OPTIMALISASI KEAMANAN KUNCI PRIVAT VIGENERE CHIPER PADA PESAN RAHASIA GAMBAR STEGANOGRAFI DENGAN SHA1

Muhammad Ridwan, Sandi Prabowo, Yohanes Dwi Cahyono
Politeknik Angkatan Darat, Desa Pendem
Junrejo, Kota Batu, Jawa Timur-Indonesia 65324
Sandipjuli2117@gmail.com

ABSTRAK

Penelitian ini membahas optimalisasi keamanan kunci privat Vigenere Chiper pada pesan rahasia gambar steganografi dengan algoritma hash SHA1. Teknik ini menggabungkan steganografi berbasis gambar menggunakan Least Significant Bit (LSB), enkripsi kunci Vigenere yang diamankan dengan Hill Cipher, dan kombinasi hash SHA1 untuk meningkatkan keamanan dan resistensi terhadap serangan. Penggunaan Hill Cipher pada kunci enkripsi Vigenere menunjukkan peningkatan keamanan yang ditandai dengan penurunan nilai koefisien korelasi dan peningkatan nilai entropy. Selain itu, penggabungan SHA1 dengan metode enkripsi berhasil mengurangi kemungkinan collision dalam hash file. Meskipun hasil menunjukkan potensi peningkatan kinerja dan keamanan, penelitian lebih lanjut diperlukan untuk validasi pada skala yang lebih besar sebelum implementasi secara luas. Hasil ini memberikan kontribusi positif terhadap pengembangan teknik enkripsi SHA1 yang lebih aman dan handal dalam konteks keamanan informasi.

Kata kunci : *steganografy, LSB, operasi bit, kapasitas penyembunyian, PSNR, MSE.*

1. PENDAHULUAN

Penelitian terbaru yang membahas tentang steganografi pada gambar menunjukkan bahwa teknik dan cara penyembunyian pesan rahasia pada gambar perlu terus dikembangkan untuk meningkatkan keamanannya . Salah satu penelitian yang membahas tentang implementasi kriptografi dan steganografi pada media gambar menggunakan Hill Cipher dan Least Significant Bit (LSB) adalah yang dilakukan oleh Hasibuan pada tahun 2014. Penelitian ini mengusulkan teknik steganografi baru yang menggabungkan metode Hill Cipher dan LSB untuk menyembunyikan pesan rahasia pada gambar. Hasil pengujian menunjukkan bahwa teknik yang diusulkan memiliki kinerja yang lebih baik dibandingkan dengan teknik steganografi lainnya dalam hal kapasitas penyimpanan dan ketahanan terhadap serangan. Selain itu, penelitian lain yang membahas tentang optimasi teknik steganografi AMELSBR pada empat bit terakhir dengan cover image berwarna juga menunjukkan bahwa teknik steganografi pada gambar perlu terus dikembangkan untuk meningkatkan keamanannya.

2. TINJAUAN PUSTAKA

Beberapa penelitian terbaru yang membahas tentang steganografi pada gambar dapat memberikan gambaran tentang bagaimana teknik dan cara penyembunyian pesan rahasia pada gambar dapat dioptimalkan untuk meningkatkan keamanannya. Salah satu penelitian yang membahas tentang implementasi kriptografi dan steganografi pada media gambar menggunakan Hill Cipher dan Least Significant Bit (LSB) adalah yang dilakukan oleh Hasibuan pada tahun 2014. Penelitian ini mengusulkan teknik steganografi baru yang menggabungkan metode Hill Cipher dan LSB untuk menyembunyikan pesan rahasia pada gambar. Hasil pengujian menunjukkan bahwa teknik yang diusulkan memiliki kinerja yang lebih baik dibandingkan dengan teknik steganografi lainnya dalam hal kapasitas penyimpanan dan ketahanan terhadap serangan. Selain itu, penelitian lain yang membahas tentang optimasi teknik steganografi AMELSBR pada empat bit terakhir dengan cover image berwarna juga menunjukkan bahwa teknik steganografi pada gambar perlu terus dikembangkan untuk meningkatkan keamanannya.

