IMPLEMENTASI KRIPTOGRAFI ALGORITMA *RIJNDAEL* DAN STEGANOGRAFI METODE *LEASTSIGNIFICANTBIT* UNTUK KEAMANAN DATA (STUDI KASUS : PT CITCALL TEKNOLOGI INDONESIA)

BosarPanjaitan, S.Si.,M.Kom, Muhammad Chairul
Jurusan Teknik Informatika
Fakultas Teknik Universitas Satya Negara Indonesia
Email: bosarpjtn@gmail.com, muhammad_chairul@outlook.com

Abstrak

Teknologi dan informasi saat ini berkembang semakin pesat.Proses pertukaran data dan informasi dapat dilakukan dengan sangat mudah melalui berbagai macam media. Tentunya keamanan dalam pertukaran data dan informasi sangat diperlukan demi menjaga kerahasian data tersebut. Dari permasalahan diatas didapat sebuah solusi dengan membuat sebuah aplikasi yang dapat menjaga kerahasiaan dari informasi ataupun data pada PT. Citcall Teknologi Indonesia. Salah satu cara untuk menyembunyikan data tersebut dengan menggunakan teknik kriptografi dan steganografi. Teknik kriptografi yang digunakan adalah kriptografi algoritma *Rijndael* dengan melakukan enkripsi menjadi chiperteks, sehingga tidak dapat dibaca lagi. Untuk membacanya lagi perlu dilakukan proses dekripsi. Selain itu dilakukan pengamanan ganda dengan menggunakan teknik steganografi *Least Significant Bit*(LSB).Aplikasi ini menggunakan metode algoritma kriptografi *Rijndael* dengan kombinasi steganografi LSB (*Least Significant Bit*) sehingga sangat optimal untuk mengamankan data. Dengan adanya Aplikasi ini diharapkan dapat mengamankan dan menjaga kerahasiaan data pada PT. Citcall Teknologi Indonesia sehingga dapat mencegah terjadinya pencurian dan manipulasi data.

Keywords: Algoritma, Kriptografi, *Rijndael*, Steganografi, *LeastSignificantBit*

Abstract

Technology and information are currently growing more rapidly.The process of exchanging data and information can be done very easily through a variety of media. Of course security in the exchange of data and information is needed to maintain the confidentiality of the data. From the above problems obtained a solution by making an application that can maintain the confidentiality of information or data at PT. Citcall Technology Indonesia. One way to hide the data is by using cryptographic and steganographic techniques. The cryptographic technique used is cryptographic Rijndael algorithm by encrypting it into ciphertext, so it cannot be read anymore. To read it again it is necessary to do the decryption process. In addition, double security is done using Least Significant Bit (LSB) steganography techniques. This application uses the Rijndael cryptographic algorithm method with a combination of LSB (Least Significant Bit) steganography so that it is very optimal for securing data. With this application it is expected to secure and maintain the confidentiality of data at PT. Citcall Technology Indonesia so that it can prevent theft and data manipulation.

Keywords:*Algorithms, Cryptography, Rijndael, Steganography, Least Significant Bit*

PENDAHULUAN

Latar Belakang

Teknologi dan informasi saat ini berkembang semakin pesat proses pertukaran data dan informasi dapat dilakukan dengan sangat mudah melalui berbagai macam media. Tentunya kemanan dalam pertukaran data dan informasi sangat diperlukan demi menjaga kerahasiaan data tersebut. Bahkan masih ada saja pihak yang kurang sadar untuk menjaga kerahasiaan datanya, salah satu dampak negatif dalam perkembangan teknologi adalah adanya pencurian data. Bila hal itu sampai terjadi maka kemungkinan akan terjadi pemalsuan data, penyalahgunaan, penyadapan dan lain sebagainya.

PT. Citcall Teknologi Indonesia merupakan perusahaan yang bergerak di bidang penyedia jasa komunikasi berbasis cloud seperti *MiscallOTP*, dan *SMS*. Dokumen transaksi serta pendapatan perusahaan harus terjaga kerahasiaannya dari pihak yang tidak berhak mengaksesnya. Tetapi selama ini sistem PT. Citcall Teknologi Indonesia hanya menyimpan data, tanpa adanya keamanan untuk menjaga kerahasiaan data atau file yang telah disimpan oleh PT. Citcall Teknologi Indonesia. Hal ini dapat menyebabkan terjadinya resiko dari pencurian data serta penyalahgunaan data tersebut. Dengan demikian sistem keamanan terhadap data atau *file* sangat diperlukan untuk menghindari tindakan-tindakan tersebut yang dapat merugikan.

