Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 51-61
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Implementasi Keamanan Citra Menggunakan Algoritma AES-128 Dengan Aplikasi Client-Server

Azanuddin, Suardi Yakub, Jaka Prayudha
STMIK Triguna Dharma
Jl. A.H Nasution No.73 Medan Johor, 061-8224051
azdin.bpc@gmail.com, suardiyakub@gmail.com, jakaprayudha3@gmail.com

Abstract

Digital images that are private and confidential are very vulnerable to eavesdropping by irresponsible parties. Especially when distributed over the internet, such as chat-based applications such as Facebook, WhatsApp and e-mail media. Image sent via the internet. Because digital images are still recognizable images and can be used by eavesdroppers for personal gain, to the detriment of those who have access to image data. The act of tapping the image data can be minimized by the application of cryptographic encryption techniques. This research will secure digital images with 128 bit AES method for encryption and decryption of digital images in client-server based applications. The results of the AES algorithm encryption produce a cipherimage with pixel values that are much different from the plainimage pixel values.

Keywords*: Digital Image, AES 128 Bit, Cryptography, Client Server*

Abstrak

Citra digital yang bersifat pribadi dan rahasia sangat rentan terhadap peyadapan oleh pihak-pihak yang tidak bertanggung jawab. Terutama bila didistribusikan melalui jaringan internet seperti pada aplikasi berbasis chatting facebook, whatsapp dan media e-mail. Citra yang dikirim melalui jaringan internet. Karena citra digital masih berupa citra yang dapat dikenali dan dapat dimanfaatkan oleh pihak penyadap untuk keuntungan pribadi sehingga merugikan pihak yang memiliki akses terhadap data citra. Tindakan penyadapan data citra tersebut dapat diminalisir dengan aplikasi teknik enkripsi kriptografi. Penelitian ini akan mengamankan citra digital dengan metode AES 128 bit untuk enkripsi dan dekripsi citra digital pada aplikasi berbasis client-server. Hasil dari enkripsi Algoritma AES menghasilkan cipherimage dengan nilai-nilai pixel yang jauh berbeda dengan nilai-nilai pixel plainimage

Kata kunci*: Citra Digital, AES 128 Bit, Kriptografi, Client Server*

1. PENDAHULUAN

Citra digital yang bersifat pribadi dan rahasia sangat rentan terhadap peyadapan oleh pihak-pihak yang tidak bertanggung jawab. Terutama bila didistribusikan melalui jaringan internet seperti pada aplikasi berbasis *chatting facebook*, *whatsapp* dan media *e-mail*. Citra yang dikirim melalui jaringan internet rawan terhadap penyerangan dan penyadapan, serta penyimpanan yang dilakukan didalam media *stroge* rawan terhadap pengaksesan oleh orang-orang yang tidak memiliki wewenang [1]. Karena citra digital masih berupa citra yang dapat dikenali dan dapat dimanfaatkan oleh pihak penyadap untuk keuntungan pribadi sehingga merugikan pihak yang memiliki akses terhadap data citra. Tindakan penyadapan data citra tersebut dapat diminalisir dengan aplikasi teknik enkripsi kriptografi.

Algoritma AES adalah salah satu algoritma yang dapat diandalkan dalam mewujudkan teknik kriptografi, di mana metode AES ini terlebih dahulu

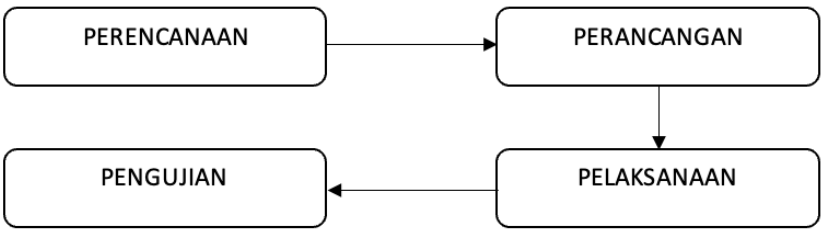
Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 51-61
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

melakukan 4 kali proses operasi pada saat enkripsi dan dekripsi yaitu transformasi subtitusi *byte*, kemudian pergeseran baris, melakukan percampuran kolom, dan kemudian melakukan penambahan kunci. Penelitian yang dilakukan Shaikh dan Kaul menunjukkan bahwa *Advanced Encryption Standard* (AES) adalah algoritma yang terbaik dariteknologi enkripsi simetri [2]. Berbagai serangan sudah pernah dilakukan terhadap algoritma AES yaitu *differential cryptanalysis, truncated differentials, the square attacks* dan *interpolation attacks*, dari pembuktian matematis, AES dapat bertahan dari serangan tersebut [3].

