Penggunaan Kombinasi Kriptografi Triple DES dan Teknik Steganografi LSB dalam Mengamankan Pesan Militer

Adityan Wisnu Yuda Prasetya[1], Bambang Suhardjo[2], Rinaldy Munir[3]
Institution/affiliation
addres, telp/fax of institution/affiliation
e-mail:
[1]adityan.prasetya@tp.idu.ac.id,[2]bambang_suharjo@tnial.mil.id,[3]rinaldi@staff.stei.itb.ac.id

ABSTRAK

Pengamanan data informasi merupakan hal krusial dalam proses komunikasi. hal ini dikarenakan informasi sangat rentan disalahgunakan pihak yang tidak bertanggung jawab sehingga dapat merugikan pihak yang mengirimkan informasi. Pada penelitian ini algoritma kriptografi yang digunakan adalah kombinasi triple DES dan Steganografi LSB. Dimana Algoritma 3DES akan melakukan proses enkripsi selama 3 kali. Setelah dilakukan enkripsi selanjutnya data informasi yang dienkripsi akan disisipkan dengan metode steganografi LSB. Tujuan dari penelitian ini adalah untuk mengamankan informasi sehingga sulit dipecahkan oleh pihak yang tidak bertanggung jawab dengan menggunakan kombinasi 3DES dengan Teknik Steganografi LSB. Hasil Dari penelitian ini menunjukkan bahwa penggunakan enkripsi 3DES dan LSB dapat menampung hingga 2000 karakter pesan dengan waktu 8,8 detik.

Kata Kunci :Kriptografi 3DES, Steganografi LSB

ABSTRACT

Securing information data is a crucial aspect of the communication process. This is because information is highly susceptible to misuse by irresponsible parties, potentially harming the sender of the information. In this research, the cryptographic algorithm used is a combination of triple DES and LSB Steganography. The 3DES algorithm performs encryption in three rounds. After encryption, the encrypted information data will be embedded using LSB Steganography. The aim of this study is to secure information to make it difficult for unauthorized parties to decipher, using a combination of 3DES and LSB Steganography techniques. The results of this research indicate that the use of 3DES encryption and LSB can accommodate up to 2000 characters of message within 8.8 seconds.

.

Keywords: *Cryptography 3DES, Steganography LSB*

1. PENDAHULUAN

Teknologi informasi dan komunikasi telah memberi pengaruh peningkatan jumlah pertukaran data yang terjadi antara pengguna. Selain itu perkembangan jaringan komputer, dalam hal ini teknologi nirkabel juga telah berpengaruh dalam mobilitas user dan transmisi data[1].

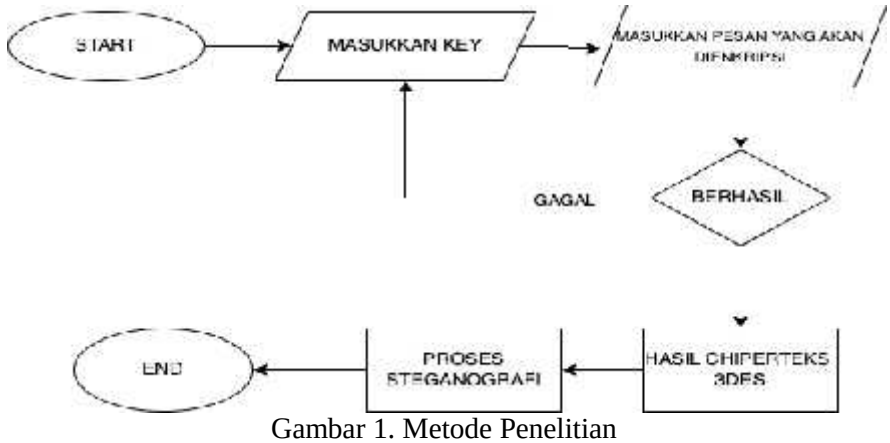
Pengiriman data harus memperhatikan tiga prinsip keamanan jaringan yaitu kerahasiaan data, integristas data dan ketersediaan data saat dibutuhkan. Hal ini diperlukan untuk menghindari penyadapan atau modifikasi pesan yang diperbuat oleh pengguna yang tidak

memiliki hak membaca maupun mengubah informasi.

Teknik keamanan terdiri dari beberapa model. Sala satunya adalah Teknik Steganografi. Teknik ini akan menyembunyikan pesan rahasia pada media gambar. Dengan pertimbangan masalah yang telah dijelaskan maka diperlukan pengenkrispsian data sebelum data disembunyikan dengan teknik kriptografi, dimana Teknik dipakai menggunakan metode gabungan dari algoritma kriptografi Triple Data Encryption Standard (DES) dan metode steganografi Least Significant Bit (LSB) yang diharapakan memberikan proteksi terhadap pesan yang akan dikirim secara berlapis.