Berdasarkan uraian diatas maka dalam penelitian tugas akhir ini penulis memilih kriptografi algoritma *Rijndael* dikombinasikan dengan steganografi dengan metode *LeastSignificantBit* dikarenakan teknik menyembunyikan atau menyisipkan file rahasia pada suatu media penampung, penyandian pada algoritma *Rijndael* ini memiliki mekanisme mengacak informasi dan menggunakan operasi XOR serta transformasi linier, sehingga sangat optimal untuk mengamankan data.

Rumusan Masalah

1. Bagaimana mengamankan data rahasia perusahaan dengan cara mengenkripsi dokumen/*file* dengan algoritma *Rijndael* kemudian menyisipkan dokumen/*file* tersebut kedalam sebuah gambar dengan menggunakan metode steganografi *LeastSignificantBit* (LSB) ?
2. Bagaimana mengimplementasikan kriptografi menggunakan algoritma *Rijndael* dengan steganografi menggunakan metode *LeastSignificantBit* (LSB) pada dokumen/*file* di PT Citcall Teknologi Indonesia ?

Batasan Masalah

1. Penelitian ini hanya membahas kriptografi algoritma *Rijndael* dan steganografi *LeastSignificantBit*(LSB).
2. *File* gambar yang digunakan sebagai penampung berformat *.jpg dan *.png.
3. *File* yang akan disisipkan pada aplikasi steganografi ini berekstensi .pdf.
4. *File* dokumen tidak lebih dari 1 Mb dan file gambar tidak lebih dari 1,5 MB.
5. Bahasa pemrograman yang digunakan adalah PHP dengan *database* MySql.

LANDASAN TEORI

PenelitianTerdahulu

Penelitian yang berjudul "Metode *Least Significant Bit* (LSB) Dan *End Of File* (EOF) Untuk Menyisipkan Teks Ke Dalam Citra *Grayscale*" yang dilakukan oleh Krisnawati dari Jurusan Manajemen Informatika STMIK AMIKOM Yogyakarta. Dalam penelitian ini memaparkan proses implementasi metode LSB dan EOF untuk menyisipkan pesan teks ke dalam citra grayscale. Persamaan dengan penelitian yang dilakukan sekarang adalah penerapan metode LSB untuk menyisipkan file teks ke dalam media gambar. Perbedaannya terletak pada media yang digunakan. Jika pada penelitian sebelumnya pada citra *grayscale* maka pada penelitian sekarang menggunakan media gambar dengan format bebas. Selain itu aplikasi yang digunakan pada penelitian sebelumnya menggunakan Matlab 6.1, sedangkan pada penelitian sekarang menggunakan aplikasi yang dibuat sendiri.

Penelitian yang berjudul "Implementasi Algoritma *Rijndael* untuk Enkripsi Dan Dekripsi Pada Citra Digital". Dalam penelitian ini diimplementasikan teknik kriptografi pada citra berformat bitmap

dengan menggunakan algoritma *Rijndael*. Penelitian sebelumnya dengan yang sekarang dilakukan memiliki persamaan yakni menerapkan kriptografi Rijndael, sedangkan perbedaannya penelitian sebelumnya yang dienkripsi adalah *file bitmap*, sedangkan pada penelitian sekarang yang dienkripsi adalah *file* bertipe dokumen (berekstensi .pdf).

Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu "*cryptos*" yang berarti rahasia dan "*graphein*" yang berarti tulisan. Jadi, kriptografi adalah tulisan rahasia. Secara umum, kriptografi diartikan sebagai ilmu dan seni untuk menjaga kerahasiaan berita.

Menurut Kurniawan (2004) dalam bukunya yang berjudul "Kriptografi Keamanan Internet dan Jaringan Komunikasi", menjelaskan bahwa "kriptografi merupakan seni dan ilmu untuk menjaga keamanan pesan".

Selain itu pengertian kriptografi Menurut Sentot Kromodimoeljo (2009) menyatakan bahwa "kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi". Enkripsi adalah proses merubah *plainteks* (pesan asli) menjadi suatu pesan tersandi (*cipherteks*).

