REPUBLIC OF TÜRKİYE
KIRŞEHİR AHİ EVRAN UNIVERSITY
INSTITUTE OF NATURALAND APPLIED SCIENCES
DEPARTMENT OF ADVANCED TECHNOLOGIES

ENHANCED DATA HİDİNG USİNG SOME ATTRİBUTE OF COLOR IMAGE

THULFIQAR MUAYAD HAMEEDI

MSc THESIS

KIRŞEHİR
2023

REPUBLIC OF TÜRKİYE
KIRŞEHİR AHİ EVRAN UNIVERSITY
INSTITUTE OF NATURALAND APPLIED SCIENCES
DEPARTMENT OF ADVANCED TECHNOLOGIES

ENHANCED DATA HİDİNG USİNG SOME ATTRİBUTE OF COLOR IMAGE

THULFIQAR MUAYAD HAMEEDI

MSc THESIS

SUPERVISOR

ASS. PROF. DR. GÜLSÜM AKKUZU KAYA

KIRŞEHİR

2023

KIRŞEHİR AHİ EVRAN UNIVERSITY

GRADUATE SCHOOL OF SCIENCE

MSc THESIS

ETHICS DECLARATION

In this thesis study, which I have read and understood the Kırşehir Ahi Evran University Scientific Research and Publication Ethics Directive and which I have prepared in accordance with the Kırşehir Ahi Evran University Institute of Science Thesis Writing Rules;

● I have obtained the data, information and documents I have presented in the thesis within the framework of academic and ethical rules,

● I present all information, documents, evaluations and results in accordance with scientific ethical rules,

● I have cited all the works I have benefited from in the thesis by making appropriate references,

● I have not made any changes in the data used and the results,

● This study, which I have presented as a thesis, is original,

Otherwise, I declare that I accept all legal actions to be taken against me in this regard and all loss of rights that may arise against me. ...../……./20….

Student

Thulfiqar Muayad Hameedi

LIST OF CONTENTS

Page No

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to:

With immense pleasure and deep sense of gratitude, I wish to express my sincere thanks to my supervisors Ass. Prof. Dr. Gülsüm AKKUZU KAYA without their motivations and continuous encouragements, this research would not have been successfully completed.

Last but not the least, I wish to extend my profound sense of gratitude to my family for all the sacrifices and their prayeries they made during my research and also providing me with financial, moral support, and encouragement whenever required.

August, 2023 Thulfiqar Muayad Hameedi

ÖZET

YÜKSEK LİSANS TEZİ

RENKLİ GÖRÜNTÜNÜN BAZI ÖZELLİKLERİNİ KULLANARAK GELİŞMİŞ VERİ GİZLEME

Thulfiqar Muayad Hameedi

KIRŞEHİR AHİ EVRAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
İLERİ TEKNOLOJİLER ANABİLİM DALI

Danışman: **Dr. Öğr. Üyesi Gülsüm AKKUZU KAYA**
Yıl: 2023 Sayfa: 88
Jüri: **Dr. Öğr. Üyesi Gülsüm AKKUZU KAYA**
Dr. Öğr. Üyesi Mehmet Servi
Doç. Dr. Mustafa YAĞCI

