PROSIDING

SEMINAR NASIONAL METODE KUANTITATIF

SNMK 2017

PENGGUNAAN MATEMATIKA, STATISTIKA,
DAN KOMPUTER DALAM BERBAGAIDISIPLIN ILMU
UNTUK MEWUJUDKAN KEMAKMURAN BANGSA

LEMBAGA PENELITIAN DAN PENGABDIAN MASYARAKAT

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS LAMPUNG

SEMINAR NASIONAL
METODE KUANTITATIF
2017

PROSIDING
Seminar Nasional
Metode Kuantitatif 2017

ISBN No. 978-602-98559-3-7

Penggunaan Matematika, Statistika, dan Komputer dalam Berbagai Disiplin Ilmu
untuk Mewujudkan Kemakmuran Bangsa

Editor :
Prof. Mustofa Usman, Ph.D
Dra. Wamiliana, M.A., Ph.D.

Layout & Design :
Shela Malinda Tampubolon

Alamat :
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Lampung, Bandar Lampung
Jl. Prof. Dr. Sumantri Brojonegoro No. 1 Bandar Lampung
Telp. 0721-701609/Fax. 0721-702767

KATA SAMBUTAN
KETUA PELAKSANA
SEMINAR NASIONAL METODE KUANTITATIF 2017

Seminar Nasional Metode Kuantitatif 2017 diselenggarakan oleh Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam (FMIPA) Universitas Lampung yang dilaksanakan pada tanggal 24 – 25 November 2017. Seminar terselenggara atas kerja sama Jurusan Matematika FMIPA, Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Unila, dan Badan Pusat Statistik (BPS).

Peserta dari Seminar dihadiri lebih dari 160 peserta dari 11 institusi di Indonesia, diantaranya : Kementrian Pendidikan dan Kebudayaan, Badan Pusat Statistik, Universitas Indonesia, Institut Teknologi Bandung, Universitas Sriwijaya, Universitas Jember, Universitas Islam Negeri Sunan Gunung Djati, Universitas Cendrawasih, Universitas Teknokrat Indonesia, Universitas Malahayati, dan Universitas Lampung. Dengan jumlah artikel yang disajikan ada sebanyak 48 artikel hal ini merefleksikan pentingnya seminar nasional metode kuantitatif dengan tema "pengunaan matematika, statistika dan computer dalam berbagai disiplin ilmu untuk mewujudkan kemakmuran bangsa".

Kami berharap seminar ini menjadi tempat untuk para dosen dan mahasiswa untuk berbagi pengalaman dan membangun kerjasama antar ilmuan. Seminar semacam ini tentu mempunyai pengaruh yang positif pada iklim akademik khususnya di Unila.

Atas nama panitia, kami mengucapkan banyak terima kasih kepada Rektor, ketua LPPM Unila, dan Dekan FMIPA Unila serta ketua jurusan matematika FMIPA Unila dan semua panitia yang telah bekerja keras untuk suksesnya penyelenggaraan seminar ini.

Dan semoga seminar ini dapat menjadi agenda tahunan bagi jurusan matematika FMIPA Unila`

Bandar Lampung, Desember 2017

Prof. Mustofa Usman,Ph.D

Ketua Pelaksana

KEPANITIAAN

Penasehat : 1. Prof. Dr. Hasriadi Mat Akin, M.P
2. Prof. Dr. Bujang Rahman
3. Prof. Dr. Ir. Kamal, M.Sc
4. Ir. Warsono, M.Sc., Ph.D
5. Dr. Hartoyo, M.Si

Pengarah : 1. Prof. Warsito, S.Si., DEA, Ph.D
2. Prof. Dr. Sutopo Hadi, S.Si., M.Sc
3. Dian Kurniasari S.Si., M.Sc
4. Drs. Suratman Umar, M.Sc.

Penanggung Jawab : Dra. Wamiliana, M.A., Ph.D

Ketua Pelaksana : Prof. Drs. Mustofa, M.A., Ph.D

Sekretaris : Dra. Dorrah Aziz, M.Si

Bendahara : Amanto, S.Si., M.Sc

Kesekretariatan : Subian Saidi, S.Si., M.Si
Dr. Notiragayu, M.Si
- Syamsu Huda, S.I.P., M.M
- Srimiati, S.Pd
- Johan, S.P
- Riendi Ferdian, S.I.P
- Siti Marbiyah, S.Si
- Rosihin Anwar, S.Kom
- Shela Malinda T
- Della Desiyana
- Nandra Adi Prayoga
- Himatika

Seksi-seksi :

Acara : Dr. Aang Nuryaman, M.Si
Dr. Khoirin Nisa, M.Si
Drs. Rudi Ruswandi, M.Si

Drs. Eri Setiawan, M.Si

Konsumsi : Widiarti S.Si., M.Si
Dr. Asmiati, M.Si

Transportasi/akomodasi : Drs. Nusyirwan, M.Si
Agus Sutrisno, S.Si., M.Si

Perlengkapan : Drs. Tiryono R., M.Sc., Ph.D
- Agus Suroso, A.Md
- Tamrinsyah
- Supriyadi
- Drajat
- Maeda Sulistiana

Reviewer : Drs. Suharsono, M.Sc., Ph.D
- Dr. La Zakaria S.Si., M.Sc
- Dr. Muslim Ansori, S.Si., M.Si
- Dr. Ir. Netti Herawati, M.Sc

DAFTAR ISI

ISBN No. 978-602-98559-3-7

Proses Pengamanan Data Menggunakan Kombinasi Metode Kriptografi *Data Encryption Standard* dan Steganografi *End Of File*

Dedi Darwis[*1) **1)], Wamiliana[2)], Akmal Junaidi[3)]
[*1)] Program Studi Sistem Informasi, Universitas Teknokrat Indonesia
[**1)] Mahasiswa S3 Doktor Ilmu MIPA, Universitas Lampung
E-mail : darwisdedi@teknokrat.ac.id
[2)] Jurusan Matematika, FMIPA, Universitas Lampung
3) Jurusan Ilmu Komputer, FMIPA, Universitas Lampung
E-mail : wamiliana.1963@unila.ac.id