2. METODE PENELITIAN

Pada gambar 1 menampilkan metode penelitian pada penelitian ini.



Gambar 1. Metode Penelitian

Pada Gambar 1 merupakan gambaran proses enkripsi menggunakan kombinasi 3DES dan Steganografi LSB. Proses awal dimulai dengan memasukkan key yang akan digunakan untuk otentikasi pesan yang akan dirahasiakan. Selanjutnya adalah memasukkan pesan yang ingin dirahasiakan. Setelah pesan sudah dimasukkan. Program akan melakukan enkripsi menggunakan 3DES dengan kombinasi key yang telah dimasukkan sebelumnya. Jika berhasil akan menampilkan hasil enkripsi berupa chiperteks dari pesan yang telah dienkripsi. Hasil Chiperteks yang telah dienkripsi akan disisipkan ke gambar menggunakan Teknik steganografi LSB.

3. HASIL DAN PEMBAHASAN

Pada tahapan ini, metode yang digunakan kemudian dievaluasi dengan melihat hasil proses enkrip dan dekrip dengan menggunakan algoritma Triple DES dan LSB. Tahapan enkripsi dan dekripsi algoritma Triple DES dicapai dengan menggunakan model enkripsi $DES - EEE2$, $K1 \neq K2$, $K3 = K1$, $C = E[E\{E(P,K1\ )K2\ \},K3\ ]$, dekripsi $DES - DDD2$, $K1 \neq K2$,$K3 = K1$, $P = D[D\{D(C, K3\ ), K2\ \}K1\ ]$ dimana C = Ciphertext , E = Enkripsi, D = Dekripsi, P = Plaintext, $K1$ = Kunci 1, $K2$ = Kunci 2 dan $K3$ = Kunci 3. Misalnya kita menggunakan plainteks "komputer" dan dua kunci yang berbeda yaitu "password" dan "drowssap". Hasil keluaran dari ciphertext dalam bentuk biner 01001001 10011001 11100100 11101101 11100010 00010000 10111011 11101110.

Cipherteks yang didapat merupakan operasi DES pertama. Selanjutnya lakukan operasi DES lagi dengan kunci yang lain atau dengan kunci yang sama,namun penulis menggunakan dua kunci yang berbeda, dengan kunci kedua drowssap, operasi ini dilakukan sebanyak tiga kali dan didapat hasil kebentuk Hexadecimal dari Triple DES adalah 58 a6 e0 b5 b6 7c 3d ea 0e d5 dc d4 49 99 9d de 76 d7 17 71 bb be e7 44 1d b3 02 06 d2 23 22 76 fe 8b 76 8d 28 97 4a c0 1d 86 46 61 2a 02 3d. Proses enkripsi dan dekripsi boleh memanfaatkan algoritma DES yang serupa. Apabila susunan kunci internal yang di pakai dalam proses enkripsi adalah $K1, K2, \ldots, K16$, maka proses dekripsi pada susunan kunci yang dipakai antara lain $K16, K15, \ldots, K1$. Setiap byte warna dalam sebuah pixel yang tergolong bit LSB di proses perubahan bit-bit nya dengan teknik steganografi LSB. Bit – bit ini kemudian dimodifikasi masing – masing LSB yang tersedia dengan bit – bit yang ber isi informasi lain yang ingin di sembunyikan. Informasi sudah berhasil disisipkan apabila seluruh bit informasi dapat mengganti bit LSB di dalam file tersebut. Saat pesan rahasia ingin di buka kembali, bit – bit LSB di ambil satu per satu selanjutnya di gabungkan untuk berubah kembali menjadi informasi sempurna sesuai dengan sediakala.

Bit – bit LSB di tentukan berdasarkan dengan kesesuaian susunannya, ukuran dari panjang data rahasia yang disembunyikan kemudian disesuaikan mulai dari binary yang awal sampai dengan byte yang terakhir. Persepsi visual tidak terpengaruh terhadap perubahan nilai bit LSB hanya karena mengubah isi byte satu lebih tinggi atau lebih rendah. Menentukan bit yang termasuk dalam bit LSB dapat dilihat pada angka berikut 11010010 dimana 1 angka awal termasuk MSB dan 0 diangka terakhir termasuk LSB.

Gambar latih yang akan digunakan pada penelitian ini ditunjukkan pada gambar 1 Dalam bentuk format rgb dengan ekstensi .png.

