

**PERBANDINGAN TEKNIK STEGANOGRAFI SEBAGAI KEAMANAN
DATA DAN INFORMASI DENGAN METODE EOF DAN LSB**

SKRIPSI

Untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



diajukan oleh

Nur Cahyo Kurniawan

18.83.0204

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

**PERBANDINGAN TEKNIK STEGANOGRAFI SEBAGAI KEAMANAN
DATA DAN INFORMASI DENGAN METODE EOF DAN LSB**

SKRIPSI

Untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



diajukan oleh

Nur Cahyo Kurniawan

18.83.0204

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

PERSETUJUAN

SKRIPSI

**PERBANDINGAN TEKNIK STEGANOGRAFI SEBAGAI
KEAMANAN DATA DAN INFORMASI DENGAN METODE
EOF DAN LSB**

Yang disusun dan diajukan oleh

Nur Cahyo Kurniawan

18.83.0204

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 juni 2022

Dosen Pembimbing,

Dony Ariyus M.Kom

NIK. 190302128

PENGESAHAN

SKRIPSI

**PERBANDINGAN TEKNIK STEGANOGRAFI SEBAGAI
KEAMANAN DATA DAN INFORMASI DENGAN METODE
EOF DAN LSB**

yang disusun dan diajukan oleh

Nur Cahyo Kurniawan

18.83.0204

telah dipertahankan di depan Dewan Penguji
pada tanggal 22 juni 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Muhammad Kopravi, S.Kom., M.eng

NIK. 190302454

Rini Indrayani, ST, M.eng

NIK. 190302417

Dony Ariyus, M.Kom

NIK. 190302128

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 juni 2022

DEKAN FAKULTAS ILMU KOMMPUTER

Hanif Al Fattah, S.Kom., M.Kom.

NIK. 190302096

PERNYATAAN

Yang bertandatangan di bawah ini,

Nama mahasiswa : Nur Cahyo Kurniawan
NIM : 18.83.0204

Menyatakan bahwa Skripsi dengan judul berikut:

**PERBANDINGAN TEKNIK STEGANOGRAFI SEBAGAI KEAMANAN
DATA DAN INFORMASI DENGAN METODE EOF DAN LSB**

Dosen Pembimbing : Dony Ariyus, M.Kom

1. Karya tulis ini adalah benar-benar **ASLI** dan **BELUM PERNAH** diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian **SAYA** sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab **SAYA**, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini **SAYA** buat dengan sesungguhnya, apabila di kemudian hari terdapat **penyimpangan dan ketidakbenaran** dalam pernyataan ini, maka **SAYA** bersedia menerima **SANKSI AKADEMIK** dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 22 juni 2022

