

**APLIKASI DAN IMPLEMENTASI SECRET SHARING
MENGUNAKAN KRIPTOGRAFI VISUAL PADA CITRA BINER**

PUBLIKASI JURNAL SKRIPSI



Disusun Oleh:

LUQMAN HAKIM

NIM. 0710633061-63

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

UNIVERSITAS BRAWIJAYA

FAKULTAS TEKNIK

MALANG

2014



KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS BRAWIJAYA
FAKULTAS TEKNIK
JURUSAN TEKNIK ELEKTRO
Jalan MT Haryono 167 Telp & Fax. 0341 554166 Malang 65145

KODE
PJ-01

**PENGESAHAN
PUBLIKASI HASIL PENELITIAN SKRIPSI
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK UNIVERSITAS BRAWIJAYA**

NAMA : LUQMAN HAKIM

NIM : 0710633061- 63

PROGRAM STUDI : TEKNIK REKAYASA KOMPUTER

**JUDUL SKRIPSI : APLIKASI DAN IMPLEMENTASI SECRET SHARING
MENGUNAKAN KRIPTOGRAFI VISUAL PADA CITRA
BINER**

TELAH DI-REVIEW DAN DISETUJUI ISINYA OLEH:

Pembimbing I

Pembimbing II

Waru Djurianto, ST., MT.
NIP. 19690725 199702 1 001

Ir. Muhammad Aswin, MT.
NIP 19640626 199002 1 001

APLIKASI DAN IMPLEMENTASI SECRET SHARING MENGGUNAKAN KRIPTOGRAFI VISUAL PADA CITRA BINER

Luqman Hakim NIM. 0710633061
Jurusan Teknik Elektro, Fakultas Teknik, Universitas Brawijaya
Jalan MT. Haryono 167, Malang 65145, Indonesia
E-mail: qulhak_sboy@yahoo.com
Pembimbing :
Waru Djurianto, ST., MT., Ir. Muhammad Aswin, MT.

Abstrak

Secret sharing merupakan salah satu metode untuk mengamankan suatu rahasia dengan membagi atau mendistribusikan rahasia tersebut menjadi beberapa bagian yang disebut *share*, setiap bagian dari rahasia tersebut tidak memberikan informasi apa-apa mengenai rahasia yang dimaksud bila tidak digabungkan dengan bagian yang lainnya. Salah satu alasan adanya *secret sharing* adalah perlindungan terhadap ancaman kehilangan kunci kriptografi. Pada skripsi ini dibuat suatu program aplikasi *secret sharing* menggunakan algoritma kriptografi visual. Kriptografi visual adalah skema pembagian yang digunakan dalam distribusi gambar. Kriptografi visual merupakan salah satu perluasan dari *secret sharing* yang diimplementasikan untuk suatu citra. Seperti halnya teknik kriptografi yang lain, kriptografi visual memiliki persyaratan kerahasiaan, integritas data, dan otentikasi. Kriptografi visual yaitu teknik kriptografi data berupa gambar atau citra dengan membagi gambar tersebut menjadi beberapa bagian. Setiap bagian gambar tersebut merupakan subset dari gambar aslinya. Hasil dari proses aplikasi ini adalah citra rahasia yang berupa hasil enkripsi citra yaitu citra share 1 dan citra share 2 dan hasil dekripsi. Dari hasil enkripsi citra yang diujikan diperoleh prosentase keberhasilan dalam merahasiakan isi informasi dari citra aslinya. Dan pada hasil citra dekripsi menampilkan isi informasi dari citra asli. Prosentase keberhasilan pada citra share 1 dan share 2 menunjukkan kedua share tersebut 100% tidak menampilkan isi informasi pada citra aslinya.

Kata kunci: *Secret Sharing, kriptografi, kriptografi visual.*

I. PENDAHULUAN

1.1 Latar Belakang

Pada zaman yang semakin modern ini, teknologi yang digunakan saat ini semakin berkembang. Perkembangan teknologi yang begitu

pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi. Semakin banyak kebutuhan dalam berkomunikasi, semakin tinggi permintaan kelengkapan spek atau fitur pada alat komunikasi tersebut. Salah satu fungsi yang dibutuhkan saat ini adalah keamanan agar privasi informasi dapat terpenuhi.

