

ANALISIS KEAMANAN STEGANOGRAFI PADA GAMBAR YANG DIUNGGAH KE MEDIA SOSIAL MENGGUNAKAN LEAST SIGNIFICANT BIT (LSB)

Yoga Bagus Pratama, Fahmi Fachri

Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen
Jalan Raya Kutoarjo km 5 Jatisari, Kebumen, Indonesia
ybp090@gmail.com

ABSTRAK

Di era digital saat ini, keamanan informasi menjadi semakin krusial, terutama dalam konteks penyebaran informasi melalui platform media sosial yang masif. Banyak kejahatan yang terjadi akibat informasi yang disebar ke media sosial. Media yang digunakan berupa file gambar, audio, video dan dokumen. Penelitian ini menganalisis keamanan *steganografi* pada gambar yang diunggah ke media sosial dengan menggunakan *Tools Steghide*. *Steghide* ini menggunakan metode *Least Significant Bit (LSB) substitution* yang memungkinkan penyisipan data ke dalam gambar tanpa mengubah kualitas visual secara signifikan. Tujuan penelitian ini adalah mengevaluasi seberapa baik pesan rahasia yang disisipkan dapat bertahan dari deteksi pihak ketiga, terutama setelah gambar mengalami kompresi atau modifikasi oleh platform media sosial. Metode yang digunakan meliputi penyisipan pesan dalam berbagai format gambar, pengujian kompresi oleh media sosial, dan analisis potensi deteksi oleh teknik *steganalysis*. Hasil penelitian ini menunjukkan bahwa pesan rahasia yang disisipkan dalam gambar dapat terbaca pada platform Facebook Messenger, dan Gmail. Untuk platform WhatsApp beberapa gambar terkompresi dan pesan tidak terbaca. Namun, pada platform Telegram, pesan tidak dapat terbaca setelah gambar mengalami proses kompresi atau modifikasi oleh platform tersebut. Gambar setelah diupload ke media sosial juga mengalami perubahan dari segi ukuran, resolusi dan format.

Kata kunci : *Steganografi, Steghide, Least Significant Bit (LSB), keamanan informasi, media sosial*

1. PENDAHULUAN

Di era digital yang semakin berkembang pesat, keamanan informasi menjadi aspek yang sangat penting dalam kehidupan sehari-hari. Informasi birokrasi di media sosial dapat disampaikan melalui dokumen berbasis teks atau gambar, yang dianggap lebih praktis dan efisien [1]. Dalam era digital ini, email banyak digunakan di dalam dan luar kantor, tetapi email juga rentan terhadap serangan yang mengancam kerahasiaan data seperti pencurian data atau penggunaan data secara tidak sah [2]. Saat ini, perkembangan teknologi informasi berlangsung dengan sangat cepat, dan kejahatan yang memanfaatkan teknologi informasi juga semakin meningkat [3]. Seiring dengan kemajuan pesat teknologi saat ini, proses pengiriman data menjadi semakin mudah. Namun, kemajuan ini juga menimbulkan tantangan besar, terutama dalam hal keamanan data yang dikirim [4]. Dengan semakin banyaknya metode ilegal untuk memperoleh informasi, banyak individu yang berusaha mendapatkan informasi secara tidak sah hanya demi kepuasan pribadi mereka [5]. Berbagai metode kini dapat digunakan untuk mengakses informasi secara ilegal yang bukan hak mereka [6]. Kemajuan teknologi memungkinkan manusia meningkatkan kualitas hidup dengan memanfaatkan teknologi sebagai alat pemenuhan kebutuhan, menciptakan nilai-nilai baru dalam kehidupan sosial, serta mendorong perkembangan dan kemajuan manusia [7]. Namun, di sisi lain, perkembangan ini juga menuntut tanggung jawab lebih besar dalam pengelolaan dan perlindungan

informasi agar kemajuan ini tidak merugikan individu maupun masyarakat.

Keamanan dan kerahasiaan data dan informasi sangat penting selama proses pertukaran pesan dan informasi di internet. Oleh karena itu, teknik penyembunyian data dapat membantu menjaga informasi yang dikirim [8]. Pengiriman dan penerimaan data dan informasi melalui jaringan internet memiliki banyak kelebihan, salah satunya adalah kecepatan transmisi. Namun, kejahatan internet (*cybercrime*) seperti penyadapan dan perubahan data adalah kelemahannya [9]. Selain itu, ada juga serangan *virus*, *spam*, dan *hacker* yang juga dapat membahayakan keamanan data, terutama di media sosial. Media sosial menjadi target utama bagi penjahat siber karena tingginya volume data yang dipertukarkan setiap hari, sehingga perlindungan terhadap data pengguna menjadi semakin penting. Keamanan data mencakup mencegah pihak yang tidak berwenang mengakses data, melindungi data pribadi, mencegah perubahan, dan sebagainya [10]. Oleh karena itu, penerapan sistem keamanan yang kuat, yang mencakup teknik penyembunyian data, merupakan langkah penting dalam menjaga integritas dan kerahasiaan data. Salah satu teknik penyembunyian data yang sering digunakan adalah *steganografi*.

