Contents lists available at Egyptian Knowledge Bank

Labyrinth: Fayoum Journal of Science and Interdisciplinary Studies

Journal homepage: https://lfjsis.journals.ekb.eg/

Secure Hiding Messages Technique Based on the Effect of Camera Settings on the Image's Quantum Noise

Mohammed R. AbdEltawwab [a *], Shereen A. Taie [b], Hany H. El-Bahnasawy [c], Amir Eissa [c]

[a] Basic Science Department, Faculty of Computers and Artificial Intelligence, Fayoum University, El Fayoum, 63514, Egypt.
[b] Computer Science Department, Faculty of Computers and Artificial Intelligence, Fayoum University, El Fayoum, 63514, Egypt.
[c] Physics Department, Faculty of Science, Al-Azhar University, Nasr City, 11884, Cairo, Egypt.

ARTICLE INFO

Keywords:
Image Steganography
Hiding Information
Quantum Noise
Camera Settings

ABSTRACT

Image steganography is considered one of the most promising secure data transmission methods because it hides the data in an image file. The image file has a substantial role. A lot of methods of image steganography have been presented in the literature. Most researchers in the field of image steganography are indifferent to the image file's origin and the camera settings that directly affect the image itself. They often design their algorithms to consider the image as one channel or a combination of three color channels. They don't consider that the performance of their algorithms can be influenced by the sensor's noise, which is affected by the camera settings. To address this issue, we have studied the relationship between the camera settings and the camera sensor's noise and the effect of that on the performance of a steganography algorithm. In a case study, we have investigated the steganography algorithm that is based on quantum noise. We have used numerous images that have been captured with various camera settings for various objects at different times of the day to assess the generalizability of the proposed study. 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 photons. Thus, the quantum noise level in the resulting image increases, which in turn increases the number of non-equal pixels in two consecutively images and enables the steganogaraphy algorithm to transmit high-capacity secret messages and decode them without bit error.

1.Introduction

As communication in its different forms between two partners or two organizations, namely sender and receiver, is crucial in our daily life, and since the privacy of correspondence is a right granted by the constitution of most countries [1], it has become mandatory to guarantee this right. Due to the widespread use of the Internet for transmitting massive amounts of data and the increasing number of technologies that have paved the way for data theft, it has become a challenge to secure data transmission over the Internet. Thus, numerous methods have been proposed by researchers to address the issue of secure data transmission [2]. Cryptography is one of these methods. It encrypts a secret message by changing it from one form to another, so an unauthorized reader sees it as a meaningless jumble of characters. However, the encrypted secret message can be located and intercepted, but it can't be decoded easily. This interception can be considered damaging to the secret message [3]. Thus, cryptography does not guarantee privacy.

Steganography provides a solution by masking the secret message's existence. It is a widely used method for secure data transmission because it allows the sender to hide the secret message in another file, and no one other than the intended recipient knows of its existence [4, 5]. Thus, it attracts no suspicion at all. The file used to mask the secret message is called carrier (cover). Among all the carrier files, images have been widely used [6, 7]. This is due to their redundancy in representation [8, 9]. In addition to that, images are easily and frequently shared on the Internet [2, 9]. Thus, many studies have shown a significant interest in image steganography as a safe method for data transmission over the last decade.

A steganography system involves two stages: embedding (masking) and extraction, as shown in Fig. 1. The embedding stage involves selecting specific bits or bytes within the carrier file and replacing them with the corresponding bits or bytes from the secret message. Different data types can be concealed inside the cover file. The locations in which the secret message bits are embedded have been described

* Corresponding author.
E-mail address: mrs00@fayoum.edu.eg (M. R. AbdEltawwab); Tel.: +201080137779

DOI: 10.21608/ifjsis.2024.313955.1086
Received 20 August 2024; Received in revised form 29 September 2024; Accepted 13 November 2024
Available online 6 December 2024

through an embedding key that is later used to retrieve the embedded secret message. Once the embedding stage has been performed, the resulting file is termed a stego file and denoted by S, for example, a stego-image.

The least significant bit (LSB) substitution technique is an example of embedding techniques. The literature introduced two different approaches for LSB substitution: least significant bit replacement (LSBR) and least significant bit matching (LSBM)[10]. To hide the secret message bits, the two approaches exploit the least significant bits (LSBs) of the cover image. In the first approach, the LSBs of the cover image are replaced with the secret message bits when there is no matching between them, i.e., even pixel values are increased by one and odd values are decreased by one, but the second approach randomly increments or decrements the value by one. Both approaches leave the LSBs unchanged if they match with the secret message bits.

The embedding process can be carried out in two schemes: sequential and random. In contrast to the sequential scheme, the random scheme disperses the positions of the pixel values that will be modified due to embedding. Thus, it has attracted attention and is very strong against visual attacks [11]. The embedding process can be carried out in the spatial or transform domains.

Fig. 1 Stages of a steganography system.

During the extraction stage, as well as the embedding key, a decoding algorithm must be used to reverse the embedding stage and retrieve the hidden secret message. The decoding algorithm should know where to look for the hidden message and how it has been embedded. In the case where the embedding key is the same as the extraction key, steganography is classified as secret key steganography, while in the case where they are not identical, steganography is classified as public key steganography [1].

The performance of an image steganography algorithm is evaluated according to three criteria: capacity, imperceptibility, and security. While other researchers mentioned that there are four criteria, the fourth one is robustness [12-15]. There is a trade-off between these criteria[16]. For example, increasing the capacity of embedded data usually degrades the stego-image quality significantly [2, 17]. Thus, in a single-cover image-based steganography, the resulting stego-image may be attached with distortion. The amount of distortion varies depending on the steganography algorithm and the amount of embedded data. The stego-image, as a result of distortion, will raise suspicion.

Thus, the researchers think about how to perfectly hide the secret message without embedding it in the cover image. Using two cover images instead of a single cover image to mask the secret message has been adopted by the researchers in Refs. [1, 18]. In [1], the author relies on the fact that it is impossible to perfectly define the number of emitted photons from a source per unit time, and the number of photons absorbed by a sensor during exposure time follows the random Poisson distribution. This randomness leads to what is known as quantum noise, which enables the author to create a stego image that simulates the original statistical distribution of the cover image. The author has used two visually identical cover images, termed K and C, which differ only in quantum noise level. They have been photographed consecutively for the same scene. The stego-image's pixels are picked either from K or C according to the secret message bits. This steganography algorithm was termed steganography without embedding (SWEM).

