PROPOSAL SKRIPSI S1

Analisis Skema *Image Sharing* berdasarkan Metode *Singular Value Decomposition* (SVD) dan *Fourier Transform* (FT)

Disusun Oleh :

Zainul Insaan Abdul Hafiidhl

M0514056

PROGRAM STUDI INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS SEBELAS MARET

SURAKARTA

2018

UNIVERSITAS SEBELAS MARET
PROGRAM STUDI INFORMATIKA

PROPOSAL SKRIPSI S1

Nama : Zainul Insaan Abdul Hafiidhl

NIM : M0514056

PERSETUJUAN PEMBIMBING

Proposal Skripsi S1 ini telah disetujui oleh :

Pembimbing I

HERI PRASETYO, S.Kom, M.Sc.Eng., Ph.D.

NIP. 1983030220161001

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1. Latar Belakang

Pada akhir-akhir ini, semakin banyak fasilitas-fasilitas atau layanan yang memanfaatkan penyimpanan data pada *cloud server*. Hal ini dikarenakan penyimpanan data pada *cloud server* memberikan keuntungan dalam segi mobilitas. Serta dikarenakan kebanyakan tempat sudah mendapat akses internet, sehingga penyimpanan data pada *cloud server* semakin mudah untuk diterima oleh *end-user*.

Namun dibalik keuntungan tersebut, penyimpanan data pada *cloud server* memiliki kelemahan adalah keamanan data pada *cloud server*. Hal ini dikarenakan seiring berkembangnya teknologi dan ilmu pengetahuan, maka cara peretasan *cloud server* semakin canggih. Oleh sebab itu maka, sistem keamanan data pada *cloud server* perlu diperbarui beberapa waktu sekali.. Selain itu, peningkatan sistem keamanan pada *cloud server* sangatlah penting agar *end-user* percaya bahwa data yang disimpan di *cloud server* aman dan hanya dapat dilihat oleh *end-user* tersebut.

Banyak cara telah dilakukan untuk mengamankan data yang terdapat di *cloud server*. Salah satu cara untuk mengamankan data di *cloud server* adalah dengan menggunakan metode *secret sharing*, yang mana memecah data tersebut menjadi beberapa bagian dan mengirimkan pecahan data tersebut ke bebrapa *server*.

Dalam *paper* yang diajukan oleh (Singh, Raman, & Misra, 2017), untuk mengamankan data pada *cloud server* digunakan skema *Shamir Secret Sharing* (SSS) beserta *Singular Value Decomposition* (SVD) dan *Fractional Fourier Transform* (FrFT) untuk memasukkan dan memastikan informasi spesifik pemilik data. Dalam *paper* tersebut, skema SSS

digunakan untuk mengengkripsi gambar menjadi beberapa *shares*, untuk selanjutnya disimpan ke *server-server cloud*. Sedangkan metode FrFT digunakan untuk mendekomposisi *shares* yang terpilih berdasarkan *secret key* untuk selanjutnya ditanam gambar *watermark* menggunakan metode SVD.

Namun dalam *paper* yang diajukan oleh (Loukhaoukha, Refaey, & Zebbiche, 2016) menyebutkan bahwa algoritma *watermarking* (Liu & Tan, 2002) yang menggunakan metode SVD memiliki kecacatan secara fundamental dikarenakan matriks vektor singular U_W dan V_W dari *watermark* W yang mana merepresentasikan informasi penting dapat menyebabkan permasalahan *false positive detection* meskipun watermark yang ditanam berbeda atau bahkan tidak ada. Dalam *paper* yang diusulkan oleh (Guo & Prasetyo, 2014a) menyebutkan bahwa kelemahan utama dari skema *watermarking* gambar berdasarkan (SVD) adalah *false positive detection* yang dapat menyebabkan attacker dapat dengan mudah mengklaim dan mendapatkan watermark dari gambar.

Dari *paper* yang telah disebutkan diatas, dapat dismpulkan bahwa watermarking gambar berdasarkan SVD memiliki kelemahan utama yakni *false positive detection*. Oleh sebab itu, muncullah gagasan bahwa skema (Singh et al., 2017) memiliki kemungkinan untuk terjadi *false positive detection*. Dari gagasan tersebut diangkatlah penelitian ini, untuk menguji apakah terjadi permasalahan *false positive detection*.

1.2. Rumusan Masalah

Rumusan masalah dari penelitian ini adalah apakah skema *image sharing* berdasarkan metode SVD dan FT mengalami permasalahan *false positive detection*.

1.3. Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut:

1. Gambar input yang digunakan adalah gambar RGB.
2. Skema *image sharing* yang akan digunakan adalah *Shamir Secret Sharing* dan *Chinese Remainder Theorem-based Secret Sharing*.
3. Skema image sharing yang digunakan memiliki *threshold* (k, n)

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah melakukan pengujian pada skema *image sharing* berdasarkan metode SVD dan FT bebas dari permasalahan *false positive detection*.

1.5. Manfaat Penelitian

Manfaat dari melakukan penelitian ini adalah mengetahui apakah skema *image sharing* yang berdasarkan metode SVD dan FT aman dan bebas dari permasalahan *false positive detection*.

1.6. Sistematika Penulisan

Sistematika penulisan dari laporan penelitian untuk tugas akhir adalah sebagai berikut:

BAB I PENDAHULUAN

Pada Bab I menguraikan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan. Pada latar belakang menguraikan tentang kisah yang menjadi latar belakang munculnya gagasan untuk melakukan penelitian ini. Rumusan masalah menguraikan tentang permasalahan apa yang terjadi di latar belakang serta permasalahan yang akan diselesaikan pada penelitian ini. Batasan masalah menguraikan tentang batasan-batasan yang diterapkan pada penelitian ini, baik secara disengaja maupun tidak disengaja. Tujuan penelitian menguraikan tujuan yang diharapkan untuk dicapai pada

penelitian ini. Manfaat penelitian menguraikan manfaat apa saja yang diperoleh dari hasil penelitian ini, jika penelitian ini berhasil. Sistematika penulisan menguraikan sistematika yang digunakan pada penulisan penelitian ini.

