Abstrak


Dalam skripsi ini dirancang aplikasi kriptografi visual yang diterapkan pada gambar hitam putih berjenis bitmap. Gambar dienkripsi menjadi beberapa bagian yang harus digabungkan untuk dapat merekonstruksi gambar yang dienkripsi. Dengan adanya aplikasi ini diharapkan dapat memenuhi kebutuhan pengguna awam kriptografi yang membutuhkan kemudahan dalam pemakaian tetapi memiliki tingkat keamanan yang tinggi.

Dari perancangan ini memperlihatkan hasil yang cukup baik dan memiliki tingkat keamanan sempurna sehingga aman dari pihak attacker.

Kata Kunci:
visual cryptography, visual secret sharing schemes
UCAPAN TERIMA KASIH

Puji syukur kepada Tuhan Yang Maha Esa atas berkat dan rahmatnya sehingga penulis dapat menyusun dan menyelesaikan skripsi ini. Skripsi ini disusun sebagaimana salah satu syarat dalam menyelesaikan program studi Strata 1 di Universitas Bina Nusantara, Jakarta.

Penulis juga mengucapkan banyak terima kasih atas keterlibatan berbagai pihak yang telah membantu. Ucapan terima kasih ditujukan kepada:

- Rektor Universitas Bina Nusantara, Dr. Ir. Th. Widia S., MM. (Almh.) yang telah memberikan kesempatan kepada penulis untuk mendapatkan pengajaran dan membuat penulisan skripsi ini.
- Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam, Prof. Gerardus Polla, Dr., Drs., M.App.Sc. yang telah memberikan mata kuliah Seminar sebagai persiapan penulis dalam membuat penulisan skripsi ini.
- Ketua Jurusan Teknik Informatika dan Matematika, Wikaria Gazali, S.Si., M.T. yang telah membantu dalam persiapan skripsi.
- Sekretaris Jurusan Teknik Informatika dan Matematika, Ngarap Imanuel Manik, Drs., M. Kom yang telah membantu dalam awal pemilihan topik serta dosen pembimbing.
- Dosen Pembimbing, Wikaria Gazali, S.Si., M.T. dan Haryono Socparno, Dr., Ir. yang telah banyak memberikan pengarahan dan bimbingan sehingga skripsi ini dapat terselesaikan dengan baik.
- Para dosen yang selama ini telah memberikan bimbingan selama melaksanakan perkuliahan dan bimbingan tersebut menjadi bekal untuk melakukan penulisan skripsi ini.
- Orang tua dan kehargaan penulis yang telah banyak memberikan dorongan, baik dorongan spiritual maupun material selama penulisan skripsi ini.
- Rekan-rekan penulis yang telah banyak memberikan dorongan moril dan banyak membantu penulisan dalam penyelesaian skripsi ini.
- Semua pihak yang telah membantu penulis dalam menyelesaikan penulisan skripsi yang tidak dapat disebutkan satu persat.
- Akhir kata, penulis berharap skripsi ini dapat bermanfaat dan dapat dikembangkan lagi bagi para pembaca dan para almamater.

Jakarta, Januari 2005

Penulis
# DAFTAR ISI

<table>
<thead>
<tr>
<th>Halaman Judul Luar</th>
<th>Halaman</th>
<th>i</th>
</tr>
</thead>
<tbody>
<tr>
<td>Halaman Judul Dalam</td>
<td>Halaman</td>
<td>ii</td>
</tr>
<tr>
<td>Halaman Persetujuan Hardcover</td>
<td>Halaman</td>
<td>iii</td>
</tr>
<tr>
<td>Halaman Pernyataan Dewan Penguji</td>
<td>Halaman</td>
<td>iv</td>
</tr>
<tr>
<td>Abstrak</td>
<td>Halaman</td>
<td>v</td>
</tr>
<tr>
<td>Ucapan Terima Kasih</td>
<td>Halaman</td>
<td>vi</td>
</tr>
<tr>
<td>Daftar Isi</td>
<td>Halaman</td>
<td>vii</td>
</tr>
<tr>
<td>Daftar Tabel</td>
<td>Halaman</td>
<td>ix</td>
</tr>
<tr>
<td>Daftar Gambar</td>
<td>Halaman</td>
<td>x</td>
</tr>
<tr>
<td>Daftar Lampiran</td>
<td>Halaman</td>
<td>xii</td>
</tr>
</tbody>
</table>

## BAB 1 PENDAHULUAN

1. Latar Belakang
   1.1 Sejarah Singkat
   1.2 Ruang Lingkup
   1.3 Rumusan Perancangan
   1.4 Metodologi Penelitian
   1.5 Tujuan dan Manfaat

## BAB 2 LANDASAN TEORI

2. Kriptografi (Cryptography)
   2.1 Sejarah Singkat
   2.2 Shift Transformation Cryptosystem (Julius Cipher)
   2.3 Symmetric dan Asymmetric Cryptosystem
   2.4 Cryptanalyt
   2.5 Polyalphabetic Cryptosystem
   2.6 One-Time Pad Cryptosystem
   2.7 Password dan Jenis Kunci Enkripsi Lainnya
   2.8 Penggunaan Enkripsi
   2.9 Secret Sharing Schemes