Kritografi Algoritma Rijndael

Algoritma Rijndael merupakan algoritma yang ditetapkan oleh *National Institute* of *Standards and Technology* (NIST) sebagai *Advanced Encryption Standard* (AES) pada bulanOktober 2000. Algoritma *Rijndael* ditemukan oleh Vincent Rijmen dan Joan Daemen dari Belgia. *Rijndael* termasuk dalam algoritma kriptografi yang sifatnya simetris dan *block cipher*. *Rijndael* mendukung panjang kunci 128 bit, 192 bit, dan 256 bit. Panjang kunci dan ukuran blok dapat dipilih secara independen. Tabel berikut adalah perbandingan jumlah proses yang harus dilalui untuk masing-masing masukan.

Tabel 1. Jumlah Proses Berdasarkan Bit Blok dan Kunci.

Panjang kunci (Nk) dalam *words*	Ukuranblok data (Nb) dalam *words*	Jumlah proses (Nr)
4	4	10
6	4	12
8	4	14

1 Proses Pembuatan Kunci (*Roundkey*)

Proses pembuatan kunci terdiri dari empat tahap yaitu *Rot Word*, *Sub Word*, proses XOR dengan nilai Rcon dan proses XOR dengan *word* sebelumnya.

2 Proses Enkripsi *Rijndael*

Proses enkripsi pada algoritma *Rijndael* terdiri dari 4 jenis transformasi *byte*, yaitu *Sub Bytes*(), *Shift Rows*(), *Mix Columns*(), dan *Add Round Key*(). Pada awal proses enkripsi, masukan yang telah berbentuk *array state* akan mengalami transformasi *Add Round Key*(). Setelah itu, array state akan mengalami transformasi *Sub Bytes*(), *Shift Rows*(), *Mix Columns*(), dan *Add Round Key*() secara berulang- ulang sebanyak Nr. Proses ini dalam algoritma *Rijndael* disebut sebagai *round function*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya di mana pada *round* terakhir, *array state* tidak mengalami transformasi *Mix Columns*(). Proses ini dalam algoritma Rijndael disebut sebagai *round function* (Kristoforus and 2012).

3 Steganografi

Menurut Rinaldi Munir (2004) steganografi (*steganography*) adalah suatu teknik yang digunakan untuk menyembunyikan data rahasia di dalam wadah (media) digital sehingga keberadaan data rahasia tersebut tidakdiketahui oleh orang lain. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara (audio), teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video.

4 Steganografi Metode *Least Significant Bit* (LSB)

Metode steganografi yang paling umum pada tipe berkas citra adalah LSB (*Least Significant Bit*). Metode ini menyembunyikan data dengan mengganti bit-bit data yang paling tidakberarti di dalam cover dengan bit-bit data rahasia. Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang paling berarti *Most Significant Bit* (MSB) dan bit yang paling kurang berarti *Least Significant Bit* (LSB). Bit yang cocok untuk diganti adalah LSB, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan pada cover citra, *byte* tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti, apalagi mata manusia tidak dapat membedakan perubahan kecil (Budiman, 2009).

METODE PENELITIAN

A. Waktu dan TempatPenelitian

Penelitian dilakukan selama bulan Oktober 2019 di PT Citcall Teknologi Indonesia Jalan tanjung 1 nomor 20, Kembangan, Meruya Selatan, Jakarta Barat.

B. Analisis Kriptografi Rijndael

Contoh enkripsi sebuah plain text yang diuji coba dalam penelitian ini adalah sebagai berikut. Diketahui plain text : usni2020usni2020, dengan key abcdefghabcdefgh maka chiphertext yang dihasilkan adalah sebagaiberikut:

Masukkan kekolom 4x4

Plaintext

u	2	u	2
s	0	s	0
n	2	n	2
i	0	i	0

CipherKey

a	e	a	e
b	f	b	f
c	g	c	g
d	h	d	h

Konversi ke heksa decimal

Plaintext

75	32	75	32
73	30	73	30
6E	32	6E	32
69	30	69	30

CipherKey

61	65	61	65
62	66	62	66
63	67	63	67
64	68	64	68

Konversi ke biner

Plaintext

01110101	00110010	01101110	01101001
01110011	00110000	00110010	00110000
01101110	00110010	01101110	01101001
01101001	00110000	00110010	00110000

