

ANALISIS PESAN STEGANOGRAPH PADA SETELAH PENGIRIMAN FILE PADA PLATFORM SOCIAL MEDIA

Ichwan Kurniawan¹⁾, Much. Rifqi Maulana²⁾, Christian Yulianto Rusli³⁾
STMIK Widya Pratama¹²³⁾
ichwan.ana10@gmail.com¹⁾, rifqi@stmik-wp.ac.id²⁾, cyr.tata@gmail.com³⁾

Abstrak

Penggunaan media sosial sebagai media transmisi informasi birokrasi pada masa sekarang ini menjadi alternatif birokrasi. Informasi birokrasi pada media sosial dapat berupa, dokumen berbasis text maupun gambar, hal ini dirasakan mudah dan efisien tanpa harus menggunakan sistem komputer yang terstruktur. Namun, ada beberapa hal yang harus dipertimbangkan dalam penggunaan media sosial sebagai media pertukaran informasi birokrasi, salah satunya yaitu terjadinya proses perubahan dokumen pada Social Network Platforms(SNP). Selain itu steganografi atau penyembuyian data digunakan untuk melindungi privasi informasi dalam transaksi melalui Online Social Network (OSN). Penggunaan steganografi dapat digunakan sebagai metode atau teknik untuk memastikan bahwa informasi yang dikirim atau diterima melalui sosial media adalah asli. Hasil dari Analisis data file gambar dan dokumen dengan melihat detail file setelah pengiriman pada platform social media messenger facebook, whatsapp dan telegram adalah bahwa detail hasil yang dihasilkan setelah pengiriman pada platform whatsapp, terjadi perubahan utama pada Kb Bit Depth dan dpi Resolution. Setelah pengiriman Bit Depth berubah menjadi 24 Bit dan dpi Resolution menjadi 96 dpi, sedangkan pada platform telegram Bit Depth berubah menjadi 24 Bit dan dpi Resolution menjadi 120 dpi, dan pada platform messenger facebook baik file gambar dan dokumen tidak mengalami perubahan dan pesan masih tetap dan tidak berubah. kesimpulan dari penelitian ini adalah bahwa untuk mempertahankan otentifikasi atau keaslian file yang akan dikirim melalui platform social media disarankan menggunakan file dengan tipe dokumen, sedangkan penggunaan file gambar tidak disarankan untuk digunakan, hal ini dikarenakan platform social media akan merubah struktur file gambar sesuai dengan format standar mereka.

Kata Kunci : *Steganografi, Keamanan, Image, Sosial Media*

1. Pendahuluan

Penggunaan media sosial sebagai media transmisi informasi birokrasi pada masa sekarang ini menjadi alternatif birokrasi, baik pada lingkungan instansi swasta maupun instansi pemerintah. Informasi birokrasi pada media sosial dapat berupa, dokumen berbasis text maupun gambar, hal ini dirasakan mudah dan efisien tanpa harus menggunakan sistem komputer yang terstruktur. Namun, ada beberapa hal yang harus dipertimbangkan dalam penggunaan media sosial sebagai media pertukaran informasi birokrasi, salah satunya yaitu terjadinya proses perubahan dokumen pada *Social Network Platforms(SNP)* (Feng, et al. 2022). Melalui media sosial dimungkinkan file yang dikirim mengalami perubahan struktur file, hal ini akibat dari proses kompresi file pada media sosial, secara otomatis file akan terkompresi atau mengalami degradasi struktur file. Proses ini

mengakibatkan file mengalami perubahan struktur dan kualitas, hal ini bertujuan untuk mempercepat proses pengiriman file dari pengirim ke penerima pesan.

Dilihat dari sisi penerima proses kompresi mengakibatkan file yang dikirim menjadi file yang kurang otentik dan integritas file mengalami perubahan yang tidak diinginkan (B, Thejus dan Namboothiri 2022). Hal ini menjadi celah bagi penyerang untuk melakukan generate ulang pada file, dan dimungkinkan pada file telah disusupi oleh *malware* yang berbahaya. Sebagai usaha untuk menghindari tersebut, dimungkinkan untuk dilakukan otentikasi file yang diterima apakah telah berubah atau masih dalam keadaan asli.

