JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 2, April 2022, Page 1272-1281
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i2.3902

Implementasi Metode Kriptografi dengan Menggunakan Algoritma RC4 dan Steganografi Least Significant Bit Dalam Mengamankan Data Berbasis Android

Niki Ratama, Munawaroh*

Program Studi Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia
Email: [1]dosen00835@unpam.ac.id, [2,*]dosen00831@unpam.ac.id
Email Penulis Korespondensi: dosen00831@unpam.ac.id

Abstrak−Pengamanan adalah sebuah perlindungan atau melindungi sesuatu hal yang penting dari sesuatu hal yang tidak diinginkan atau hal lainnya dari hal yang bersifat pencurian teknik pengamanan data terdapat beberapa cara dalam memberikan sebuah perlindungan salah satunya adalah dengan menyisipkan sesuatu data yang ingin dilindungi kesebuah media lainnya, pengamanan pesan rahasia dengan cara menyisipkan sebuah pesan kedalam file gambar atau lebih dikenal sebagai steganografi adalah sebuah pengembangan dari sebuah kriptografi, dimana kriptografi sendiri adalah sebuah teknik pengamanan data yang mengandung unsur pengelolaan atau perumusan data sebelum menjadi data yang baru dan data baru tersebut hanya dapat dibaca atau dibuka oleh seseorang tertentu yang dapat mengelahui pola dari pengelolaan data tersebut. Keamanan dan keharasiaan sebuah pesan adalah hal yang sangat penting dan harus dijaga, pada permasalahan data kerahasiaan pada sebuah perusahaan atau lembaga menjadi persoalan utama dimana banyak sekali data yang menjadi kerahasiaan itu terbuka atau tersebar luas, hal ini sangat merugikan bagi perusahaan tersebut, 75% terkait data dapat dilihat dan terbaca seseorang yang tidak memiliki kepentingan, selain data kerahasiaan tersebut tersebar faktor lainnya adalah data kerahasiaan merupakan sebuah asett lanjuttan untuk perusahaan untuk melanjutkan kepada pengelola pada divisi lain yang memang harus dijaga dan digunakan kepada seseorang yang ditunjuk. dari permasalahan tersebut diperlukannya sebuah metode kriptografi dimana algoritma yang digunakan adalah RC4 dan steganografi yang digunakan menggunakan Least Significant Bit (LSB) sebagai metodenya. kelebihan dari RC4 adalah, data pada pengelolaan dalam membuat kriptografi lebih terstruktur dan memiliki pola yang tidak statis dimana didalamnya terdapat pembuatan data kerahasiaan dapat dibuat dengan cepat dan aman, sedangka metode Least Significant Bit (LSB) merupakan metode penyisipan data berupa binner kedalam sebuah citra yang memiliki citra warna dan didalamnya dapat menampung 6 bit untuk pesannya. Tujuan dari penelitian ini adalah membuat sistem aplikasi kriptografi yang mengkombinasikan teknik Least Significant Bit (LSB) untuk mengamankan sebuah data berbasis android dalam menghasilkan aplikasi yang dapat memberikan keamanan dalam data.

Kata Kunci: Kriptografi; Algoritma RC4; Algoritma Steganografi Least Significant Bit; Keamanan Data; Android

Abstract−Security is a protection or protecting something important from something unwanted or other things that are theft of data security techniques, there are several ways to provide protection, one of which is by inserting something data that you want to protect into other media, message security. secret by inserting a message into an image file or better known as steganography is a development of a cryptography, where cryptography itself is a data security technique that contains elements of data management or formulation before it becomes new data and the new data can only be read or opened. by a certain person who can know the pattern of managing the data. The security and confidentiality of a message is very important and must be maintained, the problem of data confidentiality in a company or institution is a major problem where a lot of data that is confidential is open or widespread, this is very detrimental to the company, in addition to data confidentiality The other factor is that data confidentiality is a continued asset for the company to continue to managers in other divisions which must be maintained and used by someone appointed. From these problems, a cryptographic method is needed where the algorithm used is RC4 and steganography is used using Least Significant Bit (LSB) as the method. The advantage of RC4 is that the data in the management of making cryptography is more structured and has a non-static pattern in which the creation of confidential data can be made quickly and safely, while the Least Significant Bit (LSB) method is a method of inserting binary data into an image that has a color image and in it can accommodate 6 bits for the message. The purpose of this research is to create a cryptographic application system that combines the Least Significant Bit (LSB) technique to secure an android-based data.

Keywords: Cryptography; RC4 Algorithm; Least Significant Bit Steganography Algorithm; Data Security; Android

1. PENDAHULUAN

Keamanan data adalah suatu hal yang sangat penting dan sangat menjadi sebuah kerahasiaan baik dari sebuah kelompok pribadi maupun sebuah kelompok yang memiliki organisasi seperti sebuah perusahaan atau lainnya, kerahasiaan menjadikan sebuah hal yang penting dimana bila data tersebut menjadi data yang bersifat harus disimpan kerahasiaan, dalam penyimpanan data biasanya seseorang menyimpan data melalui media lainnya baik itu media yang berbentuk fisik maupun berbentuk cloud storage, banyak beberapa faktor data yang disimpan hilang atau bahkan data tersebut diambil atau dilihat oleh seseorang yang tidak seharusnya melihat, dalam melakukan perlindungan data ada beberapa cara yang dapat dilakukan, baik itu menggunakan fasilitas dari beberapa tools seperti bawaan aplikasi tersebut atau menggunakan metode Kriptografi lainnya, seperti algoritma Rc4.

