p-ISSN : ?, e-ISSN : ? , available at : https://ejournal.unsrat.ac.id/index.php/informatika

Hybrid End of File Stenganography and Super Encryption Cryptography

Hybrid Stenganografi End of File dan Kriptografi Super Enkripsi

Muhammad Rivaldy Cadullah [1)]
Jurusan Teknik Elektro, Universitas Sam Ratulangi Manado, Jl. Kampus Bahu, 95115, Indonesia
Email : 16021106027@student.unsrat.ac.id [1)]
Received: [date]; revised: [date]; accepted: [date]

Abstract* — This study aims to apply encryption and decryption using the ECC (Elliptic Curve Cryptography) and Vigenere methods and to hide and extract messages in images by applying the End of File method. This type of research is software engineering by applying the forward engineering method which in this study will provide results in the form of a model combining three encryption algorithms into an application. From testing the functionality and accuracy of the calculations it is known that the use of the Vigenere algorithm and the ECC algorithm can properly carry out the encryption and decryption process of the input message. Furthermore, from testing the functionality and accuracy of calculations in the steganography process, it is known that the text message has been successfully inserted (hidden) at the end of an image file. As well as successfully re-extracted from the image file, so the message can be read. So that the encryption converter that has been made is feasible to use.

Keywords: Cryptography, ECC, Vigenere, Steganography, End of File.

Abstrak* — Penelitian ini bertujuan untuk menerapkan enkripsi dan dekripsi menggunakan metode ECC *(Elliptic Curve Cryptography)* dan Vigenere serta untuk menyembunyikan dan mengekstrak pesan pada citra dengan menerapkan metode End of File (EoF). Jenis penelitian ini adalah rekayasa perangkat lunak dengan menerapkan metode forward enginering dimana pada penelitian ini akan memberikan hasil berupa sebuah model penggabungan tiga buah algoritma enkripsi menjadi sebuah aplikasi. Dari pengujian fungsionalitas dan akurasi perhitungan diketahui bahwa penggunaan algortima Vigenere serta algoritma ECC dapat dengan baik melakukan proses enskripsi dan dekripsi dari pesan yang diinputkan. Selanjutnya dari pengujian fungsionalitas dan akurasi perhitungan pada proses steganografi diketahui bahwa pesan text berhasil disisipkan (disembunyikan) pada bagian akhir dari file sebuah citra. Serta berhasil kembali diekstrak dari file citra, sehingga pesan dapat dibaca. Sehingga konverter enkripsi yang telah dibuat layak untuk digunakan.

Kata Kunci : Kriptografi, ECC, Vigenere, Steganografi, End of File.

I. PENDAHULUAN

Dengan semakin berkembangnya jaman kebutuhan akan informasi semakin meningkat. Selain itu dengan perkembangan teknologi yang semakin pesat, kemudahan untuk mencari informasi ataupun saling bertukar informasi akan semakin mudah. Pertukaran informasi dapat dilakukan dengan berbagai macam media, salah satu media yang sering digunakan pada saat ini adalah media digital. Media digital menjadi semakin populer dikarenakan kemudahan dan kecepatan penyampaian informasi antar pengguna. Namun media digital memiliki kelemahan dimana informasi yang bersifat rahasia dapat dicuri oleh pihak yang tidak berhak. Hal ini membuat pertukaran informasi yang bersifat rahasia harus dilakukan dengan hati-hati. Seiring dengan berkembangnya teknologi pada jaman sekarang ini, kejahatan sistem informasi pun akan semakin berkembang dengan berbagai macam metode-metode mengakses informasi rahasia yang merupakan hak pelaku. Maka dari itu pengaman sistem informasi pun harus lebih berkembang mengikuti perkembangan teknologi.

Dalam hal ini salah satu teknik yang bisa digunakan dalam melakukan pengamanan dalam pertukaran informasi adalah Kriptografi. Kriptografi adalah ilmu yang mempelajari tentang pengamanan pesan atau teks yang akan dikirimkan kepada orang yang akan dituju. Kriptografi akan mengubah pesan asli atau yang disebut dengan *Plaintext* menjadi suatu pesan acak atau biasa disebut dengan *Ciphertext* dengan menggunakan algoritma dan kunci tertentu, proses ini disebut dengan enkripsi. Setelah pesan telah diterima oleh penerima yang dituju, maka pesan yang dalam bentuk *ciphertext* akan diubah kembali kebentuk aslinya atau *plaintext* dengan menggunakan algoritma dan kunci yang sama pada saat melakukan enkripsi, proses ini disebut dengan dekripsi. Dengan menggunakan kriptografi maka pesan atau informasi yang dikirimkan akan berupa sekumpulan teks acak yang tak bermakna ketika telah dienkripsi dan hanya akan dapat dimengerti oleh penerima yang dituju.

Namun kriptografi juga memiliki kelemahan dimana teks tersebut masih dapat terlihat oleh orang lain. Teks acak yang tak bermakna tersebut akan tampak mencurigakan dan dapat dimanfaatkan oleh para pelaku kejahatan dengan memanipulasi dan memodifikasi *ciphertext* tersebut, sehingga menyebabkan kerusakan pesan yang dikirimkan.

Selain kriptografi, ada juga teknik yang dapat digunakan untuk pengamanan informasi atau pesan, yaitu teknik Steganografi. Steganografi adalah teknik menyembunyikan informasi dengan cara menyembunyikan pesan kedalam suatu media atau disebut dengan cover object yang tidak dapat dilihat dengan kasat mata sehingga tidak menimbulkan kecurigaan terhadap pesan tersebut. Namun dengan menggunakan teknik steganografi pun tidak menjamin informasi yang dikirimkan sudah benar-benar aman dari para pelaku kejahatan.

