Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202071838
Vol. 7, No. 4, Agustus 2020, hlm. 661-666 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018 e-ISSN: 2528-6579

ALGORITMA KRIPTOGRAFI TRIPLE DES DAN STEGANOGRAFI LSB SEBAGAI METODE GABUNGAN DALAM KEAMANAN DATA

Parma Hadi Rantelinggi*[1], Eka Saputra[2]

[1,2] Jurusan Teknik Informatika, Universitas Papua, Manokwari
Email: [1] p.rantelinggi@unipa.ac.id, [2] eka97saputra27@gmail.com
*Penulis Korespondensi

(Naskah masuk: 25 Februari 2019, diterima untuk diterbitkan: 14 Maret 2019)

Abstrak

Keamanan data merupakan hal yang terpenting dalam proses komunikasi data, yang menjadi faktor penting dalam transmisi data jarak jauh seperti tranmisi untuk pengiriman data yang terditribusi lewat internet dalam jumlah pengguna yang banyak, sehingga sangat rentan dan memungkinkan pihak lain dengan sengaja menyadap dan mengubah data sehingga merugikan pihak pemilik data. Dalam penelitian ini menggunakan algoritma TripleDES yang merupakan salah satu algoritma kriptografi untuk menjaga kerahasiaan data dengan mengubah pesan yang dikirim dalam bentuk kode-kode tertentu, dimana algoritma TrpleDES ini melakukan proses enkripsi sebanyak tiga kali. Setelah data di sandikan proses selanjutnya data disisipkan dalam model metode steganografi LSB yang mekanisme kerjanya merekayasa nilai *bit* terakhir dalam satu *byte* data, kedua kombinasi model keamanan ini data sulit untuk dipecahkan oleh pihak lain yang tidak bertanggung jawab. Dalam proses percobaan ini media gambar yang digunakan pada saat menyisipkan pesan hasil ukurannya bertambah sedikit lebih besar dari ukuran asli media gambar karena sudah terdapat pesan rahasia di dalam media gambar tersebut.

Kata kunci: *Keamanan Data, Kriptografi, LSB, TripleDES, Steganografi*

TRIPLE DES CRYPTOGRAPHY ALGORITHM AND LSB STEGANOGRAPHY AS COMBINED METHODS IN DATA SECURITY

Abstract

Data security is crucial in a data communication process. It is an important factor in long-distance data transmissions such as data transmission distributed over the internet loaded with a large number of other users. This causes the transmission very vulnerable and allows other parties to intentionally tap in and possibly change the data that might be harmful for the data owner. In this study a TripleDES algorithm is used. It is one of the cryptographic algorithms that maintains the confidentiality of data by changing sent messages in the form of certain codes. The advantage of the Triple DES algorithm is because this algorithm performs the encryption process three times. After the data has been encrypted, the process is then inserted into the LSB steganographic model, whose mechanism works to engineer the value of the last bit into one byte of data. The combination of the two security models are difficult to breach by other irresponsible parties. In this experimental process, the image used to insert the message results in a size that is slightly larger than the original size of the image media because there is already a secret message in the media image.

Keywords: *Data Security, Cryptography, LSB, TripleDES, Steganography*

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 (Rantelinggi & Djanali, 2015; Rantelinggi, Paiki & Rantelobo, 2017).

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 (Zebua & Ndruru, 2017). Tidak ada jaminan keamanan data maka pihak

lain dengan mudah memperoleh data melalui jaringan komunikasi.(Darwis, Prabowo & Hotimah, 2018)

Berbagai model Teknik keamanan data telah dikembangkan salah satunya adalah Teknik steganografi(Prabowo & Ahmad, 2018), teknik ini menggunakan model penyembunyian pesan rahasia pada sebuah media utama

Namun saat ini banyak pola serangan yang memanfaaatkan kelemahan steganografi, pola tersebut seperti *visual attack* dan *statistical attack*. Pola ini menimbulkan masalah karena itu bagaimana memperoleh keamanan pada suatu data agar dapat disembunyikan dan terjaga kerahasiaan isi nya dari pihak yang tidak berwenang untuk mengaksesnya.