BAB II TINJAUAN PUSTAKA

Pada Bab II menguraikan tentang landasan / dasar teori yang digunakan dalam penelitian serta memberikan pembahasan tentang penelitian terkait yang pernah dilakukan sebelumnya. Landasan atau dasar teori menguraikan tentang teori-teori dasar apa yang digunakan dalam penelitian ini serta metode-metode apa yang akan digunakan dalam penelitian ini untuk menyelesaikan permasalahan. Penelitian terkait menguraikan tentang penelitian-penelitian yang pernah dilakukan sebelumnya yang mana berkaitan dengan permasalahan serta metode-metode yang ada pada penelitian ini.

BAB III METODOLOGI PENELITIAN

Pada Bab III menguraikan tentang metodologi yang akan digunakan dalam penelitian. Metodologi penelitian yang digunakan dalam penelitian ini memiliki tahapan-tahapan sebagai berikut Studi literatur, Analisis dan Perencanaan, Implementasi, Pengujian, serta Penarikan kesimpulan. Pada tahapan studi literatur, dilakukan studi terhadap literatur-literatur yang digunakan untuk menjadi sumber pada dasar teori. Literatur-literatur yang digunakan dapat bersumber dari buku, artikel dalam jurnal atau makalah, maupun dari internet. Pada tahapan analisis dan perencananaan, dilakukan analisis terhadap metode yang digunakan, analisis input dan output yang digunakan pada program, analisis hasil yang mungkin dicapai dalam penelitian, perencanaan lama waktu penelitian, perencanaan bahasa pemrograman yang akan digunakan, perencanaan bagaimana mengimplementasi metode menjadi program, dan perencanaan pengujian yang akan digunakan dalam penelitian.

Pada tahap implementasi, dilakukan implementasi kedalam bentuk program berdasarkan analisis dan perencanaan. Dalam implementasi ini, metode-metode yang mana berbentuk persamaan matematika akan diterapkan menjadi dalam bentuk program. Pada tahap pengujian, dilakukan pengujian terhadap metode-metode yang telah menjadi bentuk program. Dalam pengujian ini, juga dilakukan pengujian menggunakan alat-alat pengujian yang telah direncanakan pada tahap anlisis dan perencanaan. Serta pembuktian teori pada penelitian ini dilakukan didalam tahap ini.

Lalu tahap yang terakhir adalah Penarikan Kesimpulan. Pada tahap ini, hasil yang diperoleh dari tahap pengujian dianalisis untuk ditarik kesimpulannya. Biasanya hasil dari penelitian menyelesaikan permasalahan yang terdapat pada rumusan masalah. Jika hasil dari penelitian tidak dapat menyelesaikan permasalahan, maka dituliskan penyebab kenapa penelitian tidak dapat menyelesaikan permasalahan.

BAB IV PEMBAHASAN

Pada Bab IV menguraikan tentang pembahasan dan hasil dari penelitian yang dilakukan, yang mana merupakan penyelesaian dari rumusan masalah berdasarkan metodologi penelitian yang digunakan untuk mencapai tujuan dari penelitian. Dalam pembahasan, diuraikan tentang penjabaran metode-metode yang digunakan dalam penelitian dan bagaimana metode tersebut diimplementasikan ke dalam program. Penjabaran metode-metode tersebut dapat berbentuk penjabaran atau penurunan secara matematika. Dalam pembahasan ini, juga dibahas cara metode tersebut diimplementasikan ke dalam program. Dalam pembahasan ini juga, dijabarkan flowchart program beserta dengan metode-metode yang digunakan.

BAB V PENUTUP

Pada Bab V menguraikan tentang kesimpulan yang dicapai dari penelitian serta menguraikan saran untuk penelitian kedepannya. Dalam kesimpulan ini, hasil yang diperoleh dari program yang telah diimplementasikan dijabarkan. Dalam kesimpulan ini juga, dapat dijelaskan kenapa bisa memperoleh hasil yang diperoleh dari program. Dari kesimpulan yang telah dituliskan, dituliskan saran untuk penelitian kedepannya agar penelitian kedepannya memiliki hasil yang lebih bagus atau memperbaiki penelitian yang ada.

BAB II
TINJAUAN PUSTAKA

2.1. Dasar Teori

2.1.1. Shamir Secret Sharing

Shamir Secret Sharing (SSS) adalah sebuah algoritma atau skema untuk mengamankan data yang bersifat rahasia. Algoritma ini diciptakan oleh Adi Shamir dimana data yang menjadi rahasia (*secret*) dibagi-bagi atau dipecah menjadi beberapa bagian atau *shares* sebanyak n. Bagian-bagian tersebut lalu dibagikan ke n *participant* yang mana setiap bagian tersebut unik dan setiap bagian tersebut tidak dapat memberi tahu *secret* tersebut. Untuk mendapatkan data yang menjadi rahasia, diperlukan menggabungkan bagian-bagian tersebut sebanyak *threshold* k tertentu, dimana nilai k adalah $0 < k \leq n$. Bagian-bagian yang digabung tersebut tidak dapat membentuk *secret* jika jumlah bagian kurang dari *threshold*. Berikut adalah fungsi SSS untuk membuat *share*:

$$f(x) = \left(a_0 + \sum_{i=0}^{k-1} a_i x^i \right) mod\ m$$

Dengan a_0 adalah secret yang ingin disimpan, a_i adalah koefisien dimana $a_i < m$ dan $a_1, a_2, a_3, \dots, a_n$, lalu m adalah bilangan prima besar. Untuk mendapatkan secretnya dapat dilakukan dengan menerapkan *Lagrange Interpolation* yang mana memenuhi syarat jumlah *threshold*.