Pada penelitian sebelumnya terdapat pembahasan terkait penggunaan kritografi dalam mengamankan data salah satunya adalah diteliti oleh Soeb Aripin dan Muhammad Syahrizal dengan judul Pengaman File Video Menggunakan Algoritma Merkle Hellman Knapsack yang diterbitkan pada tahun 2020 [1], dimana pada penelitian ini membahas pengamanan sebuah file video menggunakan algoritma Merkle Hellman Knapsack, penggunaan algoritma dalam pemberian keamanan tersebut menggunakan logika xor dan panjang tabel yang digunakan dalam

Submitted: **09/03/2022**; Accepted: **25/04/2022**; Published: **25/04/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 2, April 2022, Page 1272-1281
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i2.3902

algoritma tersebut adalah 8 sampai 72 bit, dan terdapat juga penelitian yang membahas keamana yang diteliti oleh Kirman dengan judul Implementasi Algoritma Rc4 Untuk Proteksi File Mp3 pada tahun 2018 [2], pada peneliti kedua ini menggunakan algoritma Rc4 dimana kelebihan dari rC4 adalah memberikan byte informasi dari 1 sampai 256 byte dalam pengelolaan datanya, penggunaan kritografi menjadi salah satu dalam memberikan keamanan bagi sebuah data yang dianggap penting atau rahasia, kehilangan atau tercurinya data penting akan menjadikan dampak kerugian bagi pemilik datanya, baik itu data pribadi maupun data perusahaan, dari hal tersebut pemilihan penggunaan metode kritografi dipilih dalam penelitian ini [3].

Kriptografi adalah sebuah metode pengamanan data dimana didalamnnya terdapat beberapa cara atau aturan dalam melakukan keamanan data baik itu dalam mengelola rule atau aturan dan perhitungan didalamnya [4], dimana data yang dimasukkan akan diolah atau diubah menjadi beberapa sekumpulan bit dan di ubah penyusunan dalam membaca data tersebut, dan salah satu algoritma dalam melakukan teknik Kriptografi adalah algoritma Rc4, algoritma Rc4 adalah algoritma perlindungan data yang dimana memiliki mekanis yang sederhana yang dimana berbentuk stream chipper, bentuk tabel dari data yang digunakan algoritma Rc4 dalam menganalisa sebuah informasi tabel yaitu 1 sampai 256 byte dimana memiliki panjang tabel yaitu 256 byte per-data yang akan diolah sehingga keamanan data yang akan dijaga akan lebih terjaga dan aman, hasil dari pengamanan data menggunakan algoritma Rc4 ini akan menghasilkan enkripsi dimana data enkripsi akan diamankan kembali menggunakan algoritman LSB atau Steganografi Least Significant Bit, istilah LSB lebih dikenal dengan mengamankan data ke media citra atau gambar, penggunaan algoritma LSB dalam melakukan pengamanan enkripsi adalah pada LSB dapat menampung sebuah informasi dan tidak mengubah isi dari informasi didalamnya baik ukuran ataupun informasinya dengan hal tersebut akan memberikan keamanan tanpa menimbulkan kecurigaan, dengan memberikan sebuah teknik kriptografi dan steganografi pada data yang akan disimpan atau diamankan ini dimana data tersebut adalah data rahasia memberikan solusi dari keamana data untuk sebuah perlindungan sebuah data, teknik ini akan diimplementasikan dalam bentuk aplikasi berbasis android dimana aplikasi android adalah sebuah aplikasi smartphone dimana sebuah orang sudah memiliki hal tersebut dan akan menjadi kemudaan untuk pengguna dalam melakukan pengamanan data baik itu enkripsi atau deksipsi [5].

Metode penelitian yang digunakan dalam penelitian ini menggunakan metode studi pustaka dimana mengamati beberapa penelitian sebelumnya serta tanggapan untuk tahapan selanjutnya dan mengamati menggunakan observasi, baik perlindungan data yang dilakukan secara langsung dimana metode kritografi yang digunakan menggunakan metode *Rivers Code 4*, dalam melakukan atau tahapan dalam membuat kunci awal sebuah proses *encode* dan *Least Significant Bit* yang dimana melakukan sebuah perlindungan dari file menjadi sebuah citra atau gambar, dan dijelaskan digambar bagaimana proses enkripsi diproses, dimana dijelaskan bagaimana cara mengambil data asli yang berada didalam gambar dengan *dekripsi*. Pada proses encode dibutuhkan tiga input sebagai kunci utama atau kunci rahasianya, file rahasia dan file gambar, data yang akan disimpan kedalam gambar yaitu *.docx, *.txt, *.xlcx, dan *.pdf. selanjutnya file ini akan dimasukkan kedalam file gambar, dan tahapan selanjutnya adalah memsukkan kunci keamana untuk proses encode yang akan mengeksripsikan dile menggunakan metode Rivest ode 4 atau Rc4 [6] [7].

Tujuan dari penelitian ini adalah membuat sebuah aplikasi Kriptografi dimana mengimplementasikan algoritma Rc4 untuk kriptografi dan algoritman Least Significant Bit untuk steganografi, untuk keamanan data yang dianggap penting dan rahasia, dimana data tersebut akan dikemas kedalam sebuah media citra tanpa mengurangi informasi didalamnya dan tanpa memberikan kecurigaan terhadap bentuk dan jenis media yang dihasilkan nantinya.

2. METODOLOGI PENELITIAN

2.1 Metode Pengambilan Data

Metode pengambilan data adalah tahapan dimana pencarian data yang dilakukan berdasarkan pengamatan permasalahan yang didapat, diantaranya :

a. Observasi : Pengamatan langsung yangdilakukan peneliti pada lokasi dan kondisi dilapangan, dimana mengamati setiap langkah dari pemberkasan dan penyimpanan yang dilakukan pada sebuah data pada umumnya.
b. Wawancara : Tahapan dimana mencari data berdasarkan sumber pernyataan seseorang dalam menghadapi permasalahan dalam pengamanan dari sebuah data, dimana keamanan sangatlah dibutuhkan demi melindungi sebuah kerahasiaan.
c. Studi Pustaka : Sebuah tahap dimana mencari referensi yang diambil berdasarkan penelitian dan referensi lainnya dari sumber terdahulu, baik beruapa jurnal, ataupun buku dimana membahas topik dan permasalahan yang sama.

