IMPLEMENTASI STEGANOGRAFI DENGAN METODE PENGGABUNGAN BYTE MENGGUNAKAN VISUAL BASIC NET 2008

Suroso[1] , Mustar Aman[2]
Jurusan Sistem Informasi, STMIMInsan Pembangunan
Jl. Raya Serang Km.10 Bitung – Tangerang – Banten
Telp. (021) 59492836, Fax. (021) 59492837
Email[1]: suroso.ip@gmail.com [1] , Email[2]: mustar.ip@yahoo.com [2]

Abstrak : **Keamanan data adalah suatu hal yang sangat penting dalam dunia teknologi yang semakin canggih, dimana dengan data tersebutlah sumber informasi bisa didapatkan. Salah satu cara dalam melindungi data agar informasi yang terkandung didalamnya dapat terjaga dan aman adalah dengan menggunakan steganografi.**
Steganografi merupakan suatu teknik dan seni dalam menyembunyikan informasi (data) dengan menggunakan data lain sebagai media penyimpanan. Dalam paper ini akan dibahas bagaimana suatu data informasi (teks) akan sisipkan kedalam sebuah image (citra digital) dengan metode penggabungan jumlah byte antara image, keyword dan juga teks. Jumlah masing-masing byte dari teks dan keyword adalah hasil konversi dari ASCII menjadi byte dari masing-masing karakter yang terdapat dalam teks dan keyword. Penggabungan jumlah byte dari ketiga unsur tersebut akan dikombinasikan sedemikian rupa sehingga ketiga unsur tersebut akan saling bergantung satu sama lain. Implementasi ini dibuat dengan menggunakan Microsoft Visual Studio 2008 dengan bahasa pemrograman Visual Basic NET (VB.NET)

Kata kunci : **Steganografi, Citra Digital, ASCII, Byte, Encode, Decode**

I. PENDAHULUAN

Perkembangan teknologi komunikasi di Indonesia pada saat ini sangat berkembang cepat dan baik, seperti halnya penggunaan media komunikasi sebagai alat pengiriman pesan, data, dan informasi. Penggunaan teknologi informasi sudah mulai merambah keseluruh lapisan masyarakat baik di lingkungan bisnis, rumah tangga, pelajar maupun mahasiswa. Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang rentan dan harus dijaga untuk proses pengiriman dan maupun penerimaan pesan, data atau informasi. Karena pesan, data dan informasi yang dikirim tanpa adanya keamanan akan mudah di akses oleh orang yang tidak berhak atau berkepentingan di saat proses pengiriman berlangsung yang dapat menyebabkan kerusakan data dan informasi tersebut sudah tidak berguna lagi. Teknik pengamanan data yang saat ini banyak dipakai yaitu kriptografi dan steganografi. Pada kriptografi mengenkripsi pesan yang dapat menimbulkan kecurigaan orang lain, sedangkan steganografi pesan-pesannya tidak menarik perhatian orang lain karena pesan-pesan tersebut dimasukkan ke sebuah media pembawa.

Demi menjaga integritas data, di dalam steganografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/ data yang hendak dikirim berupa data jelas *(plaintext)* diubah menjadi bentuk yang hampir tidak dapat dikenali berupa data random *(ciphertext)* sebagai informasi awalnya dengan menggunakan algoritma tertentu. Sedangkan dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk yang tersamar atau tersembunyi sebelumnya *(chipertext)* kembali menjadi informasi awal *(plaintext).* Hingga saat ini pun, ada banyak sekali model dan metode enkrispi, diantaranya adalah enkripsi dengan algoritma metode manipulasi byte ASCII dengan menggunakan Visual Basic NET 2008.

Pada hakekatnya data adalah fakta yang berupa angka, karakter, simbol, gambar, tanda-tanda, isyarat, tulisan, suara, bunyi yang mempresentasikan keadaan sebenarnya yang selanjutnya digunakan sebagai masukan suatu informasi. Data juga merupakan sumber dari segala informasi yang bisa diolah untuk mengambil suatu keputusan bagi penggunanya. Apalagi sekarang perkembangan teknologi digital sangat berkembang pesat. Banyak juga produk digital yang di hasilkan, salah satu nya adalah citra digital.

Dengan perkembangan teknologi kamera yang semakin canggih yang dapat menghasilkan citra dengan resolusi yang tinggi. Data sangat diperlukan dalam semua aspek kebutuhan informasi. Karena sangat pentingnya data tersebut maka keamanan data adalah satu hal yang mutlak yang harus diperhatikan guna menjaga keaslian data tersebut.

