1. Pendahuluan

Saat ini sering terjadi kasus kriminal yang menyangkut tentang keamanan dari suatu data berupa citra digital. Permasalahan ini terjadi dikarenakan belum banyak fasilitas untuk keamanan citra digital (*image*) yang dimiliki seseorang. Menurut beberapa media berita seperti detiknews.com sering dijumpai kasus-kasus beredarnya foto-foto yang berbau pornografi milik pribadi seseorang yang telah diekspos oleh orang yang tidak bertanggung jawab. Contoh kasus yang ada seperti ayu ashari, ariel peterpan, luna maya dan beberapa tokoh lainnya yang menjadi korban dari kurangnya keamanan pada data berupa citra digital.

Untuk mengatasi permasalahan tersebut dapat dibangun sebuah aplikasi kriptografi yang bertujuan mengamankan citra digital khususnya *raw file image*. Pada aplikasi tersebut pengguna dapat menyimpan foto-foto pribadi miliknya dengan menggunakan kunci dan tidak dapat di buka oleh orang lain kecuali dirinya sendiri. Salah satu algoritma yang dapat digunakan untuk mengenkripsi sebuah *raw file iamge* adalah algoritma AES (*Advanced Encryption Standard*). Dalam penelitian ini membahas tentang implementasi algoritma AES pada enkripsi-dekripsi citra digital. Pengimplementasian algoritma AES pada enkripsi-dekripsi citra digital ini dilakukan untuk memberikan keamanan suatu data dan informasi yang dimiliki sehingga menghasilkan suatu informasi yang efektif.

Berkaitan dengan solusi tersebut, muncul sebuah gagasan untuk menerapkannya dalam skripsi berjudul "Implementasi Algoritma *Advanced Encryption Standard* pada Enkripsi-Dekripsi *Raw File Image*". Metode yang digunakan dalam penelitian ini menggunakan algoritma AES (*Advanced Encryption Standard*) untuk proses enkripsi dekripsi dan untuk data citra digital dapat disimpan pada *database* sehingga dengan aplikasi tersebut dapat mewujudkan kerahasiaan pada sebuah data karena yang dapat mengakses hanya pengguna yang mengetahui kunci enkripsi dekripsi algoritma AES. Aplikasi yang digunakan dalam penelitian ini menggunakan teknologi *Framework.Net* dengan bahasa pemograman VB.Net dan *database* yang digunakan adalah *MySql*. Tujuan dari penelitian ini yaitu merancang sistem enkripsi-dekripsi citra digital yang mampu memberikan keamanan *raw file* citra digital (*image*), mengimplementasikan algoritma AES (*Advanced Encryption Standard*) pada sistem enkripsi-dekripsi citra digital, mengetahui dan membuktikan sistem enkripsi-dekripsi dapat dipergunakan untuk semua jenis format *image* atau citra digital, serta mengetahui dan membuktikan algoritma AES tidak dapat mempengaruhi perubahan spesifikasi (warna, ukuran dan resolusi) *raw file* citra digital. Selain itu manfaat yang didapat dari penelitian ini adalah memberikan keamanan data berupa citra digital sehingga hanya pengguna yang memiliki wewenang atau izin akses dapat menampilkan citra digital tersebut dan memberikan alternatif pengelolaan penyimpanan citra digital yang aman dilindungi dengan algoritma AES (*Advanced Encryption Standard*) yang tersimpan di dalam suatu *database server*. Sehingga untuk mempersempit masalah yang bakal muncul pada penelitian maka perlu adanya pembatasan masalah sebagai berikut: satu, algoritma kriptografi AES (*Advanced Encryption Standard*) yang dipergunakan menggunakan *chiper key* berukuran 128 bit, yaitu panjang kuncinya berukuran 4 *word* dan untuk tiap *word*-nya berukuran 32 bit.

Mode *hash* yaitu mode ECB; dua, tidak membahas dan membandingkan mode *hash* yang dipergunakan pada algoritma kriptografi AES; tiga, tidak membahas *encoding hash* MD5 pada kunci enkripsi dan dekripsi algoritma AES; empat, *database Server* yang dipergunakan adalah *MySql Server*; lima, tidak membahas teknologi aplikasi *client-server* yang dipergunakan pada sistem enkripsi-dekripsi citra digital.

2. Kajian Pustaka

Pada penelitian-penelitian terdahulu, banyak peneliti menggunakan macam-macam algoritma kriptografi untuk mengamankan data yang dimiliki. Salah satunya adalah penelitian yang berjudul "Implementasi Algoritma *Chaos-Based Feedback Stream Cipher* pada Enkripsi-Dekripsi Data Citra Digital." Pada penelitian ini sangat memberikan gambaran tentang fungsi dan kegunaan dari setiap algoritma yang akan diterapkan pada aplikasi keamanan data [1].

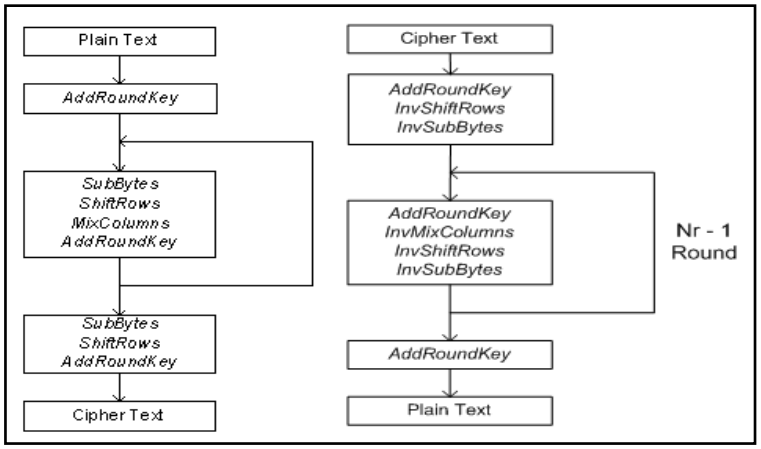
Penelitian yang berjudul "Enkripsi Gambar Menggunakan Algoritma Secure Image Protection" memberikan gambaran tentang proses mengamankan informasi citra dengan membangun suatu aplikasi untuk menyembunyikan informasi citra tersebut dengan menggunakan metode *Secure Image Protection*. Penelitian [2].

Berdasarkan penelitian yang pernah dilakukan terkait Enkripsi-Dekripsi, maka akan dilakukan penelitian yang membahas tentang algoritma *advanced encryption standard* pada enkripsi-dekripsi *raw file* citra digital (*image*). Aplikasi yang dibangun menggunakan algoritma kriptografi yang berfungsi untuk pengenkripsian *file* gambar. Penelitian ini dapat memberikan keamanan suatu data dan informasi yang dimiliki, sehingga menghasilkan suatu informasi yang efektif. Perbedaan dengan perancangan sebelumnya adalah algoritma yang digunakan berbeda serta data *file* yang dienkripsikan berbeda.

Raw file image adalah bagian *file image* yang berisi tentang informasi gambar asli yang diperoleh dari alat sensor kamera saat pengambilan *image* tersebut [3]. Sehingga, untuk dapat memproses *raw file image* harus menggunakan piranti lunak (*software*) khusus dari perangkat komputer.

Algoritma AES merupakan algoritma kriptografi yang menggunakan kriptografi simetris atau *block chiper* simetris untuk proses enkripsi dan dekripsi. Proses enkripsi dan dekripsi algoritma AES memproses data masukan berukuran 128 bit menggunakan *cipher key* berukuran 128, 192 dan 256 bit [4].

