APLIKASI DAN IMPLEMENTASI SECRET SHARING MENGGUNAKAN KRIPTOGRAFI VISUAL PADA CITRA BINER

SKRIPSI

KONSENTRASI REKAYASA KOMPUTER

Diajukan Untuk Memenuhi Sebagian Persyaratan

Memperoleh Gelar Sarjana Teknik

Disusun Oleh:

LUQMAN HAKIM

NIM. 0710633061-63

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

UNIVERSITAS BRAWIJAYA

FAKULTAS TEKNIK

MALANG

2014

LEMBAR PERSETUJUAN

APLIKASI DAN IMPLEMENTASI SECRET SHARING MENGGUNAKAN KRIPTOGRAFI VISUAL PADA CITRA BINER

SKRIPSI

KONSENTRASI REKAYASA KOMPUTER

Diajukan Untuk Memenuhi Sebagian Persyaratan
Memperoleh Gelar Sarjana Teknik

Disusun oleh:

LUQMAN HAKIM

NIM. 0710633061-63

Telah diperiksa dan disetujui oleh :

Dosen Pembimbing I	Dosen Pembimbing II
Waru Djuriatno, ST., MT.	**Ir. Muhammad Aswin, MT.**
NIP. 19690725 199702 1 001	**NIP. 19640626 199002 1 001**

LEMBAR PENGESAHAN

APLIKASI DAN IMPLEMENTASI SECRET SHARING MENGGUNAKAN KRIPTOGRAFI VISUAL PADA CITRA BINER

SKRIPSI

KONSENTRASI REKAYASA KOMPUTER

Diajukan Untuk Memenuhi Sebagian Persyaratan

Memperoleh Gelar Sarjana Teknik

Disusun oleh:

LUQMAN HAKIM

NIM. 0710633061-63

Skripsi ini telah diuji dan dinyatakan lulus pada

tanggal 11 Agustus 2014

MAJELIS PENGUJI

Adharul Muttaqin, ST., MT.	**R. Arief Setyawan, ST., MT.**
NIP. 19760121 200501 1 001	**NIP. 19750819 199903 1 001**

Ali Mustofa, ST., MT.

NIP. 19710601 200003 1 001

Mengetahui

Ketua Jurusan Teknik Elektro

M. Aziz Muslim, S.T., M.T., Ph.D.

NIP. 19741203 200012 1 001

PENGANTAR

Alhamdulillah, segenap puji dan syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan rahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul "Aplikasi Dan Implementasi Secret Sharing Menggunakan Kriptografi Visual Pada Citra Biner" yang diajukan untuk memenuhi sebagian persyaratan memperoleh gelar Sarjana Teknik di Jurusan Teknik Elektro Universitas Brawijaya.

Penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada berbagai pihak yang telah membantu dan mendukung dalam penyelesaian skripsi ini, yaitu :

- Bapak M. Aziz Muslim, S.T., M.T., Ph.D. selaku Ketua Jurusan dan Bapak Hadi Suyono, S.T., M.T., Ph.D. selaku Sekretaris Jurusan Teknik Elektro Universitas Brawijaya,
- Bapak Mochammad Rif'an, S.T., M.T. selaku Ketua Program Studi Strata 1.
- Ibu Rusmi Ambarwati, ST., MT., selaku dosen penasehat akademik yang telah memberikan nasehat, arahan, dan motivasi selama proses akademik penulis,
- Bapak Waru Djuriatno, ST., MT., selaku Ketua Kelompok Dosen Keahlian Rekayasa Komputer Jurusan Teknik Elektro Universitas Brawijaya,
- Bapak Waru Djuriatno, ST., MT., dan Bapak Ir. Muhammad Aswin., MT., selaku Dosen Pembimbing atas segala bimbingan, nasehat, pengarahan, motivasi, saran dan masukan yang telah diberikan dalam pengerjaan skripsi,
- Keluarga di rumah. Ibu Dra. Hj. Jamilah, Abah Dr. H. A. Muhtadi Ridwan, MA. ,Kakak M. Nanang Choiruddin, SE., MM., Adik Zakiah Hidayati S.kep., Ns., Adik Ustadz Arif Furqon, dan Adik Luluk Arifah Kamila. atas segala nasehat, kasih sayang, perhatian dan kesabarannya serta telah banyak mendoakan kelancaran penulis hingga terselesaikannya skripsi ini,
- Tito, Wiro (Sableng), Wildan (Gitok), Novandra, Abdur, Lipo, Indra Haris, Ahda Gahara, Tomi Putro, Ulinnuha (Satria), dan CORE 2007 yang telah memberikan bantuan dan motivasi yang banyak selama menyelesaikan skripsi ini.
- Keluarga Besar Panti Asuhan Anak Yatim dan Piatu At-taufiq Malang yang telah memberi dukungan dan mendoakan untuk kelangsungan kelancaran pengerjaan skripsi ini sehingga dapat terselesaikan.

Dalam penulisan skripsi ini, penulis menyadari bahwa skripsi ini masih belum sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun untuk kelengkapan dan kesempurnaan skripsi ini. Penulis berharap semoga skripsi ini dapat bermanfaat khususnya bagi rekan-rekan mahasiswa.

Malang, Agustus 2014

Penulis

ABSTRAK

Luqman Hakim, Jurusan Teknik Elektro, Fakultas Teknik Universitas Brawijaya, Aplikasi Dan Implementasi Secret Sharing Menggunakan Kriptografi Visual Pada Citra Biner.
Dosen Pembimbing: Waru Djuriatno, ST., MT., dan Ir. Muhammad Aswin, MT.

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 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 citra 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.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 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 kriptografi visual dengan algoritma *halftoning*. 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 4subpiksel yaitu 2x2. 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 hitam putih menjadi dua buah citra yang tidak diketahui isi informasinya.

1.5 Manfaat

Diharapkan manfaat yang dapat diperoleh melalui pengerjaan skripsi ini adalah:

a) Bagi penyusun

1. Diharapkan penulis mampu membuat aplikasi secret sharing menggunakan algoritma kriptografi visual pada citra biner.
2. Memperoleh pemahaman mengenai kelebihan serta kekurangan perangkat lunak yang telah dibuat.
3. Memahami bahwa sistem yang telah dibuat adalah hasil pengembangan daya pikir manusia, sebagai sumber daya terpenting dalam pembangunan sistem.
4. Menambah wawasan ilmu pengetahuan yang telah dipelajari sebelumnya, dan serta sebagai pelatihan berpikir kritis dalam menyelesaikan suatu masalah yang dihadapi.
5. Menerapkan ilmu yang telah didapat dalam perkuliahan.
6. Memberikan sumbangan bagi perkembangan ilmu pengetahuan khususnya dalam bidang *Information Technology (IT).*

b) Bagi pengguna

1. Memberi kemudahan dalam mengamankan informasi data berupa citra biner.

1.6 Sistematika Penulisan

Penulisan skripsi dibagi dalam tujuh bab dengan sistematika penulisan sebagai berikut :

BAB 1 PENDAHULUAN

Memuat latar belakang, rumusan masalah, batasan masalah, tujuan penulisan, manfaat dan sistematika pembahasan.

BAB II DASAR TEORI

Membahas kajian pustaka dan dasar teori yang digunakan pada skripsi ini.

BAB III METODE PENELITIAN

Membahas metode yang digunakan dalam skripsi ini serta langkah – langkah yang diambil.

BAB IV PERANCANGAN

Menjelaskan langkah – langkah perancangan aplikasi secret sharing beserta penjelasan algoritma yang digunakan.

BAB V PENGUJIAN DAN ANALISIS

Pengujian perangkat lunak dan analisis hasil pengujian.

BAB VI PENUTUP

Memuat kesimpulan yang diperoleh serta saran untuk pengembangan lebih lanjut.

BAB II

TINJAUAN PUSTAKA

Adapun beberapa teori yang akan dipakai oleh penulis untuk merancang aplikasi secret sharing pada citra biner ini diantaranya adalah:

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan yang dikirim dari suatu tempat ke tempat lain.

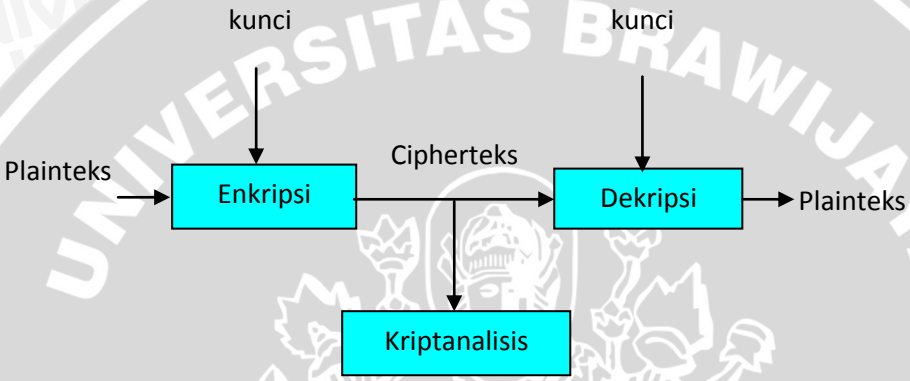
Kriptografi adalah ilmu yang digunakan untuk mengacak data sedemikian rupa sehingga tidak bisa dibaca oleh pihak yang tidak berwenang. Hal ini data yang sudah diacak harus bisa dikembalikan lagi seperti semula oleh pihak yang berwenang. Proses pengacakan disebut dengan Enkripsi *(Encryption)* dan data 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).*

Ada beberapa terminologi dasar dalam memahami kriptografi yang sebelumnya sudah dijelaskan diatas yaitu plainteks, cipherteks, enkripsi, dekripsi, kriptanalisis, dan kunci :

1. Plainteks mengacu kepada berbagai jenis informasi dalam bentuk asli, dapat dibaca, tidak dalam bentuk tersandikan.
2. Cipherteks merupakan pesan dalam bentuk tersandikan. Sehingga informasi dalam bentuk cipherteks tidak jelas isi dari pesan tersebut.
3. Enkripsi adalah proses perubahan plainteks menjadi cipherteks.
4. Dekripsi adalah proses kebalikan dari enkripsi. Cipherteks diubah menjadi plainteks.

5. Kriptanalis adalah orang yang mencoba mencari kelemahan pola enkripsi. Seorang kriptanalis akan mencari cara untuk memecahkan suatu pola kriptografi dan kemudian, para ahli menggunakan informasi tersebut untuk membuat pola kriptografi menjadi lebih kuat.
6. Kunci adalah sesuatu yang melindungi data. Kunci dibutuhkan untuk membuka pesan terenkripsi.

Untuk lebih jelasnya pada gambar 2.1 dapat dilihat sistem kriptografi secara umum.



Gambar 2.1 sistem kriptografi secara umum.

2.1.1 Tujuan Kriptografi

Dari penjelasan kriptografi sebelumnya maka dapat diketahui tujuan dari kriptografi yaitu untuk memberi layanan keamanan seperti kerahasiaan data, integritas data, otentikasi, dan nirpenyangkalan.

1. Kerahasiaan data adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak untuk menerima pesan tersebut. Dalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi cipherteks.
2. Integritas data adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi adalah layanan yang berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling

berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diautentikasi keaslian, isi datanya, waktu pengiriman dan lain-lain.

4. Nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman.

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 dapat dilihat sebagai fungsi kontinyu f(x,y) yang berada pada bidang dua dimensi dimana (x,y) merupakan koordinat spasial dari suatu titik sedangkan nilai f(x,y) merupakan intensitas cahaya pada titik koordinat tersebut. Citra digital dapat diperoleh dari proses pencuplikan objek tiga dimensi dan membentuk suatu matriks dimana setiap elemennya menyatakan intensitas cahaya. Citra digital dapat dihasilkan dari penangkapan objek menggunakan kamera digital, sensor, scaner atau perekam lainya yang menghasilkan data format raster.

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.

Citra digital memilliki resolusi yang menunjukkan tingkat kerincian suatu citra. Resolusi dapat dinyatakan dengan banyaknya piksel per satuan panjang atau sering disebut dengan piksel per inci (dot per inci – dpi). Semakin besar nilai dpi yang dimiliki oleh suatu citra, maka resolusinya akan semakin tinggi. Nilai resolusi juga dapat dinyatakan dengan satuan panjang, misalnya 120 x 100 m.

Citra digital didefinisikan sebagai fungsi *f(x,y) berukuran M baris dan N kolom*, Citra digital dapat ditulis dalam bentuk matrik sebagai berikut.

