BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini pertukaran informasi semakin mudah dan cepat dilakukan dan tidak dibatasi media informasinya. Hal tersebut mengakibatkan lalu lintas informasi-informasi tersebut sangat besar sehingga sulit dipantau keamanannya. Data dari perusahaan keamanan siber Surfshark dalam Katadata Insight Center (2022) menjelaskan bahwa Indonesia menempati urutan ke-3 dengan jumlah kasus kebocoran data terbanyak di dunia setelah Rusia dan Prancis per kuartal III-2022. Oleh karena itu, informasi rahasia yang akan dibagikan harus dilindungi untuk menghindari kebocoran informasi dan ancaman keamanan informasi lainnya. Belakangan ini, banyak digunakan metode kriptografi dan steganografi dalam menjaga informasi rahasia dari ancaman keamanan informasi.

Kriptografi menyediakan layanan keamanan informasi berupa kerahasiaan (*privacy*), integritas data (*data integrity*), autentikasi (*authentication*), dan anti-penyangkalan (*non-repudiation*) (Schneier dalam Munir, 2019, hlm. 15). Kriptografi berfokus pada penyandian informasi rahasia sehingga makna informasi rahasia tersebut tidak dapat dipahami lagi (Meyer dalam Munir, 2019, hlm. 4). Di samping lengkapnya layanan keamanan yang ditawarkan kriptografi, dalam kasus tertentu kriptografi belum cukup untuk mengamankan informasi rahasia. Hasil penyandian informasi rahasia yang maknanya tidak dipahami tersebut menimbulkan kecurigaan. Untuk menghindari kecurigaan tersebut, dibutuhkan tambahan metode lain yaitu steganografi.

Berbeda dengan kriptografi, fokus steganografi adalah pada penyembunyian keberadaan informasi rahasia sehingga pihak lain, yaitu pihak yang tidak diharapkan terlibat tidak menyadari keberadaan informasi rahasia tersebut. Steganografi dapat menutup kekurangan dari kriptografi, yaitu dengan menyembunyikan informasi rahasia yang telah disandikan. Dengan demikian, kecurigaan pada hasil penyandian dapat terhindarkan. Oleh karena itu, penggabungan kriptografi dan steganografi dapat mengurangi tingkat ancaman pada keamanan informasi rahasia.

Miftah Fadillah Sopian, 2024
IMPLEMENTASI KRIPTOGRAFI SECRET SHARING SCHEME DAN STEGANOGRAFI AUDIO LEAST SIGNIFICANT BIT MENGGUNAKAN PSEUDORANDOM HITZL-ZELE
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

Metode kriptografi pada umumnya membutuhkan sebuah kunci untuk mendekripsi informasi yang terenkripsi. Umumnya kunci tunggal tersebut disimpan pada sebuah tempat yang dirasa aman, misalnya pada sebuah komputer, ingatan manusia, atau tempat lain. Akan tetapi, jika kunci tunggal atau tempat penyimpanan tersebut hilang, terhapus, rusak, atau terlupakan, maka informasi asli tidak dapat diakses, bahkan oleh pemiliknya. Di sisi lain, jika kunci tunggal tersebut disimpan pada banyak tempat, maka akan meningkatkan ancaman keamanan data, misalnya penyerangan siber, pengkhianatan, dan kelalaian manusia. Masalah tersebut dapat diatasi dengan skema pembagian rahasia (*secret sharing scheme*) yang dikemukakan oleh Shamir (1979). Skema tersebut memungkinkan pemilik informasi untuk membagikan informasi rahasia menjadi beberapa bagian yang diberikan kepada sejumlah pemegang kunci. Ketika sejumlah pemegang kunci bekerja sama, informasi asli dapat diperoleh kembali. Hal tersebut memberikan tingkat keamanan tambahan, karena tidak ada pemegang kunci tunggal yang dapat mengakses informasi asli. Skema pembagian rahasia atau skema (t, w) membutuhkan seorang *dealer* yang memiliki informasi rahasia (*secret*) dan membaginya sebanyak *w* bagian (*share*), *w participant* yang masing-masing diberikan *share*, dan *t* sebagai minimum banyaknya *participant* untuk mengonstruksi *secret*.

Hasil dari skema pembagian rahasia adalah *w* banyaknya *share* yang maknanya tidak dipahami. *Share* tersebut berpotensi menimbulkan kecurigaan dari pihak lain. Dengan demikian, diperlukan metode steganografi untuk menyematkan *share* ke dalam media tertentu supaya *share* tersembunyi. Media yang dapat digunakan sebagai penutup (*cover*) dari *share* yang akan disembunyikan umumnya adalah teks, gambar, audio, dan video. Media *cover* yang akan digunakan dalam penelitian ini adalah *file* audio dengan ekstensi *waveform audio format* (*wav*). Ekstensi *wav* dipilih karena ekstensi tersebut tidak mengalami kompresi saat didigitalkan, sehingga memiliki tingkat presisi yang tinggi (*high fidelity*). Selain itu, walaupun tidak sepopuler *mp3*, ekstensi *wav* cukup umum digunakan sehingga mudah didapatkan.

