Perlindungan Data Informasi Digital Dengan Teknik Steganografi Metode Least Significant Bit

Widiyono*[1], Ari Putra Wibowo[2], Risqiati[3], Anas Syaifudin[4]
[1,2,3,4] Teknik Informatika, STMIK Widya Pratama, Pekalongan
E-mail: *[1]widdyono@gmail.com, [2]ariputra.stmikwp@gmail.com, [3]risqiati24@gmail.com, [24]anzt@gmail.com

Abstrak

Perkembangan teknologi pada era digital dibidang informasi dan komunikasi telah mengubah prilaku masyarakat secara global, serta menyebabkan dunia tanpa batas berkembang secara cepat. Transformasi data pada jejaring secara global menjadi kebutuhan untuk memberikan informasi yang akurat. Transformasi data pribadi pada jejaring secara global akan memungkinkan menjadikan ancaman bagi pemilik data informasi atas perbuatan pihak lain yang tidak bertanggungjawab untuk tujuan tertentu. Perlindungan data informasi digital menjadi penting untuk menjaga ancaman kejahatan data pribadi, yang akan ditranformasikan melalui jajaring secara global. Teknik Steganografi merupakan cara menyisipkan informasi pada data digital misalnya citra/gambar digital, yang kelihatanya tidak terlihat ada perbedaan serta tidak mengubah informasi yang terkandung pada data digital. Metode Least Significant Bit salah satu metode yang mempunyai kelebihan dalam hal imperceptibility yaitu data hasil embedding dengan data hasil extracting tidak ada perbedaan secara kasat mata. Perlindungan informasi data digital ini dapat diterapkan pada data file citra, dimana disisipkan data/file pesan rahasia.

Kata Kunci*— Perlindungan Data Digital, Steganografi, Least Significant Bit*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah berdampak pada keseluruhan bidang kehidupan manusia dan mengubah prilakau masyarakat, sehingga sering disebut transformasi kultural. Perubahan prilaku masyarakat yang bebas menyebabkan dunia menjadi tanpa batas, perubahan sosial masyarakat yang secara signifikan berlangsung cepat memunculkan interaksi dan transformasi data informasi melalui jejaring secara bebas dan luas [1].

Transformasi data pribadi atau data rahasia pada jejaring secara luas sering dibutuhkan untuk kegiatan transaki seperti marketpace, perbangkan, data kependudukan, data bidang kesehatan dan lain sebagainya [2]. Data informasi dalam bentuk digital pelanggan pada marketplace misalnya, jika tidak ada perlindungan data dapat pula digunakan oleh pihak yang tidak bertanggungjawab untuk kejahatan.

Perlindungan data informasi digital pada penelitian ini difokuskan pada pemberian kode tertentu dengan menyisipkan file kode pesan, pada file citra/gambar digital, sebelum dilakukan transformasi data kejejaring internet [3].

Sebagai contohnya citra motif batik yang telah di hak patenkan disisipkan logo pembuatnya, logo yang didalamnya mengandung deskripsi makna tertentu seperti visi misi , ataupun citra/gambar digital yang didalamnya perlu adanya keterangan hak cipta atau hak paten pemiliknya.

1.1. Steganografi

Steganografi berasal dari bahasa Yunani "stegos" dan "grafia". "Stegos" tersembunyi atau terselubung, sedangkan "grafia" adalah tulisan atau menggambar. Steganografi adalah sebuah teknik untuk menyembunyikan pesan dengan menggunakan sebuah media atau juga disebut cover [4]. Penelitian lainnya mengartikan Steganografi adalah teknik untuk menyembunyikan informasi dalam media yang sesuai seperti teks, gambar, audio atau video, sehingga orang yang berwenang tidak menyadarinya. Penelitian ini menggunakan steganografi yang diterapkan pada citra untuk menyembunyikan pesan rahasia [5].

1.2. Least Significant Bit

Bit atau binary digit adalah unit dasar penyimpanan data di dalam komputer, nilai bit suatu data adalah 0 (nol) atau 1 (satu). Semua data di dalam komputer di simpan kedalam satuan bit citra/gambar. Format pewarnaan di dalam citra gambar seperti monochrome, grayscale, RGB, CMYK juga menggunakan satuan bit dalam penyimpanannya. Sebagai contoh pewarnaan monochrome bitmap (menggunakan 1 bit untuk setiap pikselnya), RGB–24 bit (8 bit red, 8 bit green, 8 bit blue), grayscale menggunakan 8 bit untuk menentukan tingkat kehitaman suatu piksel [6].