Garis besar algoritma AES yang beroperasi pada blok 128 bit dengan kunci 128 bit adalah sebagai berikut: Transformasi *AddRoundKey*, Putaran sebanyak *Nr*–1 kali, *Final round* [4]. Garis besar algoritmaAES ditunjukkan pada Gambar1.



Gambar 1. Diagram Proses Enkripsi dan Dekripsi [4]

Basis data *(database)* merupakan suatu bentuk pengorganisasian sekumpulan data yang saling terkait sehingga memudahkan aktivitas untuk memperoleh informasi. Suatu basis data yang berbasis komputer dibuat dan dipelihara oleh sekumpulan program aplikasi yang ditulis secara khusus untuk menyelesaikan masalah tertentu atau dengan menggunakan suatu Sistem Manajemen Basis Data *(Database Management System)*. Sistem Manajemen Basis Data merupakan suatu perangkat lunak yang terdiri atas sekumpulan program untuk mengelola dan memelihara data di dalam suatu struktur yang digunakan oleh banyak aplikasi, bebas terhadap media penyimpanan dan metode akses [5].

Transformasi yang digunakan Base64 yang dimana salah satu algoritma untuk *encoding* dan *decoding* suatu data ke dalam format kode ASCII, yang didasarkan pada bilangan 64. Karakter yang dihasilkan dari Base64 terdiri dari A-Z , a-z dan 0..9, serta ditambah dengan 2 karakter terakhir yaitu / dan +. Karakter dalam transformasi base64 tersusun dalam tabel *index* data pada Gambar 2 [6].

Base64 index table							
value	char	value	char	value	char	value	char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Gambar 2 Tabel Base64 [6]

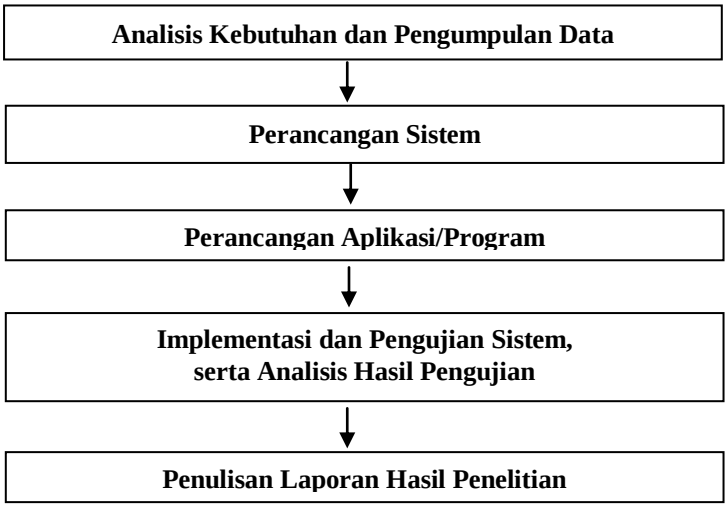
Pengertian citra digital adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra terbagi 2 yaitu ada citra yang bersifat analog dan ada citra yang bersifat digital. Citra analog adalah citra yang bersifat kontinu seperti gambar pada monitor televisi, foto sinar X, hasil CT Scan dll. Sebuah citra digital dapat mewakili oleh sebuah matriks yang terdiri dari M kolom N baris, dimana perpotongan antara kolom dan baris disebut piksel (piksel = *picture element*), yaitu elemen terkecil dari sebuah citra. Piksel mempunyai dua parameter, yaitu koordinat dan intensitas atau warna. Nilai yang terdapat pada koordinat (x,y) adalah f(x,y), yaitu besar intensitas atau warna dari piksel di titik itu. Oleh sebab itu, sebuah citra digital dapat ditulis dalam bentuk matriks seperti terlihat pada Gambar 3 [7].

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M-1) \\ f(1,0) & \dots & \dots & f(1,M-1) \\ \dots & \dots & \dots & \dots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,M-1) \end{bmatrix}$$

Gambar 3. Matrik representasi citra digital [7]

3. Metode dan Perancangan Sistem

Penelitian yang dilakukan, diselesaikan melalui tahapan penelitian yang terbagi dalam lima tahapan, yaitu: (1) Analisis kebutuhan dan pengumpulan data, (2) Perancangan sistem, (3) Perancangan aplikasi/program, (4) Implementasi dan pengujian sistem, serta analisis hasil pengujian, (5) Penulisan laporan hasil penelitian.



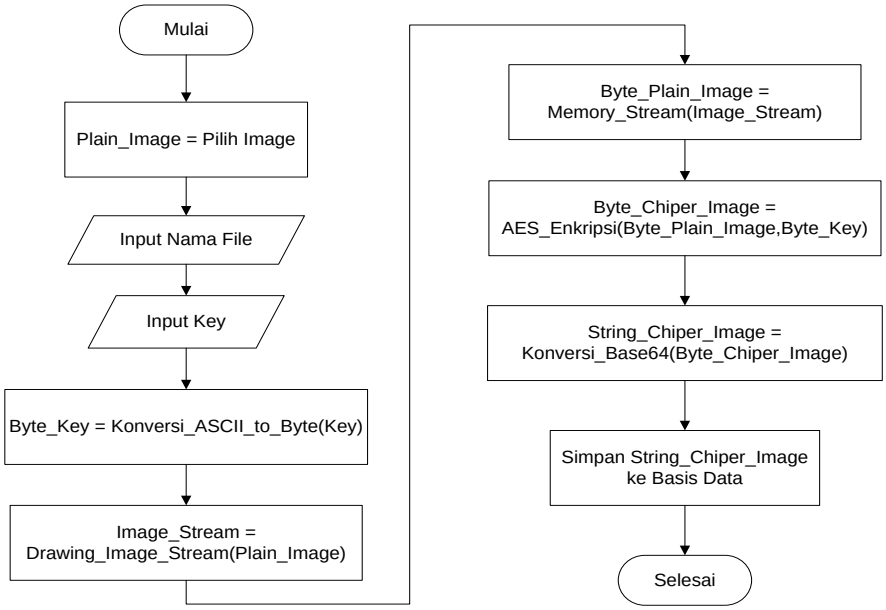
Gambar 4. Tahapan Penelitian

Tahapan penelitian pada Gambar 4, dapat dijelaskan sebagai berikut:

Tahap pertama: analisis kebutuhan dan pengumpulan data. Terdapat dua analisis kebutuhan, yaitu kebutuhan pengguna dan kebutuhan sistem. Analisis kebutuhan adalah menganalisis kebutuhan pengguna yang muncul disebabkan karena permasalahan yang ada yaitu kebutuhan pengguna dalam mengamankan citra digital. Sedangkan pengumpulan data merupakan kegiatan yang dilakukan untuk