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 diharapkan memberikan proteksi terhadap pesan yang akan dikirim secara berlapis.

Struktur dari penelitian ini sebagai berikut Bab II menjelaskan teori pustaka dan metode yang digunakan, hasil dan pembahasan dijelaskan pada Bab III, penelitian ini disimpulkan pada Bab IV.

2. TINJAUAN PUSTAKA

Pada bagian ini akan dijelaskan secara singkat prinsip kerja model *Triple* DES yang merupakan model pengembangan dari algoritma DES dan teori Steganografi LSB.

2.1. Algoritma Triple DES

Umumnya pola dasar algoritma *Triple* DES menyerupai algoritma DES, perbedaannya terletak pada *Triple* DES mempunyai tiga buah kunci berukuran 128 *bit* yang terdiri dari tiga kunci dengan ukuran 168 *bit* dengan kata lain tiga kali kunci 56 *bit* pada DES, dalam percobaan data disisipkan dalam bentuk sampel *audio* yang dikompres dengan algoritma *arithmetic coding,* kemudian menggunakan algoritma *Triple* DES untuk mengamankan sampel tersebut dengan hasil percobaan kualitas gambar tetap bagus (Patil, dkk., 2016; Ratnadewi, dkk., 2018, Nasution, Efendi & Suwilo, 2018).

Algoritma *Triple* DES memiliki dua model kunci eksternal, pertama yaitu K_1, K_2 dan K_3 merupakan kunci-kunci yang saling bebas, $K_1 \neq K_2 \neq K_3$. Kedua K_1 dan K_2 merupakan pola kunci-kunci yang tidak terkait, dan K_3 sama dengan K_1, $K_1 \neq K_2$ dan $K_3 = K_1$.

2.2. Steganografi LSB

Algoritma steganografi *Least Significant Bit* (LSB) tergolong dalam model algoritma yang merekayasa *bit* terakhir yang terdapat dalam satu *byte* data (Nofriansyah, dkk., 2018; Muhammad, dkk., 2016; Shojae Chaeikar, dkk., 2018; Wang, dkk., 2015). Sederhananya file gambar dimana terdapat pesan yang tersembunyi yang telah disisipkan *bit* rendah dari susunan warna seperti merah, hijau dan biru dalam data *pixel* pada citra, dimana bilangan 8 *bit* dari 0 sampai 255 tersusun dengan bentuk pola biner 00000000 sampai 11111111. Dengan begitu dalam satu *pixel* file bitmap 24 *bit* mampu menyisipkan 3 *bit* data. Sebagai contoh huruf a dapat disisipkan dalam 3 *pixel,* umpamanya pola raster data asli pada Gambar 1 sebagai berikut.

00100111	11101001	11001000
00100111	11001000	11101001
11001000	00100111	11101001

Gambar 1. Data raster asli huruf a

Seperti dalam Gambar 2 huruf a di representasikan dalam biner 01000001 dengan menyisipkan *pixel*.

00100110	11101001	11001000
00100110	11001000	11101000
11001000	00100110	11101001

Gambar 2. Penyisipan huruf a

Sehingga prinsip algoritma LSB bisa diterapkan dalam steganografi gambar. Jenis file citra sebagai media pembawa pesan bisa dalam bentuk file *Joint Photographic Experts Group* (JPEG), *Graphics Interchange Format* (GIF) maupun *Bitmap Image File* (BMP).

3. HASIL DAN PEMBAHASAN

Pada bagian 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 $DES - EEE2$, $K_1 \neq K_2$, $K_3 = K_1$, $C = E[E\{E(P, K_1)K_2\}, K_3]$, dekripsi $DES - DDD2$, $K_1 \neq K_2, K_3 = K_1, P = D[D\{D(C, K_3), K_2\}K_1]$ dimana C = Ciphertext , E = Enkripsi, D = Dekripsi, P = Plaintext, K_1 = Kunci 1, K_2 = Kunci 2 dan K_3 = 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.

