

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan *Cryptocurrency* telah mendapatkan popularitas yang signifikan dalam beberapa tahun terakhir. *Cryptocurrency* telah menarik perhatian dari investor institusi, perusahaan besar, dan bahkan pemerintah. Banyak orang melihat *Cryptocurrency* sebagai alternatif investasi yang menjanjikan [1]. Namun, keamanan penyimpanan mata uang kripto menjadi suatu aspek krusial yang perlu diperhatikan. Keberhasilan teknologi *blockchain* dalam memberikan keamanan yang tinggi terhadap transaksi masih dihadapkan pada risiko kehilangan akses akun yang dapat terjadi melalui pencurian *Seed Phrase*, serangan *phishing*, atau kebocoran data [2].

Seed Phrase Wallet (atau disebut juga *recovery phrase*) adalah urutan 12 hingga 24 kata yang digunakan untuk mengakses dan memulihkan akses ke *Cryptocurrency* yang disimpan dalam sebuah *wallet* [3]. Keamanan *Seed Phrase* ini menjadi sangat penting karena siapa pun yang memiliki *Seed Phrase* dapat mengakses dan mengendalikan *Cryptocurrency* yang ada dalam *wallet*.

Ancaman terhadap keamanan *Seed Phrase* dapat datang dari berbagai sumber, termasuk *malware*, pencurian fisik, dan akses ilegal ke perangkat komputer atau perangkat penyimpanan [2]. Untuk mengatasi risiko ini, penting untuk menyimpan *Seed Phrase* dengan cara yang aman dan tidak mudah terdeteksi oleh pihak yang tidak berwenang. Oleh karena itu, diperlukan metode yang efektif untuk menyembunyikan *Seed Phrase*.

Steganografi adalah salah satu solusi yang telah dikembangkan untuk mengatasi masalah ini. Steganografi adalah suatu teknik yang digunakan untuk menyembunyikan pesan atau informasi sensitif dalam suatu media yang tampak tidak mencurigakan [4]. Steganografi sering kali dikaitkan dengan kriptografi, yang melibatkan enkripsi pesan untuk menjaga kerahasiaan konten. Namun, steganografi berbeda dengan kriptografi dalam cara pendekatannya. Kriptografi melindungi pesan dengan cara mengubah isi pesan menjadi bentuk yang tidak

terbaca, sedangkan steganografi fokus pada menyembunyikan pesan itu sendiri dalam media yang tidak mencurigakan.

Penerapan steganografi mencakup berbagai bidang, seperti keamanan komunikasi, perlindungan hak cipta digital, forensik digital, dan penyelidikan kejahatan. Meskipun steganografi memiliki fungsi yang bermanfaat, ada juga potensi penyalahgunaan, seperti menyembunyikan informasi teroris atau aktivitas kriminal. Dalam konteks ini, penggunaan steganografi dalam citra digital dapat membantu dalam menyembunyikan *Seed Phrase Wallet* sehingga tidak mudah terdeteksi oleh pihak yang tidak berwenang.

Pada penelitian sebelumnya, telah ditemukan beberapa penelitian menggunakan metode *End of File* dalam mengamankan suatu informasi. Penelitian pertama pada tahun 2020 dengan judul “*Implementasi Algoritma End of File (EoF) Pada Steganografi Citra*” yang disusun oleh Minarni dan Andre Gesta Fernando. Penelitian tersebut menguji 50 karakter sampai 100000 karakter dengan ukuran citra GIF 200 kb hingga 2 MB. Pengujian tersebut dapat menyisipkan pesan dengan baik tanpa merusak citra GIF dan dapat menyisipkan pesan hingga 100000 karakter.

