# PENGIRIMAN PESAN *TEXT* DALAM GAMBAR MENGGUNAKAN METODE STEGANOGRAFI

Alif Adriawan[1)], Dahlia[1)], Sahbuddin Abdul Kadir[1)]
[1)] *Dosen Teknik Elektro, Politeknik Negeri Ujung Pandang*

## ABSTRACT

Rapid technological developments and fast data transmission in communication networks can experience tapping data from parties not concerned. Message sending uses Electronic Messages (EMAIL) make it easier for users in terms of efficient time use, data transmission activities in data communication challenges the user in securing information that is possessed in transmitting data to be safe and protected by confidentiality. In this study, the technique of steganography is a security technique for hiding confidential information in other media that seems meaningless, except for people who understand the key. Steganography Technique The Least Significant Bit (LSB) method allows to store 1 bit of data in each primary color which means it can store 3 bits of data symbols in each pixel. By entering characters (messages) and images as media cover, encode the image and then send it by email from the SMTP protocol. Email recipients decode steg-image files to see the characters (messages) inserted. The results of the research carried out by the system on the 99x57 resolution web browser can accommodate 2116 characters. The initial image of the hex value shows a lot of free space, but after encoding the hex value the image becomes full because a message has been inserted.

**Keywords:** *Email, Steganography, Least Significant Bit*

## 1. PENDAHULUAN

Teknologi informasi dalam perjalanannya selalu menghadirkan kemudahan baru bagi umat manusia, termasuk bidang jaringan komputer. Jaringan komputer bukanlah sesuatu yang baru saat ini, hampir di setiap instansi terdapat jaringan komputer untuk memperlancar arus informasi di dalam instansi tersebut. Jaringan komputer adalah sebuah kumpulan komputer yang saling terhubung sehingga memungkinkan pengguna dapat saling bertukar data dan informasi, juga untuk bertukar sumber daya [1]. Di dalam jaringan terdapat baberapa aplikasi pendukung yang mempermudah para penggunanya. Beberapa contoh aplikasi yang dimaksud di antaranya aplikasi *chating* dan *mailer* yang berguna untuk berkomunikasi, *website* dan *blogging* menyampaikan informati terbaru.

Surat elektronik sudah mulai dipakai di tahun 1960-an. Pada saat itu internet belum terbentuk, yang ada hanyalah kumpulan 'mainframe' yang terbentuk sebagai jaringan. Mulai tahun 1980-an, surat elektronik sudah bisa dinikmati oleh khalayak umum. Sekarang ini banyak perusahaan pos di berbagai negara menurun penghasilannya disebabkan masyarakat sudah tidak memakai jasa pos lagi [2]. Untuk mengirim surat elektronik diperlukan suatu program *Email-client*. Dengan program penguna dapat mengirimkan *email* kita pada alamat tujuan melalui jaringan publik, dengan menggunakan *protocol* SMTP. Sedangkan untuk dapat menerima pesan dari pengiriman hasil maka *Email Client* menggunakan *protocol* POP3 atau IMAP.

Pengiriman sebuah pesan dengan bentuk surat yang dikirim menggunakan pos akan membutuhkan waktu yang lama. Sedangkan jika menggunakan *electronic messaging* (*email*), pengiriman data, dokumen maupun gambar bisa diterima dalam hitungan detik. Namun dengan kemajuan teknologi tersebut juga membuat pengiriman pesan menjadi tidak aman. Untuk meningkatkan keamanan dalam pengiriman pesan, dibutuhkan sebuah ilmu atau metode yang bisa menjaga pesan terkirim dengan aman kepada penerima yang dituju, dan tidak terjadi perubahan pesan di tengah jalan oleh pihak ketiga. Ilmu tersebut lebih dikenal dengan sebutan steganografi. Steganografi adalah teknik pengamanan untuk menyembunyikan informasi rahasia didalam suatu media lain yang tampak tidak bermakna, kecuali bagi orang yang mengerti kuncinya. Teknik steganografi menggunakan dua media yang berbeda secara bersamaan, dimana salah satu berfungsi sebagai media yang berisikan informasi rahasia [3].

