

## INTISARI

Selama beberapa tahun terakhir, video digital dengan watermark telah menjadi lebih populer di beberapa bisnis. Namun, karena ketersediaan Internet yang luas, video digital mudah diubah dan salinan ilegal dapat dibuat. Watermarking video digital sebagai metode untuk mengidentifikasi pengeditan dan mencegah penyalinan tanpa izin semakin populer. Watermark memungkinkan transendensi hak cipta aset multi-media, meskipun pesan tersemat masih ada. Watermark dapat digunakan di area data multimedia yang kecil karena kurangnya Fidelity. Penelitian ini bertujuan untuk melindungi data dari pelanggaran hak cipta. Watermark (gambar dan pesan) dienkripsi menggunakan dua algoritma enkripsi yang berbeda (RSA+ DES, AES) sebagai tahap awal penyelidikan. Metode kedua adalah teknik steganografi yang disebut robust watermarking berbasis LSB. Metode ini menggunakan rata-rata gambar skala abu-abu yang berbeda untuk mengambil variasi terpenting antara dua gambar dan menyematkan pesan bit rahasia terenkripsi dan gambar dalam keyframe file video MP4. Studi sebelumnya menunjukkan bahwa RSA untuk watermark pesan dan AES untuk watermark gambar dapat mencegah pencurian hak cipta.

Kata kunci: Kriptografi, Steganografi, Video digital, AES, RSA

## **ABSTRACT**

*Digital watermarked video has grown in popularity over the past few years across a variety of businesses. However, due to its widespread availability on the Internet, digital video is easily manipulated and illegal copies can be made. Digital video watermarking has grown in popularity as a way to identify edits and stop unauthorized copying. Although embedded messages are still present, a watermark is a viable solution for the copyright transcendence of multi-media assets. In a small multimedia data area, a watermark may be used due to fidelity limitations. This study aims to protect data against copyright infringement. The watermark (image and message) is encrypted using two different encryption algorithms (RSA + DES, AES) as the initial phase in the study. The second method is a steganography technique called LSB-based robust watermarking. It uses the mean of the grayscale images that differ to take the most important variations between the two images and embeds an encrypted secret bit message and image in key frames of an MP4 video file. A number of previous studies have shown that copyright theft can be prevented by using RSA for message watermarks and AES encryption techniques for image watermarks*

*Keywords: Cryptography, Steganography, Digital Video, AES, RSA*