JURNAL SINTAKS LOGIKA Vol. 2 No.3 , September 2022 **E-ISSN : 2775-412X**
https://jurnal.umpar.ac.id/index.php/sylog

STEGANOGRAFI GAMBAR DALAM VIDEO MENGGUNAKAN METODE BASE64 DAN XOR

Fakhriyyah Saleh[1*], Andi Wafiah [2]
[1]Teknik Informatika, Universitas Muhammadiyah Parepare, Indonesia
Fakhriyyahsaleh25@gmail.com, andiwafiah01@gmail.com

InformasiArtikel

Riwayat Artikel:

Dikirim *Author* : 16-9-2022
Diterima Redaksi : 17-9-2022
Revisi *Reviewer*: 28-9-2022
Diterbitkan *online*: 30-9-2022

Keywords: *Keywords: Steganography, Information, Security, Base64, XOR*

Kata kunci*: Steganografi, Informasi, Keamanan, Base64, XOR*

ABSTRACT

Steganography is an important component in the process of hiding information. The theory of steganography has a technique of its own characteristics in using files that are the protective media. This steganography technique is carried out in such a way that the inserted information does not damage the protected digital data. Hidden files cannot be noticed by the human senses. The problem that exists today is the security of the confidentiality of information or data that is exchanged. So it is not desirable if the information submitted is known by others. Based on the above background, this study aims to design and build an image-in- video steganography application using the base64 and XOR methods.This research method uses literature review research methods and experimental research. The testing method used is black box.Where the black box only observes the results of execution through test and functional data from the software, evaluating only on appearance.

ABSTRAK

Steganografi merupakan komponen penting dalam proses penyembunyian informasi. Teori steganografi memiliki teknik dari ciri khas sendiri dalam menggunakan file-file yang menjadi media pelindungnya. Teknik steganografi ini dilakukan sedemikian rupa sehingga informasi yang disisipkan tidak merusak data digital yang dilindungi. File yang tersembunyi tidak dapat disadari oleh indera manusia. Permasalahan yang ada saat ini adalah keamanan terhadap kerahasiaan sebuah informasi atau data yang saling dipertukarkan. Maka hal itu tidak diinginkan jika informasi yang disampaikan diketahui oleh orang lain. Berdasarkan latar belakang di atas penelitian ini bertujuan merancang dan membangun sebuah aplikasi steganografi gambar dalam video menggunakan metode *base64* dan *XOR*. Metode penelitian ini menggunakan metode penelitian kajian kepustakaan dan penelitian eksperimen. Adapun metode pengujian yang digunakan adalah *black box*. Dimana *black box* hanya mengamati hasil eksekusi melalui data uji dan fungsional dari perangkat lunak, mengevaluasi hanya pada tampilannya saja.

Penulis Korespondensi:

Fakhriyyah Saleh,
Teknik Informatika,
Universitas Muhammadiyah Parepare,
Jl. Jendral Ahmad Yani KM.6 Kota Parepare, Indonesia
Email: Fakhriyyahsaleh25@gmail.com

I. PENDAHULUAN

Kemajuan teknologi komputer membantu semua aspek kehidupan manusia, dari hal yang kecil sampai berbagai hal yang sangat rumit sekalipun bisa dikerjakan oleh teknologi komputer. Contoh dari kemajuan teknologi komputer yang paling nyata yang dapat digunakan semua orang adalah kecepatan dalam menyampaikan pesan dari tempat yang jauh. Namun dibalik perkembangannya teknologi, sistem keamanan data sangat perlu ditingkatkan. Seiring dengan tuntutan akan keamanan terhadap kerahasiaan sebuah informasi atau data yang saling dipertukarkan tersebut, maka semakin meningkat dan banyaknya pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain, maka muncul lah cabang ilmu yang mempelajari tentang cara-cara pengamanan data.[2]

