ABSTRACT

QR codes are two-dimensional barcodes with black and white modules, providing fast response time, robustness, and large data capacity. They are widely used in various fields, such as finance, gaming, the Internet of Things, and secret messaging media. QR codes can be used as a secret message by embedding an encrypted message, exploiting an error correction mechanism, or embedding an encrypted secret message in the padding area. Exploiting the error correction mechanism has the drawback of decreasing the error-correcting ability. As for embedding only in the padding area, it is necessary to consider the number of cover characters used. One type of cryptography that can be embedded into QR codes is threshold cryptography called (k,n)-thresholds [1]. Previous research generated random grid-based shares. However, there is a weakness in the secret reconstruction result when $k < n$. The proposal of this research consists of the use of codewords in QR codes and share generation mechanisms. The proposed mechanism for embedding shares in the QR code uses error-correcting exploitation and padding codeword and modified generating shares based on a random grid. The results of the experiments that have been carried out result in a decrease in the use of codewords as covers and shares and an increase in the secret reconstruction results when $k \leq n$.

Keywords: Visual Secret Sharing, Threshold Cryptography, QR Code Visual Secret Sharing, Sequential Visual Secret Sharing.