Yang Menyatakan,

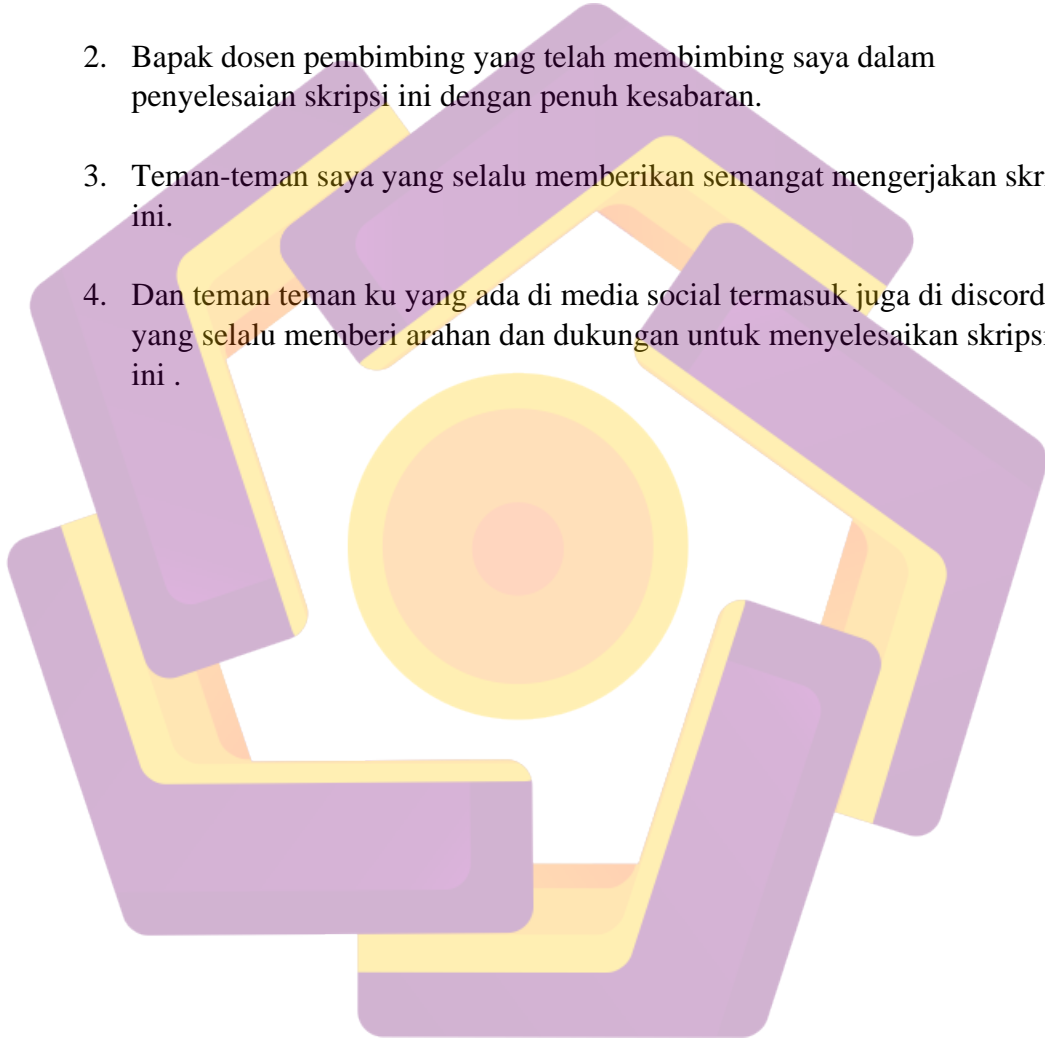


Nur Cahyo Kurniawan

PERSEMBAHAN

Pertama saya ucapkan syukur kepada Allah SWT atas selesainya naskah skripsi ini dengan baik dan lancar. Dan skripsi ini saya persembahkan untuk :

1. Orangtua saya bapak dan ibu yang telah memberikan kasih sayang hingga dewasa, selalu mendoakan, dan mendukung untuk sukses di masa mendatang.
2. Bapak dosen pembimbing yang telah membimbing saya dalam penyelesaian skripsi ini dengan penuh kesabaran.
3. Teman-teman saya yang selalu memberikan semangat mengerjakan skripsi ini.
4. Dan teman teman ku yang ada di media social termasuk juga di discord yang selalu memberi arahan dan dukungan untuk menyelesaikan skripsi ini .



KATAPENGANTAR

Bismillahirrohmanirrohim.

Puji dan syukur saya panjatkan kepada Allah Swt. atas ridanya saya dapat menyelesaikan penyusunan skripsi ini. Adapun judul skripsi yang saya ajukan adalah perbandingan teknik steganografi sebagai keamanan data dan informasi dengan metode eof dan lsb.