2.1.2. Chinese Remainder Theorem (CRT)

Chinese Remainder Theorem atau (CRT) adalah sebuah teorema matematika yang memungkinkan seseorang mengingat kembali sebuah angka asalkan seseorang mengingat beberapa angka pembagi dan sisa bagi-nya (atau hasil modulusnya) dengan angka numerik tersebut. Angka

pembagi atau modulusnya dalam CRT adalah merupakan bilangan integer positif yang mana bilangan satu adalah bilangan prima dengan yang lainnya atau bilangan prima integer positif relatif.

Untuk mencari angka x dalam CRT adalah sebagai berikut, misalkan terdapat $m_1, m_2, m_3, \dots, m_n$ adalah merupakan bilangan prima integer positif relatif, dan $a_1, a_2, a_3, \dots, a_n$ adalah bilangan integer. Lalu terdapat sistem $x \equiv a_i (mod\ m_i)$ untuk $1 \leq i \leq n$ serta $M = m_1 \times m_2 \times m_3 \times \dots \times m_n$, maka nilai x dapat dicari dengan:

$$x = \left[\sum_{i=1}^{n} a_i M_i b_i \right] (mod\ M)$$

Dengan $M_i = \frac{M}{m_i}$ dan b_i diperloeh dari $b_i \frac{M}{m_i} \equiv 1 (mod\ m_i)$. Atau dapat dikatakan bahwa b_i adalah sebuah invers dari M_i yang mana adalah *Extended Euclidian Algorithm* untuk $gcd(M_i, m_i)$.

2.1.3. Singular Value Decomposition (SVD)

Singular Value Decomposition atau yang disingkat dengan SVD adalah merupakan metode mendekomposisi matriks yang bertujuan untuk memudahkan perhitungan matrik menjadi lebih sederhana. Bentuk umum dari SVD dari sebuah matriks A adalah sebagai berikut:

$$A = U\ D\ V^T$$

Dimana A adalah sebuah matriks real berukuran $m \times n$, U adalah matriks *unitary* berukuran $m \times m$, D adalah matriks diagonal berukuran $m \times n$, dan V adalah matriks *unitary* berukuran $n \times n$ dengan V^T adalah *conjugate transpose* dari matriks V. Nilai dari matriks diagonal D adalah *singular value* dari matriks A. Kolom pada matriks U adalah *left-singular vector* dari matriks A dan Kolom pada matriks V adalah *right-singular vector* dari matriks A.

2.1.4. Fourier Transform

Fourier transform dalam definisi *image processing* adalah alat transformasi gambar yang digunakan untuk mendekomposisi gambar menjadi komponen sinus dan cosinus pada gambar tersebut. Output dari transformasi ini adalah sebuah gambar yang terletak pada domain Fourier atau frekuensi, sedangkan inputnya adalah gambar yang berasal dari domain spasial (dimensi ruang pada dunia nyata baik 2D maupun 3D). Atau dengan kata lain, setiap titik pada domain fourier merepresentasikan frekuensi yang terdapat pada domain spasial.

Secara umum, berdasarkan sinyal yang digunakan Fourier Transform dapat dibagi menjadi 4 kategori yaitu:

a. Continous-time aperiodic signal
b. Continous-time periodic signal (Fourier Series expansion, FS)
c. Discrete-time aperiodic signal (Discrete-time Fourier Transform, DTFT)
d. Discrete-time periodic signal (Discrete Fourier Transform, DFT)

Dikarenakan sinyal yang digunakan merupakan gambar dan masuk kedalam kategori sinyal Discrete-time periodic signal, maka Fourier Transform yang digunakna adalah Discrete Fourier Transform (DFT). Persamaan Discrete Fourier Transform 2 dimensi untuk gambar berukuran $N \times N$ adalah seperti berikut:

$$F(k,l) = \sum_{a=0}^{N-1} \sum_{b=0}^{N-1} f(a,b) e^{-i2\pi\left(\frac{ki}{N} + \frac{lj}{N}\right)}$$

Dengan $f(a,b)$ adalah gambar yang berada pada domain spasial, dan exponensial adalah fungsi basis untuk menghubungkan setiap titik domain spasial ke setiap titik dimensi fourier. Atau dengan kata lain setiap titik pada dimensi fourier didapat dengan cara mengalikan setiap titik pada domain spasial dengan fungsi basis. Dengan konsep ini, dapat dikatakan

dimensi fourier dapat ditransformasi kembali menjadi domain spasial atau yang disebut invers Fourier Transform:

$$f(a,b) = \frac{1}{N^2} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} F(k,l) e^{i2\pi\left(\frac{ka}{N}+\frac{lb}{N}\right)}$$

Untuk menghitung Fourier Transform, setiap pixel yang terdapat pada gambar dihitung. Namun karena Fourier Transform dapat dihitung secara terpisah, maka persamaan diatas dapat ditulis kembali menjadi:

$$F(k,l) = \frac{1}{N} \sum_{b=0}^{N-1} f(k,b) e^{-i2\pi\frac{ib}{N}}$$

Dan,

$$f(k,b) = \frac{1}{N} \sum_{a=0}^{N-1} f(a,b) e^{-i2\pi\frac{ka}{N}}$$

2.2. Penelitian Terkait

Penelitian sebelumnnya yang berkaitan dengan penelitian yang diajukan adalah sebagai Berikut:

1. **Singh, P., Raman, B., & Misra, M. (2017). A Secure Image Sharing Scheme based on SVD and Fractional Fourier Transform. Signal Processing: Image Communication.**

   Penelitian ini membahas tentang skema *image sharing* pada arsitektur *cloud server* untuk mengamankan dan menjaga agar media gambar yang di simpan pada arsitektur *cloud server* tidak rentan terhadap peretasan. Pada penelitian tersebut, untuk menjaga media gambar yang disimpan, verifikasi kepemilikan multimedia menggunakan metode *singular value decomposition* (SVD) serta *Fractional Fourier Transform* (FrFT). Tahapan dalam mengamankan dan melakukan verifikasi

kepemilikan media gambar yang disimpan di arsitektur *cloud server* dalam penelitian ini adalah sebagai berikut:

1. Pada media gambar yang akan disimpan ke dalam arsitektur *cloud server*, informasi dari media gambar tersebut akan dikaburkan dan dibagi-bagi menjadi beberapa bagian. Dimana setiap bagian-bagian tidak dapat memeberi tahu informasi tentang media gambar. Media gambar tersebut dikaburkan dan dibagi-bagi menggunakan skema *Shamir Secret Sharing* (SSS). Dan bagian-bagian tersebut disebarkan ke beberapa server yang terdapat di arsitektur.
2. Media gambar yang telah dikaburkan dan disimpan ke beberapa server, informasi kepemilikannya di pertegas dengan menanam informasi spesifik dari pemilik ke beberapa bagian berdasarkan *secret key* tertentu dengan menggunakan metode *Singular Value Decomposition* (SVD) dan *Fractional Fourier Transform* (FrFT).
3. Informasi spesifik dari pemilik tersebut dapat diekstrak langsung dari arsitektur *cloud server* maupun setelah media gambar yang dienkripsi diperoleh kembali.

2. **Guo, J. & Prasetyo, H. (2014). False-positive-free SVD-based image watermarking. Journal of Visual Communication and Image Representation.**

Penelitan ini membahas tentang mengatasi permasalahan utama dalam *watermarking* gambar menggunakan metode *Singular Value Decomposition* (SVD). Dalam penelitian tersebut disebutkan bahwa kelemahan utama dari metode SVD untuk *watermarking* gambar adalah permasalahan *false positive detection*. Untuk mengatasi permasalahan tersebut, dalam penelitian tersebut diajukan metode *watermarking* gambar berdasarkan metode SVD yang baru, yakni dengan cara menanam komponen utama dari *watermark* ke dalam *host image* yang terbagi ke dalam blok-blok menggunakan konsep *spread spectrum*. Tahapan dari metode baru yang diajukan dalam penelitian tersebut adalah:

1. *Host image* yang akan di *watermark*, pertama-tama di dekomposisi menggunakan *Discrete Wavelet Transform* (DWT) menjadi empat *sub-bands*.
2. Kemudian *sub-band* LL dibagi menjadi beberapa blok gambar yang tidak tumpang-tindih yang mana kemudian SVD diapliaksikan kesetiap blok gambar.
3. Informasi *watermark* kemudian ditanam ke dalam blok gambar LL miliknya *host image* dengan memodifikasi *singular value* terbesar ke dari setiap blok gambar.

Hasil dari penelitian ini adalah metode yang diajukan dapat mengatasi permasalahan *false positive problem*, memperoleh *payload* yang tinggi, serta memiliki performa yang melebihi dari metode *watermarking* SVD yang telah ada.

3. **Loukhaoukha, K., Refaey, A., & Zebbiche, A. (2016). Comments on "Homomorphic image watermarking with a singular value decomposition algorithm.". Information Processing and Management.**

Dalam artikel makalah ini, membahas tentang kesalahan pada artikel makalah yang di usulkan oleh (Abdallah et al., 2014). Dalam artikel makalah tersebut mengometari bahwa skema watermarking pada artikel makalah (Abdallah et al., 2014) memiliki kesalahan fundamental pada algoritma yang digunakan. Karena pada algoritma yang digunakan, menggunakan algoritma SVD yang diusulkan oleh (Liu & Tan, 2002), yang mana algoritma tersebut memiliki kesalahan fundamental, yakni *false positive detection*.

4. **Yan et. al. (2017). Chinese Remainder Theorem-Based Secret Image Sharing for $(\boldsymbol{k}, \boldsymbol{n})$ Threshold.**

Dalam penelitian ini, membahas tentang skema *secret image sharing* (SIS) menggunakan metode Chinese Remainder Theorem (CRT). Dalam penelitian ini diklaim bahwa CRTSIS memiliki keunggulan

dibandingkan dengan Shamir SIS original, yakni pemulihan *host image* tanpa kehilangan informasi, kompleksitas komputasi pemulihan *host image* yang rendah, serta tidak memerlukan metode lain untuk membantu pemulihan *host image*. Skema CRTSIS yang diusulkan dalam penelitian ini berguna untuk memperbarui skema CRTSIS tradisional yang mana memiliki permasalahan tidak memiliki *threshold* (k, n) , kehilangan informasi pada saat pemulihan *host image*, karakteristik *host image* yang dihiraukan oleh skema tersebut, serta memerlukan metode tambahan lain untuk membantu pemulihan *host image*.