Seiring dengan tuntutan keamanan terhadap kerahasiaan informasi yang saling dipertukarkan tersebut, semakin meningkat. Dalam kegiatan penting seperti transaksi bisnis, penyimpanan barang berharga, dan data rahasia pribadi membutuhkan keamanan agar tidak merugikan pihak yang berhak untuk mengetahui dan memiliki informasi tersebut. Walaupun informasi atau data tersebut tidak ditujukan kepada pihak lain, ada kemungkinan data tersebut dapat tersebar dan dilihat dengan bebas tanpa sepengetahuan pemilik yang kemudian mengakibatkan kebocoran informasi. Salah satu penyebabnya adalah lemahnya keamanan metode, algoritma, virus, atau serangan dari pihak lain. Adapun untuk berkomunikasi dengan pihak lain tanpa tersadap pihak ketiga, kedua pihak yang berkebutuhan untuk berkomunikasi dapat melakukan perjanjian dalam menggunakan kode atau simbol yang hanya diketahui oleh kedua belah pihak yang disampaikan secara bertatap muka atau metode komunikasi lainnya. Dengan banyaknya pengguna seperti suatu perusahaan ataupun individu yang tidak ingin suatu informasi yang disampaikannya dapat diketahui oleh orang lain atau kompetitornya yang bukan haknya untuk mengetahui isi dari informasi tersebut. Oleh karena itu dikembangkanlah ilmu yang mempelajari tentang cara pengamanan data atau yang dikenal dengan kriptografi.

Dalam algoritma kriptografi terdapat dua konsep utama yaitu enkripsi dan dekripsi. Enkripsi merupakan hal yang sangat penting dalam kriptografi, yaitu proses dimana informasi yang akan dikirim diubah menjadi kode-kode yang tidak dimengerti. Sedangkan Dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya.

Dengan banyaknya informasi berupa citra/gambar, maka dalam skripsi ini dibuat suatu

program aplikasi yang mampu mengenkripsi sebuah citra/ gambar untuk merahasiakan isi pesan gambar dari pihak yang tidak bertanggung jawab. Dan pada studi kasus ini citra/ gambar yang akan dienkripsi yaitu citra hitam putih atau citra biner menggunakan algoritma visual kriptografi. Penulis mengharapkan pembuatan aplikasi ini mampu merahasiakan data-data penting berupa gambar/ citra biner. Sehingga tidak dapat diketahui oleh pihak yang tak bertanggung jawab.

Kriptografi visual merupakan teknik kriptografi data berupa gambar atau citra dengan membagi gambar tersebut menjadi beberapa bagian. Setiap bagian gambar tersebut adalah subset dari gambar awalnya. Jika dihasilkan n bagian dalam proses enkripsi, maka jika hanya terdapat $n-1$ bagian, gambar tidak dapat didekripsi. Tujuan awal penggunaan metode ini yaitu untuk membuat sebuah model kriptografi data berupa gambar atau citra yang dapat didekripsi tanpa bantuan komputer. Skema yang digunakan pada tugas akhir ini adalah (2,2). Sebuah citra rahasia akan dilakukan pembagian citra menjadi dua buah citra dengan membagi setiap piksel menjadi 4 subpiksel yaitu 2×2 . Dalam pendekripsian dilakukan penumpukan kedua buah citra yang telah dienkripsi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan diatas, maka rumusan masalah ditekankan pada :

1. Bagaimana membuat aplikasi yang mampu untuk mengenkripsi citra/ gambar hitam putih atau citra biner.
2. Bagaimana cara membagi sebuah citra asli menjadi dua buah citra/ gambar tersamar.