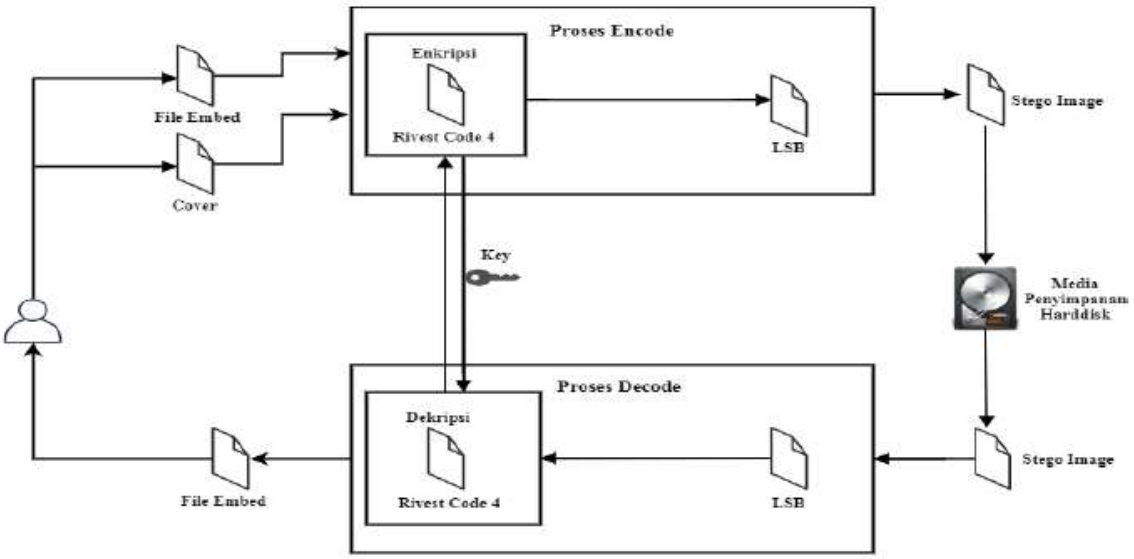
2.2 Metode Rivest Code 4

Metode Rivest Code 4 atau Rc4 adalah sebuah metode kritografi yang menggunakan dua buah Substitution Box (S-Box) yaitu array sepanjang 256 yang berisi permutasi dari bilangan 0 sampai 255, dan S-Box kedua, yang berisi permutasi merupakan fungsi dari kunci dengan panjang variabel, keamana menggunakan metode ini memberikan

Submitted: **09/03/2022**; Accepted: **25/04/2022**; Published: **25/04/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 2, April 2022, Page 1272-1281
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i2.3902

perlindungan yang baik dikarenakan terdapat beberapa bit yang akan diatur dengan bilangan 0 sampaii 255, dan pada penelitian ini dimana pengemasan data yang akan disimpan dimasukkan kedalam sebuah gambar/cover dan dapat dilihat berdasarkan gambar 1 dibawah ini [8].



Gambar 1. Arsitektur Sistem

Pada algoritma Rc4 menjadi bentuk algoritma simetris, dimana kuncinya menggunakan kunci yang sama pada saat proses enkripsi, dan terdapat dua bagian dalam algoritma simetris ini, yaitu:

a. *Stream Cipher* (Cipher Aliran) : Dimana terjadinya proses enkripsi dan dekripsi yang dilakukan menggunakan aturan tahapan bit per bit dalam aliran dalam prosesnya.
b. Block Cipher (Cipher Blok) : Diimana enksipsi dan dekripsinya dilakukan terhadap data yang akan diproses dan dipisah menjadi beberapa bagian atau blok, dimana blok tersebut akan terbentuk beberapa bagian blok dan proses enkripsi – deskripsi akan dilakukan berdasarkan bagian blok yang terpisah tersebut atau masing – masing blok.

Algoritma Rc4 ini menggunakan model Stream Cipher, dimana enkripsi yang dilakukan menggunakan kombinasi plainteks dengan menggunakan bit-wise-Xor (*Exclusive-or*) [9].

2.3 Steganografi

Steganografi adalah sebuah istilah dimana seseorang melakukan penyisipan data kedalam sebuah cover baik itu berupa gambar atau menyamarkannya kedalam sebuah citra image, dalam penggunaan ini dapat menampung informasi tanpa mengurangi informasi didalamnya sehingga dapat memberikan ketidak curigaan terkait data didalamnya [10], perbedaan Steganografi dengan Kriptografi terdapat pada cara proses dari teknik ters[3]ebut melakukan penyembunyian data, dimana dapat menghasilkan bentuk yang berbeda dalam pengemasannya. Dimana Kriptografi memproses data asli dengan mengubah data tersebut atau mengacaknya dari data asli ke data yang tidak dapat dibaca oleh sembarang penelihatan, bahkan bentuknya ter-enkripsi yang sangat berbeda dengan data aslinya, selanjutnya pesan juga dapat berupa plaintext, chipertext, citra, atau apapun yang dapat ditempelkan ke dalam bit-stream [11].

Dalam Steganografi terdapat dua proses utama, yaitu proses penyisipan (embedding/encoding) dan proses penguraian (extraction/decoding), dimana dapat diberikan kaitan juga dengan beberapa istilah dibawah ini [12] :

a. *Hidden Text* atau *embedded message* : dimana istilah ini dimaksud dengan pemahaman penghilang sebuah pesan atau pesan yang disembunyikan.
b. *Cover Text* atau *Cover-Object* : Dimana istilah ini dimaksud dengan sebuah pesan yang disembunyikan kedalam sebuah citra atau juga istilah lainnya adalah *embedded Message*.
c. Stego Text ataau Stego-Object : Dimana istilah ini memberikan arti sebuah pesan yang sudah ber-isi embedded Message.

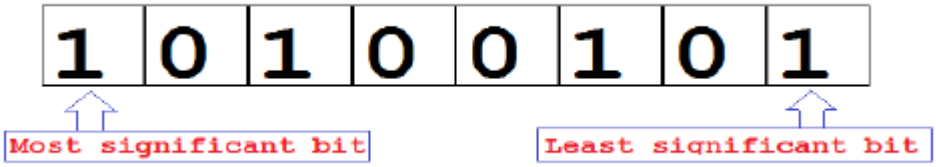
2.3.1 Steganografi LSB

Least sicnificant bit (LSB) merupakan sebuah algoritma dari metode kriptografi yang sering digunakan dalam melakukan penyembunyaan suatu data atau informasi, dimana langkah dari sebuah proses ini mengberikan suatu penyembunyian sebuah informasi kedalam seuatu media, seperti citra atau sebuah gambar, dasar dari algoritma ini menggunakan sebuah bilangan biner dimana bilangannya terdiri dari dua angka, 0 dan 1, pada teknik ini kita

Submitted: **09/03/2022**; Accepted: **25/04/2022**; Published: **25/04/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 2, April 2022, Page 1272-1281
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i2.3902

mengganti bit pada posisi LSB pada data dengan bit dimana data yang akan disembunyikan, dan bit yang diganti adalah bit yang terakhir, sehingga walau data tersebut sudah diubah kita dapat mengenalinya [13].



