ABSTRACT

Steganography is a technique for embedding secret information into digital media such as images, making its presence visually imperceptible. To detect such hidden messages, an effective steganalysis method is required. This study proposes a combination of Discrete Wavelet Transform (*DWT*) *and Random Forest as an approach to distinguish stego images from cover images. DWT is used to extract frequency-domain features through multi-level decomposition into four sub-bands* (*LL, LH, HL, HH*)*, representing low to high-frequency components of the image. The extracted statistical features are then classified using a Random Forest algortihm. The evaluation involved four wavelet types: Haar, Symlet* (*Sym4*)*, Coiflet* (*Coif1*)*, and Daubechies* (*Db4*)*. The dataset used was a* 2,500*-image subset of IStego100K, consisting of* 1,250 *cover and* 1,250 *stego images. The cover images were selected from the training and testing folders of the dataset, while the stego images were independently generated by embedding random messages into the cover images using the Least Significant Bit* (*LSB*) *replacement technique. The data was split into training* (80%) *and testing* (20%) *sets. The results show that the Db4 wavelet model achieved the best performance, with* 91.4% *accuracy,* 94.0% *precision,* 88.4% *recall, and* 91.1% *F1-score. These findings indicate that the combination of DWT and Random Forest is effective for steganography detection in digital images and holds promise for applications in cybersecurity and digital forensics.*

Keywords: *Digital Image, Discrete Wavelet Transform, LSB, Random Forest, Steganalysis*