TEKNIK STEGANOGRAPHY DENGAN METODE LEAST SIGNIFICANT BIT (LSB)

Conference Paper · September 2015

DOI: 10.13140/RG.2.2.14942.23362

1 author:

Michael Sitorus
University of Satya Negara Indonesia
6 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Jurnal Ilmiah Fakultas Teknik LIMIT'S
Volume 11 No. 2 September 2015 Halaman 54 ISSN 0216-1184

TEKNIK STEGANOGRAPHY DENGAN METODE LEAST SIGNIFICANT BIT (LSB)

Michael Sitorus
Universitas Satya Negara Indonesia
Jalan Arteri Pondok Indah No. 11 Kebayoran Lama, Jakarta Selatan 12240
email : mr.michaelsitorus@gmail.com

ABSTRAK

Steganografi adalah metode untuk menyembunyikan informasi pada sebuah media, bisa berupa media gambar, suara ataupun video. Aspek terpenting pada steganografi adalah tingkat keamanan penyembunyian informasinya, yang mengacu pada seberapa besar ketidakmampuan pihak ketiga dalam mendeteksi keberadaan informasi yang tersembunyi. Tujuannya untuk menghindari kecurigaan.

Steganografi yang umum digunakan adalah penyembunyian informasi text pada media gambar. Namun metode yang sering digunakan masih cukup sederhana sehingga pihak ketiga masih bisa mendapatkan informasi yang disembunyikan.

Sebuah implementasi yang membuat steganografi text pada media gambar menjadi lebih kuat dan aman. Implementasi yang digunakan adalah mengenkripsi pesan text terlebih dahulu dengan sebuah kata kunci menggunakan algoritma kriptografi. Metode yang dipakai adalah Least Significant bit insertion (LSB). Dari hasil uji coba, diketahui bahwa dengan metode Least Significant Bit Insertion (LSB) penyisipan dan ekstraksi pesan dapat dilakukan dengan baik. Jenis pesan yang dapat disisipkan adalah pesan text.
Kata kunci : *Steganografi, Metode LSB, Text*

1. PENDAHULUAN

Komunikasi sudah menjadi bagian dalam kehidupan manusia. Terutama pada era informasi seperti sekarang, komunikasi menjadi hal yang sangat krusial. Ada saat di mana informasi itu bersifat penting dan rahasia. Oleh karena itu metode komunikasi yang digunakan harus dibuat sedemikian rupa sehingga tidak ada pihak lain yang mengetahui tentang informasi tersebut.

Dengan alasan tersebut lahirlah kriptografi, yaitu metode pengolahan informasi dengan algoritma tertentu sehingga menjadi samar dan sulit dimengerti maknanya. Namun metode ini sering menimbulkan kecurigaan pihak ketiga, sebab pesan yang sulit dimengerti pasti sudah diolah dan menunjukkan bahwa pesan itu merupakan informasi penting.

Untuk menghindari permasalahan tersebut maka lahirlah steganografi, yaitu metode menyembunyikan informasi pada sebuah media, bisa berupa media gambar, suara ataupun video. Aspek terpenting dari steganografi adalah tingkat keamanan penyembunyian informasinya, yang mengacu pada seberapa besar ketidakmampuan pihak ketiga dalam mendeteksi keberadaan informasi yang tersembunyi.

Steganografi yang umum dipakai adalah penyembunyian informasi pada media gambar, di mana informasi text dimasukkan ke dalam bit pixel gambar. Namun metode yang sering digunakan masih cukup sederhana sehingga pihak ketiga masih bisa mendapatkan informasi yang disembunyikan. Oleh karena itu makalah ini membahas tentang sebuah implementasi yang membuat steganografi text pada media gambar menjadi lebih kuat dan aman. Dengan menggunakan algoritma LSB (Least Significant Bit) Embedding Process akan lebih kuat [1].