Dalam penelitian ini penulis akan mengkombinasikan steganografi dan kriptografi. Dimana steganografi akan menggunakan metode *End of File* (EoF), dan kriptografi akan menggunakan algoritma super enkripsi dengan menggunakan metode *Elliptic Curve Cryptography* (ECC) dan metode

Vigenere. Dengan ini penulis mengangkat penelitian dengan judul "HYBRID STEGANOGRAFI END OF FILE DAN KRIPTOGRAFI SUPER ENKRIPSI".

A. Penelitian Terkait

Terdapat beberapa penelitian sebelumnya yang terkait dengan steganografi dan kriptografi, yaitu sebagai berikut :

1) Steganografi Citra Menggunakan Kriptografi Hybrid Playfair Cipher dan Caesar Cipher. Penelitian ini merupakan penelitian terapan dibidang komputasi berkaitan dengan kriptografi playfair cipher dan caesar cipher serta steganografi, bertujuan untuk mengetahui konsep matematis kriptografi hybrid playfair cipher dan caesar cipher serta steganografi pada penyisipan pesan. Metode playfair cipher digunakan pada proses enkripsi dilanjutkan dengan metode caesar cipher. Hasil enkripsi dari gabungan kedua metode disisipkan pada citra (proses embedding). Simulasi Penyisipan Pesan yang telah dienkripsi disimulasikan dengan MATLAB sebagai alat bantu komputasi. Citra hasil simulasi disimpan dengan format bitmap (.bmp). Adapun bentuk matematika proses enkripsi pesan menggunakan hybrid playfair cipher dan caesar cipher yaitu $E(E(P,K1),K2) = C$, proses dekripsi yaitu $D(D(C, K2),K1) = P$ dan proses steganografi citra yaitu $M(K2(K1(P,K1),K2), G) = S$. Hasil penelitian ini menunjukkan bahwa dengan menggunakan gabungan metode kriptografi playfair cipher dan caesar cipher dalam penyandian, pesan yang disandikan semakin sulit dikembalikan kepesan asal oleh pihak yang tidak berwenang. Dengan menyisipkannya ke dalam citra membuat pengamat tidak menyadari adanya informasi yang disisipkan pada citra yang berperan sebagai pesan.[4]
2) Penggunaan Multiple Kriptografi Dan Steganografi Berbasis Android Untuk Penyembunyian Pesan Teks Pada Citra Digital. Perkembangan Teknologi yang semakin canggih, mengakibatkan kenyamanan bagi pengguna dalam memberikan segala informasi tanpa mengetahui ancaman–ancaman yang ada dibelakangnya, sehingga menjadikan sebuah kerugian dari perkembangan teknologi tersebut. Maka dari itu, dibutuhkan sebuah aplikasi yang memiliki aspek dalam segi keamanan teknologi dalam penyampain dan penerimaan informasi antara kepentingan diri sendiri maupun kepentingan kedua belah pihak. Dengan sebab itu, dibutuhkannya sebuah penarapan dari ilmu keamanan informasi yang dinamakan kriptografi dan Steganografi yang diimplementasikan kedalam sebuah perangkat hardware dan software. Banyak metode kriptografi yang dapat digunakan yaitu kriptografi klasik ataupun kriptografi modern. Pada penelitian ini mengkombinasikan kriptografi klasik dan modern yang dimana metode tersebut yaitu affine cipher, hill cipher, caesar cipher, dan advanced encrypt standard (AES). Sedangkan untuk steganografi, penelitian menggunakan metode least significant bit (LSB). Dari hasil penelitian yang diperoleh, menunjukan dengan menambah proses perhitungan pada kriptografi klasik dan mengkombinasikan dengan kriptografi modern memperkuat keamanan informasi. Keempat metode tersebut dapat dikombinasikan menjadi satu dalam proses kriptografi untuk menutupi kelemahan–kelemahan dari metode tersebut. Serta dengan melakukan proses kombinasi antara kriptografi dan steganografi, memberikan sebuah hasil dari segi keamanan pada pengelihatan, sehingga data informasi yang berlalu lalang bebas tidak memberikan kecurigaan sama sekali.[7]
3) Implementasi Algoritma Rivest Shamir Adlemant (Rsa) Pada File Citra. Keamanan data merupakan hal yang sangat penting bagi instansi maupun perusahaan. Salah satu data penting yang perlu diamankan adalah data citra. Citra merupakan pesan multimedia yang sering disalahgunakan. Sehingga diperlukan aplikasi untuk pengamanan data citra. Salah satu ilmu yang berkaitan dengan pengamanan adalah kriptografi. Algoritma Rivest Shamir Adlemant (RSA) merupakan salah satu algoritma kriptografi yang dapat digunakan untuk enkripsi dan dekripsi data. Keunggulan dari algoritma RSA adalah belum ditemukan algoritma yang tepat untuk melakukan dekripsi algoritma RSA dengan memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Oleh karena itu pada penelitian ini akan diimplementasikan algoritma RSA pada file citra. Proses pengamanan data citra pada penelitian ini dimulai dari pembangkitan kunci, enkripsi, dekripsi, dan pengujian. Pengujian yang dilakukan dalam penelitian ini meliputi pengujian pembangkitan kunci, pengujian citra terenkripsi, dan pengujian kemiripan menggunakan nilai MSE dan PSNR. Hasil dari penelitian ini dapat digunakan untuk mengenkripsi dan mendekripsi citra dengan baik. Pada pengujian pembangkitan kunci didapatkan hasil penggunaan kunci dengan rentang yang lebih besar dapat menghasilkan citra enkripsi yang sulit dikenali. Namun, hasil enkripsi pada algoritma ini ketika diuji menggunakan *enhancement*, *bluring*, dan *cropping* tidak dapat kembali sesuai citra aslinya. Dari hasil MSE dan PSNR antara citra asli dengan citra hasil dekripsi nilainya mendekati 0, namun tidak 100% mirip. Hal itu disebabkan ketika proses dekripsi ada beberapa nilai *pixel* citra yang tidak kembali sesuai nilai semula. [6]
4) Enkripsi dan Dekripsi Pesan Menggunakan Algoritma RSA dan Affine Cipher dengan Metode Matriks. Enkripsi merupakan proses mengubah suatu yang terbaca menjadi tidak terbaca, sedangkan dekripsi adalah kebalikan proses enkripsi yaitu mengubah suatu yang tidak terbaca menjadi terbaca. Terdapat dua algoritma yang sering digunakan yaitu algoritma simetri dan asimetri. Umumnya algoritma simetri cepat dalam proses enkripsi dan dekripsi tetapi kuncinya kurang aman, sedangkan algoritma asimetri umumnya lama dalam proses enkripsi dan dekripsi tetapi kuncinya sangat aman. Untuk mendapatkan proses enkripsi dan dekripsi yang cepat dan keamanan kunci yang kuat maka dapat menggabungkan algoritma simetri dengan asimetri yang disebut dengan algoritma hibrida. Pada penelitian ini proses enkripsi dan dekripsi pesan menggunakan algoritma simetri yaitu *affine cipher* dengan metode matriks menggunakan kunci sesi, sedangkan untuk

