الملخص

في هذه الأطروحة تم اقتراح نظام لتشفير الصور تتضمن تقنيات التشفير بالتبديل. كل واحدة تشرك مع الأخريات للحصول على الصورة المشفرة.

الطريقة الأولى المقترحة هي (التبديل المتعاقب المتكرر CIP) والتي تقوم بتكرار تبديل مواقع نقاط الصورة (Pixels) للصورة ذات التدرج الرمادي (256x256) لعدة مرات. الطريقة الثانية المقترحة هي (التبديل المتعاقب المدمج CCP) الذي يقوم بتقسيم الصورة السرية ذات التدرج الرمادي (256 (256x إلى أربعة أرباع, كل جزء يشفر بتقنية تشفير مختلفة ثم يعاد دمج الأرباع بصورة واحدة ثم تشفر بتقنية تبديل أخرى لتنتج الصورة المشفرة. إن عملية التشفير بهذه الطريقة لها نقاط قوة تتمثل بدرجة ترتيب التقنيات, كذلك قيم المعاملات a, b لكل خوارزمية تشفير. التشفير المعتمد على عملية التبديل بهذين الطريقتين تعطي معامل تقارب (Corr.) جيد.

ولحماية أكثر للصورة السرية, من الضروري تغيير قيم وعنوان نقاط الصورة (Pixels) بدلاً من تغيير عنوان مواقع نقاط الصورة فقط. بتحويلة فورير السريعة تتغير قيم نقاط الصورة. لذا تم دمج الطرق الأنفة الذكر (التبديل بنوعيه) كل على حده مع تحويلة فورير مما جعل من عملية التشفير أقوى وأكثر أمنا.

هناك طريقتين أخريين من خلالهما يمكن تغيير قيم نقاط الصورة وهما (Hadamard Transform) و (Walsh-Hadamard Transform). لذا فان دمج (التبديل المتعاقب المتكرر CIP) او (التبديل المتعاقب المدمج CCP) مع HT و WHT نتج عنها عملية تشفير جيدة وكفوءة وكذلك من خلالها تمت المحافظة على حجم الصورة السرية.

Abstract

In this thesis, the proposed image encryption approach presented that were based permutation techniques, each of them is combined with other permutation techniques to obtain the encrypted image.

The first proposed approach is cascaded Iterated permutation (CIP) that iterated the pixels permutation of a grayscale image (256x256 pixels) for several times. In the second proposed approach which is Cascaded Combined Permutation (CCP) decomposed the secrete grayscale image (256x256 pixels) into four quarters, each part is to be encrypted by different permutation technique. The encrypted quarters are combined and further encrypted with another permutation technique to produce the encrypted image. The resulting encryption has several key points of strength such as the sequence order. Another key points are the coefficients a, b for each permutation algorithm. The permutation based image encryption technique gives a good encryption interms of MSE and correlation.

For more security, it is needed to change the pixels position and value instead of changing position only. FFT increase the degree of security by altering the pixels value. The merging of the two approaches led to strong encryption takes the benefits of each of the merged approach.

Another transform that changing the pixels position is Hadamard Transform (HT) and Walsh-Hadamard Transform (WHT). So, the merging of the two approaches (CIP and CCP) with (HT & WHT) led to a efficient and good encryption while conserve the size of encrypted image unchanged.