2. METODOLOGI

Metode penelitian yang di gunakan adalah dengan melakukan pendekatan metode sequence linear yaitu :

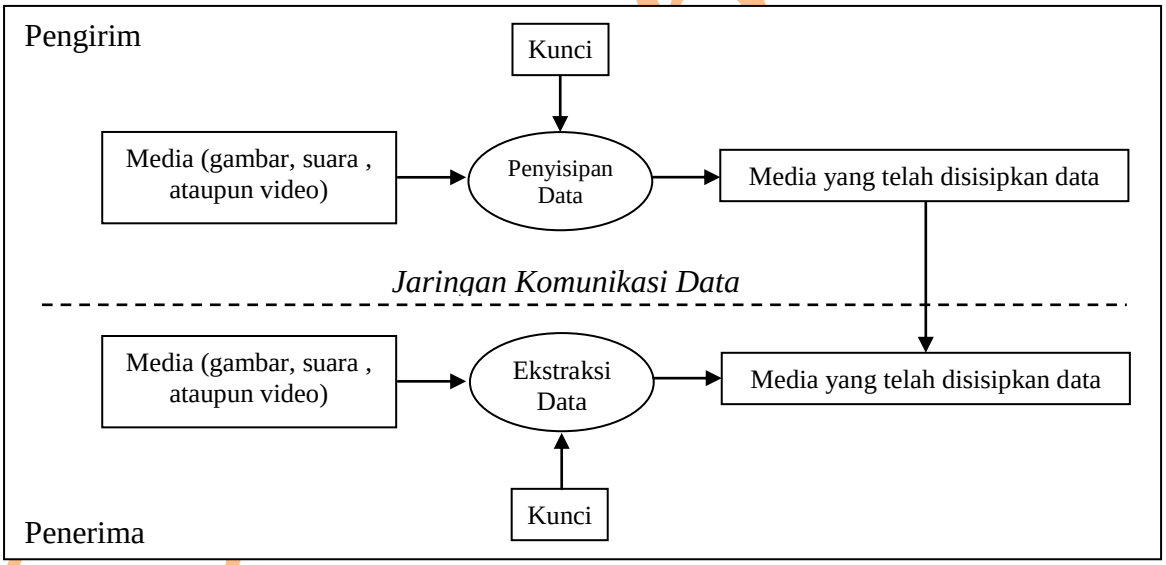
1. Analisa Sistem
   Pada tahapan pertama dilakukan analisa cara kerja dari metode LSB terhadap data teks yang akan di sisipkan ke dalam gambar sebagai media penyisipan dan algoritma yang di gunakan.

2. Perancangan Sistem
   Setelah sistem di analisa selanjutnya di lakukan perancangan sistem yang meliputi pemodelan sistem dengan menngunakan UML dan perancangan antar muka sistem.
3. Implementasi Sistem
   Implementasi sistem meliputi pembuatan kode program dengan menggunakan bahasa pemrograman C#.
4. Pengujian Sistem
   Pengujian sistem di lakukan untuk dapat mengukur besaran data gambar setelah di sisipkan teks dan mengukur waktu kompleksitas algoritma dalam melakukan penyisipan dan ekstrasi data.

3. STUDI LITERATUR

Steganografi (*Steganography*) berasal dari bahasa Yunani *steganos* (*hidden*) dan *gráphein* (*writing*). Jadi, steganografi berarti *hidden writing* (tulisan tersembunyi). Steganografi adalah seni dan ilmumenyembunyikan pesan ke dalam sebuah media dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa sebenarnya ada suatu pesan rahasia. Pada steganografi modern, arti steganografi berkembang menjadi penyembunyian informasi pada sebuah media file digital, bisa berupa media gambar, suara ataupun video.

Pengguna pertama (pengirim pesan) dapat mengirim media yang telah disisipi informasi rahasia tersebut melalui jalur komunikasi publik, hingga dapat diterima oleh pengguna kedua (penerima pesan). Penerima pesan dapat mengekstraksi informasi rahasia yang ada di dalamnya. Penyembunyian data rahasia ke dalam media digital mengubah kualitas media tersebut [2].



Gambar 3.1. Proses Steganography

Dalam penelitian ini adalah menggunakan metode LSB. Sistem Steganografi akan menyembunyikan sejumlah informasi dalam suatu berkas dan akan mengembalikan informasi tersebut kepada pengguna yang berhak. Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia.

Ukuran data yang akan disembunyikan bergantung pada ukuran data penampung. Misalkan saja pada file citra 8-bit yang berukuran 256x256 pixel terdapat 65536 pixel, setiap pixel berukuran 1 byte. Setelah diubah menjadi citra 24-bit, ukuran data bitmap menjadi 65536 x 3 = 196608 byte [3].