Steganografi mengambil keuntungan dari konsep dasar gambar untuk menyembunyikan data dengan cara mengubah nilai setiap warna primer yang ada pada setiap *pixel* baik 1 atau 0. Seperti yang kita tahu bahwa semua data digital hanya berupa urutan dari kedua angka ini yakni 1 dan 0, ada beberapa cara untuk mengubah sebuah 1 dan 0, cara yang digunakan oleh Steganografi adalah mengubah angka berdasarkan urutan

[1] Korespondensi penulis: Alif Adriawan, Telp 82348666820, alif.adry11@gmail.com

ganjil maupun genap [3]. Langkah ini memungkinkan kita untuk menyimpan 1 bit data pada setiap warna primer yang berarti kita bisa menyimpan 3 bit simbol data didalam setiap *pixels*.

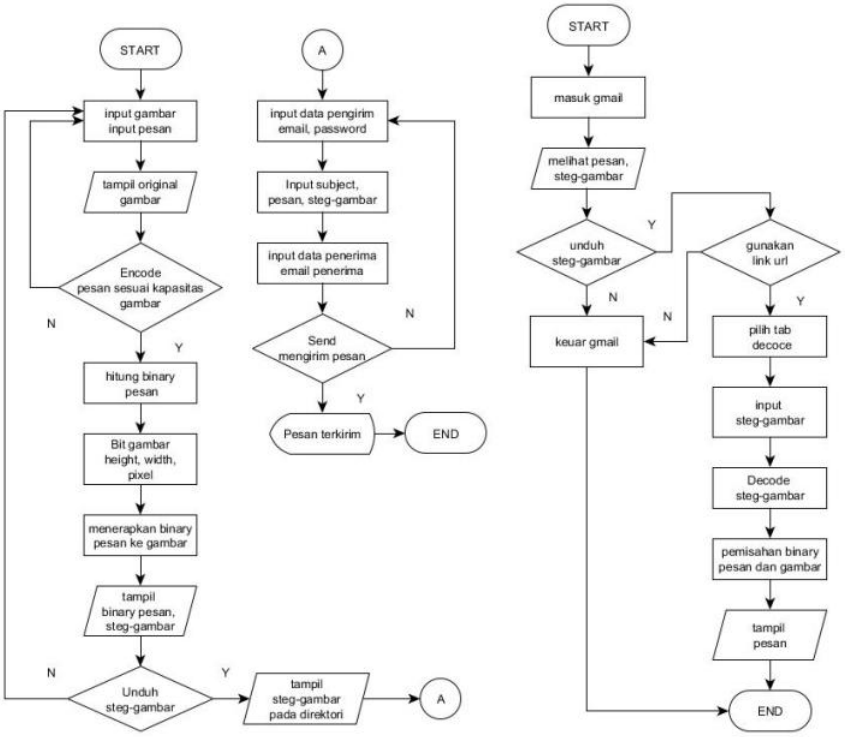
## 2. METODE PENELITIAN

Metode penelitian yang dilakukan adalah analisis terhadap sistem yang telah dibangun. Analisis sistem ini mencakup analisis terhadap masalah seperti bagaimana proses penyisipan pesan pada file gambar dengan metode *LSB*.

A. *Flowchart*

Berikut gambaran *flow chart* perangkat lunak menggunakan Metode LSB. Proses Encode dilakukan dengan memasukkan data gambar yang akan digunakan sebagai media *cover* selaku file yang menjadi canvas. Memasukkan pesan pada teks area, dengan syarat terpenuhi *encode* dilakukan hingga proses berakhir.

*Binary* pesan dan steg-gambar dapat dilihat pada tampilan sistem, dapat dilakukan pengunduhan pada steg-gambar yang telah ada. Data pengirim dilakukan pada proses pengriman, dengan mulai memasukkan alamat *email* serta *password* selaku pengirim pesan, memasukkan *subject*, pesan arahan yang di tujukan pada penerima serta steg-gambar, lalu poin terakhir memasukkan data penerima alamat email yang ditujukan dan tekan tombol kirim.