ABSTRAK

Metode Data Encrytption Standard (DES) merupakan salah satu metode Kriptografi yang dapat digunakan sebagai alternatif pengamanan data seperti keamanan password, keamanan jaringan ataupun pengiriman pesan rahasia dalam pertukaran informasi, namun hasil kriptografi hanya dalam bentuk kode penyandian kata sehingga menimbulkan kecurigaan orang lain untuk memecahkan kode penyandian tersebut. Pada penelitian ini dikembangkan kombinasi kriptografi yang lebih aman sehingga pesan rahasia dalam bentuk hasil enkripsi yang akan dikirim disisipkan terlebih dahulu ke media digital seperti image dan media lainnya yang disebut teknik steganografi, sehingga pihak lain tidak akan curiga bahwa dalam media digital tersebut terdapat pesan rahasia. Metode yang digunakan dalam penelitian ini untuk steganografi adalah End Of File (EOF) karena metode ini mampu mempertahankan kualitas citra yang baik karena antara cover image dan stego image memiliki kemiripan yang signifikan sehingga tidak menimbulkan kecurigaan. Berdasarkan hasil pengujian yang dilakukan pesan rahasia berhasil dienkripsi dengan menggunakan panjang kunci 56 bit kemudian disisipkan pada citra digital menggunakan EOF dan memiliki hasil pengujian bahwa pesan yang disisipan dapat diambil kembali untuk dapat dilakukan proses dekripsi.

Kata kunci: EOF, DES, Kriptografi, Steganografi

1. PENDAHULUAN

Data dan Informasi merupakan hal yang sangat penting untuk dijaga keamanannya atau kerahasiannya agar pihak-pihak yang tidak berkompeten terhadap data tersebut misalkan Laporan Keuangan, keamanan password, dan keamanan jaringan ataupun data-data penting lainnya. Salah satu cara untuk mengamankan data adalah menggunakan teknik Kriptografi yaitu ilmu yang mempelajari teknik – teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data,serta otentikasi[1]. Pada implementasinya banyak sekali metode kriptografi yang dapat digunakan, dari mulai kriptografi klasik sampai kriptografi modern. Salah satu metode yang cukup populer adalah *Data Encryption Standard* (DES) karena dapat mengatasi masalah-masalah yang terjadi seperti pencurian data, penyalahgunaan data, dan kerahasiaan data[2]. Namun saat ini penggunaan teknik kriptografi masih belum cukup dalam melakukan proses pengamanan data karena masih menimbulkan kecurigaan karena teks yang disandikan masih terlihat walaupun dalam bentuk-bentuk simbol-simbol sehingga membuat orang lain ingin memecahkan sandi tersebut, maka dari itu diperlukan teknik lain yang dapat dikombinasikan dengan teknik kriptografi.

Salah satu teknik yang dapat dikombinasikan adalah steganografi yang merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi rahasia di dalam suatu informasi lainya[3]. Sama halnya seperti kriptografi, steganografi juga memiliki banyak metode yang dapat digunakan, salah satunya adalah metode *End Of File (EOF)* di mana metode ini berfokus pada ukuran suatu citra digital untuk menyisipkan pesan pada *file* yang terakhir. Pada metode *End Of File*, data yang telah dienkripsi akan disisipkan pada nilai akhir file gambar, sehingga hanya menambah ukuran file dan terdapat penambahan garis-garis pada bagian bawah file gambar tersebut sehingga tidak banyak merubah kualitas citra aslinya[4].

Pada penelitian ini akan dilakukan kombinasi dengan menggabungkan teknik kriptografi menggunakan metode *Data Encryption Standard* dan teknik steganografi *End Of File* dengan cara informasi rahasia dalam bentuk *text* dienkripsi terlebih dahulu, lalu hasil enkripsi akan dimasukkan ke dalam sebuah citra digital menggunakan format *JPEG*. Diharapkan dengan penggabungan dua metode ini dapat meningkatkan keamanan data pada pesan-pesan rahasia sehingga pihak yang tidak berkompeten tidak akan dapat mengetahui kerahasiaan informasi yang disimpan.

2. LANDASAN TEORI

2.1 Tinjauan Pustaka

1. Pada [5] digunakan Algoritma *Data Encryption Standard (DES)* dan dibangun menggunakan bahasa pemrograman Java untuk menerapkan metode DES dengan kunci simetri sepanjang 64 bit. Hasil dari penelitian ini adalah dengan adanya aplikasi kriptografi yang dikembangkan berdasarkan algoritma DES, maka data-data penting dapat diamankan (dienkripsi) ketika hendak dikirim melalui media internet [5].
2. Pada [2] masalah diterapkan Algoritma DES pada keamanan data pesan text dilakukan dengan cara permutasi pada blok plainteks permutasi awal kemudian di-*enciphering* sebanyak 16 kali putaran serta dalam merancang keamanan data pesan teks dilakukan perancangan input, proses, *output* dan salah satunya dapat melakukan program *visual basic 6.0* dan dapat melakukan *initial permutation* kemudian dipermutasikan dengan matriks permutasi balikan (*invers initial permutation*) menjadi blok *Cipertext*.
3. Pada [6] digunakan. Metode *End Of File* untuk menyembunyikan pesan rahasia ke dalam citra digital dengan format ekstensi berupa Jpg dan selanjutnya pesan akan disisipkan pada file terakhir pada sebuah citra, dengan metode ini ukuran file jumlahnya tidak terbatas. Hasil dari penelitian ini menunjukkan bahwa pesan teks yang disisipkan ke dalam file citra dapat diambil kembali dari citra tersebut, kemudian berdasarkan pengujian yang dilakukan Pengujian *imperectibility* memberikan hasil steganografi pada gambar, dengan metode kuesioner yang menghasilkan 70% mahasiswa dibidang komputer tidak mengetahui tentang Steganografi dan 100% menyatakan gambar hasil steganografi tidak dapat terlihat oleh indra mata manusia secara kasat mata. Pada proses pengujian tahap fidelity tidak nampak nilai MSE yang hanya menghasilkan nilai "0" dan PSNR menghasilkan nilai "∞" (tak hingga) dikarenakan metode yang digunakan menyisipkan pesan di akhir file tanpa merubah nilai intensitas warna pikselnya dan Pembuatan aplikasi steganografi dapat diterapkan dan dijalankan dengan *mobile smartphone android*.
4. Pada [4] metode *Cryptosystem* digunakan untuk mengenkripsi data atau pesan rahasia yang berupa teks angka dengan jumlah maksimum yang dimasukkan adalah 24 digit angka kemudian hasil enkripsi *(Cipertext)* akan disembunyikan ke dalam suatu file gambar yang berformat bitmap dengan ukuran minimum 25x25. Selanjutnya, dilakukan proses ekstraksi dan dekripsi *Cipertext*, sehingga diperoleh kembali *Plaintext* yang berupa data teks angka. Hasil pengujian menunjukkan Algoritma Rabin Public Key tidak aman untuk serangan chosen-*Cipertext* attack karena untuk kombinasi *Plaintext* dan kunci yang merupakan angka kelipatan "11" akan menghasilkan *Cipertext* yang