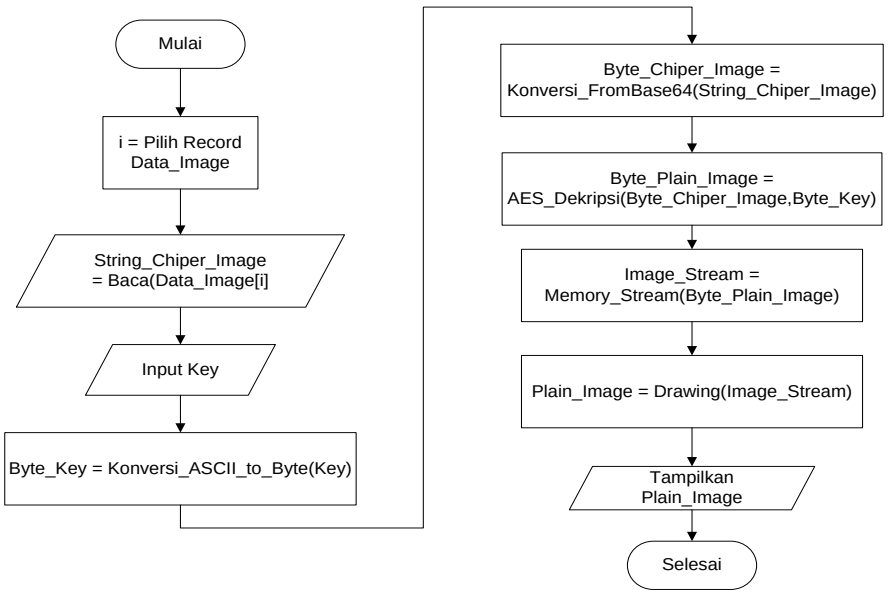
mendapatkan data dan informasi yang terkait dengan aplikasi yang dibangun, misalnya data *image* dan referensi pustaka tentang algoritma AES dan citra digital. Berdasarkan perumusan masalah maka ditentukan bahwa aktor didalam aplikasi adalah tunggal, yaitu pengguna (*user*) sehingga tidak ada pembagian hak akses terhadap pengguna. Hasil analisis kebutuhan pengguna adalah bahwa sistem atau aplikasi mampu melakukan enkripsi dekripsi terhadap suatu *image* dan menyimpan data *image* pada suatu *server* basis data tanpa merubah kualitas dan spesifikasi *image*. *Tahap kedua:* perancangan sistem adalah merancang aplikasi/program sesuai kebutuhan sistem berdasarkan perancangan sistem yang telah dilakukan. Misalnya bagaimana proses enkripsi terhadap *file* gambar, apakah *file* enkripsi dapat kembali serupa dengan *file original*, ada perubahan pada ukuran gambar, pengaruh kunci pada hasil enkripsi; *Tahap ketiga*, perancangan aplikasi/program meliputi perancangan aplikasi menggunakan *Unified Modelling Language* (UML) karena bahasa pemrograman yang digunakan adalah VB.Net adalah pemrograman berorientasi obyek. Kemudian perancangan arsitektur dari sistem yang dibangun, perancangan antarmuka, yaitu merancang antarmuka yang berfungsi sebagai penghubung interaksi antara *user* dengan sistem berupa tampilan *interface* aplikasi kriptografi yang dibuat yaitu aplikasi untuk enkripsi *file* gambar; *Tahap keempat:* implementasi dan pengujian sistem, serta analisis hasil pengujian, yaitu mengimplementasikan tahapan penelitian kedua dan ketiga ke dalam sebuah program, apabila implementasi program sudah selesai, maka dilakukan pengujian, serta dianalisis untuk melihat apakah aplikasi yang telah dibuat sudah sesuai dengan yang diharapkan atau tidak ada *error*, jika belum sesuai maka akan dilakukan perbaikan; *tahap kelima,* penulisan laporan hasil penelitian, yaitu mendokumentasikan proses penelitian yang sudah dilakukan dari tahap awal hingga akhir ke dalam tulisan, yang nantinya akan menjadi laporan hasil penelitian.

Pada tahap ini, dilakukan perancangan proses sistem enkripsi-dekripsi citra digital yang menerapkan algoritma kriptografi AES untuk digunakan didalam aplikasi. Perancangan menggunakan diagram alir *(flowchart*) yang terdiri dari proses enkripsi dan proses dekripsi *image*. Pada aplikasi yang dibangun, proses enkripsi merupakan sebuah proses sistem yang melakukan enkripsi *image*, diawali dari proses pemilihan *file image* sebagai data *plaintext*, kemudian dienkripsi lalu hasilnya (*chipertext*) disimpan kedalam basis data. Untuk dapat lebih jelas dapat dilihat pada Gambar 5.



Gambar 5. Diagram Alir Proses Enkripsi Citra Digital

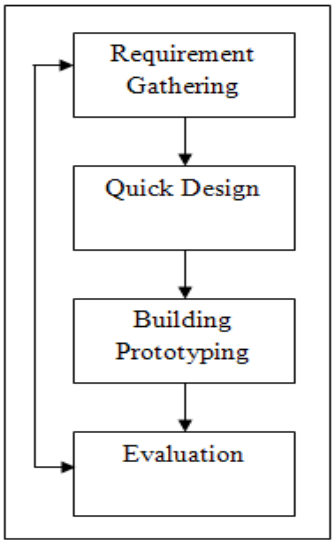
Pada tahap ini dilakukan perancangan alur dekripsi citra digital, suatu proses sistem yang melakukan dekripsi data *Chipertext* hasil proses enkripsi, diawali dari proses pengambilan data *chiper image* di basis data sebagai data *ChiperText*, kemudian didekripsi lalu hasilnya ditampilkan pada aplikasi. Untuk dapat lebih jelas dapat dilihat pada Gambar 6.



Gambar 6. Diagram Alir Proses Dekripsi Citra Digital

Metode yang digunakan dalam perancangan sistem adalah *prototyping model*. Metode *Prototyping* dipilih karena *prototype* yang dibuat dapat digunakan untuk

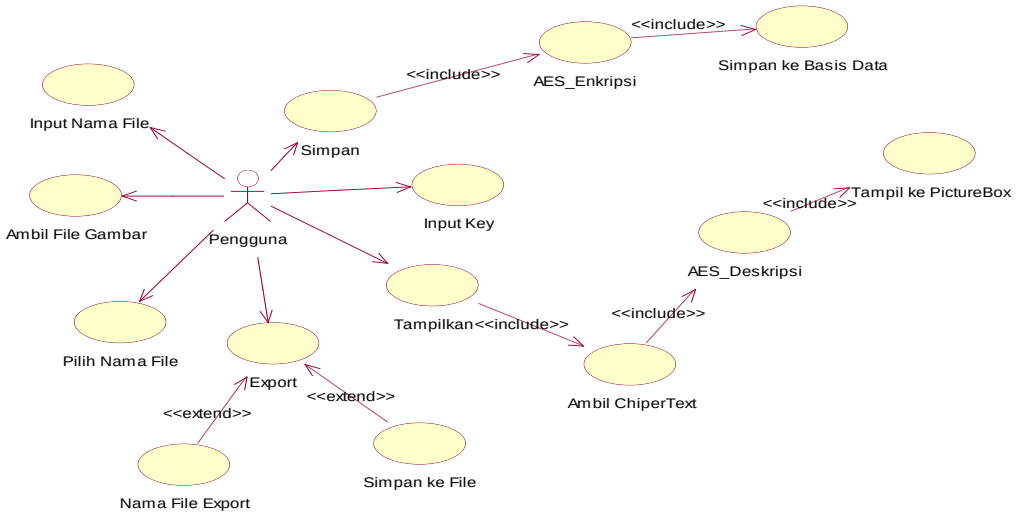
mengelola kembali kebutuhan dari perangkat lunak yang akan dikembangkan, sehingga pengembang perangkat lunak tidak harus merancang lagi semua dari awal. Model metode *prototyping* dapat ditunjukkan pada Gambar 7.