1.3 Batasan Masalah

Beberapa hal yang menjadi batasan-batasan dalam pembuatan program ini adalah sebagai berikut :

1. Pembuatan program menggunakan MATLAB.
2. Masukan citra/ gambar berupa citra hitam putih atau citra biner.

1.4 Tujuan

Tujuan penyusunan skripsi ini adalah :

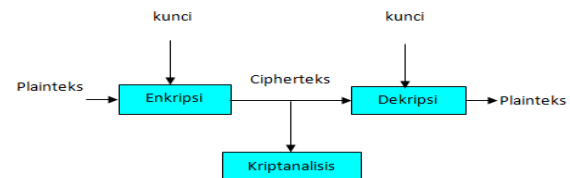
Merancang dan membangun suatu aplikasi software yang dapat mengenkripsi sebuah citra/ gambar biner menjadi dua buah citra yang tidak diketahui isi informasinya dan mendekripsikan untuk mengetahui isi dari citra asalnya.

II. TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi adalah ilmu yang digunakan untuk mengacak data sedemikian rupa sehingga tidak bisa dibaca oleh pihak yang tidak berwenang. Hal ini data yang sudah diacak harus bisa dikembalikan

lagi seperti semula oleh pihak yang berwenang. Proses pengacakan disebut dengan Enkripsi (*Encryption*) dan data yang diacak disebut *plain text*. Data yang diacak menggunakan kunci Enkripsi (*Encryption key*). Hasil dari proses pengacakan itu sendiri disebut *Chiper text*. Kemudian proses untuk mengembalikan *Chiper text* ke *Plain text* disebut dekripsi (*Decryption*). Kunci yang dipergunakan pada tahapan dekripsi disebut kunci dekripsi (*Decryption key*).



Gambar 2.1 sistem kriptografi secara umum

2.2 Citra Digital

Citra digital terdiri dari pixels (picture element). Setiap piksel merepresentasikan warna atau tingkat keabuan pada satu titik di dalam citra. Citra digital tersusun dalam bentuk raster (grid atau kisi). Titik dalam suatu citra disebut piksel (picture element). Nilai x pada titik koordinat (x,y) merupakan sumbu mendatar (horisontal) yang menunjukkan kolom dari suatu piksel dalam citra sedangkan y (sumbu vertikal) menunjukkan baris dari suatu piksel. Setiap piksel memiliki nilai yang menunjukkan tingkat intensitas keabuan dari piksel itu sendiri.

2.3 Karakteristik File citra

Karakteristik file citra ditentukan oleh resolusi dan kedalaman bit. *Image resolution* adalah jumlah *pixel* per inci (kepadatan *pixel* per inci) yang dinyatakan dengan *pixel x pixel*. Semakin tinggi resolusi citra, maka semakin baik kualitas citra tersebut. citra dengan resolusi tinggi akan lebih detil serta jika citra diperbesar maka detil citra masih jelas. Namun, resolusi yang tinggi akan mengakibatkan jumlah bit yang diperlukan untuk menyimpan atau mentransmisikannya meningkat.

Kedalaman bit merupakan jumlah bit yang digunakan untuk merpresentasikan tiap *pixel*. Semakin banyak jumlah bit yang digunakan untuk merepresentasikan sebuah *pixel*, yang berarti semakin tinggi kedalaman *pixel*-nya, maka semakin tinggi pula kualitasnya, dengan resiko jumlah bit yang diperlukan menjadi lebih tinggi.

Kedalaman warna	Resolusi Warna	Kalkulasi
1 bit	2 warna	$2^1 (2)$
2 bit	4 warna	$2^2 (2x2)$
3 bit	8 warna	$2^3 (2x2x2)$
4 bit	16 warna	$2^4 (2x2x2x2)$
5 bit	32 warna	$2^5 (2x2x2x2x2)$
6 bit	64 warna	$2^6 (2x2x2x2x2x2)$
7 bit	128 warna	$2^7 (2x2x2x2x2x2x2)$
8 bit	256 warna	$2^8 (2x2x2x2x2x2x2x2)$

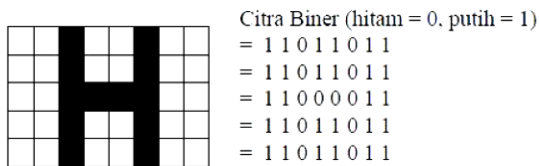
Tabel 2.1 Hubungan Antara Kedalaman Warna Dan Resolusi Warna

Color depth yang digunakan dalam pengerjaan skripsi ini yaitu *color depth* dengan kedalaman citra 1 bit. Informasi warna hanya sebanyak dua monokrom atau hitam dan putih. *Pixel* dengan nilai 0 sebagai warna hitam. *Pixel* dengan nilai 1 sebagai warna putih.

