Faculty of Engineering
Department of Electrical Engineering

SECURING MULTIMEDIA DATA

A thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy

In

Electrical Engineering

Presented by

Wessam Mohamed Abd El-Fatah Salama

B.Sc. in Communication and Electronics
Faculty of Engineering, Alexandria University, 2008

M.Sc. in in Communication and Electronics
Faculty of Engineering, Alexandria University, 2013

2018

ABSTRACT

The purpose of this dissertation is to develop novel algorithms for image encryption, image steganography and crypto-stego systems. Moreover, three new encryption video algorithms are proposed.

Fractional Fourier transforms (FrFT), Fractional Wavelet Transform (FWT) and Random Phase Masks (RPMs) are the basic tools for digital images encryption in the first system. Moreover, bit shifts of pixel values are used to obtain a more uniform histogram for the encrypted image and to broaden the key space.

The second image encryption algorithm is based on combining random interleaved pixel permutation with Arnold Cat map and fractal images. This combination ensures a large key space, improved security and helps to get a uniform histogram distribution. Histogram equalization is performed to change intensity values in image to enhance its contrast.

In the proposed data hiding algorithm, we consider the use of one-dimensional (Tent map) versus two-dimensional (Baker's map) chaotic maps for the selection of the set of pixels where the secret message bits are to be embedded. The preliminary results ensure that, to eavesdroppers, there will be almost no suspicion regarding the existence of a secret message hidden within the sent image since the peak-signal-to-noise- ratio (PSNR) is high and the mean-squared-error (MSE) is low for the different alternatives investigated. Additionally, a system which uses both cryptography and steganography, a crypto-stego system, is developed with the aim to obtain enhanced security and confidentiality.

Compression and cryptography are two opposing techniques. Encryption ensures that the transmitted data is reliable and integral by converting it from legible into illegible data through an encoding process. Conversely, a compression method seeks to reduce the size of transferred or stored data by finding out and removing duplicate parts of evidence or patterns of data. However, data compression and cryptographic system are deeply connected and mutually useful that they are capable of being employed together. The aims of our algorithm are to generate a smaller size of data to ensure a quality of data during reconstruction, to speed up data transmission, to reduce bandwidth requirement, and to ensure its safety. Comparison between compression-encryption technique and encryption-compression technique are mentioned in this thesis. Compression technique is applied to different test images.

This thesis investigates a new scheme for embedding encrypted grayscale image in color cover image which is called Crypto-Stego technique. First a new image encryption scheme named (ArMTFr) is proposed which is used to encrypt grayscale images. In this algorithm Arnold chaotic map and Mersenne-Twisters are used to scramble image pixels and then the scrambled image is XORed with fractal images. Fractal images are utilized to improve the performance of the encryption scheme and to increase the encryption key space, to sustain its security. Before, the encryption process starts, histogram equalization is used to enhance the contrast of the image by transforming the intensity values in it, so that the histogram of the

output image approximately matches a uniform histogram. Second, encrypted image is hidden in a colored cover image in the spatial domain. One-dimensional (Tent map) versus two-dimensional (Baker's map) chaotic maps are performed to select set of pixels where the secret message bits are to be embedded. The red color channel of the cover image for the formerly selected pixels is affected by the embedding process since the eye is not very sensitive for slight variations in this color channel. Furthermore, two LSB embedding schemes are examined by embedding one bit per pixel and embedding two bits per pixel. The preliminary results ensured that there would be no doubt about the existence of a secret message hidden inside the sent image because the peak signal-to-noise ratio (PSNR) is high. However, there is a clear impact on the time required for the embedding process if two-dimensional maps and/or one bit per pixel LSB technique are used.

In this thesis, we propose three new techniques for video encryption based on MPEG-2 compression and different chaotic maps. In the first two algorithms chaotic maps are used to achieve high computational efficiency and increase the encryption key space. Before the encryption process starts, color channel multiplexing is used to enhance security of the algorithm. In the third algorithm, an explicit selected frame is encrypted using Arnold map then XORed with the encrypted video frames resulted from Skew Tent map. Moreover, bit shifts of pixel values are used to obtain a more uniform histogram for the encrypted video, improve the performance of the encryption scheme and increase the security. Before the encryption process starts, row vector technique is applied to decrease processing time. The experimental results show that the encrypted video has low correlation coefficients among adjacent pixels, good entropy, good histogram, low time consumption, as well as resistance to differential attacks, additive noise and cropping attacks.

It is observed that our proposed algorithms have low correlation coefficients among adjacent pixels, a good histogram distribution, acceptable quality, as well as resistance to differential attacks.