ISSN: 2548-9704

# ENKRIPSI PESAN TEKS DENGAN ALGORITMA ONE TIME PAD XOR DAN STEGANOGRAFI PADA CITRA GAMBAR DENGAN LEAST SIGNIFICANT BIT

**Eka Hari Setyawan[1], Novriyenni[2], Siswan Syahputra[3]**

STMIK KAPUTAMA
Program Teknik Informatika
Jln. Veteran No. 4A-9A Binjai, Sumut, Indonesia
setyadisini@gmail.com, novri_yenni@yahoo.com, siswansyahputra90@gmail.com

**ABSTRAK**

Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Kriptografi digunakan agar kerahasiaan pesan tersebut dapat terjaga, sehingga tidak diketahui oleh orang lain. Kriptografi ini muncul atas dasar keamanan dari suatu bentuk informasi-informasi penting yang bersifat rahasia. Steganografi merupakan cara menyisipkan pesan ke dalam media tertentu misalnya gambar, audio, video, dan lainnya. Cara ini terbukti efektif untuk mengamankan pesan teks dengan cara disisipkan pada file gambar, dan pesan tersebut tidak akan diketahui oleh pengguna lain jika didalam gambar yang sudah disisipkan pesan terdapat suatu pesan rahasia. Dan dalam penelitian ini dilakukan proses enkripsi dengan algoritma One Time Pad (OTP) XOR untuk mengubah pesan teks menjadi chiper atau pesan acak dalam bentuk bilangan biner. Kemudian chiper tersebut disisipkan ke dalam file gambar melalui bit-bit paling tidak berarti dengan metode Least Significant Bit (LSB).

**Kata Kunci** : Kriptograf, Steganografi, One Time Pad (OTP), XOR, Least Significant Bit (LSB).

***ABSTRACT***

*Cryptography is the science and art to maintain health. Messages are sent from place to place. Cryptoformation to keep the message secret can be dried, not found by others. This cryptography emerges on the basis of the secret of important information that is confidential. Steganography is a way of inserting messages into the media especially such as images, audio, video, and more. This method proves to be effective for securing text messages inserted in the image file, and the message will not be known by other users if there is a picture that has been inserted messages available secret messages. And in this research is done encryption process with XOR One Time Pad (OTP) algorithm to convert text message into chiper or random message in the form of binary number. Then the chiper is inserted into the bit image file at least using the Least Significant Bit (LSB) method.*

***Keywords****: Cryptograph, Steganography, One Time Pad (OTP), XOR, Least Significant Bit (LSB).*

## 1. PENDAHULUAN

Teknologi sudah menjadi kebutuhan bagi manusia, hampir disemua bagian kehidupan manusia menggunakan teknologi baik untuk kebutuhan pribadi, sosial, karir, maupun bisnis. Dengan adanya teknologi, pekerjaan yang dilakukan akan lebih efisien, cepat dan akurat. Salah satu teknologi yang menjadi kebutuhan manusia adalah komputer. Dengan komputer, user dapat dengan mudah untuk saling

ISSN: 2548-9704

berbagi informasi, baik berupa file, audio, video, dan data-data lainnya.

Namun dibalik berkembangnya 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 munculah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Dari latar belakang di atas, maka dibuatlah sebuah penelitian yang berjudul **"Enkripsi Pesan Dengan Algoritma *One Time Pad Xor* Dan Steganografi Pada Citra Gambar Dengan *Least Significant Bit***

## 2. LANDASAN TEORI

Kemajuan teknologi komputer membantu semua aspek kehidupan manusia, dari hal yang kecil sampai keberbagai 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. Komputer saat ini sudah dipakai oleh berbagai kalangan, seperti pemerintahan, organisasi, militer, bank, pendidikan, transportasi, perdagangan, kriminalitas, industri, dan sebagainya.

Seiring berkembangnya kemajuan teknologi komputer, maka masalah keamanan juga harus ditingkatkan. Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kali kurang mendapat perhatian dari para perancang dan pengelola siistem informasi. Seringkali masalah keamanan berada diurutan setelah tampilan, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performansi dari sistem, seringkali masalah keamanan tidak begitu diperdulikan bahkan ditiadakan.