To integrate the three or four criteria in an image steganography algorithm, we must consider the carrier image file, how it has been formed, and what affects it. The image file is produced by a camera, a system that uses a light signal as an input and digital data as an output. The camera's input is in the form of incident photons[19]. The final camera's output signal is produced by encoding each pixel's signal into a digital number, often utilizing 8, 12, or 16 bits. An electronic device called a sensor is the heart of a camera. All sensors work with the same principle, which is termed the photoelectric effect, where the incident light that is formed into a stream of photons creates free electrons in the sensor's light-sensitive region. Each absorbed photon generates a single electron. The generated electrons are gathered over an amount of time called the exposure or integration time. These electrons are converted into a digitized voltage. If there is no technical noise, the digital values would be a direct representation of the number of photons absorbed by the pixel. But the emitted photons contribute to noise where they are emitted at an unpredictable rate. Thus, it is impossible to perfectly define the number of emitted photons per unit time. In addition to that, the number of absorbed photons by a sensor's pixel during exposure follows the Poisson distribution, which is random. This randomness leads to what is known as quantum (shot) noise. The characteristics of shot noise of light are plotted as a function of illumination level on a Log-Log graph. The shot noise profile is a straight line with a slope of ½ on the Log-Log curve, as shown in Fig. 2[19].

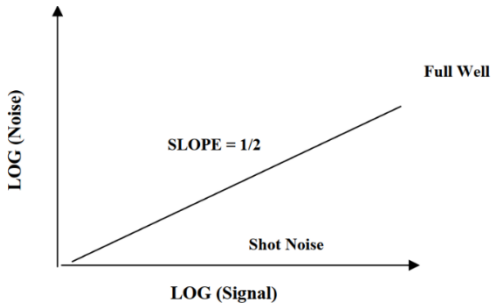

Fig.2 shot noise of input light plotted on a Log-Log curve[19].

In addition to the photon's noise, every integrated circuit, including image sensors, suffers from noise that can be classified into two types: temporal noise and spatial noise. Each of them has a unique nature and impact on the image[20]. Temporal noise refers to the fluctuation in pixels' responses under constant illumination over a specific time period. Spatial noise refers to the variation of pixel responses within a frame, i.e., pixel-to-pixel variations that are steady over time. These are statistical variations in "offset" and "gain" of the pixel over a frame and are fixed at constant illumination, therefore referred to as fixed pattern and hence fixed pattern noise (FPN).

Dark current noise, read noise, and reset noise are examples of temporal noise. Dark current noise is the result of thermal random generation of electron-hole pairs in the dark, i.e., dark current, and it depends exponentially on temperature[21]. The dark current is usually different from pixel to pixel [22]. The average value of dark current for all pixels might be referred to as the dark current bias. Read noise is a sensor's inherent noise that is equal to the noise level under no illumination. Reset noise is the noise that is sampled on the floating diffusion capacitor due to charge redistribution and uncertainty of charge on the capacitor when the reset switch is turned on or off. In modern image sensors, the reset noise is cancelled out.

Fixed pattern noise (FPN) is an example of spatial noise. After the photoelectric effect takes place, the charge collection mechanism is not ideal because some pixels gather charge more efficiently than others, resulting in pixel-to-pixel sensitivity discrepancies. This effect creates FPN in an image. This noise is fixed because it is not random. It is geographically the same pattern from image to image. It is proportional to the signal, unlike shot noise, which varies as the square root of the signal. It is for this reason that FPN for visible and near IR applications will dominate signal shot noise over most of a sensor's dynamic range.

The photon transfer curve (PTC) that is shown in Fig. 3 is a standardized test procedure used during camera manufacturing to provide consistent, quantitative, and verifiable performance data such as read noise, dark current, full well capacity, sensitivity, dynamic range, gain, and linearity. Four distinct noise regions are identified in a PTC. The first region, read noise, represents the noise measured under totally dark conditions, which often includes several different noise contributors. As the light illumination is increased, read noise gives way to photon shot noise, which represents the middle region of the curve. The third region is associated with pixel FPN, which generates a characteristic unity slope. Finally, the fourth region occurs when the subarray of pixels enters the full-well region. In this region, the noise modulation typically decreases as saturation is approached. Although shot noise always decreases, for some arrays, the FPN may actually increase. This characteristic is frequently present in the CMOS sensor.

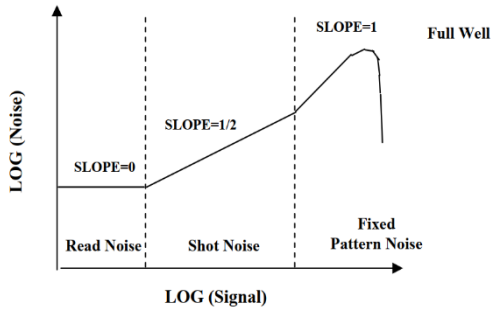

Fig.3 Photon Transfer Curve (PTC)[19].

Until now, different methods for perfect image steganography have been proposed. Several image steganography techniques in the spatial domain have been presented and reviewed in [16]. Each technique attempts to produce a stego image that is identical to its cover image. Each technique has its own advantages and disadvantages. Some techniques have high payload cut-off points and exhibit exceptional sensitivity and blur depending on the chosen cover for concealed or obscured data, specifically in terms of spatial domain hiding. However, some are more powerless against attacks, while others are solid against attacks. Up to this point, they have cut down on the payload limit. So, there is a trade-off between the criteria. However, researchers did not consider that camera settings at the instant of taking the image could be the reason for this trade-off.

The LSB substitution technique has been widely used in image steganography since its inception [23]. It has remained popular to this day because of its ability to embed large secret data without visible visual distortions. The traditional embedding procedure is done in order and the asymmetric modification makes the resulted stego image vulnerable to common statistical attacks. Gutub et al. [24], the author hid the secret message in the LSBs of a red-green-blue (RGB) image's pixels, with randomization in the selection of the number of LSBs used and the color channels that were used. The message has been encrypted using the AES algorithm and then has been hidden based on two randomly generated numbers: s1 and s2, where s1 is used to determine the RGB image's channel that is going to be used in hiding, and s2 is used to determine the number of the LSBs that are used to hide the encrypted secret message. Parvez & Gutub [25], the author proposed a new technique for RGB image steganography, where the R-G-B color intensity values were used to determine the number of bits that can be stored in each pixel; channels with lower color values can store more data bits. In LSBM, each secret message bit may match the LSB of a pixel value with a probability equal to 0.5. Thus, by using the LSBM, the probability that a pixel is changed is 0.5. A revisited version of LSBM has been proposed [26]. The author used gray-scale cover images and embedded the secret message by using two cover image pixels at the same time. It improved the performance by lowering the probability of modification per pixel from 0.5 to 0.375. Sarreshtedari [27], the author used the LSBM approach. Bits of the secret message have been embedded using three adjacent cover image pixels at the same time. Thus, the probability of modification per pixel is reduced from 0.375 to 0.333.