merupakan angka kelipatan "11" juga. Sehingga, seorang kriptanalis dapat mengetahui bentuk *Plaintext* yang sebenarnya. sedangkan pada metode *End Of File*, data yang telah dienkripsi akan disisipkan pada nilai akhir file gambar, sehingga akan menambah ukuran file dan terdapat penambahan garis-garis pada bagian bawah file gambar tersebut.

2.2 Konsep Kriptografi

Kriptografi yaitu berasal dari bahasa yunani, *Crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain[7].

Algoritma dalam kriptografi di bagi menjadi dua, yaitu :[7]

1. Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses deskripsi. Adapun contoh algoritma kunci simetris adalah DES (*Data Encryption Standard*), Blowfish, Twofish, MARS, IDEA, 3DES (DES diaplikasikan 3 kali), AES(*Advanced Encryption Standard*) yang bernama asli Rijndael, *Vigenere* , dan lain - lain.
2. Algoritma asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan deskripsi. Adapun contoh algoritma yang menggunakan kunci asimetris adalah RSA (*Riverst Shamir Adleman*) dan ECC (*Elliptic Curve Cryptography).*

2.3 Algoritma *Data Encryption Standard*

Standar Enkripsi Data (*Data Encryption Standard* – DES) merupakan algoritma enkripsi yang paling banyak dipakai di dunia, yang diadopsi oleh NIST (*National Institute of Standards and Technology*) sebagai standar pengolahan informasi Federal AS. Secara umum standar enkripsi data terbagi menjadi tiga kelompok yaitu pemrosesan kunci, enkripsi data 64 bit dan dekripsi data 64 bit yang mana satu kelompok saling berinteraksi satu sama lain[7].

Pada akhir 1960 IBM memulai riset proyek *Lucifer* yang dipimpin oleh Horst Feistel untuk kriptografi komputer. Proyek ini berakhir tahun 1971 dan *Lucifer* pertama kali dikenal sebagai blok kode pada pengoperasian blok 64 bit dan menggunakan ukuran kunci 128 bit. Setelah IBM mengembangkan sistem enkripsi yang dikomersilkan maka *Lucifer* disebut dengan DES (*Data Encryption Standard*).Proyek ini dipimpin olehWalter Tuchman.Hasil dari riset ini merupakan versi *Lucifer* yang bersifat menentang pemecahan algoritma kriptografi.

DES merupakan sistem kriptografi simetri dan tergolong jenis blok kode. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit teks asli menjadi 64 bit teks kode dengan menggunakan 56 bit kunci internal (*internal key*) atau upa-kunci (*subkey*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit[7].

Skema global dari algoritma DES adalah sebagai berikut :

1. Blok teks-asli dipermutasi dengan matrik permutasi awal (*initial permutatiaon* atau IP). Bisa ditulis x0 = IP (x) = *L*0*R*0, dimana *L*0 terdiri dari 32 bit pertama dari x0 dan 32 bit terakhir dari *R*0.
2. Hasil permutasi awal kemudian di-*enciphering* sebanyak 16 kali (16 putaran). Setiap putaranmenggunakan kunci internal yang berbedadengan perhitngan *LiRi* $1 \leq i \leq 16$, dengan mengikuti aturan $Li = Ri - IRi = Li - I \pm f\ (Ri - 1, Ki)$
3. Hasil enciphering kemudian dipermutasikan dengan matriks permutasi balik (*invers initialpermutation* atau IP-1) menjadi blok teks kode. IP-1 ke bitsring *R16L16*, memperoleh teks-kode *y*, kemudian *y* = IP-1 (*R16L16*).

2.4 Konsep Steganografi

Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi rahasia di dalam suatu informasi lainya[3].

Steganography membutuhkan dua aspek yaitu media penyimpan dan informasi rahasia yang akan disembunyikan. Metode *steganography* sangat berguna jika digunakan pada *steganography* komputer karena banyak format *file digital* yang dapat dijadikan media untuk menyembunyikan pesan.*Steganography digital* menggunakan media *digital* sebagai wadah penampung, misalnya teks, citra, suara, dan *video*.Data rahasia yang disembunyikan juga dapat berupa teks, citra, suara, atau *video*.

Steganography memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata (*Human Visual System*) dan telinga (*Human Auditory System*), sehingga tidak diketahui kehadirannya oleh indera manusia (indera penglihatan atau indera pendengaran) dan mampu menghadapi proses-proses pengolahan sinyal *digital* dengan tidak merusak kualitas data yang telah disisipi sampai pada tahap tertentu.