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

dengan:

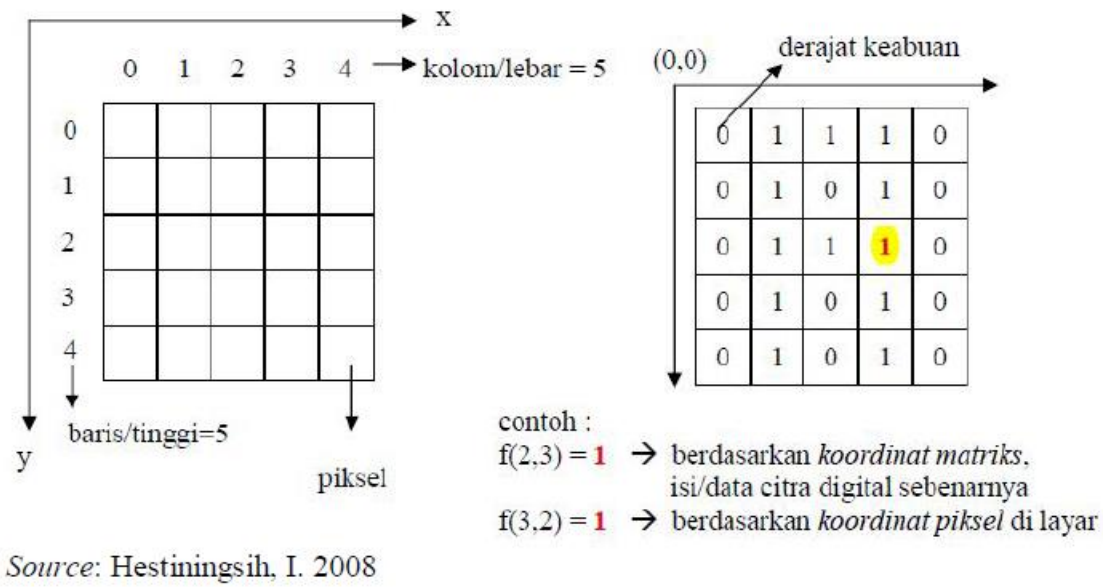
f(x, y) = intensitas pixel pada posisi x dan y

M = jumlah kolom

N = jumlah baris

Nilai pada suatu irisan antara baris dan kolom (pada posisi x,y) disebut dengan pixel.

Pixel adalah unsur gambar atau representasi sebuah titik terkecil dalam sebuah gambar grafis yang dihitung per inci. Pixel sendiri berasal dari akronim bahasa Inggris (Picture Element) yang disingkat menjadi Pixel. Untuk menunjukkan tingkat pencahayaan suatu piksel, sering kali digunakan bilangan bulat yang besarnya delapan bit dengan lebar selang nilai 0 – 255 dimana 0 untuk warna hitam dan 255 untuk warna putih, dan tingkat abu – abu berada diantara 0 dan 255.



Gambar 2.2 Posisi pixel

2.3 Karakteristik File Citra

Karakteristik file citra ditentukan oleh resolusi *(resolution)* dan kedalaman bit *(bit depth).* Karakteristik – karakteristik ini akan menentukan tawar – menawar antara kualitas *file* citra dan jumlah bit yang dibutuhkan untuk menyimpan atau mentransmisikannya.

2.3.1 *Image Resolution*

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, dalam arti bahwa dalam ukuran fisik yang sama, 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.

2.3.2 *Bit Depth*

Bit Depth merupakan jumlah bit yang digunakan untuk merpresentasikan tiap *pixel*. *Bit Depth* adalah jumlah bit untuk 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.

Dengan 1 byte (8bit) untuk tiap pixel, diperoleh 2^8 atau 256 level intensitas. Dengan level intensitas sebanyak itu, umumnya mata manusia sudah dapat dipuaskan. Kedalaman pixel paling rendah terdapat pada binary-value image yang hanya menggunakan 1 bit untuk tiap *pixel*, sehingga hanya ada dua kemungkinan bagi tiap *pixel*, yaitu 0 (hitam) atau 1 (putih).

Color resolution merupakan jumlah warna yang dapat ditampilkan pada sebuah citra sedangkan color *depth* adalah jumlah maksimum warna pada citra berdasarkan bit depth dari citra dan layar monitor komputer. Tabel 2.1 berikut menunjukkan hubungan antara bit depth dan *color resolution*.

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)

16 bit	65.536 warna	2^{16}
24 bit	16.777.216	2^{24}
32 bit	4.294.967.296	2^{52}

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. Piksel dengan nilai 0 sebagai warna hitam. Piksel dengan nilai 1 sebagai warna putih.

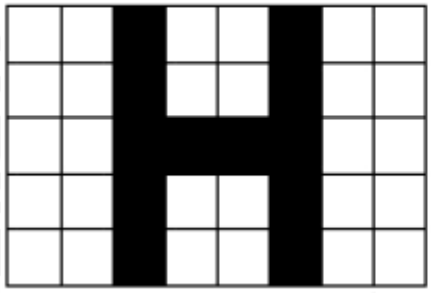
2.4 Citra Biner

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. Berikut adalah contoh citra biner pada gambar 2.3 dan gambar 2.4 contoh pengkodean citra biner.

a. Citra Teks b. Citra kode batang *barcode*

Gambar 2.3 Contoh citra biner



Citra Biner (hitam = 0, putih = 1)
= 1 1 0 1 1 0 1 1
= 1 1 0 1 1 0 1 1
= 1 1 0 0 0 0 1 1
= 1 1 0 1 1 0 1 1
= 1 1 0 1 1 0 1 1

Gambar 2.4 Contoh pengkodean citra biner

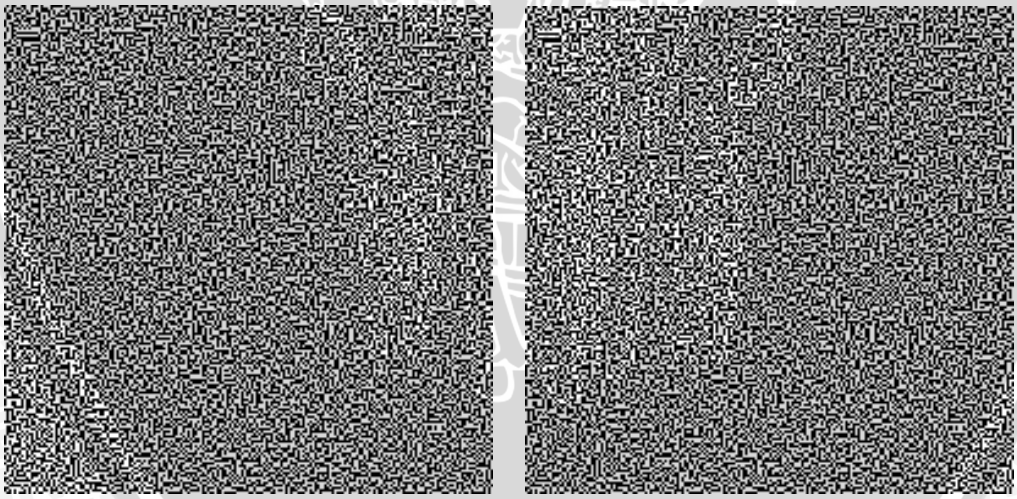
2.5 Kriptografi Visual

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.

Kriptografi visual pertama kali diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994. Kriptografi jenis ini hanya dapat diterapkan terhadap gambar atau citra, dan sama sekali tidak menggunakan komputasi kriptografi seperti yang biasa dilakukan pada teknik kriptografi umumnya. Skema yang diperkenalkan oleh Naor dan Shamir ini merupakan pembagian rahasia berbasis pada gambar atau citra hitam putih/ citra biner. Gambar/citra rahasia dibagi menjadi beberapa bagian, dimana bagian-bagian tersebut tidak mencapai informasi isi gambar/citra aslinya. Untuk memulihkan dan mencapai isi informasi gambar/citra seperti aslinya, yaitu dengan melapiskan/menumpuk bagian-bagian gambar tersebut. Teknik ini hanya dilakukan dengan mencetak bagian-bagian gambar tersebut pada kertas transparan untuk mewujudkan gambar aslinya dengan cara menumpuk bagian-bagian gambar yang telah dicetak. Namun apabila salah satu bagian tersebut tidak ada, maka gambar asli tidak akan bisa dilihat dengan jelas dan tak seperti gambar/citra aslinya. Maka dengan ini proses pembacaan sandi atau dalam kriptografi dikenal dengan dekripsi tidak membutuhkan software seperti kriptografi pada umumnya untuk mewujudkan citra asli, dan hanya membutuhkan visual manusia untuk mengetahui isi dari gambar asli tersebut.

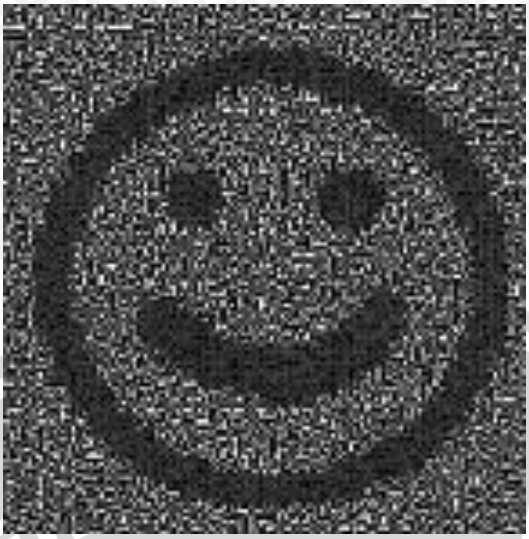
Versi dasarnya mempresentasikan secret sharing (2,2). Maksudnya skema tersebut menghasilkan 2 (dua) citra pembagi dari gambar aslinya (P) yaitu sebuah gambar hitam putih. Dimana gambar P1 untuk bagian gambar 1 dan P2 untuk bagian gambar 2. P1 dan P2 merupakan distribusi acak dari pixel hitam putih dan 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:

Gambar 2.5 Citra asli (plainteks)