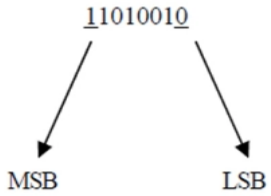
Cipherteks yang didapat merupakan operasi DES pertama. Selanjutnya lakukan operasi DES lagi dengan kunci yang lain atau dengan kunci yang sama,

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 $K_1, K_2, \dots, K_{16}$, maka proses dekripsi pada susunan kunci yang dipakai antara lain $K_{16}, K_{15}, \dots, K_1$.

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 Gambar 3.



Gambar 3. Metode LSB

Gambar latih yang di pakai dalam penelitian ini seperti Gambar 4. Dalam bentuk format *grayscale* dengan kata lain setiap *pixcel* dari gambar ini di sajikan ulang dengan nilai 8 *bit*.

Gambar 4. Lena Grayscale

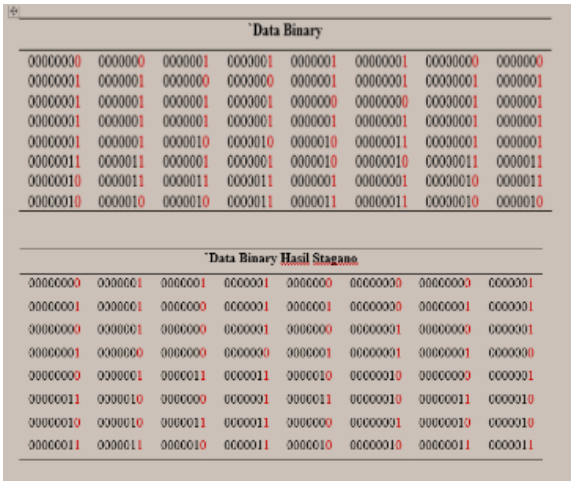
Dimisalkan data berupa kalimat “secret” yang kemudian disisipkan ke dalam Gambar 4. Bila disajikan ulang di dalam bentuk *binary* kata “secret” menjadi seperti pada Tabel 1.

Tabel 1. Data informasi

Karakter	ASCII	Hexadecimal	Binary
s	115	73	01110011
e	101	65	01100101
c	99	63	01100011
r	114	72	01110010
e	99	63	01100011
t	116	74	01110100

Bila dilihat dari proses kerja nya, LSB artinya *bit* yang tidak mempunyai pengaruh besar, maka pola ini mengubah nilai *bit* ke 8 dari Gambar 4 untuk menyisipkan data rahasia. Bisa dilihat pada Gambar 5 merupakan gambar data *binary* dan data *binary* yang disisipan dari Gambar 4.

Setelah data *binary* Gambar 4 disisipkan informasi, Tabel 2 merupakan hasil stegano dalam penelitan ini.



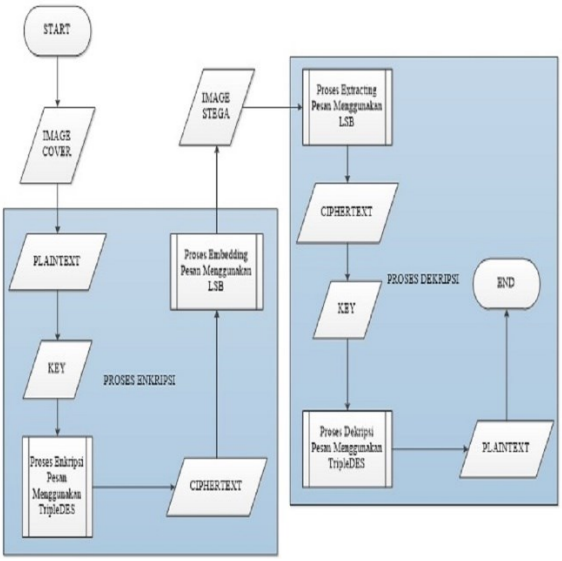
Gambar 5. Data Binary dan Binary Hasil Stegano

Setelah dikontruksi kembali berdasarkan representasi binernya, Gambar 4 akan menjadi gambar yang telah disisipkan pesan rahasia namun tidak akan memiliki perbedaan jauh dengan gambar aslinya, karena yang diubah hanya *bit* paling akhir dari representasi biner gambar aslinya sehingga perubahannya tidak disadari oleh mata manusia.