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. Menurut Ariyus (2006, h. 6-7) ada 4 (empat) ancaman keamanan yang terjadi terhadap informasi, yaitu:

1. *Interruption :* merupakan suatu ancaman terhadap *avaibability*, informasi, data yang ada dalam sistem komputer dirusak, dihapus, sehingga jika data, informasi tersebut dibutuhkan tidak ada lagi.
2. *Interception :* merupakan ancaman terhadap kerahasiaan. Informasi yang ada disadap atau pihak yang tidak berhak mendapat akses ke komputer dimana informasi tersebut disimpan.
3. *Modification :* merupakan ancaman terhadap integritas. Pihak yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan dirubah sesuai dengan keinginan pihak tersebut.

ISSN: 2548-9704

4. *Fabrication :* merupakan ancaman terhadap integeritas. Pihak yang tidak berhak berhasil meniru atau memalsukan suatu informasi yang ada sehingga pihak yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh pihak yang menerima informasi tersebut.

**Pengertian Kriptografi**

Kriptografi berasal dari bahasa yunani, menurut bahasa dibagi menjadi dua yaitu kripto dan graphia, kripto 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 lain.

Algoritma berasal dari Bahasa Arab yaitu *Algorism* yang mempunyai arti proses perhitungan dengan bahasa Arab. Definisi terminologinya, Algoritma adalah urutan langkah-langkah logis untuk penyelesaian masalah yang disusun secara sistematis. Sedangkan Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*". (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan), sehingga kriptografi berarti "*secret writing*" (tulisan rahasia).

Dapat didefinisikan bahwa algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari pihak-pihak yang tidak berhak atas pesan tersebut.

Pada algoritma *One Time Pad* mempunyai cara kerja dimana penerima pesan mempunya salinan kunci yang sama dan kunci tersebut hanya dipakai satu kali (*one time*) untuk enkripsi dan dekripsi dan setelah digunakan maka pad (kertas *blocknot*)harus segera dihancurkan agar tidak bisa dipakai lagi untuk enkripsi dan dekripsi pesan yang lain.Pengirim danpenerimaharus sama-samamemiliki satu set materi kunci yang besar dan juga acak, selamakombinasi dari semuapesan yang pernah dikirimkan. (Fauzi, Maulita & Novriyenni, 2016)

**Pengertian Steganografi**

Steganografi *(steganography)* berasal dari bahasa Yunani yaitu *"steganos"* yang berarti tersembunyi atau terselubung, dan *"graphein"* yang artinya menulis. Steganografi dapat diartikan tulisan tersembunyi *(covered writing).* Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak diketahui. Steganografi membutuhkan 2 (dua) properti, yaitu media penampung dan pesan rahasia.

Media penampung yang umum digunakan dapat berupa sebuah gambar, suara, video, atau teks. Pesan yang dapat disembunyikan dapat berupa sebuah artikel, gambar, kode program, atau pesan lainnya.

## 3. METODOLOGI PENELITIAN

Metodologi Penelitian yang digunakan oleh penulis dalam pengumpulan data adalah sebagai berikut:

1. Wawancara *(Interview),* yaitu melakukan wawancara dengan cara memberikan pertanyaan-pertanyaan kepada pihak-pihak yang berkompeten dibidangnya.

2. Riset Perpustakaan *(Library Reseach),* yaitu mengumpulkan data yang tersedia dari sumber-sumber buku yang ada kaitannya dengan penelitian ini.

ISSN: 2548-9704

3. Browsing / Surfing Internet, memperoleh data dari situs-situs yang berhubungan dengan sistem penelitian ini dan mendownloadnya sebagai bahan refrensi

## 4. HASIL DAN PEMBAHASAN

Berikut ini adalah contoh perhitungan menggunakan algoritma OTP XOR dan akan dilakukkan proses enkripsi dan dekripsi pada plainteks "SAYA" dan kunci "KAMU". Plainteks dan kunci harus diubah menjadi bilangan biner berdasarkan tabel ASCII.

**Tabel 1.** Konversi Plainteks dan Kunci Menjadi Bilangan Biner Berdasarkan Tabel ASCII

| Plainteks | **S** | **A** | **Y** | **A** |
|---|---|---|---|---|
| Biner | 01010011 | 01000001 | 01011001 | 01000001 |
| Kunci | **K** | **A** | **M** | **U** |
| Biner | 01001011 | 01000001 | 01001101 | 01010101 |

Setelah dilakukan proses konversi, langkah selanjutnya adalah proses enkripsi plainteks terhadap kunci dengan OTP XOR.