Steganografi dan kriptografi dapat digunakan sebagai teknik keamanan dalam menjaga kerahasiaan, integritas dan ketersediaan data (Deepak dan Enireddy 2021). Selain itu steganografi atau penyembuyian data digunakan

untuk melindungi privasi informasi dalam transaksi melalui *Online Social Network (OSN)* (Gurunath, et al. 2021). Penggunaan steganografi dapat digunakan sebagai metode atau teknik untuk memastikan bahwa informasi yang dikirim atau diterima melalui sosial media adalah asli. Melalui *digital forensic steganalizer*, sebuah informasi dapat diketahui apakah informasi tersebut utuh atau sudah terdapat perubahan.

Uraian diatas menunjukkan bahwa file yang dikirim melalui sosial media mengalami perubahan, baik struktur, kualitas maupun kapasitas. Hal ini mengakibatkan file tersebut menjadi file yang kurang otentik dan integritas file mengalami perubahan yang tidak diinginkan. Menggunakan Steganografi file yang telah diterima dapat diidentifikasi, apakah file yang diterima asli atau tidak. Dalam penelitian ini akan dilakukan Analisis penggunaan steganografi pada perubahan struktur file sebagai perlindungan informasi pada lingkungan media sosial.

Berdasarkan latar belakang maka dapat diambil rumusan masalahnya adalah “Apakah Penggunaan Steganografi dapat Digunakan sebagai Metode Perlindungan Informasi pada Lingkungan Sosial Media?”. Sedangkan tujuan dari penelitian ini adalah Analisis Penggunaan Steganografi dapat Digunakan sebagai Metode Perlindungan Informasi pada Lingkungan Sosial Media. Kemudian manfaat dari penelitian ini adalah memberikan gambaran kepada pengguna media sosial mengenai jenis file yang tidak mengalami perubahan struktur file dalam pengiriman pesan pada platform media sosial.

2. Metode Penelitian

Jenis penelitian ini adalah penelitian experimental dengan metode penelitian sebagai berikut:

- Penentuan masalah penelitian adalah dengan menggunakan studi literatur dan studi lapangan.
- Penentuan *Computing Approach* penelitian ini dipilih studi lapangan mengenai pengiriman informasi birokrasi yang berada pada lingkungan Kampus STMIK Widya Pratama Pekalongan. Pada penelitian ini *steganography* dipilih dengan pemikiran bahwa, *steganography* dapat digunakan

sebagai teknik perlindungan informasi birokrasi.

- Analisis penggunaan *Steganography* pada Perubahan Struktur *File* sebagai pengamanan Informasi
- Evaluasi dengan melakukan komparasi dengan data empiris.
- Pengujian dengan melakukan pengolahan data *stego* setelah data dikirim dan sebelum data dikirim pada media sosial.

3. Hasil dan Pembahasan

3.1 Pengumpulan Data

Data yang digunakan dalam penelitian ini adalah berhubungan dengan masalah yang diteliti, data tersebut adalah data yang berhubungan dengan informasi birokrasi di Kampus STMIK Widya Pratama, baik berupa surat menyurat maupun pengumuman yang dikirim melalui platform sosial media dalam bentuk gambar maupun dokumen. Data ini nantinya akan dilakukan eksperimen perubahan struktur file setelah pengiriman pada platform sosial media, kemudian diuji dengan menggunakan beberapa aplikasi steganografi.

platform sosial media yang digunakan sebagai pengujian adalah *whatsapp*, *facebook messenger* dan *telegram*. Sedangkan Aplikasi yang digunakan <https://hexed.it/> untuk menguji pada file *.pdf dan <https://stylesuxx.github.io/steganography/> untuk menguji pada file gambar.