Gambar 2. LSB dan MSB

Pada bit LSB sangat cocok untuk diganti, dan dimana perubahannya hanya akan mengganti nilai byte satu lebih tinggi atau juga nilai yang lebih rendah dari nilai sebelumnya

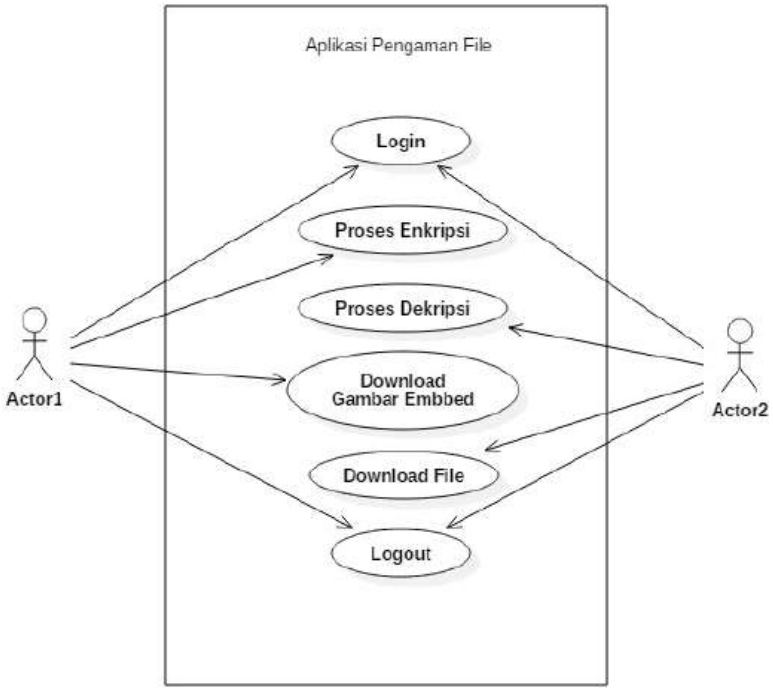
Tahapan didalam melakukan penelitian, bagaimana tahapan penerapan metode dalam penelitian serta pengujian metode dalam mendapatkan hasil penelitian sesuai dengan harapan dan gambaran penelitian. Lebih baik jika terdapat gambar dan tabel, itu harus disajikan dengan nama tabel dan gambar yang disertai dengan nomor urut.

Peak Signal-to-Noise Ratio (PSNR) merupakan rumus untuk mengukur nilai perbandingan antara nilai maksimum gambar dengan nilai Mean Squared Error (MSE). Pada umumnya rumus dari melihat nilai kecil dari MSE maka semakin sedikit juga nilai perubahannya yang akan dihasilkan, Rumus Peak *Signal-to-Noise Ratio* (PSNR).

$$PSNR = 20\text{x}log_{10}\left(\frac{265}{rms}\right) dengan\ rms = \sqrt{\frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I_{ij} - \hat{I}_{ij}\right)^2} \quad (1)$$

2.4 Usecase Diagram

Pada perancangan sistem dilakukan sebuah analisa dimana pada tahap awal adalah menentukan penggunaan user dari aplikasi yang akan dibuat, usecase diagram merupakan sebuah diagram yang memberikan pemahaman terkait penggunaan sistem dengan aktor, dimana aktor nantinya adalah mempunyai hak terkait sistem yang akan diolahnya berdasarkan fungsi – fungsi didalamnya [14]. Berikut adalah usecase diagram dari aplikasi yang akan dibuat :



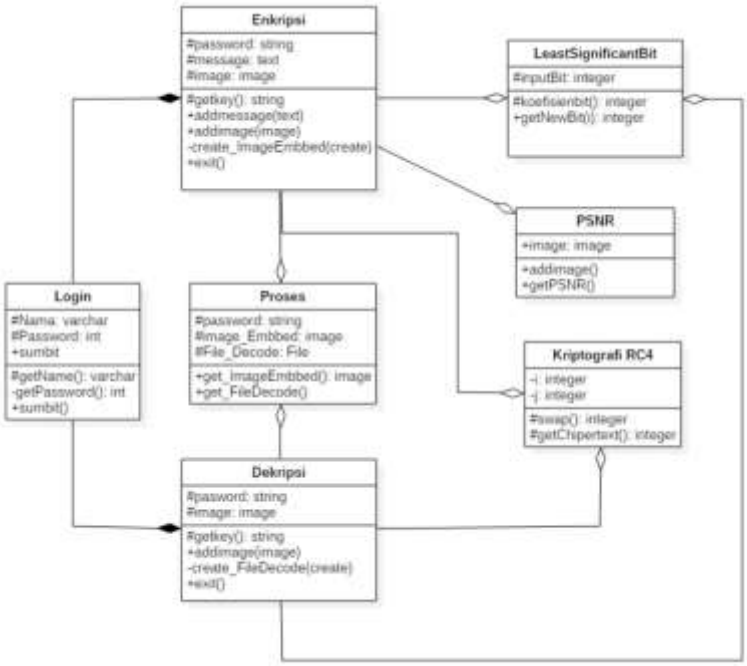
Gambar 3. Usecase Diagram

2.5 Class Diagram

Pada tahapan pembuatan class diagram, mengindentifikasi pengelompokkan terkait tabel didalam database untuk memberikan kemudahan dalam melakukan penyimpanan arsip atau informasi berdasarkan data yang sudah di enkripsi, dimana tabel class diagram dapat dilihat pada tabel 5 berikut ini [15].

