00000000 sampai 11111111.

Metode lsb merupakan steganografi yang paling sederhana dan mudah diimplementasikan.

Metode ini menggunakan citra digital sebagai *covertext* dalam susunan bit pada sebuat byte (1 byte – 8 bit). bit yang paling depan di sebut *most significant bit (msb)* dan bit yang paling akhir di sebut *least significant bit (lsb)*[6].

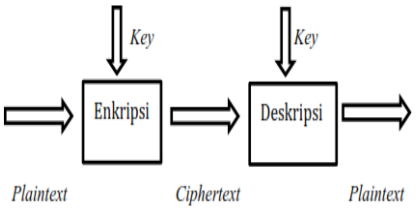
2.2 Algoritma KriptografiAES

Kriptografi adalah cara yang paling efektif untuk digunakan dalam informasi- informasi penting baik yang ditramisikan dalam jaringan komunikasi dan yang tersimpan dalam media peyimpinan. Kriptografer adalah sebutan untuk orang yang melakukan penyandian sedangkan kriptanalis adalah orang yang mendalami ilmu dan seni atau orang yang bisa memecahkan algoritmanya tanpa perlu mengetahuikuncinya.[1].

Ilmu dan seniyang digunakan untuk menjaga pesan rahasia dengan cara menyandikannya kedalam bentuk yang tidak mudah lagi di mengerti adalah pengertian dari kriptografi. dan dalam kriptografi juga terdiri dari duaproses yakni prosesenkripsi dan deskripsi. Proses penyandian pesan dari yang terbuka menjadi pesan rahasia (*chipertext*) adalah arti dari enkripsi. *chipertext inilah* yang nantinya dikirimkan melalui saluran komunikasi.[1].

Chipertext yang diterima oleh penerima pesan, akan diubah lagi menjadi pesan terbuka yang melalui proses enkripsi sehingga pesan dapat dibaca kembali oleh penerima pesan[1].

Secara umum, proses enkripsi dan proses deskripsi akan digambarkan dibawah ini



Gambar 1. Proses enkripsi dan deskripsi

2.3 Citra Digital

Sederetan atau sekumpulan pixel (*picture element*) adalah semua citra digital yang ditampilkan pada layar komputer. Citra digital dapat dikatakan sebagai citra digital akan bentuk representasinya yang berupa bilangan oleh komputer akan dikenaldalam urutan ‘0’ dan ‘1’. Format pada citra digital diantaranya *bmp, png, jpg, gif, pxc*, dan lainya. Adapun perbedaanya dengan yang lain terdapad pada *header file*-nya[1].

2.4 PHP

PHP singkatan *Hypertext Preprocessor* yaitu bahasa pemograman *web server-side* yang bersifat *open source*. PHP merupakan *script* yang akan berintegrasi dengan HTML danakan berada pada server (*server side* HTML*embedded scripting*). *Script* yang digunakan untuk membuat halaman web dinamis adalah PHP. Halam yang akan di tampilkan akan dibuat pada saat halaman itu diminta oleh *client* di sebut dinamis [2].

2.5 MYSQL

MYSQL*(My Structure Query Language*) adalah salah satujenis *database server* yang sangat terkenal dan banyak digunakan untuk

membangun aplikasi *web* yang menggunakan *database* sebagai sumber dan pengelolaan datanya. MYSQL bersifat *open source* dan menggunakan sql (*structure query language*). MYSQL biasanya dijalankan si berbagai *platform* misalnya *windows, linux* dan sebagainya [2.]

2.6 UML

Salah satu dari standar yang banyak digunakan pada dunia *industry* untuk membuat desain dan menggambarkan arsitektur serta untuk menganalisis dalam pemograman berorientasi objek merupakan pengertian dari UML (*Unified Modeling Language*). Beberapa element grafis yang dimiliki oleh UML yang bisa dikombinasikan dengan beberapa aspek dari sebuah sistem. UML terdiri dari abstraksi dari *structural classification, dynamic bhavior,* dan model *management*[2].