Steganografi menjadi semakin popular setelah kasus pemboman di WTC, 11 September 2001 di Amerika Serikat, teroris menyembunyikan pesan-pesan kegiatan terornya dalam berbagai media yang dapat dijadikan penampung untuk menyediakan *file* seperti pada *image, audio,* dan *video.* Pada peristiwa tersebut disebutlah oleh " pejabat pemerintah dan para ahli dari pemerintahAmerika Serikat" yang tidak disebut namanya bahwa "para teroris menyembunyikan peta-peta dan foto-foto target dan juga perintah untuk aktivitas teroris di ruang *chat sport, bulletin boards* porno dan *web site* lainnya". Dalam perkembangan dengan menggunakan media elektronik dan jaringan

komunikasi, pesan bias dipertukarkan dengan cepat dan tanpa dibatasi jarak dan waktu

II. LANDASAN TEORI

2.1. Sejarah Steganografi

Steganografi adalah teknik menyembunyikan atau menyamarkan keberadaan pesan rahasia dalam suatu media penampung sehingga orang lain tidak menyadari adanya pesan di dalam media tersebut. Kata steganografi pada awalnya berasal dari kata *steganos*, *steganos* sendiri sebenarnya merupakan kata dari bahasa Yunani. Lebih lengkapnya : *steganos* memiliki arti penyamaran atau penyembunyian dan *graphein* atau *graptos* memiliki arti tulisan. Steganografi merupakan paduan antara seni dan ilmu pengetahuan yang mempelajari cara menuliskan pesan tersembunyi. Isi maupun arti pesan tersebut hanya bisa diterjemahkan oleh pembuat dan orang yang berhak menerima pesan. Steganografi menggunakan *file image* dalam *file image* lainnya [4]

Seiring perkembangan teknologi terutama teknologi komputasi juga bertambahnya kebutuhan dan keinginan dengan kontinuitas yang tinggi, steganografi merambah juga ke media digital. Ada dua proses utama dalam steganografi digital yaitu penyisipan (*embedding/encoding*) dan penguraian (*extraction/decoding*) pesan. Pesan dapat berupa *plaintext*, *chipertext*, citra, atau apapun yang dapat ditempelkan ke dalam *bit-stream*. *Embedding* merupakan proses menyisipkan pesan ke dalam *berkas* yang belum dimodifikasi, yang disebut media cover (*cover object*). Kemudian media cover dan pesan yang ditempelkan membuat media stego (*stego object*). *Extraction* adalah proses menguraikan pesan yang tersembunyi dalam media stego. Suatu password khusus (*stego key*) juga dapat digunakan secara tersembunyi, pada saat penguraian selanjutnya dari pesan. Ringkasnya, steganografi adalah teknik menanamkan *embedded message* pada suatu *cover object*, dimana hasilnya berupa *stego object*.

2.2. Citra Digital

Citra atau *image* istilah lain untuk gambar sebagai salah satu komponen multimedia. Memegang peranan yang sangat penting sebagai bentuk informasi visual. Citra mempunyai karakteristik yang tidak dimiliki oleh data, teks yaitu citrakaya dengan informasi. Ada sebuah peribahasa yang berbunyi sebuah gambar bermakna lebih dari seribu kata, maksudnya adalah sebuah gambar dapat memberikan informasi yang lebih banyak dari pada informasi tersebut di sajikan dalam bentuk kata-kata atau *tekstual.* Citra digital saat ini banyak digunakan di berbagai bidang, contohnya dapat dilihat dalam bidang biomedis, penginderaan jauh, visual desain, fotografi, volumetric, dll

2.3. ASCII

ASCII merupakana singkatan dari *American standard code for information interchange* dikembangkan oleh ANSI *(American National Standards Institute)*. Pada awalnya standar ini menggunakan 7 bit untuk menyatakan sebuah kode. Dengan menggunakan 7 buah bit, karakter yang tersedia meliputi karakter control, huruf (A sampai dengan Z dan a sampai dengan z), digit (0 sampai dengan 9), dan sejumlah simbol seperti * dan +. Belakangan ASCII dikembangkan dengan menggunakan 8 buah bit, dengan tambahan sejumlah simbol Yunani dan karakter grafis.