Pada penelitian kedua, tahun 2021 dengan judul “*Algoritma End of File dan Rijndael pada Steganografi Video*” yang disusun oleh Imam Riadi, Sunardi, Dwi Aryanto. Penelitian tersebut menghasilkan bahwa pesan rahasia berhasil disisipkan pada 6 video. Dapat menampung *Byte* pesan yang tidak terbatas, tidak terjadi perubahan kualitas warna

Pada penelitian ketiga, Pertama, pada tahun 2023 dengan judul “*Implementasi Algoritma Vigenere Cipher Dan End of File Pada Steganografi Video*” yang disusun oleh Minarni, Aliyul Ikram, Indra Warman, Ganda Yoga Swara. Penelitian tersebut menghasilkan bahwa pesan berhasil disisipkan pada file video. Pengujian tersebut dapat menyisipkan pesan dengan baik tanpa merusak video dan dapat menyisipkan pesan hingga 5000 karakter.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka diperoleh rumusan masalah sebagai berikut:

1.2.1 Permasalahan

Cryptocurrency telah menjadi alternatif investasi yang populer, namun keamanan penyimpanan aset digital masih menjadi tantangan utama. Kehilangan atau pencurian *Seed Phrase* dapat berakibat fatal bagi pemilik aset kripto. Risiko keamanan *Seed Phrase* dapat datang dari berbagai sumber, termasuk *malware*, pencurian fisik, dan akses ilegal ke perangkat komputer atau perangkat penyimpanan.

1.2.2 Solusi Permasalahan

Untuk mengatasi risiko ini, penelitian ini mengusulkan metode steganografi *End of File (EoF)* untuk mengamankan *Seed Phrase Crypto Wallet* pada citra digital. Steganografi dipilih sebagai solusi karena kemampuannya menyembunyikan informasi sensitif dalam media yang tidak mencurigakan, sehingga *Seed Phrase* dapat disembunyikan tanpa merusak kualitas citra asli.

1.3 Pertanyaan Penelitian

1. Bagaimana mengimplementasikan steganografi *End of File* untuk menyembunyikan *Seed Phrase*?
2. Bagaimana perubahan pada gambar setelah disisipi *Seed Phrase*?

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun tujuan dari penelitian ini sebagai berikut:

1. Mengimplementasikan metode steganografi *End of File* untuk menyembunyikan seed phrase.
2. Menganalisis perubahan yang terjadi pada gambar setelah dilakukan proses penyisipan *Seed Phrase*.

1.4.2 Manfaat

Adapun manfaat dari penelitian ini sebagai berikut:

1. Mengetahui kemampuan metode *End of File* dalam menyembunyikan *Seed Phrase*.
2. Mengetahui perubahan yang terjadi pada gambar setelah dilakukan proses penyisipan *Seed Phrase*.

1.5 Batasan Masalah

1. *Seed Phrase* disisipkan pada baris terakhir gambar

2. Dataset yang digunakan adalah beberapa gambar yang dapat didownload pada
[https://informatika.stei.itb.ac.id/~rinaldi.munir/Koleksi/Citra%20Uji/Citra Uji.htm](https://informatika.stei.itb.ac.id/~rinaldi.munir/Koleksi/Citra%20Uji/Citra%20Uji.htm).

1.6 Sistematika Proposal

Sistematika laporan penelitian ini tersusun dalam beberapa bab yaitu:

BAB I PENDAHULUAN

Pada bab ini membahas tentang penjelasan *Seed Phrase*, metode yang digunakan yaitu Steganografi *End of File*, rangkuman dari penelitian sebelumnya, permasalahan yang timbul berdasarkan penelitian sebelumnya, metode yang diusulkan peneliti, rumusan masalah, tujuan, manfaat dan batasan dari penelitian yang dilaksanakan.

BAB II KAJIAN PUSTAKA

Pada bab ini membahas tentang teori lengkap yang dibutuhkan dalam melakukan penelitian yaitu penjelasan lengkap *Seed Phrase*, metode dan algoritma yang digunakan yaitu Steganografi *End of File*, metode evaluasi dan daftar penelitian terkait yang telah dilakukan sebelumnya.

BAB III METODE USULAN

Pada bab ini membahas tentang metode yang diusulkan, arsitektur sistem yang berisi alur dari sistem yang akan dijalankan serta dataset yang digunakan dalam penelitian

BAB IV HASIL DAN PEMBAHASAN

Bab ini menguraikan implementasi dari metode usulan pada bab sebelumnya, yaitu tahap pembuatan program, pengujian program, dan pengujian hasil.

BAB V PENUTUP

Pada bab ini berisi kesimpulan dari penelitian yang disesuaikan dengan pertanyaan penelitian dan saran terkait pengembangan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

Berisi jurnal atau referensi yang dijadikan acuan dalam penelitian ini