III. METODOLOGI PENELITIAN

3.1 Metode Pengumpulan Data

Pada penelitian ini peneliti menggunakan metode pengumpulan data sebagai berikut :

1. Observasi

Observasi dilakuan untuk tujuan pengumpulan data dengan cara berinteraksi secara langsung dengan datang ketempat yang akan menjadi objek penelitian, dan bertatap langsung dengan Kepala Desa Tanding Marga untuk mencatat atau merekam setiap peristiwa/kejadian dengan tujuan ilmiah ataupun lainnya dengan bantuanalat.[9]

2. Wawancara

Wawancara dilakukan sebagai proses komunikasi dengan cara bertanya langsung kepada narasumber terkait untuk mendapatkan informasi yang akurat dan terpercaya sebagai sebuah acuan untuk dijadikan bahan penelitian. Pertanyaan bersifart serius dengan tujuan yang telah ditetapkan agar mendapatkan informasi sesuai keinginanpeneliti.[3]

3. Studipustaka

Studi pustaka dimaksudkan agar mendapatkan wawasan yang lebih mendalam untuk menganalisa setiap permasalahan dengan cara menelaah setiap sumber yang tertulis dari berbagai pendapat para ahli yang ada didalam buku ataupun jurnal dan lain sebagainya, untuk menunjang pengumpulan data dalam mengkaji setiap permasalahan yang sedang diteliti.[5]

3.2 Metode Pengembangan Sistem

Pada pengembangan sistem kali ini peneliti menggunakan metode *prototype* . yang akan dimulai dengan pengumpulan kebutuhan *user*, stelah itu membuat *prototype* yang akan di bangun, kemudian pengevaluasian oleh *user* pada *Prototype,* dan akan digunakan untuk mendefinisikan apa yang dibutuhkan untuk pengembangan perangkat lunak[11].

Pada *prototyping* ada beberapa tahap yakni sebagai berikut :

1) PengumpulanKebutuhan

Pelanggan dan pengembang awalnya akan bersama-sama untuk mendefinisikan seluruh format perangkat lunak, kemudian mengidentifikasikan semua yang dibutuhkan dan garis sistem yang akan di bangun

2) Membangun*prototyping*

Membuat perancangan sistem sementara dan berfokus pada penyajian untuk pengguna merupakan cara membangun *prototype.*

3) Evaluasi*Prototyping*

Tahap ini akan mengevaluasi apakah rancangan *prototyping* yang di buat sudah sesuai dengan yang diinginkan. Jika telah sesuai maka langkah ke 4 bisa diambil, dan jika belum sesuai maka *prototyping* akan di ulang kembali ke langkah 1,2, dan3.

4) MengkodekanSistem

Pada tahap ini, *prototyping* yang telah sesuai akan di terapkan kedalam bahasa pemograman yang disepakati.

5) Menguji Sistem

Sistem yang sudah menjadi suatu perangkat lunak, dan siap di pakai. Maka harus diuji terlebih dahulu sebelum digunakan. Adapun pengujian yang akan dilakukan yaitu dengan cara *white box, black-box, basic path,* pengujian arsitektur, dan lain sebagainya.

6) Evaluasi Sistem

Pengevaluasian sistem dilakukan oleh pengguna apakah sistem telah sesuai dengan yang di inginkan. Apabila telah sesuai maka selanjutnya langkah 7 akan diambil.

7) Menggunakan Sistem

Perangkat lunak yang telah diuji dan telah sesuai kemudian diterima oleh pengguna siap untuk digunakan. Setelah melalui tahapan-tahapan pembangunan *prototyping*, dapat dilanjutkan dengan tujuan yang ingin dicapai dengan adanya *prototyping* tersebut.[11]

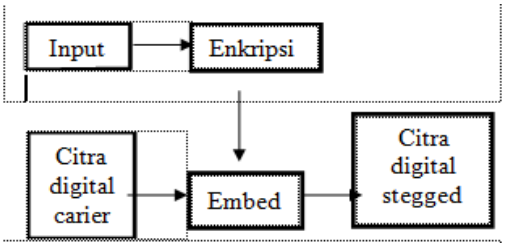
IV. HASIL DAN PEMBAHASAN

4.1 Analisis Sistem

Secara umum pada steganografi terdapat dua proses yaitu proses penyisipan (*embed*) dan pengungkapan (ekstrak).

a. Proses *Embedding*Pesan

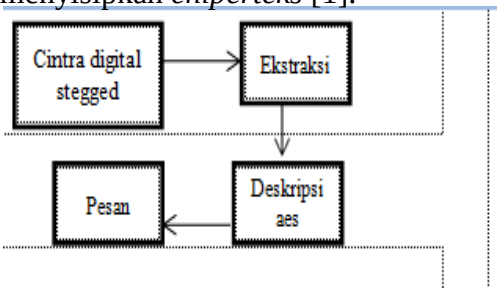
Tahapan yang dilakukan dalam proses penyisipan (*embeding*) yakni dimulai dari enkripsi aes yang mentranformasikan pesan asli (*plaintekx*) yang kan menjadi pesan acak (*chiperteks*), selanjunya *embedding* dalam *citra digital* pembawa (*carrier*). Untuk ilustrasi akan dijelaskan dibawah ini [1].



