PROPOSAL SKRIPSI S1

Skema Image Sharing Menggunakan Shamir Secret Sharing dengan Berdasarkan Metode Single Value Decomposition dan Fourier Transform

Disusun Oleh :

Zainul Insaan Abdul Hafiidhl

M0514056

PROGRAM STUDI INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS SEBELAS MARET

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

Keamanan data di cloud server merupakan salah satu topik yang masih dibicarakan dan dikembangkan. Hal ini dikarenakan peretasan data pada cloud server masih ditemukan. Selain itu, peningkatan security 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 (Singh, Raman, & Misra, 2017), dalam 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 (Loukhaoukha, Refaey, & Zebbiche, 2016) menyebutkan bahwa algoritma watermarking (Liu & Tan, 2002) yang menggunakan metode SVD secara fundamental cacat dikarenakan matriks vektor singular U_W dan V_W dari watermark W yang mana merepresentasikan

informasi penting dapat menyebabkan *false positive detection* meskipun watermark yang ditanam berbeda atau bahkan tidak ada. Dalam paper (Guo & Prasetyo, 2014) 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*. Serta dalam paper tersebut ditemukan kelemahan lain, yakni kemampuan skema tersebut untuk memperoleh kembali gambar pada *shares* yang telah ditanam oleh watermark. Dari gagasan tersebut diangkatlah penelitian ini, untuk menguji apakah terjadi *false positive detection* serta untuk menguji apakah *shares* yang telah ditanam oleh watermark dapat diperoleh kembali.

1.2. Rumusan Masalah

Rumusan masalah dari penelitian ini adalah apakah skema *secure image sharing* berdasarkan metode SVD dan FrFT 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. Sebagai pengganti metode Fractional Fourier Transform, metode yang digunakan adalah Fourier Transform biasa.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah melakukan pengujian pada skema yang digunakan pada paper (Singh et al., 2017) yakni skema *secure image sharing* berdasarkan metode SVD dan FrFT bebas dari permasalahan *false positive detection*.

1.5. Manfaat Penelitian

Manfaat dari melakukan penelitian ini adalah mengetahui apakah skema *image sharing* yang berdasarkan metode *Singular Value Decomposition* dan *Fourier Transform* 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.

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.

BAB III METODOLOGI PENELITIAN

Pada Bab III menguraikan tentang metodologi yang akan digunakan dalam penelitian. Metodologi penelitian yang digunakan adalah Studi literature, Analisis dan Perencanaan, Implementasi, Pengujian, serta penarikan kesimpulan.

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.

BAB V PENUTUP

Pada Bab V menguraikan tentang kesimpulan yang dicapai dari penelitian serta menguraikan saran untuk penelitian kedepannya.

BAB II
TINJAUAN PUSTAKA

2.1. Dasar Teori

2.1.1. Shamir Secret Sharing

Shamir Secret Sharing 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, sedemikian rupa sehingga (k ≤ n). Bagian-bagian yang digabung tersebut tidak dapat membentuk *secret* jika jumlah bagian kurang dari threshold (≤ k-1). Berikut adalah function *Shamir Secret Sharing* 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 thresholdnya.

2.1.2. 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.

2.1.3. 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:

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

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, double-sum harus dihitung untuk setiap titik pada gambar. 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 image yang di simpan pada arsitektur cloud server tidak rentan terhadap peretasan. Pada penelitian tersebut, agar menjaga image yang disimpan dan verifikasi kepemilikan multimedia menggunakan basis *singular value decomposition* (SVD) serta *Fractional Fourier Transform* (FrFT). Tahapan dalam mengamankan umage yang disimpan di arsitektur cloud server dan verifikasi kepemilikan image tersebut dalam penelitian ini adalah sebagai berikut:

   1. Image yang akan disimpan ke dalam arsitektur cloud server, informasi dari image akan dikaburkan dan dibagi-bagi menjadi beberapa bagian yang mana setiap bagian tidak dapat memeberi tahu informasi tentang image menggunakan skema *Shamir Secret Sharing*. Dan bagian-bagian tersebut disebarkan ke beberapa server yang terdapat di arsitektur
   2. Image yang telah dienkripsi dan disimpan ke beberapa server, kepemilikannya ditegaskan dengan menanam informasi spesifik dari pemilik ke beberapa bagian berdasarkan *secret key* tertentu dengan menggunakan metode *Singular Value Decomposition* dan *Fractional Fourier Transform*.
   3. Informasi spesifik dari pemilik tersebut dapat diekstrak langsung dari arsitektur cloud server maupun setelah image 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*. Dalam penelitian tersebut disebutkan bahwa kelemahan utama dari metode *Singular Value Decomposition* untuk watermarking gambar adalah *false positive problem*. Untuk mengatasi permasalahan tersebut, dalam penelitian tersebut diajukan metode watermarking gambar berdasarkan metode *Singular Value Decomposition* 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 diwatermark, 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 *false positive problem*, memperoleh payload yang tinggi, serta memiliki performa yang melebihi dari metode watermarking *Singular Value Decomposition* terpercaya 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 paper ini, membahas tentang kesalahan pada paper (Abdallah et al., 2014). Dalam paper tersebut mengometari bahwa skema watermarking pada paper (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*.