A novel image data hiding technique by adaptive LSB substitution has been proposed in [28]. The scheme exploits the brightness, edges, and texture masking of the cover image to estimate the number k of LSBs for data hiding. Pixels in the noise non-sensitive regions are embedded by a k-bit LSB substitution with a lager value of k than that of the pixels in noise-sensitive regions. A novel reversible information hiding method to conceal secret data into a grayscale cover image has been proposed in Chang et al.[29]. The binary secret message is first converted into secret digits in the base-5 numeral system. Two secret digits are then hidden into one cover pixel pair at a time by encoding them into two cover images. This method of embedding is secure because an attacker with a single stego image cannot extract the complete

embedded secret data and recover the original cover image. Several steganographic models based on two cover images have been proposed. In Ref. [18], the proposed model used two different images: a reference image and a cover image, combined with a secret embed key. The reference image is divided into blocks with assigned block-codes. The secret message is converted to binary, and bit pairs are made. The bit pairs of the secret message are encoded using the bit pairs of the different blocks of the reference image, sometimes updating a few LSBs in the reference image. Later, the researchers think about how to escape attack by perfectly hiding the secret message bits without embedding through the cover image's bits. In [1], the author has depended on the fact that it is impossible to perfectly define the number of emitted photons from a source per unit time, and the number of photons absorbed by a sensor during exposure time follows the random Poisson distribution. This randomness leads to what is known as quantum noise that enabled the author to construct a stego image that emulate the original statistical distribution of the cover image. The author has used two visually identical cover images, termed K and C, which differ only in the quantum noise level. The two cover images have been photographed consecutively for the same scene. The stego-image's pixels are picked either from K or C according to the secret message bits. This steganography method is termed SWEM and forced an attacker to deal with a hypothesis test problem until we proposed our novel steganalysis method for attacking the stego image that was created by the SWEM algorithm[30].

Inefficiency of image steganography based on LSB substitution in the spatial domain propelled researchers to develop it in the frequency domain [31]. In the frequency domain, secret data is embedded after applying a transformation to the carrier image file. One of these transformations is the Discrete wavelet transform (DWT) which has been used in many practical image steganography algorithms due to its ability to hide data in a way that is imperceptible to the human visual system (HVS) and also resist detection by steganalysis methods [31]. Thus, we get a stego-image with better resistance against attacks. As well, it can increase the hiding capacity by using the optimum block replacement approach to hide data into the coefficients of the cover image. Motamedi & Jafari [31], the author proposed a method for embedding the information within the noisy area of a carrier image; thus, he decomposed the carrier image by using 2-D DWT, excluded the approximation coefficients from the embedding process and used the details coefficients to hide the information.

Sidhik et al. [32], the author proposed an image steganography method based on the Haar wavelet transform, which is applied to the normalized version of the three layers (red, green, and blue) of the carrier image and the payload image. After that, the author used wavelet fusion to add the two decomposition matrices that resulted from the decomposition process. Finally, the author applied the inverse discrete wavelet transform (IDWT) to get the stego-image. Abdelwahab & Hassaan [33], the author used the DWT to decompose both the cover image and the secret image into approximation coefficients (LL), horizontal (HL), vertical (LH), and diagonal (HH) details coefficients. These coefficients are divided into non-overlapping blocks. The blocks of approximation coefficients of the cover image are subtracted from the approximation coefficients of the secret image, and the results are called error blocks. Then, the author replaced these error blocks with the best matched HL blocks. In [34], the author proposed an image steganography method based on the Haar wavelet transform and tried to improve the capacity and imperceptibility criteria. He divided the binary sequence of a secret message into packets of five bits and hid them in the integer part of the coefficients HL, LH, and HH, where 2 bits are embedded in the 1st and 2nd LSB of the 1st two coefficients, and the last bit is embedded in the 2nd LSB of the last coefficient. The security criterion is fortified by a key that chooses randomly the coefficients where to hide data. Kumar & Kumar [35], the author proposed the effect of embedding the secret message in different sub-bands on the peak signal to noise ratio (PSNR) of the stego-image. He decomposed the cover and secret image into the four sub-bands LL, HL, LH, and HH. The approximation coefficients (LL) of the two images and the horizontal detail coefficients (HL) of the cover image are portioned into blocks of 4X4 pixels, calculating the error blocks between the approximation coefficients of the two images. For each error block, and by using the root mean square error (RMSE), the best matched block in HL is searched for replacement with the error block. The author used four cover images, each of size 256X256, and four secret images, each of size 128X128. The author concluded that embedding in the HH band gives better PSNR than when embedding is done in the other two sub-bands, HL and LH.

The authors produced better and novel image steganography methods within the past few years, which showed a better direction for image steganography. Primarily, they have showed the fundamental causes of image steganography by achieving the basic criteria of a steganography algorithm. However, still there is a trade-off between these criteria, and they did not consider that camera settings could be the reason for this trade-off.

Camera settings can have a significant effect on an image's noise, and any difference between the noise at the input and the noise at the output must have been caused by the camera's sensor. Setting up camera settings is an important foundational step. However, most researchers in the field of image steganography are indifferent to the image's formation stages and the camera settings that directly affect the image itself. They often design their algorithms by considering the image as one array of pixels or a combination of three color channels, with each channel being represented as an array of pixels according to the camera's sensor. They don't consider that the performance of their algorithms can be influenced by the sensor's noise, which is affected by the camera settings. The paper's main contribution is to address this issue, where the relationship between the camera settings and the sensor's noise has been studied. In a case study, we have applied the SWEM algorithm. We have used numerous cover images that have been captured with various camera settings for different objects at different times of the day to assess the generalizability of the proposed study.

The configuration of the paper is as follows: Section 2 embodies the proposed model and includes the steps for building the dataset used in this paper. The experimental results are presented in Section 3. Finally, Section 4 is a brief discussion about the relationship between the camera settings and the image's quantum noise level, which in turn affects the performance of the steganograghy algorithm.

