ABSTRACT

SYSTEM AND METHOD FOR SECURELY ADDING REDUNDANCY TO AN ELECTRONIC MESSAGE

A system for adding a redundancy check to an electronic message to discourage tampering and facilitate identification of altered messages provides a communication device for composing message content, a messaging module with a formatting and encoding layer for encoding the message content with header information in a series of message blocks, and an encryption layer for calculating a redundancy check value and inserting the value in one or more locations within the series of message blocks according a rule defined by a characteristic of the message content or the header information, and encrypting the message for delivery to a recipient. Upon receipt, the recipient communication device decrypts the message, extracts the redundancy check value from the message, and compares a calculated redundancy check value with the extracted redundancy check value to determine if the message had been altered before receipt.

Figure 3