Least Significant Bit (LSB) adalah metode steganografi yang memanfaatkan bit dengan nilai yang tidak berarti sebagai media penampung (*cover*) informasi rahasia. Umumnya, bit yang digunakan sebagai *cover* adalah bit terakhir dalam kumpulan 8-bit (1-byte). Penyematan bit dapat dilakukan pada byte pertama hingga byte terakhir secara berurutan. Pemilihan byte juga dapat diperoleh menggunakan *chaotic map-based pseudorandom*, contohnya *Ikeda, Hitzl-Zele, Henon, Tinkerbell, Logistic, Zig-zag*, dan lain sebagainya. Penggunaan *chaotic map* pada metode steganografi dapat meningkatkan pencegahan dari ancaman terhadap keamanan informasi (Kordov dan Stoyanov, 2017). Pada penelitian ini digunakan *LSB* dengan *pseudorandom Hitzl-Zele*, yaitu penyematan bit dengan pemilihan byte berdasarkan byte acak yang dibagun oleh *pseudorandom Hitzl-Zele*.

Penelitian sebelumnya terkait *LSB* dengan *pseudorandom Hitzl-Zele* telah dilakukan oleh Kordov dan Stoyanov (2017), yaitu meneliti tentang penyembunyian informasi pada media gambar. Penelitian tersebut menggunakan *LSB* untuk menyematkan informasinya pada *pixel* gambar yang dipilih dengan *Hitzl-Zele chaotic map*. Penelitian yang membahas penggabungan kriptografi dan steganografi sudah banyak dilakukan. Pertama, penelitian oleh Mufadilah (2019) yang membahas implementasi kriptografi RSA dengan 3 buah bilangan prima dan steganografi *LSB* dengan *Linear Congruential Generator* pada media gambar. Kedua, penelitian yang dilakukan oleh Ulfah (2020) tentang pengamanan pesan teks dengan menggunakan kriptografi *AES* dan steganografi *LSB* pada media gambar. Ketiga, penelitian yang dilakukan Humaira, dkk. (2023) terkait kriptografi skema pembagian rahasia dan steganografi *LSB* pada *file* audio *wav*. Namun, penelitian Humaira, dkk. (2023) membatasi masalah pada skema (3, 4), yaitu skema untuk membagi pesan kepada 4 *participant* dengan jumlah minimum *participant* yang dapat mengonstruksi kembali pesan adalah 3 *participant*, lalu penyematan dilakukan pada 4 buah *file* audio *wav* dan hanya mengakomodasi pesan berupa 6 digit angka serta penyematan *LSB* dilakukan pada byte secara berurutan.

Pembatasan masalah pada penelitian sebelumnya menjadi dorongan dilakukannya penelitian ini. Oleh karena itu, pada penelitian ini mengkaji kriptografi skema (t, w), yaitu skema untuk membagi pesan kepada w *participant* dengan jumlah minimum *participant* yang dapat mengonstruksi kembali pesan adalah t *participant* dengan $w, t \in \mathbb{Z};\ 2 \leq t \leq w$; dan steganografi audio *Least Significant Bit* dengan *pseudorandom Hitzl-Zele* serta implementasinya pada program komputer yang menghasilkan skema (t, w) dan disematkan pada w buah *file* audio *wav*.

1.2 Rumusan Masalah

1. Bagaimana pengamanan *plaintext* dengan penggabungan kriptografi skema (t, w) dan steganografi *LSB* menggunakan *pseudorandom Hitzl-Zele* pada *file* audio *wav*?
2. Bagaimana implementasi dari penggabungan kriptografi skema (t, w) dan steganografi *LSB* menggunakan *pseudorandom Hitzl-Zele* pada *file* audio *wav* dalam program aplikasi dengan bahasa pemrograman Python?
3. Bagaimana validasi program aplikasi penggabungan kriptografi skema (t, w) dan steganografi *LSB* menggunakan *pseudorandom Hitzl-Zele* pada *file* audio *wav* yang dikonstruksi?

1.3 Tujuan Penelitian

1. Merancang skema pengamanan *plaintext* dengan penggabungan kriptografi skema (t, w) dan steganografi *LSB* menggunakan *pseudorandom Hitzl-Zele* pada *file* audio *wav*.
2. Mengonstruksi algoritma dan program aplikasi penggabungan kriptografi skema (t, w) dan steganografi *LSB* menggunakan *pseudorandom Hitzl-Zele* pada *file* audio *wav* dengan bahasa pemrograman Python.
3. Memvalidasi program aplikasi penggabungan kriptografi skema (t, w) dan steganografi *LSB* menggunakan *pseudorandom Hitzl-Zele* pada *file* audio *wav*.

1.4 Batasan Masalah

1. *Plaintext* berupa bilangan bulat nonnegatif.
2. Skema pembagian rahasia yang digunakan adalah skema (t, w) dengan $t, w \in \mathbb{Z}; 2 \leq t \leq w \leq 50$.
3. Format *file* audio yang digunakan adalah format *.wav atau *.wave dengan *bit depth* 8-bit, 16-bit, 24-bit, dan 32-bit.

1.5 Manfaat Penelitian

1. Manfaat dari segi teoritis

   Penelitian ini diharapkan memberikan kontribusi dalam menambah banyaknya pilihan pada metode pengamanan informasi terutama pada kriptografi skema pembagian rahasia dan steganografi *LSB* menggunakan *pseudorandom Hitzl-Zele* pada *file* audio *wav*, sehingga dapat membantu pengembangan metode terkait.
2. Manfaat dari segi praktis

   Penelitian ini menghasilkan program aplikasi penggabungan kriptografi skema (t, w) dan steganografi *LSB* menggunakan *pseudorandom Hitzl-Zele* pada *file* audio *wav* dengan bahasa pemrograman Python, yang dapat digunakan oleh *user*.