

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada kehidupan manusia, tidak lepas dari adanya komunikasi. Pada masa ini, masyarakat berkomunikasi tidak hanya dengan bertatap muka, namun dapat dilakukan dengan perangkat komunikasi. Teknologi komunikasi secara nyata telah menjadi bagian dari masyarakat di Indonesia. Hal ini terutama didorong oleh pertumbuhan komunikasi berbasis seluler dan internet sebagai media digital untuk penyampaian informasi.

Keberhasilan dalam penerapan media digital karena memiliki beberapa kelebihan yang dimiliki media digital, seperti transmisi bebas derau, penyimpanan yang padat, penyalinan yang sempurna, dan kemudahan dalam melakukan pengeditan. Akan tetapi, di samping kelebihan yang dimiliki dari media digital, terdapat juga kelemahan dari penggunaan media digital, yaitu keamanan informasi yang terkandung di dalamnya [1]. Salah satu media digital yang dapat digunakan dalam penyampaian pesan dalam bentuk lambang-lambang auditif adalah audio.

Dalam pengiriman pesan melalui media audio dan ketika sampai kepada penerima pesan, informasi tersebut harus tetap rahasia dan terjaga keasliannya atau tidak dimodifikasi. Penerima informasi tersebut harus yakin bahwa informasi itu dikirim oleh orang yang tepat, begitu juga sebaliknya, pengirim yakin bahwa penerima pesan adalah orang yang sesungguhnya [2]. Untuk permasalahan berikut diperlukan suatu metode untuk menjaga keamanan suatu informasi yaitu proses enkripsi dan dekripsi. Proses ini digunakan untuk menyembunyikan informasi dari orang lain yang tidak berkepentingan [2].

1.2 Rumusan Masalah

Dari latar belakang tersebut, masalah yang didapat adalah bagaimana mengoptimalkan enkripsi audio menggunakan Algoritma Pseudorandom dan Teori Kekacauan pada pesan suara.

1.3 Batasan Penelitian

Dari rumusan masalah tersebut, masalah yang akan dibahas dalam batas tertentu yaitu:

1. Analisa algoritma untuk mengacak gelombang audio asli menjadi gelombang terenkripsi.
2. Algoritma yang dipakai adalah *Pseudorandom* dan fungsi Kekacauan.
3. Software yang digunakan untuk memecah gelombang audio adalah GoldWave versi 6.35.
4. Software yang digunakan untuk mengaplikasikan algoritma adalah Visual Studio Enterprise 2017 versi 15.6.3
5. Objek Input adalah file plain *audio*, dan output adalah file *chipper* audio.

1.4 Maksud dan Tujuan Penelitian

Maksud dari penelitian ini adalah menganalisa, mengoptimalkan, dan menguji kemampuan dari enkripsi file audio dengan menggunakan *Pseudorandom* dan fungsi Kekacauan dengan tujuan :

1. Menguji kesesuaian algoritma untuk enkripsi audio.
2. File chipper dapat diubah menjadi bentuk noise.
3. Audio lain yang ditumpangi tidak jauh berbeda sebelum ditumpangi chipper.

1.5 Metode Penelitian

1.5.1 Pengumpulan Literatur

Metode ini dilakukan dengan mengumpulkan jurnal dan buku referensi yang berkaitan dengan penelitian terkait.

1.5.2 Pengumpulan Data

Data yang diambil adalah file audio dengan format wav yang dipecah gelombangnya menjadi serangkaian nomor dengan nilai amplitudo. Audio yang diambil memiliki *sample rate* 44100 Hz dengan 2 *channels*.

Sample rate 44100 Hz diambil karena menjadi standar *sample rate* untuk kebanyakan audio. Menurut *Nyquist-Shannon Sampling Theory*, *Sample rate* 44100 dipilih karena batas kemampuan telinga manusia untuk menangkap frekuensi suara adalah dari 20 Hz sampai 20000 Hz, sehingga *sample rate* yang paling efisien untuk digunakan adalah 44100 Hz [9].

1.5.3 Desain

Sistem didesain dengan menggunakan model berupa flowchart sebagai penggambaran proses yang akan dilakukan di sistem.

1.5.4 Implementasi

Pada tahap implementasi, setiap tahap proses akan diaplikasikan secara urut untuk menghindari ketidaksesuaian proses dan mendapatkan hasil.

1.5.5 Pengujian

Pada tahap pengujian, hasil penelitian akan diuji dengan menggunakan Uji Analisa Ruang Kunci, Uji Sensitifitas Kunci, dan Uji Mel-frequency Cepstral Coefficients (MFCC). Analisa Ruang Kunci digunakan untuk menentukan berapa batas atas dan bawah angka yang

dapat digunakan sebagai kunci. Uji Sensitifitas Kunci digunakan untuk menguji tingkat sensitifitas kunci. Uji MFCC digunakan untuk menganalisa kesamaan audio.

1.6 Sistematika Penulisan

Sistematika penulisan dijelaskan sebagai berikut:

BAB I PENDAHULUAN

Bab ini memuat latar belakang masalah, rumusan masalah, batasan-batasan penelitian, tujuan serta manfaat dari penelitian ini, metode yang digunakan, serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini memuat tinjauan pustaka dimana memuat berbagai literatur penelitian terkait penelitian ini, pengenalan tentang kriptografi, konsep dasar kriptografi, dan pengenalan tentang algoritma yang digunakan.

BAB III METODE PENELITIAN

Bab ini memberikan gambaran umum, alat dan bahan yang diperlukan dalam penelitian, dan alur penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi hasil dari penelitian, pembahasan sistem, dan pengujian.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran untuk para peneliti yang dirangkum selama proses penelitian makalah diskusi.