## BAB 3 PERANCANGAN PROGRAM

3.1 Struktur Menu

vii
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>State Transition Diagram ((STD)</td>
<td>36</td>
</tr>
<tr>
<td>3.3</td>
<td>Rancangan Jilay</td>
<td>39</td>
</tr>
<tr>
<td>3.4</td>
<td>Spesifikasi Modul</td>
<td>45</td>
</tr>
<tr>
<td>BAB 4</td>
<td>IMPLEMENTASI DAN EVALUASI</td>
<td>71</td>
</tr>
<tr>
<td>4.1</td>
<td>Implementasi Sistem</td>
<td>71</td>
</tr>
<tr>
<td>4.1.1</td>
<td>Kebutuhan Perangkat Keras dan Perangkat Lunak</td>
<td>71</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Spesifikasi Minimum Perangkat Keras dan Perangkat Lunak</td>
<td>72</td>
</tr>
<tr>
<td>4.1.3</td>
<td>Kebutuhan Sumber Daya Manusia</td>
<td>74</td>
</tr>
<tr>
<td>4.1.4</td>
<td>Prosedur Pengoperasian Aplikasi</td>
<td>74</td>
</tr>
<tr>
<td>4.1.5</td>
<td>Analisis Masalah Ssnt Implementasi</td>
<td>79</td>
</tr>
<tr>
<td>4.2</td>
<td>Hasil Penelitian</td>
<td>88</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Hasil Penelitian dengan menggunakan teknik 2 out of 2</td>
<td>89</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Hasil Penelitian dengan menggunakan teknik 3 out of 3</td>
<td>94</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Pengujian keamanan data untuk teknik 3 out of 3</td>
<td>99</td>
</tr>
<tr>
<td>4.3</td>
<td>Evaluasi Hasil Penelitian</td>
<td>102</td>
</tr>
<tr>
<td>BAB 5</td>
<td>KESIMPULAN DAN SARAN</td>
<td>104</td>
</tr>
<tr>
<td>5.1</td>
<td>Kesimpulan</td>
<td>104</td>
</tr>
<tr>
<td>5.2</td>
<td>Saran</td>
<td>105</td>
</tr>
<tr>
<td></td>
<td>Daftar Pustaka</td>
<td>xiii</td>
</tr>
<tr>
<td></td>
<td>Daftar Riwayat Hidup</td>
<td>xv</td>
</tr>
<tr>
<td></td>
<td>Lampiran</td>
<td>xvi</td>
</tr>
<tr>
<td>Tabel 2.1</td>
<td>Tabel alphabet shift transformation cryptosystem</td>
<td>Halaman 7</td>
</tr>
<tr>
<td>Gambar</td>
<td>Gambar Isi</td>
<td>Halaman</td>
</tr>
<tr>
<td>--------</td>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>2.1</td>
<td>Perbedaan symmetric cryptosystem dengan asymmetric cryptosystem</td>
<td>9</td>
</tr>
<tr>
<td>2.2</td>
<td>Barbagai share berukuran 2 x 2 subpixel</td>
<td>23</td>
</tr>
<tr>
<td>2.3</td>
<td>Share untuk pemrosesan visual secret sharing 4 out of 4</td>
<td>25</td>
</tr>
<tr>
<td>2.4</td>
<td>Diagram Classic Life Cycle</td>
<td>32</td>
</tr>
<tr>
<td>2.5</td>
<td>Notasi Modul</td>
<td>33</td>
</tr>
<tr>
<td>2.6</td>
<td>Notasi Tampilan</td>
<td>33</td>
</tr>
<tr>
<td>2.7</td>
<td>Notasi Tindakan</td>
<td>33</td>
</tr>
<tr>
<td>2.8</td>
<td>Notasi Kondisi dan Aksi</td>
<td>33</td>
</tr>
<tr>
<td>2.9</td>
<td>Contoh penggambaran kondisi dan aksi</td>
<td>34</td>
</tr>
<tr>
<td>3.1</td>
<td>Rancangan Struktur Menu Utama</td>
<td>35</td>
</tr>
<tr>
<td>3.2</td>
<td>Rancangan Struktur Menu File</td>
<td>35</td>
</tr>
<tr>
<td>3.3</td>
<td>Rancangan Struktur Menu Tools</td>
<td>36</td>
</tr>
<tr>
<td>3.4</td>
<td>Rancangan Struktur Menu Help</td>
<td>36</td>
</tr>
<tr>
<td>3.5</td>
<td>STD Menu Utama</td>
<td>37</td>
</tr>
<tr>
<td>3.6</td>
<td>STD Menu File</td>
<td>37</td>
</tr>
<tr>
<td>3.7</td>
<td>STD Menu Tools</td>
<td>38</td>
</tr>
<tr>
<td>3.8</td>
<td>STD Menu Help</td>
<td>39</td>
</tr>
<tr>
<td>3.9</td>
<td>Rancangan Layar Utama</td>
<td>40</td>
</tr>
<tr>
<td>3.10</td>
<td>Rancangan Layar How to Use</td>
<td>44</td>
</tr>
<tr>
<td>3.11</td>
<td>Rancangan Layar About</td>
<td>44</td>
</tr>
<tr>
<td>3.12</td>
<td>Rancangan Layar Konfirmasi</td>
<td>45</td>
</tr>
<tr>
<td>4.1</td>
<td>Layar Utama program aplikasi Kriptografi Visual</td>
<td>74</td>
</tr>
<tr>
<td>4.2</td>
<td>Tampilan layar setelah pengguna memilih gambar yang akan dienkripsi</td>
<td>75</td>
</tr>
<tr>
<td>4.3</td>
<td>Tampilan layar setelah pengguna melakukan enkripsi (tabshet Share 1 aktif)</td>
<td>76</td>
</tr>
<tr>
<td>4.4</td>
<td>Tampilan layar setelah pengguna melakukan enkripsi (tabshet Share 2 aktif)</td>
<td>77</td>
</tr>
<tr>
<td>4.5</td>