Gambar 2. Gambar Latih

Pada Penelitian ini penulis menerapkan Teknik Enkripsi 3DES dan LSB menggunakan Bahasa pemograman Python. Library yang dibutuhkan pada penelitian ini terdiri dari : pycryptodomex, dan Python Imaging tools yang digunakan untuk melakukan Teknik Steganografi. Berikut listing code untuk melakukan enkripsi menggunakan 3Des.

```
def encrypt_des(msg):
    cipher = DES3.new(key, DES3.MODE_EAX)
    nonce = cipher.nonce
    ciphertext = cipher.encrypt(msg.encode('ascii'))
    return nonce, ciphertext
```

Selanjutnya dilakukan proses Teknik stegranografi yang ditunjukkan pada listing code dibawah ini .

```
def encode_enc(newimg, data):
    w = newimg.size[0]
    (x, y) = (0, 0)
    for pixel in modPix(newimg.getdata(), data):
        newimg.putpixel((x, y), pixel)
        if (x == w - 1):
            x = 0
            y += 1
        else:
            x += 1
```

Berikut spesifikasi computer yang penulis butuhkan untuk penelitian ini. Ditunjukkan pada tabel 1. Hasil percobaan dari penelitian ini ditunjukkan pada tabel 2 dimana parameter yang digunakan pada penelitian ini adalah ukuran byte hasil enkripsi waktu enkripsi dan dekripsi dengan 3 variasi karakter sejumlah 500, 1000 dan 2000 karakter.

Spesifikasi PC	Ukuran Byte Gambar Hasil Enkripsi
Processor	Intel Core i3-3350M CPU 2.30GHz
Memory	4096 MB
OS	Windows 10
Harddisk	500GB

Tabel 2. Hasil Pengujian

Karakter	Ukuran Byte Gambar Hasil Enkripsi	Waktu Enkripsi	Waktu Dekripsi
500	10	6.8648	7.3658
1000	15	6.9818	7.5178
2000	20	9.8232	8.8152

Dari hasil percobaan yang dilakukan semakin besar jumlah karakter pesan yang di enkripsi dan sisipkan pada gambar maka besar juga ukuran gambar akan tetapi karena menggunakan steganografi LSB secara kasat mata tidak terdapat perbedaan warna walaupun gambar telah disisipkan pesan rahasia, karena bit yang rendah dalam pesan rahasia yang disisipkan pada data pixel citra tersebut yang tersusun dari warna seperti merah, hijau dan biru. Selain itu dengan memanfaatkan algoritma kritografi Triple DES maka pesan rahasia di enkrip sebelum disisipkan

dan hanya diakses oleh pengguna yang memiliki kunci pesan. Besar format pesan dapat mempengaruhi perubahan waktu pada masing - masing percobaan.

4. KESIMPULAN

Penelitian ini menggunakan dua mode keamanan data, yang dapat ditarik kesimpulan sebagai berikut semakin banyak pesan yang di enkripsi dan disembunyikan maka semakin besar ukuran gambar yang disisipkan pesan. Algoritma kriptografi Triple DES dan steganografi LSB sanggup memberikan keamanan ganda karena pesan bukan hanya tersembunyi dalam gambar tetapi juga terenkrip menggunakan algoritma kriptografi Triple DES. Kerahasiaan informasi hanya dapat dimanfaatkan oleh pihak yang berwenang yang tahu kunci untuk mengakses, selain itu kualitas keaslian data yang dikirim dan diterima tetap sama karena kunci untuk membuka pesan dan mengubah hanya di katahui oleh pihak yang berwenang.

5. SARAN

Untuk penelitian selanjutnya pada penelitian ini dapat dilakukan kombinasi beberapa metode agar dari sisi keamanan dapat ditingkatkan lebih baik lagi.

DAFTAR PUSTAKA

[1] MUHAMMAD, K., SAJJAD, M., MEHMOOD, I., RHO, S. & BAIK, S.W., 2016. A novel magic LSB substitution method (M-LSBSM) using multi-level encryption and achromatic component of an image. Multimedia Tools and Applications, 75(22), pp.14867–14893.

[2] NASUTION, A.B., EFENDI, S. & SUWILO, S., 2018. Image Steganography In Securing SoundFile Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB). Journal of Physics: Conference Series, 1007, p.012010.

[3] NOFRIANSYAH, D., DEFIT, S., NURCAHYO, G.W., GANEFRI, G., RIDWAN, R., AHMAR, A.S. & RAHIM, R., 2018. A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm. Journal of Physics: Conference Series, 954, p.012003.

[4] PATIL, P., NARAYANKAR, P., NARAYAN D.G. & MEENA S.M., 2016. A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science, 78, pp.617– 624.

[5] RANTELINGGI, P.H. & DJANALI, S., 2015. Kinerja Protokol Routing Pada Lingkungan Wireless Mesh Network dengan combined scalable video coding. JUTI: Jurnal Ilmiah Teknologi Informasi, 13(1), p.86.

[6] RANTELINGGI, P.H., PAIKI, F.F. & RANTELOBO, K., 2017. Performance of routing protocol in MANET with combined scalable video coding. In: 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). 2017

4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). pp.1–4.