Dalam bidang ilmu komputer menjelaskan bahwa ASCII disebut juga dengan (*American National Standard Code for Internation Interchange).* Fungsi kode ASCII digunakan untuk mewakili karakter-karakter angka maupun huruf didalam komputer, sebagai contoh dapat kita lihat pada karakter 1, 2, 3, A, B, C, dan sebagainya

Contohnya pada huruf W, huruf W diwakili dengan kode ASCII 87. Keseluruhan kode ASCII memiliki 256 karakter, akan tetapi yang digunakan sebagai karakter standard hanya 128 karakter, dimana 32 karakternya digunakan untuk mengendalikan kerja komputer. Karakter-karakter kode ASCII tidak ditampilkan pada layar monitor, dan sisa dari 32 karakter kode tersebut digunakan untuk angka, huruf, atau tanda baca. ASCII merupakan kode standar yang digunakan dalam pertukaran informasi pada Komputer. Setiap simbol yang ada di keyboard memiliki kode ASCII

2.4. Byte

byte merupakan satuan yang digunakan untuk menyatakan sebuah karakter. Sebagai contoh byte pada sistem ASCII dinyatakan dengan sebuah byte. Sebuah byte tersusun atas 8 bit.

Pada papan keyboard, aktifkan numlock (tidak terdapat pada laptop), tekan tombol ALT secara bersamaan dengan kode karakter maka akan dihasilkan karakter tertentu. Misalnya: ALT + 44 maka akan muncul karakter koma (,). Mengetahui kode-kode ASCII sangat bermanfaat misalnya untuk membuat karakter-karakter tertentu yang tidak ada di keyboard

2.5. Encode

Encode merupakan proses penerjemahan kode data-data digital menjadi informasi yang lebih bermakna bagi penggunanya. Format file dapat dianologikan sebagai aturan-aturan standar dengan struktur tertentu

2.6. Decode

decode pada prinsipnya sama dengan fungsi *CASE* yaitu fungsi yang mempunyai struktur *IF-THEN-ELSE*. Bedanya *decode* merupakan fungsi *oracle proprietary* (milik oracle), sedangkan CASE menngunakan fungsi dari *ANSI SQL.*

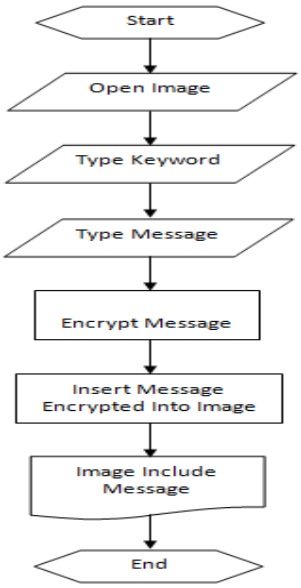
III . PERANCANGAN

a. Perancangan Sistem

Perancangan sistem merupakan tahap awal dalam pembuatan perangkat lunak. Perancangan ini dilakukan untuk mengetahui sistem secara umum [1]. Dalam perancangan ini dibagi menjadi dua bagian yaitu

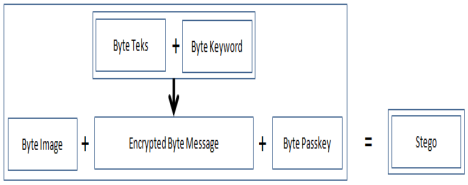
i. Penyisipan *(decoding)*

Pada proses penyisipan dibutuhkan 3 buah masukan yaitu media cover *(image)*, kata kunci *(keyword)* dan pesan rahasia *(text message)* [2]



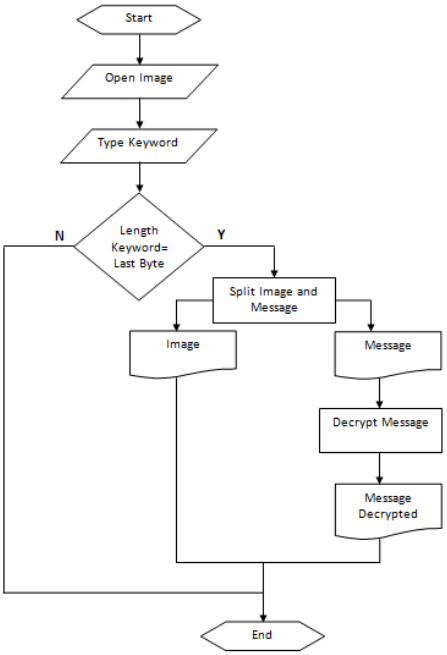
Dari gambar diatas dapat dijelaskan alur proses penyisipan *(encoding)*

