Al-Azhar University
Faculty of Science
Physics Department

Adaptive Techniques for Hiding Messages in The Quantum Noise of Pictures

THESIS
Submitted in Partial Fulfillment of the Requirements for the Degree of
Doctor of Philosophy in Science – Physics (Image and Data Processing)

By

Mohammed Ramadan Saady Abd El Tawwab
Assistant Lecturer of Physics, Department of Basic Scienc
Faculty of Computers and Artificial Intelligence,
Fayoum University –Fayoum.
M.Sc In Science (Electronics) – 2016

To

Physics Department, Faculty of Science (Boys), Al-Azhar University.

SUPERVISED BY

Prof. Dr/ Hany Hamdy El-Bahnasawy
Professor of Solid State,
Department of Physics
Faculty of Science
Al-Azhar University – Cairo.

Prof. Dr/ Shreen Ali Taie
Professor of Computer Science
Department of Computer Science
Faculty of Computers and Artificial Intelligence
Fayoum University – Fayoum.

Dr/ Amir Mohammed Eissa
Lecturer of Bio Physics, Department of Physics
Faculty of Science
Al-Azhar University – Cairo.

Cairo – 2025

ABSTRACT

Noise attached to an image during the image acquisition stage has been exploited to hide data in the image file that is termed the cover image file. A special type of this noise that is called quantum (shot) noise has been exploited to hide data in the image file and produce what is called image steganography. Image steganography is considered one of the most promising secure data transmission methods. Most researchers in the field of image steganography are indifferent to the image file's origin and the camera settings that directly affect the camera's sensor's noise, which directly affects the image itself. They often design their image steganography algorithms by considering the image as one array of pixels or a combination of three color channels.

In this thesis, we have studied the relationship between the camera settings and the camera's sensor's noise and the effect of that on the performance of an image steganography algorithm. In a case study, we have studied the performance criteria of the image steganography algorithm that is based on a pair of images that differ only in quantum noise. To assess the generalizability of the proposed study, we have built a dataset composed of numerous images that have been captured with various camera settings for various objects at different times of the day. These

images have been used to construct stego images by using the image steganography algorithm.

In terms of evaluating the embedding capacity criterion and retrieving the embedded data and their relationship with the camera settings, the experimental results showed that raising the sensitivity of the camera's sensor enables it to capture more photons, which in turn increases the interacting quantum efficiency. This leads to increasing the quantum noise level in the resulting image, which in turn increases the number of non-equal pixels in two consecutively captured images. As a result of that, the steganography algorithm will be able to embed and transmit high-capacity secret messages and finally decode them without bit error.

Also, to ensure that the security criterion of the steganography algorithm is affected by camera settings, we have proposed a novel image steganalysis method to check whether a suspected image is a stego or not. The results showed that the steganography algorithm that doesn’t consider the origin of the cover image can be attacked easily. To evaluate the performance of our steganalysis method, it has been compared with two other well-known standard steganalysis methods that concern attacking stego-images that were produced by random or sequential embedding. The data set of stego images has been attacked with

the **three** steganalysis methods. For the two standard steganalysis methods, the stego images' recognition rate is small compared to that of our novel steganalysis method. The recognition rate for one standard steganalysis method was 50.76% and 0% for the other method.