323. DETECTION OF MALICIOUS ATTACK IN DIGITAL VIDEO USING WATERMARKING

Saranya.N
Department of ECE,
Meenakshi College of Engineering,
Chennai, India
Amutharajan27@gmail.com

We present our project to distinguish malicious attack from common processing operation such as recompression, noise and brightness increasing using practical watermarking scheme. Analysis of the error is used to detect tampering. A well-known solution to the above problems are watermarking, which hides important information in the media. A well-designed watermarking system must provide three main features such as transparency, robustness and capacity. To apply data hiding to content authentication, a semi fragile watermarking technique could be considered to tolerate certain kinds of processing, such as recompression and at the same time detect malicious tampering manipulation. We verify our performance by simulation using MATLAB. Additionally,the following algorithms used in our project are DCT (discrete cosine transform), DFT (discrete wavelet transform), HEVC (high-efficiency video coding) and DWT (discrete wavelet transform) H.264/AVC.The Main advantage of our project is content- based cryptography and increases the security of the system. The applications of our project are military purpose, government work and security purpose.

Keywords— Video authentication, video tampering detection, video watermarking,Data hiding.

ISBN 978-81-904760-6-5