Submitted: **09/03/2022**; Accepted: **25/04/2022**; Published: **25/04/2022**

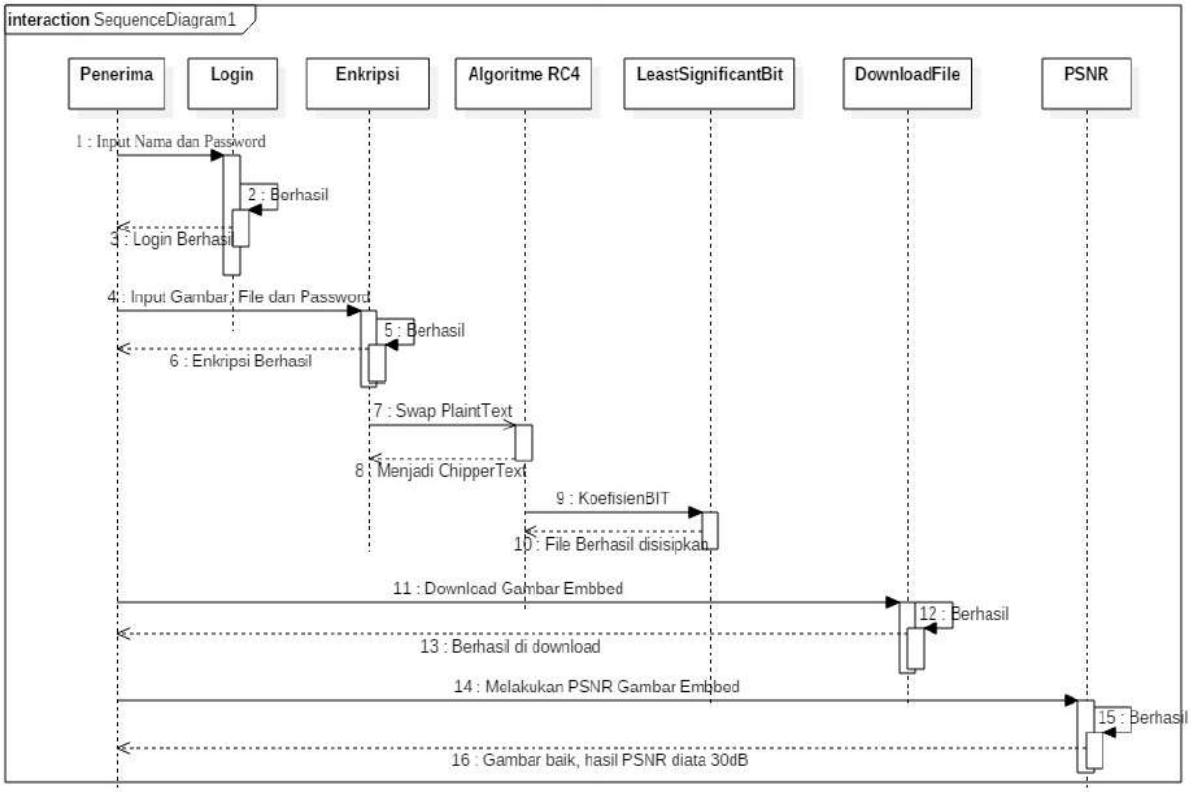
JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 2, April 2022, Page 1272-1281
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i2.3902



Gambar 4. Class Diagram

2.6 Squence Diagram

Squence diagram adalah sebuah diagram yang menggambarkan pemodelan logika dan fungsi dari sebuah program yang dirancang, pada tahapan ini dibuat sebuah squence diagram dalam menjelaskan fungsi dari aplikasi tersebut dimana terdapat dua penggambaran diagram, squence diagram Enkripsi untuk memanipulasi data dan squence diagram Dekripsi untuk mengembalikan data yang sudah di manipulasi. Gambar 5 adalah diagram squence untuk enksipsi data [16].

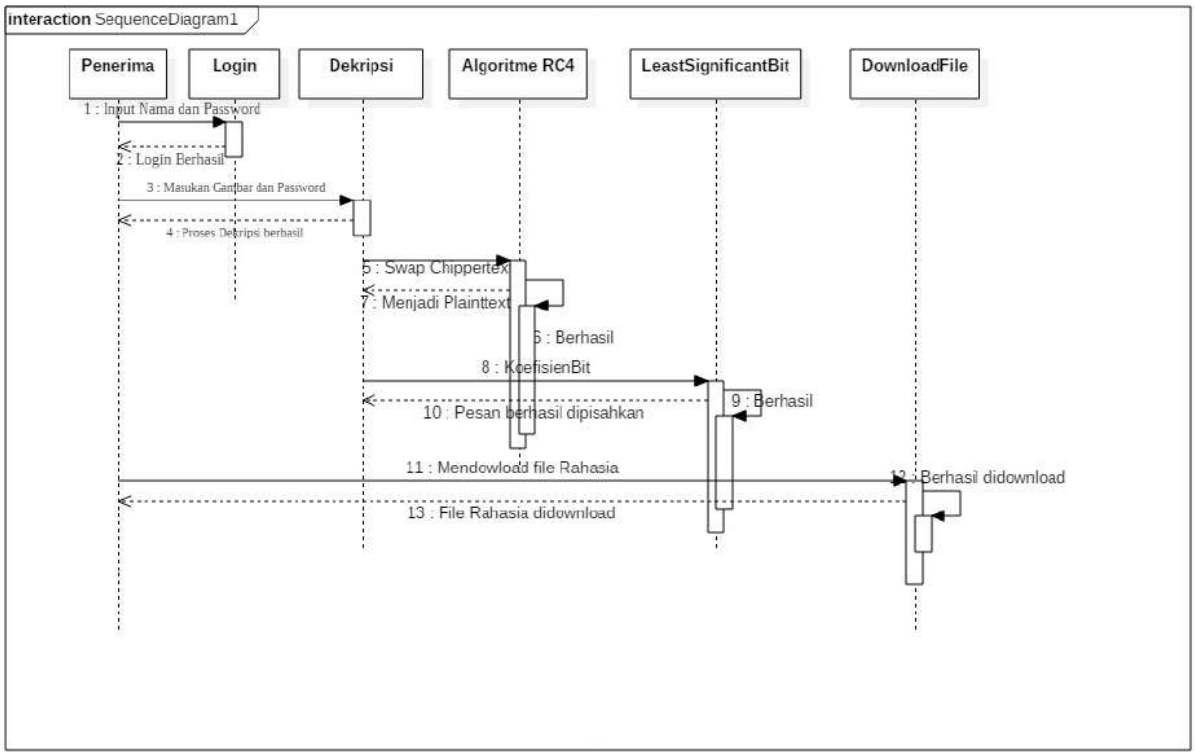


Gambar 5. Squence Enkripsi

Gambar 6 adalah diagram squence dekripsi data.