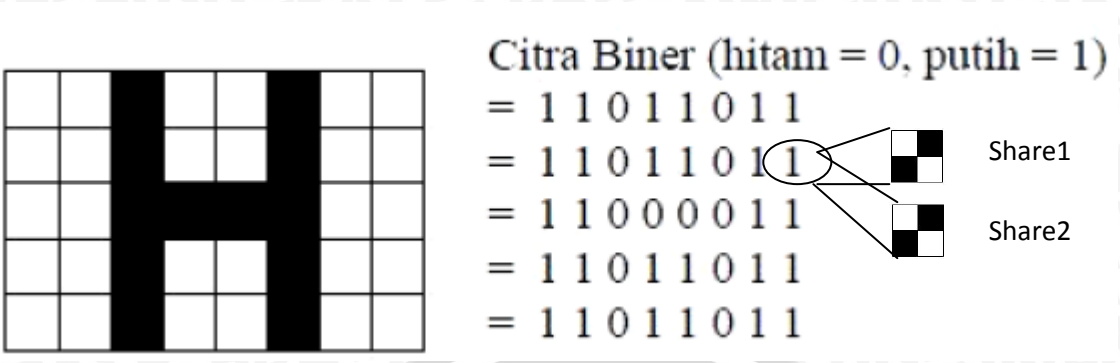
Share 1 Share 2

Gambar 2.6 Citra tersandikan (cipherteks) share 1 dan share 2

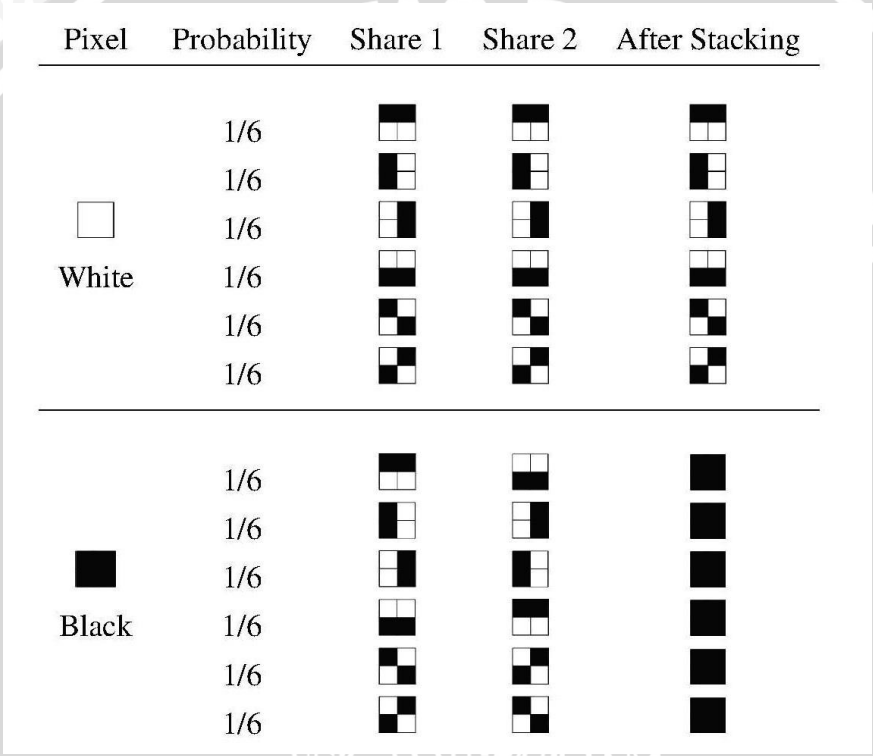


Gambar 2.7 Citra dekripsi: share 1 ditumpuk dengan share 2

Secara Umum sebuah (k, n) menghasilkan skema n bagian, tapi membutuhkan kombinasi k untuk memulihkan gambar/ citra rahasia. Salah satu pengembangan kriptografi visual adalah metode kriptografi visual dengan metode *halftone*. Metode *halftone* ini adalah piksel gambar dapat dibagi dua untuk dua buah share. setiap pixel pada gambar asli dapat digantikan pada gambar pembagi 2 x 2 blok dari subpiksel. Dapat dilihat pada gambar 2.9 jika gambar asli putih. 1 (satu) dari 6(enam) kombinasi piksel pada gambar akan membentuk bagian-bagian yang dapat ditumpangkan untuk memulihkan gambar. Sama juga dengan kemungkinan kombinasi untuk piksel hitam. Penumpukan dapat dilihat secara matematis, yang mana putih = 1 dan hitam = 0 untuk gambar biner sederhana. Yang perlu diperhatikan pada penumpukan bagian untuk memulihkan gambar adalah bahwa hasil gambar dan yang sudah tertutupi gambar rahasia mempunyai piksel 4 kali piksel lebih banyak dari pada gambar aslinya. Hal ini dipengaruhi oleh kontras antara putih dan hitam telah menurun. Pada saat piksel putih pulih sebenarnya terdiri dari 2 putih dan 2 hitam dan piksel hitam mempresentasikan 4 subpiksel hitam pada gambar pulih. Berikut adalah gambar contoh pembagian citra untuk setiap piksel dan tabel kombinasi piksel :



Gambar 2.8 Pembagian share1 dan share2 pada setiap piksel



Gambar 2.9 kombinasi piksel

Tabel kombinasi piksel pada gambar 2.9 digunakan untuk mengacak piksel agar setiap piksel yang bersebelahan tidak menunjukkan informasi apapun pada citra share. Distribusi acak dari piksel hitam putih dilakukan dengan cara permutasi.

BAB 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:

3.1 Studi Literatur

Dalam penyusunan skripsi ini, pengumpulan data dilakukan dengan melakukan studi literatur dengan sasaran tinjauan antara lain :

1) Pustaka Referensi
2) Pustaka Penunjang
3) Informasi Internet

Studi literatur yang dilakukan bertujuan untuk mengkaji hal-hal yang berhubungan dengan teori-teori yang mendukung dalam perencanaan dan perealisasian aplikasi. Adapun teori – teori yang dikaji adalah sebagai berikut :

1) Teori mengenai kriptografi
2) Teori mengenai citra digital
3) Teori mengenai kriptografi visual
4) Pemrograman menggunakan MATLAB

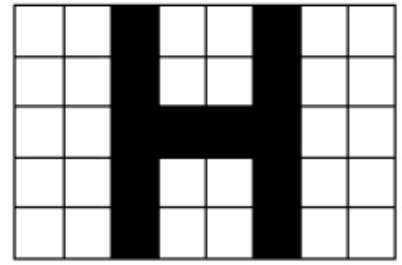
3.2 Penentuan Spesifikasi Aplikasi

Menentukan perangkat yang digunakan untuk menunjang pembuatan aplikasi:

1. Perangkat Keras
   a. Komputer / Laptop
      Intel(R) Celeron(R) CPU 847 @ 1.10GHz (2 CPUs), DDR II 4,00GB RAM, harddisk 450 GB
2. Perangkat Lunak
   a. Windows 8 Single Language
   b. MATLAB R2012b (8.0.0.783) 64-bit (win64)

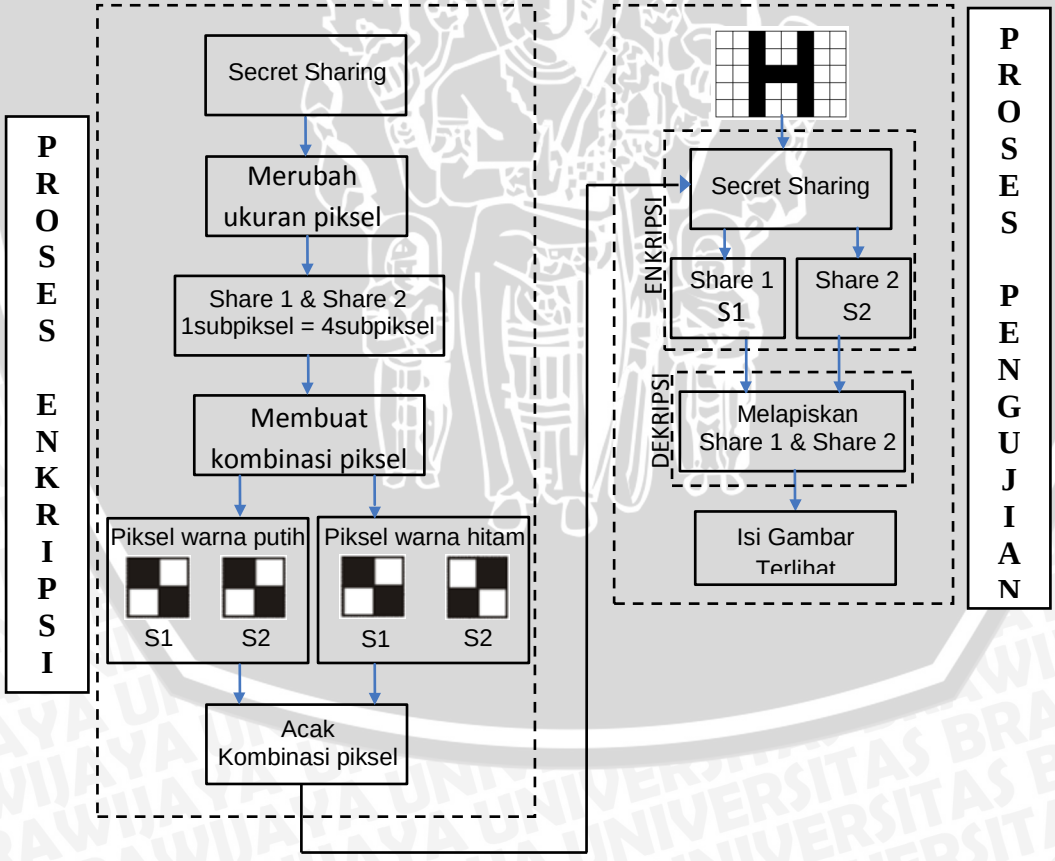
3.3 Perancangan dan Implementasi Sistem

Pembuatan diagram sistem merupakan dasar dari perancangan sistem agar perancangan dan perealisasian aplikasi berjalan secara sistematis. Dalam sistem ini,citra masukan merupakan citra biner. Hal ini dapat ditunjukkan seperti contoh pada gambar dibawah ini:



Gambar 3.1 contoh citra masukan

Sebelum sistem tersebut dibuat terlebih dahulu direncanakan sistematika pembuatan sistem itu sendiri agar diperoleh hasil yang maksimal. Dengan mengacu dasar teori yang telah dibuat sebelumnya. Berikut urutan diagram sistem:



Gambar 3.2 Diagram Sistem

(**Sumber :** Perancangan)

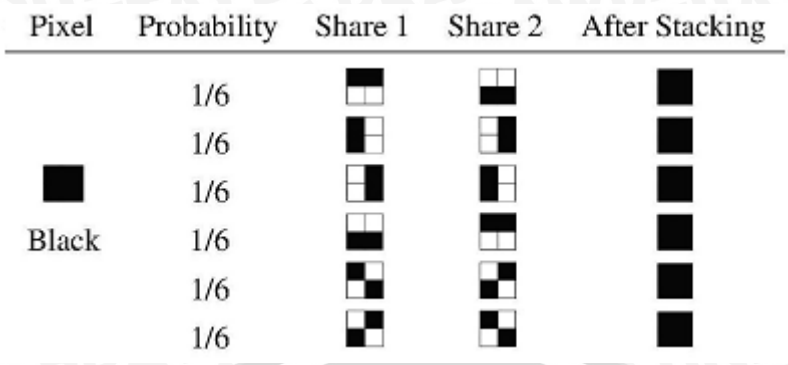
Gambar 3.2 menunjukkan gambaran sistem secara keseluruhan. Pada proses pengujian dilakukan dengan mengupload citra hitam putih atau citra berwarna yang nantinya akan diubah menjadi citra biner yang hanya memiliki kedalaman warna 1 bit yaitu hanya terdapat dua warna hitam dan putih. Setelah citra sudah diupload pada program, proses berikutnya secret sharing yaitu proses untuk enkripsi citra. Dalam proses enkripsi dilakukan pembagian citra asli menjadi citra rahasia (share 1 dan share 2).

Citra rahasia didapat dari proses enkripsi seperti gambar 3.2. Dalam skripsi ini menggunakan metode algoritma *halftone,* metode ini adalah suatu piksel gambar dapat dibagi dua untuk dua buah *share*. Cara membagi citra asli yaitu setiap subpiksel pada gambar asli digantikan dengan 4 subpiksel untuk masing – masing citra share. Berikut adalah gambar pembentukan setiap subpiksel menjdi 4 subpiksel :

Gambar 3.3 Pembentukan subpiksel dengan m = 4 subpiksel

Setelah proses pembentukan setiap subpiksel menjadi 4 subpiksel, proses berikutnya dilakukan dengan membuat kombinasi piksel untuk share 1 dan share 2. Kombinasi piksel untuk warna putih akan membentuk piksel warna dengan kombinasi yang sama dan apabila kedua share ditumpuk akan menghasilkan dua warna hitam dan dua warna putih. Sedangkan untuk kombinasi warna hitam akan membentuk piksel warna dengan kombinasi yang berbeda dan hasil tumpukan *share* menghasilkan empat warna hitam. Berikut adalah gambar kombinasi piksel untuk warna putih dan warna hitam :

Pixel	Probability	Share 1	Share 2	After Stacking
White	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
	1/6			



Gambar 3.4 kombinasi piksel warna putih dan warna hitam

Gambar 3.4 merupakan gambar kemungkinan pembentukan kombinasi yang akan menggantikan piksel warna putih dan warna hitam pada gambar asli. Dilihat dari gambar 3.4 untuk kombinasi piksel warna putih pada share 1 dan share 2 mempunyai kombinasi yang sama sehingga pada proses melapiskan atau proses dekripsi dalam menampilkan informasi citra akan didapat dua warna hitam dan dua warna putih, sehingga untuk warna putih tidak menampilkan waran putih sepenuhnya. Sedangkan untuk warna hitam mempunyai dua kombinasi share yang berbeda, karena dalam kombinasi share untuk warna hitam digunakan untuk menampilkan informasi gambar dengan penumpukan share yang sepenuhnya akan membentuk warna hitam, sehingga informasi citra akan bisa didapat.

Setelah membentuk kombinasi piksel, proses berikutnya yaitu mengacak kombinasi piksel. Dalam proses mengacak kombinasi piksel ini dilakukan agar informasi pada citra asli tidak bisa terlihat dan hanya terlihat gambar titik hitam dan putih yang tak beraturan untuk citra share 1 dan share 2. Untuk proses mengacak dilakukan dengan cara permutasi yang akan menghasilkan kombinasi seperti pada gambar 3.4 diatas. Berikut pengacakan kombinasi.