**Tabel 2.** Proses Enkripsi Plainteks Terhadap Kunci Dengan Algoritma OTP XOR

| Plainteks | 01010011 | 01000001 | 01011001 | 01000001 |
|---|---|---|---|---|
| Kunci | 01001011 | 01000001 | 01001101 | 01010101 |
| **Chiper** | **00011000** | **00000000** | **00010100** | **00010100** |

Pesan "SAYA" setelah dienkripsikan dengan kunci "KAMU" maka akan didapat chiper : 00011000 00000000 00010100 00010100. Chiper tersebut akan disisipkan pada file gambar melalui pixel-pixel gambar, baik gambar *True Color* (24 bit/pixel), *Grayscale Image* (8 bit/pixel), dan *Binary image* (1 bit/pixel). Pada contoh berikut akan digunakan gambar *True Color* (24 bit/pixel) dengan ukuran gambar 100 pixel X 100 pixel = 1000 pixel dikali 24 bit = 24.000 bit. Contoh misalkan segmen pixel-pixel citra/gambar sebelum penambahan bit-bit bernilai (4B, 2F, 33, 62, 2B, S6, 16, 48, 78, 32, 22, 62, 2A, 26, 16, 16, 49, 79, 08, 23, 26, 39, 79, 08, 23, 26, 59, 10, 65, 0D, 27, 4F), maka proses steganografi adalah sebagai berikut:

**Tabel 3.** Contoh Pixel Gambar Asli

| Pixel gambar asli | 4B | 2F | 33 | 62 |
|---|---|---|---|---|
| | 01001011 | 00101111 | 00110011 | 01100010 |
| Pixel gambar asli | 2B | 26 | 16 | 48 |
| | 00101011 | 00100110 | 00010110 | 01001000 |
| Pixel gambar asli | 78 | 32 | 22 | 62 |
| | 01111000 | 00110010 | 00100010 | 01100010 |
| Pixel gambar asli | 2A | 26 | 16 | 16 |
| | 00101010 | 00100110 | 00010110 | 00010110 |
| Pixel gambar asli | 49 | 79 | 08 | 23 |
| | 01001001 | 01111001 | 00001000 | 00100011 |
| Pixel gambar asli | 26 | 39 | 79 | 08 |
| | 00100110 | 00111001 | 01111001 | 00001000 |
| Pixel gambar asli | 23 | 26 | 59 | 10 |
| | 00100011 | 00100110 | 01011001 | 00010000 |
| Pixel gambar asli | 65 | 0D | 27 | 4F |
| | 01100101 | 00001101 | 00100111 | 01001111 |

Pesan "SAYA" : 00011000 00000000 00010100 00010100

Pesan (telah dikonversi ke sistem biner), dan akan disisipkan pada tiap-tiap bit dari pesan tersebut menggantikan posisi LSB dari segmen *pixel-pixel* gambar menjadi:

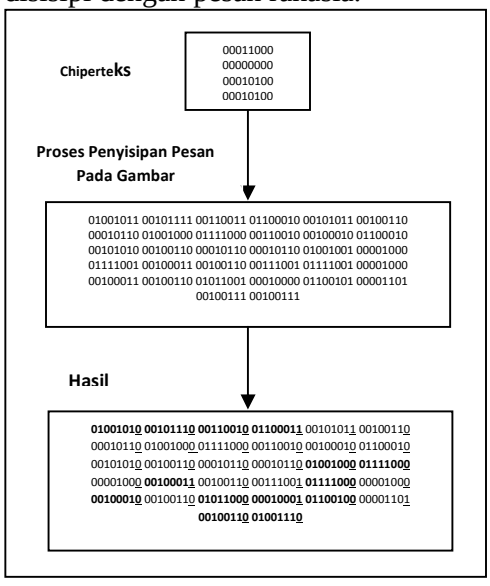
**Tabel 4.** Contoh Pixel Gambar Dengan Pesan Yang Tersembunyi

| Pixel Gambar Dengan Pesan Tersembunyi | 4A | 2E | 32 | 63 |
|---|---|---|---|---|
| | **0100101<u>0</u>** | **0010111<u>0</u>** | **0011001<u>0</u>** | **0110001<u>1</u>** |
| Pixel Gambar Dengan Pesan Tersembunyi | 2B | 26 | 16 | 48 |
| | 0010101<u>1</u> | 0010011<u>0</u> | 0001011<u>0</u> | 0100100<u>0</u> |
| Pixel Gambar | 78 | 32 | 22 | 62 |
| | 0111100 | 0011001 | 0010001 | 0110001 |