Submitted: **09/03/2022**; Accepted: **25/04/2022**; Published: **25/04/2022**

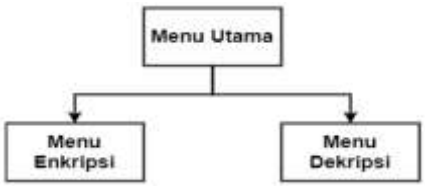
JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 2, April 2022, Page 1272-1281
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i2.3902



Gambar 6. Squence Dekripsi

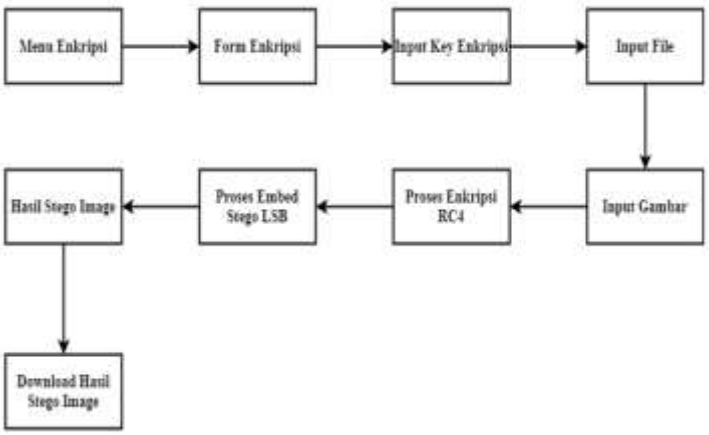
2.7 Rancangan Tampilan

Rancangan tampilan adalah tahapan dimana merancang atau mendesain tampilan user interface dari aplikasi yang akan dibuat, pada tahapan ini dilakukan sebuah analisa berdasarkan implementasi algoritma yang akan diimplementasikan kedalam sebuah aplikasi [17]. Tahapan pertama adalah merancang menu utama aplikasi, dapat dilihat berdasarkan gambar 8 dibawah ini.



Gambar 7. Rancangan Menu Utama

Tahapan kedua dari merancang tampilan adalah merancang tampilan enkripsi dari tampilan aplikasi dimana akan menjelaskan proses dari tahapan aplikasi melakukan enkripsi, dapat dilihat pada gambar 9 sebagai berikut.

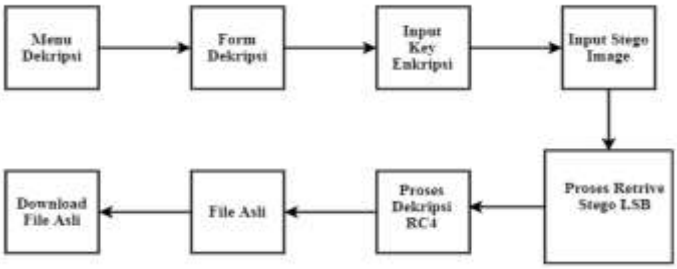


Gambar 8. Menu Enkripsi

Tahapan ketiga adalah merancang tampilan Dekripsi, dimana menjelaskan proses tahapan dari melakukan dekripsi, dan dapat dilihat pada gambar 10 sebagai berikut.

Submitted: **09/03/2022**; Accepted: **25/04/2022**; Published: **25/04/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 2, April 2022, Page 1272-1281
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i2.3902



Gambar 9. Menu Dekripsi

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Algoritma Rc4

Algoritme RC4 mengenkripsi dengan plainteks dengan menggunakan bit-wise Xor (Exclusive-or). RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte. Untuk menghasilkan keystream, cipher menggunakan state internal yang meliputi dua bagian.

a. Tahap key scheduling dimana state automaton diberi nilai awal berdasar kan kunci enkripsi, Berikut adalah algoritme KSA dalam bentuk pseudo-code dimana key adalah kunci enkripsi dan keylength adalah besar kunci enkripsi dalam bytes (untuk kunci 128 bit, keylength = 16). Algoritme 1. KSA
b. Tahap pseudo-random generation di mana state automaton beroperasi dan outputnya menghasilkan keystream. Setiap putaran, bagian keystream sebesar 1 byte (dengan nilai antara 0 sampai dengan 255) dioutput oleh PRGA berdasarkan state S. Berikut adalah algoritme PRGA dalam bentuk pseudo – Code :

Berikut adalah implementasi algoritme RC4 dengan mode 4 byte untuk lebih menyederhanakan dalam perhitungan manual. S-Box dengan panjang 4 byte, dengan S[0]=1, S[1]=2, S[2]=3 dan S[3]= 0 sehingga array S menjadi : 1 2 3 0

Inisialisasi 4 byte kunci array K. Misalkan kunci adalah 1 7 1 7, sehingga array K berisi 1 7 1 7 dan mencoba untuk mengenkripsikan kaya KAMU. Inisialisasi I dan J dengan 0 kemudian dilakukan KSA agar tercipta state – array yang acak. Penjelasan tentang iterasi dapat dilihat sebagai berikut :

1) Iterasi pertama :
   I = 0 ; J=0;
   J = (j + S[0] + K[0]) mod 4;
   J = (0 + 1 + 1) mod 4
   J = 2 mod 4
   J = 2
   Swap (S[0] , J[2])
   Hasil array = 3 2 1 0
2) Iterasi kedua :
   I = 1 ; J = 2;
   J = (j + S[1] + K[1]) mod 4;
   J = (2 + 2 + 7) mod 4;
   J = 3;
   Swap (S[1], J[3])
   Hasil array = 3 0 2 1
3) Iterasi ketiga :
   I = 2; J = 3;
   J = (j + S[2] + K[2]) mod 4;
   J = (3 + 2 + 1) mod 4;
   J = 2;
   Swap (S[2] ,J[2];
   Hasil array = 3 0 2 1
4) Iterasi keempat :
   I = 3; J = 2;
   J = (j + S[3] + K[3]) mod 4;
   J = (2 + 0 + 7) mod 4;
   J = 1
   Swap (S[3], J[1])
   Hasil array = 1 0 2 3

Setelah hasil array S di dapatkan dari iterasi keempat, maka proses selanjutnya adalah mengXOR-kan pseudo random byte dengan plaintext, misalnya plaintext yang dimasukkan adalah “KAMU”. Karena plaintext terdiri dari lima karakter maka terjadi empat iterasi.