Piksel 1 Piksel 2 Piksel 3 Piksel n+1

$$\begin{bmatrix} a1 & a2 \\ a3 & a4 \end{bmatrix}\begin{bmatrix} b1 & b2 \\ b3 & b4 \end{bmatrix};\ \begin{bmatrix} a2 & a1 \\ a4 & a3 \end{bmatrix}\begin{bmatrix} b2 & b1 \\ b4 & b3 \end{bmatrix};\ \begin{bmatrix} a4 & a1 \\ a2 & a3 \end{bmatrix}\begin{bmatrix} b4 & b1 \\ b2 & b3 \end{bmatrix};\ \text{dst.}$$

Share1 Share2 Share1 Share2 Share1 Share2

3.4 Pengujian

Pengujian dilakukan untuk menjamin dan memastikan bahwa aplikasi yang telah dirancang memiliki tingkat kesalahan yang kecil. Untuk mengetahui apakah aplikasi bekerja dengan baik dan sesuai dengan perancangan, maka diperlukan serangkaian pengujian. Pengujian aplikasi secret sharing pada citra biner dilakukan terhadap beberapa gambar yang berasal dari citra uji. Pengujian juga dilakukan dengan bantuan mata telanjang manusia. Karena hasil enkripsi citra menciptakan gambar yang tak terlihat informasinya seperti citra aslinya.

3.5 Pengambilan Kesimpulan dan Saran

Pada tahap ini, diambil kesimpulan dari hasil pengujian dan analisis terhadap Aplikasi Secret Sharing Untuk Citra Biner. Tahap selanjutnya adalah pembuatan saran yang dimaksudkan untuk memperbaiki kesalahan-kesalahan yang terjadi dan menyempurnakan penulisan serta untuk memberikan pertimbangan atas pengembangan aplikasi selanjutnya.

BAB 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:

3.6 Studi Literatur

Dalam penyusunan skripsi ini, pengumpulan data dilakukan dengan melakukan studi literatur dengan sasaran tinjauan antara lain :

4) Pustaka Referensi
5) Pustaka Penunjang
6) Informasi Internet

Studi literatur yang dilakukan bertujuan untuk mengkaji hal-hal yang berhubungan dengan teori-teori yang mendukung dalam perencanaan dan perealisasian aplikasi. Adapun teori – teori yang dikaji adalah sebagai berikut :

5) Teori mengenai kriptografi
6) Teori mengenai citra digital
7) Teori mengenai kriptografi visual
8) Pemrograman menggunakan MATLAB

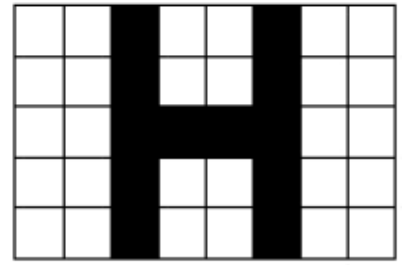
3.7 Penentuan Spesifikasi Aplikasi

Menentukan perangkat yang digunakan untuk menunjang pembuatan aplikasi:

3. Perangkat Keras
   a. Komputer / Laptop
      Intel(R) Celeron(R) CPU 847 @ 1.10GHz (2 CPUs), DDR II 4,00GB RAM, harddisk 450 GB
4. Perangkat Lunak
   a. Windows 8 Single Language
   b. MATLAB R2012b (8.0.0.783) 64-bit (win64)

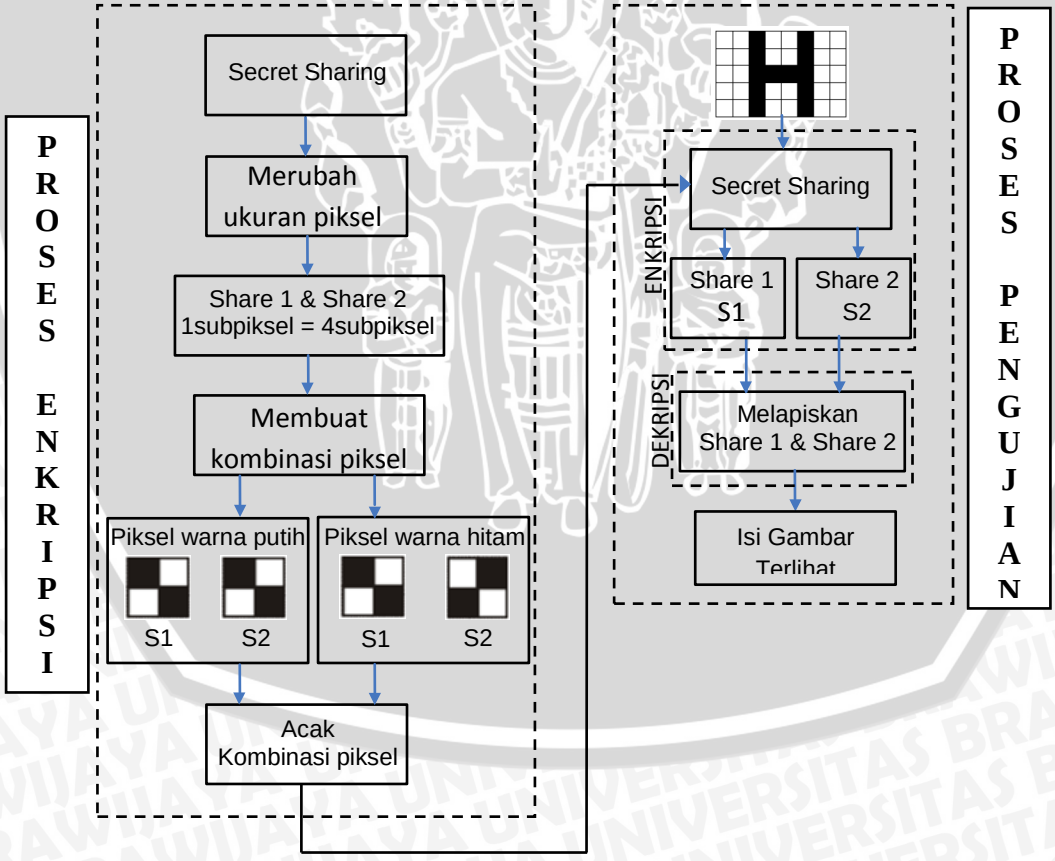
3.8 Perancangan dan Implementasi Sistem

Pembuatan diagram sistem merupakan dasar dari perancangan sistem agar perancangan dan perealisasian aplikasi berjalan secara sistematis. Dalam sistem ini,citra masukan merupakan citra biner. Hal ini dapat ditunjukkan seperti contoh pada gambar dibawah ini:



Gambar 3.1 contoh citra masukan

Sebelum sistem tersebut dibuat terlebih dahulu direncanakan sistematika pembuatan sistem itu sendiri agar diperoleh hasil yang maksimal. Dengan mengacu dasar teori yang telah dibuat sebelumnya. Berikut urutan diagram sistem:



Gambar 3.2 Diagram Sistem

(**Sumber :** Perancangan)

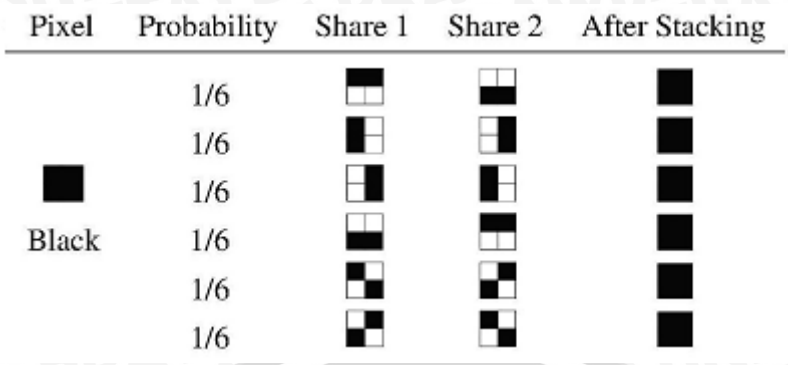
Gambar 3.2 menunjukkan gambaran sistem secara keseluruhan. Pada proses pengujian dilakukan dengan mengupload citra hitam putih atau citra berwarna yang nantinya akan diubah menjadi citra biner yang hanya memiliki kedalaman warna 1 bit yaitu hanya terdapat dua warna hitam dan putih. Setelah citra sudah diupload pada program, proses berikutnya secret sharing yaitu proses untuk enkripsi citra. Dalam proses enkripsi dilakukan pembagian citra asli menjadi citra rahasia (share 1 dan share 2).

Citra rahasia didapat dari proses enkripsi seperti gambar 3.2. Dalam skripsi ini menggunakan metode algoritma *halftone,* metode ini adalah suatu piksel gambar dapat dibagi dua untuk dua buah *share*. Cara membagi citra asli yaitu setiap subpiksel pada gambar asli digantikan dengan 4 subpiksel untuk masing – masing citra share. Berikut adalah gambar pembentukan setiap subpiksel menjdi 4 subpiksel :

Gambar 3.3 Pembentukan subpiksel dengan m = 4 subpiksel

Setelah proses pembentukan setiap subpiksel menjadi 4 subpiksel, proses berikutnya dilakukan dengan membuat kombinasi piksel untuk share 1 dan share 2. Kombinasi piksel untuk warna putih akan membentuk piksel warna dengan kombinasi yang sama dan apabila kedua share ditumpuk akan menghasilkan dua warna hitam dan dua warna putih. Sedangkan untuk kombinasi warna hitam akan membentuk piksel warna dengan kombinasi yang berbeda dan hasil tumpukan *share* menghasilkan empat warna hitam. Berikut adalah gambar kombinasi piksel untuk warna putih dan warna hitam :

Pixel	Probability	Share 1	Share 2	After Stacking
□ White	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
	1/6			



Gambar 3.4 kombinasi piksel warna putih dan warna hitam

Gambar 3.4 merupakan gambar kemungkinan pembentukan kombinasi yang akan menggantikan piksel warna putih dan warna hitam pada gambar asli. Dilihat dari gambar 3.4 untuk kombinasi piksel warna putih pada share 1 dan share 2 mempunyai kombinasi yang sama sehingga pada proses melapiskan atau proses dekripsi dalam menampilkan informasi citra akan didapat dua warna hitam dan dua warna putih, sehingga untuk warna putih tidak menampilkan waran putih sepenuhnya. Sedangkan untuk warna hitam mempunyai dua kombinasi share yang berbeda, karena dalam kombinasi share untuk warna hitam digunakan untuk menampilkan informasi gambar dengan penumpukan share yang sepenuhnya akan membentuk warna hitam, sehingga informasi citra akan bisa didapat.

Setelah membentuk kombinasi piksel, proses berikutnya yaitu mengacak kombinasi piksel. Dalam proses mengacak kombinasi piksel ini dilakukan agar informasi pada citra asli tidak bisa terlihat dan hanya terlihat gambar titik hitam dan putih yang tak beraturan untuk citra share 1 dan share 2. Untuk proses mengacak dilakukan dengan cara permutasi yang akan menghasilkan kombinasi seperti pada gambar 3.4 diatas. Berikut pengacakan kombinasi.

Piksel 1 Piksel 2 Piksel 3 Piksel n+1

$$\begin{bmatrix} a1 & a2 \\ a3 & a4 \end{bmatrix}\begin{bmatrix} b1 & b2 \\ b3 & b4 \end{bmatrix};\ \begin{bmatrix} a2 & a1 \\ a4 & a3 \end{bmatrix}\begin{bmatrix} b2 & b1 \\ b4 & b3 \end{bmatrix};\ \begin{bmatrix} a4 & a1 \\ a2 & a3 \end{bmatrix}\begin{bmatrix} b4 & b1 \\ b2 & b3 \end{bmatrix};\ \text{dst.}$$

Share1 Share2 Share1 Share2 Share1 Share2

3.9 Pengujian

Pengujian dilakukan untuk menjamin dan memastikan bahwa aplikasi yang telah dirancang memiliki tingkat kesalahan yang kecil. Untuk mengetahui apakah aplikasi bekerja dengan baik dan sesuai dengan perancangan, maka diperlukan serangkaian pengujian. Pengujian aplikasi secret sharing pada citra biner dilakukan terhadap beberapa gambar yang berasal dari citra uji. Pengujian juga dilakukan dengan bantuan mata telanjang manusia. Karena hasil enkripsi citra menciptakan gambar yang tak terlihat informasinya seperti citra aslinya.