Karena setiap byte hanya bisa menyembunyikan satu bit di LSB-nya, maka ukuran data yang akan disembunyikan di dalam citra maksimum 196608/8 = 24576 byte. Ukuran data ini harus dikurangi dengan panjang nama berkas, karena penyembunyian data rahasia tidak hanya menyembunyikan isi data tersebut, tetapi juga nama berkasnya.

Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB). Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir, cetak tebal) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna kuning, maka perubahan satu bit LSB tidak mengubah warna kuning tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut [4]. Misalkan segmen pixel-pixel citra/gambar sebelum penambahan bit-bit adalah:

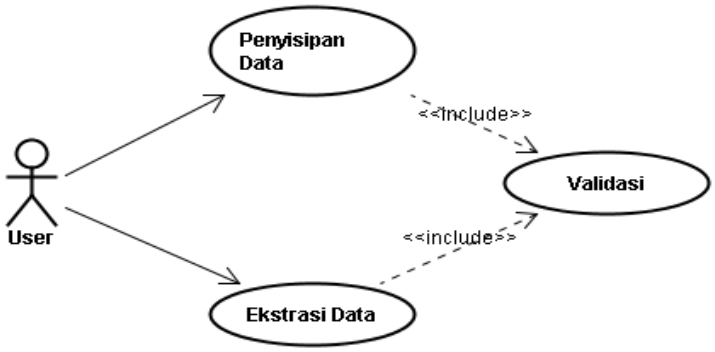
00110011	10100010	11100010
10101011	00100110	10010110
11001001	11111001	

Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan '11100101', maka setiap bit dari pesan tersebut menggantikan posisi LSB dari segmen pixel-pixel citra menjadi (di cetak tebal):

0011001**1**	1010001**1**	1110001**1**
1010101**0**	0010011**0**	1001011**1**
1100100**0**	1111100**1**	

Pada saat ekstrasi data ambil tiap bit dari LSB dari setiap byte pixel pada gambar, selanjutnya bit tersebut di satukan dan konversi ke dalam karakter.

Pemodelan sistem menggunakan UML dengan menggunakan usecase diagram. Aktor pada sistem adalah user dan terdapat dua fungsi dari sistem penyisipan teks ke dalam gambar yaitu fungsi penyisipan data dan ekstrasi data.



Gambar 5.1. Usecase Diagram

Algoritma penyisipan data di gunakan untuk menyisipkan data teks ke dalam gambar.

```
DEKLARASI
charIndex, charValue, pixelElementIndex : integer
zeros, R, G, B : integer
text : string
status : boolean
bmp : Bitmap

ALGORITMA ENKODE DATA
function Bitmap encode (text,  bmp)
BEGIN
  charIndex, charValue, pixelElementIndex ← 0
  zeros, R, G, B ← 0
  FOR (I ← 0; I < bmp.Height ; I++)
    FOR ( j ← 0; j < bmp.Height ; J++)
      clear LSB from each pixel element
      FOR (n ← 0; n<3; n++)
        cekBitProses()
        switchPixelElement()
      END FOR
    END FOR
  END FOR
  return bmp
END
```

```
DEKLARASI
charIndex, charValue, pixelElementIndex : integer
zeros, R, G, B : integer
text : string
status : boolean
bmp : Bitmap

ALGORITMA CEK PEMROSESAN BIT
Function cekBitProses()
BEGIN
  IF (pixelElementIndex MOD 8 → 0) THEN
    IF (status → true AND zeros → 8) THEN
      IF ( (pixelElement – 1) MOD 3  < 2) THEN
        setPixelOfBmp (j, I, COLOR(R, G, B)
      END IF
      return bmp
    END IF
    IF (charIndex >= LengthOfText) THEN
      status ← true; ELSE
      charValue ← text[charIndex++];
    END IF
  END IF
END
```

```
DEKLARASI
charIndex, charValue, pixelElementIndex : integer
zeros, R, G, B : integer
text : string
status : boolean
bmp : Bitmap

ALGORITMA SWITCH PIXEL
Function switchPixelElement()
BEGIN
    SWITCH (pixelElementIndex MOD 3)
    BEGIN
      CASE 0 :
        IF (status → false) THEN
        R ← charValue MOD 2
        charValue DIV 2
        END IF
      CASE 1:
        IF (status → false) THEN
        G ← charValue MOD 2
        charValue DIV 2
        END IF
      CASE 2:
        IF (status → false) THEN
        B ← charValue MOD 2
        charValue DIV 2
        END IF
    END SWITCH
    pixelElementIndex ← pixelElementIndex + 1
    IF (status → true) THEN
      Zeros ← zeros +1
    END IF
END
```