ISSN: 2548-9704

| | | | | |
|---|---|---|---|---|
| Dengan Pesan Tersembunyi | 0 | 0 | 0 | 0 |
| Pixel Gambar Dengan Pesan Tersembunyi | 2A | 26 | 16 | 16 |
| | 00101010 | 00100110 | 00010110 | 00010110 |
| Pixel Gambar Dengan Pesan Tersembunyi | 48 | 78 | 08 | 23 |
| | **01001000** | **01111000** | 00001000 | **00100011** |
| Pixel Gambar Dengan Pesan Tersembunyi | 26 | 39 | 78 | 08 |
| | 00100110 | 00111001 | **01111000** | 00001000 |
| Pixel Gambar Dengan Pesan Tersembunyi | 22 | 26 | 58 | 11 |
| | **00100010** | 00100110 | **01011000** | **00010001** |
| Pixel Gambar Dengan Pesan Tersembunyi | 64 | 0D | 26 | 4E |
| | **01100100** | 00001101 | **00100110** | **01001110** |

Terlihat pada bit (garis bawah) diganti dengan representasi biner pesan "SAYA", dan ada 14 (empat belas) bit rendah yang berubah (cetak tebal). Penglihatan mata manusia sangatlah mustahil untuk dapat membedakan warna pada file gambar yang sudah diisi pesan rahasia jika dibandingkan dengan file gambar asli sebelum disisipi dengan pesan rahasia.




**Gambar 1.** Implementasi Algoritma One Time Pad XOR dan Least Significant Bit

Kemudian dilakukan proses dekripsi dengan Algoritma OTP XOR untuk mengembalikan Chiper menjadi Plainteks.

**Tabel 5.** Proses Dekripsi Dengan Algoritma OTP XOR

| | | | | |
|---|---|---|---|---|
| Chiper | 00011000 | 00000000 | 00010100 | 00010100 |
| Kunci | 01001011 | 01000001 | 01001101 | 01010101 |
| **Plainteks** | **01010011** | **01000001** | **01011001** | **01000001** |

## 5. IMPLEMENTASI

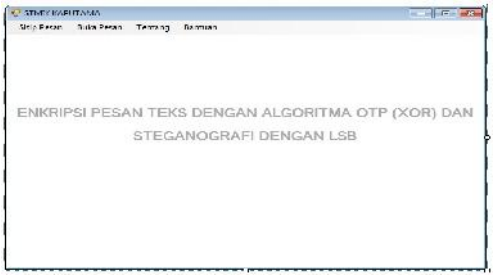
Setelah aplikasi dibangun, akan dilakukan implementasi dan uji coba aplikasi enkripsi pesan dengan algoritma OTP (XOR) dan steganografi dengan algoritma LSB, dan hasil implementasi uji coba aplikasi ini berjalan dengan baik, dan akan dibahas tentang implementasi uji coba aplikasi ini.

### Tampilan Program

Adapun tampilan dari program ini adalah sebagai berikut :

1. Menu Utama

Pada menu ini akan ditampilkan beberapa pilihan menu, yaitu Sisip Pesan, Baca Pesan, Tentang dan Bantuan.