2.Materials and Methods

2.1 The Proposed Model

The proposed model introduces how camera settings and quantum noise level relate to each other, as well as how this affects the performance of a steganography algorithm that is based on quantum noise. The proposed model consists of six phases: The first phase includes building the used data set from images of different scenes that have been captured with different camera settings. The second phase involves selecting two cover images from each group composed of ten consecutive images. The third phase entails converting the two selected images into raw format, rescaling them, and constructing two arrays of zeroes A and B with the same size as the two selected images. The

fourth phase involves, for each exposure triangle, calculating and drawing of histograms of the two selected images, A and B, and the result of the division of one of the selected images on the A array. In the fifth phase, the histogram of B's pixels whose values range from 1 up to 15 is drawn. In the last phase, the relationship between camera settings and the number of equal and non-equal pixels in a pair of consecutive images and the effect of that on the SWEM algorithm have been deduced. The general structure of the proposed model is shown in Fig. 4.

2.1.1 Data Set

The proposed experiment has been performed using the Canon EOS 1300D camera, known as the Canon EOS Rebel T6 in the United States. It is a popular DSLR camera released in March 2016. It has an 18-megapixel APS-C CMOS sensor, a DIGIC 4+ image processor, and a 9-point automatic focus system. The DIGIC 4+ image processor allows you to take clear images with little noise, even in indoor and low-light environments. The camera has a 3-inch LCD screen with 920,000 dots, which can be used to shoot live videos, review photos and videos, and access camera settings. The camera produces RGB images with size of 5184X3456. Building the used data set involves:

(1) Camera setup: The camera has been mounted on a strong tripod to remain stationary during photography of the data set's consecutive images.
(2) Images differ only by quantum noise: Images of 13 different static objects with different colors have been captured. These objects include buildings, plants, tables and chairs, cars, and people with closed eyes. The default quantum noise introduces a measurable difference between any two consecutive images, leading to independence of pixel values.
(3) External lighting conditions: The images have been captured at different intervals of the day, ranging from the time of the sun's baptism to the night.
(4) Camera settings and controlling it manually: There are several camera settings that can be adjusted to control aspects such as exposure, focus, depth of field, shutter speed, ISO, and white balance. Exposure is the amount of light allowed to enter the camera and is controlled by three parameters: ISO speed, aperture size, and shutter speed. ISO speed values can be 50, 100, 200, 400, 800, 1600, 3200, and 6400. A higher ISO, a more sensitive camera's sensor, allows for photography in low-light conditions, but it can also add digital noise to the image. Aperture size determines the amount of light that enters the camera and affects the depth of field, or how much of the scene appears in focus. A larger aperture lets in more light, which can reduce image noise but produce a shallower depth of field, while a smaller aperture lets in less light but produces a deeper depth of field. Shutter speed controls the duration of time that the camera's sensor is exposed to light. A rapid shutter speed requires a higher ISO setting, which leads to more noise in the image. In addition to that, a rapid shutter speed freezes motion in the scene, while a slow shutter speed creates motion blur. ISO speed, aperture size, and shutter speed are related to each other and construct, in combination, what is called an exposure triangle. Finding the right exposure triangle is the key to capturing high-quality images.
   In this experiment, the camera setting's indicator has been turned to mode (M). The aperture size, ISO speed, and shutter speed are adjusted to vary between numbers (5.6, 8, 11), (100, 200, 400, 800), and (100, 125, 200, 250, 320, 500, 1000), respectively. In one shot at each exposure triangle, ten consecutive images of the same scene have been captured. i.e., at the aperture size (APER) of 5.6, the ISO speed was set to 100, and the shutter speed was set to 100. After that, for the same aperture and ISO values, the shutter speed was set to 125 and so on until up to 1000, and again, ten consecutive images were captured per exposure triangle. Then, at the same aperture size value, the ISO speed was changed to 200, and the shutter speed was changed again from 100 up to 1000. The ISO speed was changed until 800 for the same aperture size of 5.6, and in each iteration, the shutter speed was changed from 100 up to 1000. Again, the same procedures were repeated for the aperture sizes of 8 and 11. The different combinations of these settings for the 13 different objects are summarized in Table 1. Setting up the camera settings can be abbreviated as follows:
   a) The aperture size ranges from large to small, and the amount of light that enters the lens decreases. The aperture size of 5.6 lets in twice as much light as the aperture size of 8.
   b) The ISO speed value ranges from low to high. The ISO speed value of 100 allows the camera to capture less light than the ISO speed value of 200, which allows the camera to capture less light than the ISO speed value of 400. The most light is captured in the case of the ISO speed value of 800.
   c) The shutter speed ranges from slow to fast.

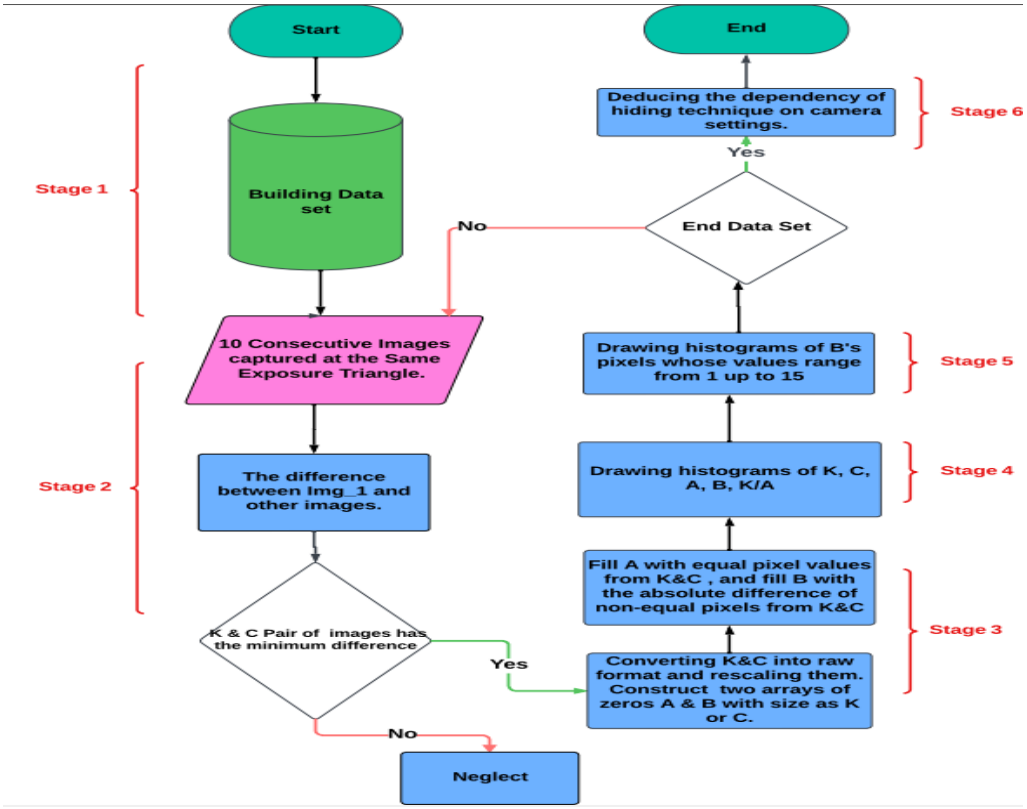

Fig.4 Stages of the proposed study.