mengamankan kunci sesinya menggunakan algoritma asimetri yaitu RSA dengan kunci publik. Hasil yang didapatkan setelah proses enkripsi pesan adalah perubahan setiap karakter lebih dari satu selain itu kunci yang digunakan tidak terbatas hanya bergantung pada ukuran matriks dan determinannya harus relatif prima dengan modulo yang digunakan. Selain itu kunci sesi yang digunakan untuk mengenkripsi pesan juga diamankan dengan RSA yang terkenal sulitnya memfaktorkan bilangan bulat besar untuk mendapatkan faktor primanya. Keamanan proses enkripsi terletak pada keamanan kunci simetri sedangkan keamanan proses dekripsi terletak pada keamanan kunci asimetri. Pada penelitian selanjutnya disarankan menggunakan metode lain dalam mengamankan pesan.[8]

B. Steganografi

Steganografi adalah suatu ilmu yang mempelajari tentang penyembunyian pesan atau suatu informasi pada suatu media. Hasil dari steganografi akhirnya akan diekstrak pada tempat tujuan. Steganografi berasal dari bahasa Yunani, steganos yang berarti "tersembunyi" dan graphy berarti "tulisan". Terdapat banyak format file yang dapatt digunakan seperti teks, gambar, dan video, tetapi gambar digital dan audio adalah yang paling sering digunakan untuk menyembunyikan pesan.

Proses embedding dilakukan dengan menyisipkan pesan rahasia pada suatu cover file. Hasil dari proses embedding adalah versi modifikasi dari cover file atau disebut dengan stegofile. Setelah penerima telah menerima stegofile, penerima akan memulai proses ektraksi dengan stegofile dan key sebagai parameter. Jika key yang dimiliki penerima sama dengan key yang digunakan pengirim untuk menyisipkan pesan rahasia dan jika stego data yang digunakan oleh penerima sebagai input adalah data yang sama dengan yang dihasilkan pengirim, maka proses ekstraksi akan menghasilkan pesan rahasia asli.[1]

C. End of File (EoF)

End of File atau EoF adalah salah satu metode steganografi yang menyisipkan pesan pada bagian akhir suatu *file* dan merupakan metode yang dikembangkan dari metode *Least Significant Bit* atau LSB. EoF dapat digunakan untuk menyisipkan pesan yang memiliki ukuran sama dengan ukuran *file* sebelum disisipkan pesan ditambah dengan ukuran pesan yang disisipkan kedalam *file* tersebut. Pada metode EoF, pesan yang disisipkan pada akhir *file* akan diberi tanda khusus sebagai tanda pengenal awal dari pesan yang disisipkan dan pengenal akhir dari pesan tersebut.[2]

Prinsip kerja dari EoF adalah dengan menggunakan karakter khusus yang akan diberikan pada setiap bagian akhir file. Karakter khusus tersebut sering digunakan pada sistem operasi DOS sebagai penanda akhir dari penginputan data.

D. Kriptografi

Kriptografi merupakan ilmu yang mempelajari mengenai penyamaran pesan, dimana pesan yang dikirimkan hanya dapat dirubah, dihapus, maupun dibaca oleh penerima pesan yang dituju dan bukan pihak lain yang tidak berhak. Kriptografi berasal dari bahasa Yunani, *kryptos* yang berarti "tersembunyi" dan *graphein* yang artinya "menulis".

Kriptografi terdiri dari dua bagian utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana suatu pesan asli atau dalam hal ini disebut dengan *plaintext* diubah menjadi bentuk pesan acak atau disebut dengan *ciphertext* yang tidak dapat dipahami, hal ini bermaksud agar informasi yang dikirimkan terlindungi dari pihak yang tidak berhak. Sedangkan dekripsi adalah kebalikan dari enkripsi, dimana *ciphertext* akan diubah kembali kedalam bentuk *plaintext* atau pesan aslinya. [16]

Berdasarkan dari jenis kuncinya, algoritma kriptografi terbagi atas dua jenis, yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi. Algoritma asimetris dilain sisi, menggunakan sepasang kunci yang terdiri dari *private key* dan *public key*, dimana jika satu bagian dari kunci tersebut digunakan untuk mengenkripsi, maka kunci yang satunya lagi digunakan untuk mendekripsi.

E. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography adalah kriptografi kunci publik. Setiap pengguna atau perangkat yang berpartisipasi dalam komunikasi memiliki pasangan kunci, khususnya kunci publik dan kunci pribadi, dalam kriptografi kunci publik. Kunci pribadi yang cocok hanya dapat digunakan oleh pengguna yang cocok, sedangkan kunci publik dibagikan dengan entitas yang mengirim data. [11]

Rumus standar yang digunakan dalam membangun sebuah kurba eliptik pada algoritma ECC, yaitu

$$y^2 = x^2 + ax + b \ (mod\ p)$$

F. Vigenere Chiper

Vigenère *cipher* adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Cara kerja dari Vigenère *cipher* ini mirip dengan Caesar cipher, yaitu mengenkripsi plainteks pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet.[9][12]

Berikut merupakan contoh enkripsi menggunakan Vigenere *Chiper*:

Plain Text	T	H	E	S	K	Y	I	S	F	A	L	L	I	N	G
Kunci	E	N	C	O	D	E	E	N	C	O	D	E	E	N	C
Chiper Text	X	U	G	G	N	C	M	F	H	O	O	P	M	A	I

Gambar 1. Contoh Enkripsi Menggunakan Vigenere *Chiper*

Seperti contoh pada gambar 1 dapat kita lihat bahwa huruf "Y" dienkripsi dengan kunci "E" dan menghasilkan *ciphertext* "C". Hasil enkripsi didapatkan dari karakter pesan "Y" bernilai 24 dan karakter kunci "E" yang bernilai 4. Masing-masing nilai karakter ditambahkan 24 + 4 = 28. Karena 28 lebih besar dari pada 26 yang merupakan jumlah karakter yang digunakan, maka 28 dibagi dengan 26. Sisa pembagian tersebut adalah 2 yang merupakan nilai karakter "C". Proses enkripsi dapat dihitung dengan persamaan berikut:

$$Ei = (Pi + Ki)\ mod\ 26$$

dimana Ei, Pi dan Ki merupakan karakter hasil enkripsi, karakter pesan dan karakter kunci. Dan proses dekripsi dapat dihitung dengan persamaan berikut:

$$Di = (Ci - Ki)\ mod\ 26$$

dengan Di adalah karakter hasil dekripsi, Ci adalah karakter cipher text atau sandi, Ki adalah karakter kunci.[12]

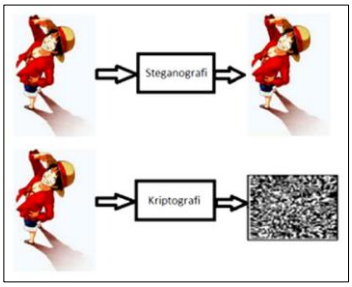
G. Perbedaan Steganography dan Cryptography

Berikut adalah perbedaan algoritma steganography dan cryptography adalah sebagai berikut ;

Tabel 1
Perbedaan Algoritma *Steganography* dan *Cryptography*

Steganography	Cryptography
Hasil keluaran dari steganography memiliki bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut adalah oleh indera manusia (khususnya visual), namun bila digunakan komputer atau perangkat pengolah digital lainnya dapat dengan jelas dibedakan antara sebelum proses dan setelah proses.	Hasil keluaran dari cryptography biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya data seolah-olah berantakan sehingga tidak dapat diketahui informasi apa yang terkandung didalamnya (namun sesungguhnya dapat dikembalikan ke bentuk semula lewat proses dekripsi).

Tabel 1 menjelaskan perbedaan antara algoritma cryptography dengan algoritma steganography. Perbedaan pada hasil keluaran dari algoritma cryptography adalah berupa data yang berbeda dengan bentuk aslinya, sedangkan untuk hasil keluaran algoritma steganography adalah berupa data yang sama dengan file aslinya. Adapun contoh gambar pada hasil keluaran steganografi dan kriptografi ditampilkan pada gambar 2 berikut ini :



Gambar 2. Contoh Perbedaan *Steganography* dan *Cryptography*

H. Kode ASCII

Kode ASCII (*American Standard Code for Information Interchange*) merupakan representasi numerik dari suatu karakter seperti ‘a’ atau ‘@’ atau karakter yang tidak tercetak, misalnya ‘Σ’. ASCII merupakan kombinasi kode 8 bit, yang terdiri atas 7 bit data dan 1 bit parity, sehingga mempunyai 27 atau 128 kode karakter yang berbeda dan unik yang terdiri dari bit 0 dan bit 1.[14]

Berikut adalah gambar tabel dari karakter ASCII:

Binary	Oct	Dec	Hex	Glyph
010 0000	040	32	20	␣
010 0001	041	33	21	!
010 0010	042	34	22	"
010 0011	043	35	23	#
010 0100	044	36	24	$
010 0101	045	37	25	%
010 0110	046	38	26	&
010 0111	047	39	27	'
010 1000	050	40	28	(
010 1001	051	41	29	)
010 1010	052	42	2A	*
010 1011	053	43	2B	+
010 1100	054	44	2C	,
010 1101	055	45	2D	-
010 1110	056	46	2E	.
010 1111	057	47	2F	/
011 0000	060	48	30	0
011 0001	061	49	31	1
011 0010	062	50	32	2
011 0011	063	51	33	3
011 0100	064	52	34	4
011 0101	065	53	35	5
011 0110	066	54	36	6
011 0111	067	55	37	7
011 1000	070	56	38	8
011 1001	071	57	39	9
011 1010	072	58	3A	:
011 1011	073	59	3B	;
011 1100	074	60	3C	<
011 1101	075	61	3D	=
011 1110	076	62	3E	>
011 1111	077	63	3F	?