Dalam konteks penggunaan *steganografi* pada gambar digital, salah satu tantangan yang muncul adalah proses kompresi gambar yang dilakukan oleh platform media sosial. Kompresi ini bertujuan untuk mengurangi ukuran file guna menghemat *bandwidth* dan mempercepat pengunggahan. Namun, proses

kompresi tersebut dapat mengakibatkan hilangnya atau rusaknya informasi yang tersembunyi di dalam gambar. Platform seperti *WhatsApp*, *Facebook*, *Gmail*, dan *Telegram* menerapkan kompresi otomatis pada gambar yang dikirim, yang dapat mempengaruhi integritas pesan tersembunyi. Kompresi berpotensi mengubah struktur bit yang digunakan dalam metode *Least Significant Bit* (LSB) untuk menyisipkan pesan, sehingga mengganggu keberhasilan metode steganografi. Penelitian ini melakukan implementasi menyembunyikan pesan ke dalam file gambar dilanjutkan dengan melakukan *steganalisis* terhadap file gambar [11]. Data yang akan diolah pada penelitian ini adalah gambar, pada umumnya tipe gambar yang sering digunakan adalah 8-bit atau 256 warna. Sangat penting untuk mengevaluasi bagaimana pesan yang disembunyikan menggunakan teknik LSB dapat bertahan setelah gambar mengalami kompresi otomatis oleh platform-platform tersebut.

Berdasarkan latar belakang yang telah ada, penelitian ini bertujuan untuk mengevaluasi seberapa baik pesan rahasia yang disisipkan dapat bertahan dari deteksi pihak ketiga, terutama setelah gambar mengalami kompresi atau modifikasi oleh platform media sosial. Dengan melakukan penelitian ini, diharapkan dapat memperoleh pemahaman yang lebih baik mengenai efektivitas teknik steganografi, khususnya dalam konteks penggunaan metode *Least Significant Bit* (LSB) pada file gambar.

2. TINJAUAN PUSTAKA

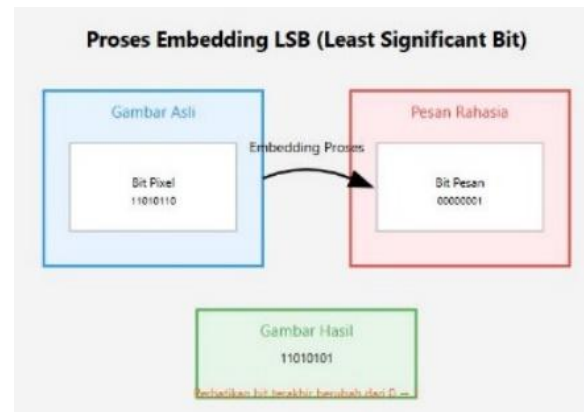
2.1. Steganografi

Steganografi adalah teknik menyembunyikan pesan rahasia di dalam wadah sehingga selain yang berwenang tidak dapat mengetahuinya [12]. Steganografi adalah seni dan ilmu menyembunyikan data pada media lain dengan cara yang membuatnya terlihat lebih halus [13]. Teknik steganografi memanfaatkan dua media yang berbeda pada saat yang sama, satu file rahasia dan satunya file pembawa. Steganografi bertujuan untuk merahasiakan atau menyembunyikan pesan rahasia melalui sebuah media [14]. Steganografi juga dapat menyembunyikan informasi rahasia berupa citra atau gambar dalam media digital [15]. Terdapat dua proses utama dalam steganografi digital yaitu, *embedding/encoding* dan *extraction/decoding*. Singkatnya, steganografi adalah metode menanamkan pesan tertanam pada *cover object*, yang menghasilkan *stego object* [16]. Teknik steganografi yang menggunakan modifikasi *Least Significant Bit* (LSB) adalah salah satu metode paling sederhana untuk menyisipkan informasi ke dalam citra digital sebagai media penutup (*cover medium*) [17]. Sehingga untuk pengembangan *steganography*, perlu dua algoritma utama yang digunakan yaitu, untuk mengembedding dan mengekstrak [18].

2.2. Least Significant Bit (LSB)

Salah satu algoritma dalam steganografi adalah LSB (*Least Significant Bit*), yang dapat menambah

lebih banyak pesan ke media gambar dengan mengganti bit terakhir dari susunan *byte* yang terdiri dari 8 bit dalam gambar [19]. Algoritma ini digunakan karena kemampuannya untuk meningkatkan keamanan media gambar digital ketika digunakan bersamaan dengan enkripsi [20].



Gambar 1. Konsep algoritma LSB

Pada Gambar 1. Misalnya, bit pixel 11010110, kita dapat mengubah bit terakhir menjadi 11010101 untuk menyisipkan informasi rahasia, seperti bit 00000001. Perubahan ini sangat kecil dan praktis tidak terdeteksi oleh mata manusia, sehingga gambar asli terlihat sama persis. Metode ini memungkinkan seseorang menyembunyikan pesan rahasia dalam gambar digital tanpa menimbulkan kecurigaan, dengan cara yang hampir tidak dapat dibedakan dari gambar aslinya.

2.3. Keamanan Data

Keamanan data adalah tindakan yang perlu dilakukan oleh suatu perusahaan atau individu untuk melindungi ekosistem teknologi informasi [21]. Konsep ini menjadi sangat penting di era digital saat ini, di mana informasi memiliki nilai strategis yang tinggi. Adanya keamanan data ini, perusahaan atau individu tidak perlu khawatir lagi apabila terjadi pelanggaran keamanan. Hal ini karena keamanan data dirancang untuk mencegah, mendeteksi, dan merespons potensi ancaman terhadap informasi digital [22].

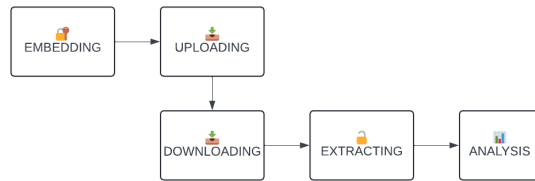
3. METODE PENELITIAN

Pada bagian ini memuat metode yang digunakan pada pembuatan skripsi.