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Banyaknya terjadi pertukaran informasi yang tersebar melalui

internet serta terjadinya pencurian data dari informasi itu sendiri, memaksa pengguna harus lebih mementingkan tingkat keamanan sistem informasi tersebut agar informasi yang akan digunakan tidak diganggu oleh pihak-pihak yang tidak bertanggungjawab. Istilah penyembunyian tersebut dapat di istilahkan sebagaiSteganografi.[1]

Peranan steganografi merupakan komponen penting dalam proses penyembunyian informasi. Dengan *file* yang terlihat sama sekali tidak mencurigakan, data anda sebenarnya tidak akan terdeteksi dengan mata telanjang. Secara teori, semua *file* umum yang ada dalam komputer dapat digunakan sebagai media, seperti *bmp, jpg, gif* atau dalam *mp3* atau bahkan dalam *file avi* atau *wav*. Semua dapat disajikan dalam tempat tersembunyi, asalkan *file* tersebut memiliki *bit-bit* data redudan yang dapat di modifikasi. *Bit-bit* data redudan artinya *bit-bit* data yang merupakan *bit* ganda yang jika di modifikasi, maka kualitas tampilan *file* yang sesungguhnya tidak akan terganggu banyak.[3]

File-file yang dapat disisipi juga tergantung pada aplikasi steganografi apa yang digunakan kebanyakan aplikasi steganografi memiliki teknik dari ciri khas sendiri dalam menggunakan *file-file* yang menjadi media pelindungnya. Penyisipan data dengan teknik steganografi ini dilakukan sedemikian rupa sehingga informasi yang disisipkan tidak merusak data *digital* yang dilindungi. Data yang disisipkan bersifat tersembunyi keberadaannya tidak disadari oleh indera manusia. Untuk pengamanan data, pemilik data tersebut dapat mengekstraksi data yang telah disembunyikan ke dalam suatu data *digital*.

Dengan melihat penggunaan gambar di internet, maka pada penelitian ini akan dilakukan percobaan untuk melihat salah satu keunikan yang dapat dilakukan di internet, yaitu menyembunyikan gambar pada video yang telah disediakan. Dapat berupa video yang akan diposting di akun media sosial.[11]

II. METODOLOGI PENELITIAN

1. *Jenis Penelitian*

Jenis penelitian yang digunakan adalah penelitian deskriptif dimana memberikan gambaran mengenai apa yang sesungguhnya terjadi. Dalam pembuatan Skripsi ini digunakan metode deskripsif yang menggambarkan fakta-fakta dan informasi secara sistematis, faktual dan akurat.

Penelitian ini dilakukan melalui internet yang dapat memberikan sumber data dan pengetahuan mengenai sistem yang diteliti, kemudian mencocokkan dengan kemungkinan yang terjadi dalam usaha penyelesaian masalah.

2. *Lokasi dan Waktu Penelitian*

Lokasi penelitian dilaksanakan di kampus Universitas Muhammadiyah Parepare Fakultas Teknik Program Studi Teknik Informatika. Adapun waktu penelitian dilakukan selama 2 bulan dimulai pada bulan Juni sampai dengan bulan Oktober tahun 2022.

3. *Alat dan Bahan*

a. Hardware (Perangkat Keras)

Instrumen penelitian yang digunakan selama interaksi pemeriksaan mencakup hal-hal berikut:

Laptop *Asus A516M*, dengan spesifikasi :

Processor : *Processor Intel ® Core ™ i3-7020U CPU @ 2.30GH.z*

RAM : 4 GB

Monitor : 15.6' FHD 1920x1080 16:9

SSD : 256 GB

b. Software (Perangkat lunak)

Produk yang digunakan untuk membuat aplikasi adalah:

Sistem Operasi : *Windows 10 Pro*

Aplikasi : *Pyhton*

Bahasa pemrograman : *Pyhton*

4. *Metode Pengumpulan Data*

Untuk memperoleh data-data yang dibutuhkan dalam rangka melakukan penelitian, maka penulis mengumpulkan data melalui beberapa cara yaitu :

a) Analisis Data
Menganalisa data-data yang sebelumnya telah dikumpulkan.

b) Perancangan Program
Sebagai pedoman dalam penulisan program atau kode-kode agar berjalan sesuai rencana.

c) Uji Coba Program
Pengujian program dilakukan untuk memastikan bahwa program yang dibuat dapat berjalan dengan baik.

d) Evaluasi
Sistem yang telah selesai dibangun perlu adanya evaluasi untuk menemukan kelemahan yang terdapat pada program yang telah dibangun tadi, yang nantinya bisa digunakan sebagai acuan untuk memperbaiki program sehingga lebih sempurna.

e) Jenis Data
Data yang digunakan dalam penelitian ini berupa data-data yang telah dikumpulkan melalui Penelitian Pustaka (*Library Research*). Adapun jenis data primer dan data sekunder yang relevan dengan masalah yang akan dibahas.

f) Data primer
Data Primer adalah data yang berasal atau data yang diperoleh langsung dari sumber data dan pengetahuan.

g) Data Sekunder
Data sekunder adalah data yang diperoleh tidak secara langsung dari objek penelitian. Peneliti

mendapatkan data yang sudah jadi dari internet, *website* dan jurnal.

5. *Tahapan Penelitian*

Tahapan penelitian yang dimaksud dalam penelitian ini ada beberapa tahapan yaitu persiapan penelitian, pengumpulan data, analisis perancangan, pengujian dan implementasi. Adapun Uraian dari tahapan tersebut adalah sebagai berikut :

a) Persiapan Penelitian
Pada tahapan ini peneliti melakukan persiapan penelitian. Persiapan penelitian yang dimaksud adalah menyiapkan buku-buku, artikel-artikel tentang topik penelitian serta *software* yang digunakan selama penelitian.

b) Pengumpulan Data
Pada tahap ini peneliti melakukan observasi dengan peninjauan, pencatatan dan pengamatan langsung di tempat penelitian.

c) Analisis
Pada tahap analisis, peneliti melakukan analisa terhadap sistem yang di terapkan sekarang berdasarkan kemudian merumuskan masalah yang menjadi pokok penelitian sehingga dapat dibuat alternatif pemecahan masalah.

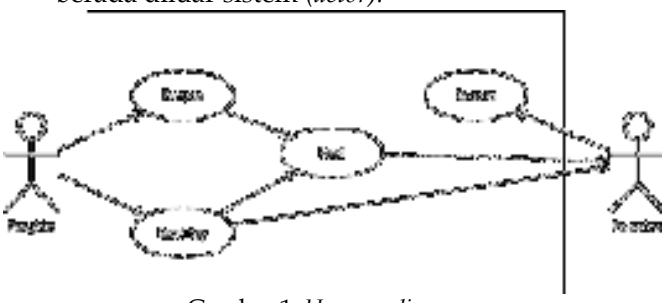
d) Perancangan
Peneliti kemudian merancang aplikasi yang ingin dibuat berdasarkan alternatif pemecahan masalah.

e) Pengujian
Setelah melakukan perancangan, peneliti kemudian menguji hasil perancangan yang telah dibuat. Jika hasil perancangan terdapat kekurangan atau kelemahan maka kembali ke tahap analisis.

f) Implementasi
Setelah pada perancangan tidak terdapat kekurangan maka aplikasi siap untuk di gunakan oleh user

6. *Analisis Kebutuhan Sistem*

a) *Use Case Diagram*
Use case diagram berfungsi untuk menjelaskan alur sistem jika dilihatmenurut pandangan orang yang berada diluar sistem *(actor).*