Binary	Oct	Dec	Hex	Glyph
100 0000	100	64	40	@
100 0001	101	65	41	A
100 0010	102	66	42	B
100 0011	103	67	43	C
100 0100	104	68	44	D
100 0101	105	69	45	E
100 0110	106	70	46	F
100 0111	107	71	47	G
100 1000	110	72	48	H
100 1001	111	73	49	I
100 1010	112	74	4A	J
100 1011	113	75	4B	K
100 1100	114	76	4C	L
100 1101	115	77	4D	M
100 1110	116	78	4E	N
100 1111	117	79	4F	O
101 0000	120	80	50	P
101 0001	121	81	51	Q
101 0010	122	82	52	R
101 0011	123	83	53	S
101 0100	124	84	54	T
101 0101	125	85	55	U
101 0110	126	86	56	V
101 0111	127	87	57	W
101 1000	130	88	58	X
101 1001	131	89	59	Y
101 1010	132	90	5A	Z
101 1011	133	91	5B	[
101 1100	134	92	5C	\
101 1101	135	93	5D	]
101 1110	136	94	5E	^
101 1111	137	95	5F	_

Binary	Oct	Dec	Hex	Glyph
110 0000	140	96	60	`
110 0001	141	97	61	a
110 0010	142	98	62	b
110 0011	143	99	63	c
110 0100	144	100	64	d
110 0101	145	101	65	e
110 0110	146	102	66	f
110 0111	147	103	67	g
110 1000	150	104	68	h
110 1001	151	105	69	i
110 1010	152	106	6A	j
110 1011	153	107	6B	k
110 1100	154	108	6C	l
110 1101	155	109	6D	m
110 1110	156	110	6E	n
110 1111	157	111	6F	o
111 0000	160	112	70	p
111 0001	161	113	71	q
111 0010	162	114	72	r
111 0011	163	115	73	s
111 0100	164	116	74	t
111 0101	165	117	75	u
111 0110	166	118	76	v
111 0111	167	119	77	w
111 1000	170	120	78	x
111 1001	171	121	79	y
111 1010	172	122	7A	z
111 1011	173	123	7B	{
111 1100	174	124	7C	|
111 1101	175	125	7D	}
111 1110	176	126	7E	~

Gambar 3. Tabel Kode ASCII

I. Citra Digital

Citra digital adalah representatif dari suatu citra yang diambil oleh mesin dengan pendekatan sesuai dengan *sampling* dan kuantisasi. *Sampling* disini menyatakan besarnya kotak-kotak yang tersusun kedalam baris dan kolom. Dalam kata lain, *sampling* pada citra menggambarkan besar atau kecilnya ukuran dari *pixel* pada citra, dan kuantisasi disini menyatakan besarnya nilai dari tingkat kecerahan yang dinyatakan kedalam nilai tingkat keabuan atau *grayscale* sesuai dengan jumlah *bit* biner yang dipakai mesin, dalam kata lain kuatisasi pada citra merupakan jumlah dari warna yang ada pada citra. [18]

J. *MATLAB*

MATLAB adalah suatu sistem interaktif dimana elemen data dasarnya adalah *array* yang tidak membutuhkan dimensi. Hal ini memungkinkan kita untuk menyelesaikan masalah komputasi teknis, terutama dengan yang memiliki formulasi matriks dan *vector*, dalam waktu singkat untuk menulis sebuah program dalam Bahasa scalar non-interaktif seperti C atau Fortran.

II. METODE

A. Metode Penelitian

Metode penelitian yang digunakan adalah metode *engineering* dengan jenis *Forward Engineering*. Metode *engineering* merupakan penelitian yang memberikan hasil dapat berupa model, formula, algoritma, struktur, arsitektur, produk, maupun sistem yang telah teruji[15].

B. Metode Pengumpulan Data

Metode pengumpulan data dilakukan dengan melakukan studi literatur, mempelajari materi-materi untuk penelitian

kriptografi, steganografi, dan juga penggunaan program MATLAB.

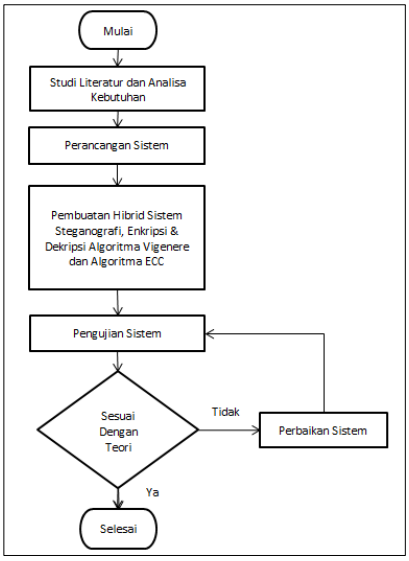
C. Metode Perancangan Sistem

Metode perancangan sistem meliputi dua bagian yaitu analisis sistem aktual dan perancangan sistem baru.