- Langkah pertama adalah dengan membuka file image *(citra digital)* sebagai wadah atau penampung dari pesan teks yang akan disisipkan atau disembunyikan.
- Input keyword atau kata kunci. Keyword inilah yang akan dijadikan dasar dalam melakukan enkripsi pada pesan teks yang akan disisipkan.
- Input pesan teks yang akan disisipkan kedalam image *(citra digital)* yang telah disediakan
- Tahap berikutnya adalah proses enkripsi atas pesan teks yang akan dikirimkan. Proses enkripsi sendiri adalah dengan cara mengkombinasikan byte karakter per karakter dari pesan teks dengan byte pada keyword sesuai dengan susunannya. Tujuan dari enkripsi pesan teks ini adalah agar pesan yang terbuka tidak dapat dibaca dengan sempurna jika keyword yang dimasukan salah atau tidak sesuai.
- Setelah pesan teks yang sudah dienkripsi selesai maka langkah berikutnya adalah dengan menggabungkan byte dari image, keyword dan pesam teks yang sudah dienkripsi. Pada byte terakhir akan ditambahkan satu byte yang berisi panjang keyword yang diperlukan sebagai proses ekstraksi *(decoding)*.
- Tahap terakhir dari alur ini adalah menyimpan image tersebut kedalam file image *(citra digital)* yang baru yang tentunya sudah berisi pesan teks yang disembunyikan



ii. Ekstraksi *(encoding)*

Pada proses ekstraksi dibutuhkan 2 buah masukan yaitu stego *(image)* dan kata kunci *(keyword)* [3]



Dari gambar diatas dapat dijelaskan alur proses dari ekstraksi *(decoding)*

- Langkah pertama adalah dengan membuka file image *(citra digital)* yang akan di baca informasinya yang tersembunyi pada image *(citra digital)* tersebut.
- Input keyword sebagai kata kunci untuk dapat membaca informasi teks yang tersembunyi pada image tersebut. Keyword ini harus sama dengan keyword pada saat melakukan penyisipan *(encoding)*, karena keyword ini akan digunakan sebagai dekripsi dari pesan teks yang disembunyikan.
- Jika panjang keyword tidak sama dengan nilai byte terakhir dari total byte image *(citra digital)* yang dibuka maka proses

pembacaan informasi teks pada image *(citra digital)* tersebut tidak dapat dilakukan.

- Tetapi jika panjang keyword sama dengan nilai byte terakhir dari total byte image *(citra digital)*, maka proses berikutnya adalah identifikasi informasi teks yang disembunyikan pada image *(citra digital)* tersebut.
- Setelah semua informasi teks berhasil di identifikasi, tahap berikutnya adalah melakukan dekripsi atas informasi teks tersebut berdasarkan keyword yang sudah di input sebelumnya. Jika keyword yang di input tidak sesuai maka teks yang ditampilkan tidak bisa terbaca sebagai mana mestinya. Artinya pesan teks yang diterima akan berbeda dengan pesan teks yang dikirim

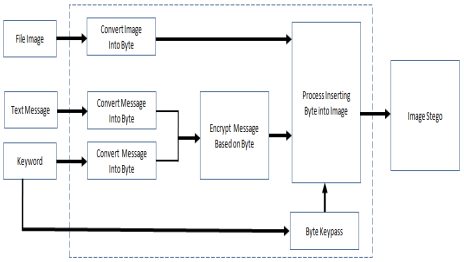
b. Perancangan Algoritma

Ditinjau dari segi fungsional, maka aplikasi yang akan dibangun memiliki dua proses, yaitu proses penyisipan (*encoding*) dan proses ekstraksi (*decoding*). Algoritma proses penyisipan dan ekstraksi dengan metode penggabungan byte dapat dijelaskan sebagai berikut :

i. Penyisipan *(encoding)*

Langkah-langkah proses penyisipan byte pesan (teks) ke dalam media image *(citra digital)* [2] adalah sebagai berikut :

- File image *(citra digital)* akan dibuka dan didapatkan total byte berdasarkan size image *(citra digital)* tersebut. Total byte tersebut akan disimpan dalam array satu dimensi dengan variable **"arrBytePict"**
- Keyword yang akan dijadikan enkripsi pesan teks akan disimpan kedalam array satu dimensi dengan variable **"arrByteKeyword"** dan akan disisipkan setelah byte terakhir image *(citra digital)*. Sedangkan panjang keyword tersebut akan disimpan kedalam variable **"lngLengthKeyword"**
- Pesan teks yang akan disisipkan akan disimpan kedalam array satu dimensi dengan variable **" arrByteMessage"** dan akan disisipkan setelah byte terakhir keyword.
- Proses selanjutnya adalah melakukan enkripsi atas pesan teks tersebut berdasarkan keyword
- Setelah proses penggabungan selesai, tahap selajutnya adalah menambahkan satu byte pada variable **" arrBytePictAndText"** yang berfungsi sebagai keypass proses ekstraksi *(decoding)* yang berisi panjang dari keyword
- Tahap terakhir dari proses ini adalah menyimpan **"arrBytePictAndText"** kedalam file image *(citra digital)* yang baru



ii. Ekstraksi *(decoding)*

Berikut adalah penggalan program untuk proses penyisipan *(encoding)* yang dibuat dengan menggunakan Visual Basic NET 2008 [3]

