ISSN : 2548-6985

Aplikasi Pengamanan Data Gambar Dengan Menerapkan Algoritma Vigenere Chiper

Ayu Wandira Simatupang
STMIK Budi Darma Medan, Sumatera Utara, Indonesia
Jl. Sisingamangaraja No. 338 Simpang Limun Medan
http://stmik-budidarma.ac.id // Email : ctuphank@ymail.com

ABSTRACT
The security and confidentiality of data is very important considering the rapid development of technology at this time which allows the emergence of new techniques that are misused by certain parties that can threaten security from data that are considered insignificant.
Cryptography is a field of science to maintain image security. Cryptography has been implemented in many ways. The way it works is to change the original data that can be understood / read by humans (plaintext) to other forms that cannot be understood / read by humans (ciphertext). The process of transforming plaintext into chiperteks is termed encryption. While the process of returning a chipertext message to plaintext is termed decryption.
Vigenere Cipher is an asymmetric cryptographic algorithm, where the key used to encrypt is different from the one used to decrypt. Vigenere Cipher is a cryptographic algorithm that uses letters and numeric values. Vigenere Cipher requires three steps in the process, namely key generation, encryption, and decryption. The process of encryption and decryption is almost the same process.

Keywords: Cryptography, Vigenere Cipher Algorithm, Image

PENDAHULUAN

Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi terlebih apabila data tersebut berada dalam suatu jaringan komputer yang terkoneksi dengan jaringan publik misalnya internet. Tentu saja data yang sangat penting tersebut tidak sembarangan dilihat atau dibajak oleh orang yang tidak berwenang. Apabila hal ini sampai terjadi kemungkinan data akan rusak bahkan dapat hilang dan akan menimbulkan kerugian material yang besar.

Gambar (citra) sering digunakan dalam menyajikan informasi. Gambar (citra) dapat direpresentasikan ke dalam sebuah bidang datar yang mempunyai dua buah ukuran (lebar dan tinggi). Dalam dunia komputasi gambar terdiri dari pixel-pixel dimana nilai pixel menunjukkan warna gambar (citra). Gambar direpresentasikan dengan kombinasi tiga warna primer yaitu warna merah, warna hijau dan warna biru. Gambarpun tidak lepas dari masalah keamanan, salah satu masalah yang umum ditemui pada gambar adalah data tersebut dapat diambil oleh pihak yang tidak berhak dan tidak bertanggung jawab yang kemudian disalahgunakan untuk hal-hal yang tidak diinginkan [3].

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan data termasuk gambar. Penyandian data gambar melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan data gambar dan keutuhan dari data gambar tersebut. Data gambar tersebut harus tetap rahasia dengan bertujuan untuk menjaga karahasiaannya terhadap akses orang-orang yang tidak berhak.

Vigenere cipher merupakan salah satu algoritma kriptografi klasik dengan teknik substitusi. *Vigenere cipher* menggunakan suatu kunci yang memiliki panjang tertentu. Panjang kunci tersebut bisa lebih pendek ataupun sama dengan panjang plainteks. Apabila panjang kunci kurang dari panjang plainteks, maka kunci tersebut akan diulang secara periodik hingga panjang kunci tersebut sama dengan panjang plainteksnya. Penggunan metode ini cukup baik digunakan dalam penyandian citra karena kunci matrik yang cukup besar [9].

Salah satu solusi untuk menyelesaikan masalah di atas adalah melakukan proses penyandian (enkripsi dan dekripsi) data gambar. Cara ini dilakukan dengan menyandikan data gambar berdasarkan metode tertentu, sehingga orang yang tidak berkepentingan dan tidak memiliki hak akses mengalami kesulitan untuk melakukan hal-hal

ISSN : 2548-6985

yang tidak diinginkan. Sebaliknya ketika data tersebut diakses oleh orang yang berhak, maka data gambar yang telah disandikan tersebut dapat dikembalikan ke bentuk semula

Berdasarkan latar belakang di atas, maka perumusan masalah yang akan di bahas dalam penelitian ini adalah sebagai berikut:

1. Bagaimana prosedur penyandian data gambar?
2. Bagaimana menerapkan *algoritma vigenere chiper* dalam penyandian data gambar?
3. Bagaimana merancang aplikasi penyandian data gambar dengan bahasa pemograman *visual basic 2008?*

Adapun beberapa manfaat dari penulisan penelitian ini adalah sebagai berikut : 1) . Menambah pengetahuan penulis tentang prosedur penyandian data gambar berdasarkan algoritma *vigenere cipher. 2)* Meningkatkan keamanan data gambar dari tindakan-tindakan pengerusakan atau hal-hal lain dari orang-orang yang tidak bertanggung jawab*. 3)* Meningkatkan efesiensi waktu dan keakuratan proses pengamanan data gambar melalui sebuah aplikasi.

LANDASAN TEORI

2.1 Keamanan

Keamanan merupakan salah satu aspek terpenting dari sebuah system informasi. Masalah keamanan sering kurang mendapatkan perhatian dari para perancang dan pengelola system informasi. Masalah keamanan sering berada diurutan setelah tampilan, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting [5].

2.2 Kriptografi

Kriptografi adalah ilmu yang berguna untuk mengacak data sedemikian rupa, sehingga tidak bisa dibaca oleh pihak ketiga. Tentu saja data yang diacak harus bisa dikembalikan kebentuk semula oleh pihak yang berwenang. Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *Graphia* berarti tulisan. Kriptografi adalah ilmu dan seni untuk menjaga keamanan data ketika data dikirim dari suatu tempat ke tempat yang lain [2].

Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan data dari orang-orang yang tidak berhak atas data [5].

Adapun fungsi algoritma kriptografi adalah sebagai berikut :

1. Enkripsi
   Enkripsi merupakan hal yang sangat penting dalam kriptografi yang merupakan pengamanan data yang dikirimkan terjaga kerahasiaannya. Data asli disebut *plaintext* yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode.
2. Dekripsi
   Dekripsi merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (*plaintext*) disebut dengan dekripsi data. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi.
3. Kunci
   Kunci yang dimaksud adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi.

2.3 Vigenere Cipher

Vigenere Cipher termasuk sandi abjad-majemuk (*polyalphabetic substitution cipher*). Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, *Blaise de Vigenere* pada abad 16, tahun 1586. Sebenarnya Giovan Batista Belaso telah menggambarkannya untuk pertama kali pada tahun 1533 seperti ditulis di dalam buku *La Cifra del Sig*. *Cipher* ini dipopulerkan kembali oleh *Blaise de Vigenere*, Sehingga nama cipher ini diambil dari namanya. Algoritma ini baru dikenal luas 200 tahun kemudian dan dinamakan kode *Vigenere.* Kode *Vigenere* berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19 [5].

Cipher ini menggunakan bujur sangkar *Vigenere* untuk melakukan enkripsi. Kolom paling kiri dari bujur sangkar menyatakan huruf-hurf kunci, sedangkan baris paling atas menyatakan huruf-huruf *plainteks*. Setiap baris dalam bujur sangkar menyatakan huruf-huruf *cipherteks*, yang mana jumlah pergesaran huruf *plainteks* ditentukan nilai numerik huruf kunci tersebut (yaitu, A = 0, B = 1, C = 2,…, Z = 25). Secara matematis proses enkripsi dan dekripsi pada *vigenere cipher* [5] adalah sebagai berikut :

Rumus Enkripsi : Ci = (Pi + Ki) Mod(256)

Rumus Dekripsi : Pi = (Ci - Ki) Mod(256)

Dimana : Ci = nilai desimal karakter cipherteks ke-i

Pi = nilai desimal karakter plainteks ke-i

Ki = nilai desimal karakter kunci ke-i

Bujur sangkar *Vigenere* digunakan untuk memperoleh *cipherteks* dengan

menggunakan kunci yang sudah ditentukan. Apabila panjang kunci lebih pendek dari pada panjang *plainteks*, maka kunci diulang penggunaanya. Algoritma enkripsi jenis ini sangat dikenal karena mudah dipahami dan diimplementasikan. Teknik untuk menghasilkan *ciphertext* bisa dilakukan menggunakan substitusi angka maupun bujur sangkar *vigenere*. Teknik susbtitusi *vigenere* dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser.