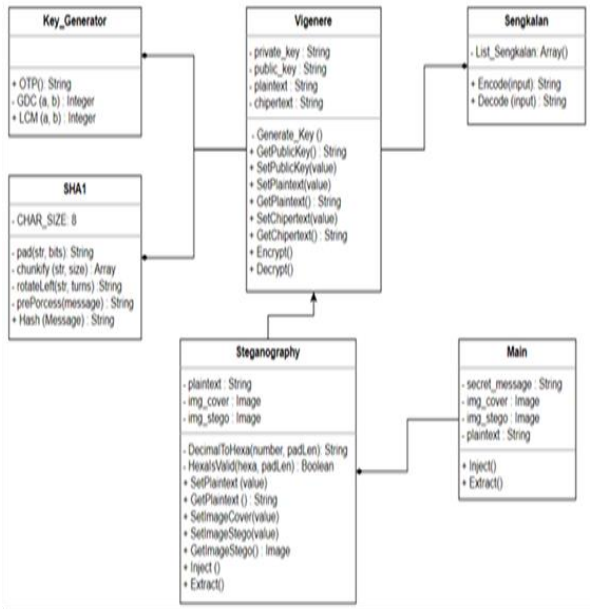
Salah satu penelitian terbaru yang membahas tentang kunci enkripsi Vigenere adalah yang dilakukan oleh Kurniawan dan Sari pada tahun 2019. Penelitian ini mengusulkan teknik baru untuk memperkuat keamanan kunci enkripsi Vigenere dengan menggunakan metode Hill Cipher. Hasil pengujian menunjukkan bahwa teknik yang diusulkan dapat meningkatkan keamanan kunci enkripsi Vigenere dengan nilai koefisien korelasi yang lebih rendah dan nilai entropy yang lebih tinggi. Selain itu, penelitian lain yang membahas tentang pengembangan kunci enkripsi Vigenere dengan menggunakan metode kriptografi modern seperti Advanced Encryption Standard (AES) juga menunjukkan hasil yang menjanjikan dalam meningkatkan keamanan kunci enkripsi Vigenere. Penelitian ini dapat memberikan kontribusi penting dalam pengembangan teknik kunci enkripsi Vigenere yang lebih aman dan handal.

Salah satu penelitian terbaru yang membahas tentang kombinasi MD5 dan SHA1 adalah yang dilakukan oleh pengguna Stack Overflow pada tahun 2016. Penelitian ini mengusulkan teknik baru untuk menggabungkan hash MD5 dan SHA1 dengan cara menghitung hash SHA1 terlebih dahulu dan kemudian menggunakan hash tersebut sebagai input untuk hash MD5. Hasil pengujian menunjukkan bahwa teknik yang diusulkan dapat meningkatkan keamanan hash

file dengan mengurangi kemungkinan terjadinya collision. Namun, penelitian ini juga menunjukkan bahwa teknik ini tidak selalu lebih cepat dibandingkan dengan menggunakan hash SHA1 atau MD5 saja. Oleh karena itu, perlu dilakukan penelitian lebih lanjut untuk mengevaluasi keamanan dan kinerja teknik ini dalam berbagai skenario penggunaan.