1. Script untuk mengambil file image *(citra digital)*

```
dgBrowse.Title = "Open Picture Files"
dgBrowse.DefaultExt = "*.jpg"
dgBrowse.Filter = "JPEG|*.jpg|Bitmap|*.bmp|GIF|*.gif"
dgBrowse.ShowDialog()
txtImage.Text = dgBrowse.FileName
```

Fungsi script diatas digunakan untuk membuka file image *(citra digital)* yang ber ekstension *.JPG, *.BMP dan *.BMP

2. Fungsi untuk membaca byte dari image *(citra digital)*

```
Dim tmpLong As Long
picStreamFile = picBufferInfo.OpenRead
lngLengthPict = picStreamFile.Length
tmpLong = lngLengthPict - 1
ReDim arrBytePict(tmpLong)
picStreamFile.Read(arrBytePict, 0, tmpLong)
```

Fungsi script diatas digunakan untuk membaca size image yang telah dibuka dengan metode buffering. Setelah didapatkan size image tersebut *(dalam byte)*, maka size tersebut akan disimpan dalam variable array satu dimensi dengan nama "arrBytePict"

3. Fungsi untuk membaca kode ASCII dari teks keyword

```
For intLoopArr1 As Integer = 0 To (strKeyword.Length - 1)
    ReDim Preserve arrByteKeyword(intLoopArr1)
    arrByteKeyword(intLoopArr1) =
    CByte(AscW(Mid(strKeyword, (intLoopArr1 + 1), 1)))
Next
```

Fungsi script diatas digunakan untuk membaca kode ASCII dari masing-masing karakter teks keyword dan akan disimpan kedalam variable array satu dimensi dengan nama "arrByteKeyword"

4. Fungsi untuk membaca kode ASCII dan proses enkripsi pesan teks

```
For intLoopArr2 As Long = 0 To (strMessage.Length - 1)
    If intLoopKeyWord = lngLengthKeyWord Then
        intLoopKeyWord = 0
    End If
    intModText =
    CByte(AscW(strKeyword.Chars(intLoopKeyWord))) Mod 2
    arrByteMessage(intLoopArr2) =
    CByte(AscW(strMessage.Chars(intLoopArr2)))
    + intModText + 2
    intLoopKeyWord = intLoopKeyWord + 1
Next
```

Fungsi script diatas digunakan untuk membaca kode ASCII dari masing-masing karakter teks pesan yag akan disisipkan dan kemudian akan dilakukan proses enkripsi (manipulasi byte) berdasarkan keyword yang dimasukan. Proses ini akan disimpan kedalam variable array satu dimensi dengan nama "arrByteMessage"

5. Fungsi penggabungan byte

```
For intLoopArr3 As Long =
    0 To (lngLengthPict - 1)
    arrPictAndText(intLoopArr3) =
    arrBytePict(intLoopArr3)
Next
```

Fungsi script diatas digunakan untuk menggabungkan byte-byte dengan susunan byte image, byte keyword, byte message dan byte keypass

6. Tahap terakhir adalah menyimpan berkas image stego berdasarkan proses diatas

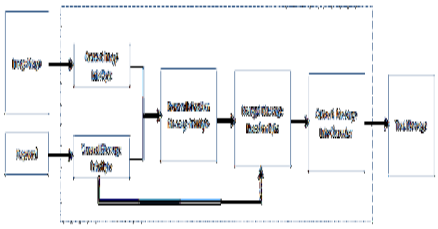
```
dgSave.DefaultExt = "*.jpg"
dgSave.Filter =
"JPEG|*.jpg|Bitmap|*.bmp|GIF|*.gif"
dgSave.ShowDialog()
strNewFile = dgSave.FileName
My.Computer.FileSystem.WriteAllBytes
(strNewFile, arrPictAndText, False)
```

Fungsi script diatas digunakan untuk menyimpan file image kedalam local drive berdasarkan byte-byte yang sudah digabungkan diatas

iii. Ekstraksi *(decoding)*

Langkah-langkah proses ekstraksi byte pesan *(teks)* dari file image *(citra digital)* stego [3] adalah sebagai berikut :