Tabel 1 : Vigenere

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

sumber : Dony Ariyus, 2008

Tabel 2 : Contoh Penyelesaian
Plaintext : PLAINTEXT
Kunci : CIPHER

Plain	Karakter	P	L	A	I	N	T	E	X	T
	Angka Sub	15	11	0	8	13	19	4	23	19
Kunci	Karakter	C	I	P	H	E	R	C	I	P
	Angka Sub	2	8	15	7	4	17	2	8	15
Ciphertext	Karakter	R	T	P	P	R	K	G	F	I
	Angka Sub	17	19	15	15	17	10	6	5	8

Berdasarkan metode pertukaran angka dengan huruf di atas, diperoleh bahwa teks asli (PLAINTEXT) memiliki kode angka (15,11, 0, 8, 13, 19, 4, 23, 19), sedangkan kode angka untuk teks kunci (CIPHER) yaitu (2, 8, 15, 7, 4, 17). Setelah dilakukan perhitungan, maka dihasilkan kode angka *ciphertext* (17, 19, 15, 15, 17, 10, 6, 5, 8). Jika diterjemahkan kembali menjadi huruf sesuai urutan awal, maka menjadi huruf RTPPRKGFI.

PEMBAHASAN

3.1 Analisa Sistem

Adapun penerapan dalam mengenkripsi gambar adalah sebagai berikut :

1. Ambil Citra Plain (Citra Asli)

Gambar 1 : Gambar Asli ukuran 432x808

2. Ambil nilai-nilai elemen warna setiap piksel citra plain

Tabel 3. Nilai-nilai Elemen Warna Setiap Piksel Citra Plain

Piksel	0			1			2			3		
	RED	GREEN	BLUE	RED	GREEN	BLUE	RED	GREEN	BLUE	RED	GREEN	BLUE
0	187	184	205	176	173	194	132	129	150	203	200	221
1	181	178	199	133	130	151	106	103	124	175	172	193
2	138	128	139	56	46	57	41	31	42	103	93	104
3	126	116	127	54	44	55	36	26	37	91	81	92
4	129	115	115	103	89	89	76	62	62	122	108	108
5	136	122	122	147	133	133	115	101	101	138	124	124
6	104	94	92	120	110	108	96	86	84	90	80	78

3. Input kunci
   Penginputan kunci yang dilakukan pada gambar sebanyak 12 piksel menggunakan kunci sebanyak 3 karakter yaitu A=65, B=66, C=67. Panjang plainteks dengan kunci haruslah sama panjang, maka kunci yang digunakan untuk mengenkripsi piksel-piksel selanjutnya adalah 3 karakter kunci yang diulang sehingga total karakter kunci sama dengan total pikselnya, lalu di moduluskan dengan 256.
4. Proses enkripsi
   Proses enkripsi dilakukan dengan menambahkan nilai desimal setiap elemen warna piksel dengan nilai kunci kemudian di moduluskan dengan 256.

```
                R   G   B
            R   G   B
Piksel 0,0 = 187 184 205
  Piksel 0,1 = 176 173 194
Kunci    =  65  66  67
  Kunci      =  65  66  67
Cipher   = 252 250 272
  Cipher   = 241 239 231
Mod 256  = 252 250  16
  Mod 256  = 241 239 231
```

R G B
R G B
Piksel 0,2 = 132 129 150
Piksel 0,3 = 203 200 221
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 197 195 217
Cipher = 268 266 288
Mod 256 = 197 195 217
Mod 256 = 12 10 32

R G B
R G B
Piksel 1,0 = 181 178 199
Piksel 1,1 = 133 130 151
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 246 244 266
Cipher = 198 196 218
Mod 256 = 246 244 10
Mod 256 = 198 196 218