Penelitian ini akan mengamankan citra digital dengan metode AES 128 bit untuk enkripsi dan dekripsi citra digital pada aplikasi berbasis *client-server*. Hasil dari enkripsi Algoritma AES menghasilkan *cipherimage* dengan nilai-nilai pixel yang jauh berbeda dengan nilai-nilai pixel *plainimage*. Pembuatan aplikasi perangkat lunak enkripsi dan dekripsi berbasis *client-server,* bertujuan untuk *transfer* data digital berupa *plainimage* yang sudah dienkripsi menggunakan algoritma AES dari satu *client* ke *client* yang lainya. *Client* akan berinteraksi menggunakan kabel LAN (*local area network*) untuk menghubungkan satu komputer dengan komputer lainnya, dengan settingan *TCP/IP* sebagai indetifikasi alamat komputer. Keuntungan dari perangkat lunak yang akan dirancang berbasis *client-server* adalah tidak dibutuhkan lagi *flashdisk* untuk mentransfer data citra digital dari satu komputer ke kemputer yang lain, keamanan data yang akan dikirim lebih aman dengan pengaturan

2. METODOLOGI PENELITIAN

Metode pengumpulan data yang digunakan dalam pembahasan penelitian ini adalah Studi Literatur yang merupakan tahap pengumpulan data dengan cara mengumpulkan literatur, jurnal, *paper*, dan buku-buku yang berkaitan dengan judul penelitian, serta mencari informasi dari berbagai sumber di internet untuk mengetahui perkembangan terbaru dari data yang diambil sebagai bahan dalam pembuatan tugas akhir. Secara garis besar, langkah-langkah dalam penelitian ini meliputi perencanaan (*planning*), Perancangan, pelaksanaan (*acting*), pengujian. Keempat langkah tersebut dapat dilihat dari bagan berikut ini.



Gambar 1. Framework Penelitian

2.1. Metode Perancangan Sistem

Dalam pengembangan system ini menggunakan metode waterfall yang dimana metode ini sesuai dengan framework penelitian yang dirancang. Proses waterfall sebagai berikut :

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 51-61
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

a) Requierments
Proses pengumpulan data yang dibutuhkan terkait permsalahan yang ditemukan, data berbentuk primary dan sekunder yang dijadikan bahan Analisa dalam implementasi.

b) Design
Proses perancangan system dari membangun pemodalan system menggunakan Unifield Modeling Language (UML), perancangan database, perancangan user interface dan user experience serta perancangan aplikasi keamanan citra berbasis client server.

c) Development
Proses pembangunan system atau dengan kata lain pengkodean dengan menggunakan Bahasa pemrograman tertentu yang dapat digunakan sebagai media pembangungan aplikasi keamanan citra berbasis client server.

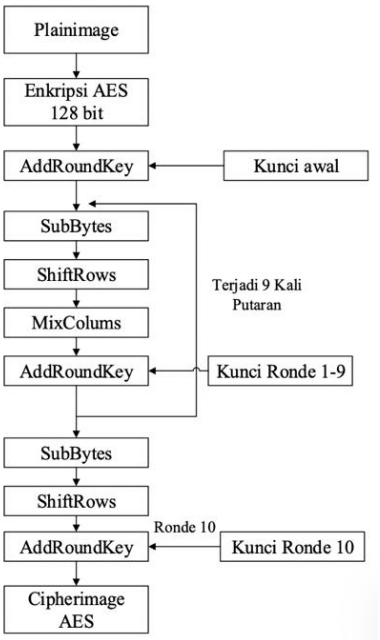
d) Implementation
Proses penerapan aplikasi pada area penelitian secara langsung, untuk digunakan sebagai bahan verifikasi hasil penelitian.

e) Verification
Proses verifikasi hasil penelitian, dengan tujuan apakah riset yang dilakukan telah sesuai dan berjalan sebagaimana mestinya.