3.2 Penentuan *Computing Approach*

Computing approach pada penelitian ini adalah Analisis penggunaan *Steganography* terhadap struktur file pada platform sosial media. *Steganography* dipilih dengan alasan bahwa steganografi dapat digunakan untuk menyembunyikan atau menyusupkan informasi dalam sebuah file, hal ini dapat digunakan untuk mengidentifikasi struktur file berubah atau tidak setelah pengiriman file pada platform sosial media. Hal ini memungkinkan pada lingkungan *Online Social Network (OSN)* file dapat disusupi oleh perintah yang berbahaya.

3.3 Implementasi

Implementasi pesan steganografi dengan membandingkan tiga file yang berbeda dalam

platform *whatsapp*, *messenger facebook* dan *telegram*.

1. Whatsapp

Tabel 1. Hasil Detail File pada Whatsapp

Periode	Sebelum	Sesudah	Sebelum	Sesudah
Bahan	JPEG	JPEG	PDF	PDF
Ukuran (Kb)	1137	294	234	234
Bit Depth (Bit)	32	24	8	8
V resolution (dpi)	96	96	200	200
H resolution (dpi)	96	96	200	200
resolution W (pixel)	1240	1131	1654	1654
resolution H (pixel)	1753	1600	2338	2338
Steganografi	stego_s tmik_w p_2023	Tidak terbaca	hex_st mik_w p_2023	hex_st mik_w p_2023

Dapat dilihat dari hasil detail file, dalam pengiriman file menggunakan whatsapp, bahwa terdapat perubahan file pada pengiriman gambar setelah pengiriman, selain itu steganografi file tidak terbaca. Sedangkan pada pengiriman dokumen tidak mengalami perubahan file dan steganografi masih dapat terbaca.

2. Facebook Messenger

Tabel 2. Hasil Detail File pada Facebook Messenger

Periode	Sebelum	Sesudah	Sebelum	Sesudah
Bahan	JPEG	PNG	PDF	PDF
Ukuran (Kb)	1137	1137	234 Kb	234 Kb
Bit Depth (Bit)	32	32	8	8 Bit
V resolution (dpi)	96		200	200
H resolution (dpi)	96		200	200
resolution W (pixel)	1240	1240	1654	1654
resolution H (pixel)	1753	1753	2338	2338
Steganografi	stego_s tmik_w p_2023	stego_s tmik_w p_2023	hex_st mik_w p_2023	hex_st mik_w p_2023

Jika dilihat pengiriman file dengan menggunakan Facebook Messenger tidak mengalami perubahan pada file dalam bentuk gambar maupun dalam bentuk dokumen, selain itu steganografi pada bentuk gambar dan dokumen dapat terbaca.

3. Telegram

Tabel 3. Hasil Detail File pada Telegram

Periode	Sebelum	Sesudah	Sebelum	Sesudah
Bahan	JPEG	JPEG	PDF	PDF
Ukuran (Kb)	1137	100	234	234
Bit Depth (Bit)	32	24	8	8
V resolution (dpi)	96	120	200	200
H resolution (dpi)	96	120	200	200
resolution W (pixel)	1240	905	1654	1654
resolution H (pixel)	1753	1280	2338	2338
Steganografi	stego_s tmik_w p_2023		hex_st mik_w p_2023	hex_st mik_w p_2023

Dapat dilihat dari hasil detail file, dalam pengiriman file menggunakan telegram, bahwa terdapat perubahan file pada pengiriman gambar setelah pengiriman, selain itu steganografi file tidak terbaca. Sedangkan pada pengiriman dokumen tidak mengalami perubahan file dan steganografi masih dapat terbaca.

3.4 Pembahasan

Tahap pengujian ini akan dilakukan beberapa tahap, pertama menguji pengenalan wajah pada perputaran wajah depresi dan elevasi. Jika dilihat dari derajat perputaran wajah terdapat derajat perputaran wajah yang tidak terdeteksi/lost.