3.10 Pengambilan Kesimpulan dan Saran

Pada tahap ini, diambil kesimpulan dari hasil pengujian dan analisis terhadap Aplikasi Secret Sharing Untuk Citra Biner. Tahap selanjutnya adalah pembuatan saran yang dimaksudkan untuk memperbaiki kesalahan-kesalahan yang terjadi dan menyempurnakan penulisan serta untuk memberikan pertimbangan atas pengembangan aplikasi selanjutnya.

BAB IV

PERANCANGAN DAN IMPLEMENTASI

Bab ini menjelaskan mengenai langkah-langkah yang akan dilakukan untuk merancang dan mengimplementasikan aplikasi secret sharing menggunakan algoritma kriptografi visual pada citra biner. Perancangan dan implementasi dikerjakan dengan beberapa tahap meliputi proses memasukkan citra biner, proses enkripsi citra, proses dekripsi citra. Perancangan diawali dengan penggambaran blok diagram kerja sistem yang menunjukkan cara kerja aplikasi secara umum.

4.1 Perancangan Secara Umum

Perancangan aplikasi secara umum merupakan tahap awal dalam melakukan perancangan aplikasi secret sharing citra yang akan dibuat. Perancangan diawali dengan penggambaran blok diagram kerja sistem yang menunjukkan cara kerja aplikasi secara umum.

4.1.1 Blok diagram sistem

Sebelum sistem tersebut dibuat terlebih dahulu direncanakan sistematika pembuatan sistem itu sendiri agar diperoleh hasil yang maksimal. Dengan mengacu dasar teori yang telah dibuat sebelumnya. Berikut urutan blok diagram sistem:

Gambar 4.1 Blok Diagram Sistem

(**Sumber :** Perancangan)

Berikut adalah penjelasan tiap blok diagram sistem pada gambar 4.1 :

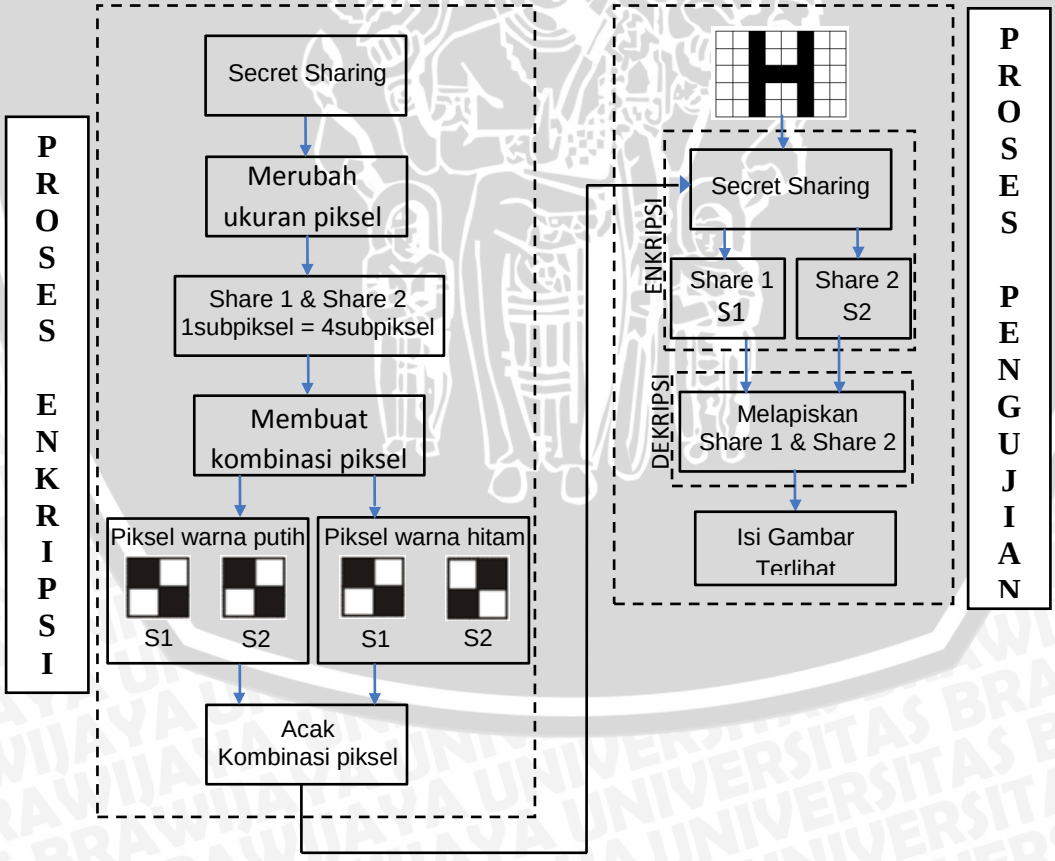
1. Citra Biner adalah citra yang hanya mempunyai dua kedalaman warna yaitu warna hitam dan warna putih yang digunakan sebagai masukan sistem.
2. Enkripsi citra pada citra biner yaitu proses awal dalam mengubah citra asli menjadi dua buah citra yang tersamarkan.
3. Hasil enkripsi merupakan keluaran dari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

4.1.2 Cara kerja aplikasi

Cara kerja aplikasi secret sharing menggunakan algoritma kriptografi visual pada citra biner dimulai dari memasukkan citra biner, citra yang hanya mempunyai dua warna yaitu warna hitam dan warna putih. Setelah citra masukan sesuai dengan citra biner, kemudian dilanjutkan dengan proses enkripsi citra yaitu membagi citra menjadi dua buah citra yang tersamarkan yaitu share1 dan share2.

4.2 Perancangan Perangkat Lunak

Pada sub bab perancangan perangkat lunak akan membahas secara detail tentang setiap tahapan proses pada aplikasi secret sharing menggunakan algoritma kriptografi visual pada citra biner. Beberapa tahap perancangan tersebut meliputi memasukkan citra, proses membagi dua citra share, membuat kombinasi piksel, proses mengacak kombinasi piksel, proses memulihkan citra. Perancangan perangkat lunak diimplementasikan dalam pemrograman MATLAB.

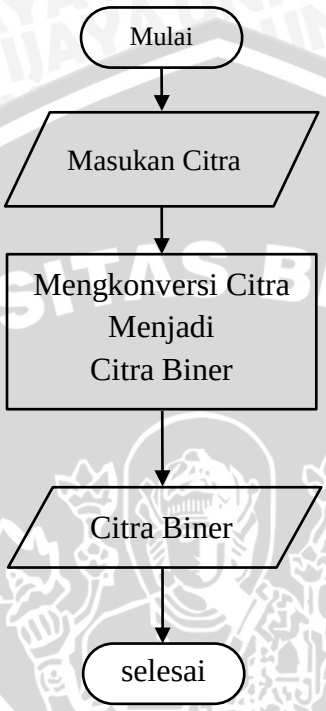


Gambar 4.2 Detail desain aplikasi

(**Sumber :** perancangan)

4.2.1 Memasukan Citra

Sebelum memulai proses pengolahan citra aplikasi ini membutuhkan masukan berupa citra. Pada skripsi ini menggunakan metode *halftone*, sehingga citra masukan akan dikonversi menjadi citra hitam putih. Proses memasukkan citra sebagai berikut :



Gambar 4.3 Flowchart memasukkan citra

(**Sumber:** Perancangan)

Berikut adalah kode bahasa pemrograman MATLAB yang berfungsi mengaktifkan menu dialog untuk memilih sumber citra:

```
%proses untuk membuka citra biner
proyek=guidata(gcbo);
[namafile,direktori]=uigetfile({'*.jpg';'*.bmp';'*.png';'*
.tif'},'Buka Gambar')

if isequal(namafile,0)
return;
end

eval(['cd ''' direktori ''';']);
```

```
I=imread(namafile);
set(proyek.figure1,'CurrentAxes',proyek.axes1);
gray=rgb2gray(I);
thresh=graythresh(gray);
imbw=im2bw(gray,thresh);
set(imshow(imbw));
imshow(imbw), title('CITRA ASLI');

set(proyek.figure1,'Userdata',imbw);
set(proyek.axes1,'Userdata',imbw);
```

4.2.2 Membagi Dua Citra

Setelah melalui tahap memasukkan citra, kemudian dilakukan proses untuk membagi citra biner menjadi dua buah citra share yaitu citra share1 dan citra share2. Untuk proses membagi dua buah citra share pada skripsi ini dilakukan dengan cara mengubah setiap subpiksel menjadi 4 subpiksel. Berikut gambar pembentukan untuk 1 subpiksel menjadi 4 subpiksel untuk masing – masing share:

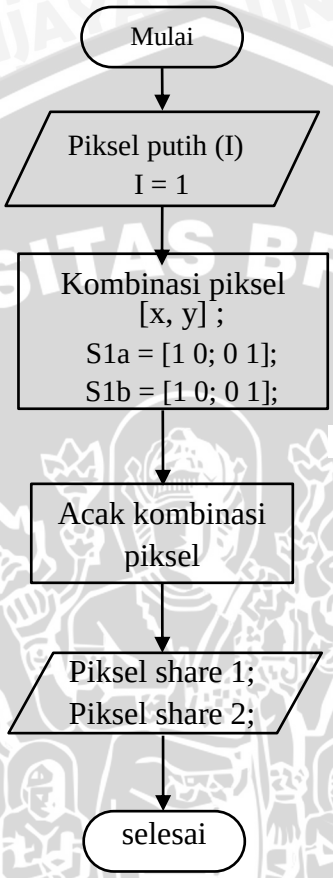
Gambar 4.4 Pembentukan setiap subpiksel menjadi 4 subpiksel

Implementasi proses membagi dua pada pemrograman MATLAB adalah sebagai berikut:

```
%program untuk merubah subpiksel menjadi (2,2) 4 subpiksel
%setiap share1 dan share2 mempunyai (2,2) 4 subpiksel
setiap pikselnya
s = size(I);
share1 = zeros(2*s(1), (2 * s(2)));
share2 = zeros(2*s(1), (2 * s(2)));
```

4.2.3 Membuat kombinasi piksel

Pada tahap membuat kombinasi piksel ini bertujuan untuk menjadikan citra yang awalnya terlihat isi informasi pada citra biner menjadi citra yang tersamarkan, dan digunakan pada saat penumpukan citra share1 dan share2. Proses yang dilakukan untuk membuat kombinasi piksel warna putih sebagai berikut :



Gambar 4.5 Flowchart kombinasi piksel warna putih

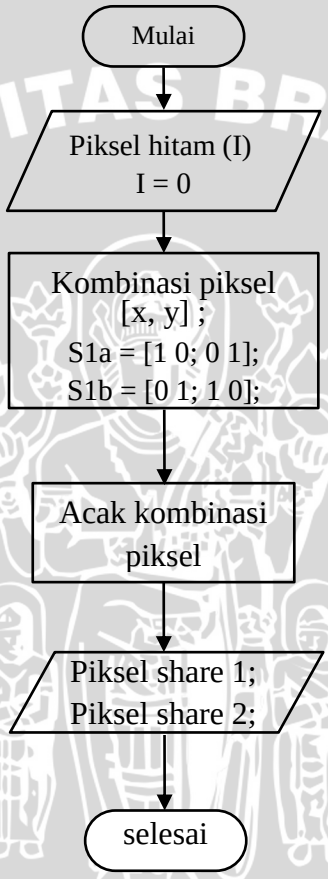
(**Sumber:** Perancangan)

Implementasi proses membentuk kombinasi piksel warna putih pada bahasa pemrograman MATLAB adalah sebagai berikut:

```
%proses pembentukan piksel putih
%kombinasi share pada piksel putih
disp('White Pixel Processing...');
s1a=[1 0;0 1];
s1b=[1 0;0 1];
[x, y] = find(I == 1);
len = length(x);
```

```
for i=1:len
    a=x(i)*2;b=y(i)*2;
    pixShare=acakpiksel(s1a,s1b);
    share1((a:a+1),(b:b+1))=pixShare(1:2,1:2);
    share2((a:a+1),(b:b+1))=pixShare(3:4,1:2);
end
```

Dan berikut proses kombinasi untuk warna hitam :



Gambar 4.6 Flowchart kombinasi piksel warna hitam

(**Sumber:** Perancangan)

Implementasi proses membuat kombinasi piksel untuk warna hitam pada bahasa pemrograman MATLAB adalah sebagai berikut:

```
%proses untuk piksel warna hitam
%kombinasi share pada piksel hitam
disp('Black Pixel Processing...');
```

```
s0a=[1 0;0 1];
s0b=[0 1;1 0];
[x, y] = find(I == 0);
len = length(x);

for i=1:len
    a=x(i)*2;b=y(i)*2;
    pixShare=acakpiksel(s0a,s0b);
    share1((a:a+1),(b:b+1))=pixShare(1:2,1:2);
    share2((a:a+1),(b:b+1))=pixShare(3:4,1:2);
end
```

4.2.4 Mengacak kombinasi piksel

Pada tahap mengacak kombinasi piksel bertujuan agar piksel piksel yang bersebelahan tidak menunjukkan apapun pada citra share. Distribusi acak dari piksel hitam putih dilakukan dengan cara permutasi. Berikut pengacakan kombinasi.

