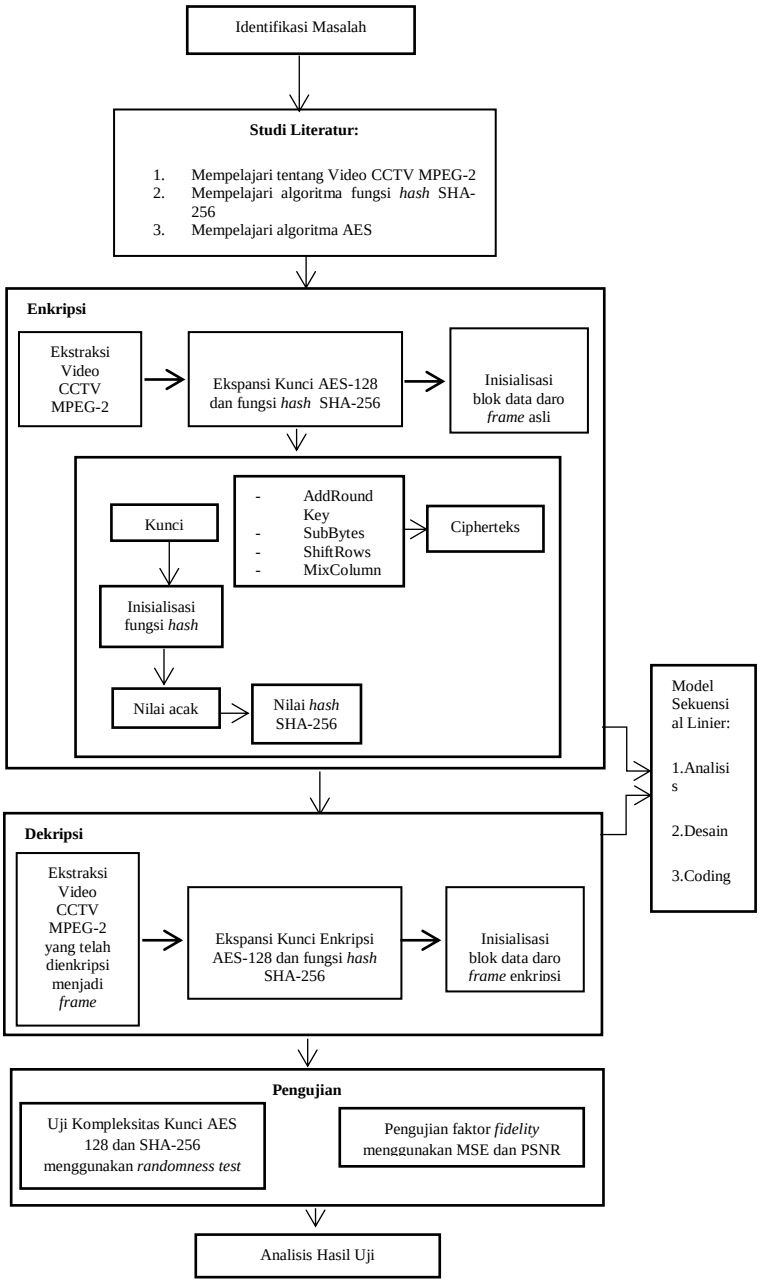
BAB III
METODOLOGI PENELITIAN

3.1 Desain Penelitian

Desain penelitian adalah tahapan atau gambaran yang akan dilakukan dalam penelitian. Desain penelitian ini dibuat sebagai panduan untuk memberikan gambar serta kemudahan dalam melakukan penelitian. Penelitian ini dilakukan melalui beberapa tahapan, diantaranya ada identifikasi masalah, studi literatur, tahap penelitian yang terdapat dua proses utama di dalamnya yaitu proses enkripsi dan proses dekripsi. Di dalam proses enkripsi memiliki proses-proses lagi yaitu proses ekstraksi video menjadi sekumpulan frame, setelah itu proses ekspansi kunci AES 128 *bits* dan fungsi *hash* SHA-256 dan proses selanjutnya yaitu implementasi AES 128 *bits* dalam video MPEG-2 dengan melakukan inisialisasi blok data dari *frame* asli. Proses dekripsi umumnya serupa dengan proses enkripsi, pada proses pertama melakukan ekstraksi video yang telah dienkripsi menjadi frame, lalu proses ekspansi kunci AES 128 *bits* dan fungsi *hash* SHA-256. Jika kunci yang dimasukan sama dengan pada saat enkripsi maka hasil dari proses dekripsi melakukan pengembalian terhadap video yang telah dienkripsi menjadi video aslinya. Setelah melakukan implementasi maka ada pengujian terhadap kompleksitas kunci yang telah dibuat dan pengujian hasil dari *frame* yang telah dienkripsi dan didekripsi, tahapan selanjutnya yaitu pengembangan perangkat lunak menggunakan metode sekuensial linier dan dilakukannya analisis hasil uji menggunakan histogram.