Görüntüler, insanlar arasındaki yazışmalarda en çok kullanılan multimedyaöğelerinden biridir. Bunun sebeplerinden biri, görüntülerin bazı özelliklerinin önemlimesajları gizlemek için kullanılabilir olmasıdır. Mesaj gizleme yöntemi kullanılangörüntünün özelliklerine bağlı olarak değişim gösterir çünkü her görüntünün farklıözellikleri vardır. Verileri hırsızlığa karşı korumak, hassas bilgilerin tahribini önlemek veverinin güvenliğini korumak amacıyla farklı araçlar ve teknikler geliştirmek ihtiyaç halinegelmiştir. Bu tezde, görüntüler üzerinde şifreleme teknikleri uygulanarak verilerin veverinin sahipliğini korunması hedeflenmektedir. En az anlamlı bit tekniği kullanılarak gizlimesajın bitleri değiştirildi. Histogram tekniği ile veri üzerinde frekans dağılımlarıincelenerek verinin gizleme işlemi öncesi ve sonrası durumu karşılaştırıldı. Benzerçalışmalar ile bu çalışma karşılaştırılarak tezin güçlü yönleri ve eksik yönleri tartışıldı Yapılan deneylerde, noktanın iki bölüme ayrıldığı görüntülerde 500'den fazla karakter kullanılmıştır. Bu algoritma, gizlenebilecek veri hacmini artırma, yazılı metni hatasız alma olasılığı ve içeriğini almadan önce görüntünün bütünlüğünü sağlamak için daha yüksek bir güvenilirlik derecesi gibi avantajlara sahiptir. Bulgular, dahil etmeden önce bir şifreleme işleminin önemini göstermektedir, çünkü yetkisiz taraf dahil etme sürecinde kullanılan yöntemi bilebilirse, şifreleme sorunu ile karşılaşılacak ve bu bilgilerin güvenliği artırılacaktır.

Anahtar Kelimeler: dijital görüntüler, mesaj gömme, steganografi, şifreleme, bilgi gizleme, güvenlik, görüntü kodlama.

ABSTRACT

MASTER'S THESIS

ENHANCED DATA HİDİNG USİNG SOME ATTRİBUTE OF COLOR IMAGE

Thulfiqar Muayad Hameedi

KIRŞEHİR AHİ EVRAN UNIVERSITY
GRADUATE SCHOOL OF SCIENCE
DEPARTMENT OF ADVANCED TECHNOLOGIES

Supervisor:	**Ass. Prof. Dr. Gülsüm AKKUZU KAYA**
	Year: 2023 Pages: 88
Juries:	**Ass. Prof. Dr. Gülsüm AKKUZU KAYA**
	Ass. Prof. Dr. Mehmet Servi
	Ass. Dr. Mustafa YAĞCI

Images are one of the most used multimedia elements in correspondence between people. One of the reasons is that some features of images can be used to hide important messages. Message hiding method varies depending on the features of the image used because each image has different features. It has become a necessity to develop different tools and techniques in order to protect data against theft, prevent the destruction of sensitive information and protect the security of data. In this thesis, it is aimed to protect the ownership of data and data by applying encryption techniques on images. The bits of the hidden message were changed using the least significant bit technique. By examining the frequency distributions on the data with the histogram technique, the situation of the data before and after the hiding process was compared. By comparing this study with similar studies, the strengths and weaknesses of the thesis were discussed. In the experiments, more than 500 characters were used in the images in which the dot was divided into two parts. This algorithm has the advantages of increasing the volume of data that can be hidden, the possibility of error-free retrieval of written text, and a higher degree of reliability to ensure the integrity of the image before retrieving its contents. The findings show the importance of an encryption before inclusion, because if the unauthorized party knows the method used in the inclusion process, the encryption problem will be encountered and the security of this information will be enhanced.

Keywords: digital images, embedding message, Steganography, encryption, information concealment, security, image coding.

LIST OF TABLE

Page No

LIST OF FIGURE

Page No

LIST OF ABBREVIATIONS

Abbreviations		Described
LSB	:	Least Significant Bit
PSNR	:	Peak Signal Noise Ratio
RGB	:	Red, Green, Blue
DRM	:	Digital rights management
HVS	:	High Vaginal Swab
OCR	:	Optical Character Recognition
XOR	:	Exclusive OR
DNA	:	Deoxyribonucleic acid

1. INTRODUCTION

Steganography techniques utilize inaudible communication on unsecured channels to conceal sensitive data among other digital content, making it difficult, if not impossible, for a third party to decipher the information (Ahmed S. Abdullah , 2015). Text, photos, sounds, and moving pictures can all be used to create covers. Pictures are frequently used as a cover to conceal information because they contain a great deal of data and modifying individual bits has little effect on the clarity of the finished image. Due of the versatility with which secret data can be transmitted, the robustness of a steganographic system is greatly dependent on the nature and kind of the images employed as well as the steganographic procedures. While it is unlawful to share certain photographs, such as those shot with the Julia Set, others are not (Hazim Noman and noor Hasan, 2018).