R G B
R G B
Piksel 1,2 = 106 103 124
Piksel 1,3 = 175 172 193
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 171 169 191
Cipher = 240 238 260
Mod 256 = 171 169 191
Mod 256 = 240 238 4

R G B
R G B
Piksel 2,0 = 138 128 139
Piksel 2,1 = 56 46 57
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 203 194 206
Cipher = 121 112 124
Mod 256 = 203 194 206
Mod 256 = 121 112 124

R G B
R G B
Piksel 2,2 = 41 31 42
Piksel 2,3 = 103 93 104
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 106 97 109
Cipher = 168 159 171
Mod 256 = 106 97 109
Mod 256 = 168 159 171

R G B
R G B
Piksel 3,0 = 126 116 127
Piksel 3,1 = 54 44 55
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 191 182 194
Cipher = 119 110 122
Mod 256 = 191 182 194
Mod 256 = 119 110 122

R G B
R G B
Piksel 3,2 = 36 26 37
Piksel 3,3 = 91 81 92
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 101 92 104
Cipher = 156 147 159
Mod 256 = 101 92 104
Mod 256 = 156 147 159

R G B
R G B
Piksel 4,0 = 129 115 115
Piksel 4,1 = 103 89 89
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 194 181 182
Cipher = 168 155 156
Mod 256 = 194 181 182
Mod 256 = 168 155 156

R G B
R G B
Piksel 4,2 = 76 62 62
Piksel 4,3 = 122 108 108
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 141 128 129
Cipher = 187 174 175
Mod 256 = 141 128 129
Mod 256 = 187 174 175

R G B
R G B
Piksel 5,0 = 136 122 122
Piksel 5,1 = 147 33 133
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 201 188 189
Cipher = 212 99 200
Mod 256 = 201 188 189
Mod 256 = 212 99 200

R G B
R G B
Piksel 5,2 = 115 101 101
Piksel 5,3 = 138 124 124
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 180 167 168
Cipher = 203 190 191
Mod 256 = 180 167 168
Mod 256 = 203 190 191

ISSN : 2548-6985

R G B
R G B
Piksel 6,0 = 104 94 92
Piksel 6,1 = 120 110 108
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 169 160 159
Cipher = 185 176 175
Mod 256 = 169 160 159
Mod 256 = 185 176 175

R G B
R G B
Piksel 6,2 = 96 94 92
Piksel 6,3 = 90 80 78
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 161 160 159
Cipher = 155 146 145
Mod 256 = 161 160 159
Mod 256 = 155 146 145

5. Hasil enkripsi gambar (representasi dalam nilai desimal setiap piksel)

Tabel 4 : Nilai-nilai Elemen Warna Setiap Piksel Citra Terenkripsi

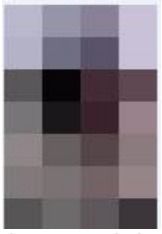
Piksel	0			1			2			3		
	R	G	B	R	G	B	R	G	B	R	G	B
0	252	250	272	241	239	231	197	195	217	12	10	32
1	246	244	10	198	196	218	171	169	191	240	138	4
2	203	194	206	121	112	124	106	97	109	168	159	171
3	191	182	194	119	110	112	101	92	104	156	147	159
4	194	181	182	168	155	156	141	128	219	107	174	175
5	201	188	189	212	99	200	180	167	168	203	190	191
6	169	160	159	185	176	175	161	160	159	155	146	145

Hasil yang diperoleh dari nilai desimal pada piksel yang terenkripsi ternyata mengalami perubahan nilai setelah di moduluskan 256.