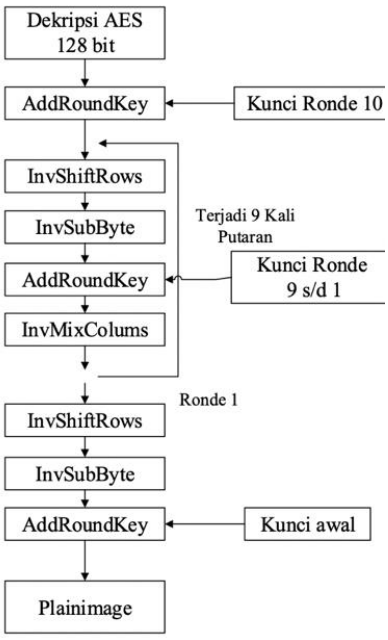
f) Maintenance
Proses perawatan dan pembaruan aplikasi selama digunakan oleh user secara langsung.

2.2. Algoritma AES 128 Bit

Penerapan algoritma AES 128 Bit untuk memberikan keamanan dengan cara enkripsi file citra digital pada saat proses transfer antara client dan server serta sebaliknya.



Gambar 2. Diagram Enkripsi AES

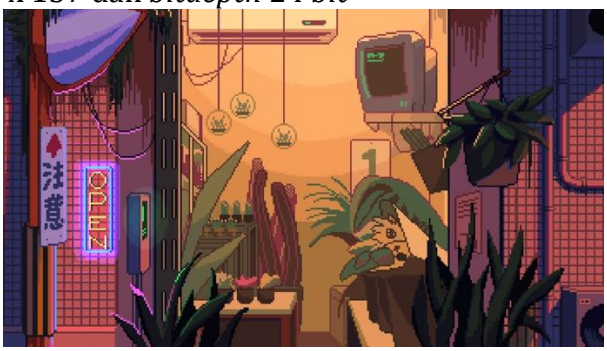


Gambar 3. Diagram Dekripsi AES

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 51-61
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Aplikasi dirancang berbasis *client* dan *server* sehingga hasil enkripsi akhir berupa *cipher image* dapat langsung dikirim melalui jaringan lokal antara *client* satu dengan yang lainya. Pemanfaatan aplikasi berbasis *client* dan *server* ini mengurangi tingkat pencurian data karena pengiriman dapat dilakukan tanpa adanya koneksi *internet* dalam ruang lingkup jaringan lokal yang saling terhubungan satu sama lain baik secara kabel dan tanpa kabel dengan pemanfaatan alamat *ip address* computer

a) Data Sample
Data yang digunakan adalah citra digital berwarna dengan ekstansi .jpg resolusi 103 x 137 dan *bitdepth* 24 *bit*



Gambar 4. Plainimage dengan resolusi 103 x 137

b) Proses Ekstraksi
Berdasarkan pada gambar di atas akan diambil 6 *pixel* sebagai sampel dalam perhitungan manual. Enam *pixel* tersebut akan diambil nilai desimal warnanya dengan cara mengektrasi setiap elemen *pixel.* Nilai desimal elemen warna pada setiap *pixel* akan diekstraksi menggunakan *software* matlab. Adapun nilai RGB dari setiap pixel sampel citra 3 x 3 dapat dilihat pada tabel di bawah ini :

Tabel 1. Nilai RGB Pixel Sample

Pixel	Warna	Plain Desimal
1	R	160
	G	109
	B	89
2	R	120
	G	87
	B	104
3	R	83
	G	77
	B	150
4	R	97
	G	81
	B	133
5	R	92
	G	75

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 51-61
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Pixel	Warna	Plain Desimal
6	B	133
	R	134
	G	117
	B	17

Berdasarkan tabel di atas, untuk mempermudah dalam hitungan manual algoritma AES, maka penulis hanya mengambil nilai R pada *pixel* 6, sehingga nilai desimal dari *plainimage* adalah 160, 109, 89, 120, 87, 104, 83, 77, 150, 97, 81, 133, 92, 75, 133, 134. Kunci yang digunakan dalam hitungan manual adalah TISTMIKTRGDHARMA panjang kunci 16 *byte*. Selanjutnya adalah tahap penyelesaian algoritma dengan proses enkripsi dan dekripsi.