Hasil analisis steganografi yang dilakukan pada tahap berikutnya, bahwa detail file mengalami perubahan pada platform sosial media whatsapp dan telegram pada pengiriman file dalam bentuk gambar. Sedangkan pengiriman file pada platform facebook messenger tidak mengalami perubahan, hal ini dimungkinkan dalam pengiriman file melalui facebook messenger tidak mengalami kompresi gambar. Selain itu pengiriman file dalam bentuk dokumen *.pdf, dalam platform sosial media yang digunakan file tidak mengalami perubahan. Hal ini dimungkinkan pada tiga platform tersebut tidak mengkompresi file *.pdf yang dikirim.

Uraian di atas, bahwa perbandingan yang akan dilakukan hanya pada platform social media whatsapp dan telegram dalam pengiriman file dalam bentuk gambar. seperti yang telah disampaikan sebelumnya, bahwa perbandingan detail file adalah ukuran dalam satuan Kilo Byte, Bit Depth dalam satuan Bit, Resolution dalam satuan Dot per Inch (dpi), Height Dimension dan Width Dimension dalam satuan pixel dan Steganography.

1. Whatsapp

Tabel 4. Hasil Perbandingan Detail File 1 pada Whatsapp

Periode	Sebelum	Sesudah	Selisih	
			Point	Prosentase
Bahan	JPEG	JPEG	Point	Prosentase
Ukuran (Kb)	1137	294	843	74%
Bit Depth (Bit)	32	24	8	25%
V resolution (dpi)	96	96	0	0%
H resolution (dpi)	96	96	0	0%
resolution W (pixel)	1240	1131	109	9%
resolution H (pixel)	1753	1600	153	9%
Steganografi	stego_stmik_wp_2023	Tidak terbaca		

Tabel 5. Hasil Perbandingan Detail File 2 pada Whatsapp

Periode	Sebelum	Sesudah	Selisih	
			Point	Prosentase
Bahan	JPEG	JPEG	Point	Prosentase
Ukuran (Kb)	116	168	-52	-45%
Bit Depth (Bit)	24	24	0	0%
V resolution (dpi)	120	96	24	20%
H resolution (dpi)	120	96	24	20%
resolution W (pixel)	992	992	0	0%
resolution H (pixel)	1559	1559	0	0%
Steganografi	stego_stmik_wp_2023	Tidak terbaca		

Tabel 6. Hasil Perbandingan Detail File 3 pada Whatsapp

Periode	Sebelum	Sesudah	Selisih	
			Point	Prosentase
Bahan	JPEG	JPEG	Point	Prosentase
Ukuran (Kb)	136	214	-78	-57%
Bit Depth (Bit)	24	24	0	0%
V resolution (dpi)	120	96	24	20%
H resolution (dpi)	120	96	24	20%
resolution W (pixel)	1025	1025	0	0%
resolution H (pixel)	1573	1573	0	0%
Steganografi	stego_stmik_wp_2023	Tidak terbaca		

Seperti yang telah disampaikan pada tahap analisis, bahwa pengiriman file gambar pada platform whatsapp mengalami perubahan struktur file, baik ukuran file, bit depth, resolusi dan pesan steganografi yang tidak terbaca. jika dilihat pada perbandingan pertama dan kedua mengalami perbedaan :

- Kapasitas file pada file pertama mengalami penurunan sebesar 74% yaitu penurunan dari kapasitas 1137Kb menjadi 294Kb. Sedangkan pada file kedua mengalami kenaikan kapasitas file sebesar -45% yaitu kenaikan dari kapasitas 116Kb menjadi 168Kb. dan pada file kedua mengalami kenaikan kapasitas file sebesar -45% yaitu kenaikan dari kapasitas 136Kb menjadi 214Kb
- Bit Depth pada file pertama mengalami penurunan sebesar 25% yaitu penurunan dari 32bit menjadi 24, sedangkan pada file yang kedua dan ketiga tidak terdapat perbedaan.
- Resolusi dpi file baik vertikal maupun horizontal pada file pertama tidak mengalami penurunan, sedangkan pada file kedua dan ketiga mengalami penurunan sebesar 20% yaitu dari 120dpi menjadi 96dpi.
- Resolusi pixel baik width maupun height pada file pertama mengalami penurunan sebesar 9% yaitu resolusi width dari 1240 pixel menjadi 1131 pixel dan resolusi height dari 1753 pixel menjadi 1600 pixel. Sedangkan pada file kedua dan ketiga resolusi pixel width dan height tidak mengalami perubahan.
- Pesan steganografi file pada file pertama dan kedua tidak terbaca.