LSB (Least Significant Bit) adalah bagian dari barisan data biner yang mempunyai nilai paling tidak berarti/paling kecil. Bit LSB letaknya di paling kanan pada barisan bit. Sedangkan MSB (Most Significant Bit) adalah kebalikan dari LSB, yaitu bit yang mempunyai nilai sangat berarti /paling besar, letaknya di paling kiri pada barisan bit. Sebagai contoh barisan biner angka 27 :

256	128	64	32	16	8	4	2	1
				1	1	0	1	1

Berdasarkan barisan angka biner di atas, angka 1 di paling kanan bernilai 1 yang berarti nilai yang paling kecil (LSB). Sedangkan angka 1 di paling kiri bernilai 16 yang berarti nilai yang paling besar dari barisan bit tersebut (MSB). Pada algoritma LSB bit pesan akan disisipkan pada bit akhir setiap piksel gambar. Pada citra 24 bit, setiap pikselnya terdiri dari 3 byte yang merepresentasikan setiap byte untuk warna RGB. Sebagai contoh dalam gambar berukuran 600 x 500 piksel dapat disisipkan pesan sebanyak 600 x 500 x 3 = 900000 bit pesan, atau dengan kata lain dapat disisipkan 900000/8 = 112500 byte pesan yang dapat disisipkan.

Metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai covertext. 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, digaris-bawahi) 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 tenyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut [7].

2. METODE PENELITIAN

2.1. Tahapan Penelitian

Penelitian akan mengimplementasikan Teknik Steganografi dengan metode LSB (Least Significant Bit) untuk menyisipkan pesan pada cover atau file citra informasi digital. Tahapan penelitian yang dilakukan sesuai Gambar 1. berikurt.

Gambar 1. Tahapan Penelitian

2.1.1. Identifikasi Masalah

Perkembangan teknologi dewasa ini menjadikan media informasi dalam bentuk citra digital difungsikan sangat luas. Informasi berbentuk citra dianggap efektif untuk menyampaikan pesan informasi. Tetapi informasi yang tersebar dijejaring digital seperti media sosial, web side belum tentusesuai dengan citra saat pertama kali di publikasikan. Hal tersebut akan menjadikan informasi yang tersirat pada citra berbeda dengan tujua awalnya. Mudahnya modifikasi citra digital sehingga diperlukan perlindungan citra digital dengan menyisipkan pesan pada citra tersebut. Perlindungan citra ini dapat dicontohkan seperti citra logo, citra produk atau citra informasi yang lainya.

Salah satu cara penyisipan pesan pada citra adalah menggunakan teknik Steganografi dengan metode LSB (Least Significant Bit). Dimana citra digital informasi (cover) dapat disisipi pesan misalnya teks, dengan tidak merubah tampilan citra. Penyembunyian pesan pada citra ini dengan menggunakan metode metode Least Significant Bit yaitu menyisipkan data binier pada bit terkecil.

P-ISSN: 2089-676X
E-ISSN: 2549-0796

2.1.2. Studi Literatur

Studi literatur yang dilakukan dengan mencari teori yang terkait dengan teknik Steganografi pada citra yang digunakan untuk melindungi citra digital. Salah satu metode yang dikembangkan dalam penelitian–penelitihan sebelumnya adalah metode LSB (Least Significant Bit). Metode LSB merupakan metode penyisipan bilangan biner data pada citra digital yang bernilai paling kecil yaitu nilai 0 (nol).

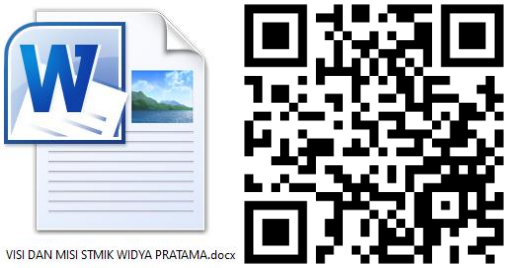
2.1.3. Pengumpulan data

Pengumpulan data pada penelitian ini dengan mengumpulkan data digital seperti citra yang akan dijadikan cover dimana citra yang memungkinkan sering dilakukan manupulasi. Selanjutnya mencari data pesan yang akan diembed kedalam cover citra tersebut. Data informasi citra yang digunakan dalam penelitian ini adalah citra berikut:

1. Data Citra sebagai Cover
   Data citra ini diambil dari kampus STMIK Widya Pratama dan Moseum Batik Pekalongan yaitu citra logo STMIK dan motif batik Jlamprang. Seperti ditunjukan pada Gambar 2.

