ANALYSIS AND MODELING OF FPGA IMPLEMENTATIONS OF SPATIAL STEGANOGRAPHY METHODS

Steganography has become an important method for concealed communication especially through image files. Recent proposed steganographic methods employ multiple levels of complex techniques. Hence, there is an increasing significance for hardware implementation and its performance metrics. The objective of this article is to analyze and model the performance of FPGA hardware implementations of several spatial steganography methods, including: least significant bit (LSB), random LSB, mix-bit LSB and texture method. This paper presents innovative models to estimate energy-to-embed-secret-bit, peak signal-to-noise-ratio (PSNR) energy cost, power and resources in complex systems. Examining the performance results of the FPGA implementations shows that embedding misalignment degrades the performance, and random embedding increases resources by 43% and power by 13%. Furthermore, the mix-bit method has the best results in terms of balancing the energy consumption and PSNR. Moreover, the accuracy of the model to predict the energy to embed a single secret bit is 2%, and the accuracy of the model to predict complex system performance is 1% for hardware resources and 16.6% for power.

Keywords: Data hiding; reconfigurable hardware; FPGA; spatial steganography; security;