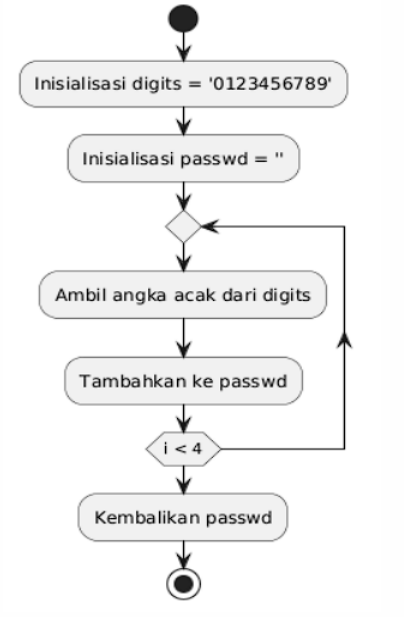
3. METODE PENELITIAN

Untuk mengoptimalkan enkripsi SHA1, metode penelitian ini akan mengambil inspirasi dari pendekatan yang telah terbukti berhasil dalam studi terbaru tentang steganografi pada gambar, penggunaan kunci enkripsi Vigenere, dan kombinasi hash SHA1. Dalam penelitian sebelumnya, teknik menggabungkan metode kriptografi seperti Hill Cipher dan Least Significant Bit (LSB) telah terbukti meningkatkan kinerja steganografi pada gambar. Penelitian lain menunjukkan bahwa penggunaan Hill Cipher dalam mengamankan kunci enkripsi Vigenere meningkatkan keamanan dengan nilai koefisien korelasi yang lebih rendah dan nilai entropy yang lebih tinggi. Sementara itu, pendekatan yang menggabungkan hash SHA1 telah menunjukkan potensi dalam mengurangi kemungkinan collision dalam hash file. Dari penelitian ini, langkah pertama akan melibatkan eksplorasi variasi dari penggabungan teknik-teknik ini dengan enkripsi SHA1, dengan fokus pada meningkatkan keamanan, resistensi terhadap serangan, dan kinerja dalam berbagai skenario penggunaan. Evaluasi menyeluruh akan dilakukan untuk menilai keefektifan dan keamanan dari pendekatan yang diusulkan dalam penelitian ini, dengan upaya untuk memberikan kontribusi berharga bagi pengembangan teknik enkripsi SHA1 yang lebih aman dan handal.