- File image *(citra digital)* akan dibuka dan didapatkan total byte berdasarkan size image tersebut. Total byte tersebut akan disimpan dalam array satu dimensi dengan variable **" arrBytePict"**
- Keyword yang akan dijadikan dekripsi pesan teks akan disimpan kedalam array satu dimensi dengan variable **"arrByteKeyword"** dan panjang keyword tersebut akan disimpan kedalam variable **"lngLengthKeyword"**
- Tahap selanjutnya adalah membanding nilai dari panjang keyword dan nilai byte terakhir dari total image
  Jika nilainya tidak sama maka proses akan berhenti atau tidak melakukan pencarian informasi pesan teks yang disisipkan
- Proses selanjutnya adalah mencari posisi byte-byte yang berisi pesan teks berdasarkan keyword
- Setelah didapatkan posisi byte dari pesan teks yang tersembunyi pada media image, maka tahap selajutnya adalah melakukan dekripsi atas pesan yang telah diekstraksi



Berikut adalah penggalan program untuk proses ekstraksi *(decoding)* yang dibuat dengan menggunakan Visual Basic NET 2008

1. Script untuk membuka file image (stego)

```
dgBrowse.Title =
   "Open Picture Files"
dgBrowse.DefaultExt = "*.jpg"
dgBrowse.Filter =
"JPEG|*.jpg|Bitmap|*.bmp|GIF|*.gif"
dgBrowse.ShowDialog()
txtImage.Text = dgBrowse.FileName
```

Fungsi script diatas digunakan untuk membuka file image *(citra digital)* yang ber ekstension *.JPG, *.BMP dan *.BMP

2. Fungsi untuk membaca byte dari image *(citra digital)*

```
picStreamFile =
 picBufferInfo.OpenRead
gLengthPict =
 picStreamFile.Length
Dim tmpLong As Long
tmpLong = lngLengthPict - 1
ReDim arrBytePict(tmpLong)
picStreamFile.Read
(arrBytePict, 0, lngLengthPict)
```

Fungsi script diatas digunakan untuk membaca size image yang telah dibuka dengan metode buffering. Setelah didapatkan size image tersebut *(dalam byte)*, maka size tersebut akan disimpan dalam variable array satu dimensi dengan nama "arrBytePict"

3. Fungsi untuk membandingkan panjang keyword dengan byte terakhir

```
strKeyword = Trim(txtKeyword.Text)
lngLengthKeyWord = strKeyword.Length
Dim intLastByte As Long
intLastByte = arrBytePict(tmpLong)
If intLastByte <> lngLengthKeyWord Then
    txtMessage.Text = "Wrong key word"
    Exit Sub
End If
```

Fungsi script diatas digunakan untuk membandingkan antara panjang keyword dengan isi dari byte terakhir variable "arrBytePict"

4. Fungsi ekstraksi teks dari image *(citra digital)*

```
Do While (intCounter < (lngLengthPict - _
  arrByteKeyword.Length - 1) And blnStop = False)
  If arrBytePict(intCounter) =
      arrByteKeyword(0) Then
      lngLeftCounter = intCounter + 1
      lngRightCounter = 1
      blnInnerSearch = True
      Do While (blnInnerSearch = True)
         And (lngRightCounter <
         arrByteKeyword.Length)
         And (lngLeftCounter <
         arrBytePict.Length)
          If (arrBytePict(lngLeftCounter) =
             arrByteKeyword(lngRightCounter)) Then
               lngRightCounter = lngRightCounter + 1
               lngLeftCounter = lngLeftCounter + 1
               If (lngRightCounter =
                  (arrByteKeyword.Length - 1)) Then
                  blnStop = True
               Else
                  intCounter = intCounter + 1
               End If
             Else
               blnInnerSearch = False
               intCounter = intCounter + 1
             End If
          Loop
        Else
          intCounter = intCounter + 1
        End If
      Loop
```

Fungsi script diatas digunakan untuk mencari posisi byte yang berisi teks sebanyak byte dalam image *(citra digital)* yang sudah dibaca diatas

5. Fungsi dekripsi atas pesan teks yang sudah didapatkan

```
Do While (lngLeftCounter <
   lngLengthPict - 1)
   If intLoopKeyWord =
      lngLengthKeyWord Then
      intLoopKeyWord = 0
   End If
   intModText =
   CByte(AscW(strKeyword.Chars
   (intLoopKeyWord))) Mod 2
   txtMessage.AppendText
   (ChrW(CInt(arrBytePict(
   lngLeftCounter)) - intModText - 2))
   lngLeftCounter = lngLeftCounter + 1
   intLoopKeyWord = intLoopKeyWord + 1
   Application.DoEvents()
Loop
```

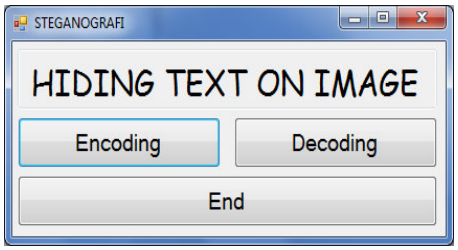
Fungsi script diatas digunakan untuk mengembalikan byte yang sudah dienkripsi sebelumnya. Setelah didapatkan nilai byte nya, selanjutnya adalah menampilkan karakter berdasarkan nilai ASCII dari masing-masing nilai byte