c) Proses Enkripsi

Adapun proses enkripsi algoritma AES sesuai dengan contoh kasus sebagai berikut: Enkripsi Algoritma AES 128 bit

1) Sebelum proses enkripsi, terlebih dahulu melakukan proses pembangkitan kunci. Pembangkitan kunci dilakukan sebanyak sepuluh putaran. Kunci awal di*input* kedalam *array* 4x4 bernilai hexadesimal.

d) 54	e) 49	f) 53	g) 54
h) 4D	i) 49	j) 4B	k) 42
l) 55	m) 44	n) 49	o) 44
p) 41	q) 52	r) 4D	s) 41

2) Pembangkitan kunci ronde 1 pada kolom pertama dilakukan dengan cara mengambil nilai kolom terakhir kunci sebelumnya lalu dilakukan rotasi dengan mengeser blok paling atas ke blok paling bawah.
3) Kemudian lakukan subtitusi pada kolom yang sudah di *rotate* dengan tabel S-Box pada gambar tabel 2.2 di bab kajian pustaka.
4) Hasil subtitusi kemudian di XOR dengan nilai kolom pertama kunci sebelumnya.
5) Kemudian di XOR kembali dengan nilai tabel *Round Constant* (Rcon) kolom pertama untuk kunci ronde ke 1.
6) Untuk pencarian nilai kolom kedua kunci ronde ke 1, lakukan XOR nilai kolom kedua kunci sebelumnya dengan nilai kolom pertama untuk kunci ronde berikutnya.
7) Untuk pencarian nilai kolom ketiga kunci ronde ke 1, lakukan XOR nilai kolom ketiga kunci sebelumnya dengan nilai kolom kedua untuk kunci ronde berikutnya
8) Untuk pencarian nilai kolom keempat kunci ronde ke 1, lakukan XOR nilai kolom keempat kunci sebelumnya dengan nilai kolom ketiga untuk kunci ronde berikutnya.
9) Proses pembentukan kunci ronde ke 2 hingga ke 10 mengikuti langkah yang sama, sehingga didapatkan kunci keseluruhan ronde seperti berikut :

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 51-61
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

10) *RoundKey* 1 *RoundKey* 2 *RoundKey* 3 *RoundKey* 4 *RoundKey* 5

79	30	63	37	3C	0C	6F	58	48	44	2B	73	62	26	0D	7E	5A	7C	71	0F
56	1F	54	16	8D	92	C6	D0	10	82	44	94	BC	3E	7A	EE	49	77	0D	E3
D6	92	DB	9F	A3	31	EA	75	04	35	DF	AA	37	02	DD	77	BC	BE	63	14
61	33	7E	3F	FB	C8	B6	89	91	59	EF	66	1E	47	A8	CE	ED	AA	02	CC

11) *RoundKey* 6 *RoundKey* 7 *RoundKey* 8 *RoundKey* 9 *RoundKey* 10

6B	17	66	69	CE	D9	BF	D6	B9	60	DF	09	9F	FF	20	29	E9	16	36	1F
B3	C4	C9	2A	01	C5	0C	26	64	A1	AD	8B	F5	54	F9	72	88	DC	25	57
F7	49	2A	3E	E1	A8	82	BC	3A	92	10	AC	3D	AF	BF	13	80	2F	90	83
9B	31	33	FF	62	53	60	9F	94	C7	A7	38	95	52	F5	CD	30	62	97	5A

12) Proses pertama sebelum masuk ronde 1 dinamakan *initial round*, siapkan nilai hexadesimal *plainimage* dan kunci ke dalam bentuk *array* 4x4

13) Selanjutnya adalah melakukan proses *AddRoundKey* dengan meng XOR setiap kolom bilangan hexadesimal *plainimage* dengan setiap kolom nilai hexadesimal kunci.

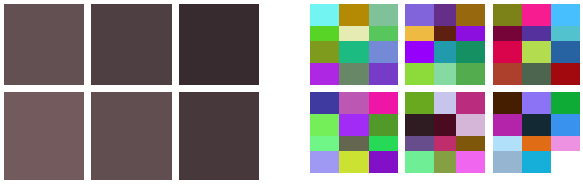
14) Lakukan XOR pada setiap kolom *state* dan kolom kunci dengan merubah nilai hexadesimal kedalam biner.