There are three components to a steganography system, according to Nada Qasim and Mohammed (2018): the concealed message, the cover media used to conceal the message within it, and the stego-cover used to conceal the steganography itself (1-1).

No one should be able to view the contents of the cover. Checking the visual or aural data of the original image and its counterpart with embedded data is one method for detecting this imperceptibility. It can also be expressed mathematically as a relationship between the steganographic cover and the authentic cover.

It is feasible to employ steganographic techniques in either the spatial or infrequency domain. Before embedding a hidden message into a cover medium, frequency domain techniques alter the message in a certain way. Without any preprocessing, the secret data is integrated directly into the cover using spatial domain methods. (2018) Nada Qasim and Mohammed both.

Figure (1-1): information hiding (Ahmed, 2015)

According to Younis (2018), the digital image is composed of pixels, which are picture elements, organized in a two-dimensional array of integers that depict varying levels of light intensity. A variety of image kinds exist, encompassing binary, gray, color, and multispectral images. For example, it has been noted that every pixel inside an RGB color image is represented by a 24-bit binary integer, where each color component is allocated 8 bits (Al-Saif & Abdullah, 2013).

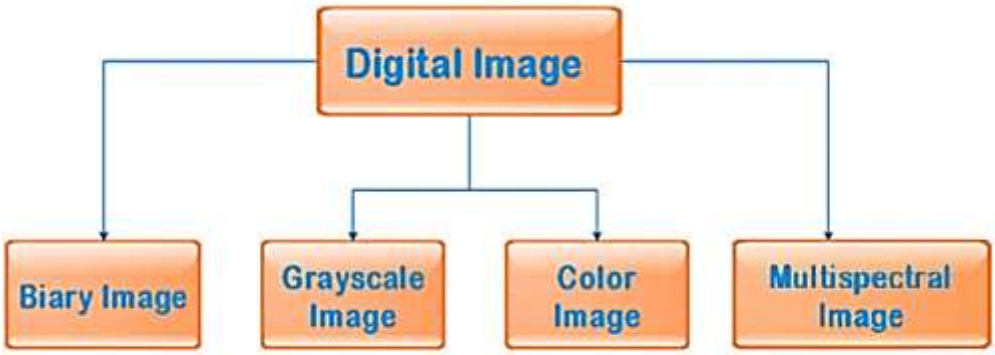


Figure (1-2): Types of Digital Images (Ahmed, 2015).

1.2 The Importance Of This Work

The significance of this study is in the examination of concealment and encryption techniques, which are employed in distinct manners to ascertain the integrity and trustworthiness of data. In the context of encryption, it is possible for any entity to ascertain if two parties are engaged in a secure and encrypted communication. The act of concealing information inherently involves the suppression of communication. The covert exchange of messages between two parties through communication channels is imperceptible to observers.

The significance is in its ability to enhance the reliability of verifying the integrity of an image prior to accessing its contents. Furthermore, the incorporation of data into the image in a random manner enhances its security and makes it more resistant to extraction by malicious individuals.

The practice of data concealment is highly advantageous, particularly in situations where the act of transmitting encrypted messages may give rise to suspicion, such as in countries where freedom of expression is suppressed. In these contexts, images are commonly

circulated, while the information contained within them is covertly concealed and decrypted using a specific algorithm.

In this study, the successful comprehension of the embedded message enables the complete restoration of the original image. The cryptosystem exhibits a high level of resistance against cryptographic attacks due to the availability of a substantial key space.

1.3 Research Objectives

The primary aim of this thesis is to discover a novel method for concealing various types of text files within color photos, while ensuring that no discernible modifications or distortions are obvious in the image data following the concealment process. Additionally, the proposed approach should be resistant to detection by spambots. The objective is to extract the concealed message from the picture in its entirety, without any loss or distortion of its contents, and without relying on the original image as a reference. To validate the effectiveness of the proposed method, various measures are employed to assess the accuracy of the concealment and ensure the successful identification of the hidden text within the image.