Gambar 2. proses embedding

b. Proses EkstraksiPesan

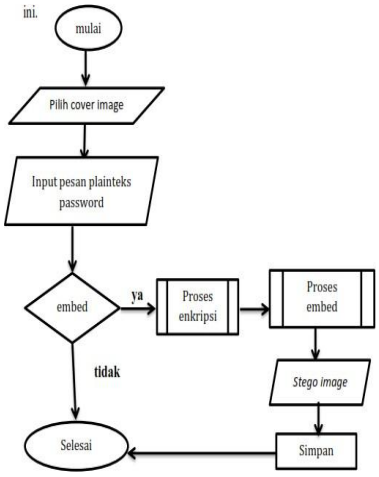
Untuk menyisipkan *chipertext* ke dalam *cover image* dapat dilakukan dengan penyembunyian pesan dengan menggunakan *modified* LSB yang akan menggantikan *diagonal byte* untuk menyisipkan *chiperteks* [1].



Gambar 3. proses pada ekstraksi

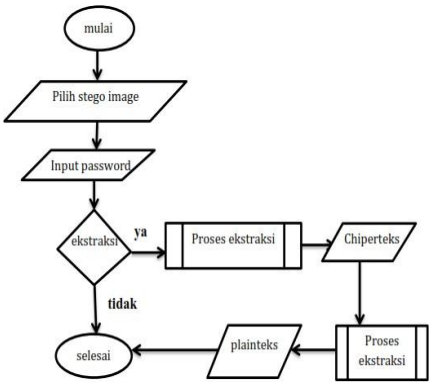
4.2 Perancangan Sistem

Proses penyisipan (*embedding*) yaitu dengan cara memilih *cover objek* yangtelah ditentukan untuk disisipkan pesan. untuk lebih jelas perhatikan gambar di bawah ini. [1].



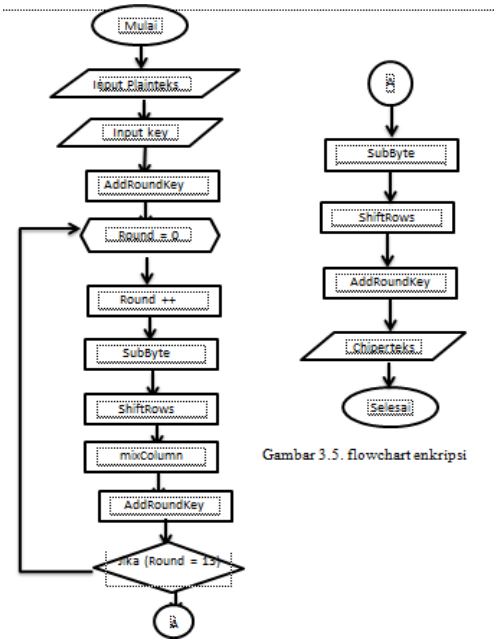
Gambar 4. Flowchart proses embedding

Kemudian melakukan proses ekstraksi. Pertama masukkan kembali *stego image* yang telah disisipkan pesan, tujuannya agar dapat membaca kembali pesan yang tersembunyi dalam gambar.[1].



Gambar 5. Flowchart proses ekstrak

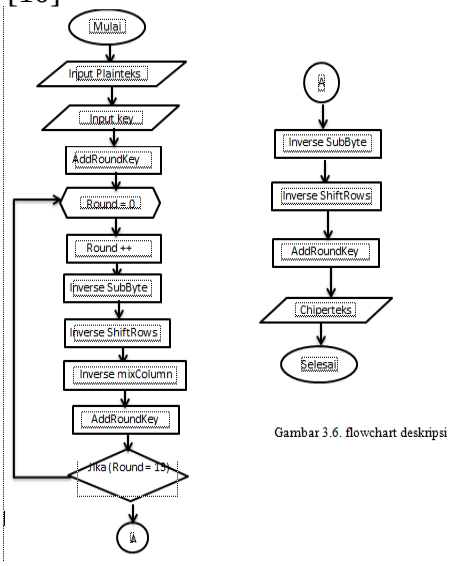
Dan dalam metode algoritma kriptografi aes terdapat prosesenkripsi dan deskripsi. Proses enkripsi yang terdiri dari 4 tahapan tranformasi *byte*, yakni *SubBytes*, *ShiftRows*, *Mixcolumns*, dam *AddRoundKey*. Dalam proses enkripsi pesan yang telah di inputkan dalam *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Secara berulang-ulang kali sebanyak Nr. Dalam algoritma aes di sebut *round function*. *State* yang tidak mengalami transformasi *MixColumns* adalah *round* yang terakhir. Dibawah ini adalah ilustrasiaes[10].