3.1. Tahapan Penelitian

Penelitian ini merupakan penelitian eksperimental, di mana teknik steganografi akan diterapkan pada gambar digital untuk mengamati perubahan yang terjadi pada pesan tersembunyi setelah gambar dikompresi oleh platform media sosial. Penelitian ini akan dilakukan untuk mengevaluasi efektivitas teknik steganografi, khususnya metode *Least Significant Bit* (LSB), dalam menjaga kerahasiaan pesan rahasia yang disisipkan pada file

gambar digital setelah mengalami kompresi atau modifikasi oleh platform media sosial.



Gambar 2. Tahapan Penelitian

a. *Embedding* (Penyisipan Pesan)

Pada tahap pertama, peneliti menyisipkan pesan rahasia ke dalam gambar digital menggunakan teknik *Least Significant Bit (LSB)*. Metode LSB bekerja dengan mengubah bit paling tidak signifikan disetiap *byte* dari citra digital untuk menyembunyikan data tanpa mengubah tampilan visual dari gambar. Proses ini memastikan bahwa pesan tidak terlihat oleh mata telanjang, namun tersimpan dalam data biner gambar. Teknik ini cocok untuk gambar karena perubahan kecil pada bit terakhir (*least significant bit*) tidak akan mempengaruhi kualitas visual secara signifikan. Prosesnya pada bit terakhir dari setiap *pixel* gambar diubah sesuai dengan bit pesan yang ingin disembunyikan.

b. *Uploading* (Pengunggahan ke Media Sosial)

Setelah pesan berhasil disisipkan, gambar diunggah ke platform media sosial seperti *Facebook*, *Instagram*, atau *WhatsApp*. Tahap ini sangat penting karena platform media sosial biasanya secara otomatis melakukan kompresi pada gambar yang diunggah. Kompresi ini bertujuan untuk mengurangi ukuran file gambar agar lebih mudah diunggah dan diakses, tetapi juga bisa merusak struktur bit dalam gambar, yang dapat memengaruhi keberadaan pesan yang disembunyikan melalui steganografi. Tujuannya untuk menguji bagaimana platform media sosial mempengaruhi gambar yang telah disisipkan pesan rahasia melalui proses kompresi. Tantangannya sendiri yaitu, kompresi dapat menyebabkan distorsi pada bit yang telah diubah oleh metode LSB, berpotensi merusak atau bahkan menghilangkan pesan yang disembunyikan.

c. *Downloading* (Pengunduhan Gambar)

Setelah gambar diunggah dan terkompresi oleh platform media sosial, tahap berikutnya adalah mengunduh kembali gambar tersebut. Proses ini dilakukan untuk mendapatkan versi gambar yang telah dimodifikasi oleh platform. Pada tahap ini, gambar yang diunduh akan memiliki ukuran file yang berbeda dari gambar asli, dan mungkin sudah mengalami perubahan pada struktur bitnya. Tujuannya untuk mengambil versi gambar yang telah dikompresi untuk dianalisis lebih lanjut.

d. *Extracting* (Ekstraksi Pesan)

Pada tahap ini, dilakukan proses ekstraksi pesan rahasia dari gambar terkompresi yang telah diunduh. Peneliti akan menggunakan teknik yang sama dengan saat penyisipan, yaitu metode LSB, untuk mengambil kembali pesan yang disembunyikan. Dalam proses ini, juga digunakan kunci steganografi (*stego key*), yang merupakan informasi tambahan yang diperlukan untuk mengakses pesan tersembunyi. Kunci ini memastikan bahwa hanya pihak yang memiliki otorisasi yang dapat mengekstrak pesan rahasia.

e. *Analysis*

Tahap terakhir dari penelitian ini adalah analisis. Pada tahap ini, pesan asli yang disisipkan akan dibandingkan dengan pesan yang diekstraksi dari gambar terkompresi. Analisis ini bertujuan untuk mengevaluasi apakah pesan rahasia masih dapat terekstrak dan terbaca dengan jelas setelah gambar melalui proses kompresi oleh media sosial. Tahapan ini juga digunakan untuk menilai efektivitas dan ketahanan metode steganografi LSB terhadap perubahan yang disebabkan oleh kompresi gambar. Selain itu, analisis ini juga mencakup *perbandingan* ukuran dan resolusi gambar sebelum dan setelah proses unggah ke media sosial. Dengan mengukur ukuran file dan resolusi asli gambar, kemudian membandingkannya dengan ukuran dan resolusi gambar setelah kompresi, penelitian ini dapat menilai dampak kompresi terhadap kualitas gambar dan efektivitas metode steganografi.

3.2. Alat dan Bahan Penelitian

Dalam penelitian ini terdapat beberapa alat dan bahan yang diperlukan berupa *software* atau *tools* steganografi serta *hardware* untuk menjalankan eksperimen terkait steganografi menggunakan metode *Least Significant Bit (LSB)* serta pengujian ketahanannya terhadap kompresi gambar oleh platform media sosial. Terdapat juga program *python* dengan platform *Jupyter Notebook* untuk mengecek resolusi dan ukuran gambar sehingga nantinya dapat dibandingkan. Berikut adalah rincian alat dan bahan yang akan digunakan :

Tabel 1. Alat dan bahan penelitian

No	Kategori	Spesifikasi
1	Hardware	Laptop Dell Latitude E7250
2	Software	Windows 10 Pro Steghide version 0.5.1

Perencanaan perangkat keras dan perangkat lunak yang akan digunakan dalam penelitian sangat penting untuk memastikan bahwa proses berjalan lancar dan hasil penelitian dapat diperoleh dengan valid. Dalam penelitian ini, berbagai alat dan teknologi akan digunakan, yang masing-masing memiliki kegunaan spesifik dalam mendukung analisis. Spesifikasi perangkat lunak yang digunakan juga

berperan besar dalam menentukan kualitas hasil penelitian.