IV. UJI COBA DAN ANALISA

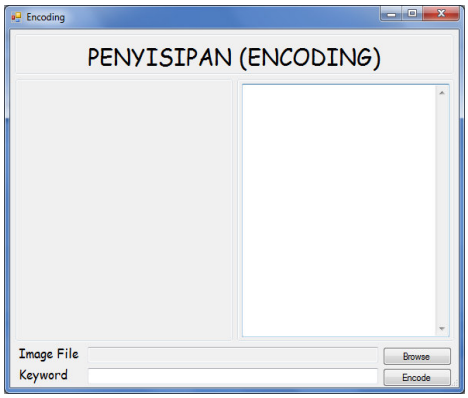
Implementasi dan uji coba aplikasi dilakukan untuk mengetahui sejauh mana system aplikasi tersebut mampu

melakukan penyisipan dan ekstraksi terhadap pesan teks yang disisipkan dalam image *(citra digital)*

- Tampilan awal program aplikasi steganografi yang meliputi Encoding dan Decoding

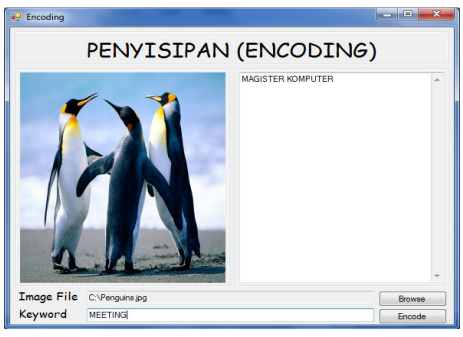


- Tampilan awal proses penyisipan *(Encoding)*

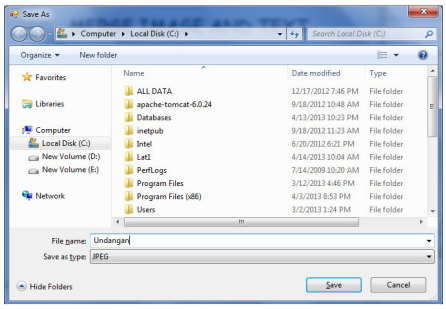


- Input image (citra digital) sebagai object wadah atau penampung pesan teks yang akan disisipkan

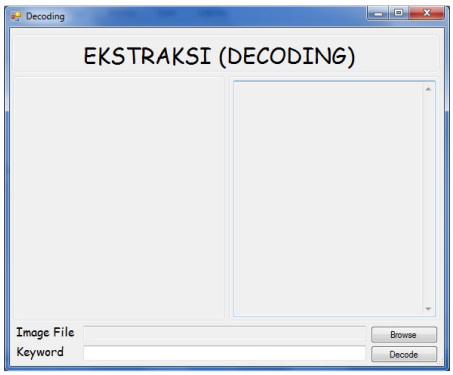
- Setelah image (citra digital) dipilih, selanjutnya adalah input Keyword dan pesan teks yang di sisipkan pada kolom yang telah disediakan



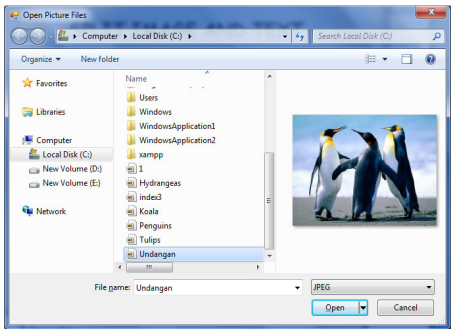
- Setelah semua parameter input terisi, tahap selanjutnya adalah proses penyimpanan stego *(image yang sudah berisi pesan teks yang disembunyikan)*



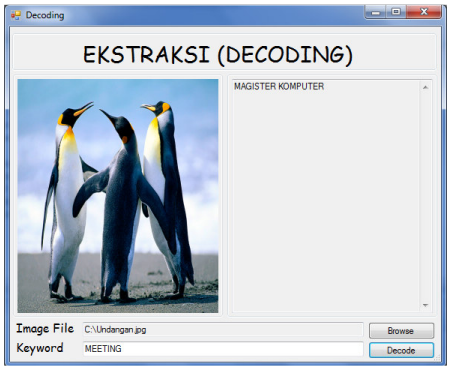
- Tampilan awal proses ekstraksi *(decoding)*