15) Untuk kolom selanjutnya dilakukan perhitungan XOR dengan cara yang sama yaitu kolom kedua state di XOR dengan kolom kedua kunci dan seterusnya. Sehingga didapat hasil *AddroundKey* pertama (*initial round*e

16) Setiap ronde memiliki 4 proses yaitu *SubBytes, ShiftRows, Mixcolumns* dan *Addroundkey*, pada ronde terakhir hanya memiliki 3 proses yaitu *SubBytes, ShiftRows* dan *AddroundKey*. AES butuh 1 blok 128 bit *plainimage* yang didapat dari setiap nilai RGB *pixel*. Ronde pertama dapat dilakukan ketika hasil proses *initial round* pertama sudah didapat.

17) Hasil di atas adalah *cipherimage* AES untuk enkripsi pertama. Adapun proses enkripsi keseluruhan ronde.

Nilai desimal *plainimage* berbeda dengan nilai desimal *cipherimage*. Perbedaan ini akan membuat citra digital memiliki bentuk yang tidak dapat dimengerti manusia. Sedangkan pada *pixel* 6 nilai GB tidak mengalami perubahan dikarenakan nilai GB pada *pixel* 6 tidak diikutkan dalam enkripsi manual. Hasil perbandingan perubahan *plainimage* yang di enkripsi menggunakan algoritma AES 128 *bit* ke enam *pixel* adalah sebagai berikut:

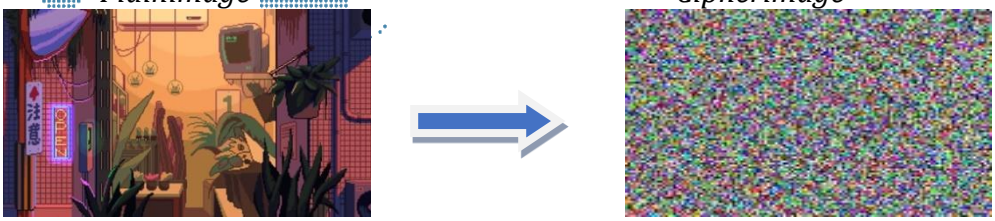


Gambar 5. *pixel Cipherimage* sampel

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 51-61
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Hasil perbandingan perubahan *plainimage* yang di enkripsi menggunakan algoritma AES 128 *bit* kesuluruhan adalah sebagai berikut:

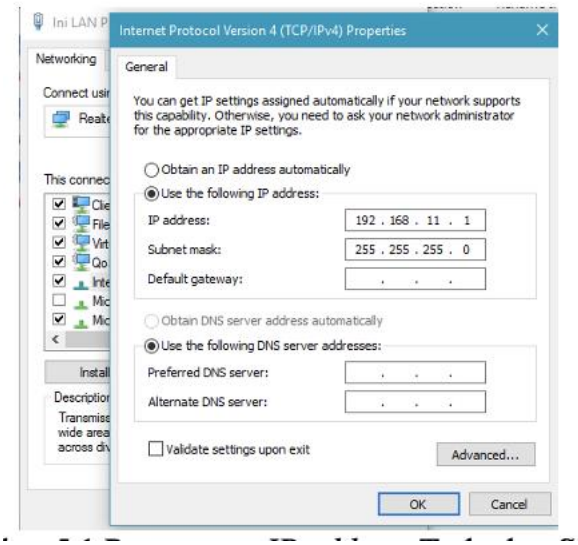
Plainimage *Cipherimage*



Gambar 6. *Cipherimage* Keseluruhan

3. HASIL DAN PEMBAHASAN

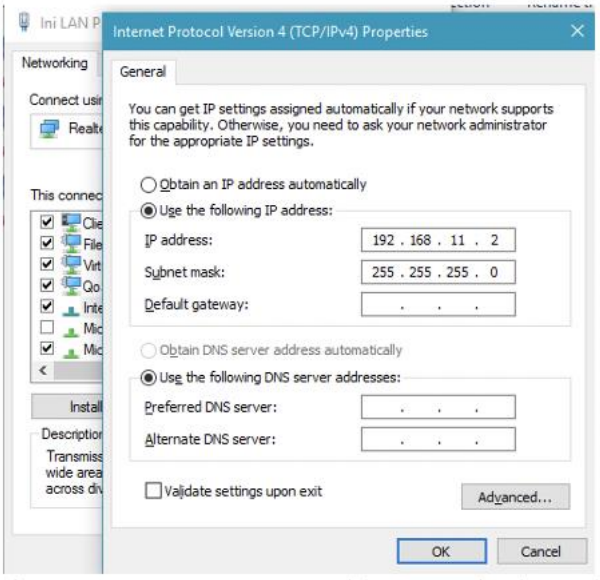
Aplikasi yang telah dibuat memerlukan beberapa kebutuhan sistem tambahan agar aplikasi dapat berjalan dengan sebagaimana mestinya. Adapun kebutuhan sistem aplikasi kriptografi berbasis *client server* pada pembahasan ini dibagi menjadi 3 bagian yaitu, kebutuhan perangkat keras, kebutuhan perangkat lunak dan proses koneksi antara *server* (pengirim) dan *client* (penerima).



Gambar 7. Pengaturan IP di Server

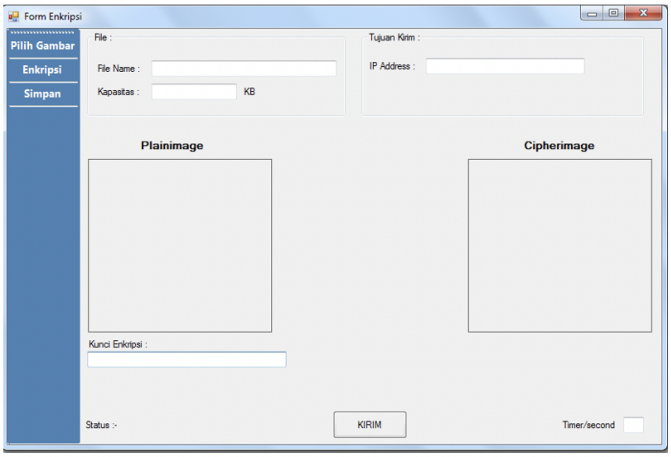
Berdasarkan pada gambar di atas pengaturan *ip address* terhadap *server* dilakukan dengan *ip address* kelas C yaitu 192.168.11.1. Sedangkan pengaturan *ip address* terhadap komputer *client* harus sama *Net* ID dan berbeda *Host* ID

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 51-61
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



Gambar 8. Pengaturan IP di Client

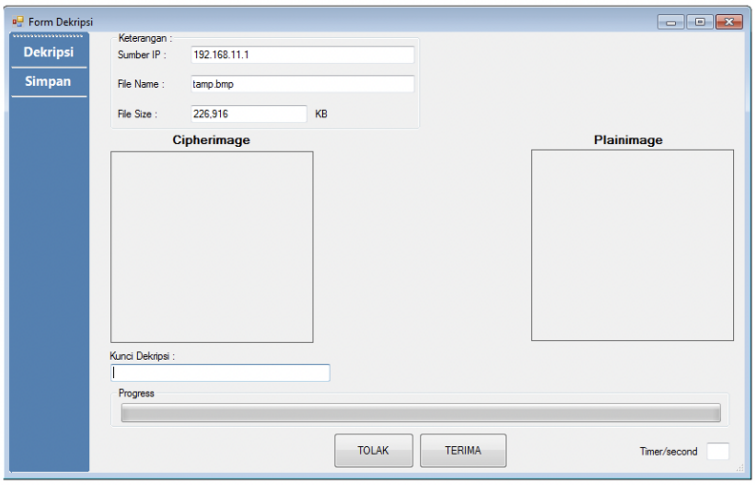
Proses koneksi dengan media *wireless* membutuhkan sinyal *wifi* yang menghubungkan antara komputer *server* dan *client*. Koneksi *wifi* umumnya memiliki pengaturan *ip address* secara dinamis.