6. Simpan gambar terenkripsi ke media penyimpanan.

Adapun penerapan dalam mengdekripsi gambar yang telah terenkripsi adalah sebagai berikut :

1. Input gambar terenkripsi



Gambar 2 : Citra terenkripsi ukuran 4x7

2. Ambil nilai-nilai elemen warna setiap piksel gambar terenkripsi

Tabel 5 : Hasil Nilai-nilai Elemen Warna Setiap Piksel Citra Terenkripsi

Piksel	0			1			2			3		
	R	G	B	R	G	B	R	G	B	R	G	B
0	252	250	272	241	239	231	197	195	217	12	10	32
1	246	244	10	198	196	218	171	169	191	240	138	4
2	203	194	206	121	112	124	106	97	109	168	159	171
3	191	182	194	119	110	112	101	92	104	156	147	159
4	194	181	182	168	155	156	141	128	219	107	174	175
5	201	188	189	212	99	200	180	167	168	203	190	191
6	169	160	159	185	176	175	161	160	159	155	146	145

3. Input kunci

Input kunci yang dilakukan pada gambar sebanyak 12 piksel menggunakan kunci sebanyak 3 karakter yaitu A=65, B=66, C=67. Kunci yang digunakan untuk mengenkripsi piksel-piksel adalah 3 karakter kunci yang diulang sehingga total karakter kunci sama dengan total pikselnya.

4. Proses dekripsi

Proses dekripsi dilakukan dengan mengurangkan jumlah nilai elemen warrna setiap piksel dengan nilai kunci, kemudian di modulus dengan 256.

R G B
R G B
Piksel 0,0 = 252 250 272
Piksel 0,1 = 241 239 231
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 187 184 205
Cipher = 176 173 164
Mod 256 = 187 184 205
Mod 256 = 176 173 164

R G B
R G B
Piksel 0,2 = 197 195 217
Piksel 0,3 = 12 10 32
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 132 129 150
Cipher = -53 -56 -35
Mod 256 = 132 129 150
Mod 256 = 203 200 221

R G B
R G B
Piksel 1,0 = 246 244 10
Piksel 1,1 = 198 196 218
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 181 178 -57
Cipher = 133 130 151
Mod 256 = 181 178 199
Mod 256 = 133 130 151

R G B
R G B
Piksel 1,2 = 171 169 191
Piksel 1,3 = 240 238 4
Kunci = 65 66 67
Kunci = 65 66 67

Cipher = 106 103 124
Cipher = 175 172 -63
Mod 256 = 106 103 124
Mod 256 = 175 172 193

R G B
R G B
Piksel 2,0 = 203 194 206
Piksel 2,1 = 121 112 124
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 138 128 139
Cipher = 56 46 57
Mod 256 = 138 128 139
Mod 256 = 56 46 57

R G B
R G B
Piksel 2,2 = 106 97 109
Piksel 2,3 = 168 159 171
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 41 31 42
Cipher = 103 93 104
Mod 256 = 41 31 42
Mod 256 = 103 93 104

R G B
R G B
Piksel 3,0 = 191 182 194
Piksel 3,1 = 119 110 122
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 126 116 127
Cipher = 54 44 55
Mod 256 = 126 116 127
Mod 256 = 54 44 55

R G B
R G B
Piksel 3,2 = 101 92 104
Piksel 3,3 = 156 147 159
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 36 26 37
Cipher = 91 81 92
Mod 256 = 36 26 37
Mod 256 = 91 81 92

R G B
R G B
Piksel 4,0 = 194 181 182
Piksel 4,1 = 168 155 156
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 129 115 115
Cipher = 103 89 89
Mod 256 = 129 115 115
Mod 256 = 103 89 89

R G B
R G B
Piksel 5,0 = 141 128 219
Piksel 5,1 = 107 174 175
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 76 62 152
Cipher = 42 108 108
Mod 256 = 76 62 152
Mod 256 = 42 108 108

R G B
R G B
Piksel 5,2 = 201 188 189
Piksel 5,3 = 212 99 200
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 136 122 122
Cipher = 147 33 133
Mod 256 = 136 122 122
Mod 256 = 147 33 133

R G B
R G B
Piksel 6,0 = 180 167 168
Piksel 6,1 = 203 190 191
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 115 101 101
Cipher = 138 124 124
Mod 256 = 115 101 101
Mod 256 = 138 124 124