Gambar 2. Citra Logo STMIK dan Motif Batik Jlamprang

2. Data sebagai Pesan.
   Data sebagai pesan yang disipkan pada penelitian ini berupa file word berisi Visi Misi STMIK Widya Pratama dan file citra barcode lokasi Museum Batik Pekalongan seperti ditunjukan Gambar 3 sebagai berikut:



Gambar 3. File Visi Misi dan Barcode Museum Batik

2.1.4. Eksperimen dan pembuatan aplikasi

Eksperimen dilakukan dengan metode embeding dan exstract pada citra digital dan text. Pembuatan program dilakukan dengan menggunakan bahasa pemprograman java. Cover atau citra yang dimasuki pesan pada eksperimen berupa citra digital logo STMIK Widya Pratama yang disisipkan text visi misi STMIK Widya Pratama dan Citra motif Batik Jlamprang ciri khas Pekalongan yang disisipkan keterangan tentang motif batik Jlamprang.

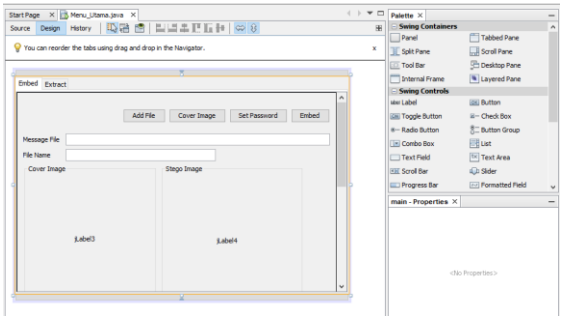
2.1.5. Analisa dan pengujian aplikasi

Pada tahapan ini menganalisa hasil eksperimen dari data yang telah diperoleh yakni citra logo dan citra batik sebagai cover, kemudian menentukan file embed atau file yang akan disisipkan kedalam citra cover. Hasil analisa bahwa dapat dilakukan embed/sisipan jika citra

P-ISSN: 2089-676X
E-ISSN: 2549-0796

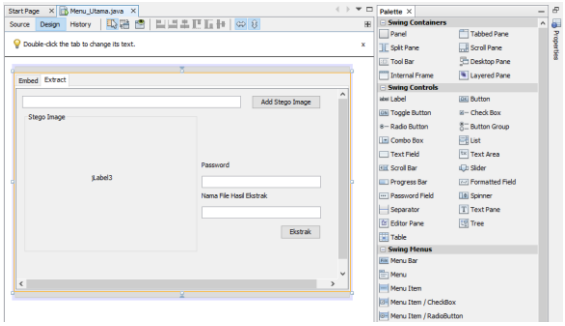
cover berukuran lebih besar dari ukuran kapasitas pesan yang disisipkan. Kemudian ukuran kapasitas file yang disispkan maksimal setengah ukuran kapasitas citra cover.

Pengujian dilakukan untuk memastikan kebenaran konsep dan metode sesuai dengan alur Steganografi metode Least Significant Bit. Pengujian aplikasi pada proses embed dan proses extract. Proses embed, proses menyisipkan file pesan ke dalam citra cover dengan terlebih dahulu membuat password autentikasi yang akan digunakan untuk proses extract. Pengujian proses embeding ditunjukan seperti Gambar 4.



Gambar 4. Proses Pengujian Embeding

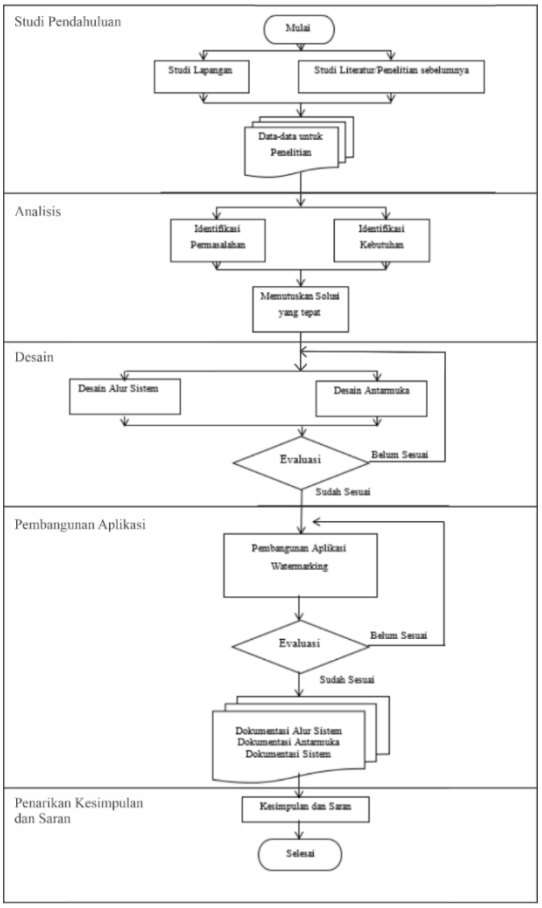
Pada proses extract pengujian dilakukan untuk memastikan keberhasilan pengeluaran file pesan yang telah disisipkan pada citra cover. File yang disispkan dan telah dikeluarkan akan diberikan nama yang diketikan pada kolom, setelah memasukan password dengan benar sesuai password yang dibuat saat embedding. Pengujian proses extract seperti ditunjukan pada Gambar 5.