Gambar 9. Form Enkripsi

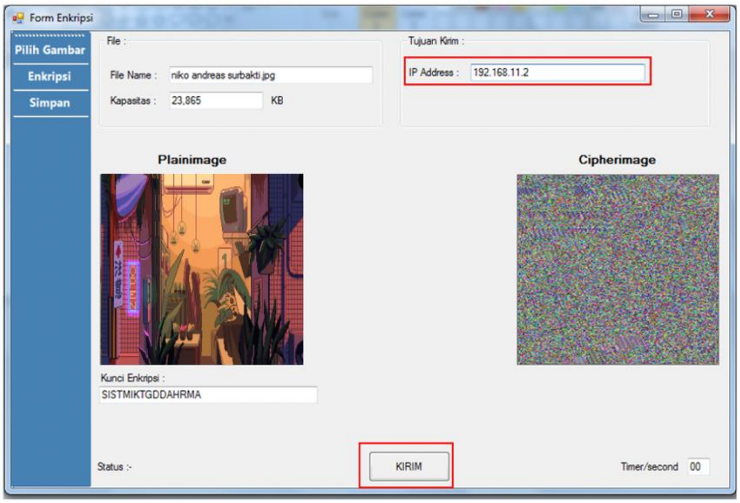
Berdasarkan pada tampilan *form* enkripsi terdiri dari beberapa *stripbutton* dan *button*. *Stripbutton* pilih gambar berfungsi untuk memilih gambar citra *image* yang akan dienkripsi. *Stripbutton* enkripsi berfungsi untuk melakukan proses enkripsi terhadap citra digital yang sudah dipilih. *Stripbutton* simpan berfungsi untuk menyimpan citra *cipherimage* didalam direktori komputer. *Button* kirim berfungsi untuk mengirimkan citra *cipherimage* kepada penerima

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 51-61
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



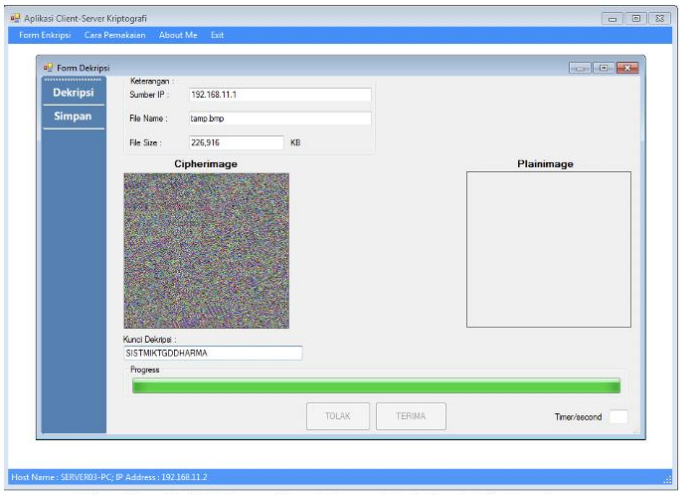
Gambar 10. Form Dekripsi

Berdasarkan pada tampilan *form* dekripsi terdiri dari beberapa *stripbutton* dan *button*. *Stripbutton* pilih dekripsi berfungsi untuk melakukan proses dekripsi terhadap citra *cipherimage* yang sudah diterima. *Stripbutton* simpan berfungsi untuk menyimpan citra *plainimage* hasil dekripsi didalam direktori komputer. *Button* terima berfungsi untuk menerima pesan yang masuk, sedangkan *button* tolak berfungsi untuk menolak pesan yang masuk



Gambar 11. Proses Enkripsi Dan Kirim ke Server

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 51-61
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



Gambar 12. Proses Dekripsi

4. SIMPULAN

Hasil proses enkripsi citra digital menggunakan algoritma AES 128 bit memberikan *output cipherimage* yang memiliki tingkat keamanan yang baik. Hal ini dapat dilihat perbedaan visual antara *plainimage* dan *cipherimage*. Hasil enkripsi citra digital menggunakan algroritma AES 128 bit berupa sebuah *cipherimage* yang memiliki perubahan ukuran *size* dari citra *plainimage*. Proses waktu enkripsi dan dekripsi dipengaruhi oleh ukuran dan resolusi citra *plainimage* serta spesifikasi komputer yang menjalankan aplikasi. Semakin tinggi resolusi dari *plainimage* maka proses enkripsi dan dekripsinya semakin lama begitu pula sebaliknya.

DAFTAR PUSTAKA

[1] R.Munir, "Analisa Keamanan Enkripsi Citra Digital Menggunakan Kombinasi Dua *Chaos Map* dan Penerapan Teknik Selektif", Juti, vol. 10, pp89-95, 2012.