Analisis sistem aktual adalah menganalisa sistem yang saat ini digunakan dan dampaknya. Perancangan sistem baru yaitu merancang atau mempebaharui sistem yang sedang digunakan atau diimplementasikan saat ini.

D. Prosedur Penelitian

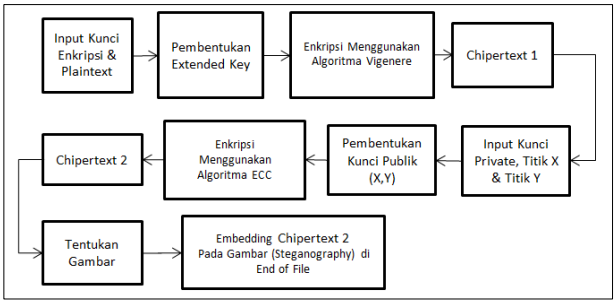
Dalam penelitian ini akan dihasilkan sistem *hybrid* steganografi dan kriptografi. Pada gambar 1 menjelaskan tentang alur prosedur penelitian dimana dimulai dengan studi literatur dan analisa kebutuhan, kemudian dilakukan perancangan sistem berdasarkan dengan materi yang telah dipelajari.



Gambar 4. Alur Pembuatan Sistem

E. Perancangan Aplikasi

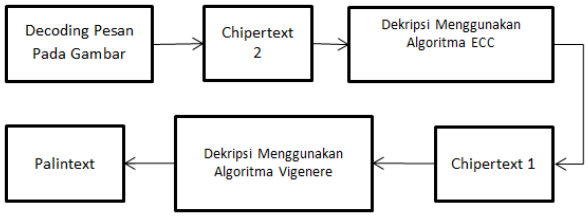
Perancangan sistem dibutuhkan untuk memudahkan penulis dalam mengilustrasikan sistem yang akan dibangun. Nantinya pada sistem yang dibangun ini akan memuat tiga buah proses yaitu enkripsi dan dekripsi menggunakan algoritma ECC, algoritma Vigenere serta proses penyisipan pesan dengan teknik steganographi pada *end of file*. Berikut adalah ilustrasi dari sistem yang akan dibangun,



Gambar 5. Diagram Blok Proses Enkripsi dan *Embedding* Pesan

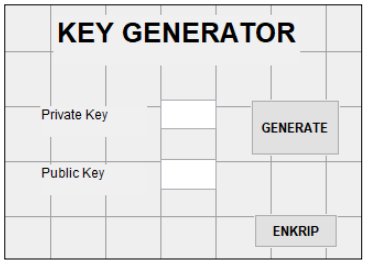
Berdasarkan blok diagram tersebut, diketahui bahwa proses enkripsi *plaintext* atau pesan rahasia pertama akan dienkripsi menggunakan algoritma ECC. Hasil enkripsi berupa *chipertext* (untuk selanjutnya diberi nama *chipertext 1*) akan menjadi inputan (*plaintext*) untuk proses enkripsi selanjutnya yaitu menggunakan algoritma Vigenere. Dari proses enkripsi menggunakan algoritma Vigenere akan dihasilkan *chipertext 2*. *Chipertext 2* ini nantinya akan di-*embed* atau disisipkan kedalam gambar pada posisi *end of file* yang telah disediakan melalui proses steganography.

Selanjutnya setelah proses enkripsi dan *embedding* berhasil dilakukan, proses selanjutnya berupa proses pengembalian (dekripsi dan decoding) pesan. Berikut adalah blok diagram untuk pengembalian pesan tersebut.

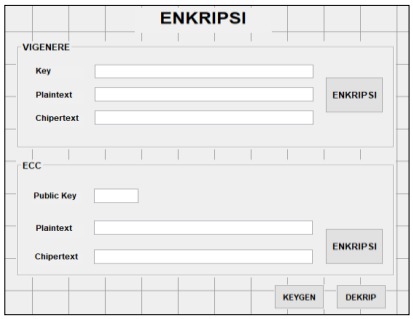


Gambar 6. Blok Diagram Proses Dekripsi dan *Decoding* Pesan

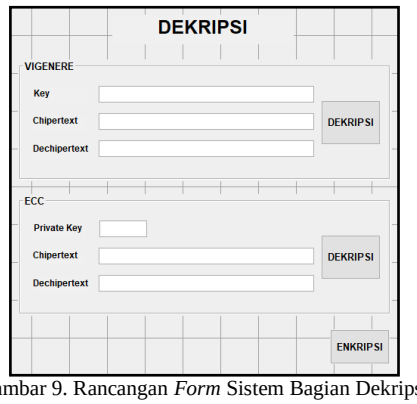
Proses dekripsi diawali dengan mengambil pesan dari gambar. Selanjutnya setelah pesan (*chipertext 2*) telah berhasil dimbail, proses berikutnya adalah melakukan proses dekripsi *chipertext 2* menggunakan algoritma Vigenere. Setelah proses dekripsi menggunakan algoritma Vigenere berhasil dilakukan maka selanjutnya akan didapat *output chipertext 1*. *Output chipertext 1* akan dilakukan proses dekripsi menggunakan algoritma ECC. Sehingga hasil akhirnya berupa *plaintext* atau pesan yang sama ketika awal diinput.