Terdapat tiga aspek yang perlu diperhatikan dalam menyembunyikan pesan:kapasitas, keamanan, dan ketahanan. Kapasitas merujuk kepada besarnya informasi yang dapat disembunyikan oleh media, keamanan merujuk kepada ketidakmampuan pihak lain untuk mendeteksi keberadaan informasi yang disembunyikan, dan ketahanan merujuk kepada sejauh mana medium *steganography* dapat bertahan sebelum pihak lain menghancurkan informasi yang disembunyikan.

Perbedaan *stegranograpy* dengan *cryptography* terletak pada bagaimana proses penyembunyian data dan hasil akhir dari proses tersebut. *Cryptography* melakukan proses pengacakan data aslinya sehingga menghasilkan data terenkripsi yang benar – benar acak dan berbeda dengan aslinya, sedangkan *stegranograpy* menyembunyikan dalam data lain yang akan ditumpanginya tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hamper sama.

2.5 Citra Digital

Citra adalah gambar pada bidang dua dimensi.Dalam tinjauan matematis, citra merupakan fungsi kontinu dari intensitas cahaya pada bidang dua dimensi.Di dalam komputer, citra digital disimpan sebagai suatu *file* dengan format tertentu.Contoh format citra digital adalah *.bmp, .jpg, .png, .gif* dan sebagainya.Ukuran citra digital dinyatakan dalam *pixel* (*picture element*)[8].

2.6 Algoritma *End Of File*

Metode ini pesan yang disisipkan jumlahnya tak terbatas. Akan tetapi efek sampingnya adalah ukuran file menjadi lebih besar dari ukuran semula. Ukuran file yang terlalu besar dari yang seharusnya, tentu akan menimbulkan kecurigaan bagi yang mengetahuinya. Oleh karena itu dianjurkan agar ukuran pesan dan ukuran citra yang digunakan proporsional [9].

Proses penyisipan pesan dengan metode EOF dapat dituliskan dalam algoritma sebagai berikut:

1.Inputkan pesan yang akan disisipkan.
2.Ubah pesan menjadi kode desimal.
3.Inputkan citra grayscale yang akan disisipi pesan.
4.Dapatkan nilai derajat keabuan masing-masing piksel.
5.Tambahkan kode desimal pesan sebagai nilai derajat keabuan diakhir citra.
6.Petakan menjadi citra baru.

Sedangkan ekstraksi pesan yang sudah disisipkan dengan metode EOF dapat dilakukan dengan algoritma berikut:

1.Inputkan image yang sudah mengandung pesan.
2.Dapatkan nilai derajat keabuan citra tersebut.
3.Ubah nilai tersebut menjadi karakter pesan.

2.7 PSNR (*Peak Signal to Noise Ration*) dan MSE (*Mean Square Error*)

PNSR merupakan parameter yang digunakan mengukur kualitas citra yang dihasilkan. Metode PNSR adalah ukuran perbandingan antara nilai piksel *cover image* dengan nilai piksel pada citra *stego* yang dihasilkan. Sebelum menentukan PNSR terlebih dahulu ditentukan nilai rata-rata kuadrat *absolute error* antara *cover image* dengan citra *stego* yaitu nilai MSE (*Mean Square Error*). Berikut ini rumus MSE untuk *cover image* berwarna[10]:

$$MSE_{AVG} = \frac{MSE_R + MSE_G + MSE_B}{X.Y} \quad (1)$$

Keterangan:

MSE_{AVG} = Nilai rata-rata MSE *cover image*.

MSE_R = Nilai MSE warna merah.

MSE_G = Nilai MSE warna hijau.

MSE_B = Nilai MSE warna Biru.

X.Y = Dimensi gambar.

Berikut ini adalah rumus atau formula ang digunakan untuk menghitung PSNR [10]:

$$PSNR = 10_{log10}\left(\frac{255^2}{MSE}\right) \quad (2)$$

Keterangan:

PNSR = Nilai PNSR citra digital.

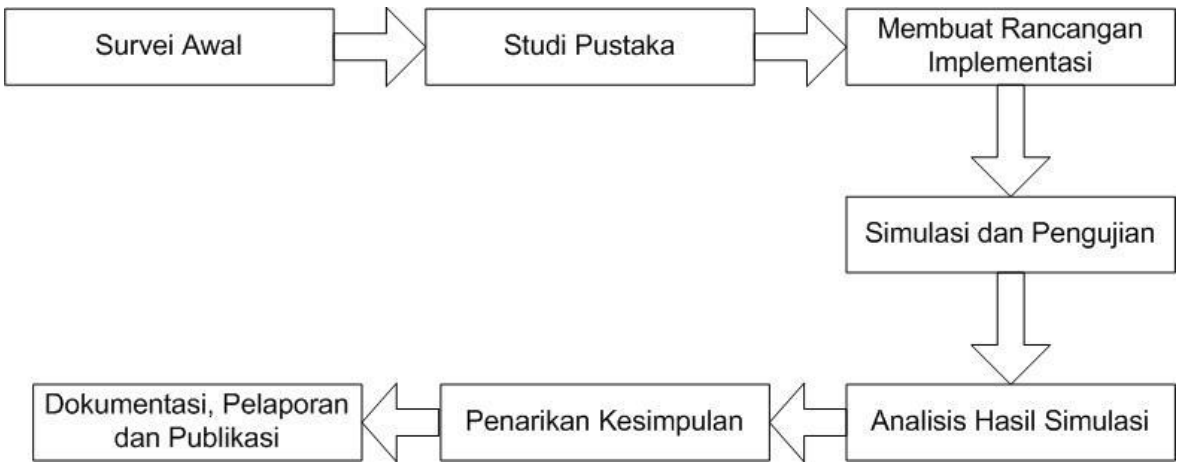
MSE = Nilai *Mean Square Error* dari citra.