Untuk memahami proses *encode* dan proses *decode* serta memahami pada saat kapan menggunakan algoritma *Triple* DES dan Metode LSB, berikut disajikan diagram alir dari proses *encode* dan *decode* dalam penelitian ini yang dapat diamati pada Gambar 6

Tabel 2. Data Binary informasi

`Data Binary Informasi							
0	1	1	1	0	0	1	1
0	1	1	0	0	1	0	1
0	1	1	0	0	0	1	1
0	1	1	1	0	0	1	0
0	1	1	0	0	0	1	1
0	1	1	1	0	1	0	0
0	1	1	1	0	0	1	1
0	1	1	0	0	1	0	1



Gambar 6. *Flowchart* proses *encode* dan *decode Triple*DES dan LSB

Berikut ini merupakan *code* untuk menentukan kunci, agar kunci dapat digunakan dalam algoritma tersebut, digambarkan pada Gambar 7.

```
Private Function TruncateHas(ByVal key As String,
ByVal length As Integer) As Byte()
    Dim keyBytes() As Byte =
System.Text.Encoding.ASCII.GetBytes(key)
    ReDim Preserve keyBytes(length - 1)
    Return keyBytes
  End Function

  Sub New(ByVal key As String)
    des.Key = TruncateHas(key, des.KeySize \ 8)
    des.IV = TruncateHas("", des.BlockSize \ 8)
  End Sub
```

Gambar 7. Kode Algoritma Kunci

Code proses enkripsi yang berada pada *class Triple* DES, dapat dilihat pada Gambar 8.

```
Public Function EncryptData(ByVal plaintext As String)
As String
    Dim plaintextBytes() As Byte =
System.Text.Encoding.ASCII.GetBytes(plaintext)
    Dim ms As New System.IO.MemoryStream
    Dim encStream As New CryptoStream(ms,
des.CreateEncryptor(),
System.Security.Cryptography.CryptoStreamMode.Wri
te)
    encStream.Write(plaintextBytes, 0,
plaintextBytes.Length)
    encStream.FlushFinalBlock()
    Return Convert.ToBase64String(ms.ToArray)
  End Function
```

Gambar 8. Kode enkripsi Class *Triple* DES

Kemudian *class* itu dipanggil pada *Form Encode* dengan *code* yang tertulis seperti pada Gambar 9.

```
Sub Encoding()
    Dim plaintext As String
    If RadioButton1.Checked Then
      plaintext = data
    Else
      plaintext = MsgHide.Text
    End If
    Dim password As String = KeyCrypt1.Text

    Dim wrapper As New TripleDES(password)
    Dim ciphertext As String =
wrapper.EncryptData(plaintext)
    eciphertex = ciphertext
  End Sub
```

Gambar 9. kode *Encode*

Sama seperti pada Gambar 10 kode algoritma dekrip dan Gambar 11, berikut *code* proses dekrip yang berada pada *class Triple* DES.

```
Public Function DecryptData(ByVal encryptedtext As
String) As String
    Dim encryptBytes() As Byte =
Convert.FromBase64String(encryptedtext)
    Dim ms As New System.IO.MemoryStream
    Dim decSteam As New CryptoStream(ms,
des.CreateDecrypton(),
System.Security.Cryptography.CryptoStreamMode.Writ
e)
    decSteam.Write(encryptBytes, 0,
encryptBytes.Length)
    decSteam.FlushFinalBlock()
    Return
System.Text.Encoding.ASCII.GetString(ms.ToArray)
  End Function
End Class
```