Table (1): the camera's settings at which the different objects have been photographed (APER=5.6, 8, 11)

Shutter	ISO			
100	√	√	√	√
125	√	√	√	√
200	√	√	√	√
250	√	√	√	√
320	√	√	√	√
500	√	√	√	√
1000	√	√	√	√

2.1.2 Selection of Two Cover Images

In this phase, the selection of the two cover images K and C for the SWEM algorithm to construct their stego-image is performed based on the minimum difference between them. For the same exposure triangle, every ten consecutive images have been numbered according to the photography process. i.e., the first image has been numbered as Img_1, and the last image has been numbered as Img_10. The difference between Img_1 and the rest of the ten images was calculated. i.e., (Img_1 minus (Img_2, Img_3,..., Img_10)). The pair of images with the minimum difference is selected as a pair of cover images and named K and C.

2.1.3 Construction of A and B Arrays

For every exposure triangle, the two selected images, K and C, have been converted into raw format, a one-layer image, and re-scaled linearly to a gray-scale of 0 to 255. Two arrays A and B of the same size as those of K or C have been created with zero values. The two selected images have been scanned and compared pixel by pixel. In the case of equality, K's pixels have been assigned to A's pixels at the same K's pixels' indices. Whereas in the case of non-equality, the absolute difference between those pixels has been assigned to B's pixels at the same K's pixels' indices as described by Eq. (1).

$$\mathrm{A}||\mathrm{B}(m,n) = \begin{cases} \mathrm{A}(m,n) = \mathrm{K}(m,n) \;\; if \;\; \mathrm{K}(m,n) = \mathrm{C}(m,n) \\ \mathrm{B}(m,n) = mod\big(\mathrm{K}(m,n) - \mathrm{C}(m,n)\big) if \;\; \mathrm{K}(m,n) \cong \mathrm{C}(m,n) \end{cases} \quad (1)$$

2.1.4 Drawing Histograms

A histogram is a graphical representation of the distribution of numerical data. It is composed of bars, with each bar's height representing the frequency (count) of data points within a specific range of values. Histograms are valuable because they provide a clear visual summary of the distribution of data. In this phase, the histograms of the two selected cover images, K and C, and the array A have been drawn in one figure. In addition to that, histograms of the array B, and the result of the division of K by A, have also been drawn in separate figures.

2.1.5 Drawing Histogram of some B's Pixels

In this phase, the histogram of pixels of B whose values range from 5 up to 15 has been drawn in another separate figure where the ratio of the number of pixels that are not identical in K and C and have an absolute difference ranging from 1 up to 15 to the total number of non-equal pixels has been shown. This ratio is cummtatively calculated.

3. Results and Discussion

MATLAB R2016b has been used for simulation and demonstration of the proposed model. The algorithms that simulate the proposed model have been written and applied to the images that have been captured with the camera settings that are described in Table 1. Every time the algorithm has been executed, among the ten consecutive images, a pair of images K and C that has a minimum difference has been selected as input for the algorithm. For example, for the two objects 1 and 13 at an exposure triangle with an aperture size of 5.6, an ISO speed of 100, and a shutter speed of 100, the mean difference between Img_1 and images (Img_2, Img_3,..., Img_10) is shown in Fig. ٥. The histograms of K (Img_1), C (Img_2), and A are shown in Fig.6. The histogram of the division of K by A is shown in Fig.7. In addition to that, the histograms of B and the pixels of B whose values range from 1 up to 15 are shown in Fig.8.

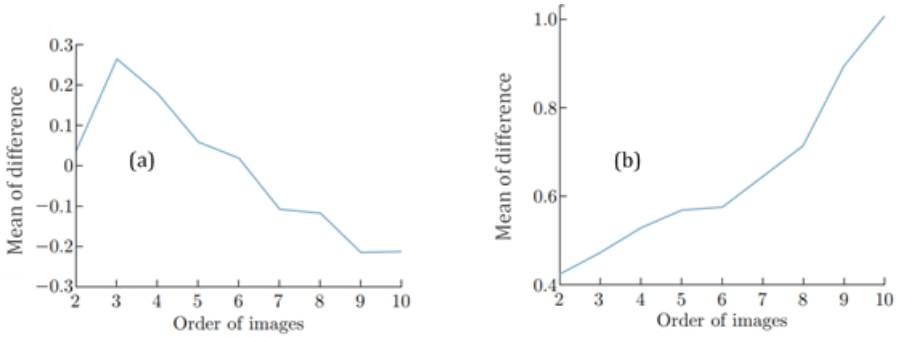

Fig. 5 Mean of difference between Img_1 and Img_2, Img_3,……,Img_10) for (a) object 1 and (b) object 13. In (a), (Img_1, Img_9) has a minimum difference. In (b), (Img_1, Img_2) has a minimum difference (APER:5.6; ISO:100; Shutter speed:100).

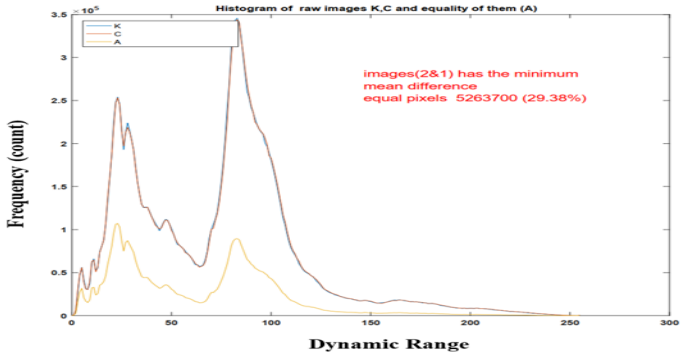

Fig.6. Histograms of K (Img_1), C (Img_2), and A (APER:5.6; ISO:100; Shutter speed:100).