4. HASIL DAN PEMBAHASAN

4.1. Embedding Pesan

```
To embed emb.txt in cvr.jpg: steghide embed -cf cvr.jpg -ef emb.txt
To extract embedded data from stg.jpg: steghide extract -sf stg.jpg
(base) PS C:\steghide> .\steghide embed -cf 1.jpg -ef test.txt -p sandi123
embedding "test.txt" in "1.jpg"... done
(base) PS C:\steghide> .\steghide embed -cf 2.jpg -ef test.txt -p sandi123
embedding "test.txt" in "2.jpg"... done
(base) PS C:\steghide> .\steghide embed -cf 3.jpg -ef test.txt -p sandi123
embedding "test.txt" in "3.jpg"... done
(base) PS C:\steghide> .\steghide embed -cf 4.jpg -ef test.txt -p sandi123
embedding "test.txt" in "4.jpg"... done
(base) PS C:\steghide> .\steghide embed -cf 1.jpeg -ef test.txt -p sandi123
embedding "test.txt" in "1.jpeg"... done
(base) PS C:\steghide> .\steghide embed -cf 2.jpeg -ef test.txt -p sandi123
embedding "test.txt" in "2.jpeg"... done
(base) PS C:\steghide> .\steghide embed -cf 3.jpeg -ef test.txt -p sandi123
embedding "test.txt" in "3.jpeg"... done
(base) PS C:\steghide> .\steghide embed -cf 4.jpeg -ef test.txt -p sandi123
embedding "test.txt" in "4.jpeg"... done
```

Gambar 3. Embedding Pesan

Pada Gambar 3. Proses penyisipan pesan rahasia ke dalam gambar menggunakan metode *Least Significant Bit* (LSB) dengan tools Steghide berhasil dilakukan tanpa mengubah kualitas visual gambar secara signifikan. Pesan yang disisipkan, yaitu *"Sepertinya sudah waktunya untuk kita berkemas dan memulai perjalanan. Jangan lupa membawa peta tua di bawah meja."*, berhasil dimasukkan ke dalam gambar dengan format JPG dan JPEG. Setiap gambar yang diunggah tetap terlihat normal secara visual, dan pesan rahasia tersebut dapat diekstraksi kembali dengan sempurna sebelum diunggah ke platform media sosial.. Detail masing-masing gambar setelah disisipi pesan rahasia dan sebelum diunggah ke media sosial terdapat pada Tabel 2. sebagai berikut :

Tabel 2. Detail file

Format File	Ukuran (KB)	Resolusi w (pixel)	Resolusi h (pixel)
1.jpg	159.98	736	1021
2.jpg	163.17	736	1304

Tabel 3. Hasil data facebook messenger

Format Awal	Format Akhir	Ukuran (kb)	Resolusi (w x h) pixel	Status Pesan tersembunyi	Keterangan
1.jpg	1.jpg	159.98	736 x 1021	Terbaca	Pesan berhasil diekstraksi.
2.jpg	2.jpg	163.17	736 x 1304	Terbaca	Pesan berhasil diekstraksi.
3.jpg	3.jpg	460.38	736 x 1030	Terbaca	Pesan berhasil diekstraksi.
4.jpg	4.jpg	425.13	675 x 1200	Terbaca	Pesan berhasil diekstraksi.
1.jpeg	1.jpg	197.51	746 x 1472	Terbaca	Pesan berhasil diekstraksi.
2.jpeg	2.jpg	60.2	735 x 736	Terbaca	Pesan berhasil diekstraksi.
3.jpeg	3.jpg	89.37	571 x 800	Terbaca	Pesan berhasil diekstraksi.
4.jpeg	4.jpg	472.22	736 x 1596	Terbaca	Pesan berhasil diekstraksi.

Pada Tabel 3. Ditampilkan semua gambar yang dikirim ke Facebook Messenger tetap mempertahankan ukuran dan resolusi yang sama. Namun, perubahan terjadi pada format file jpeg menjadi jpg. Pesan yang disisipkan dalam gambar berhasil diekstraksi dengan baik dan dapat terbaca.

4.4. WhatsApp

Pada Gambar 5. Hasil proses ekstraksi menunjukkan bahwa semua file yang diunduh kembali

Format File	Ukuran (KB)	Resolusi w (pixel)	Resolusi h (pixel)
3.jpg	460.38	736	1030
4.jpg	425.13	675	1200
1.jpeg	197.51	736	1472
2.jpeg	60.2	735	736
3.jpeg	89.37	571	800
4.jpeg	472.22	736	1596

4.2. Downloading dan Extracting Pesan

Setelah gambar yang mengandung pesan tersembunyi dikirim melalui media sosial seperti Facebook Messenger, WhatsApp, Telegram, dan Gmail, gambar tersebut diunduh kembali untuk kemudian diekstraksi guna memeriksa kondisi pesan tersembunyi di dalamnya.

4.3. Facebook Messenger

```
(base) PS C:\steghide> .\steghide extract -sf \fb\1a.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \fb\2a.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \fb\3a.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \fb\4a.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \fb\1.jpg -p sandi123
the file "test.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \fb\2.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \fb\3.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \fb\4.jpg -p sandi123
wrote extracted data to "test.txt".
```

Gambar 4. Proses ekstraksi Facebook Messenger

Pada Gambar 4. Hasil proses ekstraksi menunjukkan bahwa semua file yang diunduh kembali dari platform Facebook Messenger berubah menjadi .jpg namun, tetap berhasil diekstraksi sepenuhnya menggunakan Steghide, dengan proses yang berjalan lancar tanpa adanya kendala, dan pesan tersembunyi yang berupa file test.txt berhasil diungkapkan dari setiap file gambar.