Gambar 10. Kode algoritma Dekrip

```
Sub Decoding()
    Dim cipertext As String = etripledesresult
    Dim password As String = KeyDecrypt1.Text
    Dim wripper As New TripleDES(password)
    Try
      Dim plaintext As String =
wripper.DecryptData(cipertext)
      dplaintext = plaintext
    Catch ex As Exception
      MsgBox("The data could not be decrypted with
key !", MsgBoxStyle.Information, "Information")
      DecodeProses.Value = 0
      PathOutFile.Clear()
      OutMsg.Clear()
      KeyDecrypt1.Clear()
      RadioButton2.Checked = True
      CheckBox1.Checked = False
      dtripledesresult = ""
    End Try
  End Sub
```

Gambar 11. Kode proses Dekrip

Saat menjalankan percobaan spesifikasi *personal computer* (PC) yang di pakai untuk evaluasi enkrisi dan dekripsi dalam penelitian yang dilaksanakan sesuai dengan yang terlihat pada Tabel 3.

Hasil percobaan dari penelitian ini seperti pada Tabel 4 hasil pengujian, yang di uji adalah ukuran *byte* file asli dan file yang sudah di sisipkan karakter pesan rahasia kemudian dibandingkan selisih ukuran gambarnya dalam satuan *byte* pada setiap percobaan.

Tabel. 3 Spesifikasi PC untuk percobaan

Spesifikasi PC	Keterangan
Processor	Intel(R) Core i5-2410M CPU 2.30GHz (4 CPUs), ~2.3GHz
Memory RAM	6144 MB
Available OS Memory	5984 MB
Hard Disk	500 GB
Sistem Operasi	Windows 7 Ultimate 64 – Bit SP 1

Tabel. 4 Hasil Pengujian

Jumlah karakter Pesan	Ukuran Gambar Asli (*byte*)	Ukuran dalam Stega (*byte*)	Selisih Ukuran Gambar (*byte*)
500	198822	200051	1229
1000	198822	201247	2425
2000	198822	203627	4805
5000	198822	210739	11917
10000	198822	222579	23757
15000	198822	234431	35609
25000	198822	258143	59321
50000	198822	317407	118585

Penilaian waktu menjadi bagian dari eksperimen ini, dimana waktu yang diamanti antara lain waktu yang diperlukan untuk proses enkrip dan dekrip dalam satuan detik. Hasil ekperimental ini dapat dilihat dalam Tabel 5.

Tabel. 5 Evaluasi waktu Enkrip dan Dekrip

Jumlah karakter Pesan	Ukuran dalam Stega (*byte*)	Waktu Enkrip (detik)	Waktu Dekrip (detik)
500	200051	01.52	02.10
1000	201247	01.67	03.79
2000	203627	01.92	07.40
5000	210739	02.03	16.32
10000	222579	02.12	35.77
15000	234431	02.29	50.34
25000	258143	02.42	01:26.91
50000	317407	02.82	03:13.06

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. Ketika semakin besar ukuran pesannya maka perlu banyak waktu yang digunakan untuk enkrip dan dekrip, tetapi waktu proses enkrip pada setiap ekperimen lebih cepat dari pada proses dekrip seperti yang terlihat jelas dalam Tabel 5.

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.

DAFTAR PUSTAKA

DARWIS, D., PRABOWO, R. & HOTIMAH, N., 2018. Kombinasi Gifshuffle, Enkripsi AES dan Kompresi Data Huffman untuk Meningkatkan Keamanan Data. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 5(4), pp.389–394.

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

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

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.

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.

PRABOWO, H.E. & AHMAD, T., 2018. Peningkatan Kualitas Citra Stego pada Adaptive Pixel Block Grouping Reduction Error Expansion

dengan Variasi Model Scanning pada Pembentukan Kelompok Piksel. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 5(2), pp.185–196.

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.

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.

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.

SHOJAE CHAEIKAR, S., ZAMANI, M., ABDUL MANAF, A.B. & ZEKI, A.M., 2018. PSW statistical LSB image steganalysis. *Multimedia Tools and Applications*, 77(1), pp.805–835.

WANG, S., SANG, J., SONG, X. & NIU, X., 2015. Least significant qubit (LSQb) information hiding algorithm for quantum image. *Measurement*, 73, pp.352–359.

ZEBUA, T. & NDRURU, E., 2017. Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 4(4), pp.275–282.