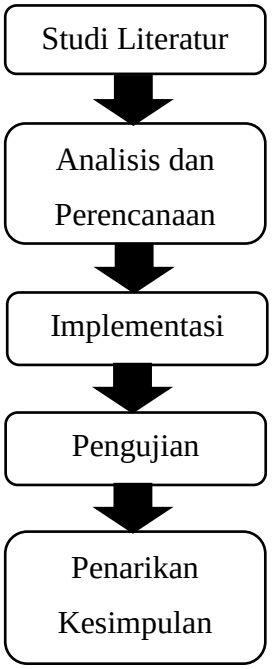
Tabel 2.1.Tabel Penelitian Terkait

No	Referensi	Judul	Metode	Hasil / Temuan
1.	Singh, P., Raman, B., & Misra, M. (2017).	A Secure Image Sharing Scheme based on SVD and Fractional Fourier Transform	a. Shamir Secret Sharing Scheme b. Singular Value Decomposition (SVD) c. Fractional Fourier Transform (FrFT)	a. Ketahanan terhadap serangan untuk mendapatkan informasi image sudah diuji. b. Skema terseebut dapat mentolerasi ketika beberapa server pada arsitektur sedang mengalami down.
2	Guo, J. & Prasetyo, H. (2014).	False-positive-free SVD-based image watermarking	a. Singular Value Decomposition (SVD) b. Discrete Wavelet Transform (DWT)	a. Mengatasi permasalahan false positive problem. b. Memperoleh payload yang tinggi. c. Memiliki performa watermarking gambar yang lebih baik dari metode yang telah ada.
3	Loukhaoukha, K., Refaey, A., & Zebbiche, A. (2016).	Comments on "Homomorphic image watermarking with a	-	Metode yang diusulkan pada paper (Abdallah et al., 2014) memiliki permasalahan *false positive detection*.

		singular value decomposition algorithm.”		
4	Yan et al. (2017)	Chinese Remainder Theorem-based Secret Image Sharin for (k, n) Threshold	a. Chinese Remainder Theorem (CRT)	Skema CRTSIS baru yang memiliki *threshold* (k, n), pemulihan *host image* tanpa kehilangan informasi, serta pemulihan *host image* tanpa memerlukan metode tambahan.

BAB III
METODOLOGI PENELITIAN

Metodologi yang digunakan dalam penelitian adalah sebagai berikut:



Gambar 3.1.Metodologi penelitian

3.1. Studi Literatur

Pada tahap studi literatur, Algoritma serta metode-metode yang diperlukan dalam penelitian dikaji dan dipelajari dengan seksama. Sumber dari algoritma ataupun metode-metode yang diperlukan dapat berasal dari jurnal yang telah diterbitkan sebelumnya, maupun buku-buku yang memiliki teori dasar yang terkait dengan penelitian. Sumber utama dari literatur yang digunakan dalam penelitian ini adalah artikel makalah yang berkaitan dengan skema image sharing yang memiliki *threshold* (k, n) dengan yang mana untuk memverifikasi kepemilikan *host image*

menggunakan metode SVD dan FT. Sumber literatur lainnya yang digunakan pada penelitian ini bersumber dari internet.