2.4 Citra Biner

Citra biner adalah citra yang hanya mempunyai dua nilai derajat keabuan yaitu hitam dan putih. Meskipun saat ini citra berwarna lebih disukai karena memberi kesan yang lebih kaya daripada citra biner, namun tidak membuat citra biner mati. Pada beberapa aplikasi citra biner masih tetap dibutuhkan, misalnya citra logo instansi (yang hanya terdiri atas warna hitam dan putih), citra kode batang (*bar code*) yang tertera pada label barang, citra hasil pemindaian dokumen teks, dan sebagainya.

Citra biner hanya mempunyai dua nilai derajat keabuan : hitam dan putih. Piksel-piksel objek bernilai 0 dan piksel-piksel latar belakang bernilai 1. Untuk warna putih pada gambar bernilai 1 dan warna hitam bernilai 0.



Gambar 2.2 contoh pengkodean citra biner

2.5 Kriptografi Visual

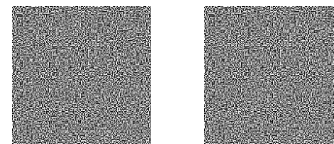
Kriptografi visual adalah skema pembagian yang digunakan dalam distribusi gambar. Kriptografi visual merupakan salah satu perluasan dari *secret sharing* yang diimplementasikan untuk suatu citra. Seperti halnya teknik kriptografi yang lain, kriptografi visual memiliki persyaratan kerahasiaan, integritas data, dan otentikasi. Kriptografi visual yaitu teknik kriptografi data berupa gambar atau citra dengan membagi gambar tersebut menjadi beberapa bagian. Setiap bagian

gambar tersebut merupakan subset dari gambar aslinya.

Versi dasarnya mempresentasikan *secret sharing* (2,2). Maksudnya skema tersebut menghasilkan 2 (dua) citra pembagi dari gambar aslinya (P) yaitu sebuah gambar hitam putih. Dimana gambar P1 untuk bagian gambar 1 dan P2 untuk bagian gambar 2. P1 dan P2 merupakan distribusi acak dari pixel hitam putih dan tidak menunjukkan informasi apapun. Namun saat P1 dan P2 dilapiskan/ ditumpuk, maka akan didapat informasi seperti gambar aslinya. Apabila hanya ada P1, maka informasi P tidak dapat diketahui tanpa ada P2. Berikut adalah ilustrasi citra asal (*plainteks*), citra tersandikan (*cipherteks*) dan citra dekripsi:

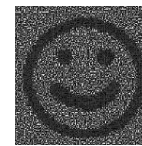


a.plainteks



Share 1 Share 2

b.cipherteks



c.dekripsi citra

Gambar 2.4 a. Citra asal (*plainteks*) b.citra enkripsi (*cipherteks*) c. Dekripsi citra

III. METODE PENELITIAN

Pada tahap ini dijelaskan mengenai langkah-langkah yang akan dilakukan untuk merancang dan mengimplementasikan perangkat lunak yang akan dibuat. Adapun langkah-langkah yang akan dilakukan adalah sebagai berikut:

1. Studi literatur
2. Penentuan spesifikasi aplikasi
3. Perancangan dan implementasi
4. Pengujian
5. Pengambilan kesimpulan dan saran

IV. PERANCANGAN DAN IMPLEMENTASI

Perancangan dan implementasi ini meliputi perancangan sistem, penentuan spesifikasi alat, perancangan perangkat keras, dan perangkat lunak.