2. Telegram

Tabel 7. Hasil Perbandingan Detail File 1 pada Telegram

Periode	Sebelum	Sesudah	Selisih	
Bahan	JPEG	JPEG	Point	Prosentase
Ukuran (Kb)	1137	100	1037	91%
Bit Depth (Bit)	32	24	8	25%
V resolution (dpi)	96	120	24	20%
H resolution (dpi)	96	120	24	20%
resolution W (pixel)	1240	905	335	27%
resolution H (pixel)	1753	1280	473	27%
Steganografi	stego_stmik_wp_2023	Tidak terbaca		

Tabel 8. Hasil Perbandingan Detail File 2 pada Telegram

Periode	Sebelum	Sesudah	Selisih	
Bahan	JPEG	JPEG	Point	Prosentase
Ukuran (Kb)	116	103	13	11%
Bit Depth (Bit)	24	24	0	0%
V resolution (dpi)	120	120	0	0%
H resolution (dpi)	120	120	0	0%
resolution W (pixel)	992	814	178	18%
resolution H (pixel)	1559	1280	279	18%
Steganografi	stego_stmik_wp_2023			

Tabel 9. Hasil Perbandingan Detail File 3 pada Telegram

Periode	Sebelum	Sesudah	Selisih	
Bahan	JPEG	JPEG	Point	Prosentase
Ukuran (Kb)	136	146	-10	-7%
Bit Depth (Bit)	24	24	0	0%
V resolution (dpi)	120	120	0	0%
H resolution (dpi)	120	120	0	0%
resolution W (pixel)	1025	834	191	19%
resolution H (pixel)	1573	1280	293	19%
Steganografi	stego_stmik_wp_2023			

Seperti yang telah disampaikan pada tahap analisis, bahwa pengiriman file gambar pada platform telegram mengalami perubahan struktur file, baik ukuran file, bit depth, resolusi dan pesan steganografi yang tidak terbaca. jika dilihat pada

perbandingan pertama dan kedua mengalami perbedaan :

- Kapasitas file pada file pertama mengalami penurunan sebesar 91% yaitu penuruan dari kapasitas 1137Kb menjadi 100Kb. Sedangkan pada file kedua mengalami penurunan kapasitas file sebesar 11% yaitu kenaikan dari kapasitas 116Kb menjadi 103Kb, dan sedangkan pada file kedua mengalami penurunan kapasitas file sebesar -7% yaitu kenaikan dari kapasitas 136Kb menjadi 146Kb
- Bit Depth pada file pertama mengalami penurunan sebesar 25% yaitu penurunan dari 32bit menjadi, sedangkan pada file yang kedua dan ketiga tidak terdapat perbedaan.
- Resolusi dpi file baik vertikal maupun horizontal pada file kedua dan ketiga tidak mengalami penurunan, sedangkan pada file kedua mengalami kenaikan sebesar 20% yaitu dari 96dpi menjadi 120dpi.
- Resolusi pixel baik width maupun height pada file pertama mengalami penurunan sebesar 27% yaitu resolusi width dari 1240 pixel menjadi 905 pixel dan resolusi height dari 1753 pixel menjadi 1280 pexel. Sedangkan pada file kedua resolusi mengalami penurunan sebesar 18% yaitu resolusi width dari 992 pixel menjadi 814 pixel dan resolusi height dari 1559 pixel menjadi 1280 pexel, dan sedangkan pada file ketiga resolusi mengalami penurunan sebesar 19% yaitu resolusi width dari 1024 pixel menjadi 834 pixel dan resolusi height dari 1573 pixel menjadi 1280 pexel
- Pesan steganograsi file pada file petama dan kedua tidak tebaca.