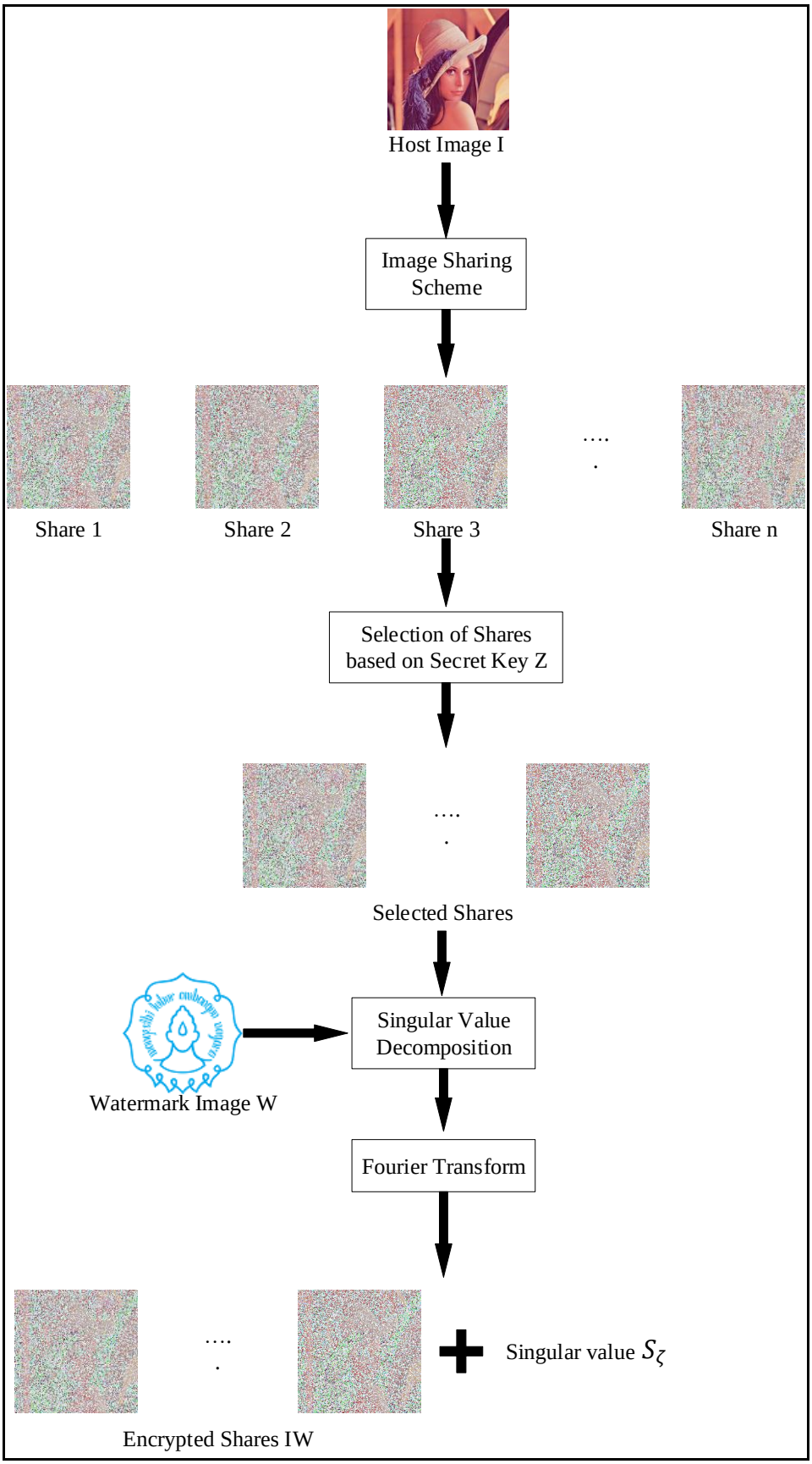
3.2. Analisis dan Perencanaan

Pada tahap analisis dan perencanaan, menganalisis input dan output apa yang akan diberikan pada program, menganalisis alat uji yang akan digunakan pada program, merencanakan waktu penelitian. Input yang digunakan pada program yang mana akan diberikan oleh *end user* adalah gambar yang akan di *watermark* atau *host image* serta gambar *watermark* itu sendiri. Sedangkan output yang diberikan oleh program berupa pecahan-pecahan *host image* yang sudah termasamarkan atau *shares*, *shares* yang sudah ditanam dengan *gambar watermark* atau *watermarked shares*, gambar yang telah diperoleh kembali dari menggabungkan beberapa *shares*, serta *watermark* yang diperoleh kembali dari *watermarked shares*.

Alat uji yang digunakan pada program adalah beberapa macam serangan baik pada *shares* mapun pada *encrypted shares*. Lama waktu penelitian diperkirakan selama 5 bulan, antara lain bulan pertama hingga bulan kedua digunakan untuk melakukan studi literatur. Lalu analisis dan perencanaan dilakukan pada bulan kedua minggu ketiga hingga bulan ketiga minggu keempat. Lalu Implementasi dilakukan pada bulan ketiga minggu ke empat hingga bulan kelima minggu kedua. Tahap pengujian dilakukan pada bulan kelima minggu pertama hingga minggu keempat, dan yang terakhir penarikan kesimpulan dilakukan pada bulan kelima minggu keempat. Bahasa pemrograman yang akan digunakan pada program untuk implementasi adalah Bahasa pemrograman Java.

3.3. Implementasi

Pada tahap implementasi, skema akan diimplementasikan ke dalam program dan dibangun sesuai dengan algoritma dan metode yang telah direncanakan. Berikut adalah flowchart skema yang akan digunakan:


Host Image I
Image Sharing Scheme
Share 1
Share 2
Share 3
....
Share n
Selection of Shares based on Secret Key Z
....
Selected Shares
Watermark Image W
Singular Value Decomposition
Fourier Transform
....
Singular value S_ζ
Encrypted Shares IW

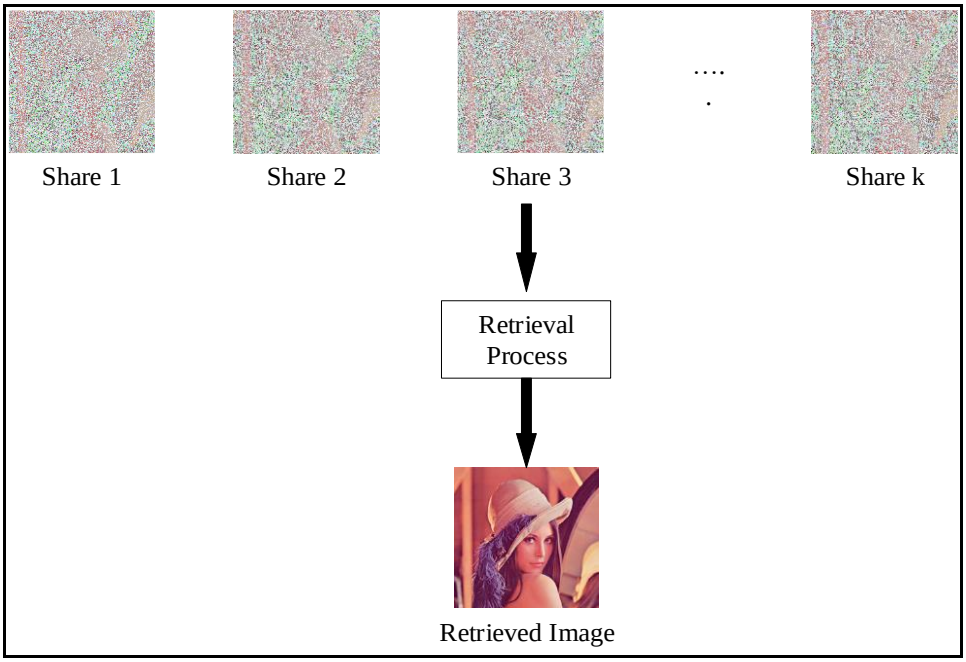
Gambar 3.2. Flowchart implementasi skema image sharing dan enkripsi

Seperti yang telah di gambarkan pada flowchart, input yang digunakan pada skema ini adalah *host image I* serta gambar *watermark* W. Sedangkan output pada skema ini adalah gambar yang sudah disamarkan sebanyak n *shares,* serta gambar terenkripsi IW yang mana telah ditanam dengan gambar *watermak* W menggunakan metode *Singular Value Decomposition* kemudian dienkripsi menggunakan *Fourier Transform*.