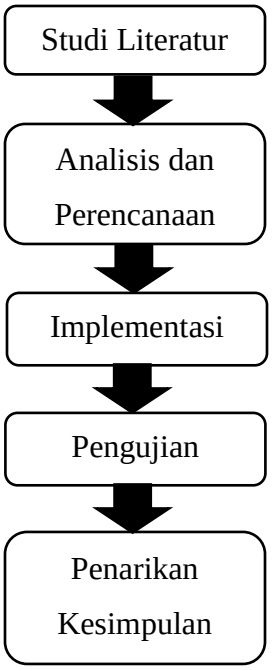
Tabel 2.1.Tabel Penelitian Terkait

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.”		

BAB III
METODOLOGI PENELITIAN

Metodologi yang digunakan dalam penelitian adalah sebagai berikut:



Gambar 3.1.Metodologi penelitian

3.1. Studi Literatur

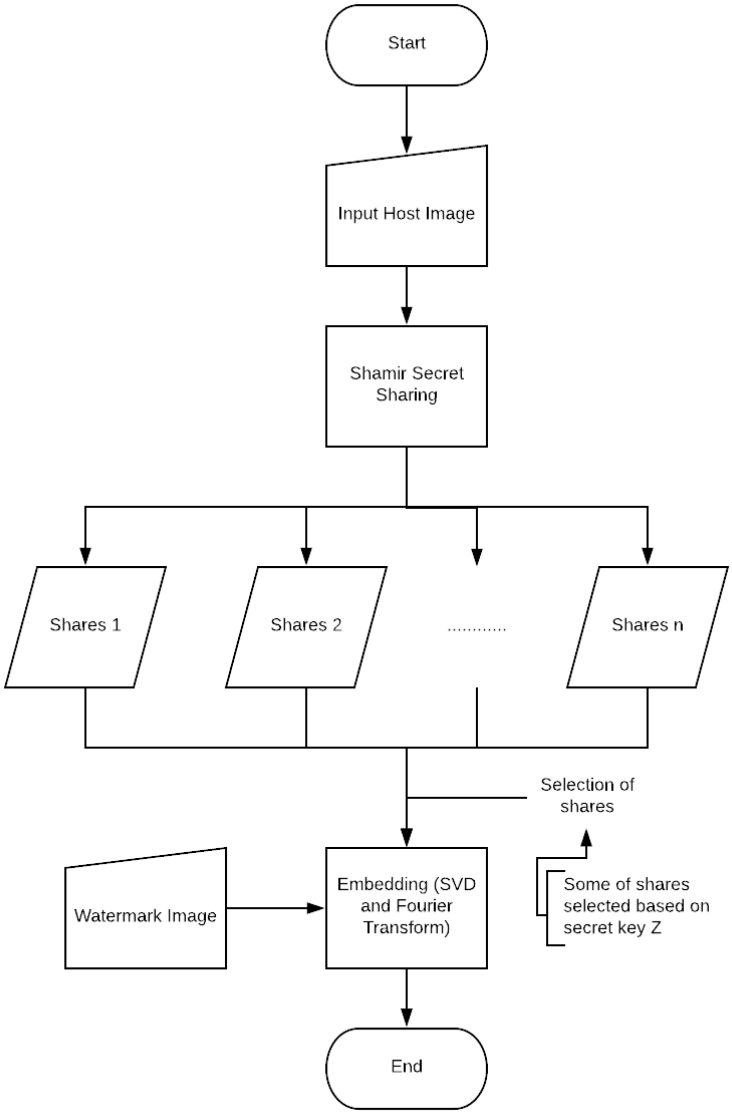
Pada tahap studi literatur, Algoritma serta metode-metode yang diperlukan dalam penelitian dikaji dan dipelajari dengan seksama. Sumber dari algoritma ataupun metode-metode yang diperlukan dapat berasal dari jurnal yang telah diterbitkan sebelumnya, maupun buku-buku yang memiliki teori dasar yang terkait dengan penelitian.

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.

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:



Gambar 3.2. Flowchart implementasi skema image sharing dan enkripsi

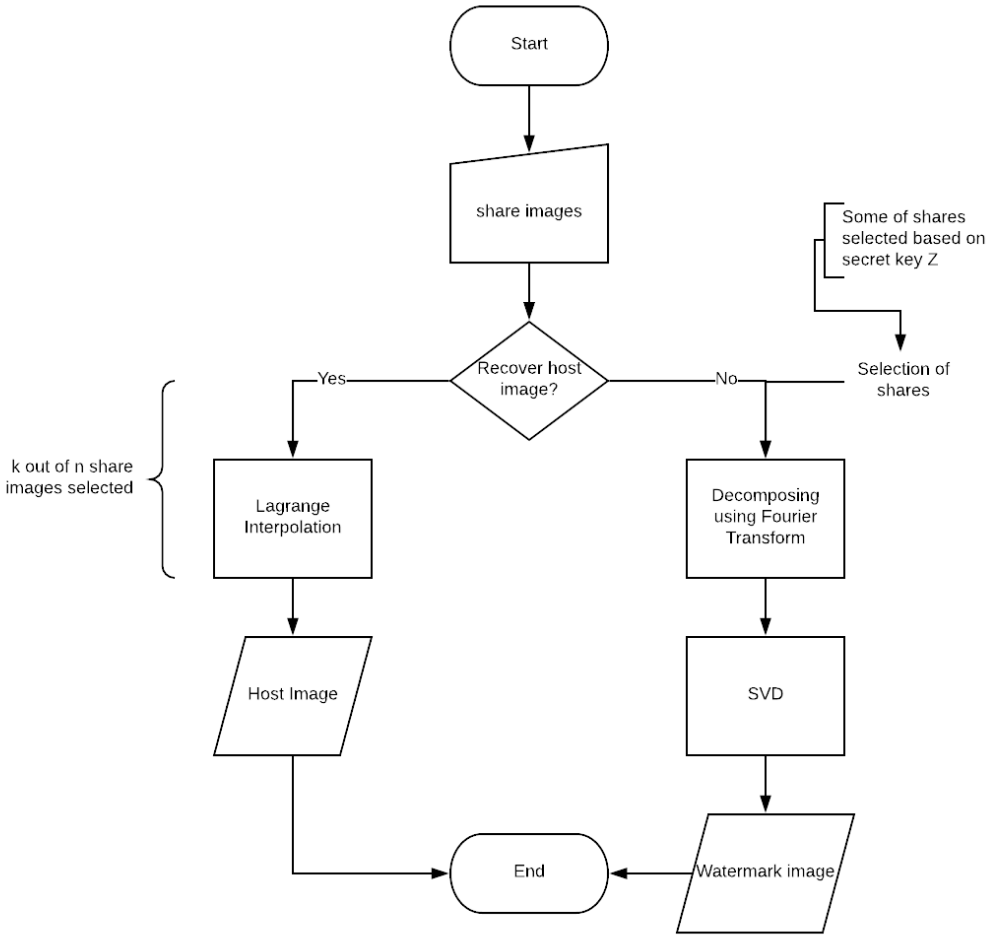
Input yang digunakan pada skema ini adalah host image atau gambar yang akan di amankan dan di watermark. Sedangkan output pada skema ini adalah gambar yang sudah disamarkan menggunakan Shamir Secret Sharing sebanyak n shares, dan gambar yang terenkripsi oleh Fourier Transform lalu di

tanam watermark menggunakan SVD yang mana dipilih dari gambar yang sudah disamarkan berdasarkan secret key Z.

Dalam flowchart diatas, host image diamankan dengan cara disamar setiap pixelnya menggunakan skema Shamir Secret Sharing terlebih dahulu. Host image yang telah dikenakan skema Shamir Secret Sharing akan terpecah-pecah menjadi gambar-gambar samar sebanyak n shares. Setiap informasi gambar shares atau dengan kata lain 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 watermark. Sebelum ditanamkan watermark, gambar-gambar share yang terpilih didekomposisi menggunakan fourier transform terlebih dahulu. Setelah terdekomposisi, watermark ditanamkan ke dalam gambar-gambar share tersebut menggunakan metode Singular Value Decomposition.

Untuk mendapatkan kembali host image dan watermark image, 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 dan watermark image

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

Untuk mendapatkan host image atau gambar yang asli, 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 function untuk mendapatkan value pixel dari host image.

Untuk mendapatkan watermark image, pertama kali yang diperlukan adalah memasukkan secret key Z. Hal ini diperlukan untuk mendapatkan share yang diberikan watermark. Setelah mendapat gambar share yang terwatermark, dilakukan dekomposisi pada gambar tersebut menggunakan fourier transform. Setelah gambar tersebut terdekomposisi, selanjutnya diberikan metode Singular Value Decomposition untuk mengekstrak watermark image.

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, selain menguji menggunakan gambar watermark yang digunakan, juga menggunakan gambar yang berbeda.

3.5. Penarikan Kesimpulan

Pada tahap penarikan kesimpulan ini, hasil yang didapat dari pengujian serta output dari skema yang digunakan ditarik kesimpulannya. Dari

JADWAL PELAKSANAAN

No	Kegiatan	Bulan											
		April				Mei				Juni			
		Munggu ke-											
		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. (2014). 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

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

Weisstein, Eric W. "Singular Value Decomposition." From MathWorld--A Wolfram Web Resource. http://mathworld.wolfram.com/SingularValueDecomposition.html. 1 Mei 2018.

Weisstein, Eric W. "Discrete Fourier Transform." From MathWorld--A Wolfram Web Resource. http://mathworld.wolfram.com/DiscreteFourierTransform.html. 1 Mei 2018.

Fisher et al., (2003). Fourier Transform. https://homepages.inf.ed.ac.uk/rbf/HIPR2/fourier.htm. 1 Mei 2018.