The objective of this work :

1. Enhancing the protection and safety of the secret that is concealed in the colorful or grey images.

2. Adding safety data for verification to confidential data, so that any change in the confidential message through transmission between the sender and the recipient is discovered.

3- Calculating the image jamming with confidential data via the method used and thus help us to know the image's ability to hide it for the text hidden inside it.

4- The inclusion process, if preceded by an encryption process, is stronger because if the unauthorized party is able to know the method used in the inclusion process, the encryption problem is encountered and the security of this information is increased.

1.4 Research Methodology

In this study, a new algorithm is discussed through texts that are included in all types of images. This algorithm relies on embedding data directly within the image. The experiments conducted used more than 500 characters within images where the point is divided into two sections. This algorithm has the advantage of increasing the volume of data that can be hidden, the possibility of retrieving the written text without errors, as well as giving a higher degree of reliability to ensure the integrity of image before retrieving its contents. The data within the image have been randomly embedded which has earned it higher security and resistance to extraction by saboteurs.

The new algorithm is compared with other algorithms and the results demonstrate the new algorithm's ability to hide and retrieve data, the high storage capacity and not being visible or detected by electronic methods.

2. LITERATURE REVIEW

2.1 Steganography

This chapter provides a comprehensive overview of the topic matter, including a discussion of its general background and an examination of relevant existing literature.
The proliferation of multimedia and online data applications in recent years has propelled steganography to the forefront of security and covert communication approaches.
The name "steganography" is derived from two Greek roots: "steganos," meaning "covered or confidential," and "graphic," meaning "writing or drawing" (Khalil Ibrahim & Alsaif Meaad, 2013). Steganography refers to the act of covertly embedding and transmitting data by utilizing a medium or carrier information. The entity in question is equipped with a mechanism for transportation, and both the entity itself and the recipient of the transported information are not exposed to any potential risks. According to Mamta Juneja and Parvinder Singh (2013), any doubts regarding the possible existence of the subject in issue have been resolved.
The differentiation between the two main categories of steganography lies in the inherent characteristics of the concealed information, with one category pertaining to linguistic aspects and the other category pertaining to technological aspects.

A. Linguistic Steganography

In this particular category, the text serves as the data carrier, commonly referred to as steganos. An ancient instance of linguistic obfuscation in ancient China involved the utilization of a specialized template for printing paper. This template featured precise perforations that served to differentiate the placement of covert words throughout the entirety of the text. To decipher the concealed message, the recipient was required to possess an identical template for the purpose of restoration (Suhaila, Shaymaa, Ghusoon, & Dhuha, 2017). In contemporary contexts, a notable illustration of this phenomenon may be observed through the utilization of tools provided by the website spammimic.com. These tools operate inside the realm of the internet, generating propaganda messages that serve as a façade for concealing covert communications. This practice is founded upon the premise that a significant portion of individuals tend to disregard or overlook the content of spam messages.

B. Technical Steganography

Regarding this particular category, the carrier data refers to any media found in nature, rather than being limited to textual information. One notable historical illustration of

complete concealing involves the utilization of invisible ink and microdots. One notable instance involves the practice of concealing information within graphics and music, as well as within executable files (exe) and other similar formats (Joshi, 2018).

According to Habeeb (2020), there exist two approaches for maintaining confidentiality. Firstly, the act of concealing objects in a discreet location with the intention of preventing their discovery by individuals other than those privy to its whereabouts.

Secondly, the act of arranging the visual characteristics of objects in a manner that renders them indistinguishable, except to individuals who possess knowledge of the specific technique employed to alter their original appearance.

Information hiding strategies utilize the initial approach to ensure the security of information, whereas cryptography approaches rely on the subsequent approach. The presence of a ciphertext has the potential to elicit suspicion, as the concealed information inside it is not readily apparent or easily discernible, hence mitigating the likelihood of arousing suspicion (Tom, Thomas, Jose, & Maria, 2015).

The term "Steganography" was coined in 1499 by Tritheism, who devised a method of encoding letters using religious vocabulary to transform covert communications into prayers with a comprehensible connotation. Steganography refers to the practice of concealing information within a medium, whereas cryptography pertains to the process of encoding information for the purpose of secrecy (Allen Tom, Anu V Thomas, Jerin Jose, Maria, 2015).

