JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI

INSTITUT TEKNLOGI SEPULUH NOPEMBER

USULAN TUGAS AKHIR

1. IDENTITAS PENGUSUL

NAMA	**:**	**Mir'atul Mahmudah**
NRP	**:**	**5110100131**
DOSEN WALI	**:**	**Daniel O. Siahaan, S.Kom, MSc, PDEng**
DOSEN PEMBIMBING	**:**	**1. Arya Yudhi Wijaya, S.Kom, M.Kom**
		2. Rully Soelaiman, S.Kom, M.kom

2. JUDUL TUGAS AKHIR

"Implementasi algoritma *blind watermarking* menggunakan metode *fractional Fourier transform* dan *visual cryptography*."

3. LATAR BELAKANG

Watermarking merupakan salah satu teknologi masa kini yang banyak menarik minat para ahli untuk melakukan riset tentang perlindungan hak cipta citra digital. Skema *watermarking* yang dapat mengekstraksi citra *watermark* tanpa menggunakan informasi citra media disebut *blind watermarking* [1]. Skema ini dinilai lebih efektif dan efisien dalam melakukan *watermarking*, namun memiliki tingkat kesulitan yang lebih tinggi pada proses ekstraksi. Hal ini mendorong para peneliti untuk terus melakukan pengembangan pada algoritma ini. Beberapa metode juga telah diterapkan untuk mendapatkan hasil *watermarking* yang aman dan tahan (*robust*) dari berbagai manipulasi citra, baik pada domain spasial maupun domain frekuensi.

Pada implementasinya, *watermarking* yang dilakukan pada domain frekuensi lebih banyak digunakan karena tidak mengubah nilai piksel citra media. Sehingga dapat dilakukan pada semua jenis citra. Salah satu metode yang biasa digunakan untuk melakukan transformasi citra ke dalam domain frekuensi yaitu FrFT. *Fractional Fourier transform* (FrFT) merupakan bentuk umum dari *Fourier transform* yang mampu melakukan transformasi dengan sembarang sudut rotasi [2]. Kelebihan ini menyebabkan FrFT dapat digunakan secara efektif pada berbagai situasi. FrFT yang diterapkan pada citra digital adalah 2D-DFrFT dengan parameter (α, β) sebagai sudut rotasi [3]. Kombinasi kedua parameter ini menjadi kunci utama algoritma. Tanpa mengetahui parameter yang benar, maka akan sulit untuk mendapatkan data yang benar. Ini menunjukkan bahwa setiap parameter yang digunakan memiliki ciri khusus yang dapat digunakan sebagai kunci untuk melakukan transformasi.

Penggunaan parameter transformasi sebagai kunci *watermarking* tidak cukup untuk menjaga keamanan informasi yang disisipkan, sehingga diperlukan metode

tambahan lainnya. Metode *visual cryptography* (VC) mampu melakukan enkripsi pada citra dengan keamanan yang baik dan cukup mudah untuk diimplementasikan. Selain itu, implementasi metode VC pada proses *watermarking* menjadikan proses dekripsi citra tidak membutuhkan bantuan dari citra asli. Sehingga metode ini cocok untuk diterapkan pada algoritma *blind watermarking*. Metode VC melakukan enkripsi citra dengan membagi citra tersebut menjadi dua bagian yaitu *master share* dan *ownership share* [4]. Bagian *ownership share* merupakan bagian yang bertanggung jawab sebagai kunci untuk mengekstraksi *watermark*. Penerapan metode VC ternyata tidak hanya mampu menjadikan citra *watermark* yang tertanam aman dari serangan tetapi juga tahan terhadap berbagai manipulasi citra [5].