Citra *stego* dapat dikatakan berkualitas baik jika nilai PNSR dari citra *stego* tersebut bernilai tinggi. Terdapat sedikit perbedaan antara *cover image* dan citra *stego* setelah penambahan pesan rahasia. Tingkatan kualitas nilai PNSR berbanding terbalik dengan nilai MSE, semakin tinggi nilai PNSR semakin rendah nilai MSE. Semakin tinggi kualitas yang dihasilkan dari citra *stego* maka semakin rendah nilai dari MSE.

3. METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Penelitian ini terdiri dari beberapa tahap yaitu studi pustaka dan literature, Analisis Data, Metode dan Pemodelan Desain, Implementasi, Pengujian, kesimpulan dan publikasi yang ditunjukkan pada gambar 1.



Gambar 1. *Tahapan Penelitian*

ISBN No. 978-602-98559-3-7

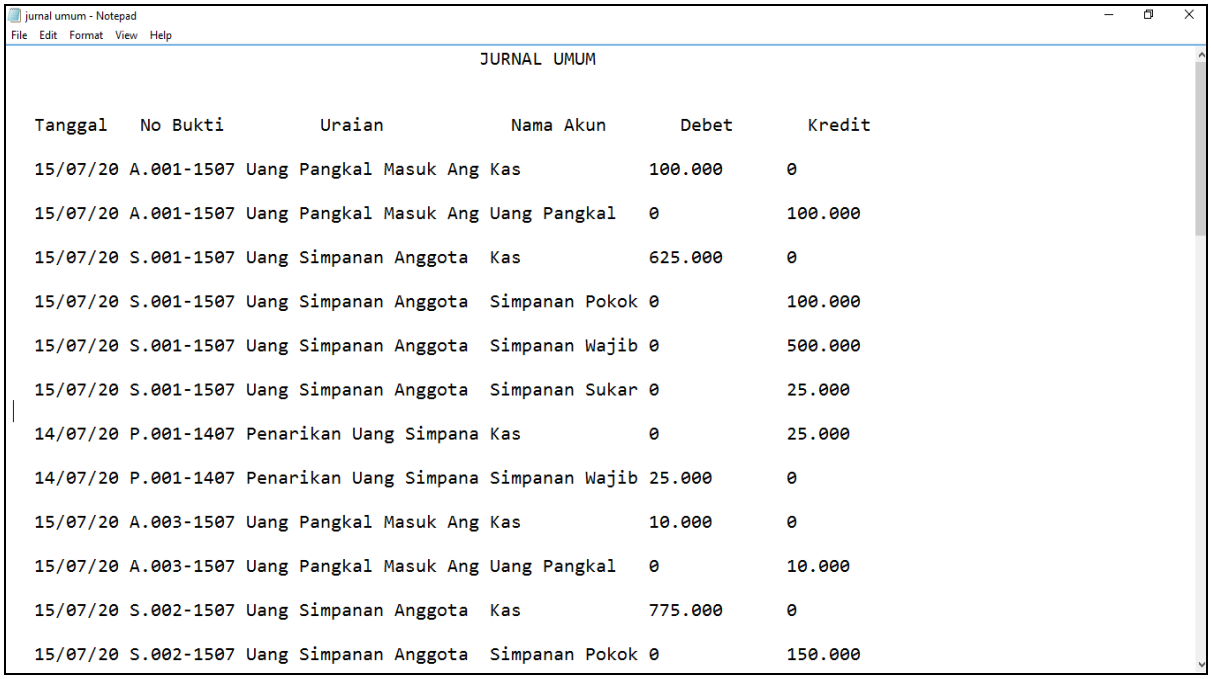
4. HASIL DAN PEMBAHASAN

4.1 Pengujian Enkripsi Kriptografi dan Steganografi

Pada proses pengujian kriptografi akan dilakukan proses pengujian pada aplikasi dari mulai file dalam bentuk *Plaintext* sampai dengan *Cipertext* menggunakan metode *Data Encryption Standard* sampai proses *Encoding*/enkripsi steganografi menggunakan metode *End Of File*. Adapun proses pengujian enkripsi kriptografi dan steganografi adalah sebagai berikut :

4.1.1 Data *Plaintext*

Data sampel yang akan digunakan pada pengujian ini untuk proses pengamanan adalah jurnal laporan keuangan, karena data ini bersifat penting dan rahasia dalam bentuk format file txt. Adapun contoh data *Plaintext* yang digunakan dapat dilihat pada gambar 2.


jurnal umum - Notepad

File Edit Format View Help

JURNAL UMUM

Tanggal	No Bukti	Uraian	Nama Akun	Debet	Kredit
15/07/20	A.001-1507	Uang Pangkal Masuk Ang	Kas	100.000	0
15/07/20	A.001-1507	Uang Pangkal Masuk Ang	Uang Pangkal	0	100.000
15/07/20	S.001-1507	Uang Simpanan Anggota	Kas	625.000	0
15/07/20	S.001-1507	Uang Simpanan Anggota	Simpanan Pokok	0	100.000
15/07/20	S.001-1507	Uang Simpanan Anggota	Simpanan Wajib	0	500.000
15/07/20	S.001-1507	Uang Simpanan Anggota	Simpanan Sukar	0	25.000
14/07/20	P.001-1407	Penarikan Uang Simpana	Kas	0	25.000
14/07/20	P.001-1407	Penarikan Uang Simpana	Simpanan Wajib	25.000	0
15/07/20	A.003-1507	Uang Pangkal Masuk Ang	Kas	10.000	0
15/07/20	A.003-1507	Uang Pangkal Masuk Ang	Uang Pangkal	0	10.000
15/07/20	S.002-1507	Uang Simpanan Anggota	Kas	775.000	0
15/07/20	S.002-1507	Uang Simpanan Anggota	Simpanan Pokok	0	150.000

***Gambar 2**. Data Plaintext*

Setelah data *Plaintext* dipersiapkan dalam format txt, selanjutnya meng-upload data tersebut ke aplikasi yang sudah dibuat.