dari platform WhatsApp berubah menjadi .jpg dan terdapat beberapa file yang gagal diekstraksi.

```
(base) PS C:\steghide> .\steghide extract -sf \wa\1a.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \wa\2a.jpg -p sandi123
steghide: could not extract any data with that passphrase!
(base) PS C:\steghide> .\steghide extract -sf \wa\3a.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \wa\4a.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \wa\1.jpg -p sandi12
steghide: could not extract any data with that passphrase!
(base) PS C:\steghide> .\steghide extract -sf \wa\2.jpg -p sandi123
the file "test.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \wa\3.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \wa\4.jpg -p sandi123
steghide: could not extract any data with that passphrase!
```

Gambar 5. Proses ekstraksi whatsapp

Tabel 4. Hasil data whatsapp

Format Awal	Format Akhir	Ukuran (kb)	Resolusi (w x h) pixel	Status Pesan tersembunyi	Keterangan
1.jpg	1.jpg	159.98	736 x 1021	Terbaca	Pesan berhasil diekstraksi.
2.jpg	2.jpg	231.6	722 x 1280	Tidak Terbaca	Pesan hilang setelah proses kompresi.
3.jpg	3.jpg	460.38	736 x 1030	Terbaca	Pesan berhasil diekstraksi.
4.jpg	4.jpg	425.13	675 x 1200	Terbaca	Pesan berhasil diekstraksi.
1.jpeg	1.jpg	230.6	640 x 1280	Tidak Terbaca	Pesan hilang setelah proses kompresi
2.jpeg	2.jpg	60.2	735 x 736	Terbaca	Pesan berhasil diekstraksi.
3.jpeg	3.jpg	89.37	571 x 800	Terbaca	Pesan berhasil diekstraksi.
4.jpeg	4.jpg	241.18	590 x 1280	Tidak Terbaca	Pesan hilang setelah proses kompresi.

Dapat dilihat terdapat perubahan ukuran file dan resolusi pada beberapa gambar setelah diunggah menggunakan *whatsapp*. Selain itu, pesan tersembunyi juga tidak dapat terdeteksi pada gambar yang mengalami kompresi.

4.2.1. Telegram

Pada Gambar 6. Hasil proses ekstraksi menunjukkan bahwa semua file yang diunduh kembali dari platform Telegram berubah menjadi .jpg dan semua file gagal diekstraksi.

```
(base) PS C:\steghide> .\steghide extract -sf \tele1.jpg -p sandi123
steghide: could not extract any data with that passphrase!
(base) PS C:\steghide> .\steghide extract -sf \tele2.jpg -p sandi123
steghide: could not extract any data with that passphrase!
(base) PS C:\steghide> .\steghide extract -sf \tele3.jpg -p sandi123
steghide: could not extract any data with that passphrase!
(base) PS C:\steghide> .\steghide extract -sf \tele4.jpg -p sandi123
steghide: could not extract any data with that passphrase!
(base) PS C:\steghide> .\steghide extract -sf \tele1a.jpg -p sandi123
steghide: could not extract any data with that passphrase!
(base) PS C:\steghide> .\steghide extract -sf \tele2a.jpg -p sandi123
steghide: could not extract any data with that passphrase!
(base) PS C:\steghide> .\steghide extract -sf \tele3a.jpg -p sandi123
steghide: could not extract any data with that passphrase!
(base) PS C:\steghide> .\steghide extract -sf \tele4a.jpg -p sandi123
steghide: could not extract any data with that passphrase!
```

Gambar 6. Proses ekstraksi Telegram

Tabel 5. Hasil data telegram

Format Awal	Format Akhir	Ukuran (kb)	Resolusi (w x h) pixel	Status Pesan tersembunyi	Keterangan
1.jpg	1.jpg	174.49	736 x 1021	Tidak Terbaca	Pesan hilang setelah proses kompresi.
2.jpg	2.jpg	163.87	722 x 1280	Tidak Terbaca	Pesan hilang setelah proses kompresi.
3.jpg	3.jpg	188.47	736 x 1030	Tidak Terbaca	Pesan hilang setelah proses kompresi.
4.jpg	4.jpg	284.2	675 x 1200	Tidak Terbaca	Pesan hilang setelah proses kompresi.
1.jpeg	1.jpg	160.99	640 x 1280	Tidak Terbaca	Pesan hilang setelah proses kompresi.
2.jpeg	2.jpg	67.82	735 x 736	Tidak Terbaca	Pesan hilang setelah proses kompresi.
3.jpeg	3.jpg	49.92	571 x 800	Tidak Terbaca	Pesan hilang setelah proses kompresi.
4.jpeg	4.jpg	162.52	590 x 1280	Tidak Terbaca	Pesan hilang setelah proses kompresi.

Hasil menunjukkan bahwa kompresi *Telegram* mengubah ukuran dan resolusi gambar setelah pengiriman. Perubahan ini membuat pesan steganografi tidak dapat dibaca. Dengan kata lain, pesan yang disisipkan hilang karena perubahan pada gambar.

4.2.2. Gmail

Pada Gambar 7. Hasil proses ekstraksi menunjukkan bahwa semua file yang diunduh kembali dari platform Gmail berhasil diekstraksi sepenuhnya menggunakan Steghide, dengan menjaga format filenya.

```
(base) PS C:\steghide> .\steghide extract -sf \gmail1.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \gmail2.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \gmail3.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \gmail4.jpg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \gmail1.jpeg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \gmail2.jpeg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \gmail3.jpeg -p sandi123
wrote extracted data to "test.txt".
(base) PS C:\steghide> .\steghide extract -sf \gmail4.jpeg -p sandi123
wrote extracted data to "test.txt".
```