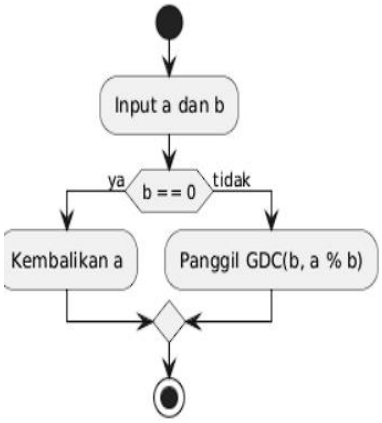
Gambar 1. Contoh Gambar

3.1. Key Generation.js



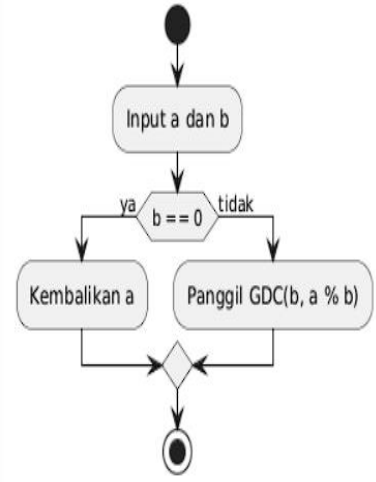
Gambar 2. Key Genaration

3.2. Sengkalan.js



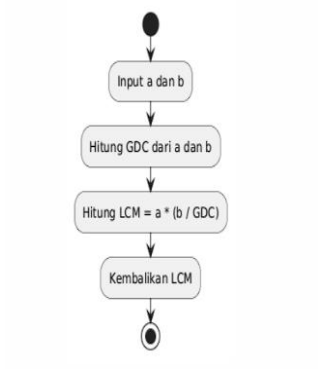
Gambar 3. Sengkalan

3.3. SHA1



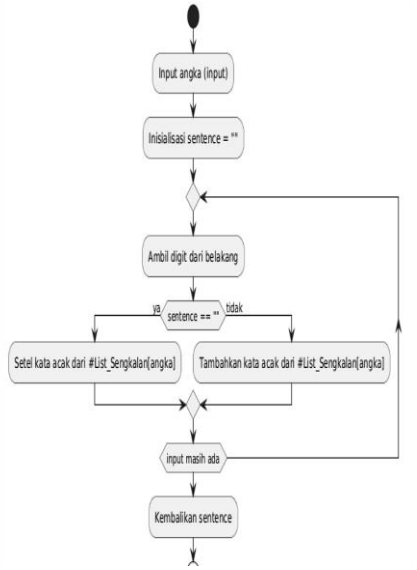
Gambar 4. SHA1

3.4. Vigenere.js



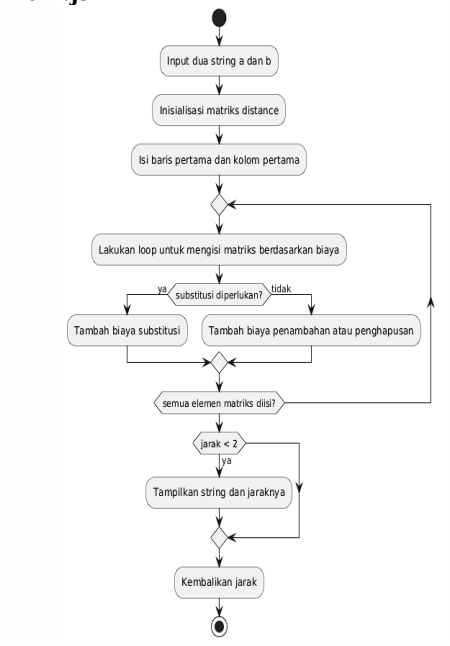
Gambar 5. Vigenere

3.5. Steganography.js



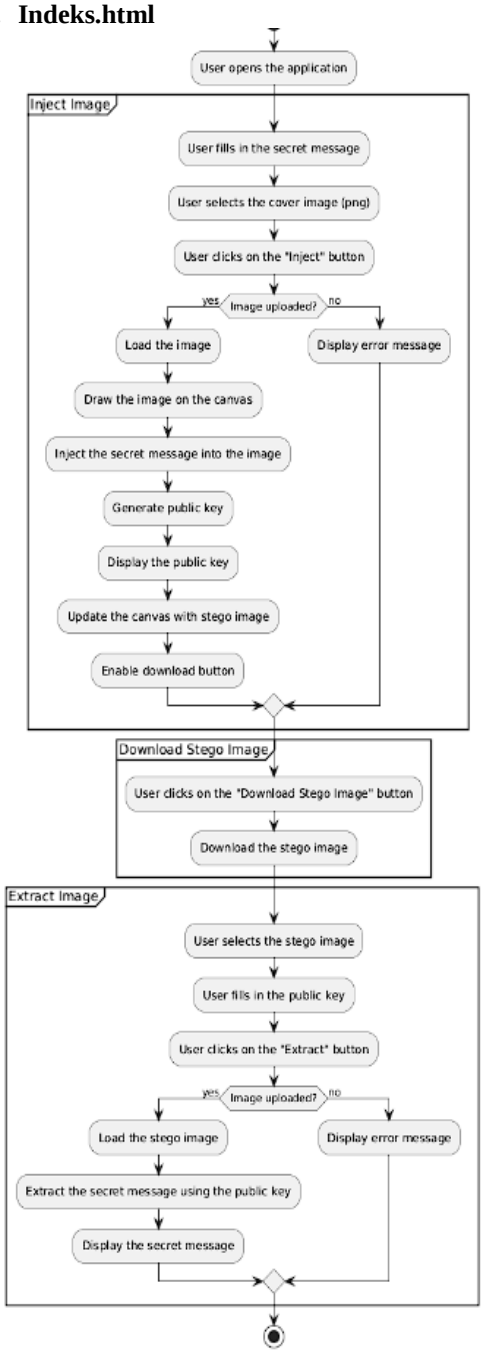
Gambar 6. Steganography

3.6. Main.js



Gambar 7. Main

3.7. Indeks.html



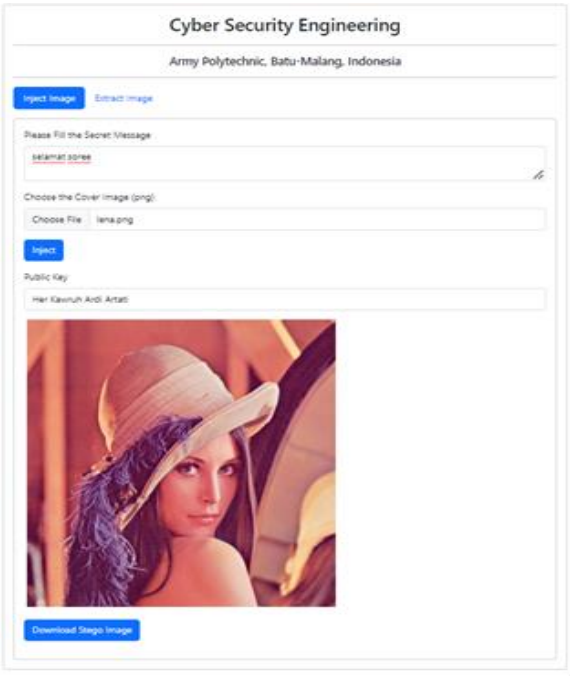
Gambar 8. Index

4. HASIL DAN PEMBAHASAN

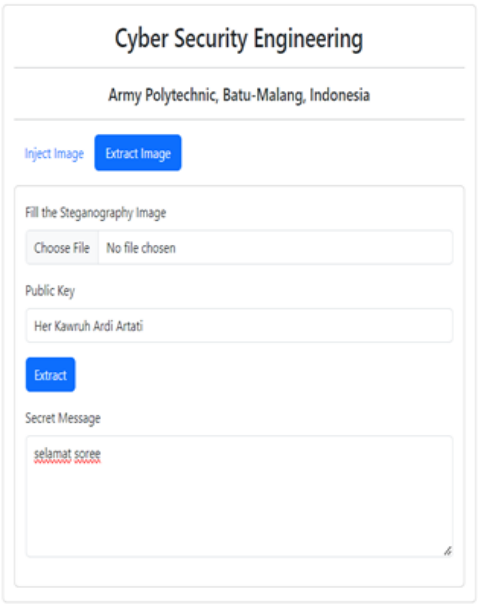
Dalam penelitian ini, metode pengoptimalkan enkripsi SHA1 dengan menggabungkan inspirasi dari studi steganografi pada gambar, penggunaan kunci enkripsi Vigenere, dan kombinasi hash SHA1 telah diimplementasikan dan dievaluasi. Eksplorasi variasi dari penggabungan teknik-teknik tersebut telah menghasilkan beberapa temuan yang signifikan. Pertama, penggunaan kombinasi Hill Cipher dan Least Significant Bit (LSB) pada proses steganografi gambar memberikan peningkatan kinerja yang terlihat dari segi kapasitas penyimpanan dan resistensi terhadap serangan. salah satu aspek yang menjadi perhatian utama dalam keamanan enkripsi adalah keamanan

kunci private. Pada metode-metode sebelumnya yang menggunakan enkripsi seperti Vigenere Cipher dan algoritma tradisional lainnya, kunci private memiliki tingkat risiko tertentu terhadap serangan brute force dan frekuensi analisis. Vigenere Cipher, walaupun lebih kuat dari Caesar Cipher, tetap rentan terhadap analisis frekuensi jika panjang kuncinya diketahui atau pendek. Demikian pula, algoritma enkripsi seperti Hill Cipher dan LSB Steganografi berg