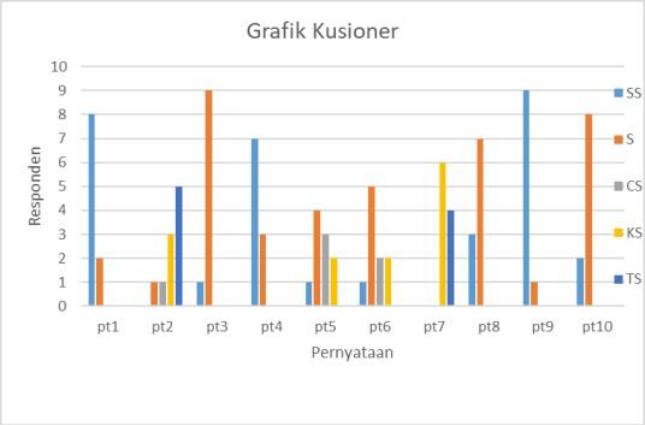

Gambar 1. *Flowchart Encode dan Decode*

## 3. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini yaitu Implementasi pada sistem merupakan sistem keamanan online berbasis web yang memungkinkan user dapat melakukan pengiriman pesan rahasia dengan aman, menampilkan *dashboard* yang merupakan halaman user melakukan *encode*, pengirman email, hingga decode. Sistem informasi web sebagai wadah bagi pengguna steganografi dalam melindungi informasi yang di kirim melalui media online sehingga pesan tidak mudah untuk di kenali serta digunakan. Berikut tampilan *interface* dari sistem informasi web

*I.* Pengujian *Imperectibility*

Pengujian aspek *impercepbility* dari metode steganografi yang dikembangkan dilakukan dengan menyebarkan angket kuesioner kepada beberapa responden. Kuesioner tersebut berisi beberapa pertanyaan dan contoh keluaran yang dihasilkandari proses steganografi. Pengisian kuesioner dilakukan dengan membandingkan tiga buah file, yaitu file cover, file stego, dan file cover hasil dari proses ekstraksi pesan.




Gambar 3. Grafik Kusioner

*II.* Pengujian *Fidelity*

Tabel 1. Hasil Pengujian *Fidelity* pertama

| No | Gambar | Resolusi | Ukuran(kB, byte) | Karakter | Ukuran Steg-gambar (kB, byte) |
|---|---|---|---|---|---|
| 1 | | 1260x672 | 70.8, 72.512 | 10 | 732, 749.794 |
| 2 | | 1260x672 | 70.8, 72.512 | 20 | 732, 749.800 |
| 3 | | 1260x672 | 70.8, 72.512 | 60 | 732, 749.824 |
| 4 | | 1260x672 | 70.8, 72.512 | 100 | 732, 749.852 |
| 5 | | 1260x672 | 70.8, 72.512 | 500 | 732, 750.261 |
| 6 | | 1260x672 | 70.8, 72.512 | 1000 | 733, 750.682 |
| 7 | | 1260x672 | 70.8, 72.512 | 2500 | 734, 751.785 |
| 8 | | 1260x672 | 70.8, 72.512 | 12500 | 740, 758.197 |
| 9 | | 1260x672 | 70.8, 72.512 | 50000 | 765, 784.322 |
| 10 | | 1260x672 | 70.8, 72.512 | 317520 | - |

Tabel 2. Hasil Pengujian *Fidelity* kedua

| No. | Gambar | Resolusi | Ukuran(kB, byte) | Karakter | Ukuran Steg-gambar (kB, byte) |
|---|---|---|---|---|---|
| 1 | | 500x708 | 79.6, 81.606 | 10 | 567, 581.151 |
| 2 | | 500x708 | 79.6, 81.606 | 20 | 567, 581.274 |
| 3 | | 500x708 | 79.6, 81.606 | 60 | 567, 581.344 |
| 4 | | 500x708 | 79.6, 81.606 | 100 | 567, 581.405 |
| 5 | | 500x708 | 79.6, 81.606 | 500 | 568, 582.122 |
| 6 | | 500x708 | 79.6, 81.606 | 1000 | 569, 583.032 |
| 7 | | 500x708 | 79.6, 81.606 | 2500 | 572, 585.920 |
| 8 | | 500x708 | 79.6, 81.606 | 12500 | 585, 599.138 |
| 9 | | 500x708 | 79.6, 81.606 | 25000 | 600, 614.782 |
| 10 | | 500x708 | 79.6, 81.606 | 132750 | - |