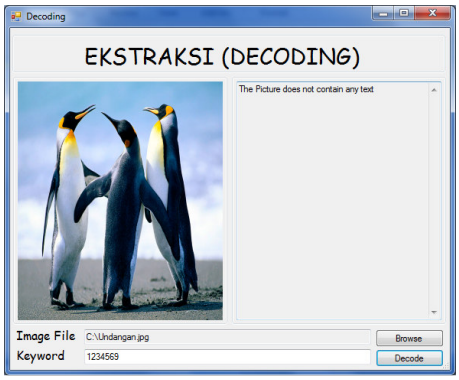
- Selanjutnya adalah membuka image stego untuk mendapatkan pesan teks yang disembunyikan



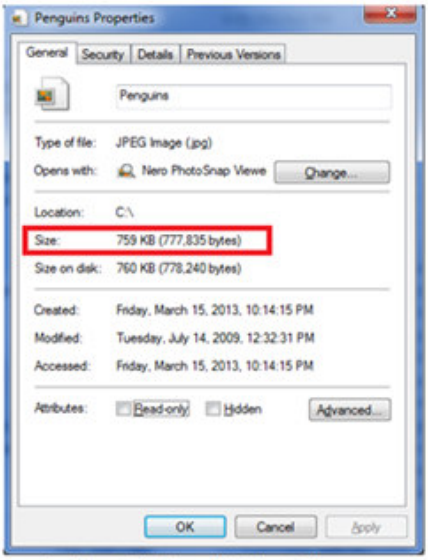
- Setelah image (citra digital) terbuka, selanjutnya adalah input keyword yang sesuai dengan proses penyisipan *(encoding)*



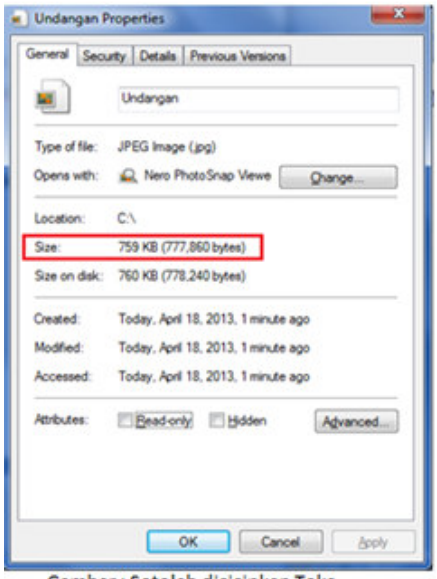
- Jika keyword yang di input tidak sesuai atau tidak sama maka akan keluar output sebagai berikut



- Hasil contoh sampel file image *(citra digital)* sebelum dan sesudah dilakukan penyisipan



Gambar : Sebelum disisipkan Teks



Gambar : Setelah disisipkan Teks

Nama File	Ukuran Data (Byte)	Keyword		Messages		Keypass (Byte)	Stego Data (Byte)
		Text	Byte	Text	Byte		
Penguins. Jpg	777,835	MEETING	7	MAGISTER KOMPUTER	17	1	777,860

Tabel : Sample Image yang diuji coba

V. Kesimpulan

Kesimpulan dari penulisan tentang aplikasi steganografi dengan metode penggabungan byte yang dibuat ini adalah sebagai berikut :

a. Aplikasi steganografi yang dibuat dapat menyisipkan pesan informasi berupa teks yang bersifat rahasia dengan menggunakan media image *(citra digital)*
b. Aplikasi steganografi yang dibuat dapat menghasilkan file image *(citra digital)* relatif lebih besar dari file aslinya tergatung pada banyaknya keyword dan pesan teks yang akan disisipkan.
c. Proses penyisipan teks yang terjadi pada fiIe image *(citra digital)* tidak menyebabkan perubahan yang

berarti pada kualitas image *(citra digital),* sehingga kualitas image *(citra digital)* sukar dibedakan dengan file image *(citra digital)* aslinya

VI. Daftar Pustaka

[1] Koniyo, Andri dan Kusrini. (2007). *Tuntunan Praktis Membangun Sistem Informasi Akuntansi dengan Visual Basic dan Microsoft SQL Server*. Yogyakarta : C.V Andi Offset

[2] Mulyanta S. Edi. (2006). *Special Workshop Teknik Airbrush Menggunakan Adobe Photoshop CS2*. Yogyakarta : C.V Andi Offset

[3]Suprato, Tommy. (2009). *Pengantar Teori Dan Manajemen Komunikasi*. Yogyakarta : MedPress

[4] Enterprise, Jubilee. (2010). *13 Ancaman PC dan Cara Mengatasinya*. Jakarta : PT Elex Media Komputindo