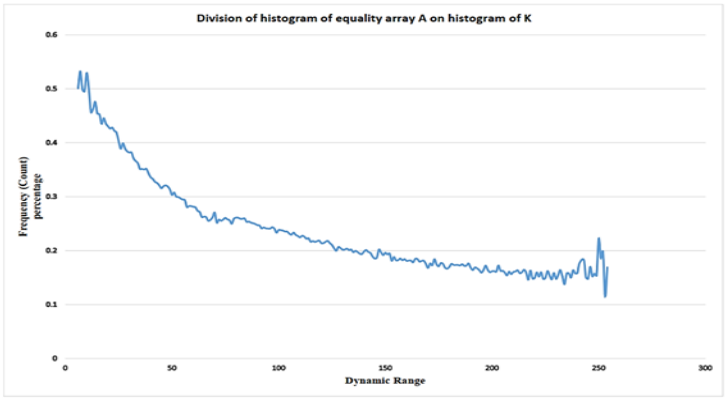

Fig.7. Division of histogram of A by histogram of K (APER:5.6; ISO:100; Shutter speed:100).

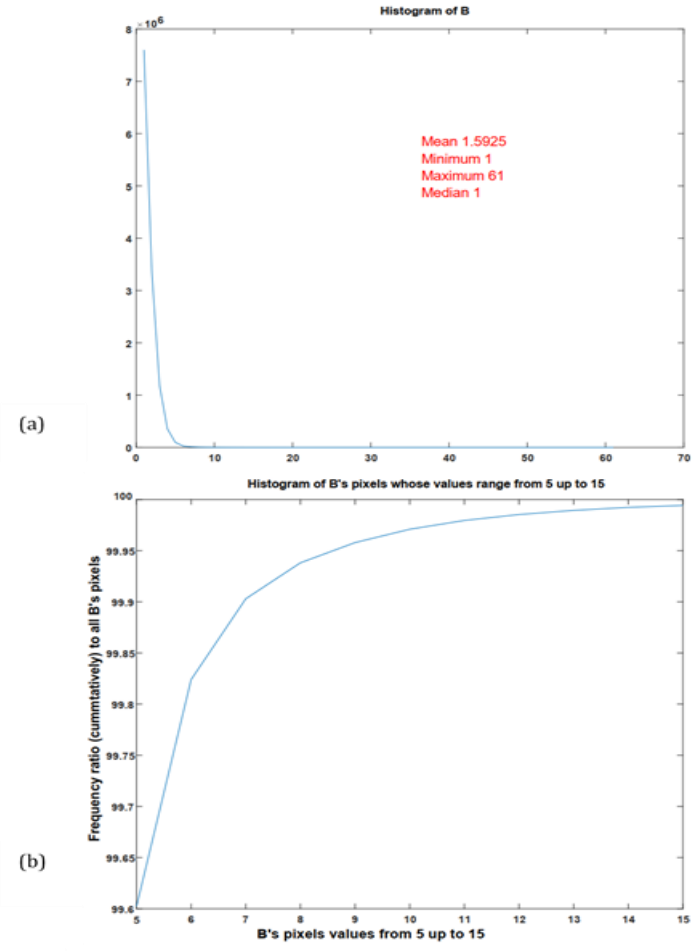

Fig.8. (a) Histogram of B pixels, (b) Histogram of B's pixels whose values range from 1 up to 15.

As Fig. 7 shows that the grey level value increases, the ratio of the histogram of the equality array A to the K's histogram decreases. This means that while the number of equal pixels decreases, the number of non-equal pixels increases. In other words, at the exposure triangle: aperture size 5.6, ISO speed 100, and shutter speed 100 the number of equal pixels decreases from 50% to 15% with an increase in the grey level value. In using the SWEM technique to build a stego-image, the probability of picking up a pixel from K or C image is 50%, according to the secret message bit, which is 0 or 1. Thus, there exists a high probability that a secret message bit equals 1 and *Ki=Ci* during the picking process, especially at the grey level values where the two images K and C have a ratio of equality of 50%. This already leads to a bit error at the extraction stage. Thus, it is essential to choose the two images K and C such that they have, as much as possible, the least percent of

equality between them per grey level value. Thus, the two images K and C that have the highest percent of non-equality pixels per grey level value are sufficient to build a stego-image that can be used to decode the secret message without bit error. Fig. 8 (b) shows the ratio of the number of pixels that are not identical in K and C and have an absolute difference ranging from 1 up to 15 to the total number of non-equal pixels. This ratio is cummtatively calculated. i.e., the ratio of the number of pixels that have an absolute difference ranging from 1 up to 5 to the total number of non-equal pixels is 99.6%, the ratio of the number of pixels that have an absolute difference ranging from 1 up to 6 to the total number of non-equal pixels is 99.825%, and so on until the ratio of the number of pixels that have an absolute difference ranging from 1 up to 15 to the total number of non-equal pixels is approximately 99.99%.

Figure. 9 (a, b, c, d) illustrates the ratio of the A array's histogram to the K's histogram for a single object from the used data set, and explains how this relates to the shutter speed value. It is noted from Fig. 9 that:

1- The aperture size and shutter speed, the two sides of an exposure triangle's, are constant. The only variable is the ISO speed value.
2- The ratio of the A array's histogram to the K's histogram decreases as the grey level value increases.
3- Decreasing the maximum starting value on the y-axis that the damping starts from. This indicates that the number of equal pixels in the two images K and C decreases, and consequently, the number of non-equal pixels increases as the ISO speed value is changed from 100 to 800. This, in turn, reduces the probability of bit error at the extraction stage.
4- During changing the ISO speed value from 100 to 800, the seven curves in the case of ISO 100, which were arranged from top to bottom as shutter 100 up to shutter 1000, were rearranged. As the ISO speed value is increased from 100 to 800, the amount of light that enters the camera increases at the same rate. i.e., when we double the ISO value, the amount of light also doubles, necessitating a 50% reduction in the exposure time. Unless the effect of the two random noise, the quantum (shot) and dark current noise, the re-arrangement must start as follows: sh 200, sh 250, sh 400, ..., sh 1000, sh 2000 in the case of ISO speed 200.
5- During changing the ISO speed value from 100 to 800, the seven curves approaches to each other.
6- The camera settings directly affect the sensor's noise, which directly affects the image itself, which in turn affects the performance of the SWEM algorithm during retrieving the embedded message.