Iterasi pertama yaitu :
Inisialisasi I dan J dengan I=0; dan J=0;

1) Iterasi pertama :
   I = (I + 1) mod 4;
   I = 0 + 1 mod 4
   I = 1
   J = (0 + S[i]) mod 4
   J = (0 + S[1]) mod 4
   J = 1
   Swap (S[i] S[j]) -> S[1], S[1]
   Array awal 1 0 2 3
   Hasil setelah swap = 1 0 2 3
   T = (S[1] + S[1]) mod 4
   T = 1 + 1 mod 4
   T = 2
   K = 00000010
2) Iterasi kedua :
   I = 1; J= 1
   I = 1 + 1 mod 4;
   I = 2;
   J = 1 + S[2] mod 4
   J = 1 + 2 mod 4
   J = 3
   Swap S[i], S[j] - > S[2], S[3]
   Array awal = 1 0 2 3

Submitted: 09/03/2022; Accepted: 25/04/2022; Published: 25/04/2022

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 2, April 2022, Page 1272-1281
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i2.3902

Hasil setelah swap = 1 0 3 2
T = (S[2] + S[3]) mod 4
T = 1
K = 00000001

3) Iterasi ketiga
I = 2 ; J = 3;
I = 2 + 3 mod 4
I = 1
J = 3 + S[1]
J = 3 + 1 mod 4
J = 0
Swap S[i] S[j] -> S[1] , S[0]
Array awal = 1 0 3 2
Hasil setelah swap = 0 1 3 2
T = S[1] + S[0] mod 4
T = 1 + 0 mod 4
T = 1
K = 00000001

4) Iterasi keempat
I = 1 ; J = 0;
I = 1 + 0 mod 4
I = 1
J = 0 + S[i] mod 4
J = 0 + 1 mod 4
J = 1
Swap S[i], S[j] -> S[1] S[1]
Array awal = 0 1 3 2
Hasil setelah swap = 0 1 3 2
T = S[i] + S[j] mod 4
T = 1 + 1 mod 4
T = 2
K = 00000011

Setelah menemukan kunci untuk tiap karakter, maka dilakukan operasi XOR antara karakter pada plaintext dengan kunci yang dihasilkan. Berikut adalah tabel ASCII untuk tiap-tiap karakter pada plaintext yang digunakan

Tabel 1. Plaintext

Huruf Code ASCII	Binary 8 Bit
K	01001011
A	01000001
M	01001101
U	01010101

Berikut adalah proses pengXOR-an dari Plaintext dengan key yang telah di dapat :

Tabel 2. Contoh Enkripsi

KAMU	01001011	01000001	01001101	01010101
Key	00000010	00000001	00000001	00000011
Chippertext	01001001	01000000	01001100	01010100
	I	@	L	T

Sedangkan proses dekripsi adalah kebalikan dari proses enkripsi, yaitu mengubah chipertext menjadi plaintext kembali, untuk lebih jelas dapat dilihat pada tabel dibawah ini:

Tabel 3. Contoh Dekripsi

I @ L T	01001001	01000000	01001100	01010100
Key	00000010	00000001	00000001	00000011
Chippertext	01001011	01000001	01001101	01010101
	K	A	M	U

3.2 Implementasi Algoritma Least sicnificant bit (LSB)

Seperti kita ketahui untuk file bitmap 24 bit maka setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian pada setiap pixel file bitmap 24 bit kita dapat menyisipkan 3 bit data. Contohnya huruf A dapat kita sisipkan dalam 3 pixel, misalnya data raster original adalah sebagai berikut:

Tabel 4. Contoh Biner Gambar

00100111	11101001	11001000
00100111	11001000	11101001
11001000	00100111	11101001

Sedangkan representasi biner huruf A adalah 10000011. Dengan menyisipkan-nya pada data pixel diatas maka akan dihasilkan.

Tabel 5. Contoh Dengan Huruf A

00100111	11101000	11001000
00100110	11001000	11101000

Submitted: **09/03/2022**; Accepted: **25/04/2022**; Published: **25/04/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 2, April 2022, Page 1272-1281
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i2.3902

11001000 00100111 11101001

Terlihat hanya empat bit rendah yang berubah, untuk mata manusia maka tidak akan tampak perubahannya. Secara rata-rata dengan metode ini hanya setengah dari data bit rendah yang berubah, sehingga bila dibutuhkan dapat digunakan bit rendah kedua bahkan ketiga.

3.3 Tampilan Aplikasi

Rancangan layar menggunakan aplikasi studio dalam desain aplikasinya, dapat dilihat berdasarkan gambar berikut ini. Selanjutnya berikut adalah halaman untuk melakukan Enkripsi, dimana klik Enkripsi maka akan menampilkan textfield untuk memasukkan kunci, dan selanjutnya memasukkan file yang ingin di enkripsi dan memasukkan gambar untuk melakukan Steganografi, selanjutnya klik submit.

Gambar 10. Tampilan Enkripsi

Setelah klik submit maka akan menampilkan gambar berikut ini :

Gambar 11. Tampilan Berhasil Enkripsi

Selanjutnya Klik download untuk mengambil gambar yang didalamnya sudah dimasukkan file enkripsi kita, untuk melakukan dekripsi maka dapat melakukan dengan memasukkan kunci dan memasukkan gambar yang sudah didownload pada halaman berhasil saat melakukan enkkripsi.