Piksel 1 Piksel 2 Piksel 3 Piksel n+1

$$\underbrace{\begin{bmatrix} a1 & a2 \\ a3 & a4 \end{bmatrix}}_{\text{Share1}}\underbrace{\begin{bmatrix} b1 & b2 \\ b3 & b4 \end{bmatrix}}_{\text{Share2}};\underbrace{\begin{bmatrix} a2 & a1 \\ a4 & a3 \end{bmatrix}}_{\text{Share1}}\underbrace{\begin{bmatrix} b2 & b1 \\ b4 & b3 \end{bmatrix}}_{\text{Share2}};\underbrace{\begin{bmatrix} a4 & a1 \\ a2 & a3 \end{bmatrix}}_{\text{Share1}}\underbrace{\begin{bmatrix} b4 & b1 \\ b2 & b3 \end{bmatrix}}_{\text{Share2}};\ \text{dst.}$$

Berikut proses mengacak kombinasi piksel dalam pemrograman MATLAB.

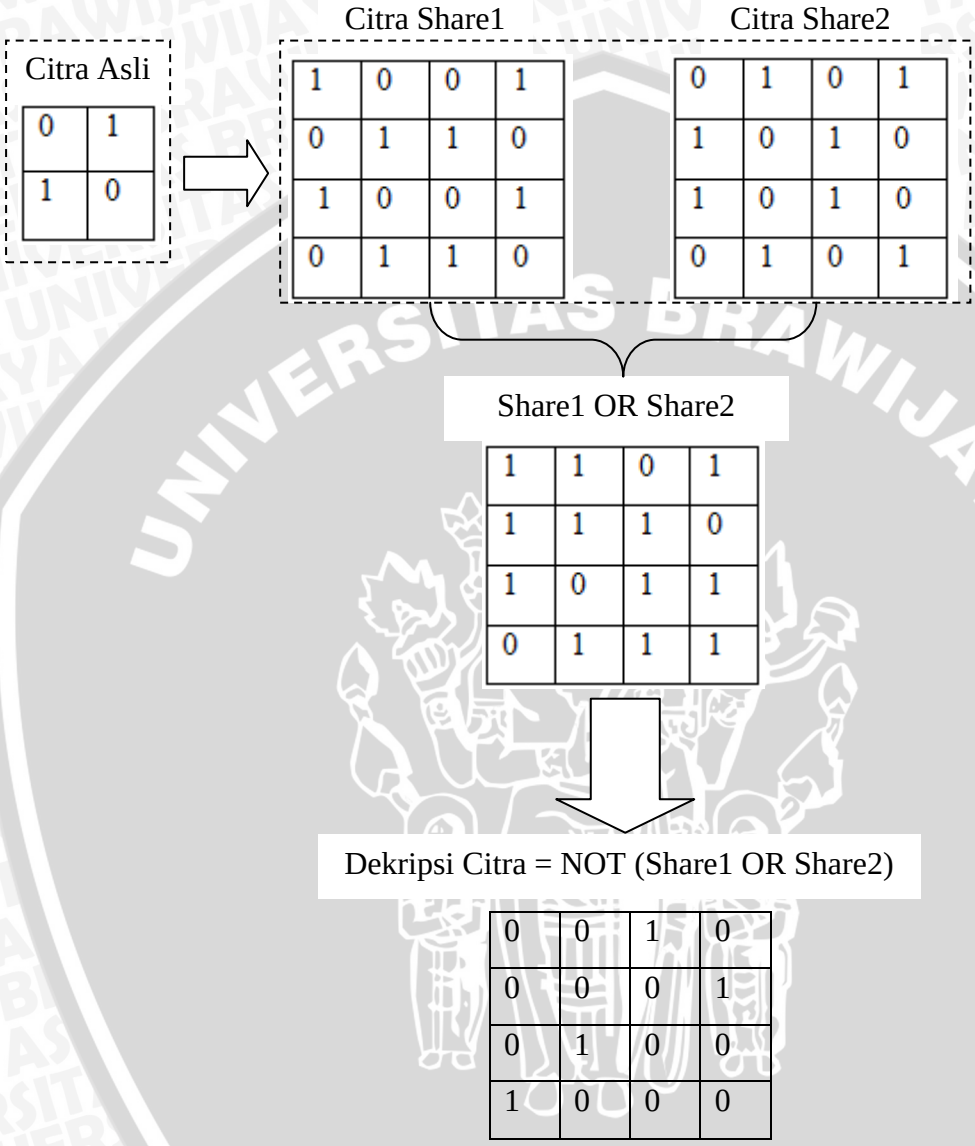
```
%Program Untuk mengacak permutasi generasi share
%menghasilkan share 1 dan share 2 secara acak untuk setiap
piksel

function out = acakpiksel(a,b)

%proses mengacak kombinasi setiap piksel pada share1 dan
share2

a1 = a(1);
```

```
a2 = a(2);
a3 = a(3);
a4 = a(4);

b1 = b(1);
b2 = b(2);
b3 = b(3);
b4 = b(4);

in = [a;b];
out = zeros(size(in));
randNumber = floor(1.9*rand(1));

if (randNumber == 0)
    out = in;
elseif (randNumber == 1)
    a(1) = a2;
    a(2) = a1;
    a(3) = a4;
    a(4) = a3;

    b(1) = b2;
    b(2) = b1;
    b(3) = b4;
    b(4) = b3;

    out = [a;b];
end
```

4.2.5 Dekripsi Citra

Pada tahap dekripsi citra ini dilakukan setelah proses enkripsi citra yang menghasilkan citra share 1 dan citra share 2. Dekripsi citra dilakukan dengan cara melapiskan citra share 1 dan citra share 2, dengan demikian citra dekripsi akan menampilkan isi informasi dari citra aslinya. Untuk hasil citra dekripsi yang semula setiap piksel berwarna putih akan menghasilkan dua piksel warna putih dan dua piksel

warna hitam. Sedangkan untuk piksel yang berwarna hitam akan sepenuhnya menghasilkan empat piksel berwarna hitam. Operasi yang digunakan pada proses dekripsi menggunakan operasi OR dan hasil dari operasi tersebut akan diubah dengan nilai sebaliknya. Berikut proses dekripsi citra :



Gambar 4.7 Proses Dekripsi Citra

(**Sumber:** Perancangan)

Berikut proses dekripsi dalam bahasa pemrograman MATLAB :

```
%proses untuk menumpuk share1 dan share2
share12=bitor(share1, share2);
share12 = ~share12;
```

4.3 Implementasi Sistem

Setelah tahap perancangan tahap selanjutnya adalah tahap implementasi. Implementasi ini merupakan proses transformasi hasil perancangan perangkat lunak yang telah dibuat kedalam kode *(coding)* sesuai dengan sintaks dari bahasa pemrograman yang digunakan.

4.3.1 Lingkungan Implementasi

Aplikasi dibuat dengan menggunakan MATLAB. Sistem diimplementasikan dengan menggunakan spesifikasi sebagai berikut:

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 :
   - Sistem operasi : Microsoft Windows 8
   - Bahasa pemrograman : MATLAB R2012b

4.4 Implementasi Antarmuka

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 4.8 Tampilan aplikasi secret sharing

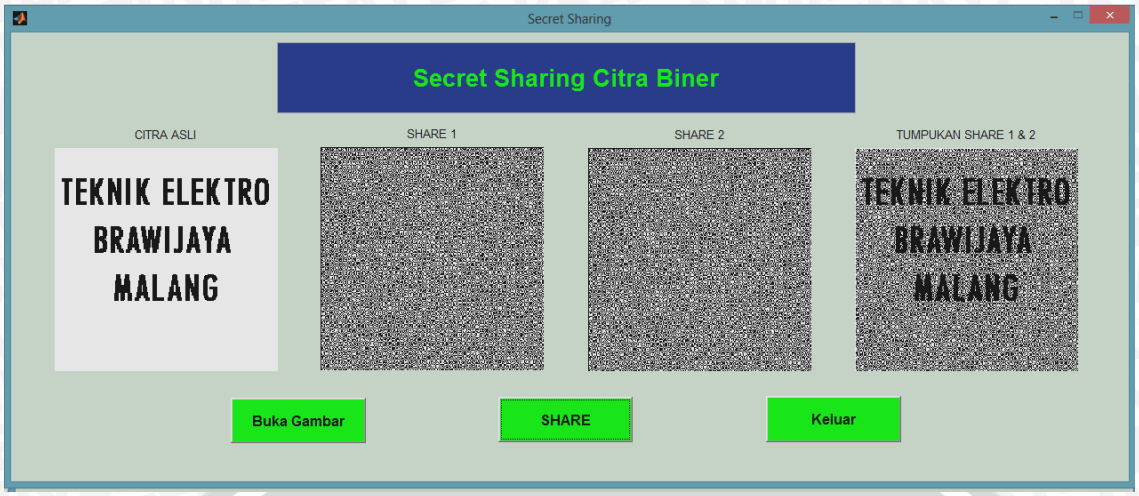
(**Sumber:** perancangan)

Pada gambar 4.8 adalah tampilan awal aplikasi secret sharing sebelum memasukkan citra biner. Pada tampilan aplikasi gambar 4.8 memiliki 4 (empat) buah kotak gambar yang mempunyai fungsi untuk menampilkan gambar dan memiliki 3 tombol untuk menjalankan aplikasi sesuai dengan perintahnya. Untuk kotak gambar yang pertama yaitu untuk menampilkan gambar masukan, sedangkan kotak nomor dua dan tiga digunakan untuk menampilkan hasil enkripsi dari citra asli menjadi dua buah citra share yang tak terlihat isi informasi gambar. Kotak gambar nomor empat digunakan untuk menampilkan hasil dekripsi citra share1 dengan share2 yang akan menghasilkan citra yang akan menampilkan isi informasi dari citra asli. Tombol yang digunakan pada aplikasi ini mempunyai tiga tombol. Tombol yang pertama yaitu tombol buka gambar digunakan untuk membuka dan menampilkan citra biner pada kotak gambar satu. Tombol kedua yaitu tombol share digunakan untuk menjalankan proses enkripsi dan hasil dari enkripsi akan ditampilkan pada kotak gambar dua dan tiga dan menampilkan hasil dekripsi pada kotak gambar empat. Tombol yang ketiga yaitu tombol keluar digunakan untuk mengakhiri dan menutup aplikasi.

Gambar 4.9 Tampilan aplikasi membuka citra biner

(**Sumber:** perancangan)

Pada gambar 4.9 adalah tampilan untuk menampilkan citra biner yang telah dipilih.



Gambar 4.10 Tampilan aplikasi hasil enkripsi dan dekripsi citra biner

(**Sumber:** perancangan)

Setelah citra biner sudah masuk proses selanjutnya dengan menekan tombol share yaitu digunakan untuk menjalankan proses enkripsi citra menjadi dua buah citra share seperti yang ditunjukkan pada gambar 4.10 dan juga menampilkan hasil dekripsi citra share1 dan share2.