Tabel 3. Hasil Pengujian *Fidelity* ketiga

| No. | Gambar | Resolusi | Ukuran(kB, byte) | Karakter | Ukuran Steg-gambar (kB, byte) |
|---|---|---|---|---|---|
| 1 |  | 99x57 | 9.31, .542 | 10 | 11,4, 11.771 |
| 2 |  | 99x57 | 9.31, .542 | 20 | 11,5, 11.795 |
| 3 |  | 99x57 | 9,31, 9.542 | 60 | 11,6, 11.894 |
| 4 |  | 99x57 | 9,31, 9.542 | 100 | 11,6, 11.971 |
| 5 |  | 99x57 | 9,31, 9.543 | 500 | 12,4, 12.771 |
| 6 |  | 99x57 | 9,31, 9.544 | 1000 | 13,0, 13.431 |
| 7 |  | 99x57 | 9,31, 9.545 | 1100 | 13,1, 13.438 |
| 8 |  | 99x57 | 9,31, 9.546 | 1200 | 13,2, 13.538 |
| 9 |  | 99x57 | 9,31, 9.547 | 1500 | 13,4, 13.798 |
| 10 |  | 99x57 | 9,31, 9.548 | 2117 | - |

Pada table di atas pengujian terhadap 3 gambar yang berbeda mulai gambar resolusi 1260 x 672, 500 x 702, dan 99 x 57, pada table 1 gambar dengan resolusi 126x672 dapat menampung karakter sebanyak 317520, dapat juga diperhatikan kapasitas yang digunakan gambar setelah penyisipan karakter menjadi lebih besar. Pada table 2 terjadi peningkatan kapasitas pada gambar resolusi 500x702 setelah penysipan dapat menampung karakter 132750, namun jumlah katarkter yang dapat di sisipkan sangat berbeda dari tabel 1. Pada table 3 gambar dengan resolusi 99x57, jumlah karater yang dapat disisipkan sebanyak 2116, namun dalam penggunaan kapasitas juga minim. Setelah melakukan percobaan pada tiga gambar yang berbeda dengan tingkatan resolusi yang bertahap, dapat di ketahui bahwa gambar yang digunakan sebagai media penyisipan semakin besar resolusinya daya tampung terhadap karakter juga sangat banyak, namun berdampak terhadap kapasitas yang dimiliki juga sangat besar sampai 732 kB, disisi lain dengan menggunakan gambar dengan resolusi 99x57 sebagai media penyisipan dengan jumlah karakter yang disisipkan tidak melebihi 2116 karakter kapasitas yang digunakan 14,299 *bytes*.

*III.* Pengujian *Recovery*

Tabel 4. Hasil Pengujian recovery

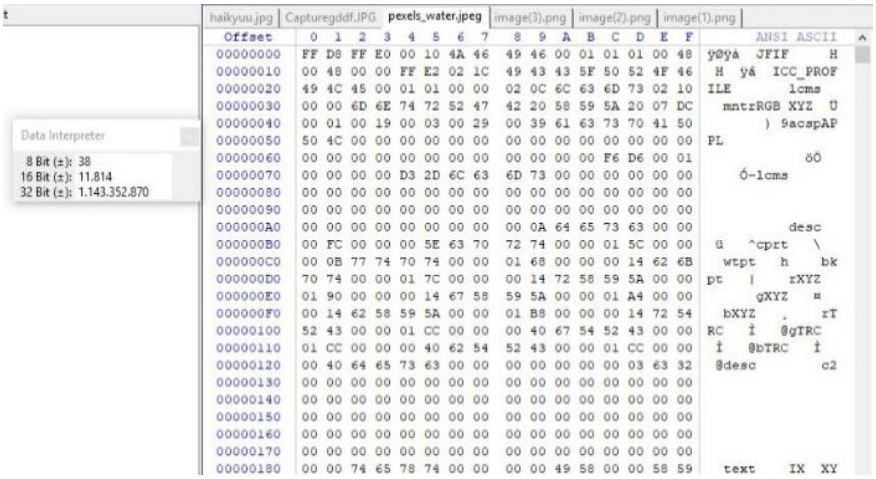
| No. | Gambar | Normal | *Recovery* |
|---|---|---|---|
| 1 |  | ✓ | Yes |
| 2 |  | ✓ | Yes |
| 3 |  | ✓ | Yes |
| 4 |  | ✓ | Yes |
| 5 |  | ✓ | Yes |
| 6 |  | ✓ | Yes |
| 7 |  | ✓ | Yes |
| 8 |  | ✓ | Yes |

Dalam sebuah metode steganografi, kemampuan *recovery* merupakan salah satu aspek penting yang mempengruhi tingkat keberhasilan sebuah metode steganografi. Salah satu cara yang dapat dilakukan untuk melihat dan mengukur kemampuan *recovery* dari sebuah metode steganografi, yaitu dengan cara memeriksa kesamaan pesan yang di sisipkan dengan pesan yang telah diekstrak.