4.1.2 Form Enkripsi

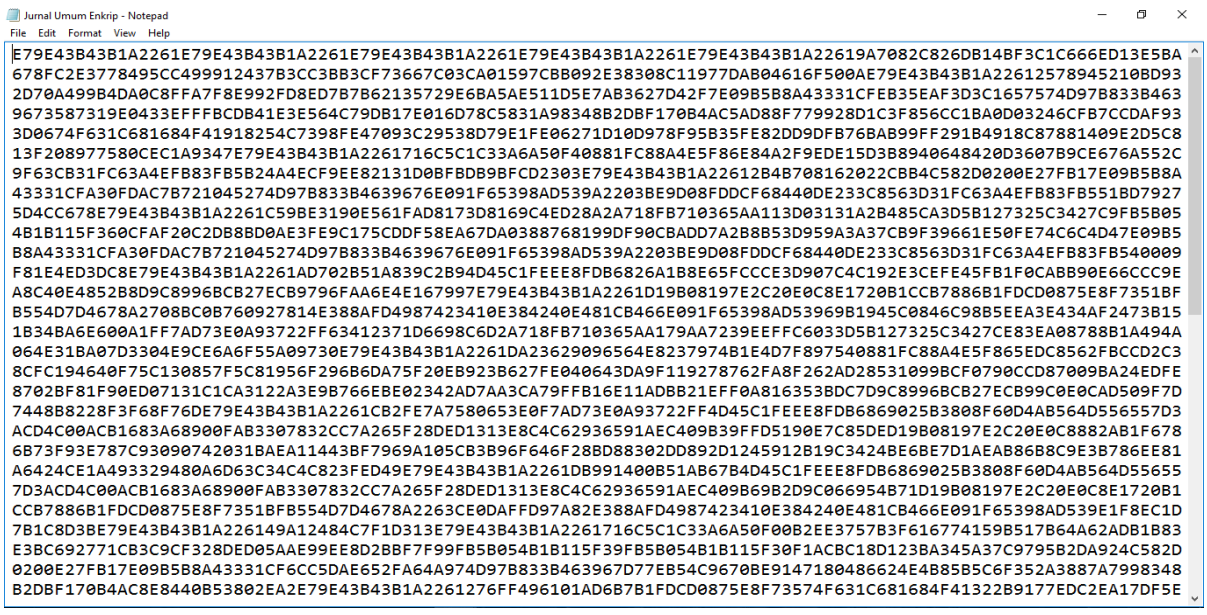
Form ini berfungsi untuk melakukan proses enkripsi data, di mana data *Plaintext* yang sudah dipersiapkan akan di-upload ke dalam aplikasi. Form enkripsi dapat dilihat pada gambar 3.

***Gambar 3**. Form Enkripsi*

Cara penggunaan form enkripsi adalah pertama memasukkan kunci enkripsi dalam hal ini pengguna bebas memasukkan kunci dalam bentuk apapun, kunci yang dimasukkan akan mempengaruhi hasil enkrispi. Selanjutnya pengguna dapat mengambil data *Plaintext* dengan cara memilih Tombol Ambil File Data lalu memilih Tombol Enkripsi File dan terakhir memilih Tombol Simpan Hasil Enkripsi. Pada gambar 3 terlihat dengan panjang karakter 3.196 dapat melakukan enkripsi hanya dalam 61 milidetik. Selanjutnya akan dilakukan proses *Encoding* steganografi dengan cara memilih Tombol Proses Selanjutnya.

4.1.3 Hasil *Cipertext*

Cipertext merupakan data hasil dari enkripsi, metode *Data Encryption Standard* mengubah data *Plaintext* menjadi *Cipertext* dalam format hexadecimal dengan panjang kunci 54 bit. Adapun hasil file *Cipertext* dapat dilihat pada gambar 4.



***Gambar 4.** Hasil Cipertext*

Dengan hasil *Cipertext* dari aplikasi yang sudah dibuat, maka dipastikan bahwa data sudah cukup aman karena orang lain yang tidak berkompeten dalam melihat data tidak akan bisa membaca informasi, karena hasil

Cipertext menjadi sandi-sandi yang tidak dapat dipahami. Namun akan lebih aman lagi jika data hasil *Cipertext* ini diamankan ke dalam citra digital menggunakan teknik steganografi metode *End Of File*.

4.1.4 Form *Encoding*/Enkripsi Steganografi

Form ini berfungsi untuk memasukkan gambar asli (cover image) yang akan disisipkan file hasil *Cipertext* lalu diproses menjadi gambar yang sudah disisipkan pesan (stego image). Adapun form *Encoding* steganografi dapat dilihat pada gambar 5.

Gambar 5. *Form Encoding/Enkripsi Steganografi*

Cara melakukan proses *Encoding* adalah memilih gambar sebagai cover image dengan browse file yang telah disediakan aplikasi, lalu mengambil file *Cipertext* dan memasukkan password sebagai kunci proses steganografi, lalu selanjutnya memilih Tombol Simpan Gambar dan Proses Enkripsi.

4.2. Pengujian *Decoding*/Dekripsi Steganografi dan Dekripsi Kriptografi

Pada proses pengujian ini akan dilakukan terlebih dahulu proses *Decoding*/enkripsi steganografi menggunakan metode *End Of File*, selanjutnya dekripsi kriptografi menggunakan metode *Data Encryption Standard*. Adapun proses pengujian adalah sebagai berikut :

4.2.1 Form *Decoding*/Dekripsi Steganografi

Form ini berfungsi untuk melakukan proses *Decoding*/dekripsi yaitu memisahkan stego image dan file isi pesan. Adapun form *Decoding* steganografi dapat dilihat pada gambar 6.

Gambar 6. *Form Decoding/Dekripsi Steganografi*

Cara melakukan proses *Decoding* adalah memilih gambar stego image dengan cara browse file yang telah disediakan aplikasi lalu memasukkan password beserta konfirmasi sesuai dengan password yang dimasukkan pada proses *Encoding*, jika password tidak sesuai maka proses *Decoding* akan gagal setelah itu menyimpan hasil steganografi ke lokasi yang diinginkan.

