ABSTRAK

IMPLEMENTASI ALGORITMA HUFFMAN UNTUK KOMPRESI CIPHERTEXT ADVANCED ENCRYPTION STANDARD 128 PADA AUTENTIKASI BERBASIS PENYISIPAN GAMBAR

Oleh: Rizki Pratama
Pembimbing I: Wisnu Uriawan, M.Kom.
Pembimbing II: Muhammad Insan Al-Amin, S.T., M.Kom.

Penggunaan metode autentikasi dengan *username* dan *password*, yang masih menjadi pilihan umum meskipun memiliki kelemahan yang telah diketahui. Beberapa ancaman terhadap keamanan seperti serangan *brute-force* dan *phishing* juga dibahas. Kemudian, disampaikan tentang inovasi dalam sistem autentikasi menggunakan Steganografi, khususnya penggunaan algoritma Huffman untuk mengompresi *ciphertext* sebelum disisipkan ke dalam gambar. Penelitian ini bertujuan untuk menerapkan dan mengetahui kinerja algoritma Huffman dalam konteks autentikasi berbasis gambar dengan menggunakan AES 128 dan LSB. Hasil penelitian menunjukkan bahwa penggunaan kompresi Huffman Coding dapat mengurangi ukuran gambar setelah dikompresi, namun proses autentikasi memerlukan tahapan yang cukup panjang. Meskipun demikian, aplikasi ini memiliki potensi keamanan yang lebih tinggi karena *password* dienkripsi dan disisipkan ke dalam gambar, serta belum banyak digunakan secara luas dalam praktik nyatanya.

Kata Kunci: AES, LSB, Huffman*, password, login,* Steganografi

ABSTRACT

IMPLEMENTATION OF HUFFMAN ALGORITHM FOR COMPRESSING ADVANCED ENCRYPTION STANDARD 128 CIPHERTEXT IN IMAGE-BASED AUTHENTICATION

By: Rizki Pratama
Supervisor I: Wisnu Uriawan, M.Kom.
Supervisor II: Muhammad Insan Al-Amin, S.T., M.Kom.

The use of authentication methods with username and password remains a common choice despite its known weaknesses. Several security threats such as brute-force attacks and phishing are also discussed. Furthermore, innovations in authentication systems using Steganography are presented, particularly the use of Huffman algorithm to compress ciphertext before embedding it into an image. This research aims to implement and evaluate the performance of the Huffman algorithm in the context of image-based authentication using AES 128 and LSB. The results show that using Huffman Coding compression can reduce the size of the image after compression, though the authentication process requires several lengthy steps. Nonetheless, this application has higher security potential because the password is encrypted and embedded into the image, and it has not been widely adopted in practical use.

Keywords*: AES, LSB, Huffman, passwod, Login, Steganografi*