Skripsi ini diajukan untuk memenuhi syarat kelulusan mata kuliah Skripsi di Universitas Amikom Yogyakarta. Tidak dapat disangkal bahwa butuh usaha yang keras dalam penyelesaian pengerjaan skripsi ini. Namun, karya ini tidak akan selesai tanpa orang-orang tercinta di sekeliling kita yang mendukung dan membantu. Terima kasih saya sampaikan kepada:

1. Prof, Dr. M. Suyanto, MM., Selaku Rektor Universitas Amikom Yogyakarta
2. Dony Ariyus M.Kom selaku Dosen pembimbing yang telah memberikan bimbingan dan berbagai pengalaman kepada saya.
3. Segenap Dosen Teknik Komputer yang telah mendidik dan memberikan ilmu selama kuliah dan seluruh staf yang selalu sabar melayani segala administrasi.
4. Semua pihak yang telah membantu dan tidak dapat disebutkan satu persatu.

Semoga segala kebaikan dan pertolongan semuanya mendapat berkah dari Allah Swt. dan akhirnya saya menyadari bahwa skripsi ini masih jauh dari kata sempurna, karena keterbatasan ilmu yang saya miliki. Untuk itu saya dengan kerendahan hati mengharapkan saran dan kritik yang sifatnya membangun dari semua pihak demi membangun laporan penelitian ini.