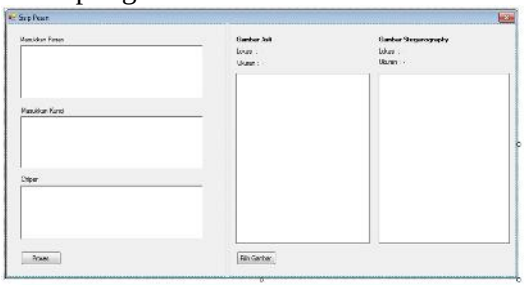



**Gambar 2.** Tampilan Menu Utama

ISSN: 2548-9704

2. Sisip Pesan

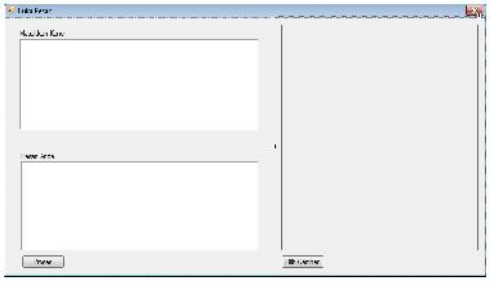
Pada menu ini terdapat beberapa proses yaitu, input pesan, input kunci, dan input gambar.



**Gambar 3.** Tampilan Menu Sisip Pesan

**3.** Buka Pesan

Pada menu ini terdapat beberapa proses yaitu Pilih Gambar, dan Masukkan Kunci. Pesan yang disisipkan pada gambar akan tampil pada bagian Pesan Anda.

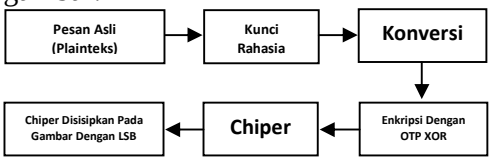


**Gambar 4.** Tampilan Menu Buka Pesan

**Uji Coba**

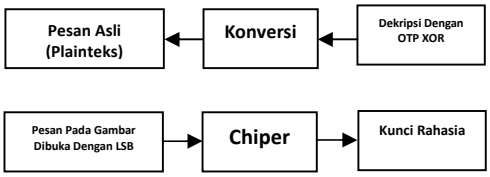
Uji coba terhadap program dilakukan dengan menggunakan VB. Net 2010 yang digunakan untuk membuat program aplikasi didalam komputer sehingga aplikasi yang kita gunakan dapat dijalankan dan diuji coba langsung didalam komputer.

Untuk menjalankan aplikasi ini, pengguna harus mengklik icon aplikasi ini, kemudian pada tampilan pertama, pilih menu buat pesan maka akan muncul layar awal yang berisikan tombol pilih gambar, tombol proses, tombol simpan dan *textbox* masukkan pesan, masukkan kunci, serta *listbox* chiper. Proses uji coba yang dilakukan meliputi proses penyisipan pesan teks pada gambar dan proses membaca pesan yang telah disisipkan pada gambar.




**Gambar 5.** Langkah - Langkah Penyisipan Pesan

Teks asli (plainteks) dan kunci akan dikonversikan terlebih dahulu menjadi bilangan desimal, kemudian dikonversikan kembali menjadi bilangan biner. Hasil konversi dienkripsikan dengan algortima OTP XOR sehingga menghasilkan chiper. Chiper tersebut yang akan disisipkan kedalam bit-bit gambar melalui segmen piksel - piksel dengan cara mengganti nilai bit-bit paling tidak berarti pada gambar dengan algoritma LSB.




**Gambar 6.** Langkah - Langkah Membuka Pesan

Pesan yang terdapat pada gambar yang telah disisipkan sebelumnya akan dibaca dengan algoritma LSB dalam bentuk chiper, kemudian kunci rahasia dimasukkan, dan algortima OTP XOR akan melakukan dekripsi untuk mengubah chiper menjadi pesan dalam bentuk bilangan biner, dan pesan tersebut akan dikonversikan menjadi bilangan desimal dan dikonverikan kembali menjadi karakter, sehingga pesan asli dapat dibaca.

**Uji Coba Penyisipan Pesan**

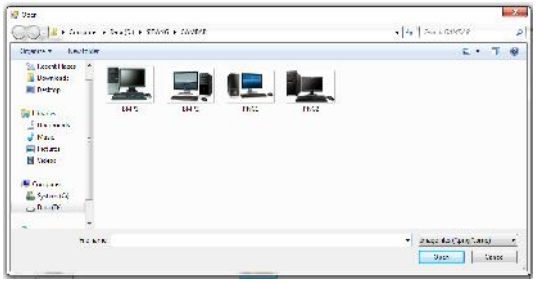
Pada tahap awal proses uji coba yang dilakukan adalah peyisipan pesan teks.

