An Efficient Image Encryption Technique by Using Cascaded Combined Permutation

Muslim Mohsin Khudhair
Department of Computer Information Systems, College of Computer
Science & Information Technology, University of Basrah,
Basrah, IRAQ

Abstract

In this paper, a new simple encryption technique is proposed for gray scale image encryption. The current technique, Cascaded Combined Permutation (*CCP*), is a simple technique based on the primary well known *2-D permutation algorithms*. The application at the permutations is performed on three steps: (1) one permutation algorithm is applied on the image; (2) the image that resulting from the first step is decomposed into four quarters. Pixels in each quarter image are then permuted with one of the permutation algorithms. The resulting encrypted quarters are combined as one image; (3) the encrypted image resulting from the second step is further encrypted by performing another permutation algorithm. Experimental results show efficient encryption that is simple in implementation and has high degree of security. It has several key points of strength such as the sequence in which the primary permutation algorithms are applied.

Keywords: Permutation, Image Encryption, Image Decryption , correlation.

1. Introduction

With the rapid development of multimedia and network technologies, the transmission of multimedia data takes place more and more frequently. Consequently, the security of multimedia data is becoming more and more important [1, 2].

Encryption is one of the ways used to ensure security and protection of secure data from any misuse and forgery. Images have been widely used in our daily life and is an important data class. It may contain diagrams, diagrams of banks, building construction or important data captured by military satellite [3]. Original images are referred as plain images. Encryption is a process that transforms the plain image to cipher image (encrypted image) which is hard to be understood. Decryption is the reverse of the encryption process to produce the original image from encrypted image [4]. Most of the algorithms specifically designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of image encryption algorithms [l]: (a) Non-chaos selective methods; and (b) Chaos-based selective or non- selective methods. Most of these algorithms are image encryption using block-based permutation transformation algorithm. Mohammad *et al*. [5] were proposed a permutation process based on the combination of the image permutation, the