3.5 Evaluasi

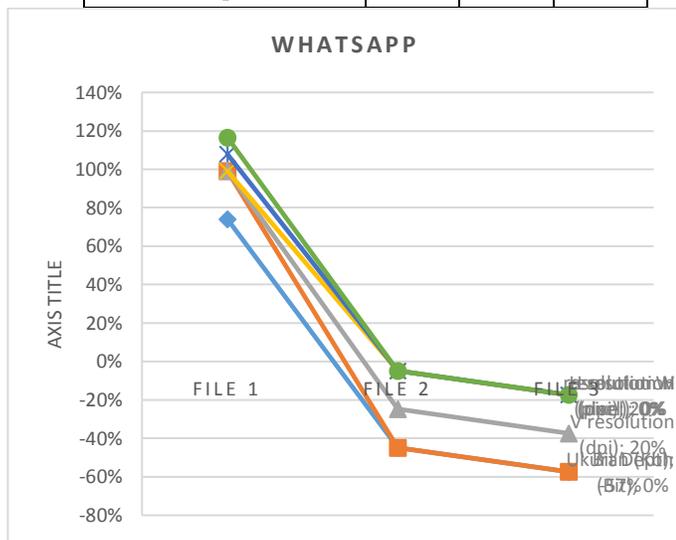
Tahap pengujian ini akan dilakukan beberapa tahap, dengan menguji tiga file yang berbeda dengan pengiriman pada social media whatsapp dan telegram. Tahap sebelumnya pada tahap analisis, menghasilkan perbedaan detail file uji yang dihasilkan setelah pengiriman pada platform social media whatsapp dan telegram. Detail hasil yang dihasilkan setelah pengiriman pada platfoem whatsapp, terjadi perubahan utama pada Kb Bit Depth dan dpi Resolution. Setelah pengiriman Bit Depth berubah menjadi 24 Bit dan

dpi Resolution menjadi 96 dpi, sedangkan pada platform telegram Bit Depth berubah menjadi 24 Bit dan dpi Resolution menjadi 120 dpi.

Hal ini mengakibatkan detail yang lain juga mengalami perubahan atau tetap sesuai dengan dua (bit depth dan dpi resolution) detail tersebut, termasuk diantaranya adalah perubahan kapasitas file, resolusi pixel dan sebagainya. Hal ini dimungkinkan pada saat pengiriman struktur file diubah untuk menyesuaikan standar yang ditentukan oleh platform social media yang digunakan.

Tabel 10. Kesimpulan Perbandingan Detail File 3 pada Whatsapp

Detail	File 1	File 2	File 3
Ukuran (Kb)	74%	-45%	-57%
Bit Depth (Bit)	25%	0%	0%
V resolution (dpi)	0%	20%	20%
H resolution (dpi)	0%	20%	20%
resolution W (pixel)	9%	0%	0%
resolution H (pixel)	9%	0%	0%