Gambar 3.5. flowchart enkripsi

Gambar 6. Flowchart Enskripsi

Selanjutnya adalah Transformasi *chipper* yang kebalikan dari enkripsi. untuk menghasilkan *invers chiper* yang mudahan untuk algoritma AES. Transformasi *Byte* yang digunakan pada *invers chipper* adalah *InvShifftRows*, *InvSubBytes*, *InvMixColumns* dan *AddRoundKey*. [10]



Gambar 3.6. flowchart deskripsi

Gambar 7. Flowchart Deskripsi

4.3 Implementasi Sistem

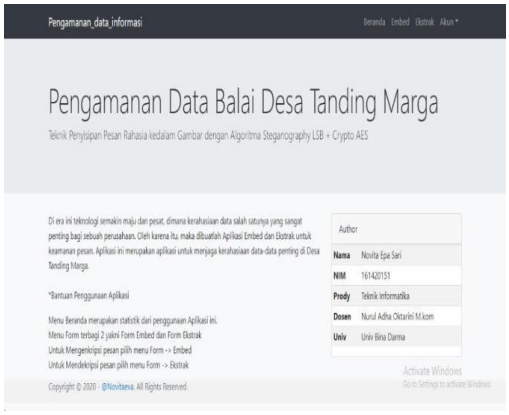
Implementasi Antar MukaSistem

Pada proses implementasi sistem peneliti menggunakan *microsoft visual studio* yang digunakan sebagai *tools* untuk menerapkan steganografi dan Kriptografi deangan menggunakan bahasa pemograman PHP. *Coding*fungsi diterapkan dan diintegrasikan kedalam GUI (*graphical user interface*).

Implementasi dari semua tahapan analisis dan perancangan dari tampilan antar muka dapat dilihat sebagai berikut :

1. Tampilan Halaman Beranda

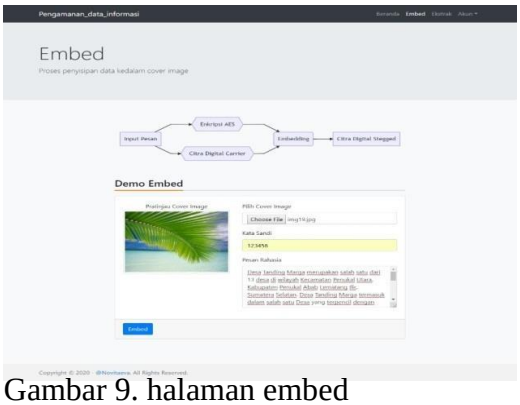
Halaman beranda adalah halaman utama sebelum melakukan penyisipan pesan.



Gambar 8. halaman beranda

2. Tampilan Halaman *Embed*

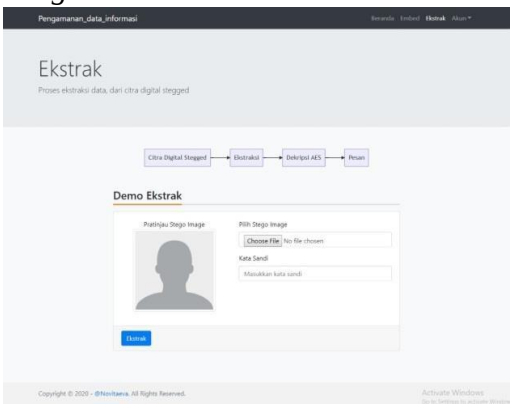
Halaman embed adalah halaman untuk menyisipkan pesan rahasia kedalam *cover objek* yaitu *citra digital* dan merupakan halaman yang berperan penting pada sistem ini karena sistem tidak akan bekerja jika tidak ada halamanembed.