ISSN: 2548-9704

Untuk menyisipkan pesan teks, pada tampilan utama pilih menu "Buat Pesan". Kemudian pengguna harus memasukkan pesan terlebih dahulu pada *textbox* "Masukkan Pesan", dan masukkan kunci rahasia pada *textbox* "Masukkan Kunci". Hal yang harus diperhatikan adalah jumlah karakter kunci yang dimasukkan harus sama dengan jumlah karakter pesan. Kemudian pilih gambar yang akan menjadi media penyisipan dengan cara mengklik tombol Pilih Gambar, maka gambar akan muncul pada *picturebox*. Adapun data yang akan digunakan dalam proses uji coba penyisipan ini adalah sebagai berikut:

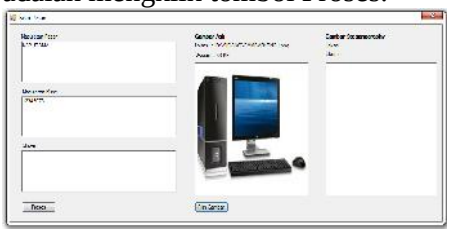
1. Media gambar true color dengan format gambar .bmp.
2. Pesan yang digunakan adalah : KAPUTAM A.
3. Kunci yang digunakan adalah : 12345678.

Langkah pertama buka aplikasi, pada menu utama pilih menu Buat Pesan, kemudian pilih gambar dan masukkan Pesan dan Kunci.



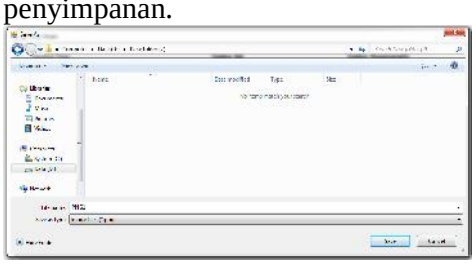
**Gambar 7.** Pemilihan File Gambar

Setelah pesan, kunci, dan gambar dimasukkan, langkah selanjutnya adalah mengklik tombol Proses.



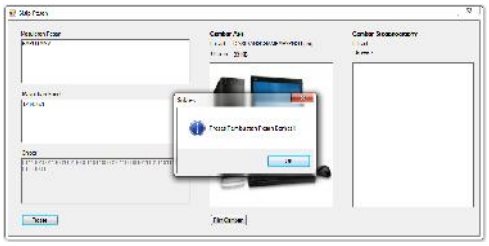
**Gambar 8.** Uji Coba Proses Penyisipan Pesan

Setelah tombol Proses diklik, gambar yang telah disisipkan pesan dapat disimpan kedalam media penyimpanan.



**Gambar 9.** Penyimpanan Gambar Yang Telah Disisipkan Pesan

Setelah file gambar disimpan, akan tampil *MassegeBox* yang memberitahu bahwa "Proses Penyisipan Pesan Berhasil".



**Gambar 10.** Proses Penyisipan Berhasil

Setelah *massegebox* "Proses Penyisipan Pesan Berhasil" muncul, pilih tombol Ok, kemudian akan tampil gambar hasil steganografi pada *PictureBox* Gambar Steganografi beserta ukuran, dan lokasi penyimpanan yang dapat digunakan sebagai perbandingan antara gambar asli dengan gambar yang sudah disisipkan pesan.

**Gambar 11.** Perbandingan Gambar Asli Dengan Gambar Yang Telah Disisipkan Pesan

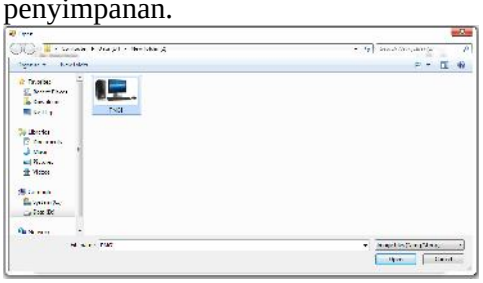
ISSN: 2548-9704

**Uji Coba Buka Pesan**

Pada tahap selanjutnya proses uji coba yang dilakukan adalah proses membuka pesan. Adapun data yang digunakan adalah sebagai berikut:

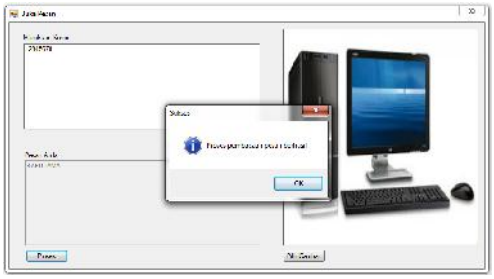
1. Gambar yang telah disisipkan pesan sebelumnya.
2. Kunci : 12345678

Untuk membaca pesan, pada tampilan utama pilih menu "Buka Pesan", kemudian klik tombol Pilih Gambar, dan pilih gambar yang telah disisipkan pesan tersebut pada media penyimpanan.



**Gambar 12.** Pilih Gambar Yang Telah Disisipkan Pesan

Selanjutnya masukkan kunci rahasia yang digunakan pada saat proses penyisipan pesan sebelumnya, dan masukkan pada *Textbox* "Masukkan Kunci". Langkah selanjutnya klik tombol Proses, maka akan tampil *MassegeBox* "Proses Pembacaan Pesan Berhasil" dan pesan dapat dilihat pada *TextBox* "Pesan Anda".



**Gambar 13.** Proses Membaca Pesan Berhasil

## 6. KESIMPULAN

Setelah melakukan serangkaian uji coba aplikasi enkripsi pesan dengan algoritma OTP (XOR) dan steganografi pada citra gambar dengan LSB, didapatlah kesimpulan bahwasanya aplikasi dapat berjalan sesuai dengan yang diharapkan. Namun beberapa hal yang perlu diingat kembali akan diuraikan sebagai berikut:

1. Aplikasi yang dirancang dengan Algoritma *One Time Pad* (OTP) XOR dapat digunakan untuk melakukan proses enkripsi dan dekripsi pada pesan teks dan metode *Least Significant Bit* (LSB) dapat digunakan untuk steganografi pada file gambar.
2. Proses enkripsi dan dekripsi dengan algoritma *One Time Pad* (OTP) XOR dilakukan dengan mengkonversikan pesan dan kunci menjadi bilangan biner, kemudian dilakukan proses proses perhitungan berdasarkan notasi XOR.
3. Proses steganografi dengan *Least Significant Bit* (LSB) dilakukan dengan cara mengganti posisi bit paling tidak berarti (bit paling kanan) pada gambar dengan pesan yang telah dienkripsikan dalam bentuk bilangan biner.

## DAFTAR PUSTAKA

[1] Adi Kurniadi. 2000. *Pemrograman Microsoft Visual Basic 6*, PT. Alex Media Komputindo, Jakarta.

[2] Basuki Rahmat dan Muhammad Fairuzabadi, M. Kom. 2010. *Steganografi Menggunakan Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenere Dan RC4*, Yogyakarta.

ISSN: 2548-9704

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

[4] Dwi Ely Kurniawan dan Narupi. 2016. *Teknik Penyembunyian Data Menggunakan Kombinasi Kriptografi Rijdael dan Steganografi Least Significant Bit (LSB)*, Batam.

[5] Erick Kurniawan. 2011. *Cepat Mahir Visual Basic 2010*, Andi, Yogyakarta.

[6] Hendrayudi. 2010. *Dasar-Dasar Pemrograman Microsoft Visual Basic 2008*, PT. Sarana Tutorial Nurani Sejahtera, Cetakan Pertama, Bandung.

[7] Indra Yatini B. 2010. *Flowchart Algoritma dan Pemrograman Menggunakan Bahasa C++ Builder*, Cetakan Pertama, Graha Ilmu, Yogyakarta.

[8] Michael Sitorus. 2015. *Teknik Steganografi Dengan Metode Least Significant Bit (LSB)*, Jakarta Selatan.

[9] Toyomud S. Waruwu dan Kristin Telaumbanua. 2016. *Kombinasi Algoritma OTP Chiper Dan Algoritma BBS Dalam Pengamanan File*,Medan.

[10]. Fauzi Achmad, Maulita Yani & Novriyenni, 2016. *Perancangan Aplikasi Keamanan Pesan Menggunakan Algoritma Elgamal Dengan Memanfaatkan Algoritma One Time Sebagai Pembangkit Kunci.* ISSN ; 2548-4540