R G B
R G B
Piksel 6,2 = 169 160 159
Piksel 6,3 = 185 176 175
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 104 94 92
Cipher = 120 110 108
Mod 256 = 104 94 92
Mod 256 = 120 110 108

R G B
R G B
Piksel 6,2 = 161 160 159
Piksel 6,3 = 155 146 145
Kunci = 65 66 67
Kunci = 65 66 67
Cipher = 96 94 92
Cipher = 90 80 78
Mod 256 = 96 94 92
Mod 256 = 90 80 78

5. Hasil dekripsi gambar

Tabel 6 : Nilai-nilai Elemen Warna Setiap Piksel Citra Terdekripsi

ISSN : 2548-6985

Piksel	0			1			2			3		
	RED	GREEN	BLUE	RED	GREEN	BLUE	RED	GREEN	BLUE	RED	GREEN	BLUE
0	187	184	205	176	173	194	132	129	150	203	200	221
1	181	178	199	133	130	151	106	103	124	175	172	193
2	138	128	139	56	46	57	41	31	42	103	93	104
3	126	116	127	54	44	55	36	26	37	91	81	92
4	129	115	115	103	89	89	76	62	62	122	108	108
5	136	122	122	147	133	133	115	101	101	138	124	124
6	104	94	92	120	110	108	96	86	84	90	80	78

Hasil yang diperoleh dari nilai desimal pada piksel yang terdekripsi ternyata mengalami perubahan nilai desimal menjadi nilai-nilai piksel citra awal.

KESIMPULAN

Beberapa kesimpulan yang diperoleh pada pembahasan bab-bab sebelumnya dalam penyelesaian penelitian di atas adalah sebagai berikut :

1. Prosedur penyandian gambar dilakukan dengan cara menginput gambar asli, lalu ambil nilai decimal dari setiap piksel lalu tambahkan kunci, kemudian hasil nilai piksel dan kunci di moduluskan maka hasil modulus tersebut adalah nilai tersandi.
2. Proses pengaman data gambar ini dilakukan dengan mengubah nilai-nilai piksel aslinya dengan cara menjumlahkan nilai elemen warna asli dengan kunci lalu di moduluskan 256 dalam proses enkripsinya, sedangkan pada proses dekripsinya jumlah nilai elemen warna terenkripsi dikurang nilai kunci lalu di moduluskan 256.
3. Perancangan aplikasi dengan *visual basic 2008* akan memberikan penyelesaian permasalahan dengan mengoperasikan aplikasi yang telah dibuat seperti *form login, form* menu utama, *form* menu enkripsi dan *form* menu dekripsi.

DAFTAR PUSTAKA

1. Abdul Kadir & Terra CH.TRIWAHYUNI, “Pengenalan Teknologi Informasi”, Penerbit Andi, Yogyakarta, 2005
2. Anjik Sukmaaji,”Jaringan Komputer”, Penerbit Andi, 2009.
3. Darma Putra, “Pengolahan Citra Digital”, Penerbit Andi, Yogyajarta, 2010.
4. Dini Hari Pertiwi (2011). Desain Dan Implementasi Sistem Informasi Perpustakaan Berbasis Web Dengan MVC (Model View Controler). Jurnal Teknologi Dan Informatika, 126.
5. Dony Ariyus, ”Komunikasi Data”, Penerbit Andi, Yogyajarta, Edisi 6, 2008.
6. Harvei Desmon Hutahaean (2015), “Teknik Penajaman Citra Digital Dengan Menggunakan Metode Contrast Streching. Pelita Informatika Budi Darma, Vol.III, Maret 2013, 35-38.
7. Hendrayudi, “Dasar-dasar Pemrograman Microsoft Visual Basic 2008”, Penerbit Satunusa, Bandung, 2010.
8. Munawar, “Pemodelan visual dengan UML”, Penerbit Graha Ilmu, 2005.
9. Rifki Sadikin, “Kriptografi Untuk Keamanan Jaringan”, Penerbit Andi, Yogyajarta, 2012.