Pada tugas akhir ini, penulis mengusulkan penerapan gabungan metode *fractional Fourier transform* (FrFT) dan *visual cryptography* (VC) untuk menerapkan algoritma *blind watermarking* pada citra digital. Mula-mula citra asli ditransformasi menggunakan FrFT dengan (α, β) sebagai orde rotasi. Kemudian dilakukan dekomposisi citra dengan SVD untuk mendapatkan fitur citra asli. Dengan bantuan fitur citra asli itulah teknik *visual cryptography* diterapkan untuk mengenkripsi citra *watermark*. Dengan penggabungan metode FrFT dan VC, diharapkan akan menghasilkan sebuah citra ber-*watermark* yang tahan terhadap berbagai manipulasi citra dan juga memiliki tingkat keamanan yang kuat terhadap pendeteksian keberadaan *watermark* yang disisipkan.

4. RUMUSAN MASALAH

Beberapa rumusan masalah yang akan diselesaikan pada tugas akhir ini, yaitu:

1. Melakukan pemahaman konsep terhadap metode FrFT dan VC yang dapat meningkatkan kemampuan algoritma *blind watermarking* dalam melakukan *watermarking* pada citra.
2. Melakukan analisis dan perancangan algoritma *blind watermarking* menggunakan metode FrFT dan VC.
3. Mengimplementasikan metode FrFT dan VC pada algoritma *blind watermarking* dengan memilih *region of interest* (ROI) secara acak pada citra untuk mendapatkan citra ber-*watermark*.
4. Melakukan uji coba ekstraksi dengan algoritma *blind watermarking* menggunakan FrFT dan VC pada citra ber-*watermark* yang sudah dimanipulasi.

5. BATASAN MASALAH

Permasalahan yang dibahas dalam tugas akhir ini memiliki beberapa batasan, yaitu:

1. Aplikasi perangkat lunak dibangun dengan menggunakan kakas bantu MATLAB R2013a (8.1.0.604)
2. Citra yang digunakan untuk pengujian merupakan citra *grayscale* berukuran 512×512 dari database citra USC-SIPI.
3. Citra yang digunakan sebagai *watermark* merupakan citra biner berukuran 64×64.
4. Kinerja hasil uji coba dihitung dengan menggunkana *normalized correlation* (NC).

6. TUJUAN PEMBUATAN TUGAS AKHIR

Beberapa tujuan dari pembuatan tugas akhir ini, yaitu:

1. Memahami konsep dari metode FrFT dan VC yang dapat meningkatkan kemampuan algoritma *blind watermarking* dalam melakukan *watermarking* pada citra.
2. Membuat rancangan algoritma *blind watermarking* menggunakan metode FrFT dan VC.
3. Mengimplementasikan algoritma *blind watermarking* menggunakan metode FrFT dan VC dengan *region of interest* (ROI) tertentu yang dipilih secara acak.
4. Mengetahui kinerja algoritma yang telah diimplementasikan berdasarkan hasil uji coba ekstraksi dari citra ber-*watermark*.

7. MANFAAT TUGAS AKHIR

Hasil dari tugas akhir ini diharapkan dapat memberikan beberapa manfaat diantaranya yaitu:

1. Digunakan sebagai metode alternatif dalam melakukan *watermarking* pada citra digital.
2. Memberikan informasi bagi pihak yang ingin mengembangkan teknik *watermarking* pada data digital, khususnya citra digital.
3. Digunakan sebagai referensi pada penelitian tentang keamanan data digital di masa mendatang.

8. TINJAUAN PUSTAKA

Digital watermarking merupakan teknik menyisipkan informasi atau pesan ke dalam suatu media digital. Terdapat dua proses utama dalam *watermarking*, yaitu proses menyisipkan data dan proses mengekstrak data. Berdasarkan informasi yang dibutuhkan selama proses ekstraksi, skema *watermarking* dibedakan menjadi dua, yaitu *non blind watermarking* dan *blind watermarking* [1]. Jika pada saat ekstraksi membutuhkan informasi citra asli, maka disebut *non blind watermarking*. Sedangkan jika sama sekali tidak membutuhkan citra asli pada saat ekstraksi, maka disebut *blind watermarking*. Pada penggunaannya, skema *blind watermarking* dinilai para ahli lebih efektif dan efisien. Namun tidak dipakainya informasi citra asli menyebabkan skema *blind watermarking* memiliki tingkat kesulitan yang lebih pada saat ekstraksi. Hal ini mendorong para ahli untuk terus mengembangkan algoritma *blind watermarking* yang lebih optimal.