[2] A.P. Shaikh and V. Kaul, "*Enhanced Security Algorithm Using Hybrid Encryption and ECC*", IOSR *Journal of Computer Engineering*, vol. 16, pp.80-85, 2014.

[3] Asriyanik, "Studi Terhadap *Advanced Encryption Standard* (AES) dan Algoritma *Knapsack* Dalam Pengamanan Data", Santika, vol. 7, pp.553.561, 2017.

[4] E. Setyaningsih, Kriptografi & Implementasi Menggunakan Matlab, Yogyakarta: Andi. 2015.

[5] A.A. Ibrahim, "Perancangan Pengamanan Data Menggunakan Algoritma AES (*Advanced Encryption Standard*)", Teknik Informatika STMIK Antar Bangsa, vol. III, pp.53-60, 2017.

[6] E.R. Agustina and A. Kurniati, "Pemanfaatan Kriptografi Dalam Mewujudkan Keamanan Informasi Pada *e-Voting* di Indonesia", Seminar Nasional Informatika, pp.22-28, 2009.

[7] S. Prabowo, (2018, Jan,2). Kriptografi-Jenis Jenis Serangan dalam Kriptografi [online]. Available: http://www.sigitprabowo.id/2013/01/kriptografi-jenis-jenis-serangan-dalam.html.

[8] N. Aleisa, "*A Comparison of the 3DES and AES Encryption Standards*", *International Jurnal of Security and Its Applications*, vol. 7, pp.241-246, 2015.

[9] Mohtashim, (2015,apr.9). *Cryptografy Hash Functions* [online]. Available:https://www.tutorialspoint.com/cryptography/cryptography.html.
[10] R. Sadikin, Kriptografi Untuk Keamanan Jaringan, Yogyakarta: Andi. 2012.
[11] A. Widarma, "Kombinasi Algoritma AES, RC4 dan Elmagal Dalam Skema *Hybrid* Untuk Keamanan Data", *Journal of Computer Engineering System and Science*, vol. 1, pp.1-8, 2016.
[12] V. Yuniati, G. Indriyanta and A. Rachmat, "Enkripsi dan Dekripsi dengan Algoritma AES 256 Untuk Semua Jenis File", Informatika, vol. 5, pp.23-31, 2009.
[13] Wikipedia, (2018,jan.12). Rijdael MixColumns [online]. Available: https://en.wikipedia.org/wiki/Rijndael_MixColumns.
[14] P. Mahajan and A. Sachdeva, " A Stduy Of Encryption Agorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology, Vol 13, pp.15-22, 2013.
[15] P. Christensson, (2008, Oct.12). *Aplication Definition* [online]. Available: https://techterms.com/definition/application.
[16] I. Sofana, Membangun Jaringan Komputer, Bandung: Informatika. 2013.
[17] M. Meyers, *Introducing Basic Network Concepts Capter* 1, 2010.
[18] A. Pamungkas, (2017, Jul.26). Pengolahan Citra [online]. Available: https://pemrogramanmatlab.com/2017/07/26/pengolahan-citra-digital/
[19] T. Sutoyo, Teori Pengolahan Citra Digital, Yogyakarta: Andi. 2009.
[20] U. Ahmad, Pengolahan Citra Digital & Teknik Pemogramannya, Yogyakarta: Graha Ilmu. 2005.
[21] A. Purnama, (2012, Jul.23). Definisi dan Pengolahan Citra Digital [online]. Available: http://elektronika-dasar.web.id/definisi-dan-pengolahan-citra-digital/
[22] D. Putra, Pengolahan Citra Digital, Yogyakarta: Andi Offset. 2010.
[23] E. Sutanta, Pengantar Teknologi Informasi, Yogyakarta: Graha Ilmu. 2005.
[24] Mohtashim, (2014, jun.12). UML Tutorial [online]. Available: https://www.tutorialspoint.com/uml/index.htm.
[25] R. A.S and M. Shalahudin, Modul Pembelajaran: Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek), Bandung: Modula. 2011.
[26] L.V. Kiong, (2012,oct.6). *Visual Basic* 2010 Tutorial [online]. Available: http://www.vbtutor.net/index.php/visual-basic-2010-tutorial/.