

## ABSTRACT

Digital signature has constraints when applied to the image by using the lossy compression method. One of them is image with JPEG format. The JPEG codec standard defines how the image through the compression process becomes a byte stream, and is decompressed back into the image. In other words, the JPEG codec manipulates imagery that has the purpose of compressing the image size, but it affects the quality degradation affecting the image content. This contradicts the digital signature function which aims to prevent manipulation of the image content. So it is necessary to develop a processing method that does not affect or change the image content.

The application of digital signatures to the image authentication process can give the wrong result in distinguishing the manipulation process performed by malicious manipulation or by the content done by the lossy compression method, which will eventually give the same result, ie the image content has been manipulated then it can not be used to verify the authentication process that should be protected by digital signatures. Therefore, in this research will be modified and improved from previous methods and create digital signature based robust content that has better and more secure results.

Keywords: Image Authentication, Robust Content, JPEG, Lossy Compression, Cryptography

## ABSTRAK

Tanda tangan digital memiliki kendala ketika diterapkan pada gambar dengan menggunakan metode kompresi lossy. Salah satunya adalah gambar dengan format JPEG. Standar codec JPEG mendefinisikan bagaimana gambar melalui proses kompresi menjadi aliran byte, dan didekompresi kembali ke dalam gambar. Dengan kata lain, codec JPEG memanipulasi citra yang memiliki tujuan mengompresi ukuran gambar, tetapi itu mempengaruhi degradasi kualitas yang mempengaruhi konten gambar. Ini bertentangan dengan fungsi tanda tangan digital yang bertujuan untuk mencegah manipulasi konten gambar. Jadi perlu untuk mengembangkan metode pemrosesan yang tidak mempengaruhi atau mengubah konten gambar.

Penerapan tanda tangan digital untuk proses otentikasi gambar dapat memberikan hasil yang salah dalam membedakan proses manipulasi yang dilakukan oleh manipulasi jahat atau dengan konten yang dilakukan oleh metode kompresi lossy, yang pada akhirnya akan memberikan hasil yang sama, yaitu konten gambar telah dimanipulasi maka tidak dapat digunakan untuk memverifikasi proses otentikasi yang harus dilindungi oleh tanda tangan digital. Oleh karena itu, dalam penelitian memberika alternatif metode dari metode sebelumnya dan membuat konten yang kuat berbasis digital signature yang memiliki hasil yang lebih baik dan lebih aman.

Kata kunci: Otentikasi Gambar, Konten Kuat, JPEG, Lossy Compression, Cryptography