Penyisipan informasi pada proses *watermarking* dapat dilakukan pada domain spasial maupun domain frekuensi. Biasanya, informasi yang disisipkan pada domain spasial akan mengubah nilai piksel-piksel pada citra media. Berbeda dengan domain frekuensi yang melakukan penyisipan dengan memodifikasi koefisien hasil transformasi, sehingga tidak mempengaruhi nilai piksel-piksel citra media. Sehingga, *watermarking* pada domain frekuensi lebih banyak diminati untuk digunakan.

Salah satu metode yang biasa digunakan untuk melakukan transformasi citra ke dalam domain frekuensi yaitu FrFT. FrFT merupakan bentuk umum dari *Fourier transform*. Jika *Fourier transform* konvensional melakukan rotasi pada α kelipatan

$\pi/2$, maka untuk FrFT rotasi dapat dilakukan pada sembarang sudut rotasi [2]. Kelebihan yang dimiliki oleh FrFT dalam melakukan rotasi menyebabkan FrFT dapat digunakana secara efektif pada berbagai situasi. FrFT yang diterapkan pada citra digital adalah 2D-DFrFT. 2D-FrFT merupakan gabungan dari dua transformasi 1D-DFrFt pada baris dan kolom dengan parameter (α, β) masing-masing sebagai sudut rotasi [3]. Kombinasi kedua parameter ini memiliki ciri khusus yang dapat digunakan sebagai kunci untuk melakukan transformasi. Karena tanpa mengetahui parameter yang benar, maka akan sulit untuk mendapatkan hasil transformasi yang sama.

Untuk menjaga keamanan informasi yang disisipkan, biasanya transformasi dilakukan pada blok-blok piksel yang dipilih secara acak menggunakan PRNG dengan kunci K. Masing-masing blok yang telah ditransformasi selanjutnya didekomposisi menggunakan *singular value decomposition* (SVD). SVD adalah salah satu kakas analisa numerik yang efektif untuk menganalisa sebuah matrik. Dengan SVD, sebuah matrik dapat didekomposisi menjadi tiga matrik. Jika diketahui sebuah matrik A berukuran $n \times n$ dengan rank $r > 0$, maka dekomposisi dari matrik A dinyatakan dengan Persamaan 1 sebagai berikut.

$$A = U * S * V^T \quad (1)$$

Kolom-kolom U merupakan *eigenvector* dari AA^T dan dinamakan matrik vektor-vektor singulir kiri. Kolom-kolom V merupakan *eigenvector* dari $A^T A$ dan dinamakan matrik vektor-vektor singulir kanan. Sedangkan S adalah matrik diagonal yang elemen diagonalnya merupakan akar positif dari *eigenvalue* matrik A. Nilai-nilai singular pada matrik S menyatakan koefisien luminans suatu citra. Modifikasi kecil terhadap nilai singular tidak akan memberi pengaruh yang berarti pada visualisasi citra secara kasat mata. Penyisipan *watermark* dengan cara memodifikasi nilai singular terbesar dari matrik S mampu menghasilkan citra yang tahan dari serangan geometri [6]. Matrik S hasil dekomposisi dari setiap blok selanjutnya dipakai untuk membentuk fitur citra media yang diambil dari nilai-nilai singular pertama dari setiap blok.