Yogyakarta, 5 oktober 2021

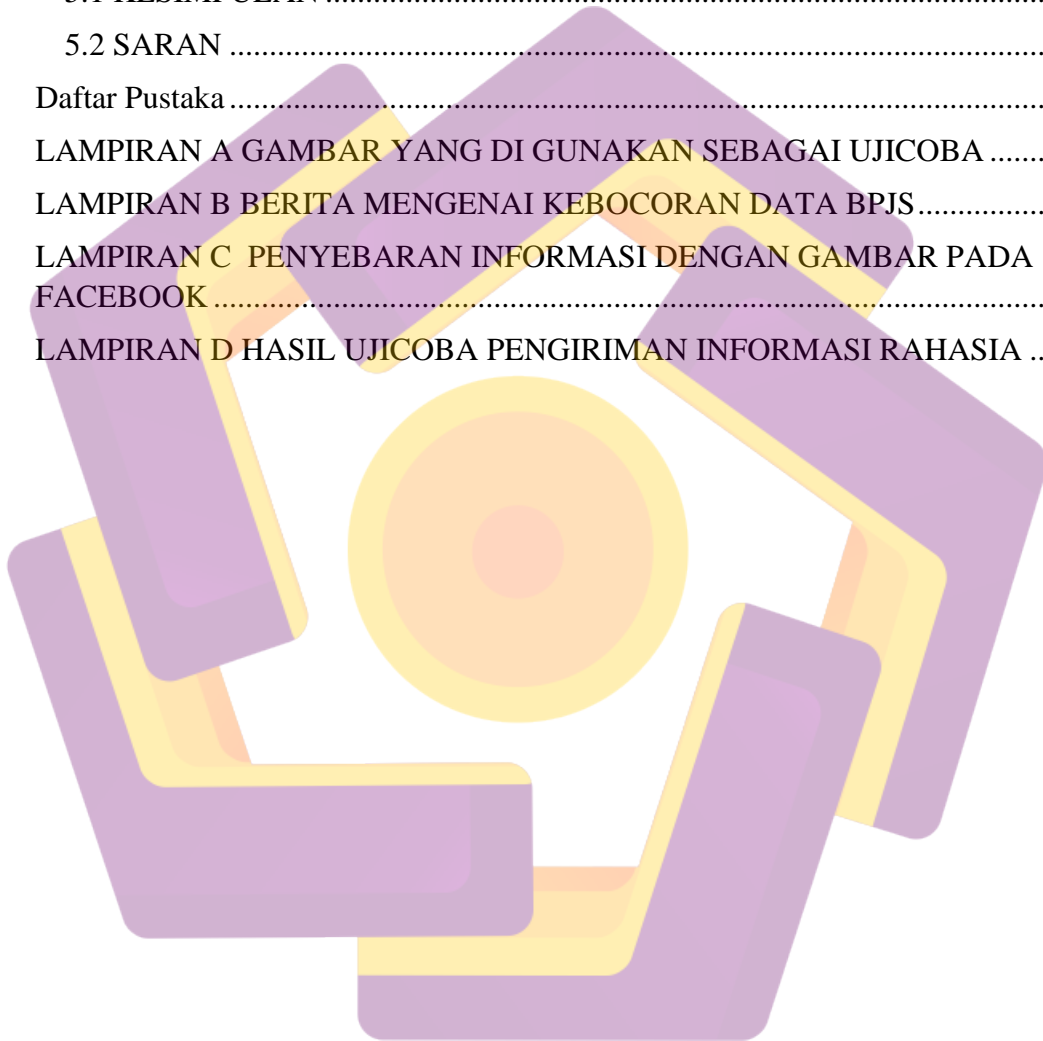
Penulis

DAFTAR ISI

PERSETUJUAN	i
PENGESAHAN	ii
PERNYATAAN.....	iii
PERSEMBAHAN	iv
KATAPENGANTAR	v
DAFTAR GAMBAR	ix
DAFTAR TABEL.....	xi
INTISARI.....	xii
ABSTRACT.....	xiii
BAB I.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Maksud dan Tujuan Penelitian	2
1.5 Manfaat Penelitian.....	2
1.6 Metode Penelitian.....	3
1.1.2 Metode Pengumpulan Data.....	3
1.1.3 Metode Perbandingan	3
1.7 Sistematika Penulisan	3
BAB II.....	4
2.1 Tinjauan Pustaka	4
2.1 Kajian teori	8
2.1.1 LSB dan MSB.....	9
2.1.2 EOF.....	10
2.1.3 Caesar Chiper.....	10
2.1.4 Vigenere Chiper	11
2.1.4 Karakteristik JPEG	11
2.1.5 Karakteristik Resolusi Gambar.....	12
2.1.6 Karakteristik audio.....	13
2.1.7 Karakteristik Video.....	13
2.1.8 Standarisasi pengiriman gambar Whatsapp.....	14

BAB III	15
3.1 ALUR PENELITIAN.....	15
3.2 ALAT DAN BAHAN PENELITIAN	15
3.2.1 Hex Editor Neo	16
3.2.2 Media Penadah Informasi rahasia.....	16
3.2.3 Virtual Machine Linux.....	16
3.2.4 Virtual Machine Android.....	16
3.3 RANCANGAN SISTEM	17
3.3.1 Rancangan Enkripsi LSB.....	17
3.3.2 Rancangan Lokasi Penyisipan	17
3.4 Metode Penelitian.....	18
3.4.1 Metode Pengumpulan data.....	18
3.4.1 Skenario Pengujian	18
3.4.2 Metode Analisis	19
BAB IV	20
4.1 HASIL PENGUJIAN DAN PEMBAHASAN	20
4.1.1 Alur Penyisipan informasi	20
4.1.2 HASIL MODIFIKASI EOF DAN LSB.....	20
4.1.3 Hasil gambar Steganografi.....	21
4.1.4 Hasil Histogram.....	23
4.2 HASIL PENGUJIAN AKHIR SEMENTARA	24
4.2.1 Hasil Percobaan JPEG	24
4.2.2 Hasil uji coba MP3 dan MP4.....	26
4.2.3 Hasil Cropping gambar	28
4.2.4 Hasil Percobaan Pada Linux	29
4.2.5 Hasil Percobaan pada Android	29
4.2.6 Hasil Percobaan Pada Discord.....	30
4.2.7 Hasil Beberapa Sampel Byte	31
4.3 Hasil ujicoba Penyisipan Informasi.....	32
4.4 Hasil Penmabahan Enkripsi VigenereChiper	33
4.5 Tabel Hasil Keseluruhan Ujicoba Steganografi	35
4.5.1 Whatsapp	35