Cipherkey

01100001	01100101	01100001	01100101

01100010	01100110	01100010	01100110
01100011	01100111	01100011	01100111
01100100	01101000	01100100	01101000

Sebelum melakukan enkripsi hitung ekspansi kunci (*key schedule*) terlebih dahulu

***Round* 0**

CipherKey

61	65	61	65
62	66	62	66
63	67	63	67
64	68	64	68

- w[0] = (61, 62, 63, 64)
- w[1] = (65, 66, 67, 68)
- w[2] = (61, 62, 63, 64)
- w[3] = (65, 66, 67, 68)
- g(w[3]) :
  - Menggeser kolom w[3] : (66, 67, 68, 65)
  - *Byte Substitution* (S-Box) : (33, 85, 45, 4D)
  - Operasi Rcon (01, 00, 00, 00) : g(w[3]) = (32, 85, 45, 4D)
- w[4] = w[0] ⊕ g(w[3]) = (53, E7, 26, 29)

01100001	01100010	01100011	0110 0100
⊕	⊕	⊕	⊕
00110010	10000101	01000101	0100 1101
0101 0011 53	1110 0111 E7	0010 0110 26	0010 1001 29

- w[5] = w[4] ⊕ w[1] = (36, 81, 41, 41)
- w[6] = w[5] ⊕ w[2] = (57, E3, 22, 25)
- w[7] = w[6] ⊕ w[3] = (32, 85, 45, 4D)

keyround 1 = 53 E7 26 29 36 81 41 41 57 E3 22 25 32 85 45 AD

Demikian seterusnya sampai *round* 10 maka hasil seluruh *round key* sebagai berikut:

- *Round* 0 = 61 62 63 64 65 66 67 68 61 62 63 64 65 66 67 68
- *Round* 1 = 53 E7 26 29 36 81 41 41 57 E3 22 25 32 85 45 4D
- *Round* 2 = C6 89 C5 0A F0 08 84 4B A7 EB A6 6E 95 6E E3 23
- *Round* 3 = 5D 98 E3 20 AD 90 67 6B 0A 7B C1 05 9F 15 22 26
- *Round* 4 = 0C 0B 14 FB A1 9B 73 90 AB E0 B2 95 34 F5 90 B3
- *Round* 5 = FA 6B 79 E3 5B F0 0A 73 F0 10 B8 E6 C4 E5 28 55
- *Round* 6 = 03 5F 85 FF 58 AF 8F 8C A8 BF 37 6A 6C 5A 1F 3F
- *Round* 7 = FD 9F F0 AF A5 30 7F 23 0D 8F 48 49 61 D5 57 76
- *Round* 8 = 7E C4 C8 40 DB F4 B7 63 D6 7B FF 2A B7 AE A8 5C
- *Round* 9 = 81 06 82 E9 5A F2 35 8A 8C 89 CA A0 3B 27 62 FC
- *Round* 10 = 7B AC 32 0B 21 5E 07 81 AD D7 CD 21 96 F0 AF DD

1 Tahapan Enkripsi

Initial Round

Add Round Key atau juga bisa disebut *initial round*

75 XOR 61 = 01110101 XOR 01100001 = 00010100

73 XOR 62 = 01110011 XOR 01100010 = 00010001

6E XOR 63 = 01101110 XOR 01100011 = 00001101
69 XOR 64 = 01101001 XOR 01100100 = 00001101
32 XOR 65 = 00110010 XOR 01100101 = 01010111
30 XOR 66 = 00110000 XOR 01100110 = 01010110
32 XOR 67 = 00110010 XOR 01100111 = 01010101
30 XOR 68 = 00110000 XOR 01101000 = 01011000
75 XOR 61 = 01110101 XOR 01100001 = 00010100
73 XOR 62 = 01110011 XOR 01100010 = 00010001
6E XOR 63 = 01101110 XOR 01100011 = 00001101
69 XOR 64 = 01101001 XOR 01100100 = 00001101
32 XOR 65 = 00110010 XOR 01100101 = 01010111
30 XOR 66 = 00110000 XOR 01100110 = 01010110
32 XOR 67 = 00110010 XOR 01100111 = 01010101
30 XOR 68 = 00110000 XOR 01101000 = 01011000