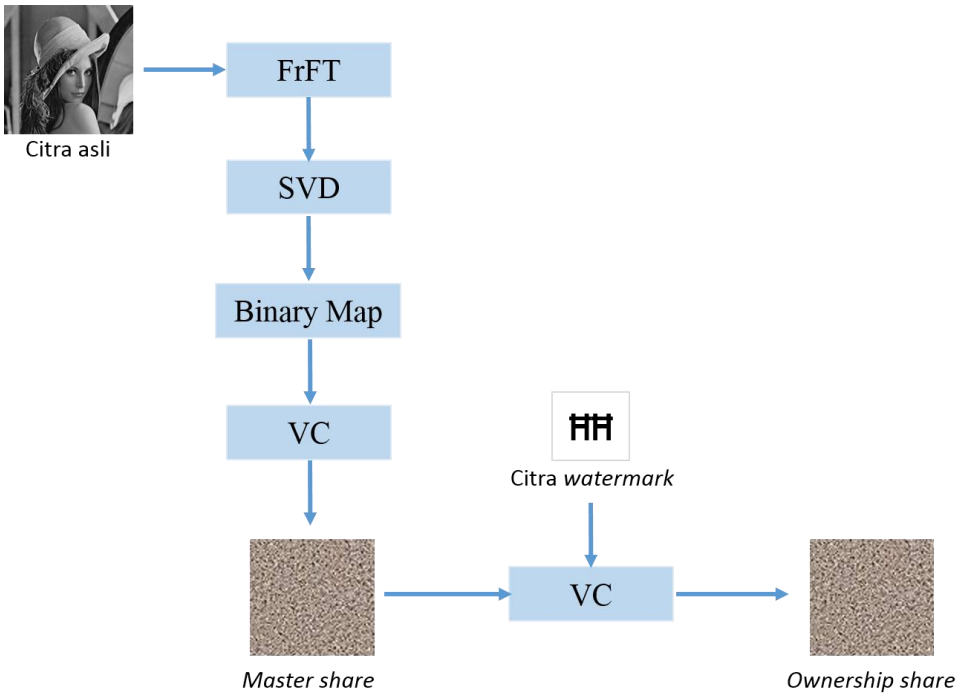
Untuk memudahkan implementasi algoritma *blind watermarking* pada proses ekstraksi digunakan metode *visual cryptography* (VC). *Visual cryptography* merupakan metode yang biasa digunakan untuk melakukan enkripsi informasi pada media visual seperti citra. Metode ini mampu membaca sandi citra tersembunyi tanpa banyak perhitungan kriptografi. Salah satu jenisnya yaitu *visual secret sharing* (VSS) dengan konsep (k, n) yang pertama kali diusulkan oleh Naor dan Shamir [4]. Skema ini memiliki tingkat keamanan yang baik dan cukup mudah untuk diimplementasikan. Pada implementasinya, skema ini membagi citra *watermark* menjadi n bagian (*share*) berbeda. Setiap *share* yang dihasilkan dari citra yang dienkripsi selanjutnya dijadikan kunci untuk melakukan dekripsi. Citra *watermark* dapat diekstrak kembali menggunakan paling sedikit k $(k \leq n)$ *share*, dan tidak memerlukan informasi citra asli.

Skema VSS (n, n) adalah skema yang paling aman dan paling nyaman dalam manajemen kunci [4]. Misalnya skema VSS (2, 2), pada skema ini tiap-tiap piksel dari citra watermark direpresentasikan ke dalam dua bagian, yaitu *master share* dan *ownership share*. Pembentukan *master share* ini membutuhkan bantuan dari fitur citra

media. Sedangkan *ownership share* dibentuk dengan memperhatikan *master share* dan citra *watermark*. Selanjutnya proses dekripsi dapat dilakukan hanya dengan menumpuk kedua bagian (*master share* dan *ownership share*) yang saling bersesuaian dari masing-masing piksel. Skema ini dianggap aman karena tanpa memiliki kedua *share*, sangat sulit bagi seseorang untuk mendapatkan citra *watermark* kembali. Hasil uji coba menunjukkan bahwa skema ini tidak hanya dapat memverifikasi *watermark* dengan jelas, tetapi juga kuat menahan berbagai serangan seperti kompresi JPEG, *scaling*, *noise adding*, *blurring* dan *sharpening* [5].