4.2.2 Form Dekripsi Kriptografi

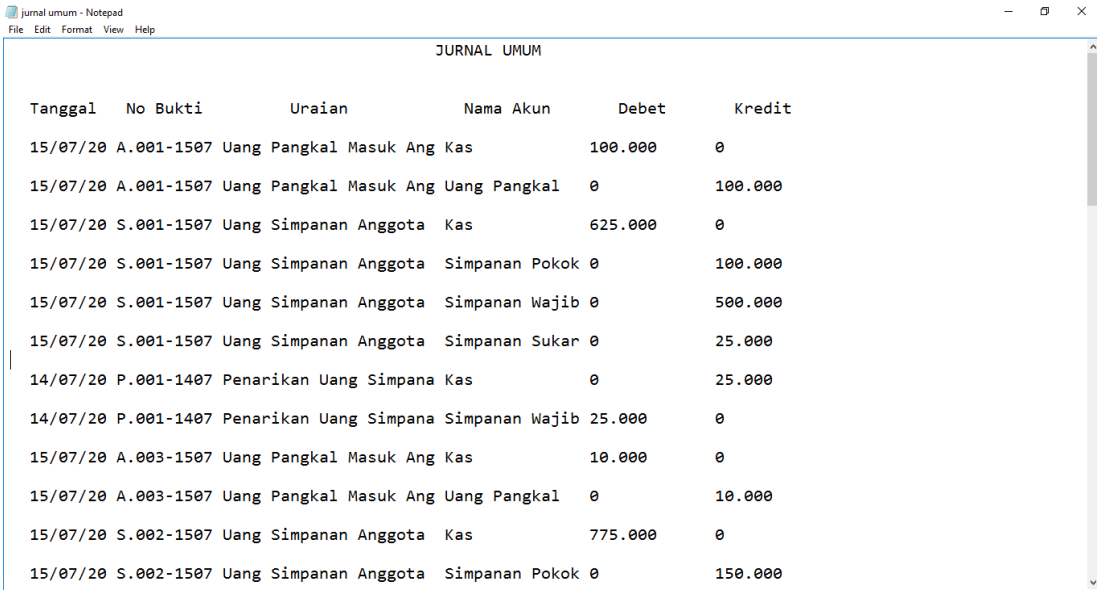
Form ini berfungsi untuk proses dekripsi data yaitu mengembalikan file *Cipertext* menjadi file *Plaintext* kembali. Adapun form dekripsi kriptografi dapat dilihat pada gambar 7.

Gambar 7. *Form Dekripsi Steganografi*

Cara melakukan proses dekirpsi adalah masukkan kunci yang sesuai pada proses enkripsi kriptografi, jika kunci salah maka proses dekripsi tidak akan dapat dilakukan. Selanjutnya pilih Tombol Ambil Laporan lalu pilih Tombol Dekripsi File dan Tombol Simpan Hasil Dekripsi, jika berhasil maka hasil dekirpis dapat ditampilkan dengan cara memilih Tombol Tampilkan Hasil Dekrip.

4.2.3 Hasil Dekripsi

Jika proses dekripsi berhasil maka hasilnya dapat ditampilkan sesuai dengan data aslinya sebelum dilakukan proses enkripsi. Adapun tampilan hasil dekripsi dapat dilihat pada gambar 8.


jurnal umum - Notepad
File Edit Format View Help

JURNAL UMUM

Tanggal	No Bukti	Uraian	Nama Akun	Debet	Kredit
15/07/20	A.001-1507	Uang Pangkal Masuk Ang	Kas	100.000	0
15/07/20	A.001-1507	Uang Pangkal Masuk Ang	Uang Pangkal	0	100.000
15/07/20	S.001-1507	Uang Simpanan Anggota	Kas	625.000	0
15/07/20	S.001-1507	Uang Simpanan Anggota	Simpanan Pokok	0	100.000
15/07/20	S.001-1507	Uang Simpanan Anggota	Simpanan Wajib	0	500.000
15/07/20	S.001-1507	Uang Simpanan Anggota	Simpanan Sukar	0	25.000
14/07/20	P.001-1407	Penarikan Uang Simpana	Kas	0	25.000
14/07/20	P.001-1407	Penarikan Uang Simpana	Simpanan Wajib	25.000	0
15/07/20	A.003-1507	Uang Pangkal Masuk Ang	Kas	10.000	0
15/07/20	A.003-1507	Uang Pangkal Masuk Ang	Uang Pangkal	0	10.000
15/07/20	S.002-1507	Uang Simpanan Anggota	Kas	775.000	0
15/07/20	S.002-1507	Uang Simpanan Anggota	Simpanan Pokok	0	150.000

Gambar 8. *Hasil Dekripsi*

Pada tampilan hasil dekripsi menunjukkan bahwa gambar 8 dan gambar 2 data *Plaintext* menghasilkan data yang sama persis, ini berarti menunjukkan bawwa proses pengujian kriptografi telah berhasil.

4.3 Pengujian Kualitas Citra Steganografi *End Of File*

Pengujian ini berfungsi untuk memastikan bawah teknik steganografi *End Of File* yang telah disisipi pesan rahasia dalam bentuk *Cipertext* mempunya kualitas yang baik. Berikut ini adalah hasil pengujian kualitas citra steganografi *End Of File* berdasarkan aplikasi yang telah dibuat.

4.3.1 Pengujian MSE (*Mean Square Error)* PNSR (*Peak Signal to Noise Ratio*)

Pengujian MSE dan PNSR digunakan untuk mengukur kualitas citra yang dihasilkan. Metode PNSR adalah ukuran perbandingan antara nilai piksel *cover image* dengan nilai piksel pada citra *stego* yang dihasilkan. Tabel 1 dan 2 menunjukkan hasil pengujian MSE dan PNSR.