Gambar 7. Rancangan *Form* Sistem Bagian *Key Generator*



Gambar 8. Rancangan *Form* Sistem Bagian Enkripsi



Gambar 9. Rancangan *Form* Sistem Bagian Dekripsi

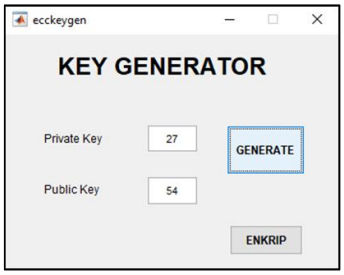
III. HASIL DAN PEMBAHASAN

Aplikasi dirancang dan dibuat dengan *tools* MATLAB. Bahasa pemrograman yang akan digunakan dalam pembuatan aplikasi adalah MATLAB sebagai bahasa utama dan *GUIDE* yang merupakan salah satu komponen dari MATLAB untuk membuat tampilan *user interface*.

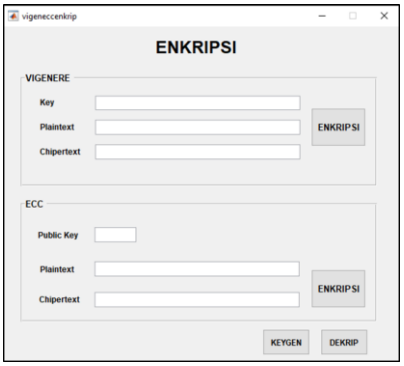
A. Pengujian Aplikasi

Pada pengujian ini dimaksudkan untuk membuktikan jawaban yang dihasilkan konventer sesuai dengan jawaban menggunakan rumus atau algoritma yang digunakan.

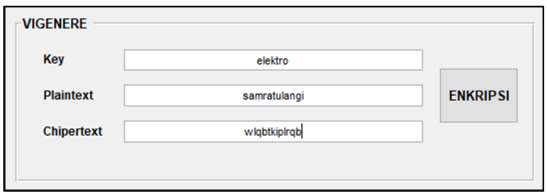
Aplikasi yang dibuat terbagi atas tiga buah bagian. Masing-masing adalah bagian untuk proses enkripsi dan dekripsi dengan menggunakan algoritma ECC. Selanjutnya bagian untuk proses enkripsi dan dekripsi dengan menggunakan algoritma Vigenere. Dan yang ketiga adalah bagian untuk proses menyisipkan pesan pada bagian akhir gambar serta membaca kembali pesan yang disembunyikan. Berikut adalah tampilan dari aplikasi yang dibuat.



Gambar 10. Tampilan Proses Pembakitan *Private* dan *Puublic Key*



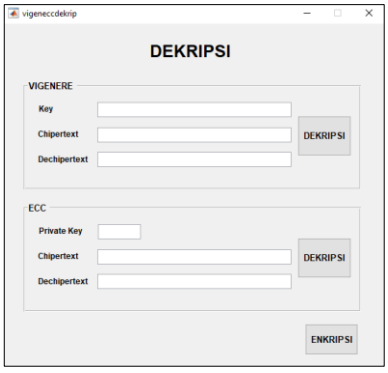
Gambar 11. Tampilan dari Sistem Bagian Enkripsi



Gambar 12. Tampilan Proses Enkripsi Algortima Vigenere pada Sistem

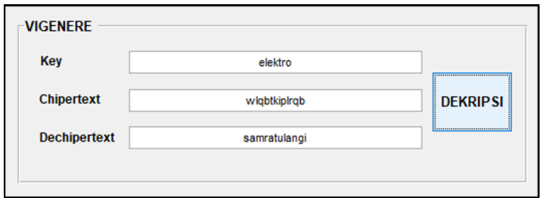
Gambar 13. TampilanProses Enkripsi Algoritma ECC pada Sistem

Gambar 10 adalah proses pembangkitan *private* dan *public key* yang akan digunakan pada saat mengenkripsi dan Mendekripsi menggunakan metode ECC. Ketika telah selesai membangkitkan *key* proses selanjutnya adalah melakukan proses enkripsi dengan menggunakan metode Vigenere setelahh itu ECC seperti yang bisa dilihat pada gambar 11, 12 dan 13.



Gambar 14. Tampilan dari Sistem Bagian Dekripsi

Gambar 15. Tampilan Proses Dekripsi Algoritma ECC pada Sistem



Gambar 16. Tampilan Proses Dekripsi Algortima Vigenere pada Sistem

Berikutnya adalah proses dekripsi pesan dari *chipertext* akan dikembalikan lagi seperti semula yaitu *plaintext* seperti yang dapat dilihat pada gambar 14, 15 dan 16.

IV. KESIMPULAN DAN SARAN

A. *Kesimpulan*

Dari pengujian fungsional serta pengujian akurasi perhitungan yang telah dilakukan dapat diambil kesimpulan adalah sebagai berikut :

1. Dari pengujian fungsionalitas dan akurasi perhitungan diketahui bahwa penggunaan algortima Vigenere serta algoritma ECC dapat dengan baik melakukan proses enskripsi dan dekripsi dari pesan yang diinputkan.
2. Dari pengujian fungsionalitas dan akurasi perhitungan pada proses steganografi diketahui bahwa pesan text berhasil disisipkan (disembunyikan) pada bagian akhir dari file sebuah citra. Tetapi tidak berhasil kembali diekstrak dari file citra, sehingga pesan tidak dapat dibaca kembali.

B. *Saran*

Berikut ini adalah saran untuk pengembangan dan penyempurnaan sistem *hybrid* menggunakan metode steganografi, enkripsi dan dekripsi menggunakan algortima Vigenere dan algoritma ECC ini adalah sebagai beikut,

1. Memberikan proses validasi pada inputan plaintext, sehingga proses perhitungan dapat dilakukan sebagaimana yang telah direncanakan.
2. Gambar pada proses penyisipan pesan pada proses steganografi sebaiknya dapat dirubah-rubah sehingga pengguna tidak bosan dan mengurangi kecurigaan dari pihak yang tidak diinginkan. Selain itu disarankan untuk dapat mencoba menggunakan berbagai macam metode lainnya untuk memperluas pengetahuan mengenai algoritma steganografi.