Gambar 7. Proses ekstrakti Gmail

Tabel 6. Hasil data gmail

Format Awal	Format Akhir	Ukuran (kb)	Resolusi (w x h) pixel	Status Pesan tersembunyi	Keterangan
1.jpg	1.jpg	159.98	736 x 1021	Terbaca	Pesan berhasil diekstraksi.
2.jpg	2.jpg	163.17	736 x 1304	Terbaca	Pesan berhasil diekstraksi.
3.jpg	3.jpg	460.38	736 x 1030	Terbaca	Pesan berhasil diekstraksi.
4.jpg	4.jpg	425.13	675 x 1200	Terbaca	Pesan berhasil diekstraksi.
1.jpeg	1.jpg	197.51	746 x 1472	Terbaca	Pesan berhasil diekstraksi.
2.jpeg	2.jpg	60.2	735 x 736	Terbaca	Pesan berhasil diekstraksi.
3.jpeg	3.jpg	89.37	571 x 800	Terbaca	Pesan berhasil diekstraksi.
4.jpeg	4.jpg	472.22	736 x 1596	Terbaca	Pesan berhasil diekstraksi.

Hasil pengiriman gambar melalui gmail, semua gambar yang dikirimkan tetap mempertahankan format, ukuran dan resolusi yang sama. Pesan yang disisipkan dalam gambar berhasil diekstraksi dengan baik dan dapat terbaca.

Hasil analisis yang dilakukan, semua gambar yang dikirim melalui *Facebook Messenger* tetap mempertahankan ukuran dan resolusi asli. Tidak ada perubahan signifikan pada file, kecuali konversi format file dari .jpeg menjadi .jpg. Pesan-pesan yang disisipkan berhasil diekstraksi dengan baik. Hal ini menunjukkan bahwa *Facebook Messenger* tidak melakukan kompresi yang berdampak pada struktur gambar, sehingga metode LSB tetap efektif untuk menyembunyikan pesan di platform ini. Dengan demikian, metode *Least Significant Bit* (LSB) tetap efektif untuk menyembunyikan pesan di platform ini. Hasil ini menunjukkan bahwa *Facebook Messenger* merupakan platform yang lebih ramah untuk teknik steganografi. Untuk pengiriman melalui *whatsapp* terjadi kompresi yang mempengaruhi beberapa gambar setelah diunggah. Beberapa gambar menunjukkan perubahan ukuran dan resolusi yang cukup signifikan, pada file 2.jpg, di mana ukuran file berubah dari 163,17 KB menjadi 231,6 KB atau mengalami kenaikan 41.94% dan resolusi turun menjadi 722 x 1280 pixel atau -1.90% x -1.84%, sehingga pesan tersembunyi tidak terbaca. File 1.jpeg

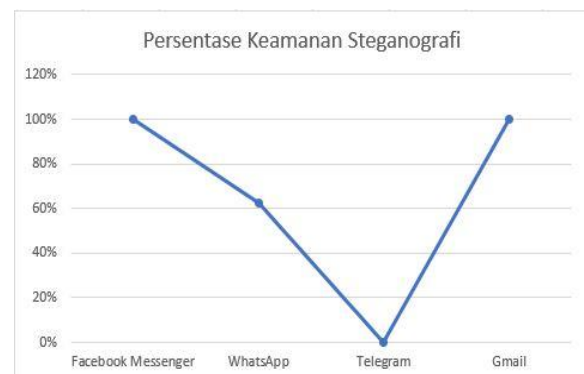
mengalami kompresi yang serupa, dengan perubahan ukuran sebesar +16.75% dan resolusi -13.04% x -13.04%. File 4.jpeg mengalami perubahan ukuran -48.93% serta resolusi -19.84% x -19.80% yang menyebabkan pesan tersembunyi tidak dapat diekstraksi. Namun, beberapa gambar, seperti 1.jpg, 3.jpg, dan 2.jpeg, berhasil mempertahankan pesan tersembunyi, yang menunjukkan bahwa kompresi *WhatsApp* tidak selalu mempengaruhi semua gambar secara sama. Ini menunjukkan bahwa kinerja steganografi menggunakan metode *Least Significant Bit* (LSB) pada platform *WhatsApp* sangat bergantung pada ukuran dan resolusi gambar asli. Gambar dengan ukuran besar atau resolusi yang lebih tinggi mungkin lebih rentan terhadap kompresi, yang menghilangkan informasi tersembunyi, sementara gambar dengan resolusi yang lebih rendah atau lebih kecil memiliki kemungkinan lebih besar untuk mempertahankan pesan.

Telegram menunjukkan dampak terbesar terhadap pesan tersembunyi pada gambar. Semua gambar mengalami kompresi yang mengakibatkan perubahan ukuran dan resolusi, serta menyebabkan pesan steganografi menjadi tidak terbaca. Berikut adalah rincian perubahan ukuran dan persentase perubahan untuk masing-masing file :

Tabel 7. Perbandingan hasil data telegram

Ukuran Awal	Ukuran Akhir	Persentase perubahan	Resolusi Awal	Resolusi Akhir	Persentase
159.98	174.49	9.07%	736 x 1021	736 x 1021	0% x 0%
163.17	163.87	0.43%	736 x 1304	722 x 1280	-1.90% x -1.84%
460.38	188.47	-59.06%	736 x 1030	736 x 1030	0% x 0%
425.13	284.2	-33.15%	675 x 1200	675 x 1200	0% x 0%
197.51	160.99	-18.49%	746 x 1472	640 x 1280	-14.21% x -13.04%
60.2	67.82	12.66%	735 x 736	735 x 736	0% x 0%
89.37	49.92	-44.14%	571 x 800	571 x 800	0% x 0%
472.22	162.52	-65.58%	736 x 1596	590 x 1280	-19.84% x -19.80%