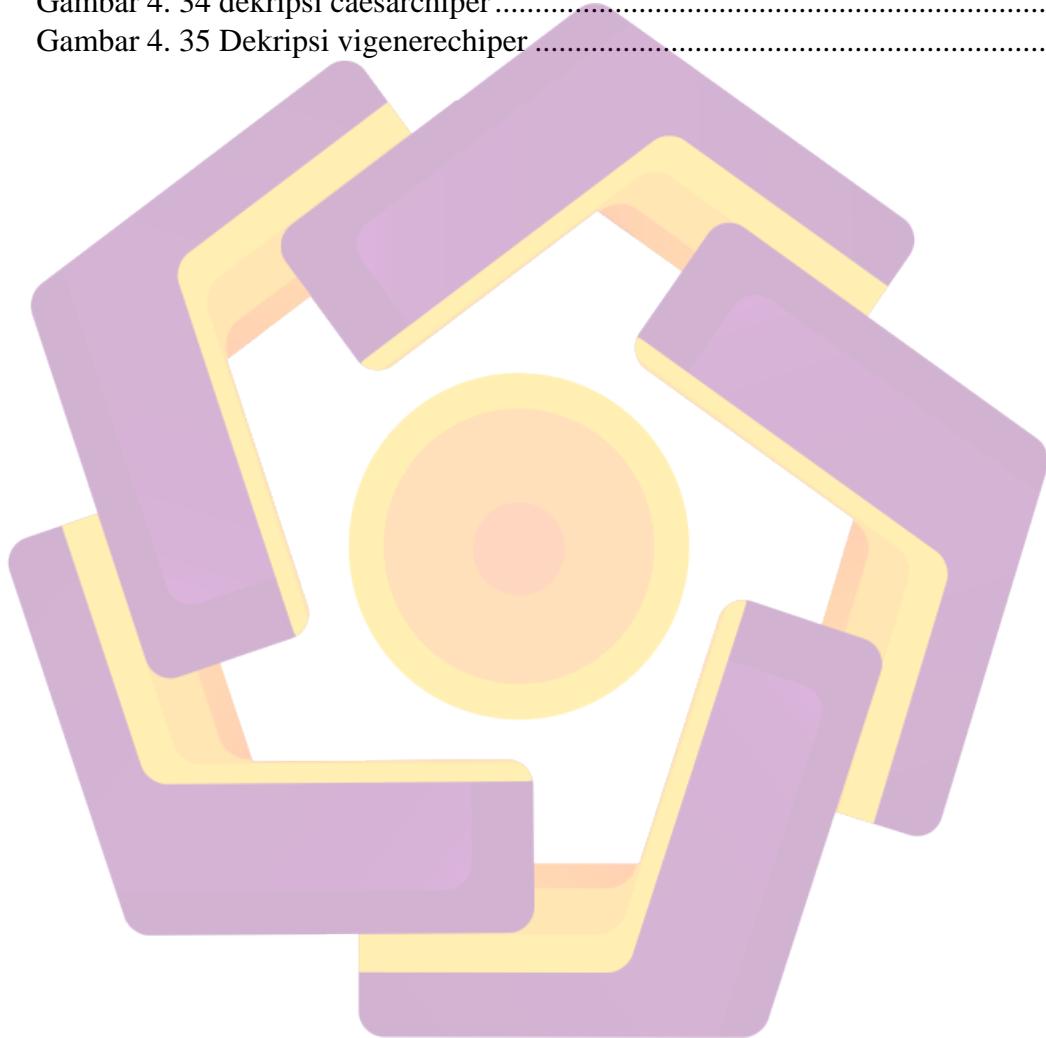
4.5.2 Telegram	36
4.5.3 Facebook.....	38
4.5.4 Discord.....	39
4.6 PROSES DEKRIPSI DAN EKSTRAKSI.....	41
BAB V.....	42
5.1 KESIMPULAN	42
5.2 SARAN	42
Daftar Pustaka	43
LAMPIRAN A GAMBAR YANG DI GUNAKAN SEBAGAI UJICOBA	44
LAMPIRAN B BERITA MENGENAI KEBOCORAN DATA BPJS.....	44
LAMPIRAN C PENYEBARAN INFORMASI DENGAN GAMBAR PADA FACEBOOK.....	45
LAMPIRAN D HASIL UJICOBA PENGIRIMAN INFORMASI RAHASIA ...	45