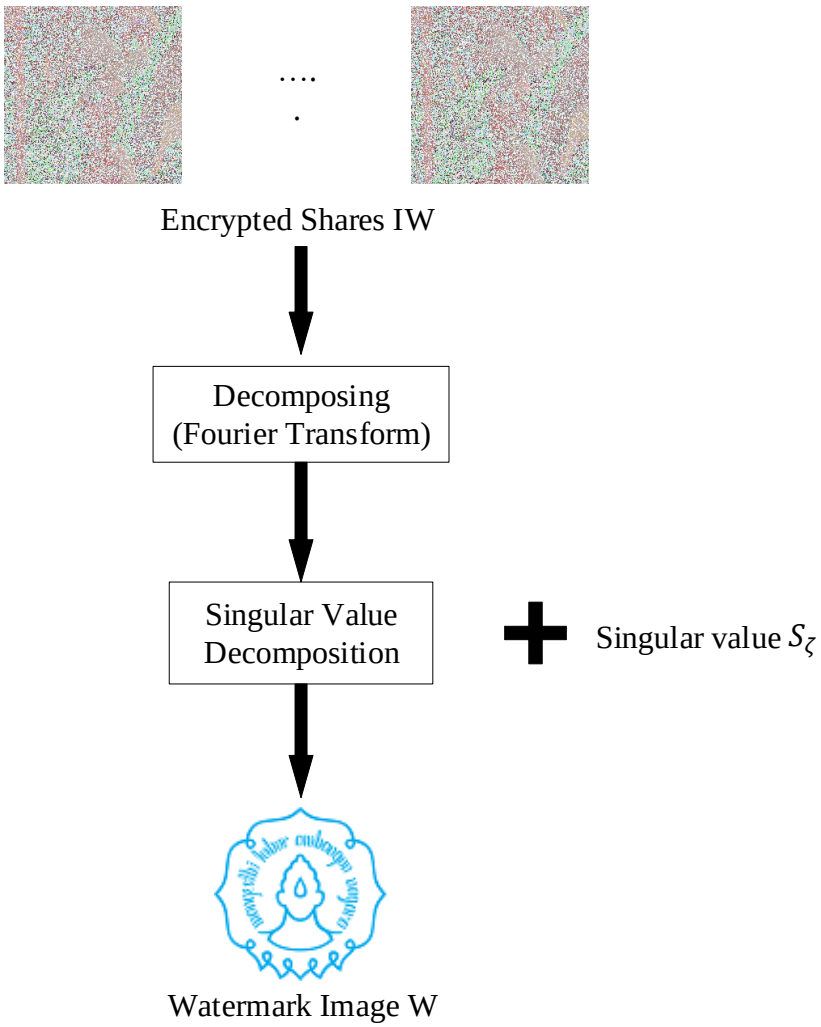
Dalam flowchart diatas, *host image* diamankan dengan cara disamarkan setiap pixelnya menggunakan skema *image sharing* terlebih dahulu. Skema *image sharing* yang diimplementasikan menjadi program ada 2 yakni *Shamir Secret Shring* serta *Chinese Remainder Theorem*. *Host image* yang telah dikenakan skema *image sharing* akan terpecah-pecah menjadi gambar-gambar samar sebanyak n *shares*. Setiap informasi gambar *shares* atau dengan kata lain setiap *value pixel* pada gambar *shares* satu dengan gambar *shares* yang lain tidak dapat memberikan informasi *value pixel* yang terdapat pada *host image*. *Value pixel* yang terdapat pada host image dapat diketahui jika menggabungkan gambar shares sebanyak *threshold* k. Banyak *threshold* k terdapat pada rentang $1 < k \leq n$.

Setelah *host image* terpecah pecah menjadi gambar-gambar *share*, gambar-gambar tersebut dipilih berdasarkan *secret key* Z untuk ditanamkan gambar *watermark* W . Gambar *watermark* W ditanamkan ke dalam gambar-gambar *share* tersebut menggunakan metode *Singular Value Decomposition*. Dari metode *Singular Value Decomosition* tersebut, diperoleh *singular value* S_ζ . *Singular value* S_ζ diperoleh dari mengoperasikan *Singular Value Decomposition* kepada *host image*. *Singular value* S_ζ nantinya akan digunakan untuk mengekstrak gambar yang sudah diwatermark dan dienkripsi IW. Setelah gambar-gambar *share* telah ditanam dengan gambar *watermark* W, selanjutnya gambar-gambar tersebut dienkripsi menggunakan metode *Fourier Transform*.

Untuk mendapatkan kembali *host image* dan gambar *watermark* W, pada skema ini dapat dilakukan secara terpisah. Berikut adalah flowchart untuk mendapatkan host image dan watermark image:



Gambar 3.3. Flowchart mendapatkan kembali Host image



Gambar 3.4. Flowchart Mendapatkan kembali gambar Watermark

Untuk mendapatkan kembali host image maupun watermark image, diperlukan input berupa gambar-gambar samar yang telah dihasilkan dari skema *Shamir Secret Sharing* maupun skema *Chinese Remainder Theorem*. Output dari flowchart diatas adalah *host image* ataupun gambar *watermark* W.

Untuk mendapatkan host image atau gambar yang asli, pada skema *Shamir Secret Sharing* diperlukan metode *Lagrange Interpolation*. Sedangkan input yang digunakan oleh metode *Lagrange Interpolation* adalah gambar share sebanyak *threshold* k. Karena jika gambar share yang digunakan kurang dari *threshold* k, maka metode *Lagrange Interpolation*

tidak dapat membentuk fungsi untuk mendapatkan value pixel dari host image.