Biner *Add Round Key*

00010100	01010111	00010100	01010111
00010001	01010110	00010001	01010110
00001101	01010101	00001101	01010101
00001101	01011000	00001101	01011000

Hasil Add Round Key
State Saat ini : 14 11 0D 0D 57 56 55 58 14 11 0D 0D 57 56 55 58

Tahap selanjutnya adalah *SubBytes* yaitu mengubah hasil *Add Round Key* menggunakan tabel S-Box. Hasil *Add Round Key* yang pertama adalah 14 berarti baris ke 1, kolom 4 sehingga diperoleh FA.Lakukan dengan cara yang sama sampai semua hasil *Add Round Key* berubah sesuai dengan tabel S-Box.Maka akan diperoleh :

FA 82 D7 D7 5B B1 FC 6A FA 82 D7 D7 5B B1 FC 6A

Tahap selanjutnya adalah *Shift Rows* yaitu hasil *Sub Bytes* digeser ke kiri mulai dari baris ke 1 dilakukan 0 pergeseran, baris ke 2 dilakukan 1 pergeseran, baris ke 3 dilakukan 2 pergeseran, dan baris ke 4 dilakukan 3 pergeseran.

State

FA	5B	FA	5B
82	B1	82	B1
D7	FC	D7	FC
D7	6A	D7	6A

ShiftRows

FA	5B	FA	5B
B1	82	B1	82
D7	FC	D7	FC
6A	D7	6A	D7

Tahap selanjutnya adalah *Mix Columns* yaitu setiap kolom hasil *Shift Rows* dikalikan dengan matriks

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

Perkalian yang dimaksud disini adalah perkalian dalam *Galois Field* (2^8) dengan aturan sebagai berikut:

- Perkalian dengan 01 berarti tidak berubah.
- Perkalian dengan 02 artinya menggese r*byte* ke kiri

- Perkalian dengan 03 artinya menggeser *byte* kekiri dan kemudian melakukan XOR dengan nilai awal sebelum digeser.
- Setelah digeser, harus dilakukan XOR dengan 0x11B (100011011) apabila hasil nilai yang digeser lebih besar dari 0xFF (11111111).

Maka akan didapat:

$$\begin{pmatrix} 02\,03\,01\,01 \\ 01\,02\,03\,01 \\ 01\,01\,02\,03 \\ 03\,01\,01\,02 \end{pmatrix} \begin{pmatrix} FA\ 5B\ FA\ 5B \\ B1\ 82\ B1\ 82 \\ D7\ FC\ D7\ FC \\ 6A\ D7\ 6A\ D7 \end{pmatrix} = \begin{pmatrix} 9A\ 00\ 9A\ 00 \\ 8B\ 8C\ 8B\ 8C \\ 40\ 58\ 40\ 58 \\ A7\ 26\ A7\ 26 \end{pmatrix}$$

Langkah-langkah diatas diulangi sampai semua hasil *Shift Rows* terhitung dan diperoleh hasil *Mix Column* ssebagaiberikut :

9A 8B 40 A7 00 8C 58 26 9A 8B 40 A7 00 8C 58 26

Hasil *Mix Columns* di XOR kan dengan *key schedule round* 1

$$\begin{pmatrix} 9A\ 00\ 9A\ 00 \\ 8B\ 8C\ 8B\ 8C \\ 40\ 58\ 40\ 58 \\ A7\ 26\ A7\ 26 \end{pmatrix} \oplus \begin{pmatrix} 53\ 36\ 57\ 32 \\ E7\ 81\ E3\ 85 \\ 26\ 41\ 22\ 45 \\ 29\ 41\ 25\ 4D \end{pmatrix} = \begin{pmatrix} C9\ 36\ CD\ 32 \\ 6C\ 0D\ 68\ 09 \\ 66\ 19\ 62\ 1D \\ 8E\ 67\ 82\ 6B \end{pmatrix}$$

Lakukan seperti proses *Round* 1 sampai *Round* 9.

***Round* 10 (*FinalRound*)**

Hasil dari *Shift Rows* di xor kan dengan *Key schedule* round 10 :

Setelah *SubBytes*

42	CE	3F	D9
81	35	39	89
35	6A	EB	EE
CA	73	90	86

Setelah *ShiftRows*

42	CE	3F	D9
35	39	89	81
EB	EE	35	6A
86	CA	73	90

Hasil Ekripsi yaitu :
39 99 D9 8D EF 67 E9 4B 39 99 D9 8D EF 67 E9 4B

Perancangan

1. Analisis Kebutuhan

Analisis kebutuhan yang digunakan dalam sistem yang akan dibangun yaitu analisis kebutuhan masukan (*input*), kebutuhan keluaran (*output*) dan analisa kebutuhan proses.