BAB 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

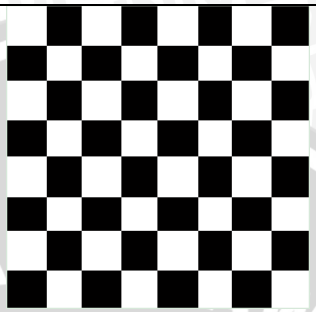
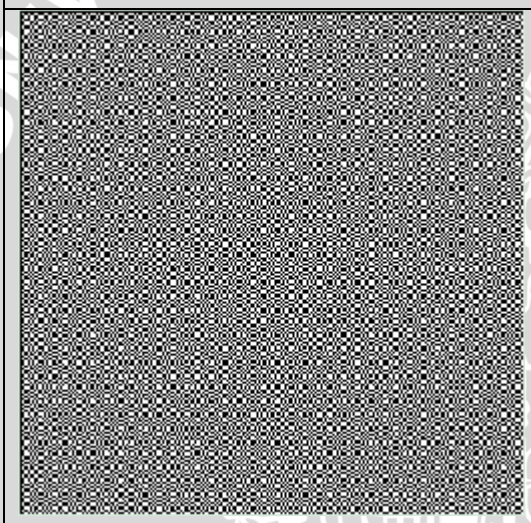
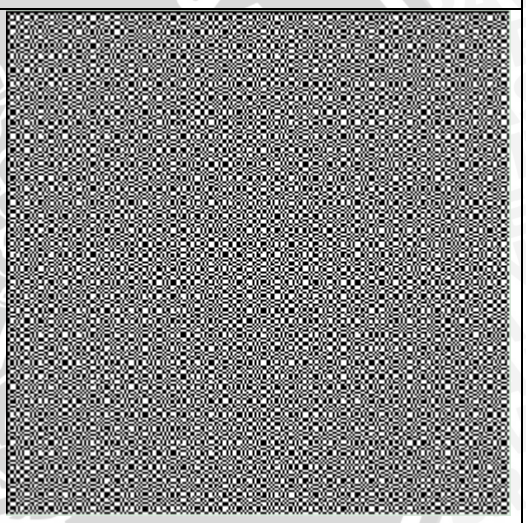
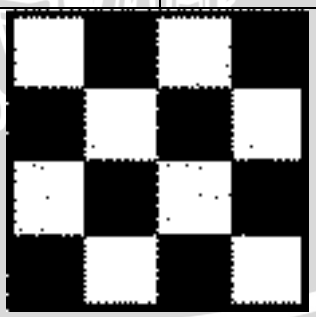
Pengujian ini bertujuan untuk mengetahui apakah program berhasil merubah ukuran piksel citra asli dengan citra hasil enkripsi dengan berbagai macam ukuran citra. Ukuran yang digunakan seperti pada tabel hasil 5.1 dibawah ini:

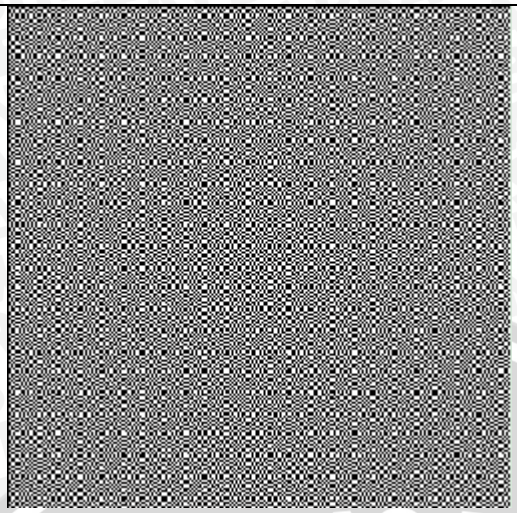
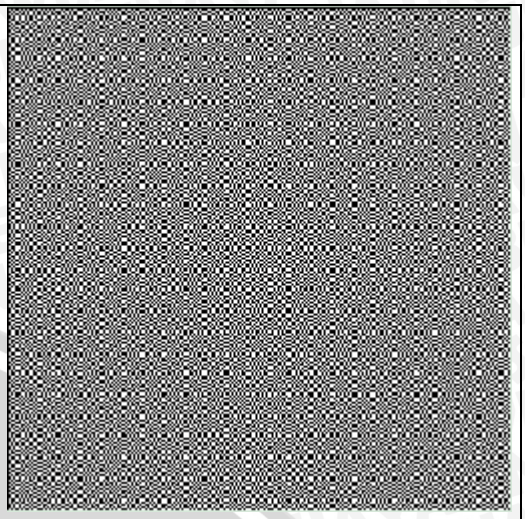
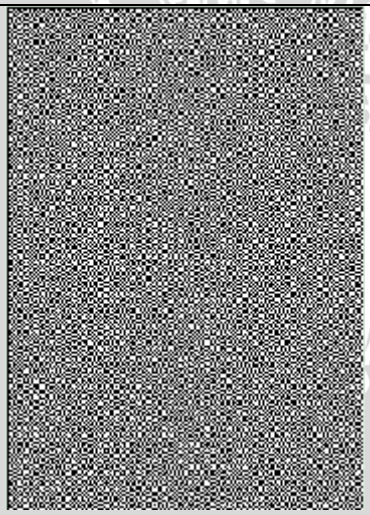
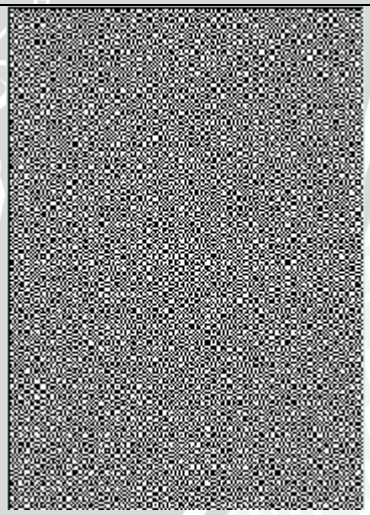
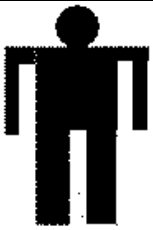
NO.	Nama Citra	Ukuran piksel citra asli	Ukuran piksel citra enkripsi	Isi gambar enkripsi	Ket
1.	Citra1	106 x 106 piksel	213 x 213 piksel	Tidak terlihat	Berhasil
2.	Citra2	113 x 113 piksel	227 x 227 piksel	Tidak terlihat	Berhasil
3.	Citra3	110 x 157 piksel	221 x 315 piksel	Tidak terlihat	Berhasil
4.	Citra4	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

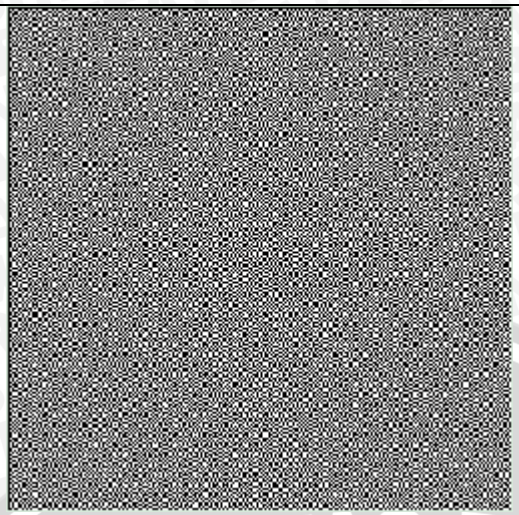
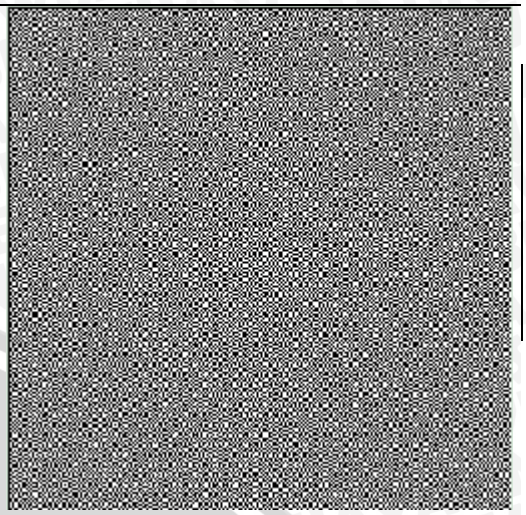
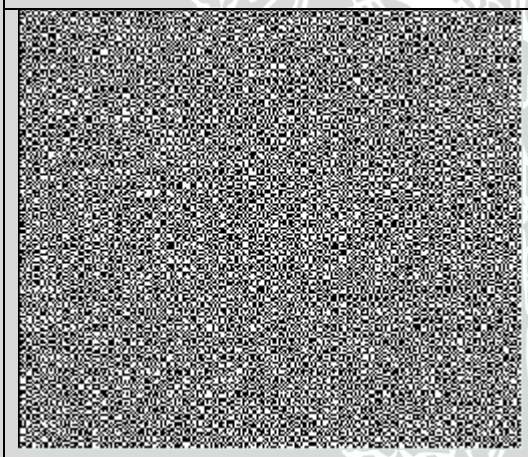
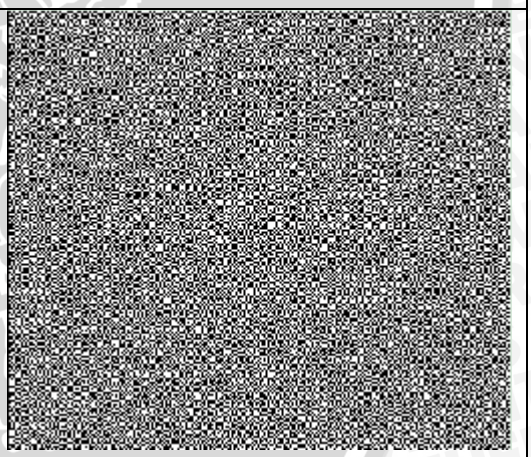
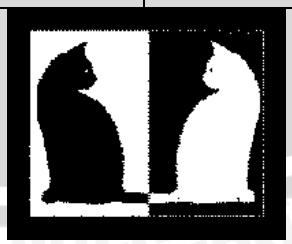
Tabel 5.1 Data pengujian perubahan ukuran piksel citra

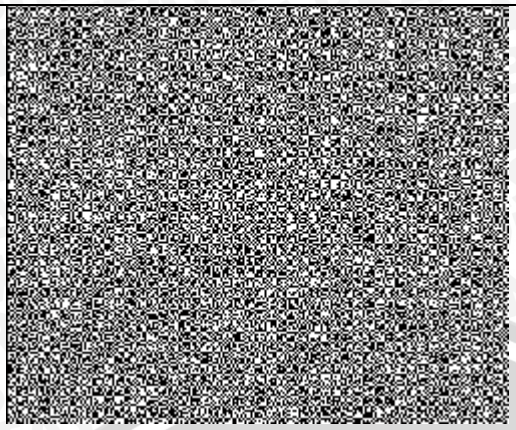
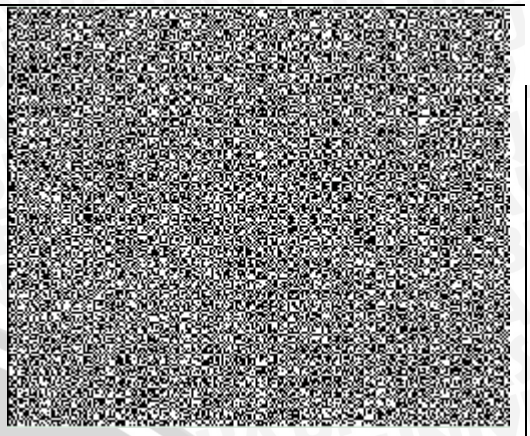
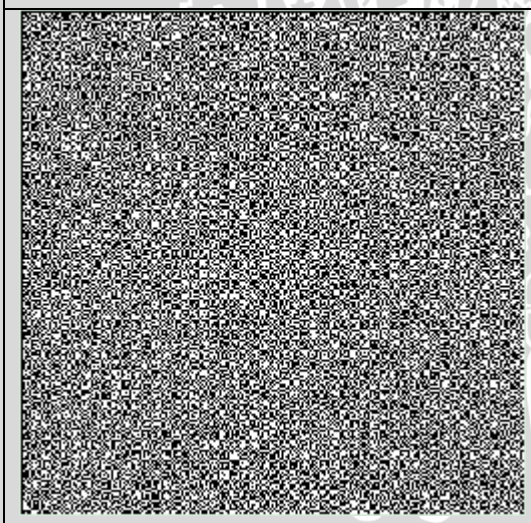
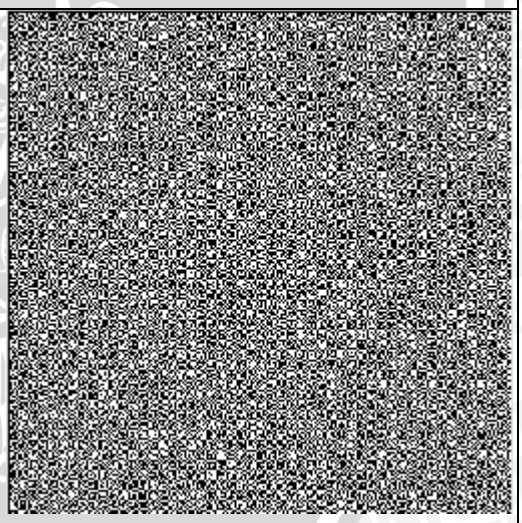
Pada tabel 5.1 menunjukkan bahwa ukuran piksel untuk citra asli dengan citra enkripsi mendapatkan perubahan ukuran pada citra enkripsi yaitu dua kali lebih besar

