

ABSTRAK

Penelitian ini bertujuan untuk mendeteksi dan mengidentifikasi keaslian citra digital yang diduga telah mengalami manipulasi menggunakan metode *National Institute of Standards and Technology* (NIST) dengan teknik *Error Level Analysis* (ELA). Penelitian menggunakan empat sampel citra yang terdiri atas dua citra asli, satu citra hasil manipulasi menggunakan Adobe Photoshop CS6 melalui teknik *image splicing*, dan satu citra hasil manipulasi berbasis *Artificial Intelligence* menggunakan fitur Magic Edit pada Canva Pro. Tahapan penelitian dilakukan berdasarkan metode NIST yang meliputi *Collection, Examination, Analysis, dan Reporting*. Proses pemeriksaan dilakukan menggunakan perhitungan nilai hash SHA-256 melalui *Command Prompt*, analisis metadata menggunakan JPEGsnoop, serta analisis visual menggunakan *Forensically Beta* dengan teknik *Error Level Analysis*. Hasil penelitian menunjukkan bahwa citra hasil manipulasi memiliki nilai hash SHA-256 yang berbeda dibandingkan citra asli, sehingga membuktikan adanya perubahan pada file. Analisis metadata menggunakan JPEGsnoop berhasil mengidentifikasi keberadaan perangkat lunak Adobe Photoshop pada citra manipulasi konvensional serta hilangnya metadata kamera pada citra manipulasi berbasis *Artificial Intelligence*. Sementara itu, hasil *Error Level Analysis* menunjukkan adanya perbedaan pola tingkat kesalahan kompresi antara citra asli dan citra manipulasi. Berdasarkan keseluruhan hasil penelitian, metode NIST yang dipadukan dengan perhitungan nilai hash SHA-256, analisis metadata menggunakan JPEGsnoop, dan teknik *Error Level Analysis* terbukti mampu mendeteksi serta mengidentifikasi manipulasi pada citra digital secara efektif.

Kata Kunci: Forensik Digital, NIST, *Error Level Analysis*, JPEGsnoop, SHA-256.

ABSTRACT

This research aims to detect and identify the authenticity of digital images suspected of manipulation by implementing the National Institute of Standards and Technology (NIST) method combined with the Error Level Analysis (ELA) technique. The study used four image samples consisting of two original images, one manipulated image created using Adobe Photoshop CS6 through the image splicing technique, and one AI-generated manipulated image created using the Magic Edit feature in Canva Pro. The investigation followed the NIST stages of Collection, Examination, Analysis, and Reporting. The examination process included SHA-256 hash calculation using Command Prompt, metadata analysis using JPEGsnoop, and visual analysis using Forensically Beta with the Error Level Analysis technique. The results showed that the manipulated images produced different SHA-256 hash values from the original images, confirming file modification. Metadata analysis using JPEGsnoop successfully identified Adobe Photoshop editing traces in the conventionally manipulated image and the absence of camera metadata in the AI-generated manipulated image. Furthermore, the Error Level Analysis revealed differences in compression error patterns between authentic and manipulated images. Therefore, the combination of the NIST method, SHA-256 hash verification, metadata analysis using JPEGsnoop, and the Error Level Analysis technique proved effective in detecting and identifying manipulation in digital images.

Keywords: Digital Forensics, NIST, Error Level Analysis, JPEGsnoop, SHA-256.