Gambar 7. *Prototyping Model* (Pressman, 2000) [8]

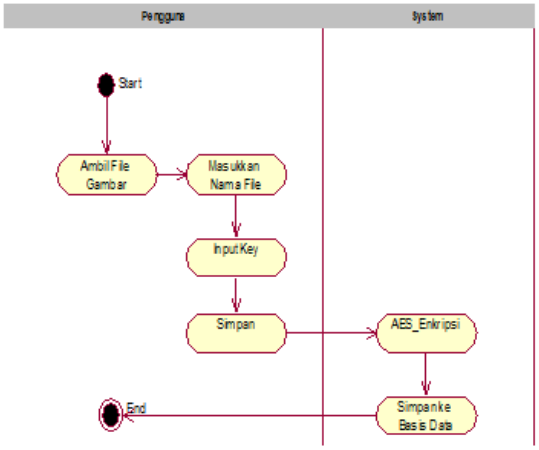
UML *(Unified Modeling Language)* adalah bahasa standar untuk melakukan spesifikasi, visualisasi, konstruksi dan dokumentasi dari komponen-komponen perangkat lunak. Hasil perancangan aplikasi menggunakan UML akan dipaparkan sebagai berikut.

Use case diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem, sehingga yang ditekankan adalah "apa" yang diperbuat sistem, dan bukan "bagaimana". Gambar 8 menjelaskan bahwa pada *use case diagram* terdapat hanya seorang aktor yaitu pengguna. Pengguna dapat melakukan empat (4) pokok proses, yaitu: Pertama, ambil *file* gambar sebagai *file* citra digital; Kedua, simpan yaitu melakukan enkripsi AES citra digital yakni *file* gambar dengan *key* yang telah dimasukkan, kemudian menyimpan ke basis data dengan nama *file* yang telah di-inputkan oleh pengguna; Ketiga, tampilkan yaitu menampilkan citra digital yang tersimpan di basis data ke *pictureBox* yang telah ditentukan dengan melakukan proses dekripsi AES dengan *key* yang di-*input*kan pengguna; Keempat, *Export* yaitu menyimpan citra digital yang tampil di *pictureBox* kedalam penyimpanan eksternal dengan nama *file* yang ditentukan oleh pengguna.

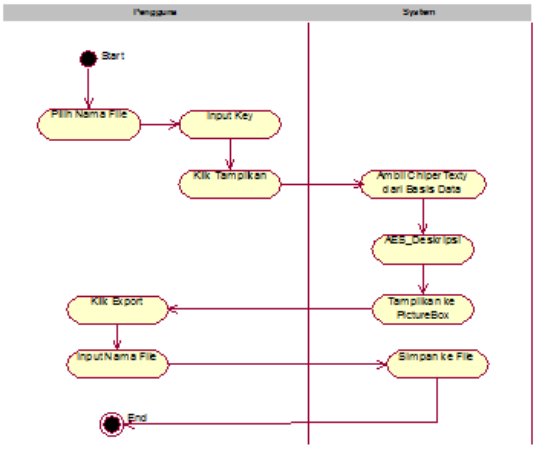


Gambar 8. *Use Case Diagram* Sistem

Activity diagram menggambarkan berbagai alir aktivitas dalam sistem yang dirancang sesuai aktor, sehingga *activity diagram* dapat menjelaskan bagaimana masing-masing alir berawal, *decision diagram* juga dapat menggambarkan proses paralel yang mungkin terjadi pada beberapa eksekusi. Pada penelitian ini, aktivitas utama dari sistem adalah proses enkripsi-dekripsi *raw* berkas citra digital. Dengan demikian, terdapat 2 (dua) aktivitas utama yaitu aktivitas enkripsi citra digital dijelaskan pada Gambar 9, dan aktivitas dekripsi citra digital dijelaskan pada Gambar 10.

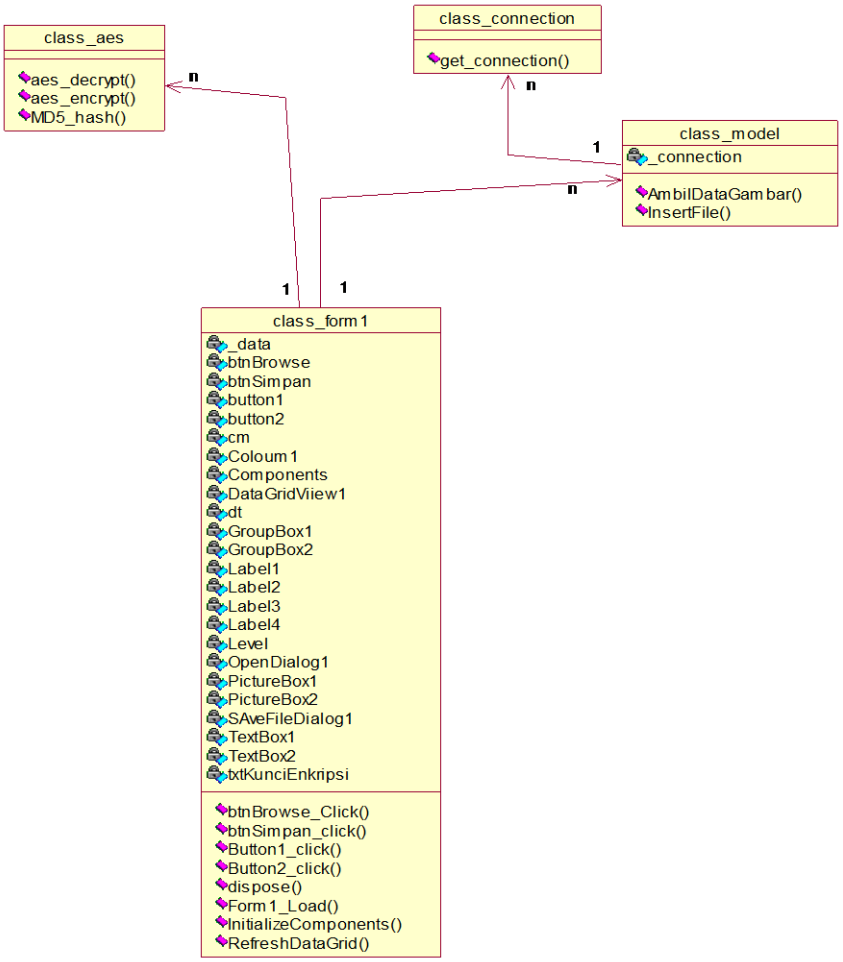


Gambar 9. *Activity Diagram* Enkripsi Citra Digital



Gambar 10. *Activity Diagram* Dekripsi Citra Digital

Class adalah sebuah spesifikasi yang akan menghasilkan sebuah obyek dan merupakan inti dari pengembangan dan desain pemrograman berorientasi obyek. *Class* menggambarkan keadaan berupa atribut/properti suatu sistem, sekaligus menyediakan layanan untuk memanipulasi keadaan atau entitas yang disebut metode atau fungsi. *Class Diagram* aplikasi enkripsi dekripsi citra digital dapat dilihat pada Gambar 11.



Gambar 11.*Class Diagram* Aplikasi

Class diagram juga menggambarkan struktur dan dekripsi *class*, *package* dan obyek beserta hubungan satu sama lain seperti pewarisan, asosiasi, dan lain-lain. Pada Gambar 11 terlihat bahwa aplikasi memiliki 4 (empat) *class*, antara lain Class_Form1, Class_aes, Class_connection dan Class_Model.

Class_Form1 memiliki relasi dengan Class_aes yaitu relasi *one to many* karena class_Form1 dapat memanggil prosedur enkrip dan dekrip yang dimiliki pada Class_aes. Class_Form1 juga memiliki relasi dengan Class_Model yaitu relasi *one to many* karena pada Class_Form1 untuk menyimpan data *byte* hasil enkrip dan dekrip citra digital. Sedangkan Class_Model memiliki relasi dengan Class_connection yaitu *one to many* untuk melakukan koneksi dalam proses menyimpan dan mengambil citra digital di basis data.