Gambar 9. halaman embed

3.Tampilan HalamanEkstrak

Pada halaman ekstrak inilah pesan yang tadinya tersembunyi dalam *stego image* bisa dibaca kembali

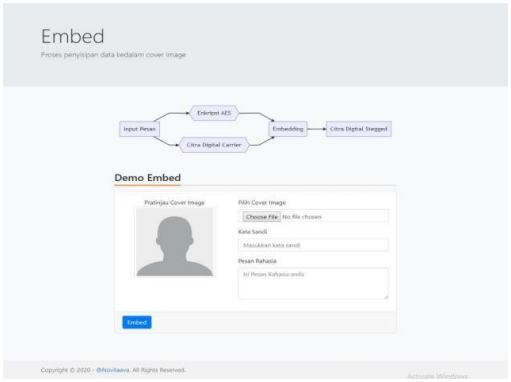


Gambar 10. halaman ekstrak

4.4 Pembahasan Sistem

1. Halaman Proses *embedding* (penyisipan)

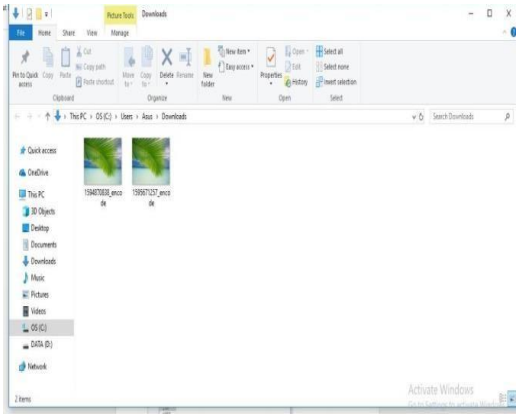
Pada proses *embeduser* diminta untuk memasukkan *image cover* sebagai media penyimpanan pesan kemudian user memasukkan kata sandi dan memasukkan data yang berupa teks yang memiliki jumlah kata maksimum 244800 bytes dengan cara meng*copy*kan *file* teks kedalam *form* pesan rahasia dan kemudian mengklik tombol *embed*.Jika teks rahasia melebihi kapasitas maka sistem akan*error*.



Gambar 11. proses embed

2. Halaman Hasil *embedding* (penyisipan)

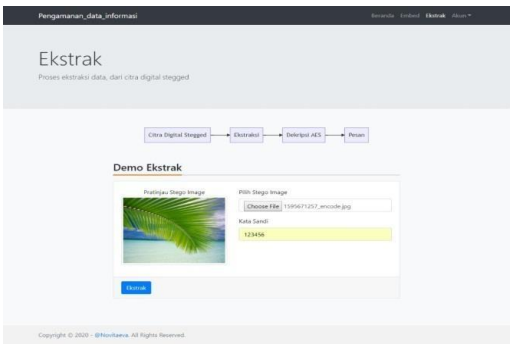
Pesan yang sudah tersisipkan dalamsebuah *stego image* kemudian secara otomatis akan tersimpan pada folder*download* didalam *computer user*, dan sulit dibedakan oleh indra manusia karena tidak ada perbedaan yangterlihat**.**



Gambar 12. hasil embed

3. Halaman ProsesEkstraksi

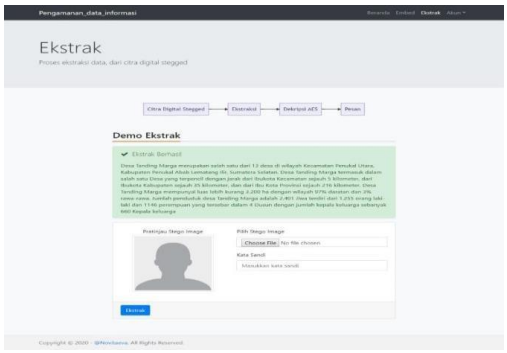
Halaman proses ekstrak ini akan menjelaskan bagaimana proses deskripsi pesan yang tersembunyi, dengan cara menginput kembali *stego image* dalam menu ekstrak dan memasukkan kata sandi yang telah dibuat pada halaman *embed* dan kemudian mengklik tombol ekstrak.



Gambar 13. proses ekstraksi

4. Hasil Ekstraksi

Pada halaman inilah hasil dari pengekstrakan pesan dan *user* bisa membaca kembali pesan yang telah tersimpan didalam *stego image* menjadi pesan teks biasa .dan siapun bisa membacanya karena tidak tersembunyi didalam citra digital lagi.



Gambar 14. hasil ekstraksi

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah semua percobaan sudah dilakukan, maka kesimpulannya adalah implementasi dengan metode steganografi lsb dan algoritma kriptografi aes bisa dibilang berhasil. Dan Pengujianpun telah dilakukan pada beberapa contoh dan dapat membuktikan jika metode modified LSB telah sesuai seperti yang di rencanakan. Dimana pesan rahasia yang tersimpan dalam citra digital susah untuk dibedakan oleh penglihatan . ini disebabkan karena tidak adanya perbedaan atau

perubahan yang terlihat pada *stego image*. Kecepatan proses enkripsi dan *embed* pada pesan tergantung seberapa besar ukurannya.