<td>Tampilan layar setelah pengguna melakukan dekripsi (tabshet Decrypted Image (Preview) aktif)</td>
<td>78</td>
</tr>
<tr>
<td>4.6</td>
<td>Tampilan layar setelah pengguna melakukan dekripsi (tabshet Decrypted Image (Without noise) aktif)</td>
<td>79</td>
</tr>
<tr>
<td>4.7</td>
<td>Gambar A</td>
<td>80</td>
</tr>
<tr>
<td>4.8</td>
<td>Pola subpixel 2 x 2 pada teknik enkripsi 3 out of 3 berdasarkan teori</td>
<td>80</td>
</tr>
<tr>
<td>4.9</td>
<td>Ketiga share hasil enkripsi gambar A dengan menggunakan teknik 3 out of 3 pola subpixel 2 x 2 berdasarkan teori</td>
<td>81</td>
</tr>
<tr>
<td>4.10</td>
<td>Pola subpixel 2 x 2 untuk teknik enkripsi 3 out of 3 berdasarkan referensi di internet</td>
<td>82</td>
</tr>
<tr>
<td>4.11</td>
<td>Ketiga share hasil enkripsi gambar A dengan menggunakan teknik 3 out of 3 dengan pola subpixel 2 x 2 dari referensi internet</td>
<td>83</td>
</tr>
</tbody>
</table>
Gambar 4.12  Hasil dekripsi 2 share acak dari 3 share hasil enkripsi teknik 3 out of 3 menggunakan pola subpixel 2 x 2 dari referensi internet .................................................. 84
Gambar 4.13  Pola-pola yang dihasilkan dengan menggabungkan dua pola subpixel 2 x 2 teknik enkripsi 3 out of 3 ................................................................. 85
Gambar 4.14  Berbagai pola subpixel 2 x 2 enkripsi teknik 3 out of 3 untuk pixel berwarna putih rancangan penulis ......................................................... 87
Gambar 4.15  Berbagai pola subpixel 2 x 2 enkripsi teknik 3 out of 3 untuk pixel berwarna hitam rancangan penulis ......................................................... 87
Gambar 4.16  Pola gabungan dua share hasil enkripsi pixel berwarna putih/hitam .................................................................................................................. 88
Gambar 4.17  Gambar B ......................................................... 89
Gambar 4.18  Share pertama hasil enkripsi teknik 2 out of 2 gambar B ................................................................. 91
Gambar 4.19  Share kedua hasil enkripsi teknik 2 out of 2 gambar B ................................................................. 91
Gambar 4.20  Hasil dekripsi kedua share gambar B ......................................................................................................................... 93
Gambar 4.21  Pola subpixel 2 x 2 untuk pixel berwarna putih ................................................................. 95
Gambar 4.22  Pola subpixel 2 x 2 untuk pixel berwarna hitam ......................................................................................................................... 96
Gambar 4.23  Share 1 hasil enkripsi teknik 3 out of 3 gambar B ................................................................. 96
Gambar 4.24  Share 2 hasil enkripsi teknik 3 out of 3 gambar B ................................................................. 97
Gambar 4.25  Share 3 hasil enkripsi teknik 3 out of 3 gambar B ................................................................. 97
Gambar 4.26  Hasil dekripsi ketiga share gambar B ......................................................................................................................... 98
Gambar 4.27  Share 1 + Share 2 ................................................................. 100
Gambar 4.28  Share 1 + Share 3 ................................................................. 101
Gambar 4.29  Share 2 + Share 3 ................................................................. 101
<table>
<thead>
<tr>
<th>Lampiran</th>
<th>Judul</th>
<th>Halaman</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Listing program</td>
<td>1. i</td>
</tr>
<tr>
<td>B</td>
<td>Pola gabungan dari dua pola subpixel 2 x 2 pada teknik enkripsi 3 out of 3</td>
<td>1.22</td>
</tr>
<tr>
<td>C</td>
<td>Contoh print-out hasil enkripsi menggunakan teknik enkripsi 2 out of 2</td>
<td>1.23</td>
</tr>
</tbody>
</table>