Sebelum memulai penelitian penulis memulai tahapan dengan menemukan masalah dan mengikuti isu-isu pada masalah tersebut yang mana dalam penelitian ini yaitu meningkatkan keamanan video CCTV agar tidak dapat dimanipulasi. Data yang digunakan pada penelitian ini berupa video CCTV dalam format MPEG-2. Tahapan penelitian yang akan dilakukan pada penelitian ini ditampilkan pada Gambar 3.1.



Gambar 3.1 Desain Penelitian

Tahapan penelitian yang dilakukan meliputi langkah-langkah berikut:

1. Identifikasi Masalah

   Tahapan awal dalam penelitian yang membantu jalannya penelitian. Pada tahap ini dilakukan identifikasi masalah dari penelitian yang sudah pernah dilakukan sebelumnya terhadap keamanan pada kriptografi video, cara enkripsi dan dekripsi dengan algoritma-algoritma kriptografi yang lain. Dilakukannya agar mendapatkan gabungan algoritma yang dapat membuat data pada video CCTV MPEG-2 aman.

2. Studi Literatur

   Tahapan studi pendahuluan terhadap penelitian sebelumnya yang terkait dengan penelitian yang akan dilakukan. Pada tahapan ini juga mempelajari metode-metode yang akan digunakan pada penelitian yaitu dengan mempelajari video dan *frame* video, MPEG-2, kriptografi, mempelajari algoritma fungsi *hash* SHA-256 dan algoritma AES baik melalui buku literatur atau jurnal ilmiah.

3. Melakukan penelitian untuk proses implementasi algoritma AES dan SHA-256 dalam enkripsi dan dekripsi pada video CCTV MPEG-2 dengan memanfaatkan ilmu kriptogtafi.

   a. Penelitian yang pertama dilakukan penelitian untuk proses enkripsi yaitu proses yang pertama adalah proses ekstraksi video CCTV MPEG-2 menjadi sekumpulan *frame* setelah itu pembangkitan kunci pada AES 128 dengan memanfaatkan fungsi *hash* SHA-256 dalam meningkatkan kompleksitas pada kunci AES 128 *bits*, dimana plainteks dalam penelitian ini yaitu berupa sekumpulan *frame* yang nantinya dikonversikan terlebih dahulu menjadi bit dan setelah itu meng-*input*-kan kunci yang akan diproses melalui empat tahap yaitu, AddRoundKey, SubBytes, ShiftRows dan MixColumns. Lalu SHA-256 akan memulai inisialisasi fungsi *hash* nya dan menghasilkan nilai acak yang akan menjadi nilai *hash* SHA-256 dan menjadi kunci yang lebih kompleks.
   b. Penelitian kedua dilakukan penelitian untuk proses dekripsi dan proses pertama pada dekripsi adalah proses ekstraksi video yang telah dienkripsi menjadi sekumpulan frame. Tahap pada proses dekripsi sama dengan proses enkripsi, jika kunci yang dimasukan sama dengan kunci yang dimasukan saat enkripsi maka video yang telah dienkripsi akan kembali menjadi video asli. implementasi AES pada video CCTV MPEG-2 yang mana video akan dikonversikan menjadi sekumpulan *frame* dan setelah itu algoritma AES diimplementasikan dan menghasilkan cipherteks berupa *frame* yang sudah diacak.

4. Tahapan ini merupakan tahapan pengujian yaitu pengujian kompleksitas kunci AES 128 *bits* yang telah dihash-kan dengan SHA-256 menggunakan *randomness* test. Setelah itu Hasil dari sekumpulan *frame* yang sudah diimplementasikan menggunakan algoritma AES akan diuji menggunakan uji faktor *fidelity* yaitu MSE dan PSNR.

5. Tahapan pengembangan perangkat lunak yaitu pembuatan perangkat lunak penelitian ini. Pengembangan perangkat lunak dilakukan sesuai model pengembangan perangkat lunak *waterfall*. Tahap pertama yang dilakukan yaitu analisis, pada tahap ini dilakukan analisis mengenai bagaimana perangkat lunak akan dibuat. Setelah itu masuk tahap desain *interface* yaitu merancang antarmuka pada aplikasi yang dibuat. Tahap selanjutnya yaitu tahap implementasi, tahap pembuatan perangkat lunak atau biasa disebut dengan tahap *coding* dan setelah itu dilakukan tahap *testing* atau pengujian perangkat lunak.

6. Tahapan ini merupakan tahapan terakhir dalam penelitian yang dilakukan yaitu tahap analisis hasil uji, pada tahapan ini menggunakan histogram untuk melihat perbandingan *frame* asli, *frame* yang telah dienkripsi dan *frame* yang telah didekripsi.