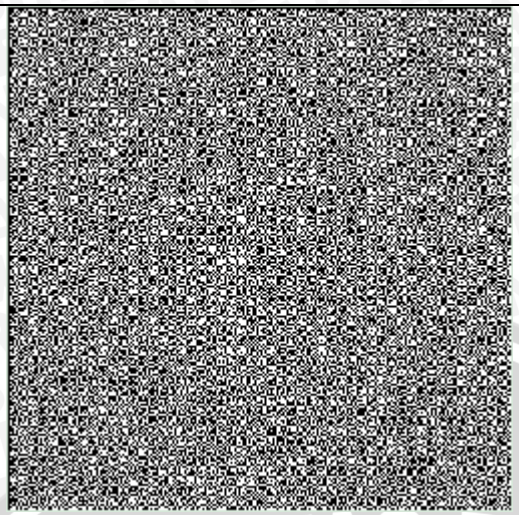
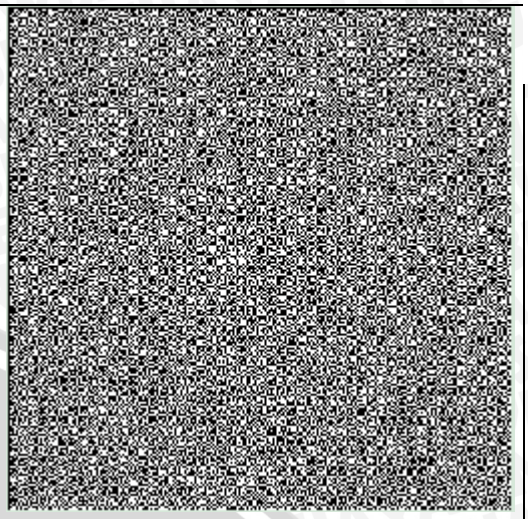
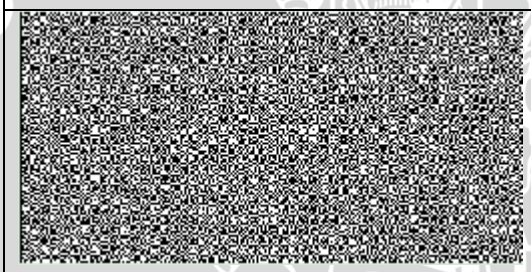
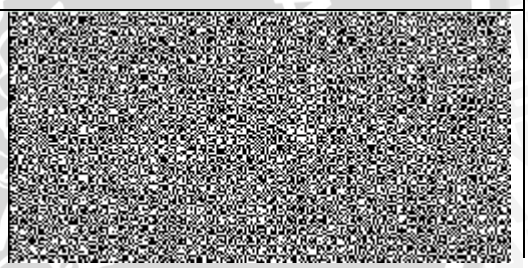
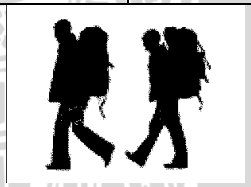
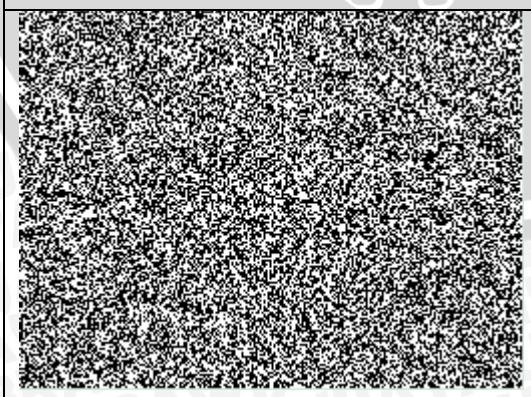
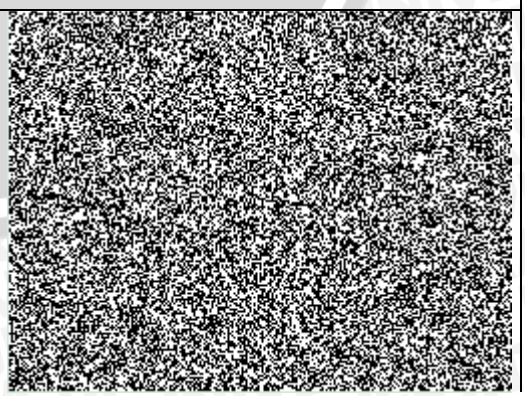
dari ukuran aslinya, ini dikarenakan dalam proses enkripsi citra setiap subpiksel akan diubah menjadi 4 subpiksel yaitu 2 x 2 subpiksel.

<table>
<tr><td>No.</td><td>Nama Citra</td><td colspan="2">Citra Asli</td></tr>
<tr><td rowspan="3">1.</td><td>Citra1</td><td colspan="2">  </td></tr>
<tr><td rowspan="2">Citra Hasil Enkripsi</td><td>Share 1</td><td>Share 2</td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td rowspan="3">2.</td><td>Citra2</td><td colspan="2">  </td></tr>
<tr><td rowspan="2"></td><td>Share 1</td><td>Share 2</td></tr>
<tr><td></td><td></td></tr>
</table>

	Citra Hasil Enkripsi		
3.	Citra3		
		Share 1	Share 2
	Citra Hasil Enkripsi		
4.	Citra4		
		Share 1	Share 2

	Citra Hasil Enkripsi		
5.	Citra5		
		Share 1	Share 2
	Citra Hasil Enkripsi		
6.	Citra6		
		Share 1	Share 2

	Citra Hasil Enkripsi		
7.	Citra7		
	Citra Hasil Enkripsi	Share 1 	Share 2 
8.	Citra8		
		Share 1	Share 2

	Citra Hasil Enkripsi		
9.	Citra9		
	Citra Hasil Enkripsi	Share 1	Share 2
			
10.	Citra10		
	Citra Hasil Enkripsi	Share 1	Share 2
			

Tabel 5.2 Pengujian hasil citra enkripsi

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.

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 5.3 adalah nilai presentase 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 5.3 Hasil Penilaian Citra Share1 dan Share2

BAB VI
PENUTUP

6.1 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%.

6.2 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

R. Panneerselvam, ”Design and Analysis of Algorithms”, School of Management Pondicherry University Pondicherry.

Jufriadif Na’am, “Metode Play Fair Chiper Dalam Mengamankan Sistem Database”, Universitas Putra Indonesia, 2008.

M. Naor and A. Shamir, *Visual Cryptography*. Eurocrypt 1994: 1-12

Ir.Rinaldi Munir,M.T., “Pengantar Kriptografi”,2004.

Makalah IF5054 a.n M.Pramana Baharsyah (“Pemanfaatan Steganografi dalam Kriptografi Visual”)

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.

N. Askari, C. Moloney and H.M. Heys,“A Novel Visual Secret Sharing SchemeWithout Image Size Expansion”, IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, pp. 1-4, 2012.

Jonathan Weir, WeiQi Yan, “Visual Cryptography And Its Applications”, 2012.

N. Askari, H.M. Heys, C.R. Moloney, “An Extended Visual Cryptography Scheme Withouth Pixel Expansion For Halftone Images”, IEEE Canadian Conference of Electrical And Computer Enginering (CCECE), 2013.

Gunaidi Abdia Away. “The Shortcut of MATLAB Programming”. Informatika Bandung. 2010.

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.

LAMPIRAN

Listing Program

```
%proses untuk membuka citra biner
proyek=guidata(gcbo);
[namafile,direktori]=uigetfile({'*.jpg';'*.bmp';'*.png';'*.tif'},'Buka
Gambar')

if isequal(namafile,0)
return;
end

eval(['cd ''' direktori ''';']);
I=imread(namafile);
set(proyek.figure1,'CurrentAxes',proyek.axes1);
gray=rgb2gray(I);

thresh=graythresh(gray);

imbw=im2bw(gray,thresh);
set(imshow(imbw));
imshow(imbw), title('CITRA ASLI');

set(proyek.figure1,'Userdata',imbw);
set(proyek.axes1,'Userdata',imbw);

% --- Executes on button press in pushbutton5.
function pushbutton5_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton5 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

proyek=guidata(gcbo);
imbw=get(proyek.axes1,'Userdata');

if isequal(imbw,[])
msgbox('Belum ada gambar!','Peringatan','warn');
else

%Kriptografi Visual
[share1, share2, share12] = ubahpiksel(imbw);

%Keluaran untuk menampilkan hasil share 1 dan share 2
set(proyek.figure1,'CurrentAxes',proyek.axes2);
imshow(share1);
imshow(share1),title('SHARE 1');

set(proyek.figure1,'CurrentAxes',proyek.axes3);
imshow(share2);
imshow(share2),title('SHARE 2');

set(proyek.figure1,'CurrentAxes',proyek.axes4);
imshow(share12);
imshow(share12);title('TUMPUKAN SHARE 1 & 2');
```

```
%Menyimpan file share 1, share 2 dan tumpukan share 1&2 dalam tipe
Bitmap
imwrite(share1,'Share1.bmp');
imwrite(share2,'Share2.bmp');
imwrite(share12,'Share 1&2.bmp');

end


% --- Executes on button press in pushbutton3.
function pushbutton3_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

%proses untuk tombol keluar

selection=questdlg(['Anda Yakin akan keluar dari '
get(handles.figure1,'name')''],...
    ['Keluar ' get(handles.figure1,'Name')''],...
    'Ya','Tidak','Ya');
if strcmp(selection,'Tidak')
    return;
end
delete(handles.figure1)

function edit1_Callback(hObject, eventdata, handles)
% hObject    handle to edit1 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of edit1 as text
%        str2double(get(hObject,'String')) returns contents of edit1
as a double



% --- Executes during object creation, after setting all properties.
function edit1_CreateFcn(hObject, eventdata, handles)
% hObject    handle to edit1 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns
called

% Hint: edit controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


%Program Kriptografi Visual
%Program Untuk mengacak permutasi generasi share
%menghasilkan share 1 dan share 2 secara acak untuk setiap piksel

function out = acakpiksel(a,b)

%proses mengacak kombinasi setiap piksel pada share1 dan share2
```

```
a1 = a(1);
a2 = a(2);
a3 = a(3);
a4 = a(4);

b1 = b(1);
b2 = b(2);
b3 = b(3);
b4 = b(4);

in = [a;b];
out = zeros(size(in));
randNumber = floor(1.9*rand(1));

if (randNumber == 0)
    out = in;
elseif (randNumber == 1)
    a(1) = a2;
    a(2) = a1;
    a(3) = a4;
    a(4) = a3;

    b(1) = b2;
    b(2) = b1;
    b(3) = b4;
    b(4) = b3;

    out = [a;b];
end


function [share1, share2, share12] = ubahpiksel(I)

%program untuk merubah subpiksel menjadi (2,2) 4 subpiksel
%setiap share1 dan share2 mempunyai (2,2) 4 subpiksel setiap pikselnya
s = size(I);
share1 = zeros(2*s(1),2*(s(2)));
share2 = zeros(2*s(1),2*(s(2)));

%proses pembentukan piksel putih
%kombinasi share pada piksel putih
disp('White Pixel Processing...');
s1a=[1 0;0 1];
s1b=[1 0;0 1];
[x, y] = find(I == 1);
len = length(x);

for i=1:len
    a=x(i)*2;b=y(i)*2;
    pixShare=acakpiksel(s1a,s1b);
    share1((a:a+1),(b:b+1))=pixShare(1:2,1:2);
    share2((a:a+1),(b:b+1))=pixShare(3:4,1:2);
end

%proses untuk piksel warna hitam
%kombinasi share pada piksel hitam
disp('Black Pixel Processing...');
s0a=[1 0;0 1];
```

```
s0b=[0 1;1 0];
[x, y] = find(I == 0);
len = length(x);

for i=1:len
    a=x(i)*2;b=y(i)*2;
    pixShare=acakpiksel(s0a,s0b);
    share1((a:a+1),(b:b+1))=pixShare(1:2,1:2);
    share2((a:a+1),(b:b+1))=pixShare(3:4,1:2);
end

%proses untuk menumpuk share1 dan share2
share12=bitor(share1, share2);
share12 = ~share12;
disp('Share Generation Completed.');
```