9. RINGKASAN ISI TUGAS AKHIR

Secara garis besar pengerjaan tugas akhir ini terbagi menjadi dua tahap, yaitu tahap penyisipan *watermark* dan tahap identifikasi *watermark*. Setiap tahap digambarkan dengan Gambar 1 dan Gambar 2.



Gambar 1. Diagram alir pada tahap penyisipan *watermark*

Diagram alir yang ditunjukkan oleh Gambar 1 merupakan gambaran umum pada tahapan penyisipan *watermark*. Detail dari masing-masing tahap dijelaskan sebagai berikut:

1. Tahap Pra Proses
   Pada tahap ini, citra asli dibagi menjadi blok-blok 4×4 *non-overlapping*. Kemudian dipilih $m \times n$ blok secara acak menggunakan PRNG dengan K sebagai kunci rahasia. Blok-blok inilah yang kemudian akan ditransformasi menggunakan FrFT. Blok-blok hasil transformasi selanjutnya didekomposisi dengan SVD untuk mendapatkan matrix X yang berisi nilai singular pertama dari tiap-tiap blok.

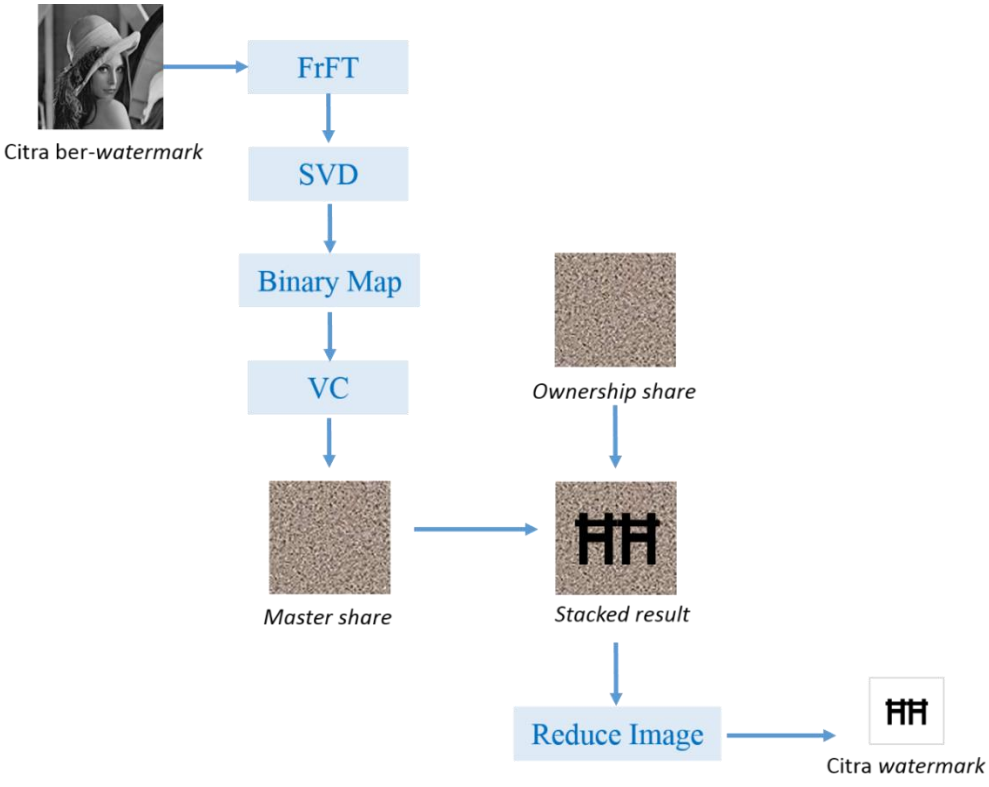
Kemudian dibangun matrik B, yaitu matrik bilangan biner sesuai dengan Persamaan 2 berikut,

$$B_{i,j} = \begin{cases} 0 & if\ X_{i,j} < X_{av} \\ 1 & if\ X_{i,j} \geq X_{av} \end{cases} \quad (2)$$

dengan X_{av} merupakan nilai rata-rata dari semua pixel di X.