Gambar 5. Proses Pengujian Extract

2.2. Metode Penelitian

Permasalahan yang akan dibahas dalam penelitian ini adalah bagaimana upaya menerapkan teknik Steganografi dengan metode LSB pada citra untuk perlindungan informasi digital. Untuk itu, langkah-langkah penelitian yang akan dilakukan terlihat pada Gambar 6.

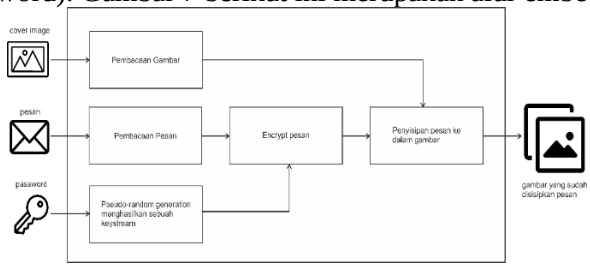


Gambar 6. Metode Penelitian

Gambar 6 menunjukkan tahapan metode penelitian yang dilakukan, terdapat tahapan-tahapan dalam melaksanakan penelitian ini. Desain Alur Proses Sistem pada dasarnya dibagi menjadi dua proses yakni prosdes Embeding dan proses Extract.

2.2.1. Proses Penyisipan (Embed)

Proses penyisipan pesan pada citra digital terdapat 3 (tiga) inputan yaitu gambar citra asli, pesan dan kata kunci (password). Gambar 7 berikut ini merupakan alur embeding.



Gambar 7. Alur proses embed

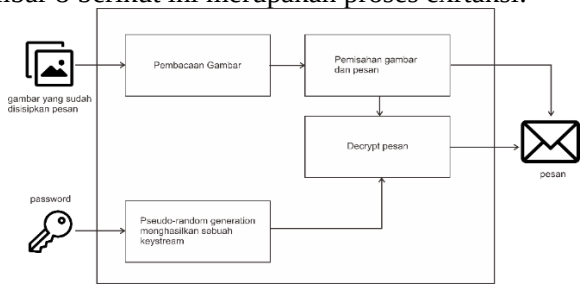
Gambar 7 menunjukkan proses penyisipan pesan ke gambar citra :

1. Mengidentifikasi citra digital yang diinput dan merubah file citra digital menjadi byte
2. Mengidentifikasi pesan dan merubah menjadi byte
3. Mengidentifikasi kata kunci (password) dan melakukan pseudorandom generation untuk menghasilkan keystream
4. Melakukan enskripsi byte pesan dengan logika XOR pada byte pada keysteam

5. Menyisipkan byte pesan yang telah dienskripsi ke dalam citra digital
6. Menyusun ulang byte pada citra digital menjadi stego (Steganografi)

2.2.2. Proses Ekstraksi (Extract)

Proses ekstraksi pesan pada citra digital terdapat 2 (dua) inputan yaitu gambar stego dan kata kunci (password). Gambar 8 berikut ini merupakan proses exrtaksi.



Gambar 8. Alur proses extract

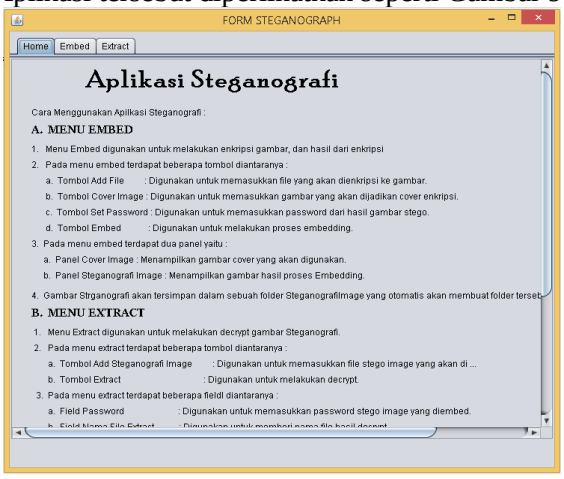
Gambar 8 menunjukkan proses ekstraksi dari gambar stego :