V. KUTIPAN

[1] Sheelu, Babita Ahuja. 2013. *An Overview of Steganography*. 11 (1):15-19

[2] Yayuk Anggraini, Dolly Virgian Shaka, Yudha Sakti. 2014. *Penerapan Steganografi Metode End Of File (EoF) Dan Enkripsi Metode Data Encryption Standard (DES) Pada Aplikasi Pengamanan Data Gambar Berbasis Java Programming*.1743-1753.

[3] Eko Ibrahim Ahmad. 2016. *Hibrid Kriptografi Dan Steganografi Menggunakan RSA Dan AMELSBR [Skripsi]*. Bandar Lampung. Universitas Lampung.

[4] Nurul Fitriani Andi Mu'Mi. 2017. *Steganografi Citra Menggunakan Kriptografi Hybrid Playfair Cipher Dan Caesar Cipher [Skripsi]*. Makassar. Universitas Negeri Makassar.

[5] Fitri Rachmawati. 2016. *Aplikasi Steganografi Berbasis Dekstop Dengan Menggunakan Metode Pvd (Pixel Value Differencing) Dan Enkripsi Pesan Rahasia Dengan Pembangkit Bilangan Acak Lcg (Linear Congruential Generator) Pada Pt Primatama Duta Antaran [Skripsi]*. Jakarta. Universitas Budi Luhur.

[6] Nofa Raihana Fajriyah. 2018. *Implementasi Algoritma Rivest Shamir Adlemant (Rsa) Pada File Citra [Skripsi]*. Universitas Negeri Sunan Ampel Surabaya.

[7] M Agus Khamsinindo, 2020. *Penggunaan Multiple Kriptografi Dan Steganografi Berbasis Android Untuk Penyembunyian Pesan Teks Pada Citra Digital [Skripsi]*. Universitas Islam Indoensia.

[8] Qorny, Muhamad Wais Al. 2018. *Enkripsi dan Dekripsi Pesan Menggunakan Algoritma RSA dan Affine Cipher dengan Metode Matriks [Skripsi]*. Universitas Islam Negeri Maulana Malik Ibrahim Malang.

[9] Wina Ayu Lestari, Rohmat Tulloh, S.T., M.T., Atik Novianti, S.ST.,M.T. 2019. *Media Pembelajaran Interaktif Enkripsi Caesar Cipher, Vigenere Cipher, dan Algoritma RSA [Jurnal]*. Universitas Telkom.

[10] Laiphrakpam Dolendro Singh, Khumanthem Manglem Singh. 2015. *Implementation of Text Encryption using Elliptic Curve Cryptography [Jurnal]. National Institute of Technology, Manipur, Imphal East 795 001, India*.

[11] Andreas Dwi Nugroho, Rinaldi Munir. 2015. *Aplikasi Enkripsi Instant Messaging Pada Perangkat Mobile Dengan Menggunakan Algoritma Elliptic Curve Cryptography (ECC) [Jurnal]*. Institut Teknologi Bandung.

[12] Muhammad Dedi Irawan. 2017. *IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP [Jurnal]*. Universitas Asahan.

[13] Tuti Alawiyah , Rian Ardianto, Dini Silvi Purnia. 2020. *Implementasi Vigenere Cipher Sebagai Pengaman Pada Proses Deskripsi Steganografi Least Significant Bit [Jurnal]*. Universitas Bina Sarana Informatika

[14] Peter Loshin. *ASCII (American Standard Code for Information Interchange).* https://www.techtarget.com/whatis/definition/ASCII-American-Standard-Code-for-Information-Interchange. Diakses 1 Mei 2019

[15] Margaret Rouse. 2014. *RSA Algorithm (Rivest Shamir Adleman).* https://searchsecurity.techtarget.com/definition/RSA. Diakses 6 Desember 2019.

[16] *Practical Cryptography*. Website. http://practicalcryptography.com/ciphers/caesar-cipher/#references. Di akses 6 Desember 2019.

[17] Website https://cimss.ssec.wisc.edu/wxwise/class/aos340/spr00/whatismatlab.htm. Di akses 6 Desember 2019.

[18] Muchlisin Riadi. 2016. *Pengolahan Citra Digital*. https://www.kajianpustaka.com/2016/04/pengolahan-citra-digital.html. Diakses 6 Desember 2019.

TENTANG PENULIS

Penulis bernama lengkap Muhammad Rivaldy Cadullah , lahir di Manado pada tanggal 5 Mei 1999. Penulis telah menyelesaikan studi di Sekolah Dasar Negeri 11 Manado pada tahun 2010, setelah itu melanjutkan studi di Sekolah Menengah Pertama Negeri 1 Manado dan lulus pada tahun 2013 dan pada tahun yang sama melanjutkan studi di Sekolah Menengah Atas Negeri 9 Binsus Manado dan lulus pada tahun 2016. Melanjutkan pendidikan strata satu (S1) di Fakultas Teknik Jurusan Teknik Elektro Program Studi Informatika Universitas Sam Ratulangi Manado yang dimulai pada bulan Juli 2016 melalui jalur Seleksi Bersama Masuk Perguruan Tinggi Negeri (SBMPTN) pada tahun 2016. Aktif dalam organisasi Himpunan Mahasiswa Elektro dan beberapa kegiatan Kerohanian Islam Fakultas Teknik.