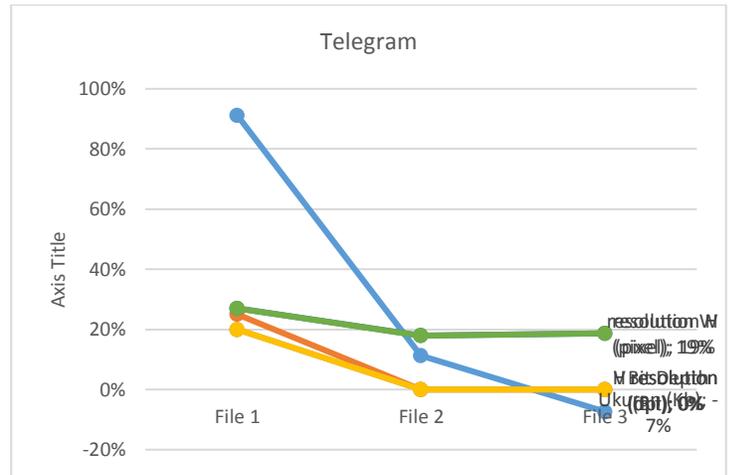


Gambar 1 Diagram Kesimpulan Perbandingan Detail File 3 pada Whatsapp

Tabel 011 Kesimpulan Perbandingan Detail File 3 pada Telegram

Detail	File 1	File 2	File 3
Ukuran (Kb)	91%	11%	-7%

Bit Depth (Bit)	25%	0%	0%
V resolution (dpi)	20%	0%	0%
H resolution (dpi)	20%	0%	0%
resolution W (pixel)	27%	18%	19%
resolution H (pixel)	27%	18%	19%



Gambar 2 Diagram Kesimpulan Perbandingan Detail File 3 pada Telegram

Nilai prosentase negatif menunjukkan bahwa perubahan yang terjadi mengalami kenaikan nilai detail, sedangkan nilai prosentase positif menunjukkan bahwa perubahan yang terjadi mengalami penurunan nilai detail. Seperti yang telah disampaikan sebelumnya bahwa platform social media akan melakukan perubahan struktur file setelah pengiriman, hal ini dimungkinkan bertujuan untuk menyesuaikan standar yang ditentukan oleh platform social media yang digunakan.

Berdasarkan tahap yang telah dilakukan, baik dari analisis, pengujian dan evaluasi dapat dilihat bahwa pengiriman file pada platform social media mempunyai standar berbeda-beda. Pada platform messenger facebook tidak melakukan perubahan pada struktur file setelah pengiriman baik file gambar maupun file dokumen dan pesan steganografi masih dapat terbaca. Sedangkan pada platform whatsapp dan telegram perubahan struktur file terjadi pada pengiriman file gambar dan pesan steganografi tidak terbaca, file dokumen tidak mengalami perubahan struktur file dan pesan steganografi masih tetap terbaca. Uraian di atas dapat disimpulkan bahwa untuk mempertahankan otentifikasi atau keaslian file

yang akan dikirim melalui platform social media disarankan menggunakan file dengan tipe dokumen, sedangkan penggunaan file gambar tidak disarankan untuk digunakan, hal ini dikarenakan platform social media akan merubah struktur file gambar sesuai dengan format standar mereka.

4. Kesimpulan dan Saran

Hasil dari Analisis data file gambar dan dokumen dengan melihat detail file setelah pengiriman pada platform *social media messenger facebook, whatsapp* dan *telegram* adalah bahwa detail hasil yang dihasilkan setelah pengiriman pada platform *whatsapp*, terjadi perubahan utama pada Kb Bit Depth dan dpi Resolution. Setelah pengiriman Bit Depth berubah menjadi 24 Bit dan dpi Resolution menjadi 96 dpi, sedangkan pada platform *telegram* Bit Depth berubah menjadi 24 Bit dan dpi Resolution menjadi 120 dpi, dan pada platform *messenger facebook* baik file gambar dan dokumen tidak mengalami perubahan dan pesan steganografi masih tetap dan tidak berubah.

Berdasarkan tahap yang telah dilakukan, baik dari analisis, pengujian dan evaluasi dapat dilihat bahwa pengiriman file pada platform *social media* mempunyai standar berbeda-beda. Pada platform *messenger facebook* tidak melakukan perubahan pada struktur file setelah pengiriman baik file gambar maupun file dokumen dan pesan steganografi masih dapat terbaca. Sedangkan pada platform *whatsapp* dan *telegram* perubahan struktur file terjadi pada pengiriman file gambar dan pesan steganografi tidak terbaca, file dokumen tidak mengalami perubahan struktur file dan pesan steganografi masih tetap terbaca. Uraian di atas dapat disimpulkan bahwa untuk mempertahankan otentifikasi atau keaslian file yang akan dikirim melalui platform social media disarankan menggunakan file dengan tipe dokumen, sedangkan penggunaan file gambar tidak disarankan untuk digunakan, hal ini dikarenakan platform social media akan merubah struktur file gambar sesuai dengan format standar mereka.