Dari hasil ini, *Telegram* menerapkan kompresi gambar yang cukup agresif, sehingga metode *Least Significant Bit* (LSB) tidak efektif untuk menyembunyikan pesan pada platform ini. Kompresi ini menghapus informasi yang diperlukan untuk mengekstrak pesan steganografi, menjadikan *Telegram* tidak ideal bagi metode ini jika gambar yang diunggah mengalami perubahan signifikan. Gmail menunjukkan hasil yang mirip dengan *Facebook Messenger*. Semua gambar yang dikirim melalui Gmail tetap mempertahankan ukuran, resolusi, dan format aslinya. Tidak ada kompresi atau perubahan signifikan pada file. Semua pesan steganografi yang disisipkan berhasil diekstraksi dengan baik. Hal ini menunjukkan bahwa Gmail efektif dalam mempertahankan integritas gambar dan informasi yang disisipkan, sehingga metode *Least Significant Bit* (LSB) tetap dapat digunakan untuk menyembunyikan pesan tanpa risiko kehilangan data.



Gambar 3. Diagram Kesimpulan

Dari data yang dihasilkan, dapat dilihat bahwa setiap platform memberikan hasil yang berbeda. *Facebook Messenger* dan *Gmail*, dengan total 8 gambar yang diuji, berhasil mengekstraksi pesan tersembunyi pada semua gambar, dengan tingkat keberhasilan 100%. *WhatsApp* menunjukkan hasil

yang lebih bervariasi, di mana dari 8 gambar yang diuji, hanya 5 gambar (62.5%) yang berhasil mempertahankan pesan tersembunyi, sementara 3 gambar (37.5%) mengalami kehilangan pesan karena kompresi. *Telegram* menunjukkan hasil terburuk, di mana semua 8 gambar yang diuji tidak berhasil mempertahankan pesan tersembunyi, dengan tingkat kegagalan 100%. Berdasarkan uraian di atas, dapat disimpulkan bahwa efektivitas metode steganografi LSB sangat dipengaruhi oleh platform media sosial yang digunakan. Platform seperti *Facebook Messenger* lebih ramah terhadap penyisipan pesan tersembunyi karena tidak melakukan kompresi atau perubahan signifikan pada file yang dikirim, baik gambar maupun dokumen, sehingga pesan steganografi tetap dapat diekstraksi dengan baik. Sebaliknya, pada platform seperti *WhatsApp* dan *Telegram*, terjadi kompresi dan perubahan struktur pada file gambar yang menyebabkan pesan steganografi menjadi tidak terbaca. Meskipun file dokumen tidak terpengaruh, perubahan pada file gambar menunjukkan bahwa platform ini kurang ideal untuk pengiriman pesan tersembunyi menggunakan metode LSB. Oleh karena itu, pemilihan platform menjadi faktor penting dalam menjaga keamanan dan integritas pesan steganografi yang dikirim.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis, pengujian, dan evaluasi yang telah dilakukan, penelitian ini menunjukkan bahwa efektivitas metode steganografi menggunakan teknik *Least Significant Bit* (LSB) sangat dipengaruhi oleh platform yang digunakan untuk pengiriman gambar. Setiap platform memiliki kebijakan kompresi yang berbeda, yang secara langsung mempengaruhi kemampuan pesan tersembunyi untuk bertahan dari modifikasi gambar. Pada platform *Facebook Messenger* dan *Gmail*, tidak terjadi kompresi yang signifikan pada file gambar maupun dokumen yang dikirim. Hal ini memungkinkan pesan yang disisipkan menggunakan metode LSB untuk tetap utuh dan dapat diekstraksi dengan baik setelah pengiriman. Karena itu, *Facebook Messenger* terbukti sebagai platform yang aman dan dapat diandalkan untuk menyembunyikan pesan tersembunyi melalui steganografi LSB, menjaga integritas pesan tanpa menyebabkan distorsi bit yang dapat mengakibatkan pesan menjadi tidak terbaca. Pada platform seperti *WhatsApp* dan *Telegram*, terjadi kompresi gambar yang cukup agresif. Kompresi ini menyebabkan perubahan ukuran dan resolusi gambar yang signifikan, sehingga pesan steganografi yang disisipkan di dalam gambar menjadi rusak dan tidak dapat diekstraksi dengan benar. Hal ini menjadikan kedua platform ini tidak ideal untuk penggunaan steganografi LSB dalam gambar.

Dari temuan ini, disarankan untuk menggunakan platform yang tidak melakukan kompresi atau hanya melakukan kompresi minimal, seperti *Facebook Messenger* atau *Gmail*, untuk menjaga integritas pesan

tersembunyi menggunakan metode LSB. Sementara itu, platform seperti *Telegram* perlu dihindari jika tujuan utamanya adalah menjaga keamanan pesan steganografi dalam gambar.