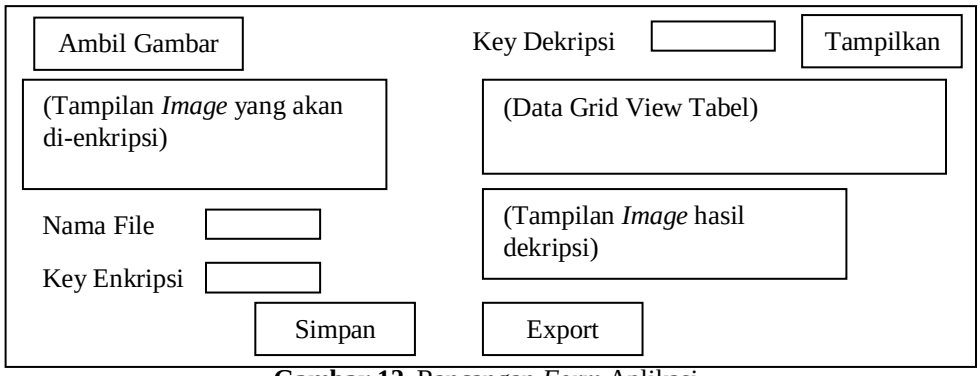
Dalam perancangan *database* pada sistem ini hanya terdapat 1 (satu) tabel dalam basis data. Tabel tersebut berfungsi untuk menyimpan *key* algoritma AES dan data *chiper* hasil enkripsi. Nama basis data adalah db_encrypt_decrypt_image, sedangkan nama tabel yaitu tbl_file. Struktur tabel tbl_file dapat dilihat pada Tabel 1.

Tabel 1. Tabel tbl_file

Field	*Data Type*	*Null*	*Extra*
Id	*int(11)*	*No*	*Foreign key*
file_encrypt	*longtext*	*No*	
nama_file	*varchar(100)*	*No*	
Kunci	*text*	*No*	
panjang_char	*int(11)*	*No*	

Tabel 1 menjelaskan *fields* yang terdapat dalam tabel tbl_file yang dirancang dalam *database* beserta dengan tipe data tiap *field*. *Field id* dipergunakan untuk menyimpan kode *file*, sehingga di-*setting* sebagai *foreign key* supaya tiap *file* masuk tidak terjadi redundansi data. *Field* file_encrypt berfungsi untuk menyimpan data hasil enkripsi *file* citra digital, sehingga diberi tipe data *longtext* karena data *chiper* berupa *string* dan memiliki kapasitas penyimpanan 2^{32}-1 karakter. *Field* nama_file memiliki tipe data *varchar* panjang 100 karakter untuk menyimpan nama data *chiper* hasil proses enkripsi AES. *Field* kunci memiliki tipe data *text* guna menyimpan kunci *private key* algoritma AES masing-masing data *chiper* citra digital. *Field* panjang_char bertipe *integer* dengan panjang 11 supaya mampu menyimpan informasi panjang atau jumlah karakter data *chiper* hasil enkripsi citra digital.

Pembuatan aplikasi akan dibangun dengan menggunakan Visual Studio 2010. Dalam pembuatan dan perancangan aplikasi, perlu adanya perancangan antar muka sebagai bagian yang berinteraksi dengan pengguna. Antar muka yang dibuat menggunakan *forms* sebagai tempat untuk menggabungkan *form-form* yang lain yang digunakan sebagai modul untuk *sub*-proses yang ada di dalam sistem ini. Pada aplikasi hasil penelitian ini, memiliki 1 (satu) desain antar muka sistem yang terlihat pada Gambar 12.

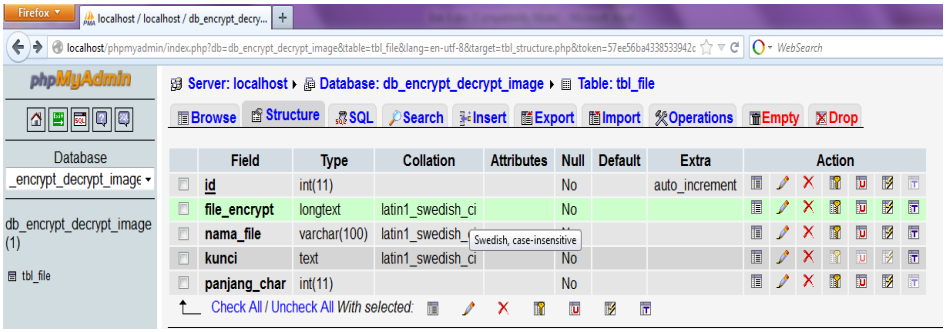


Gambar 12. Rancangan *Form* Aplikasi

4. Hasil dan Pembahasan

Aplikasi yang dibangun untuk proses enkripsi *file image* menggunakan bahasa pemrograman *Visual Basic.Net framework.Net versi* 4.0. Untuk pengkodean, aplikasi dibuat dengan metode pemrograman berorientasi obyek. Basis data yang dipergunakan adalah *MySql*.

Database dibangun sesuai dengan perancangan pada bab 3. Pembuatan tabel pada *database MySql* dibuat dengan menggunakan phpMyAdmin yang disediakan oleh paket Xampp. Implementasi *database* dan tabel dapat dilihat pada Gambar 13.



Gambar 13. Implementasi *Database* dan Tabel

Untuk dapat mengakses tabel pada *database*, aplikasi memerlukan sebuah perintah koneksi. Koneksi *database* berfungsi untuk melakukan koneksi dengan antara aplikasi dengan *database*. Implementasi perintah koneksi *database* ke dalam bahasa pemrogaman pada Kode Program 1.

Kode Program 1 Kode Program Perintah Koneksi *Database*

```
1. Public Class connection
2. Public Function getConnectionString() As String
3. Return
   "Server=localhost;Database=db_encrypt_decrypt_image;Uid=root;
   Pwd=;Allow Zero Datetime=true;"
4. End Function
5. End Class
```

Pada Kode Program 1 terlihat di baris 3 yaitu koneksi dilakukan ke *Server localhost* dengan nama *database* db_encrypt_decrypt_image, nama *user* adalah *root* tanpa *password*. Penjelasan Kode Program 1 sebagai berikut: untuk penamaan *method* ada pada baris 1, setelah itu untuk koneksi *string permission* ke *database* ada pada baris 3.

Pada penelitian skripsi ini, metode pengembangan sistem dipergunakan adalah *metode prototype*. Oleh karena itu, maka dalam proses implementasi aplikasi menghasilkan 3 (tiga) prototipe, yang berdasarkan hasil pengujian merupakan prototipe yang sudah sesuai dengan kebutuhan *customer* atau pengguna. Untuk lebih memperjelas proses pengembangan sistem dapat dilihat dalam Tabel 2 Dokumentasi Prototipe.