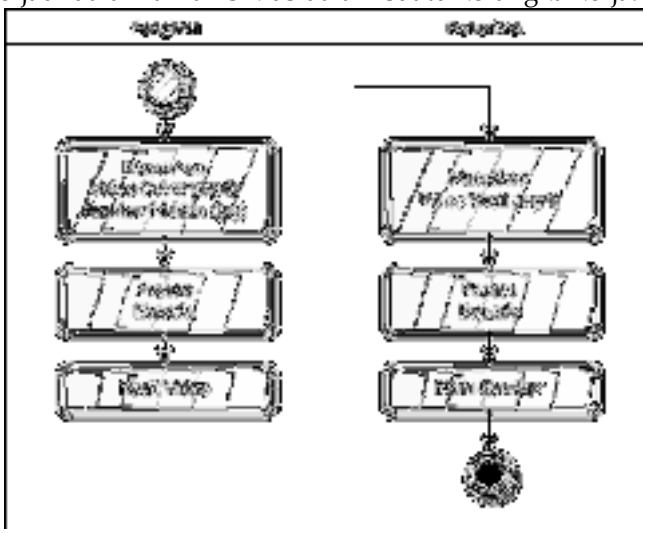


Gambar 1. *Use case diagram*

Dari gambar *use case diagram* diusulkan diatas menjelaskan bahwa pengirim akan membuat *key* dan melakukan *encode*. *Key* dan hasil dari *encode* yang dilakukan pengirim akan diberikan kepada penerima. Penerima akan menerima *key* dan data hasil *encode* yang diberikan pengirim. Penerima akan melakukan *decode*

b) *Activity Diagram*

Activity diagram ini menggambarkan latihan yang terjadi dalam aliran siklus dalam suatu kerangka kerja.

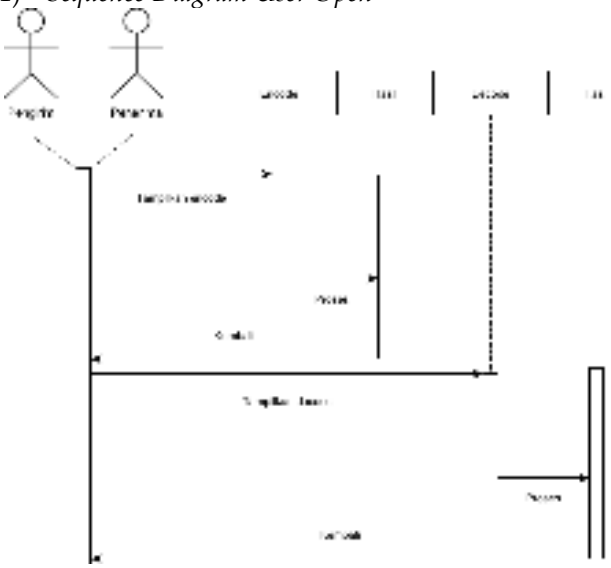


Gambar 2. *Activity diagram*

c) *Sequence diagram*

Sequence diagram adalah bagan komunikasi yang menjelaskan bagaimana suatu kegiatan diselesaikan; pesan (message) apa yang dikirim dan kapan dieksekusi.