1.1 Analisis KebutuhanMasukan (Input)

Kebutuhan masukan (*input*) yang digunakan dalam mengimplementasikan algoritma *Rijndael* dalam steganografi citra digital menggunakan metode *Least Significant Bit* adalah sebagai berikut :

a) Pesan atau file yang akan dienkripsi berupa *file* pdf (.pdf).
b) Kunci yang digunakan untuk enkripsi dan dekripsi *file* pesan rahasia.

c) Media yang digunakan dalam penyisip anadalah citra gambar *Joint Photographic Experts Group* (.jpg) dan *Portable Network Graphics* (.png) dengan tipe RGB untuk dilakukan pengujian hasil stego imagenya.
d) *File stego image* yang berisi pesan rahasia yang digunakan untuk ekstraksi pesan rahasia di dalamnya.

1.2 Analisi Kebutuhan Keluaran (output)

Kebutuhan keluaran yang ada dalam sistem yang dibangun adalah sebagai berikut :

a) File gambar bertipe *Portable Network Graphics* (.png) yang dihasilkan dari proses enkripsi file plainteks atau pesan asli dan penyisipan pesan rahasia.
b) Pesan asli atau plainteks berformat .pdf yang dihasilkan dari proses dekripsi pesan yang ada di dalam gambar yang sebelumnya sudah diestrak.

1.3 Analisis Kebutuhan Proses

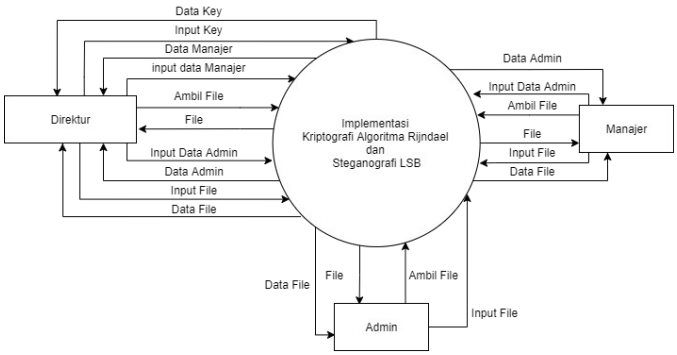
a) Pada halaman pertama terdapat menu login.
b) Pada system ini terdapat tiga halaman yaitu: halaman direktur, halaman manajer dan halaman admin.
c) Halaman direkturter dapat data file, data manajer , dan data admin. Pada Halaman direktur juga terdapat halaman input *key* yang digunakan sebagai key untuk men-*decrypt file*.
d) Halaman manajer terdapat data file dan data admin. Pada halaman manajer juga terdapat halaman manajemen admin, yang digunakan untuk melihat, membuat, mengubah, dan menghapus user admin.

Halaman admin terdapat data file, yang digunakan untuk menyimpan *file*, untuk mebuka *file* diperlukan *key* yang hanya diketahui oleh direktur.