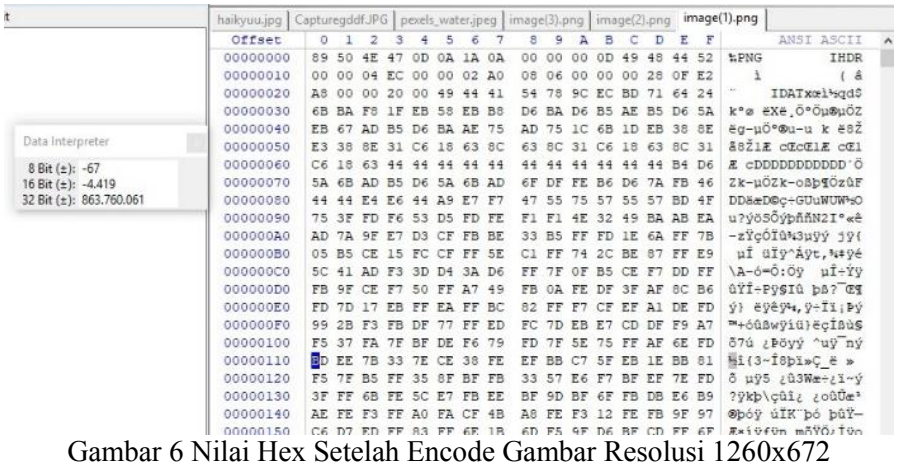
## IV. Pengujian Dengan Nilai *Hex*

Pengujian yang dilakukan dengan mengambil nilai hex dari setiap gambar lalu melihat perbedaan antara nilai hex gambar penampung serta nilai hex steg-gambar, sebagai berikut.

Gambar 4 Water Resolusi 1260x672



Gambar 5 Nilai *Hex* Awal Gambar Resolusi 1260x672



Gambar 6 Nilai Hex Setelah Encode Gambar Resolusi 1260x672

Pada gambar 5 terlihat bahwa nilai *hex* pada gambar tersebut masih terdapat ruang kosong dengan nilai 0 pada offset 0000080 sampai pada offset 0000090 dan juga pada offset 0000130 sampai pada offset 0000170.

Pada kolom Ansi ASCII juga terdapat pesan seperti JEIF yang merupakan bentuk format yang dimiliki oleh gambar tersebut.

Pada gambar 6 terlihat bahwa nilai *hex* pada gambar mengalami perubahan dari nilai *hex* seperti gambar 4.13, nilai *hex* pada gambar 4.14 berubah mulai dari offset 000000 dan seterusnya, ini menandakan nilai *hex* pada gambar 4.14 telah melalui proses *encode* dan terdapat pesan di dalamnya, Lihat pada kolom Ansi ASCII format gambar menjadi PNG serta terdapat IDAText.

## 4. KESIMPULAN

Berdasarkan hasil dari penelitian maka dapat dihasilkan simpulan sebagai berikut :

1. Penyisipan karakter pada gambar dengan resolusi 1260x672 pixel dibatasi hingga 317519 karakter dengan kapasitas 1.112.864 bytes.
2. Gambar awal nilai hex menunjukkan banyak ruang kosong, namun setalah encode nilai hex gambar menjadi penuh karena telah tersisipkan pesan.

## 5. REFERENSI

Roni Setiawan & Edhy Sutanta, "Membangun Aplikasi Chatting Berbasis Multiuser," Membangun Apl. Chating Berbas. Multiuser, vol. 10, no. 1, pp. 1–18, 2009.

M. S. Rizal, "Implementasi algoritma kriptografi kunci-publik ElGamal untuk keamanan pengiriman Email," 2010.

G. M. Arini and T. I. Widyawan, Pengamanan Pesan Steganografi dengan Metode LSB Berlapis Enkripsi dalam PHP. 2012.

R. Munir, "Steganografi dan Watermarking," vol. Bahan Kuli, pp. 1–7, 2004.

A. Sejati, "Studi dan Perbandingan Steganografi Metode EOF ( End of File ) dengan DCS ( Dynamic Cell Spreading )," 2007.

H. M. Amira, "Studi Steganografi pada Image File," Stud. Steganografi pada Image File, 2009.

## 6. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Allah SWT, kedua orang tua, saudara, kedua dosen pembimbing, teman TKJ, seluruh dosen prodi TKJ PNUP serta kerabat dekat penulis.