4.1 Perancangan Sistem

Perancangan sistem dikerjakan dengan beberapa tahap meliputi proses memasukkan citra biner, proses enkripsi citra. Perancangan diawali dengan penggambaran blok diagram kerja sistem

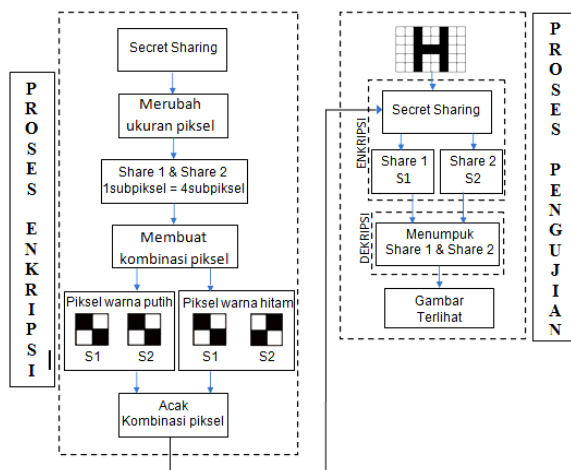
yang menunjukkan cara kerja aplikasi secara umum. Berikut urutan blok diagram sistem :



Gambar 4.1 Blok diagram sistem

Berikut adalah penjelasan tiap blok diagram sistem pada gambar 4.1 :

1. Citra Biner adalah citra yang hanya mempunyai dua kedalaman warna yaitu warna hitam dan warna putih yang digunakan sebagai masukan sistem.
2. Enkripsi citra pada citra biner yaitu proses awal dalam mengubah citra asli menjadi dua buah citra yang tersamarkan.
3. Hasil enkripsi merupakan keluaran dari hasil bagi dua citra yang tak terlihat isi informasi dari citra aslinya, hasil enkripsi tersebut yaitu citra share 1 dan citra share 2.



Gambar 4.2 diagram sistem

4.2 Implementasi Sistem

Implementasi sistem program ini mencakup spesifikasi perangkat keras dan spesifikasi perangkat lunak.

4.2.1 Spesifikasi perangkat keras dan perangkat lunak

Menentukan perangkat yang digunakan untuk menunjang pembuatan aplikasi:

1. Perangkat Keras

- A. Notebook
- Spesifikasi :
- Processor : Intel(R) Celeron(R) CPU 847 @ 1.10GHz
 - Memory : 4096 MB RAM
 - VGA : Intel(R) HD Graphics

2. Perangkat Lunak

1. Sistem operasi : Microsoft Windows 8
2. Bahasa pemrograman : MATLAB R2012b

4.2.2. Implementasi Antar Muka

Aplikasi identifikasi kombinasi pola isyarat tangan memiliki tampilan seperti pada gambar dibawah. Aplikasi ini memiliki 2 tampilan yang menampilkan informasi berbeda sesuai fungsinya.

Aplikasi secret sharing menggunakan algoritma kriptografi visual pada citra biner memiliki tampilan seperti pada gambar dibawah. Aplikasi ini memiliki 4 (empat) kotak gambar untuk menampilkan informasi yang berbeda.



Gambar 4.3 Tampilan aplikasi secret sharing

V. PENGUJIAN

Untuk mengetahui apakah sistem bekerja dengan baik dan sesuai dengan perancangan, maka diperlukan serangkaian pengujian. Pengujian yang dilakukan dalam bab ini adalah sebagai berikut:

1. Pengujian dilakukan untuk mengetahui perubahan citra asli dengan citra hasil enkripsi yang meliputi perubahan ukuran piksel.
2. Hasil pengujian dengan mata manusia dengan memberi nilai pada citra hasil enkripsi.

5.1 Pengujian perubahan piksel

Pengujian ini bertujuan untuk mengetahui apakah program berhasil merubah ukuran piksel citra asli dengan citra hasil enkripsi dengan berbagai macam ukuran citra. Ukuran yang digunakan seperti pada tabel hasil 5.1 dibawah ini:

NO.	Nama Citra	Ukuran piksel citra asli	Ukuran piksel citra enkripsi	Isi gambar enkripsi	Ket
1.	Citra1	106 x 106 piksel	213 x 213 piksel	Tidak terlihat	Berhasil
2.	Citra2	113 x 113 piksel	227 x 227 piksel	Tidak terlihat	Berhasil
3.	Citra3	110 x 157 piksel	221 x 315 piksel	Tidak terlihat	Berhasil
4.	Citra4	150 x 150 piksel	301 x 301 piksel	Tidak terlihat	Berhasil
5.	Citra5	183 x 160 piksel	367 x 321 piksel	Tidak terlihat	Berhasil
6.	Citra6	204 x 170 piksel	409 x 341 piksel	Tidak terlihat	Berhasil
7.	Citra7	200 x 200 piksel	401 x 401 piksel	Tidak terlihat	Berhasil
8.	Citra8	200 x 200 piksel	401 x 401 piksel	Tidak terlihat	Berhasil
9.	Citra9	200 x 100 piksel	401 x 201 piksel	Tidak terlihat	Berhasil
10.	Citra10	300 x 225 piksel	601 x 551 piksel	Tidak terlihat	Berhasil

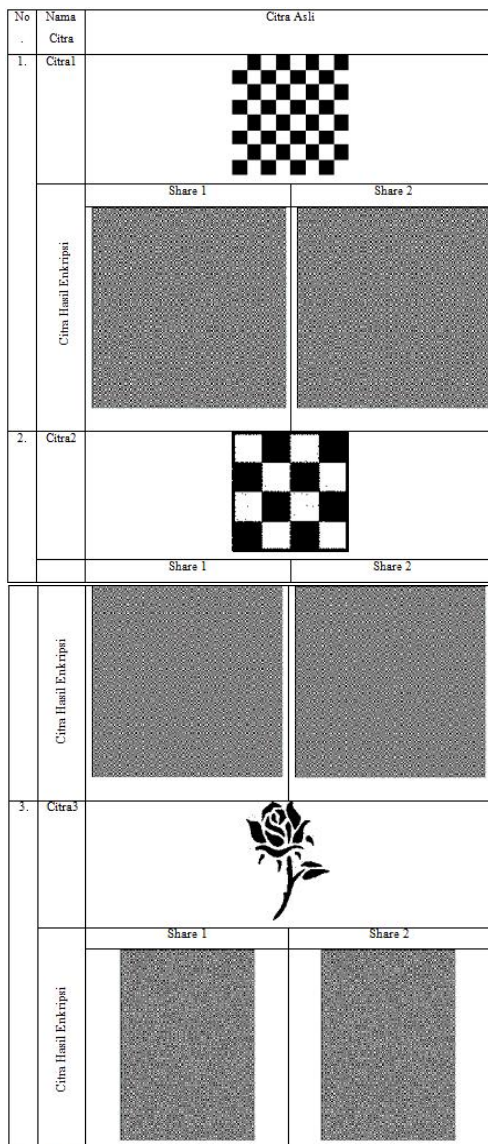
Tabel 5.1 Data pengujian perubahan ukuran piksel citra

Pada tabel 5.1 menunjukkan bahwa ukuran piksel untuk citra asli dengan citra enkripsi

mendapatkan perubahan ukuran pada citra enkripsi yaitu dua kali lebih besar dari ukuran aslinya, ini dikarenakan dalam proses enkripsi citra setiap subpiksel akan diubah menjadi 4 subpiksel yaitu 2x2 subpiksel.

5.2 Pengujian menggunakan bantuan mata manusia

Pengujian dilakukan dengan memperlihatkan citra hasil enkripsi kepada para penguji untuk mengetahui hasil enkripsi apakah gambar hasil tidak memperlihatkan isi informasi pada citra aslinya. Berikut contoh citra uji citra1, citra2 dan citra3 :



Gambar 5.1 contoh citra uji : citra1, citra2 dan citra3.

Dari hasil pengujian yang dilakukan pada citra yang telah melalui proses enkripsi, citra tersebut diperiksa dengan bantuan mata manusia untuk mengetahui apakah citra hasil tersebut tidak diketahui isi informasi gambar asli. Nilai yang digunakan adalah 1 = tidak terlihat, 2 = sedikit

terlihat informasi, 3 = lumayan terlihat informasi, 4 = terlihat jelas. Nilai yang terdapat pada tabel 5.2 adalah nilai prosentase rata – rata dari semua penilaian penguji. Pada citra uji semua citra yang sudah di enkripsi dalam penglihatan mata manusia rata – rata citra hasil tidak menunjukkan isi informasi citra aslinya.