The field of information hiding techniques can be broadly categorized into two primary domains: steganography and watermarking.

Steganographic techniques operate based on the fundamental premise of concealing observation, so rendering entities fragmented, diminutive, and arduous to discern. This is achieved through the act of concealing information amidst an abundance of disparate data, thereby diverting attention away from the desired information. This practice is commonly referred to as the art of obfuscation, when information is covertly transmitted using inconspicuous and seemingly insignificant conduits, with the intention of concealing the presence of certain data. This technique involves the deliberate camouflage of information, rendering its existence concealed and imperceptible. According to Hussein, Ahmed, Sinan, Salam, and Jasim (2018), the presence of secret information is effectively concealed.

The field of steganography primarily concerns itself with concealing information, whereas digital watermarks are designed to simultaneously occupy the central area of the cover and provide supplementary information about it (Hussein, Ahmed, Sinan, Salam, & Jasim, 2018).

2.2 Literature Review

This section discusses several techniques for concealing information about digital images, including as color, picture type, and transform coefficients (KI Al-Saif, AS Abdullah, 2013).

In the year 2016, a cohort of researchers conducted an investigation on the influence exerted by digital color schemes on the process of data embedding, subsequently disseminating their discoveries through publication. In a study conducted by Ahmed Saadi Abdullah (2019), the impact of color layers on the concealment of information was assessed. This evaluation involved the utilization of nine different color systems and the application of the least significant bit technique, with the mean square error and peak signal-to-noise ratio serving as the evaluation metrics. A comparative study was conducted by other researchers to evaluate the effects of various color schemes on data obfuscation strategies. The study assessed the impact of color layers on the concealment of information through the utilization of five distinct color schemes and the least significant bit approach. The evaluation was conducted by measuring the mean square error, signal noise ratio, and peak signal noise ratio. A study was provided by other researchers, which focused on various tactics employed for the purpose of concealing information. These strategies encompassed techniques such as watermarking specific regions within an image and embedding data through the utilization of the least significant bit approach. It is possible to hide two images behind a single "cover" photo by manipulating the coefficients of the contourlet transform, employing a technique derived from the contourlet transform. Following the determination of the energy of the transform coefficients, the coefficients exhibiting the lowest energy are utilized. Additional research has been conducted involving book covers that use visual illustrations.

2.2.1 History of Steganography

The first use of the hiding system was recorded in the legendary stories of the Greeks. The historian Herodotus states that the commander Hastie’s shaved the head of one of his

trusted servants and tattooed on his head a message that disappeared after his hair grew. After the servant reached the intended destination, he shaved his head again to read the message. The aforementioned method was used by some German spies until the beginning of the twentieth century (Ahmed, 2015).

The narratives of Herodotus detail the account of Demeratus, the Greek king of Sparta, who provided a cautionary notice to the court regarding an impending assault by Xerxes, the Persian king. Demeratus employed a wooden tablet coated with wax as a medium for conveying the message. The inscription was engraved onto the tablet, which was subsequently concealed once more with wax, rendering the board seemingly devoid of any content.

In addition, alternative methods exist, such as concealing the attire of the hunter in a manner that does not arouse suspicion, as well as concealing the message within the cavity of animals, such as a wild rabbit. The Chinese employed unique techniques for transmitting communications, wherein the message was inscribed onto a piece of silk, tightly wound into a spherical shape, coated with wax, and discreetly concealed within the attire of the messenger (Deepali and Mamta, 2014).

In conjunction with various techniques employed since the first century AD, the utilization of invisible inks emerged as an additional strategy for concealing secret messages. This involved the practice of inscribing the covert message within the interstices of a non-secret message, employing said inks. Various substances, such as the juices derived from some fruits, milk, and vinegar, can serve as invisible inks. When subjected to heat, these inks undergo a darkening process, thereby rendering the letters of a concealed message apparent and legible (Mamta Juneja and Parvinder Singh, 2013).