Tabel 1. *Hasil Pengujian MSE*

No	Nama Gambar	Ukuran Gambar Asli	Ukuran *Stego Image*	*MSE*
1	Tengkorak.jpg	17.1 KB	107 KB	27 db
2	Mobil.jpg	68 KB	1.021 KB	29 db
3	Sepeda.jpg	6.3 KB	2.52 KB	0.0003 db
4	Hitam.jpg	34.4 KB	327 KB	2.6 db
5	Putih.jppg	6.36 KB	2.51 KB	0.000008 db

Tabel 2. *Hasil Pengujian PNSR*

No	Nama Gambar	Ukuran Gambar Asli	Ukuran *Stego Image*	*PSNR*
1	Tekngkorak.jpg	210 KB	371 KB	27db
2	Mobil.jpg	210 KB	371 KB	21 db
3	Sepeda.jpg	210 KB	374 KB	133 db
4	Hitam.jpg	207 KB	322 KB	22 db
5	Putih.jpg	340 KB	575 KB	104 db

Berdasarkan pengujian MSE dan PNSR didapatkan bahwa nilai MSE yang dihasilkan kurang dari 1 dB dan PNSR di atas 50, berarti perubahan kualitas warna antara citra asli dengan *stego image* tidak mengalami perubahan yang signifikan, sehingga keberadaan dari file yang tersembunyi tidak mudah di deteksi oleh indra penglihatan manusia.

4.3.2 Pengujian *Recovery*

Pengujian *recovery* dilakukan untuk menguji apakah pesan rahasia yang disisipi pada sebuah citra harus dapat dipisahkan kembali dari stego-image-nya. Pengujian dapat dilakukan dengan melihat keutuhan pesan yang d iekstraksi dari sejumlah citra uji. Berikut pengujian *recovery* yang dilakukan dapat dilihat pada tabel 3.

Tabel 3. *Hasil Pengujian Recovery*

No	Nama Gambar	Normal	Diputar	Dipotong	*Recovery*
1	Tengkorak.jpg	✓			Berhasil
2	Mobil.jpg		✓		Gagal
3	Sepeda.jpg		✓		Gagal
4	Hitam.jpg			✓	Gagal
5	Putih.jpg			✓	Gagal

Dari hasil pengujian *recovery* yang telah dijabarkan pada table diatas dapat dilihat bahwa pesan rahasia yang disisipi pada sebuah citra dapat dipisahkan kembali dari stego-image-nya. Namun saat *cover image* di putar dan di crop maka pesan tidak dapat dibuka.

5. SIMPULAN

1. Berdasarkan hasil pengujian kriptografi menggunakan metode *Data Encryption Standard*, didapatkan bawha file *Plaintext* dapat diubah menjadi *Cipertext* dengan kecepatan 61 Milidetik dengan panjang karakter 3.196 dan berhasil dikembalikan lagi menjadi file *Plaintext*
2. Aplikasi steganografi dengan metode *End Of File* yang telah dibuat didapatkan hasil keakuratan yang 100% akurat. Dalam proses *Encoding* dan *Decoding* akan menghasilkan output yang sama dengan inputannya.

3. Hasil pengujian nilai PSNR terhadap image atau file citra digital yang dihasilkan dari aplikasi Steganografi inipun menunjukkan nilai yang cukup baik bergantung pada besar ukuran file citra yang digunakan dan besarnya jumlah karakter yang disisipkan pada file citra tersebut
4. Penggabungan metode Kriptografi Data Encrtyption Standard dan Steganografi *End Of File* dapat menjadi salah satu alternative dalam pengamanan data dan informasi

6. UCAPAN TERIMAKASIH

Ucapan terimakasih kepada Ibu Dra. Wamiliana, M.A., Ph.D. sebagai promotor yang telah membimbing penulis dalam melakukan proses penelitian.

KEPUSTAKAAN

[1] Munir, Rinaldi. (2006). Diktat Kuliah IF2153 Matematika Diskrit. Program Studi Teknik Informatika, Institut Teknologi Bandung.

[2] Sitohang, Ernita., (2013). Perangkat Aplikasi Keamanan Data Text Mengunakan Electronic Codebook Dengan Algoritma DES, Pelita Informatika Budi Darma, ISSN 2301-9425

[3] Ariyus, Dony., (2006). *Kriptografi Keamanan Data dan Komunikasi*. Graha Ilmu, Yogyakarta.

[4] Wandany, Heny., dan Budiman, (2012). Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi *End Of File* (EOF) dan Rabin Public Key Cryptosystem, Jurnal Alkhawarizmi. Vol.1, No 1.

[5] Primartha, Rifkie., (2011). Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma *Data Encryption Standard* (DES). Jurnal Sistem Informasi. Vol. 3 No 2. ISSN : 2085 – 1588

[6] Darwis, Dedi., dan Kisworo (2017). Teknik Steganografi Untuk Penyembunyian Pesan Teks Menggunakan Algoritma *End Of File*. Jurnal Explore Sistem Informasi dan Telematika. ISSN : 2087 – 2062

[7] Ariyus, Dony, (2008). *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*. Andi Offset, Yogyakarta.

[8] Mufida Khairani, Sajadin Sembiring, (2013). *Analisis dan Implementasi Steganografi Pada Citra GIF Menggunakan Algoritma GifShufle*, SNASTIKOM, ISBN 978-602-19837-3-7.

[9] Iswahyudi, C., Setyaningsih, E., (2012). *Pengamanan Kunci Enkripsi Citra Pada Algoritma Super Enkripsi Menggunakan Metode End Of File*. Jurnal Prosiding Nasional Aplikasi Sains & Teknologi (SNAST) Periode III.

[10] Cheddad, A., Condell, J., Curran, K., Kevitt, P.Mc., (2010). *Digital Image Steganography : Survey and Analysis of Current Methods*. Signal Processing, Elsevier. Northern Ireland, UK.