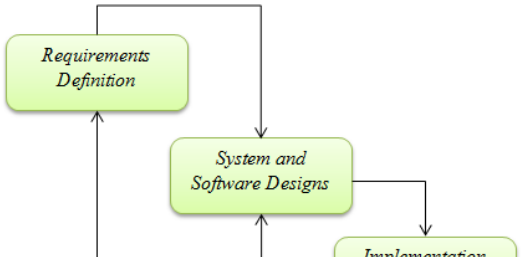
3.2 Metode Penelitian

Metode penelitian ini dibagi menjadi dua, yaitu metode pengumpulan data penelitian dan metode pengembangan perangkat lunak.

3.2.1 Metode Pengumpulan Data

Dalam penelitian kali ini data berupa bahan studi literatur berupa *textbook*, jurnal penelitian, tutorial beserta dokumen lainnya yang menunjang proses penelitian. Pada proses ini melakukan pengumpulan studi literatur yang berkaitan dengan penelitian ini seperti video dan sebagian *frame* video, kriptografi, keamanan informasi, algoritma fungsi *hash* SHA-256 dan algoritma AES. Dan dokumentasi lain yang bisa didapat melalui *World Wide Web* dan melalui observasi dari perpustakaan juga.

3.2.2 Metode Pengembangan Perangkat Lunak



Gambar 3.2 Model *Waterfall* (Sommerville, 2011)

Metode pengembangan perangkat lunak yang dilakukan pada penelitian ini dengan menggunakan model pengembangan perangkat lunak *waterfall.* Seperti yang telah dijelaskan sebelumnya, pada penelitian ini tidak akan menggunakan model pengembangan perangkat lunak *waterfall* secara keseluruhan. Pada penelitian ini tidak dilakukan dan dimasukkan tahap *operation and maintenance*. Berikut pengertian dari tahap-tahap pada model *waterfall* pada Gambar 3.2 menurut Ian Sommerville (2011):

1. *Requirements Definition*
   Tahapan awal dengan melakukan analisis untuk menentukan kebutuhan, batasan, serta tujuan dari pengembangan perangkat lunak sesuai yang diinginkan. Hal tersebut didefinisikan secara rinci sehingga menjadi spesifikasi sistem. Pada tahap ini dilakukan penentuan algoritma dan metode untuk meningkatkan keamanan pada sebagian *frame* video dari data cctv.
2. *Software Design*
   Tahap perancangan yang melibatkan identifikasi dan menggambarkan dasar sistem serta hubungan satu sama lain. Pada tahap ini dibuat desain implementasi algoritma dan metode yang akan dikembangkan.
3. *Implementation and Unit Testing*
   Pada tahap ini *software design* yang telah dilakukan sebelumnya kemudian diimplementasikan dalam bentuk unit program. Setelah unit program dibuat, kemudian dilakukan *testing* pada unit program tersebut untuk memastikan implementasi berjalan dengan baik.
4. *Integration and Testing*
   Tahap ini merupakan tajap lanjutan, ketika semua unit program berhasil diimplementasikan dan lolos *testing* yaitu dengan mengintegrasikan setiap unit untuk membentuk aplikasi yang diinginkan. Aplikasi yang sudah dibentuk kemudian di tes kembali untuk memastikan unit program dapat berjalan satu sama lain dalam aplikasi dan aplikasi yang dibuat sudah memenuhi kebutuhan.
5. *Operation and Maintenance* (Pemeliharaan)
   Dalam tahapan ini, perangkat lunak mulai digunakan. Selain itu juga memperbaiki *error* yang tidak ditemukan pada tahap pembuatan. Dalam tahap ini juga dilakukan pengembangan perangkat lunak seperti penambahan fitur dan fungsi baru.

3.3 Instrumen Penelitian

Berdasarkan kebutuhan-kebutuhan yang tela dijelaskan di atas pada *requirements definition*, maka dapat ditentukan alat dan bahan yang digunakan pada penelitian ini adalah sebagai berikut:

3.3.1 Alat Penelitian

Pada penelitian ini penulis menggunakan alat bantuk penunjang baik berupa perangkat keras *(hardware)* maupun perangkat lunak *(software)*. Adapun perangkat keras yang digunakan adalah seperangkat komputer yang memiliki spesifikasi sebagai berikut:

1. *Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz*
2. RAM 4GB
3. *Hard disk* 365GB

Kemudian perangkat lunak yang digunakan pada penelitian ini adalah sebagai berikut:

1. Sistem Operasi *Windows 10 64bit*
2. Matlab R2016a

3. Cryptool 1.4.4
4. Google Chrome *Version 57.0.2987.133*

3.3.2 Bahan Penelitian

Bahan penelitian yang digunakan adalah jurnal penelitian yang sudah dilakukan, *textbook*, *tutorial*, dan dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web* tentang video dan sebagian *frame* video, kriptografi, algoritma fungsi *hash* SHA-256 dan algoritma AES.