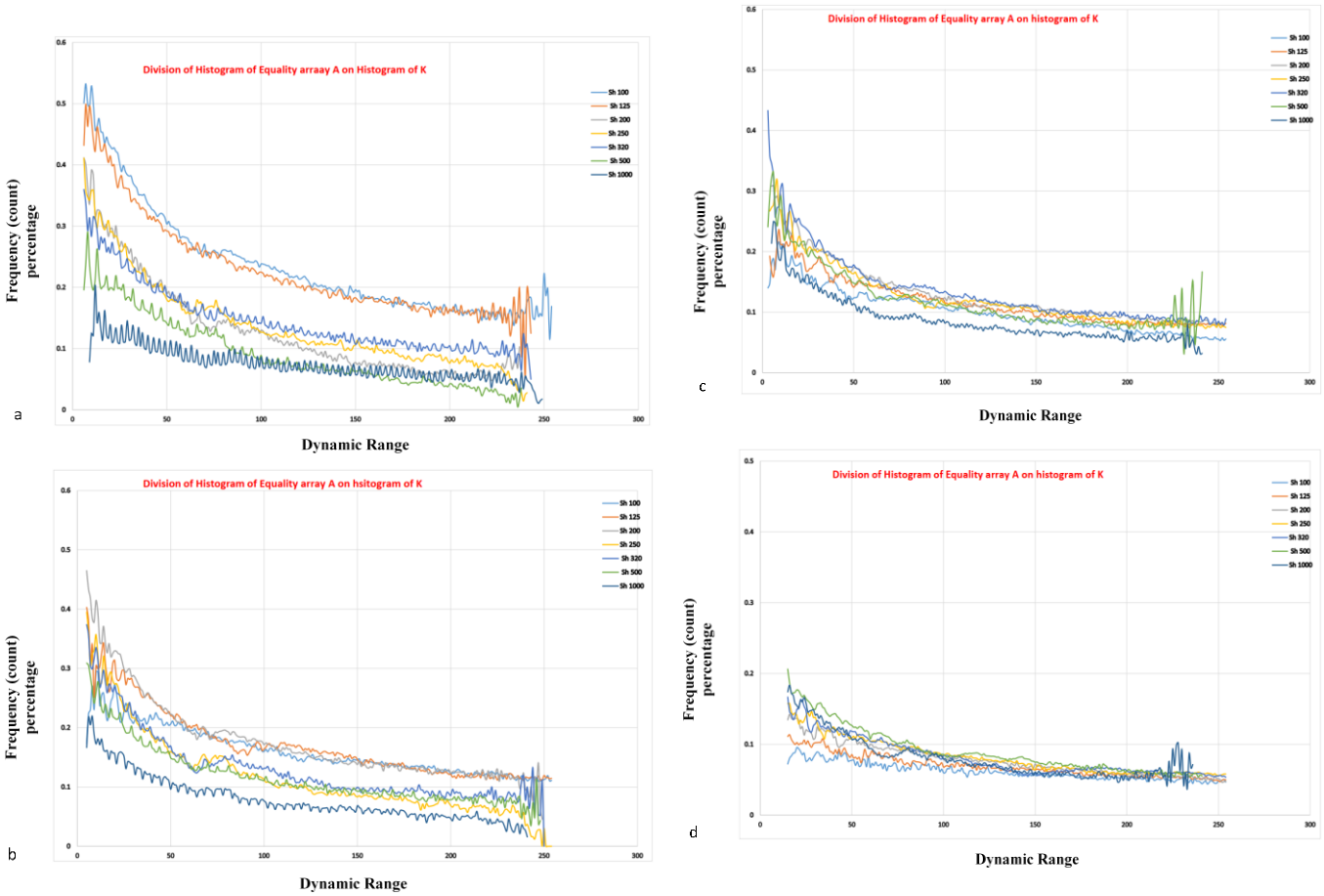

Fig.9. (a & b): The relation between the ratio of the histogram of the equality array A to the K's histogram, and shutter speed for the same aperture size and for (a) ISO 100, and (b) ISO 200. (c & d): The relation between the ratio of the histogram of the equality array A to the K's histogram, and shutter speed for the same aperture size and for (a) ISO 400, and (b) ISO 800.

Raising the sensitivity of the camera's sensor allows it to capture more photons, which in turn increases the interacting photons. This, in turn, leads to an increase in the interacting quantum efficiency, which is the ratio of interacting photons to incident photons and equals 60% in the visible light [22]. This finally leads to increasing the quantum noise level in the resulting image, which in turn increases the number of non-equal pixels in a two consecutively captured images. The built in random noise has a great effect on the performance of a steganography algorithm. To build an integrated image steganography technique capable of delivering imperceptibly a complete high-capacity secret messages with high security, we must consider the carrier image, how it has been formed, and what affects it.

4. Conclusion

Data hiding, particularly image steganography, is becoming an extensive field that attracts serious research interest. In the literature, there are several image steganography techniques, and each technique differs from the other, particularly in integrating the criteria of perfect performance. Often, there is a trade-off between these criteria. In order to build an integrated image steganography technique capable of delivering imperceptibly a complete high-capacity secret messages with high security, we must consider the carrier file (image), how it has been formed, and what affects it. But most researchers in the field of image steganography are indifferent to the image's origin and the camera settings that directly affect the image itself. They often design their algorithms by considering the image as one array of pixels or a combination of three color channels. In this paper we have addressed this issue by studying the relationship between camera settings and quantum noise level in an image, as well as its effect on, for example, the SWEM algorithm. It is noticed that raising the sensitivity of the camera's sensor allows it to capture more photons, which in turn increases the interacting photons. This, in turn, leads to an increase in the interacting quantum efficiency, which is the ratio of interacting photons to incident photons. This finally leads to increasing the quantum noise level in the resulting image, which in turn increases the number of non-equal pixels in a two consecutively captured images, as a result of that the SWEM algorithm will able to embed and transmit a high-capacity secret message and finally decode it without bit error. In the end, to satisfy the criteria of performance for a single image steganography algorithm, we must consider the carrier file (image), how it has been formed, and what affects it. To check the generalizability of the proposed study, further research entails applying it to more case studies of image steganography algorithms.