Tabel 2. Dokumentasi Prototipe

No.	Spesifikasi	Deskripsi	Testing dan Validasi	Evaluasi Customer
Prototipe I				
1.	*Login*	Proses *login* untuk masuk kedalam sistem	*Input username* dan *password.* Ditolak masuk jika *username* dan *password* salah. Dapat masuk jika *username* dan *password* benar.	Dihilangkan saja karena siapapun boleh memakai aplikasi.
2.	Ambil Gambar	Proses mengambil *file* citra digital dari *memory* eksternal	Ambil *file* citra dari *harddisk* dan *flashdisk.* Dapat ditampilkan pada *pictureBox.*	Oke.
3.	Nama *File*	Memasukkan nama *file* hasil enkripsi ke *database.*	Nama *file* diisi alphabet, simbol dan angka. Tidak terjadi *error.*	Oke
4.	*Key* Enkripsi	Memasukkan nama *file* hasil enkripsi ke *database.*	Nama *file* diisi alphabet, simbol dan angka. Tidak terjadi *error.*	Oke
5.	Simpan	Proses enkripsi *image* dan menyimpan ke *database* dengan nama *file* dan *key* yang ditentukan.	Nama *file* atau *key* enkripsi kosong maka Muncul pesan *error.* Nama *file* dan *Key* enkripsi ada maka sukses tersimpan.	Oke.
6.	Data *Grid View*	Menampilkan semua *record* yang tersimpan pada tabel tbl_file dan pengguna memilih *record* dengan nama *file* untuk di-dekripsi.	Muncul kolom id, *username, password* dalam *hash* MD5, nama *file, chiper image, key* enkripsi	- Hilangkan *username* dan *password.* - *Key* enkripsi yang ditampilkan disandikan.
7	Tampilkan	Proses dekripsi *chiper image* yang dipilih pada data *grid view* dengan *key* dekripsi yang diisi oleh pengguna.	*Image* dapat tampil di *picturebox* dengan *key* dekripsi sama dengan *key* enkripsi.	Oke.
Prototipe II				
1.	*Login*	Proses *login*	Sudah tidak ada.	Oke.

		untuk masuk kedalam sistem		
2.	Data *Grid View*	Menampilkan semua *record* yang tersimpan pada tabel tbl_file dan pengguna memilih *record* dengan nama *file* untuk di-dekripsi.	- *Username* dan *password* tidak ada. - *Key* enkripsi sudah disandikan dengan *hash* MD5.	Tambahkan info panjang karakter hasil enkripsi *image.*
3.	*Export*	Proses untuk menyimpan *image* hasil dekripsi ke *memory* eksternal.		Belum ada. Tambahkan.
Prototipe III				
1.	Data *Grid View*	Menampilkan semua *record* yang tersimpan pada tabel tbl_file dan pengguna memilih *record* dengan nama *file* untuk di-dekripsi.	Ditampilkan kolom info panjang karakter hasil enkripsi.	Oke.
2.	*Export*	Proses untuk menyimpan *image* hasil dekripsi ke *memory* eksternal.	Menyimpan *image* hasil enkripsi ke *harddisk* atau *flashdisk* berhasil dengan nama *file* yang ditentukan pengguna.	Oke.

Berdasarkan perancangan proses enkripsi citra digital, maka hasil implementasi perancangan tersebut diterapkan kedalam beberapa tahap sebagai berikut: Tahap I, yaitu Proses mengambil *file* citra digital dari *memory* eksternal dan menampilkannya kedalam *pictureBox*. Setelah itu, memasukkan nama *file* dan *key* enkripsi.

Kode Program 2 Proses Ambil Gambar pada *Class* Form1

```
1. Private Sub btnBrowse_Click(ByVal sender As System.Object, ByVal e As
   System.EventArgs) Handles btnBrowse.Click
2. If OpenFileDialog1.ShowDialog() = Windows.Forms.DialogResult.OK Then
   PictureBox1.Image = Image.FromFile(OpenFileDialog1.FileName)
3. PictureBox1.Height = 350
4. PictureBox1.Width = 500
5. End If
6. End Sub
```

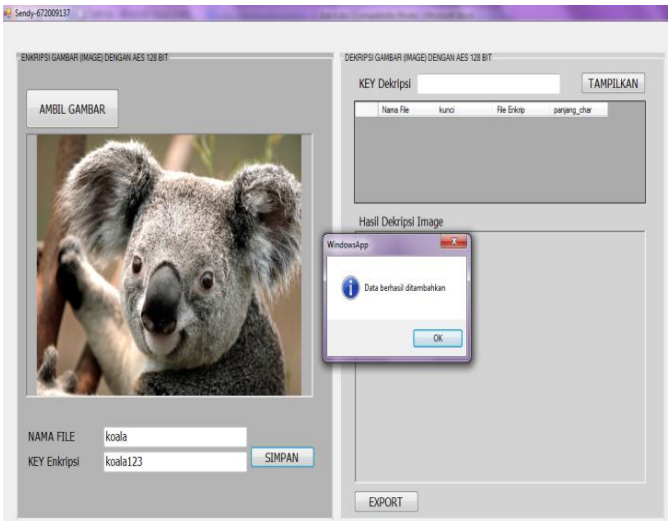
Penjelasan Kode Program 2 sebagai berikut: proses yang terjadi pada *class Form*1 untuk pengambilan gambar adalah dengan memunculkan *file* dialog yang dapat dilihat pada baris 2, pengaturan tinggi dan lebar gambar pun dapat dilihat pada baris 3 dan 4.

Tahap II, yaitu proses mengenkripsi *file* citra digital dari *pictureBox* dengan *key* enkripsi dan kemudian menyimpan kedalam *database* dengan nama *file* yang dimasukkan. Untuk melakukan enkripsi citra digital diawali dengan klik *button* Simpan, *source code* pada *button* Simpan pada Kode Program 3.

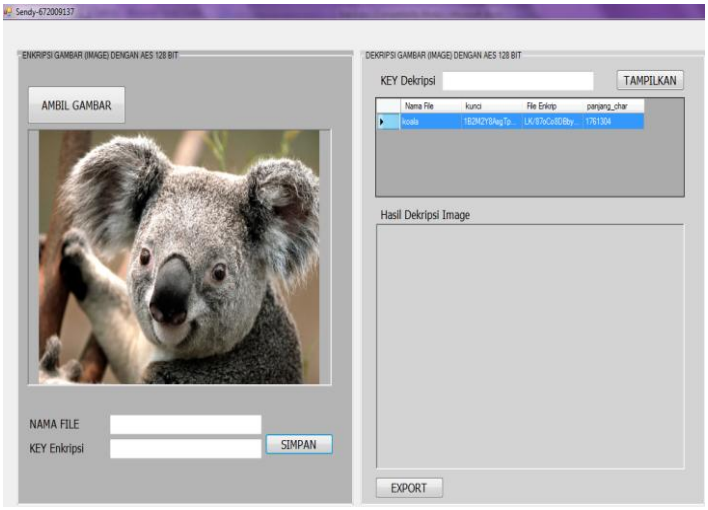
Kode Program 3 Proses Klik *Button* Simpan pada *Class* Form1

```
1.  Private Sub btnSimpan_Click(ByVal sender As System.Object, ByVal e As
    System.EventArgs) Handles btnSimpan.Click
2.  If txtKunciEnkripsi.Text = "" Then MsgBox("Nama file harus diisi!",
    MsgBoxStyle.Critical)Else
3.  If TextBox2.Text = "" Then MsgBox("Kunci enkripsi harus diisi!",
    MsgBoxStyle.Critical) Else Dim myImage As Image =
    Image.FromFile(OpenFileDialog1.FileName)
4.  Dim imgByteArray As Byte() = Nothing
5.  'Image to byte[]
6.  Dim imgMemoryStream As MemoryStream = New MemoryStream()
7.  myImage.Save(imgMemoryStream,System.Drawing.Imaging.ImageFormat.Jpeg)
8.  imgByteArray = imgMemoryStream.GetBuffer()
9.  Dim aes As New class_aes
10. Dim modData As New model
11. _data = aes.AES_Encrypt(imgByteArray, TextBox2.Text)
12. Dim key As String
13. key = aes.MD5_Hash(TextBox1.Text)
14. modData.insertFile(_data, txtKunciEnkripsi.Text, key)
15. _data = ""
16. RefreshDataGrid()
17. End If
18. End If
19. End Sub
```

Penjelasan Kode Program 3 sebagai berikut: proses simpan pada *Class Form1* dimulai dengan mengecek nama *file* sudah diisi atau belum ada pada baris 2, kemudian kunci enkripsi harus di cek dulu apakah sudah terisi apa belum ada pada baris 3. Setelah itu pada baris 8 dari *image* dijadikan kedalam bentuk *byte.* Dapat dilihat bahwa proses setelah dijadikan *byte, image* di enkrip menggunakan *Hash* MD5 yang terdapat pada baris program no 14.



