Abstract

Digital images have found usage in almost all our everyday applications. These images sometimes contain confidential and intelligible information which need to be protected when stored on memory or transmitted over networks (Intranet or Internet). Many techniques have been proposed to deal with this security issues in the past. This paper proposes a simple scrambling algorithm to encrypt and decrypt the grey level image based on random number generation and Residue Number System (Forward and Reverse Conversion). The image is first encrypted by changing the position of each pixel in the original image without changing the value of grey level. The original image reads row by row, pixel by pixel and each pixel will take a new position in the scrambled image. The new position is chosen based on random number generation from the random number generator. The key will be generated as a matrix during the encryption process and also the key saves the position of each pixel in the encrypted/scrambled image. The encryption layer transforms the scrambled image to moduli images which automatically adds an extra security layer to our data.
The encrypted moduli images is decrypted by decoding the moduli images and converting them back to a single scrambled image (Reverse Conversion) and the single scrambled image back to the Plain and Original Image by using the saved key matrix. This scheme achieves an enhanced image encryption process and a more efficient decryption process without loses of any inherent information of the recovered plain image.

References


Index Terms

Computer Science Security

Keywords

RNS, MRC, Information Security, Encryption, RSA Forward Conversion, Backward Conversion