DAFTAR PUSTAKA

- [1] I. Kurniawan, M. Rifqi Maulana, C. Yulianto Rusli, and S. Widya Pratama, "ANALISIS PESAN STEGANOGRAPH PADA SETELAH PENGIRIMAN FILE PADA PLATFORM SOCIAL MEDIA," vol. XVIII, no. 2, 2023, [Online]. Available: <http://ejournal.stmik-wp.ac.id>
- [2] R. F. Sidiq, R. Erwin, G. Rahayu, and A. D. Supriatna, "Implementasi Kriptografi Advanced Encryption Standard dan Least Significant Bit untuk Keamanan Pesan Email dalam Gambar." [Online]. Available: <https://jurnal.itg.ac.id/>
- [3] M. Ricky, F. Agus Setyaningsih, M. Dipenogoro, J. Rekayasa Sistem Komputer, and F. H. MIPA Universitas Tanjungpura Jalan Hadari Nawawi, "Jurnal Coding, Rekayasa Sistem Komputer ANALISIS KOMPRESI STEGANOGRAPHY PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE LEAST SIGNIFICANT BIT BERBASIS MOBILE ANDROID [1]."
- [4] A. Rohmanu, "IMPLEMENTASI KRIPTOGRAFI DAN STEGANOGRAFI DENGAN METODE ALGORITMA DES DAN METODE END OF FILE," *Jurnal Informatika SIMANTIK*, vol. 2, no. 1, 2017, [Online]. Available: www.jurnal.stmikcikarang.ac.id
- [5] R. Purnomo, E. D. Astuti, M. Kom, and M. Hidayat, "RANCANG BANGUN APLIKASI STEGANOGRAFI UNTUK MENGAMANKAN PESAN MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) BERBASIS ANDROID."
- [6] M. Sholihah, *Merawat ingatan, merepresentasikan tindakan: catatan arsip 43 tahun LPM Arena*. Arena Press, 2018.
- [7] S. Fajriati Romli, A. Id Hadiana, and F. Rakhmat Umbara, "Penerapan Kriptografi Advanced Encryption Standard (AES) dan Steganografi Spread Spectrum Untuk Mengamankan Pesan Dalam Gambar," *DES 2023 Journal of Informatics and Communications Technology*, vol. 5, no. 2, pp. 196–209, doi: 10.52661.
- [8] T. Handayani, T. Yuliaty, and S. Patimah, "Implementasi Steganografi Dengan Metode End Of File (EOF) Untuk Menyisipkan Pesan Teks Pada Gambar".
- [9] Aqilah Syaima' Fadel, Rianto David Saputra, Y. Fatma, and Risky Nanda Putra, "Analisis keamanan steganografi teks dengan metode lsb (least significant bit) pada citra digital," *Jurnal CoSciTech (Computer Science and Information*

- Technology), vol. 5, no. 1, pp. 36–41, Apr. 2024, doi: 10.37859/coscitech.v5i1.6759.
- [10] R. K. Dewi and R. Munir, “JIP (Jurnal Informatika Polinema) PERBANDINGAN BERBAGAI METODE STEGANOGRAFI PADA CITRA DIGITAL”.
- [11] J. Rizky Maulidina and N. Bin Idris, “IMPLEMENTASI STEGANOGRAFI DAN STEGANALISIS MENGGUNAKAN METODE LSB (LEAST SIGNIFICANT BIT) PADA FILE GAMBAR.” [Online]. Available: <https://journal.universitasmulia.ac.id/index.php/orbis>
- [12] C. Ulandari, “Penyisipan Pesan Pada File Dokumen Berektensi Xls/Xlsx Menggunakan Metode Chinese Remainder,” *Media Online*, vol. 2, no. 5, pp. 156–162, 2022, [Online]. Available: <https://djournals.com/klik>
- [13] M. Rizky, D. Putra, R. Adistya, and N. Pamudji, “IKRAM: Jurnal Ilmu Komputer Al Muslim Analisis Dan Perancangan Aplikasi Steganografi Pada Media Image Dengan Metode LSB (Least Significant Bit),” vol. 1, 2024.
- [14] M. J. Prabowo and R. Wanto, “Implementasi Steganografi Berbasis Mobile Menyembunyikan Pesan Gambar Dan Suara,” *JURNAL MERDEKA INFORMATIKA*, vol. 1, Jan. 2023.
- [15] S. Lutfi and R. Rosihan, “PERBANDINGAN METODE STEGANOGRAFI LSB (LEAST SIGNIFICANT BIT) DAN MSB (MOST SIGNIFICANT BIT) UNTUK MENYEMBUNYIKAN INFORMASI RAHASIA KEDALAM CITRA DIGITAL,” *JIKO (Jurnal Informatika dan Komputer)*, vol. 1, no. 1, pp. 34–42, Apr. 2018, doi: 10.33387/jiko.v1i1.1169.
- [16] D. Darwis, “IMPLEMENTASI STEGANOGRAFI PADA BERKAS AUDIO WAV UNTUK PENYISIPAN PESAN GAMBAR MENGGUNAKAN METODE LOW BIT CODING,” *Expert-Jurnal Manajemen Sistem Informasi Dan Teknologi*.
- [17] J. Multidisiplin Saintek and R. Wanandi, “IMPLEMENTASI SISTEM STEGANOGRAFI CITRA DENGAN METODE SUBSTITUSI LSB (LEAST SIGNIFICANT BIT),” vol. 2, no. 11, pp. 10–20, 2024, [Online]. Available: <https://ejournal.warunayama.org/kohehi>
- [18] R. R. Santosa, A. R. Pamungkas, M. Khrisna, and F. Zuhri, “Securing Email through Steganography Implementation of One Time Pad and LSB Method on Attached Images,” vol. 3, no. 1, p. 123, 2024.
- [19] L. P. Malese, “Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB),” *Jurnal Ilmiah Wahana Pendidikan*, vol. 7, Sep. 2021.
- [20] I. F. Ashari, L. R. Siwi, H. Londa, and I. Wicaksono, “ANALISIS DAN PERBANDINGAN STEGANOGRAFI PADA MEDIA AUDIO DAN GAMBAR MENGGUNAKAN LSB DAN RC4,” *Jurnal ELTIKOM*, vol. 7, no. 1, pp. 67–78, Jun. 2023, doi: 10.31961/eltikom.v7i1.583.
- [21] I. Margareta *et al.*, “Sosialisasi Keamanan Data Menggunakan Teknologi Informasi pada Kantor Camat Batang Serangan,” *IPMAS*, vol. 4, no. 2, p. 2024, 2024, doi: 10.30605/ipmas.4.2.2024.475.
- [22] W. H. M *et al.*, “Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa,” *VOKATEK*, vol. 01, Jan. 2023, [Online]. Available: <https://journal.diginus.id/index.php/VOKATEK/index>