Additional methods employed by the Germans encompassed alterations in letter height within the textual content, as well as the creation of minuscule apertures positioned either above or below the letters. Furthermore, the utilization of imperceptible inks facilitated the printing of diminutive dots in lieu of minute apertures on the letters (Suhaila & Shaymaa; Ghusoon and Dhuha, 2017).

Subsequently, the progression of chemical sciences facilitated the advancement of ink varieties, whereby chemical compounds possessing analogous attributes to traditional types were employed, hence enhancing precision and efficacy. During the First and

Second World Wars, secret military correspondences made use of them (Mamta Juneja and Parvinder Singh, 2013).

Among other techniques, the micro-film technique was used by the German photographer to enable the homing pigeon to carry a large amount of data without being detected. The use of this technique was the beginning of the use of the micro-dot which is a text or image that shrinks into a so small size that it is hardly visible to the naked eye. Those images or that text are reduced to a point, so they become unnoticeable to the observer or the opponent when they are transmitted through an unsafe path, and they are read by the receiver using a microscope. The micro dot has recently developed so that car manufacturers are sticking small numbers on the parts of cars using the micro dot to prevent them from being stolen (Hamid Mohammed and Zena Ahmed ,2018).

One more technique used during World War II was to send a hidden message inside another message that is not of importance, and this technique is based on the idea of filtering one of the letters of every word of the fake message to show the hidden message. An example is the famous message that was sent by the German spy in World War II as in (Ahmed, 2015):

Apparently, neutrals protest is thoroughly discounted and ignored Isman hard hit.
Blockade issue affects pretext for embargo on by products, ejecting suets and
vegetable oils.

By taking the second letter of each word, the message would be as follows (Ahmed, 2019):

Mount Sinai Medical School researchers applied a cutting-edge concealing technique. The Gene Coverage System was used to conceal data within the human DNA strand. This was accomplished by inserting programmed dot markers into the nucleus of the chromosome, joining the resulting strand with millions of others, and transmitting the entire construct. Specific dyes are applied to the entering strands, which are then examined under a microscope to decide which ones will be used to extract the necessary text (Ali Nasser and Entidhar Mhawes, 2017).

2.3 Terms in Steganography Techniques

The following terms are frequently used in steganography techniques :(Azal Habeeb,2020)

1. Cover - object (**C**): It is the host location for the secret message data.

2. Secret - message, (M): The secret message that will be hidden in the cover is called the Stego-message in the covered writing, and in watermarks it is called the Mark or the Watermark.

3. Stego - Key, (K): It is a shared key between two parties used to include and retrieve the secret message, and is also used to increase the degree of confidentiality. The hidden key used in the embedding process is symbolized by KE and the symbol KD for the hidden key is used in the retrieval process.

4. Stego - object, (**S**): It is the cover that contains the secret message and is the result of the concealment process.

5 . Embedding Process, (E): It is a function whose input is a Cover-object, a Secret-message and a Stego-Key, and whose output is a Stego-object (Ahmed Saadi, 2019) as shown in following equation:

$$\mathbf{E\ (c, m, k) = s} \qquad \mathbf{(2\text{-}1)}$$

6. Extracting Process, (D): It is a function to retrieve the secret message from the hide-element and the hide-key (Ahmed Saadi, 2019) as shown in following equation:

$$\mathbf{D\ (s, k) = m} \qquad \mathbf{(2\text{-}2)}$$

Some concealment techniques require the retrieval of the secret message to have the original cover as one of the inputs in addition to the concealment element and the concealment key (Ahmed Saadi, 2019) as shown in following equation:.

$$\mathbf{D\ (s, c, k) = m} \qquad \mathbf{(2\text{-}3)}$$

The coverage system can be represented using the following equation:

Cover_Object + Secret_Message + Stego_Key = Stego_Object

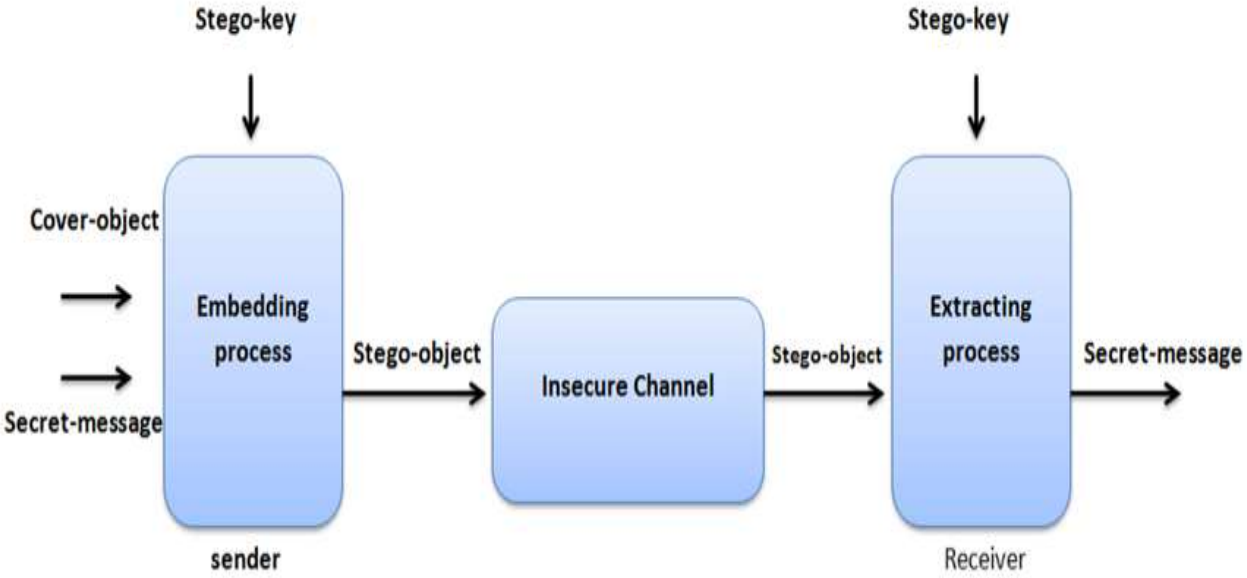


Figure (2-1): The general model of the coverage system (Azal, 2020).

2.4 Cover Types

There are several types of cover that can be used in steganography techniques, namely (Allen, 2015):

1-Text Files
2- Images Files
3- Audio Files
4-Video Files
5- Hard Disk Spaces
6 -Network Protocols
7- Software

2.5 Steganography Types

There are three basic types (**mechanisms**) of coverage systems shown in Figure (2-2), and this classification is based on encryption principles and the encryption key (Omar Younis Abdulhameed,2017)

.

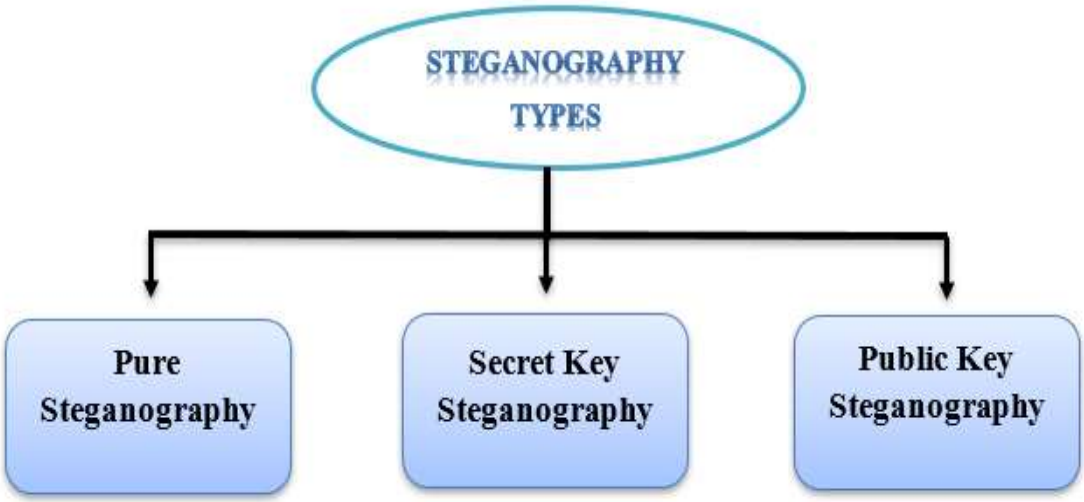


Figure (2-2): The main types of concealment.