Algoritma ekstrasi data di gunakan untuk mengambil teks yang teradapat pada gambar dengan menggunakan kunci yang cocok.

```
DEKLARASI
colorUnitIndex, charValue : integer
bmp : Bitmap
extractedText : String
pixel : Pixel
C : Char

ALGORITMA EKSTRASI DATA
Function String ektrak(bmp)
BEGIN
   colorUnitIndex ← 0
   charValue ← 0
   FOR (I ← 0; I < bmp.Height; I++)
      FOR (J ← 0; J < bmp.Height; J++)
         FOR (n ← 0; n < 3; n++)
            SWITCH (colorUnitIndex MOD 3)
               CASE 0
                  charValue ← charValue *2 + pixel.R MOD 2
               CASE 1
                  charValue ← charValue *2 + pixel.G MOD 2
               CASE 2
                  charValue ← charValue *2 + pixel.B MOD 2
            END SWITCH
            colorUnitIndex ← colorUnitIndex + 1
            IF (colorUnitIndex MOD 8 → 0)
            THEN
               charValue ← reverseBits(charValue)
               IF (charValue → 0) THEN
                  return extractedText
               END IF
               C ← (Char)charValue
               extractedText ← extractedText + C.toString
            END IF
         END FOR
      END FOR
   END FOR
   return extractedText
END
```

```
DEKLARASI
result, n : integer

ALGORITMA REVERSE BIT
Function reverseBits(n)
BEGIN
   result ← 0
   FOR (I ← 0; I < 8; I++)
      result ← result *2 + n MOD 2
      n ← n /2
   END FOR
   return result
END
```

4. KESIMPULAN

Berdasarkan penelitian dari teknik penyembunyian data dengan metode LSB, maka metode LSB adalah metode yang sederhana dan mudah di aplikasikan ke dalam sistem yang membutuhkan penyisipan data ke dalam gambar.

Dengan menggunakan teknik penyembunyian data ke dalam gambar dapat menjadi media untuk pengamanan data yang akan di kirim. Data rahasia berupa teks dapat di sisipkan ke dalam gambar dengan kunci yang di buat dan di mengerti oleh pengguna aplikasi.

Steganography dapat di implementasikan untuk proses otentikasi data dan di gunakan untuk komunikasi atau pertukaran data yang rahasia. Penggunaan steganography dapat bermanfaat dan mencegah kebocoran informasi dari proses penyadapan.

Teknik penyembunyian data ke dalam gambar dengan menggunakan metode LSB perlu di perbaiki dalam hal pembuatan dan optimalisasi algoritma. Hal ini dapat mempengaruhi performa dari aplikasi pada saat di implementasikan.

Dalam hal pengamanan data pada steganography perlu di kombinasikan dengan penggunaan kriptografi atau dengan penambahan sertifikat pada file yang di jadikan sebagai media penyisipan data.

Pengembangan selanjutnya untuk dapat menyisipkan data ke dalam media yang lain seperti video dan audio.

5. REFERENSI

[1] Andino Maselano. Pengantar Steganography. 2006, Ilmukomputer.com

[2] Morteza Bashardoost, Ghazali Bin Sulong and Parisa Gerami.2013. Enhanced LSB Image Steganography Method By Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression. IJCSI International Journal of Computer Science Issues.Vol. 10, Issue 2, No 1

[3] Linu Babu, Jais John S, Parameshachari B D,Muruganantham C, H S DivakaraMurthy.Steganographic Method for Data Hiding in Audio Signals with LSB & DCT.IJCSMC, Vol. 2, Issue. 8, August 2013, pg.54 – 62

[4] Basuki Rakhmar dan Fairuzabadi. 2010. STEGANOGRAFI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DENGAN KOMBINASI ALGORITMA KRIPTOGRAFI VIGENÈRE DAN RC4. Jurnal Dinamika Informatika. Volume 5, Nomor 2

[5] H. C. Wu, et al., "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," Vision, Image and Signal Processing, IEE Proceedings -, vol. 152, pp. 611-615, 2005.

[6] J. V. Anand and G. D. Dharaneetharan, "New approach in steganography by integrating different LSB algorithms and applying randomization concept to enhance security," presented at the Proceedings of the 2011 International Conference on Communication, Computing, Rourkela, Odisha, India 474-476, 2011.