Gambar 14a. Pesan Berhasil Disimpan



Gambar 14b. Tampilan Grid View

Sedangkan *source code* proses enkripsi pada Class_AES dapat dilihat pada Kode Program 4 Untuk Kode Program 5 adalah kode program untuk menyimpan hasil enkripsi kedalam tabel tbl_file pada *database* db_encrypt_decrypt_image.

Kode Program 4 Proses Enkripsi pada *Class* class_aes

```
1.  Public Function AES_Encrypt(ByVal input As Byte(), ByVal kunci As
    String) As String
2.  Dim AES As New System.Security.Cryptography.AesManaged
3.  Dim MD5 As NewSystem.Security.Cryptography.MD5CryptoServiceProvider
4.  Dim encrypted As String = ""
5.  Try
6.  Dim temp As Byte() =
    MD5.ComputeHash(System.Text.ASCIIEncoding.ASCII.GetBytes(kunci))
7.  AES.Key = temp
8.  AES.Mode = Security.Cryptography.CipherMode.ECB
9.  Dim AesEncrypter As System.Security.Cryptography.ICryptoTransform =
    AES.CreateEncryptor
10. encrypted =
    Convert.ToBase64String(AesEncrypter.TransformFinalBlock(input, 0,
    input.Length))
11. Catch ex As Exception
12. End Try
13. Return encrypted
14. End Function
```

Penjelasan Kode Program 4 sebagai berikut: Proses enkripsi pada class_AES terlihat bahwa kode program pada baris 4 menjelaskan tentang proses *image* dari *byte* modenya yang memakai ECB. Pada baris 9 menjelaskan tentang proses enkripsi AES pada kelas kripto menggunakan AES.CreateEncryptor dan sesudah itu di *convert* menggunakan base64 yang terlihat pada baris 10.

Kode Program 5 Simpan Hasil Enkripsi Kedalam *Database* pada *Class* Model

```
1.  Public Sub insertFile(ByVal file As String, ByVal nama As String, ByVal
    key As String)
2.  Dim dt As New DataTable
3.  _connection = New connection
4.  Dim jmlchar As New Integer
5.  jmlchar = file.Length()
6.  Using cn As New MySqlConnection(_connection.getConnectionString)
7.  Try
8.  cn.Open()
9.  Using cm As New MySqlCommand
10. cm.Connection = cn
11. cm.CommandText = "INSERT INTO tbl_file
    (file_encrypt,nama_file,kunci,panjang_char) VALUES ('" & file & "','" &
    nama & "','" & key & "','" & jmlchar & "')"
12. cm.ExecuteNonQuery()
13. End Using
14. Catch ex As ExceptionMsgBox("Gagal Konek ke Database",
    MsgBoxStyle.Critical)
15. FinallyMsgBox("Data berhasil ditambahkan", MsgBoxStyle.Information)
16. End Try
17. End Using
18. End Sub
```

Penjelasan Kode Program 5 sebagai berikut: setelah di enkrip, hasil enkripsi akan disimpan pada tbl_file dengan ukuran panjang karakter 2^{32}-1 yang terdapat pada baris 11. Setelah itu pada baris 14 menampilkan pesan *error* jika ada kesalahan saat penambahan data. Jika data berhasil ditambahkan maka akan ada pemberitahuan.

Berdasarkan perancangan proses dekripsi citra digital, maka hasil implementasi perancangan diterapkan kedalam aplikasi dengan cara yaitu diawali proses memilih data *chiper* citra digital pada *Grid View* tabel. Lalu memasukkan *key* dekripsi pada *textbox* yang ditentukan. Setelah itu klik *button* tampilkan.Untuk dapat melakukan proses menampilkan *image* tersebut kode program yang dipergunakan terlihat pada Kode Program 6.

Kode Program 6 Perintah *Button* Tampilkan pada *Class* Form1

```
1.  Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As
    System.EventArgs) Handles Button1.Click
2.  Dim imgMemoryStream As MemoryStream = New MemoryStream()
3.  Dim imgByteArray As Byte() = Nothing
4.  Dim myImage As Image
5.  Dim aes As New class_aes
6.  PictureBox1.BackgroundImage = Nothing
7.  _data = cm.Current("file_encrypt")
8.  imgByteArray = aes.AES_Decrypt(_data, TextBox1.Text)
9.  Try
10. imgMemoryStream = New MemoryStream(imgByteArray)
11.  myImage = Drawing.Image.FromStream(imgMemoryStream)
12.  PictureBox2.Image = myImage
13. Catch ex As Exception
14. MsgBox("maaf image tidak bisa di tampilkan")
15. End Try
16. End Sub
```

Penjelasan Kode Program 6 sebagai berikut: Untuk mengambil *file* ada pada kode program baris 1. Kemudian ambil data yang dituju oleh data *grid* (data dari

tabel) terdapat pada baris 7. Pada baris 8 proses dekripsi terjadi. Setelah berhasil maka data akan berubah menjadi *byte*. Setelah *byte*, kemudian diubah menjadi *image string* terdapat pada kode program baris 10.

Jika *key* dekripsi yang dimasukkan tidak sama dengan *key* enkripsi maka hasil dekripsi *error* atau data *chiper* citra digital atau *image* tidak dapat ditampilkan dan muncul pesan *error*. Kode program untuk melakukan proses dekripsi data *chiper* citra digital dapat dilihat pada Kode Program 7.

Kode Program 7 Perintah Proses Dekripsi pada *Class* class_aes

```
1.  Public Function AES_Decrypt(ByVal input As String, ByVal kunci As String)
    As Byte()
2.  Dim AES As New System.Security.Cryptography.AesManaged
3.  Dim MD5 As NewSystem.Security.Cryptography.MD5CryptoServiceProvider
4.  Dim hasil As Byte()
5.  Try
6.  Dim temp As Byte() =
    MD5.ComputeHash(System.Text.ASCIIEncoding.ASCII.GetBytes(kunci))
7.   AES.Key = temp
8.  AES.Mode = Security.Cryptography.CipherMode.ECB
9.  Dim AesDecrypter AsSystem.Security.Cryptography.ICryptoTransform =
    AES.CreateDecryptor
10. Dim Buffer As Byte() = Convert.FromBase64String(input)
11.  hasil = AesDecrypter.TransformFinalBlock(Buffer, 0, Buffer.Length)
12.  Catch ex As Exception
13. End Try
14. Return hasil
15. End Function
```

Penjelasan Kode Program 7 sebagai berikut: Baris 6, kode program untuk menjelaskan dekripsi kunci dengan MD5 *Hash*. Setelah kunci di dekrip menggunakan MD5 *Hash* maka harus diisi kunci AES dengan baris no 6. Baris 8 merupakan kode program untuk mengatur mode AES kemudian pada baris 10 *byte* dienkrip menggunakan base64.

Setelah citra digital hasil dekripsi dapat ditampilkan pada *pictureBox*, maka pengguna diberi kesempatan dapat mengeksport atau menyimpan citra digital tersebut kedalam memori eksternal sebagai *file image*. Format *file image* hasil eksport pada aplikasi hanya diberikan format jpeg. Perintah eksport dapat dilihat pada Kode Program 8.