Sedangkan pada skema *Chinese Remainder Theorem*, tidak diperlukan metode tambahan seperti yang digunakan pada skema *Shamir Secret Sharing*. Cukup menggunakan metode *Chinese Remainder Theorem*, *host image* yang telah terpecah-pecah menjadi *shares* dapat diperoleh kembali.

Untuk menekstrak *watermark* W dari *encrypted shares*, pertama kali yang diperlukan adalah memasukkan *secret key* Z. Hal ini diperlukan untuk mendapatkan *encrypted shares* yang terdapat pada *cloud server*. Setelah mendapat gambar *encrypted shares* yang terwatermark, dilakukan dekomposisi pada gambar tersebut menggunakan *Fourier Transform*. Setelah gambar tersebut terdekomposisi, selanjutnya diberikan metode *Singular Value Decomposition* serta dengan menambahkan *singular value* S_ζ untuk mengekstrak *watermark* W.

3.4. Pengujian

Pada tahap pengujian, pengujian dilakukan untuk menguji apakah skema yang digunakan dalam penelitian dapat menimbulkan permasalahan *false positive detection*. Pada tahap pengujian ini, gambar yang akan diuji adalah *shares* dan *encrypted shares*.

Alat pengujian yang digunakan kepada *shares* adalah Gaussian noise, Salt and pepper noise, Speckle noise, Histogram equalization, JPEG compression, rotation, cut, Median filtering, Gaussian filtering, dan Resizing. Lalu alat pengujian yang digunakan kepada *encrypted shares* adalah menggunakan alat pengujian tipe pertama, seperti yang terdapat pada artikel makalah (Guo & Prasetyo, 2014b). Alat pengujian tipe pertama pada artikel makalah tersebut adalah ketika *end user* memiliki sebuah *host image* I serta 2 buah *watermark* W_1 dan W_2. Setelah *host image* di tanamkan *watermark* menggunakan SVD maka akan menghasilkan *encrypted shares*

IW_1 dan IW_2 serta *singular value* $S_{\zeta 1}$ dan $S_{\zeta 2}$. Lalu kedua *singular value* tersebut ditukar dan digunakan untuk membuka *encrypted shares*, sehingga IW_1 dibuka dengan $S_{\zeta 2}$, begitu juga sebaliknya. Lalu alat pengujian lainnya adalah dengan menguji *false positive detection*. Untuk menguji *false positive detection* adalah dengan cara, misalkan *attacker* sudah mendapatkan *encrypted shares IW* serta memiliki watermark W_a. Lalu attacker mengekstrak *encrypted shares IW* menggunakan *singular value* dari watermark W_a. Jika terdapat *false positive detection*, maka *watermark* yang terekstrak adalah *watermark* W_a.

3.5. Penarikan Kesimpulan

Pada tahap penarikan kesimpulan ini, hasil yang diperoleh dari tahap pengujian dianalisis untuk ditarik kesimpulannya. Biasanya hasil dari penelitian menyelesaikan permasalahan yang terdapat pada rumusan masalah. Jika hasil dari penelitian tidak dapat menyelesaikan permasalahan, maka dituliskan penyebab kenapa penelitian tidak dapat menyelesaikan permasalahan.

JADWAL PELAKSANAAN

No	Kegiatan	Bulan																			
		Februari				Maret				April				Mei				Juni			
		Minggu ke-																			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur																				
2	Analisis dan Perencanaan																				
3	Implementasi																				
4	Pengujian																				
5	Penarikan Kesimpulan																				

DAFTAR PUSTAKA

Abdallah, H. A., Ghazy, R. A., Kasban, H., Faragallah, O. S., Shaalan, A. A., Hadhoud, M. M., … Abd El-Samie, F. E. (2014). Homomorphic image watermarking with a singular value decomposition algorithm. *Information Processing and Management*. https://doi.org/10.1016/j.ipm.2014.07.001

Guo, J. M., & Prasetyo, H. (2014a). False-positive-free SVD-based image watermarking. *Journal of Visual Communication and Image Representation*, *25*(5), 1149–1163. https://doi.org/10.1016/j.jvcir.2014.03.012

Guo, J. M., & Prasetyo, H. (2014b). Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU - International Journal of Electronics and Communications*, *68*(9), 816–834. https://doi.org/10.1016/j.aeue.2014.03.008

Loukhaoukha, K., Refaey, A., & Zebbiche, K. (2016). Comments on "Homomorphic image watermarking with a singular value decomposition algorithm." *Information Processing and Management*, *52*(4), 644–645. https://doi.org/10.1016/j.ipm.2015.12.009

Singh, P., Raman, B., & Misra, M. (2017). A secure image sharing scheme based on SVD and Fractional Fourier Transform. *Signal Processing: Image Communication*, *57*(December 2016), 46–59. https://doi.org/10.1016/j.image.2017.04.012

Yan, X., Lu, Y., Liu, L., Wan, S., Ding, W., & Liu, H. (2017). Chinese remainder theorem-based secret image sharing for (k, n) threshold. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-319-68542-7_36

Weisstein, Eric W. "Singular Value Decomposition." From MathWorld--A Wolfram Web Resource. http://mathworld.wolfram.com/SingularValueDecomposition. html. 8 Februari 2018.

Weisstein, Eric W. "Discrete Fourier Transform." From MathWorld--A Wolfram Web Resource. http://mathworld.wolfram.com/DiscreteFourierTransform.html. 8 Februari 2018.

Fisher et al., (2003). Fourier Transform. https://homepages.inf.ed.ac.uk/rbf/HIPR2/fourier.htm. 8 Februari 2018.

Weisstein, Eric W. "Chinese Remainder Theorem." From MathWorld--A Wolfram Web Resource. http://mathworld.wolfram.com/ChineseRemainderTheorem.html. 8 Februari 2018.