1) *Sequence Diagram User Open*



Gambar 3. *Sequence diagram*

III. HASIL DAN PEMBAHASAN

A. Pengujian Sample

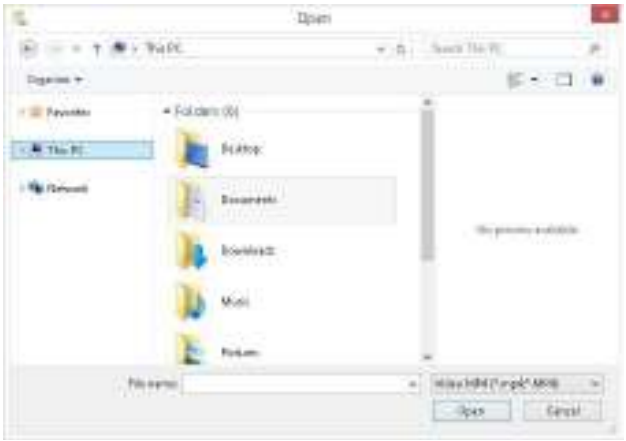
1. Menu Utama

Pada menu halaman utama terdapat pengaksesan untuk pengguna. Pada halaman ini merupakan menu utama yang berada di halaman awal. Menu utama merupakan tampilan awal yang ada pada sistem, yang digunakan untuk menjalankan aplikasi steganografi tersebut. Tampilan menu utama yang terdapat pada

gambar di atas menampilkan bagian *encode* (sebelah kiri) dan bagian *decode* (sebelah kanan). Bagian *encode* berfungsi untuk memasukkan video dan gambar yang akan diproses di *encode.* Sedangkan, *decode* berfungsi untuk memproses hasil video dari *encode.*

Gambar 6. Halaman Menu Utama

2. Menu Pilihan Choose Video



Gambar 7. Tampilan Halaman Menu Choose Video

Pada menu halaman pilihan choose video pada bagian encode berfungsi untuk mengambil video yang dibutuhkan. Format video yang dapat dipilih adalah file ber ekstensi".mp4" atau ".MP4" dari video tersebut akan diproses untuk memasukkan gambar yang akan di sembunyikan dalam video tersebut

3. Halaman Pengujian File Video, File Gambar dan Kata Kunci

Gambar 8. Tampilan Pengujian Pada Encode

Pada halaman pengujian terdapat gambar diatas dapat menyimpulkan bahwa file video dan file gambar yang diinginkan untuk diproses berhasil terpilih dan dapat menampilkan keseluruhan data path yaitu C:/dataku/videocover.mp4untuk file video dan untuk file gambar C:/dataku/imagehidden.jpgdan kemudian untuk mengamankan file harus memasukkan key sebagai kata kunci pengamanan encode agarberjalan dengan baik dan berhasil

B. Pengujian Sistem

1. Pengujian *Black Box*
   a. *Black Box Menu Utama*

Tabel 1. Pengujian pada *Form* Menu Utama

Test Factor	Hasil	Keterangan
Jika pengirim membuka aplikasi steganografi gambar.		Berhasil, karena dapat menampilkan halaman menu utama.
Screen Shoot		

2. Konsep Pengujian

Pengujian merupakan suatu keharusan dalam membuat aplikasi untuk mendapatkan informasi mengenai kualitas dari aplikasi yang telah dibuat dan mengetahui apakah fungsi-fungsi dari aplikasi tersebut telah berjalan sesuai dengan tujuan. Berdasarkan rencana pengujian, maka dapat dilakukan pengujian sebagai berikut.

Tabel 2. Hasil Pengujian Menu Utama

Kasus dan Hasil Uji			
Aksi/ data masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Menekan tombol *Choose Video*	Berpindah pada halaman data video	Pilihan aksisesuai yang diharapkan	Berhasil
Menekan tombol *Choose Image*	Berpindah pada halaman data *image*	Pilihan aksi sesuai yang diharapkan	Berhasil

Menekan tombol Kata Kunci	Menekan tombol pada *encode* pada halaman utama	Pilihan aksisesuai yang diharapkan	Berhasil

Pada pengujian encode 5 video berbeda dengan durasi yang berbeda, masing masing video di diselipkan sebuah gambar dengan resolusi 1280x720, ukuran 99KB, Hasil penyelipan dikatakan berhasil dikarenakan aplikasi berhasil menghasilkan output video yang telah diselipkan gambar.