2. Pembangkitan Citra *Master Share*
   Input yang digunakan untuk pembangkitan *master share* M yaitu matrik B. Pembangkitan *master share* M yang berukuran $2m \times 2n$ dilakukan dengan metode VC, yaitu setiap sel dari matrik B direperesentasikan dengan matrik 2×2.

3. Pembangkitan Citra *Ownership Share*
   Ownership share O merupakan matrik berukuran $2m \times 2n$ yang dibentuk dari *master share* M dan citra *watermark* S dengan metode VC. Jika piksel pada citra *watermark* berwarna hitam atau $S_i = 0$, maka piksel pada *ownership share* O_i merupakan komplemen dari piksel *master share* M_i. Sedangkan jika piksel pada citra *watermark* berwarna putih atau $S_i = 1$, maka piksel pada *ownership share* O_i sama dengan piksel *master share* M_i. Selanjutnya *ownership share* O harus disimpan dengan sebuah *certified authority (CA)* untuk autentikasi lebih lanjut.



Gambar 2. Diagram alir tahap identifikasi citra *watermark*

Diagram alir yang ditunjukkan oleh Gambar 2 merupakan gambaran umum pada tahap identifikasi citra *watermark*. Detail dari masing-masing tahap dijelaskan sebagai berikut:

1. Citra Masukan
   Citra yang menjadi masukan pada tahap identifikasi merupakan citra ber-*watermark* baik yang belum maupun sudah dilakukan pengolahan citra sebelumnya. Pengolahan citra yang digunakan seperti kompresi JPEG, *filtering, blurring, sharpening, noise addition, contrast adjustment, histogram equalization, resizing, rotation* dan *distortion.*

2. Pembangkitan *Master Share*
   Proses pembangkitan *master share* pada tahap identifikasi sama seperti proses sebelumnya. Perbedaannya hanya terletak pada masukan yang digunakan. Mula-mula citra ber-*watermark* dibagi menjadi blok-blok 4×4 *non-overlapping*. Kemudian dipilih $m \times n$ blok secara acak menggunakan PRNG dengan K sebagai kunci rahasia. Blok-blok ini kemudian ditransformasi menggunakan FrFT dengan parameter (α, β). Dari hasil transformasi, dilakukan SVD untuk mendapatkan matrix X' yang berisi nilai singular pertama dari tiap-tiap blok. Kemudian dibangun matrik B', yaitu matrik bilangan biner sesuai dengan Persamaan 3.

$$B'_{i,j} = \begin{cases} 0 & if\ X'_{i,j} < X'_{av} \\ 1 & if\ X'_{i,j} \geq X'_{av} \end{cases} \quad (3)$$

   Dengan X'_{av} merupakan nilai rata-rata dari semua pixel di X'. Matrik X' selanjutnya digunakan sebagi masukan pada metode VC untuk membentuk *master share* M' dengan aturan yang sama seperti sebelumnya.

3. Ekstraksi Citra *Watermark*
   Proses ekstraksi dilakukan dengan menumpuk *master share* M' dan *ownership share* O yang telah disimpan. Untuk mendapatkan citra *watermark* dengan ukuran $m \times n$, maka dilakukan reduksi pada citra hasil penumpukan (S') menjadi citra *watermark* S''.

Setelah citra *watermark* didapatkan, selanjutnya dilakukan pengujian ketahanan citra *watermark* menggunakan *normalized correlation* (NC). Nilai hasil perhitungan yang didapat menunjukkan akurasi kemiripan antara citra *watermark* yang terekstraksi dengan citra *watermark* asli.