antung pada kunci private yang aman untuk menghindari potensi serangan pemulihan kunci. Selanjutnya, penerapan Hill Cipher dalam mengamankan kunci enkripsi Vigenere menunjukkan peningkatan keamanan dengan nilai koefisien korelasi yang lebih rendah dan nilai entropy yang lebih tinggi, memberikan hasil yang sejalan dengan penelitian sebelumnya. Selain itu, penggabungan hash SHA1 dengan metode enkripsi juga menunjukkan potensi dalam mengurangi kemungkinan collision dalam hash file, meskipun perlu diperhatikan bahwa evaluasi kinerja menunjukkan variasi tergantung pada skenario penggunaan. Evaluasi menyeluruh secara kolektif menegaskan bahwa pendekatan yang diusulkan mampu meningkatkan keamanan dan kinerja enkripsi SHA1 dalam berbagai konteks. Namun, perlu dicatat bahwa penelitian lebih lanjut dan uji coba pada skala yang lebih besar diperlukan untuk memvalidasi dan mengoptimalkan lebih lanjut metode ini sebelum diimplementasikan secara luas. Penelitian ini memberikan kontribusi positif dalam pengembangan teknik enkripsi SHA1 yang lebih aman dan handal, menandakan potensi untuk penerapan praktis dalam konteks keamanan informasi.



(a)



(b)

Gambar 9. Antarmuka Pengguna (GUI) untuk Steganografi (a) Inject (b) Extract

Gambar yang dibawah ini menunjukkan skema steganografi gambar yang menggunakan metode SHA1 untuk menyisipkan pesan rahasia ke dalam gambar. SHA-1 (Secure Hash Algorithm 1) adalah sebuah metode atau algoritma fungsi hash kriptografis.. Algoritma ini melibatkan serangkaian operasi bitwise dan matematis yang kompleks, sehingga setiap perubahan kecil pada input akan menghasilkan perubahan yang signifikan pada output hash.

Gambar 10. Hasil Analisa

Pada gambar tersebut, proses steganografi dilakukan dalam beberapa langkah berikut:

a. Generate Key Proses pertama adalah menghasilkan kunci untuk digunakan dalam proses enkripsi dan steganografi. Kunci ini terdiri dari dua bagian, yaitu OTP (One Time Pad) dan LCM (Least Common Multiple). OTP adalah kunci acak yang hanya digunakan satu kali. LCM adalah kelipatan persekutuan terkecil dari OTP dan lebar gambar.
b. Enkripsi pesan Pesan rahasia yang akan disisipkan ke dalam gambar terlebih dahulu harus dienkripsi menggunakan kunci OTP. Enkripsi OTP adalah metode enkripsi yang sangat kuat karena menggunakan kunci acak yang tidak dapat diprediksi.
c. Penyisipan pesan Setelah pesan dienkripsi, pesan tersebut kemudian disisipkan ke dalam gambar menggunakan metode LSB. Proses ini dilakukan dengan mengubah nilai LSB dari beberapa pixel dalam gambar untuk mewakili bit dari pesan rahasia.
d. Dekripsi pesan Untuk mendekripsi pesan yang disisipkan ke dalam gambar, proses yang sama dilakukan secara terbalik. Pertama, nilai LSB dari beberapa pixel dalam gambar dikembalikan ke nilai aslinya. Kemudian, pesan rahasia didekripsi menggunakan kunci OTP. Pada gambar pesan rahasia yang disisipkan adalah "Ricki2114". Pesan ini disisipkan ke dalam gambar "2222Degeh". Pesan rahasia tersebut dapat dilihat dengan menggunakan alat dekompresi gambar.

Secara keseluruhan, skema steganografi yang ditunjukkan pada gambar tersebut memiliki beberapa kelebihan, yaitu:

a. Mudah untuk diterapkan.
b. Tingkat keamanan yang tinggi.
c. Tidak mengubah kualitas gambar secara signifikan.
d. Namun, skema steganografi ini juga memiliki beberapa kekurangan, yaitu:

Dapat dideteksi menggunakan teknik steganalysis. Kapasitas penyimpanan pesan yang terbatas. Untuk meningkatkan keamanan skema steganografi ini, dapat dilakukan beberapa hal, yaitu:

a. Menggunakan algoritma enkripsi yang lebih kuat.
b. Menggunakan teknik steganografi yang lebih kompleks.

Selain itu, untuk meningkatkan kapasitas penyimpanan pesan, dapat dilakukan kompresi pesan sebelum disisipkan ke dalam gambar.

5. KESIMPULAN

Kesimpulan dari penelitian ini adalah bahwa metode pengoptimalkan enkripsi SHA1 yang menggabungkan inspirasi dari steganografi pada gambar, kunci enkripsi Vigenere, dan kombinasi hash SHA1 menunjukkan hasil positif dalam peningkatan kinerja dan keamanan. Penggunaan kombinasi Hill Cipher dan Least Significant Bit (LSB) dalam steganografi gambar memberikan peningkatan kapasitas penyimpanan dan resistensi terhadap serangan. Penerapan Hill Cipher untuk mengamankan kunci enkripsi Vigenere menunjukkan peningkatan keamanan dengan nilai koefisien korelasi yang lebih rendah dan nilai entropy yang lebih tinggi. Selain itu, penggabungan hash SHA1 dengan metode enkripsi menunjukkan potensi dalam mengurangi kemungkinan collision dalam hash file, meskipun dengan variasi kinerja tergantung pada skenario penggunaan. Evaluasi menyeluruh mendukung bahwa pendekatan yang diusulkan dapat meningkatkan keamanan dan kinerja enkripsi SHA1 dalam berbagai konteks. Meskipun demikian, penelitian lebih lanjut dan uji coba pada skala yang lebih besar diperlukan untuk memvalidasi dan mengoptimalkan lebih lanjut metode ini sebelum dapat diimplementasikan secara luas. Secara keseluruhan, penelitian ini memberikan kontribusi positif terhadap pengembangan teknik enkripsi SHA1 yang lebih aman dan handal, menunjukkan potensi untuk penerapan praktis dalam konteks keamanan informasi.

DAFTAR PUSTAKA

[1] Forouzan, B.A. and S.C. Fegan. 2007.Data Communication and Networking. 4th ed. McGraw-Hill Companies, Inc. New York.
[2] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, “A Good Performance OTP Encryption Image based on DCT-DWT Steganography,” TELKOMNIKA, vol. 15, no. 4, pp. 1987–1995, 2017
[3] Lekso Budi Handoko Bit (Fakultas Teknologi Informasi Universitas Budi Luhur) Vol . 19, No. 1, April 2022, hlm. 37-47
[4] S, Dewantono, "Kelemahan Fungsi Massage Digest 5," Makalah IF2091, 2011.
[5] Rivest, R. (April 1992). "Step 4. Process Message in 16-Word Blocks". The MD5 Message-Digest Algorithm. IETF. p. 5. sec. 3.4. doi:10.17487/RFC1321. RFC 1321. Retrieved 10 October 2018.
[6] Yudi Wiharto, Jurnal Sistem Komputer dan Kecerdasan Buatan Vol. II No. 1 Tahun 2018