5.2 Saran

Untuk saran kedepannya pada sistem keamanan ini diharapkan untuk :

1. Diharapkan kedepannya bisa mengamankan pesan yang berbentuk *file word* agar bisa lebih efektif, dan efisien agar lebih mudah dan tidak perlu meng*copy*kan isi *file* kedalam *form* pesan rahasi pada menu*embed*.
2. Diharapkan untuk membuat sistem keamanan yang berbasis android agar lebih mudah untukdigunakan.

DAFTAR PUSTAKA

Anwar, S. (2017). *Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES*. *6*, 65–74.

fridayanthie, eka wida; M. (2016). *Rancang* Bangung Sistem Informasi Permintaan ATK Berbasis Intranet (Studi Kasus : Kejaksaan Negeri RangkasBitung)*IV*(2), 126–138.

Hakim, L. N. (2013). *ULASAN METODOLOGI KUALITATIF: WAWANCARA TERHADAP ELIT*

Review of Qualitative Method : Interview of the Elite. 165–172.

Heriyanto Yunahar. (2018). *Perancangan Sistem Informasi Rental Mobil Berbasis Web Pada PT. APM rent Car*. *2*(2), 64– 77.

Margareta, S. (1989). *Shinta Margareta, 2013 Hubungan Pelaksanaan Sistem Kearsipan Dengan Efektivitas Pengambilan Keputusan Pimpinan Universitas Pendidikan Indonesia | repository.upi.edu*.

Novianto, D., & Setiawan, Y. (2018). Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Ilmiah Informatika Global*, *9*(2), 83–89.

Swara, & Pebriadi, Y. (2016). Rekayasa Perangkat Lunak Pemesanan Tiket Bioskop. *Urnal TEKNOIF*, *4*(2), 27–39.

Wulan, R. (2016). *IMPLEMENTASI MODEL PROTOTYPING INFRASTRUKTUR DAN JARINGAN PADA SMK KESATUAN CENGKARENG JAKARTA BARAT*. *9*(4), 333–340.

SURAT KETERANGAN

Nomor: 004/SK/LPPM-UBD/III/2021

Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Bina Darma menerangkan bahwa :

No	Nama	Jabatan
1	Nurul Adha Oktarini Saputri, M.Kom.	Dosen Program Studi Teknik Informatika

Adalah benar telah dipublikasikan artikel atau paper karya ilmiah dengan judul daftar terlampir.

Palembang, 24 Maret 2021
Kepala LPPM,

Darius Antoni, S.Kom., M.M., Ph.D
NIP. 030110199

Lampiran Nomor surat: 004/SK/LPPM-UBD/III/2021

DAFTAR JUDUL ARTIKEL ILMIAH

No.	Karya Ilmiah	Judul	Identitas Karya Ilmiah (ISBN/ISSN/Edisi/TahunTerbit/Penerbit)	Alamat Unggah Online
1	Jurnal	ANALISIS SENTIMEN MASYARAKAT TERHADAP PILPRES 2019 BERDASARKAN OPINI DARI TWITTER MENGGUNAKAN METODE NAIVE BAYES CLASSIFIER	JURNAL INFORMANIKA. P-ISSN: 2407-1730, E-ISSN: 2775-5762. VOL.7 NO.01 JANUARI-JUNI 2021. Manajemen Informatika, Politeknik Anika Palembang. Jurnal Nasional Tidak Terakreditasi	http://journal.poltekanika.ac.id/index.php/inf/article/view/201/185
2	Jurnal	IMPLEMENTASI PENGAMANAN DATA DAN INFORMASI DI BALAI DESA TANDING MARGA DENGAN METODE STEGANOGRAFI LSB DAN ALGORITMA KRIPTOGRAFI AES	JURNAL INFORMANIKA. P-ISSN: 2407-1730, E-ISSN: 2775-5762. VOL.7 NO.01 JANUARI-JUNI 2021. Manajemen Informatika, Politeknik Anika Palembang. Jurnal Nasional Tidak Terakreditasi	http://journal.poltekanika.ac.id/index.php/inf/article/view/202/186

Kepala LPPM

Darius Antoni, S.Kom., M.M., Ph.D
NIP. 030110199