[7] RATNADEWI, ADHIE, R.P., HUTAMA, Y., SALEH AHMAR, A. & SETIAWAN, M.I., 2018. Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC). Journal of Physics: Conference Series, 954, p.012009.

[8] J. Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing," in IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271-2282, Oct. 2013, doi: 10.1109/TKDE.2011.78.

[9] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee and W. Lou, "Secure Deduplication with Efficient and Reliable Convergent Key Management," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 6, pp. 1615-1625, June 2014, doi: 10.1109/TPDS.2013.284.

[10] S. Tayal, N. Gupta, P. Gupta, D. Goyal, M. Goyal, "A review paper on network security and cryptography," Advances in Computational Sciences and Technology, vol. 10, no. 5, pp. 763-770, 2017. [6] P. Dixit, A. K. Gupta, M. C. Trivedi, V. K. Yadav, "Traditional and hybrid encryption techniques: a survey," in Networking communication and data knowledge engineering, Springer, pp. 239-248, 2018.

[11] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, M. F. Ijaz, "Analytical Study of Hybrid Techniques for Image Encryption and Decryption," Sensors, vol. 20, no. 18, pp. 5162, 2020, doi: 10.3390/s20185162. [8] S. Mishra and A. Dastidar, "Hybrid Image Encryption and Decryption using Cryptography and Watermarking Technique for High Security Applications," 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), 2018, pp. 1-5, doi: 10.1109/ICCTCT.2018.8551103.

[12] A. Abdullah, "Advanced encryption standard (aes) algorithm to encrypt and decrypt data," Cryptography and Network Security, vol. 16, pp. 1-11, 2017. [10] S. R. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," Indonesian Journal of Electrical Engineering and Computer Science, vol. 18, no. 2, pp.774-781, 2020, doi: 10.11591/ijeecs.v18.i2.pp774-781.

[13] T. Hidayat and R. Mahardiko, "A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing," International Journal of Artificial Intelligence Research, vol. 4, no.1, pp. 49-57, 2020.

[14] P. Semwal and M. K. Sharma, "Comparative study of different cryptographic algorithms for data security in cloud computing," 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall), 2017, pp. 1-7, doi: 10.1109/ICACCAF.2017.8344738.

[15] N. A. Al-gohany and S. Almotairi, "Comparative Study of Database Security in Cloud Computing Using AES and DES Encryption Algorithms," Journal of Information Security and Cybercrimes Research, vol. 2, no. 1, pp. 102-109, 2019.

[16] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms,"

2017 International Conference on Engineering and Technology (ICET), 2017, pp. 1-7, doi: 10.1109/ICEngTechnol.2017.8308215.

[17] Por, L.Y., Beh, D., Ang, T.F. & Ong, S.Y. 2013. An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm. The International Arab Journal of Information Technologi. pp. 51-60

[18] Kaul, N. and Bajaj, N. 2013. Audio in Image Steganography based on Wavelet Transform. International Journal of Computer Application. pp. 7-10

[19] Husain, M.P. & Rafat, K.F. 2016. Enhanced Audio LSB Steganography for Secure Communication. International Journal of Advanced Computer Science and Applications. pp. 340-347

[20] Kumar, S., Barnali, B. & Banik, G. 2012. LSB Modification and Phase Encoding Technique of Audio Steganography Revisited. International Journal of Advanced Research in Computer and Communication Engineering. pp . 1-4

[21] Habib, A. & Chowdhury, D. 2015. An Efficient Compression Technique Using Arithmetic Coding. Journal of Scientific Research & Reports 4 (1). pp. 60-67

[22] Sentilkumar, M. & Mathivanan, V. 2016. Analysis of Data Compression Techniques using Huffman Coding and Arithmetic Coding. International Journal of Advanced Research in Computer Science and Software Engineering. pp. 930-936

[23] Kumar, P. & Rajaanadan, N.S. 2016. Data Encryption and Decryption Using By Triple DES Performance Efficiency Analysis of Crypto System. International Journal of Innovative Research in Computer and Communication Engineering. pp. 4030-4040

[24] Shreya, M.S. & Khumar, S. 2013. Separable Reversible Data Hiding In Encrypted Image Using Modified Least Significant Bit and Virtual Embedding. International Journal of Science and Research. pp. 3099-3106

[25] Zaher, M.A. 2011. Modified Least Significant Bit (MLSB). Computer and Information Science. pp. 60-67

[26] Laskar, S.A. & Hamachandran, K. 2012. High Capacity Data Hiding Using LSB Steganography and Encryption. International Journal of Database Management System. pp. 57-68

[27] Prasetiyo, B. 2013. Kombinasi Steganografi Bit Matching dan Kriptografi DES untuk Pengamanan Data. Thesis. Universitas Diponegoro: Semarang