Acknowledgment

The authors would like to thank Fayoum University for supporting the publication of this work.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] G. Traverso, J. Lavoie, A. Martin, H. Zbinden, Perfectly secure steganography: Hiding information in the quantum noise of a photograph, Physical Review A 93(1) (2016).
[2] M. Hussain, A.W.A. Wahab, Y.I.B. Idris, A.T. Ho, K.-H. Jung, Image steganography in spatial domain: A survey, Signal Processing: Image Communication 65 (2018), 46-66.
[3] B. Li, J. He, J. Huang, Y.Q. Shi, A survey on image steganography and steganalysis, Journal of Information Hiding and Multimedia Signal Processing 2(2) (2011), 142 - 172.
[4] K. Bailey, K. Curran, An evaluation of image based steganography methods, Multimedia Tools and Applications 30(1) (2006),55-88.
[5] A. Westfeld, G. Wolf, Steganography in a Video Conferencing System, International Workshop on Information Hiding 1525 (1998), 32-47.
[6] A.S. Ansari, M.S. Mohammadi, M.T. Parvez, A Comparative Study of Recent Steganography Techniques for Multiple Image Formats, International Journal of Computer Network and Information Security 11(1) (2019), 11-25.
[7] I.J. Kadhim, P. Premaratne, P.J. Vial, B. Halloran, Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research, Neurocomputing 335 (2019), 299-326.
[8] M. Hashim, M.S. Rahim, IMAGE STEGANOGRAPHY BASED ON ODD/EVEN PIXELS DISTRIBUTION SCHEME AND TWO PARAMETERS RANDOM FUNCTION, Journal of Theoretical and Applied Information Technology 95(22) (2017), 5977-5986.
[9] M. Bachrach, F.Y. Shih, Image steganography and steganalysis, Wiley Interdisciplinary Reviews: Computational Statistics 3(3) (2011), 251-259.
[10] S. Manoharan, An Empirical Analysis of RS Steganalysis, 2008 The Third International Conference on Internet Monitoring and Protection, Bucharest, Romania, 2008, pp. 172-177.
[11] K. Karampidis, E. Kavallieratou, G. Papadourakis, A review of image steganalysis techniques for digital forensics, Journal of information security and applicatios 40 (2018), 217-235.
[12] M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: a survey, Computer Science Review 13 (2014), 95-113.
[13] L.M. Marvel, C.T. Retter, C.G. Boncelet, A methodology for data hiding using images, *IEEE Military Communications Conference*, IEEE, 1998, pp. 1044-1047.
[14] H. Mathkour, B. Al-Sadoon, A. Touir, A new image steganography technique, *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, IEEE, china, 2008, pp. 1-4.
[15] A.A.J. Altaay, S.B. Sahib, M. Zamani, An Introduction to Image Steganography Techniques, *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, IEEE, Kuala Lumpur, Malaysia, 2012, pp. 122-126.
[16] S. Rahman, J. Uddin, M. Zakarya, H. Hussain, A.A. Khan, A. Ahmed, M. Haleem, A Comprehensive Study of Digital Image Steganographic Techniques, *IEEE Access* 11 (2023), 6770-6791.
[17] R. Zaheer, R.S. Gaur, V. Dixit, A literature survey on various approaches of data hiding in images, (2017).
[18] G. Maji, S. Mandal, S. Sen, N.C. Debnath, Dual image based LSB steganography, Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), 2018 2nd International Conference on, IEEE, 2018, pp. 61-66.
[19] D. Gardner, Characterizing digital cameras with the photon transfer curve, *Summit imaging (undated document supplied by Jake Beverage* (2012).

[20] H.T. Hytti, Characterization of digital image noise properties based on RAW data., ELECTRONIC IMAGING 2006, SPIE, San Jose, California, United States, 2006, pp. 86-97.
[21] U. Jain, Characterization of CMOS image sensor, Mathematics and Computer Science, *Delft University of Technology*, 2016, p. 90.
[22] J.R. Janesick, *Photon transfer*, SPIE press2007.
[23] D.R.I.M. Setiadi, PSNR vs SSIM: imperceptibility quality assessment for image steganography, Multimed Tools Appl 80 (2021), 8423-8444.
[24] A. Gutub, A. Al-Qahtani, A. Tabakh, Triple-A: Secure RGB image steganography based on randomization, 2009 IEEE/ACS International Conference on Computer Systems and Applications, Rabat, Morocco, 2009, pp. 400-403.
[25] M.T. Parvez, A.A.A. Gutub, RGB Intensity Based Variable-Bits Image Steganography, 2008 IEEE Asia-Pacific Services Computing Conference, IEEE, Yilan, Taiwan, 2008, pp. 1322-1327.
[26] J. Mielikainen, LSB matching revisited, IEEE Signal Processing Letters *13*(5) (2006) 285-287.
[27] S. Sarreshtedari, & Akhaee, M. A, One-third probability embedding: a new±1 histogram compensating image least significant bit steganography scheme, *IET image processing* 8(2) (2014), 78-89.
[28] X.S. H. Yang, and G. Sun,, A high-capacity image data hiding scheme using adaptive LSB substitution, Radioengineering 18(4) (2009), 509–516.
[29] C.C. Chang, T.D. Kieu, Y.C. Chou, Reversible Data Hiding Scheme Using Two Steganographic Images, TENCON 2007 - 2007 IEEE Region 10 Conference, IEEE, Taipei, Taiwan, 2007, pp. 1-4.
[30] M.R. Abdeltawwab, S.A. Taie, H.H. El-Bahnasawy, A. Eissa, Novel Steganalysis Method for Stego-Images Directly Constructed from Color Images Based on Their Quantum Noise, Journal of Shanghai Jiaotong University (Science) (2024).
[31] H. Motamedi, A. Jafari, A new image steganography based on denoising methods in wavelet domain, 2012 9th International ISC Conference on Information Security and Cryptology, IEEE, Tabriz, Iran, 2012, pp. 18-25.
[32] S. Sidhik, S. Sudheer, V.M. Pillai, Performance and analysis of high capacity steganography of color images involving wavelet transform, Optik-International Journal for Light and Electron Optics 126(23) (2015), 3755-3760.
[33] A.A. Abdelwahab, L.A. Hassaan, A discrete wavelet transform based technique for image data hiding, 2008 National Radio Science Conference, IEEE, Tanta, Egypt, 2008, pp. 1-9.
[34] Y. Taouil, E.B. Ameur, M.T. Belghiti, New Image Steganography Method Based on Haar Discrete Wavelet Transform, Europe and MENA Cooperation Advances in Information and Communication Technologies. Advances in Intelligent Systems and Computing, Springer, Cham, Felgueiras, 2017, pp. 287-297.
[35] V. Kumar, D. Kumar, Performance evaluation of DWT based image steganography, 2010 IEEE 2nd International Advance Computing Conference (IACC), IEEE, Patiala, India, 2010, pp. 223-228.