No.	Nama Citra	Presentase nilai Share 1				Presentase nilai Share 2			
		1	2	3	4	1	2	3	4
1.	Citra1	100%	-	-	-	100%	-	-	-
2.	Citra2	100%	-	-	-	100%	-	-	-
3.	Citra3	100%	-	-	-	100%	-	-	-
4.	Citra4	100%	-	-	-	100%	-	-	-
5.	Citra5	100%	-	-	-	100%	-	-	-
6.	Citra6	100%	-	-	-	100%	-	-	-
7.	Citra7	100%	-	-	-	100%	-	-	-
8.	Citra8	100%	-	-	-	100%	-	-	-
9.	Citra9	100%	-	-	-	100%	-	-	-
10.	Citra10	100%	-	-	-	100%	-	-	-
Presentase uji %		100%	-	-	-	100%	-	-	-

Tabel 5.2 Hasil penilaian citra share1 dan share 2

IV. PENUTUP

Kesimpulan

Berdasarkan hasil perancangan, implementasi, pengujian dan analisis sistem maka dapat diambil kesimpulan sebagai berikut :

1. Skema yang digunakan untuk membagi citra asli menjadi dua buah citra enkripsi menggunakan skema (2,2), setiap subpiksel diubah menjadi empat buah subpiksel.
2. Kriptografi visual pada citra biner menghasilkan citra share yaitu share 1 dan share 2 yang tidak menampilkan isi informasi citra asli.
3. Pada citra share warna putih memiliki kombinasi yang sama, sedangkan untuk warna hitam memiliki kombinasi yang berbeda.
4. Kombinasi piksel warna putih tidak sepenuhnya menampilkan warna putih dan kombinasi piksel warna hitam sepenuhnya menampilkan warna hitam karena warna hitam merupakan isi informasi gambar.
5. Hasil dari pengujian citra asli menjadi dua buah citra enkripsi memiliki tingkat keberhasilan 100%.

Saran

Dalam perancangan dan pembuatan aplikasi secret sharing menggunakan algoritma kriptografi

visual pada citra biner diperlukan penyempurnaan untuk pengembangan selanjutnya. Berikut ini adalah beberapa hal yang perlu diperhatikan untuk pengembangan:

1. Skema yang digunakan dapat dikembangkan lebih dari (2,2) dengan skema (n,k).
2. Kriptografi visual yang telah dibuat dapat dikembangkan pada citra berwarna.

DAFTAR PUSTAKA

- [1] R. Panneerselvam, "Design and Analysis of Algorithms", School of Management Pondicherry University Pondicherry.
- [2] Jufriadif Na'am, "Metode Play Fair Cipher Dalam Mengamankan Sistem Database", Universitas Putra Indonesia, 2008.
- [3] M. Naor and A. Shamir, *Visual Cryptography*. Eurocrypt 1994: 1-12
- [4] Ir.Rinaldi Munir,M.T., "Pengantar Kriptografi",2004.
- [5] Makalah IF5054 a.n M.Pramana Baharsyah ("Pemanfaatan Steganografi dalam Kriptografi Visual")
- [6] A. Ross and A. A. Othman, "Visual Cryptography for Biometric Privacy", IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70-81, 2011.
- [7] N. Askari, C. Moloney and H.M. Heys, "A Novel Visual Secret Sharing Scheme Without Image Size Expansion", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, pp. 1-4, 2012.
- [8] Jonathan Weir, WeiQi Yan, "Visual Cryptography And Its Applications", 2012.
- [9] N. Askari, H.M. Heys, C.R. Moloney, "An Extended Visual Cryptography Scheme Without Pixel Expansion For Halftone Images", IEEE Canadian Conference of Electrical And Computer Engineering (CCECE), 2013.
- [10] Gunaidi Abdia Away. "The Shortcut of MATLAB Programming". Informatika Bandung. 2010.
- [11] V.R.Anitha, Dilip kumar Kotthapalli, "Extending the Visual Cryptography Algorithm Without Removing Cover Images", International Journal of Engineering Trends and Technology (IJETT), April 2013.