1. Mengidentifikasi gamabr stego dan mengubah menjadi byte
2. Memisahkan byte gambar dan byte pesan
3. Mengidentifikasi kata kunci (password) dan melakukan pseudorandom generation untuk menghasilkan keystream
4. Melakukan dekripsi byte pesan dengan logika XOR tiap byte pesan dengan byte keystream
5. Mengubah byte hasil deskripsi menjadi file.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Penelitian

Setelah dilakukan tahapan-tahapan sesuai metode penelitian, dihasilkan aplikasi Steganografi untuk perlindungan data informasi digital dapat dijalankan pada perangkat laptop ataupun PC Komputer. Aplikasi tersebut diperlihatkan seperti Gambar 9.



Gambar 9. Tampilan Aplikasi Steganografi

3.2. Pembahasan

Penelitian ini mendapatkan temuan bahwa data informasi digital berupa citra dapat disisipi pesan file atau pun citra sebagai informasi privasi dari data digital tersebut. Penyisipan pesan atau embedding dengan teknik steganografi merupakan suatu teknik menyisipkan pesan pada data digital.

Steganografi model Least Significant Bit menyisipkan bit terakhir pada setiap data digital yang bernilai nol. Data citra cover yang disisipi pesan harus lebih besar kapasitasnya dibandingkan dengan kapasitas pesan yang disisipkan. Kapasitas data cover tidak lebih dari 600kb. Sedangkan kapasitas pesan digital yang disisipkan maksimal memiliki kapasitas 100kb.jika akan mendapatak data steganografi cover optimal.

4. KESIMPULAN

Perlindungan data informasi digital berupa citra dapat dilakukan dengan menyisipkan pesan privasi kedalam file citra digital sebelum ditranformasikan ke jejarng internet. Sehingga jika ada modifikasi terhadap data citra tersebut bias dilacak keaslianya dengan cara di lakukan ekstrasi. Perlindungan data informasi digital citra dilakukan dengan menyisipkan pesan.

Teknik steganografi model Least Significant Bit suatu teknik yang digunakan untuk menyisipkan pesan privasi data citra tersebut. Penyisipan dengan teknik ini, dapat dilakukan jika kapasitas citra cover maksimal berukuran 600kb. dan ukuran kapasitas file pesan maksimal 100kb. untuk mendapatakan hasil optimal.

5. SARAN

Dalam bahasan ini memuat saran untuk menutup kekurangan penelitian. Tidak memuat saran-saran selain untuk penelitian yang lebih lanjut.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada xxx yang telah memberi dukungan financial terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Putri Rofifah Nabilah Muchsin, Muhammad Sultan Ririn Aswandi, "Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)," Ledislatif, vol. 3, p. 24, 2020.

[2] Nilam Andaria Kusuma Sari, Satria Unggul Masitoh Indriyani, "Perlindungan Privasi Dan Data Pribadi Konsumen Daring Pada Online Marketplace System," Justitia Jurnal Hukum Universitas Muhammmadiyah Surabaya, vol. 1, 2017.

[3] Rusydi Umar, Anton Yudhana Hermansa, "Pangamanan Pesan Menggunakan Kriptografi Caesar Cipher dan Steganografi EOF pada Citra," J-SAKTI, vol. 4, p. 13, 2020.

[4] Chaerul Umam Lekso Budi Handoko, "Penyembunyian Pesan Menggunakan Steganografi DenganMetode LSB Dan Enkripsi Kritografi," Prosiding SENDI_U, 2019.

[5] Alma,Rini Wisnu Wardhani,Surano Muhasyah,Mutia Delina, "Least Significant Bit Steganography Method for the Digital Data Protection in the Barcode," 2019.
[6] Theodora V.D Pandex, Vanessa Stefanny Sri Wahyuningsih, "Implementasi Visible Watermarking Dan Steganografi Least Significant Bit Pada File Citra Digital," Jurnal TELEMATIKA MKOM Universitas Budi Luhur Jakarta, vol. 8, p. 6, 2016.
[7] Ranganatha, Anupama Jayaram, "Information Hiding Using Audio Steganography 1," The International Journal of Multimedia & Its Applications, vol. 3, p. 11, 2011.