2. Perancangan Sistem dan Perangkat Lunak

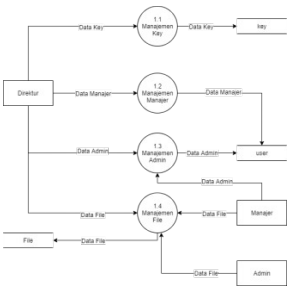
2.1 Data Flow Diagram

a) DFD Level 0



Gambar 1. DFD Level 0

b) DFD Level 1

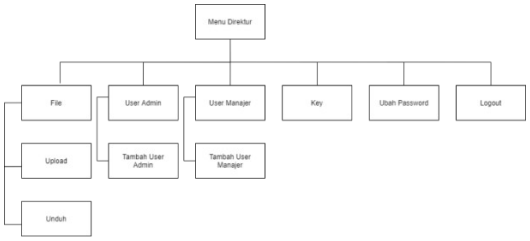


Gambar 2. DFD Level 1

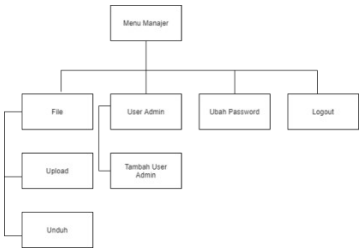
IMPLEMENTASI DAN PEMBAHASAN

A. Implementasi Program

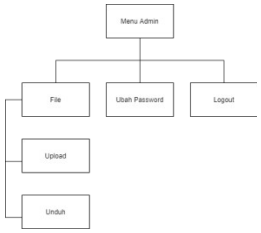
1. Implementasi Interface



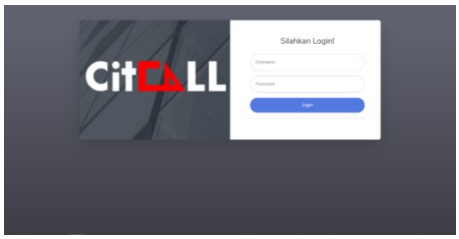
Gambar 3. Struktur Menu Direktur



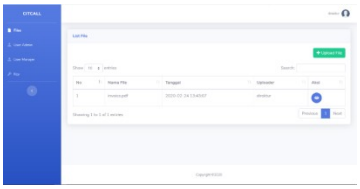
Gambar 4. Struktur Menu Manajer



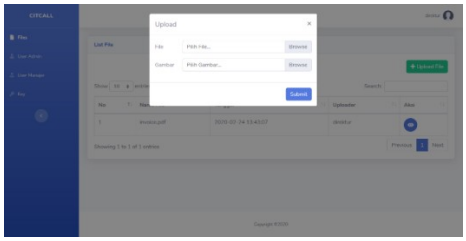
Gambar 5. Struktur Menu Admin



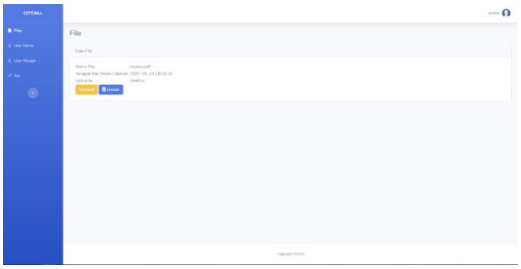
Gambar 6. *Interface Halaman Login*



Gambar 7. *Interface Halaman List Files*



Gambar 8. *Interface Halaman Upload File*



Gambar 9. *Interface Unduh File*

KESIMPULAN DAN SARAN

A. Kesimpulan

1. Dengan menggunakan metode kriptografi algoritma *Rijndael* dan metode steganografi *Least Significant Bit* (LSB) mampu mengurangi tingkat pencurian data rahasia perusahaan sehingga sulit dilakukan oleh pihak yang tidak memiliki wewenang.
2. Algoritma *rijndael* ini diimplementasikan dalam enkripsi pesan sebelum penyisipan dan dekripsi pesan setelah ekstraksi pesan dari *stego image*.

B. Saran

1. Penambahan jenis dari Algoritma *Rijndael* tidak hanya jenis 128 bit saja, sehingga dapat memilih panjang kunci yang diinginkan untuk enkripsi.
2. Pesan rahasia yang disisipkan dapat dikembangkan lagi dengan menggunakan file selain .pdf.
3. Media penyisipan file menggunakan media citra digital dengan format lain selain *Joint Photographic Experts Group* (.jpg) dan *Portable Network Graphics* (.png).

DAFTAR PUSTAKA

Krisnawati, 2008. Metode Least Significant Bit (LSB) dan End Of File (EOF) UntukMenyisipkan Teks keDalam Citra Grayscale. Seminar Nasional Informatika 2008 (semnasIF 2008). UPN "Veteran" Yogyakarta, 24 Mei 2008. ISSN: 1979-2328.

R. Kristoforus JB, Stefanus Aditya BP, 2012, Implementasi Algoritma Rijndael untuk Enkripsi Dan Dekripsi Pada Citra Digital. Yogyakarta, 15-16 juni 2012 ISSN: 1907-5022

Munir, R., 2004. Pengolahan Citra Digital Dengan Pendekatan Algoritmik. Bandung: Informatika.

Budiman, Asep.2009. "Aplikasi Steganography Pada Video Dengan Metode Least Significant Bit (LSB)".