DAFTAR GAMBAR

Gambar 2. 1 contoh LSB dan MSB	9
Gambar 2. 2 Binnary Sebelum Di sisipkan Informasi	10
Gambar 2. 3 Setelah Binnary di sisipkan informasi.....	10
Gambar 2. 4 Langkah Enkripsi Caesar Chiper.....	10
Gambar 2. 5 Vigenere Chiper	11
Gambar 2. 6 Macam Macam Resolusi gambar	12
Gambar 2. 7 struktur MP3.....	13
Gambar 3. 1 Flowchart Alur Penelitian	15
Gambar 3. 2 Hex Editor Neo	16
Gambar 3. 3 Bahan Untuk Penyisipan Informasi	16
Gambar 3. 4 Virtual Machine.....	16
Gambar 3. 5 Virtual Machine Android	16
Gambar 3. 6 EOF header.....	18
Gambar 3. 7 EOF body	18
Gambar 3. 8 EOF classic.....	18
Gambar 4. 1 Flowchart alur Steganografi	20
Gambar 4. 2 Sebelum di Enkripsi	21
Gambar 4. 3 Sesudah di Enkripsi	21
Gambar 4. 4 Hasil Gambar EOF Header 1	21
Gambar 4. 5 Hasil Gambar EOF Header 2	22
Gambar 4. 6 Hasil Gambar EOF Body 1	22
Gambar 4. 7 Hasil Gambar EOF body 2	22
Gambar 4. 8 Hasil Gambar EOF classic	23
Gambar 4. 9 Hasil Histogram Yang tersisipkan informasi	23
Gambar 4. 10 Hasil Histogram Original	23
Gambar 4. 11 send file Raw / Dokumen whatsapp.....	25
Gambar 4. 12 send File Raw telegram	25
Gambar 4. 13 Hasil send file Raw / dokumen Whatsapp	26
Gambar 4. 14 Hasil send File Raw telegram	26
Gambar 4. 15 hasil send file MP3 dan MP4 pada whatsapp.....	27
Gambar 4. 16 Hasil send file MP3 dan MP4 pada telegram.....	27
Gambar 4. 17 Hasil Crop aplikasi Paint.....	28
Gambar 4. 18 Hasil Crop Windows editor.....	28
Gambar 4. 19 Hasil percobaan di Linux	29
Gambar 4. 20 Hasil Percobaan di Android	29
Gambar 4. 21 Hasil pada aplikasi Discord.....	30
Gambar 4. 22 Hasil Pada Aplikasi Discord 2	30
Gambar 4. 23 Hasil Pada aplikasi Discord 3	30
Gambar 4. 24 Hasil Pada aplikasi discord 4	31
Gambar 4. 25 Hasil ujicoba pada byte 1-32.....	31
Gambar 4. 26 Penyisipan shortlink googledrive	32

Gambar 4. 27 Penerima menggunakan linux	32
Gambar 4. 28 Perbedaan Hasil Penyisipan informasi.....	33
Gambar 4. 29 Hasil Pengekripsian Vigenere	33
Gambar 4. 30 Hasil vigenere yang di enkrip dengan Caesarchiper LSB.....	34
Gambar 4. 31 Hasil Output penyisipan vigenere dan caesar LSB	34
Gambar 4. 32 Pengiriman stegano beserta code untuk penerima	34
Gambar 4. 33 steganografi beserta pesan clue	41
Gambar 4. 34 dekripsi caesarchiper	41
Gambar 4. 35 Dekripsi vigenerechiper	41



DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	8
Tabel 3. 1 Enkripsi dan Plaintext	17
Tabel 4. 1 Hasil pada Social Media	24
Tabel 4. 2 Hasil Pada Media Social Whatsapp	24
Tabel 4. 3 Hasil send file Raw whatsapp	25
Tabel 4. 4 Hasil Mp4.....	26
Tabel 4. 5 Hasil Mp3.....	26
Tabel 4. 6 hasil cropping.....	28
Tabel 4. 7 arti setiap pesan clue	34
Tabel 4. 8 Hasil pengiriman file gambar whatsapp.....	35
Tabel 4. 9 Hasil pengiriman file Raw gambar whatsapp	36
Tabel 4. 10 Hasil pengiriman file music whatsapp	36
Tabel 4. 11 Hasil pengiriman file video whatsapp.....	36
Tabel 4. 12 Hasil pengiriman file gambar telegram.....	37
Tabel 4. 13 Hasil pengiriman file raw gambar telegram.....	37
Tabel 4. 14 Hasil pengiriman file music telegram	38
Tabel 4. 15 Hasil pengiriman file video telegram.....	38
Tabel 4. 16 Hasil pengiriman file gambar facebook	39
Tabel 4. 17 Hasil pengiriman file music facebook	39
Tabel 4. 18 Hasil pengiriman file video facebook	39
Tabel 4. 19 Hasil pengiriman file gambar discord.....	39
Tabel 4. 20 Hasil pengiriman file music discord	40
Tabel 4. 21 Hasil pengiriman file video discord	40

INTISARI

Steganografi adalah teknik penyembunyian sebuah informasi dalam sebuah gambar, Teknik steganografi tersebut sebenarnya sudah ada sejak abad pertengahan, namun di masa digital ini masih bisa di gunakan sebagai media penyisipan informasi agar tidak mengalami pencurian data dan di jualbelikan oleh pihak yang tidak bertanggungjawab.

data yang diambil untuk tujuan penelitian ini melalui sebuah kejadian yang sempat viral mengenai Kebocoran Data Informasi BPJS dan di jualbelikan di sebuah forum, dan data ke 2 di ambil dari keseharian masyarakat di media social facebook mengenai pemberian kritik terhadap situasi sebuah negara baik itu masalah ekonomi dan politik, masyarakat lebih suka menggunakan media gambar dari pada menulis text yang Panjang, dari data yang di dapat bahwa ke 2 kejadian tersebut bisa di padukan jadi 1 dan menghasilkan hal yang lebih positif, penelitian ini bertujuan membandingkan metode steganografi sebelumnya mana yang lebih cocok di lingkungan masyarakat agar meminimalis tingkat kebocoran data informasi serta masyarakat mau untuk mempelajarinya, pada penelitian ini akan menggunakan metode EOF (end of file).

Dari analisis dan perbandingan Teknik-teknik sebelumnya seperti LSB di dapat hasil bahwa tiap metode steganografi sebelumnya memiliki Teknik dan Langkah yang berbeda dan ketersediaan tools yang di jalan kan di system operasi yang berbeda-beda di android, windows dan Linux.

Katakunci : steganografi, Penyembunyian informasi, End Of File

ABSTRACT

Steganography is a technique for hiding information in an image, the steganography technique has actually existed since the Middle Ages, but in this digital era it can still be used as a medium for inserting information so as not to experience data theft and being traded by irresponsible parties.

The Data taken for the purpose of this study through an incident that had gone viral regarding BPJS Information Data Leaks and was traded in a forum, and the second data was taken from people's daily lives on social media Facebook regarding giving criticism to the situation of a country both economic and political issues, people prefer to use image media rather than writing long text, from the data obtained that the 2 events can be combined into 1 and produce more positive things, this study aims to compare which previous steganographic method is more suitable in the community so that minimize the level of information data leakage and the public is willing to study it, in this study will use the EOF (end of file) method.

From the analysis and comparison of previous techniques such as LSB, the results show that each previous steganographic method has different techniques and steps and the availability of tools that run on different operating systems on Android, Windows and Linux.

Keyword : *steganography, Information hiding, End Of File*