Kajian berikutnya untuk melakukan re-structur file pada file yang telah diubah oleh platform social media, dan jika pada analisis perubahan file pada platform social media

disarankan menggunakan variasi file yang lebih banyak dalam mendeteksi perubahan struktur file yang lebih variatif.

DAFTAR PUSTAKA

- B, Anumol V, Pooja Thejus, dan Leena Vishnu Namboothiri. 2022. "Enhanced Security In Medical Image Steganography -A Hybrid Approach Using Spatial And Transform Domain." *2022 Second International Conference on Interdisciplinary Cyber Physical Systems (ICPS)*. Chennai, India: IEEE. doi:10.1109/ICPS55917.2022.00043.
- Bartłomiejczyk, Maciej, El Fray Imed, dan Mirosław Kurkowski. 2019. "Multifactor Authentication Protocol in a Mobile Environment." *IEEE Access (IEEE)* 7: 157185 - 157199. doi:10.1109/ACCESS.2019.2948922.
- Deepak, Tatavarthi Sai, dan Vamsidhar Enireddy. 2021. "High Payload Capacity using Steganography Combined with Cryptography." *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. Palladam, India: IEEE. doi:10.1109/I-SMAC52330.2021.9640859.
- Dostálek, Libor. 2019. "Multi-Factor Authentication Modeling." *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*. Ceske Budejovice: IEEE. doi:10.1109/ACITT.2019.8780068.
- Feng, Jinliu, Yaofei Wang, Kejiang Chen, Weiming Zhang, dan Nenghai Yu. 2022. "An Effective Steganalysis for Robust Steganography with Repetitive JPEG Compression." *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Singapore: IEEE.

- doi:10.1109/ICASSP43922.2022.9747061.
- Gordin, Ionel, Adrian Graur, dan Alin Potorac. 2019. "Two-factor authentication framework for private cloud." *2019 23rd International Conference on System Theory, Control and Computing (ICSTCC)*. Sinaia: IEEE. doi:10.1109/ICSTCC.2019.8885460.
- Gurunath, R. , Mohammad Fadel Jamil Klaib, Debabrata Samanta, dan Mohammad Zubair Khan. 2021. "Social Media and Steganography: Use, Risks and Current Status." *IEEE Access* (IEEE) 9: 153656 - 153665. doi:10.1109/ACCESS.2021.3125128.
- Hajji, Khaled Al, Abdulrahman Cenadi, dan Farouq Ahmad. 2022. "Machine Learning based Human Face Recognition for Attendance System." *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. Ankara: IEEE. doi:10.1109/HORA55278.2022.9799883.
- Mandalapu, Hareesh, Aravinda Reddy P N, Raghavendra Ramachandra, Krothapalli Sreenivasa Rao, Pabitra Mitra, S. R. Mahadeva Prasanna, dan Christoph Busch. 2021. "Audio-Visual Biometric Recognition and Presentation Attack Detection: A Comprehensive Survey." *IEEE Access* (IEEE) 9: 37431 - 37455. doi:10.1109/ACCESS.2021.3063031.
- Sharma, Reena, Kumar Vijay Sharma, dan Arjun Singh. 2021. "A Review Paper on Facial Recognition Techniques." *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. Palladam: IEEE. doi:10.1109/I-SMAC52330.2021.9640896.
- Verma, Amit, Mohammed Baljon, Shailendra Mishra, Iqbaldeep Kaur, Ritika Saini, Sharad Saxena, dan Sanjay Kumar Sharma. 2022. "Secure Rotation Invariant Face Detection System for Authentication." *Computers, Materials & Continua* (Tech Science Press) 7 (1): 1955-1974. doi:https://doi.org/10.32604/cmc.2022.020084.