Gambar 12. Tampilan Dekripsi

Setelah dimasukkan kunci dan file gambar, dan klik submit maka akan menampilkan halaman berhasil sebagai berikut.

Gambar 13. Tampilan Berhasil Dekripsi

Submitted: **09/03/2022**; Accepted: **25/04/2022**; Published: **25/04/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 2, April 2022, Page 1272-1281
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i2.3902

Bila menampilkan halaman berhasil dekripsi maka ada menu download untuk mendownload file yang sudah dikembalikan dalam bentuk awal.

4. KESIMPULAN

Berdasarkan permasalahan yang sudah dijelaskan pada pembahasan masalah maka dapat disimpulkan dengan implementasi metode kriptografi ini dengan menggunakan algoritma Rc4 dan Steganografi Least Significant Bit dapat memberikan, aplikasi Steganografi dan Kriptografi dengan Algoritma Kriptogradi RC4 dan Least Significant BIT dapat memberikan keamana pada file dengan pengamanan yang baik dimana teknik Steganografi dapat memberikan ketidak curigaan terhadap data yang dirahasiakan, dan data yang diamankan aman dikarenakan Steganografi tidak mengubah informasi didalamnya. File yang diamankan harus berupa *.pdf, *.xls, *.docx dan *.txt dan gambar yang digunakan untuk melakukan Steganografi harus menggunakan gambar dengan maksimal 24bit, agar terhindar gagal dalam melakukan enkripsi steganografi tersebut.

REFERENCES

[1] S. Aripin and M. Syahrizal, "Pengaman File Video Menggunakan Algoritma Merkle Hellman Knapsack," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 461, 2020, doi: 10.30865/mib.v4i2.2039.
[2] K. Kirman, "Implementasi Algoritma Rc4 Untuk Proteksi File Mp3," *Pseudocode*, vol. 5, no. 1, pp. 80–86, 2018, doi: 10.33369/pseudocode.5.1.80-86.
[3] R. Nuari and N. Ratama, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 2, pp. 2716–1501, 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/JOAIIA.
[4] M. B. S. Junianto, H. Ardiansyah, and ..., "Analisa Dan Perancangan Sistem Informasi Pengaman Dokumen Dengan Metode Algoritma XOR dan AES Berbasis Web (Studi Kasus: Bimbingan Belajar Matriks Pamulang)," *JOAIIA J. ...*, vol. 1, no. 2, pp. 61–66, 2020.
[5] N. Ratama, M. Kom, M. Kom, and K. Kecerdasan, *Konsep Kecerdasan Buatan Dengan Pemahaman Logika Fuzzy Dan Penerapan Aplikasi*. Penerbit Uwais Inspirasi Indonesia, CV.
[6] KPM, R. A. Ramadhani, and e D. LiceFrense, "K-Nears Neigbours Risa Helilintar , Risky Aswi Ramadhani Siti Rochana," *Python "Belajar Pemrograman Python Dasar,"* vol. 84, no. December, pp. 487–492, 2013, [Online]. Available: http://www.ask-jansen.com/wp-content/uploads/2014/04/Kontroversi-Kalori-ebook.pdf%0Ahttp://ir.obihiro.ac.jp/dspace/handle/10322/3933.
[7] M. Fauzan, E. Purnomo, W. A. Priyono, S. N. Sari, and A. Wulandari, "Sekuritas Jaringan Komunikasi Voice over Internet Protocol (VoIP)," vol. 6, no. 2, pp. 183–188, 2012.
[8] I. P. A. Dharmaadi, A. M. Barmawi, G. B. S, F. Informatika, and I. T. Telkom, "Enkripsi Gambar Parsial dengan Kombinasi Metode Stream Cipher RC4 dan Chaotic Function," pp. 1–8.
[9] E. S. Astuti, B. Prihadmantyo, and M. E. Apriyani, "Implementasi Algoritma Kriptografi Rc4 Dan Metode Steganografi Audio 2Lsb Pada Sistem Keamanan Informasi," *J. Teknol. Inf. dan Terap.*, vol. 4, no. 2, pp. 67–74, 2019, doi: 10.25047/jtit.v4i2.61.
[10] R. Mulyono and E. Z. Astuti, "Pengamanan Pesan Text Menggunakan Metode Steganografi Least Significant Bit dengan Media Digital Gambar," *Skripsi, Univ. Dian Nuswantoro*, 2015.
[11] K. Dedi Darwis, "Teknik Steganografi Untuk Penyembunyian Pesan Teks Menggunakan Algoritma End Of File," 2017.
[12] N. Anwar, "Perancangan Steganografi Hidden Message Dengan Metode Least Significant Bit Insertion (Lsb) Berbasis Matlab," *J. Algoritm. Log. dan Komputasi*, vol. 1, no. 1, pp. 25–30, 2018, doi: 10.30813/j-alu.v1i1.1107.
[13] D. Rahardika and N. Ratama, "Implementasi Network Automation Untuk Konfigurasi Jaringan Baru Dengan Netmiko," vol. 2, no. 3, pp. 190–200, 2021.
[14] Munawaroh and N. Ratama, "Penerapan Teknologi Augmented Reality Pada Matakuliah Pengantar Teknologi Informasi Di Universitas Pamulang Berbasis Android," *Satin*, vol. 5, no. 2, pp. 17–24, 2019.
[15] D. Nurpala and Munawaroh, "Perancangan Sistem Aplikasi Bank Soal pada Ujian Online Berbasis WEB (Studi Kasus : SMA NEGERI 1 CIBEBER)," *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 2, pp. 51–55, 2020.
[16] K. Li, R. G. Dewar, and R. J. Pooley, "Object-oriented analysis using natural language processing," *Linguist. Anal.*, 2005.
[17] N. Ratama, "Implementasi Metode Fuzzy Tsukamoto Untuk Deteksi Dini Autisme Pada Balita Berbasis Android," Vol. 3, No. 2, Pp. 129–139, 2020, [Online]. Available: Https://E-Journal.Stmiklombok.Ac.Id/Index.Php/Jire/Article/View/269.

Submitted: **09/03/2022**; Accepted: **25/04/2022**; Published: **25/04/2022**