Tabel 3. Hasil Pengujian Akhir pada *Encode*

Encode				
Sebelum				Sesudah
Video	Resolusi	Durasi	Ukuran	Ukuran
vid1.mp4	576x576	00:21	704KB	129MB
vid2.mp4	576x1024	00:37	1,72MB	928MB
vid3.mp4	576x576	00:40	1,24MB	448MB
vid4.mp4	576x576	00:50	2,09MB	886MB
vid5.mp4	576x576	01:00	2,51MB	542MB

Pengujian decode pada masing masing video, untuk mengeluarkan gambar yang terselip pada video, hasil decode disimpulkan berhasil karena hasil gambar sama dengan gambar yang diselipkan sebelumnya.

IV. KESIMPULAN

Dalam penggunaan *steganografi* gambar video menggunakan metode *Base64* dan *XOR* telah dibuktikan dengan menggunakan metode Pengujian *Black Box* menyatakan aplikasi yang dihasilkan sudah berjalan sesuai dengan kebutuhan dan bebas dari kesalahan. Hasil dari pembuatan aplikasi ini berhasil untuk mengamankan *file-file* penting agar tidak mudah diketahui orang lain. Hasil yang di peroleh dari steganografi menggunakan metode *Base64* dari *encode base64* akan disimpan dalam bentuk gambar sehingga menghasilkan "hasil.jpg dan Hasil gambar yang diproses melalui *LSB* akan diexctract dalam bentuk videoakan menghasilkan gambar.

REFERENSI

[1] Anak Toraja. (2019, 06). Retrieved Juli 06, 2021, from Pengertian UML : Jenis- jenis Diagram UML,Simbol dan Contohnya: https://www.anaktoraja.com/2019/06/pengertian-uml-diagram.html

[2] Andika, D., & Darwis, D. (2020). Modifikasi Algoritma Gifshuffle Untuk Peningkatan Kualitas Citra Pada Steganografi. *Jurnal Ilmiah Infrastruktur Teknologi Informasi*, *1*(2), 19–23.

[3] Anti, U. A., Kridalaksana, A. H., & Khairina, D. M. (2017). *Steganografi Pada Video Menggunakan Metode Least Significant Bit (LSB) Dan End Of File (EOF)*.

[4] Gushari, M. F. (2021). *Penerapan Steganografi Gambar Berwarna pada Delapan Image Cover menggunakan Metode LSB*. Parepare: Universitas Muhammadiyah Parepare.

[5] Heriawanto, D. (2013). *Pemanfaatan algoritma base64 pada keamanan script php (studi kasus: sistem informasi akademik universitas muhammadiyah jember)*. Universitas Muhammadiyah Jember.

[6] Irnanda, Y. (2019). pengamanan web page login menggunakan kombinasi algoritma md5 dan base64 berbasis web server lokal. *Kumpulan Karya Ilmiah Mahasiswa Fakultas Sains Dan Tekhnologi*, *1*(1), 47.

[7] Milanda, Nurwahida. (2020). *Aplikasi Perpaduan Algoritma Enkripsi RC4 dan Base64 Dengan Metode Steganografi LSB Menggunakan Bahasa Pemrograman PHP*. Parepare: Universitas Muhammadiyah Parepare.

[8] Selfi. (2021). *Aplikasi Perpaduan Enkripsi Algoritma Base64 Dengan Metode Steganografi Distrete Cosine Transform (DCT*. Parepare: Universitas Muhammadiyah Parepare

[9] Setyawan, E. H., Novriyenni, N., & Syahputra, S. (2018). Enkripsi pesan teks dengan algoritma one time pad xor dan steganografi pada citra gambar dengan least significant bit. *jtik (Jurnal Teknik Informatika Kaputama)*, *2*(1), 51–59.

[10] Syamsiah, S. (2019). Perancangan Flowchart dan Pseudocode Pembelajaran Mengenal Angka dengan Animasi untuk Anak PAUD Rambutan. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *4*(1), 86–93.

[11] YULI, T. R. I. I. (2013). *metode least significant bit (lsb) citra digital untuk steganografi pada gambar jpeg dan bitmap (bmp)*. upn" veteran" Jawa