Kode Program 8 Perintah Ekport pada *Button* Eksport *Class* Form1

```
1. Private Sub Button2_Click(ByVal sender As System.Object, ByVal e As
   System.EventArgs) Handles Button2.Click
2. If SaveFileDialog1.ShowDialog = Windows.Forms.DialogResult.OK Then
3. PictureBox2.Image.Save(SaveFileDialog1.FileName)
4. End If
5. End Sub
```

Penjelasan Kode Program 8 sebagai berikut: Baris 2, kode program untuk mengambil lokasi *file* yang akan disimpan, Baris 3 untuk menyimpan *image* ke lokasi baris. Baris 4-5, kode program untuk penutup teks.

Penerapan Algoritma AES 128 bit pada enkripsi dekripsi yang dimiliki aplikasi hasil penelitian ini membuktikan bahwa aplikasi mampu mendukung salah satu kaidah keamanan data, yaitu kerahasiaan data *(Data Confidentiality)*.

Pengujian Sistem

Pada pengujian sistem, analisis pengujian aplikasi ini akan dilakukan pengujian proses penerapan algoritma AES pada enkripsi dekripsi citra digital dengan format citra digital yang berbeda, yaitu jpeg/jpg, bmp dan gif. Pengujian juga dilakukan dengan citra digital dengan *true colour* dan *greyscale* atau tidak berwarna. Hal ini dilakukan untuk menguji bahwa proses enkripsi dekripsi menggunakan algoritma AES dapat dilakukan terhadap berbagai format *image* atau citra digital dan warna yang dimiliki citra digital tersebut. Pengujian ini juga dapat membuktikan bahwa algoritma AES dalam proses enkripsi dan dekripsi citra digital juga tidak menyebabkan perubahan terhadap ukuran, resolusi dan warna citra digital. Dengan kata lain yaitu aplikasi mampu mengamankan *raw file image*, hanya merubah ektensi *file* citra digital tersebut. Hasil pengujian ini dapat dilihat pada Tabel 3.

Tabel 3 Tabel Hasil Uji Enkripsi-Dekripsi AES terhadap Spesifikasi Citra

No.	Hasil Uji Proses Enkripsi-Dekripsi		
	Spesifikasi	**Sebelum**	**Sesudah**
1.	Format	jpeg	jpeg
	Warna	colour	colour
	Ukuran	1.48 Kb	1.48 Kb
	Resolusi	313 x 234 pixel	313 x 234 pixel
2.	Format	jpg	jpg
	Warna	colour	colour
	Ukuran	762 Kb	762 Kb
	Resolusi	1024 x 768 pixels	1024 x 768 pixels
3.	Format	bmp	jpg
	Warna	colour	colour
	Ukuran	12.4 Kb	12.Kb
	Resolusi	275 x 183 pixel	275 x 183 pixel
4.	Format	gif	jpeg
	Warna	grey	grey
	Ukuran	7.98 Kb	7.98 Kb
	Resolusi	225 x 225 pixel	225 x 225 pixel

Pengujian juga dilakukan dengan metode uji respondensi yaitu diuji oleh 10 (sepuluh) responden mahasiswa dengan cara mengoperasikan aplikasi lalu mengisi kuesioner. Hasil uji respondensi terhadap aplikasi implementasi algoritma AES pada citra digital dapat dilihat pada Tabel 4.

Tabel 4 Tabel Hasil Uji Respondensi

No.	Pertanyaan	Prosentase Jawaban Responden				
		Sangat Tidak Setuju	Tidak Setuju	Tidak Tahu	Setuju	Sangat Setuju
1.	Tampilan aplikasi cukup mudah dimengerti.	0	0	0	70	30
2.	Aplikasi mudah digunakan.	0	0	0	60	40
3.	Aplikasi dapat menyimpan (enkripsi) berbagai format citra digital.	0	0	0	20	80
4.	Aplikasi dapat menampilkan (dekripsi) berbagai format citra digital.	0	0	0	20	80
5.	Aplikasi dapat merahasiakan citra digital karena memiliki *key* enkripsi-dekripsi.	0	0	0	30	70
6.	Aplikasi layak dipergunakan sebagai salah satu cara untuk merahasiakan data (*Data Confidentiality*) citra digital.	0	0	0	30	70
Jumlah		0	0	0	230	370
Rata-rata		0	0	0	38.3	61.7

Berdasarkan Tabel 4 hasil uji terhadap responden yaitu jumlah responden menjawab Setuju berjumlah 38.3% dan Sangat Setuju berjumlah 61.7% maka dapat disimpulkan bahwa aplikasi dapat memenuhi kebutuhan pengguna dalam merahasiakan data berupa citra digital.

5. Simpulan

Berdasarkan perancangan sistem keamanan *raw file image* (citra digital) menggunakan algoritma kriptografi AES 128 bit pada *database MySql Server*, maka dapat disimpulkan bahwa: Dengan demikian aplikasi implementasi algoritma AES (*Advanced Encryption Standard*) pada *raw file image* dapat menyelesaikan permasalahan dari latar belakang penelitian ini yaitu menjaga kerahasiaan data berupa citra digital (*image*) pengguna. Disini dapat dilihat bagaimana cara kerja proses enkripsi dengan merubah *image* menjadi karakter kemudian disimpan kedalam *database* dan selanjutnya akan dienkrip menggunakan base64 sehingga keluarannya kembali dalam bentuk *string*. Begitupun sama hal dengan proses dekripsi yang merupakan kebalikan dari proses enkripsi. Dengan begitu dapat menjawab permasalahan yang ada pada keamanan data. Algoritma AES sendiri mampu merahasiakan data *raw file image* yaitu tanpa mengubah spesifikasi data (ukuran, warna, resolusi) tetapi hanya merubah ektensi *file image*. Saran–saran yang berguna untuk pengembangan lebih lanjut terhadap program aplikasi enkripsi ini adalah sebagai berikut: (1) Aplikasi enkripsi *database* ini menggunakan algoritma enkripsi AES dengan panjang kunci 128 bit, dapat dikembangkan dengan algoritma enkripsi 256 bit; (2) Aplikasi enkripsi ini hanya dapat men-*delete* data menggunakan *database mysql*, untuk pengembangan dapat dengan menambah tabel *delete* pada aplikasi; (3)

Aplikasi enkripsi ini dapat dikembangkan dengan menambah fasilitas ekspor yang mampu mendeteksi *format* citra digital aslinya.

6. Daftar Pustaka

[1] Oktavia. 2009, Implementasi Algoritma *Chaos-Based FeedBack Stream Cipher* pada Enkripsi-Deskripsi Data Citra *Digital*. Salatiga.

[2] Hafidz THR., Nadhori IU., Ramadijanti N., 2011, Enkripsi Gambar Menggunakan Algoritma Secure Image Protection, http://www.eepis-its.edu/uploadta/downloadmk.php?id=1531, Diakses pada tanggal 12 September 2013.

[3] Coolutils.com, 2013, What is Raw?, *http://www.coolutils.com/formats/raw*, Diakses pada tanggal 12 September 2013.

[4] Munir, Rinaldi. 2004. *Advanced Encryption Standard (AES)*. www.informatika.org/~rinaldi/.../MakalahIF505430708089.pdf, Diakses pada tanggal 5 Agustus 2013.

[5] Riyanto. 2003. Seri Penuntun Praktis Koneksi Data Melalui Borland Delphi dengan Database MySQL. Elex Media Komputindo: Jakarta

[6] Cahyo, 2000, …..

[7] Sutoyo, T. dkk., 2009, Teori Pengolahan Citra Digital, Yogyakarta: Penerbit Andi

[8] Sommerville, Ian. 2003. *Rekayasa Perangkat Lunak*. Erlangga : Jakarta.