10.METODOLOGI

Metode yang akan dilakukan pada pengerjaan tugas akhir ini memiliki beberapa tahapan, yaitu:

a. Penyusunan proposal tugas akhir

Tahap pertama untuk memulai pengerjaan tugas akhir yaitu penyusunan proposal. Pada proposal ini, penulis mengajukan gagasan mengenai implementasi algoritma *blind watermarking* pada citra menggunakan metode *fractional Fourier transform* dan *visual cryptography.*

b. Studi literatur

Pada tahap ini dilakukan pencarian informasi dan studi literatur yang diperlukan untuk pengumpulan data dan desain perangkat lunak yang akan dibuat. Informasi didapatkan dari jurnal ilmiah, buku dan materi-materi lain yang berhubungan dengan metode yang digunakan dalam pengerjaan tugas akhir ini, yang didapat dari internet maupun buku acuan.

c. Analisis dan desain perangkat lunak

Pada tahap ini dilakukan analisis terhadap metode-metode yang akan digunakan. Analisis setiap metode memperhatikan parameter masukan dan kompleksitas waktu komputasi. Hasil analisa selanjutnya digunakan untuk merancang pembuatan program.

d. Implementasi perangkat lunak

Implementasi merupakan tahap untuk menerapkan metode tersebut ke dalam sebuah program. Proses penerapan metode tersebut menggunakan kakas bantu yaitu MATLAB.

e. Pengujian dan evaluasi

Pada tahap ini dilakukan pengujian untuk mencoba aplikasi apakah telah sesuai dengan rancangan dan desain metode yang dibuat, serta mencari ketidaksesuaian yang ada pada program untuk selanjutnya dilakukan perbaikan dan penyempurnaan. Pengujian dilakukan dengan menggunakan citra abu-abu 512×512 sebagai media dan citra biner 64×64 sebagai *watermark*.

f. Penyusunan Buku Tugas Akhir

Pada tahap ini dilakukan penyusunan laporan yang menjelaskan dasar teori dan metode yang digunakan dalam tugas akhir ini serta hasil dari implementasi aplikasi perangkat lunak yang telah dibuat. Sistematika penulisan buku tugas akhir secara garis besar antara lain:

1. Pendahuluan
    a. Latar Belakang
    b. Rumusan Masalah
    c. Batasan Tugas Akhir
    d. Tujuan
    e. Metodologi
    f. Sistematika Penulisan
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Pengujian dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka

11.JADWAL KEGIATAN

Rencana jadwal kegiatan pengerjaan tugas akhir ini digambarkan ke dalam **Tabel 1** seperti di bawah ini.

Tabel 1. Jadwal kegiatan pengerjaan tugas akhir

Tahapan	Tahun 2014																					
	Februari				Maret				April				Mei					Juni				
Penyusunan Proposal																						
Studi Literatur																						
Perancangan system																						
Implementasi																						
Pengujian dan evaluasi																						
Penyusunan buku																						

12. DAFTAR PUSTAKA

[1] A. Bovik, Handbook of Image and Video Processing 2nd Edition, United States of America: Elsevier Academic Press, 2005.

[2] V. A. Narayanan and K. Prabhu, "The fractional Fourier transform: theory, implementation and error analysis," *Microprocessor and Microsystems*, vol. 27, pp. 511-521, 2003.

[3] S. C. Pei and M. H. Yeh, "Two dimensional discrete fractional Fourier transform," *Signal Processing*, vol. 67, pp. 99-108, 1998.

[4] M. Naor and A. Shamir, "Visual Cryptography," *Lecture Notes in Computer Science*, vol. 950, p. 1–12, 1995.

[5] D. C. Lou, H. K. Tso and J. L. Liu, "A copyright protection scheme for digital images using visual cryptography technique," *Computer Standarts and Interfaces*, vol. 29, pp. 125-131, 2007.

[6] C. C. Chang, P. Tsai and C. C. Lin, "SVD-based digital image watermarking scheme," *Patterns Recognition Letters*, vol. 26, pp. 1577-1586, 2005.

[7] S. Rawat and B. Raman, "A blind watermarking algorithm based on fractional Fourier transform and visual cryptography," *Signal Processing*, vol. 92, pp. 1480-1491, 2012.