1- Pure Steganography

The covering system that does not require a prior exchange of some confidential information such as the key-concealment is called pure concealment, and the inclusion process can be described according to the following formula (Dr. Yossra H & Ahmed. Y & Tayseer S. Atia ,2018) as show in following equation :

$$E: C \times M \longrightarrow C \qquad (2\text{-}4)$$

where

C: Cover possibilities group.
M: The set of probabilities of the secret message.

The process of extracting the message from the cover is as following equation:

$$D: C \longrightarrow M \qquad (2\text{-}5)$$

The loopback function D with property D (E (c,m)) = m for each m∈M , c ∈ C is called the pure concealment system, (Dr. Yossra H & Ahmed .Y & Tayseer S. Atia ,2018).

Pure concealment is considered to be one of the most pragmatic concealment strategies. The selection of the C group is based on its meaningfulness and widespread usage, enabling the involved parties to transmit information covertly and without arousing suspicion. Both sides possess the concealment function, denoted as E, as well as the retrieval function, denoted as D. The utilization of classical ciphers in conjunction with concealing techniques involves the integration of pure concealment methods, whereby the sender encrypts their message prior to the embedding procedure. The implementation of this particular procedure enhances the overall security of the communication process as it becomes challenging to decipher the encoded information under the cover (Dr. Yossra H & Ahmed. Y & Tayseer S. Atia, 2018).

2- Secret Key Steganography

The process bears resemblance to the Symmetric Encryption technique, wherein the sender selects a cover C and incorporates the confidential message within it through utilization of the secret key K. In order to successfully reverse the embedding process and extract the message, it is necessary for the recipient to possess knowledge of the key utilized, specifically KD = KE. Furthermore, it should be noted that none of the involved parties have knowledge of the password, rendering them incapable of accessing the confidential message. This method of secrecy is explicated by the equation presented in the work of Ali Nasser and Entidhar Mhawes (2017):

$$\mathbf{Ek: C \times M \times K \longrightarrow C\ M} \qquad \mathbf{(2\text{-}6)}$$

The general formula to retrieve the information is represented as follows equation:

$$\mathbf{Dk: C \times K \longrightarrow M\ M} \qquad \mathbf{(2\text{-}7)}$$

The loopback function D with the property Dk (Ek (c, m, k), k) = m fork$\in$K , m$\in$ M , c$\in$C is called the secret-key-hiding system (Khalil Ibrahim & Alsaif Meaad, 2013).

3- Public Key Steganography

The aforementioned concealment bears resemblance to Public Key Encryption, as it operates independently of the need to exchange a secret key. The concealing systems employ a dual-key mechanism, consisting of a public key and a private key. The public key is stored within a publicly accessible database and serves the purpose of facilitating

the embedding of a confidential message within the cover. Conversely, the private key is employed in the retrieval procedure of the aforementioned confidential message. This implies that the key employed throughout the embedding procedure is dissimilar to the key utilized during the retrieval procedure, denoted as KD ≠ KE. (Khan, Muhammad, Jamil, Haleem, & Muhammad, 2014).

2.6 Steganography Techniques

Many covered writing techniques have been proposed in recent years, most of which can be identified as substitution systems. They attempt to replace additional parts of the cover with a secret message. Recently, the development of new watermarking techniques has led to a progress in building high security and strong covered writing techniques. Therefore, some covered writing techniques that are currently used are very similar to the watermarking techniques (Hamid Mohammed and, Zena Ahmed ,2018).

There are many ways to classify concealment writing techniques. It can be classified according to the type of cover used in the embedding process (text concealment, image concealment, audio concealment, video concealment, executable file concealment, and network protocol concealment) or by modifications applied to the cover during the process of including the secret message. The last method is the one used for classification in this research, and steganography techniques are classified into (6) categories, which are: (Dr. Yossra H & Ahmed. Y & Tayseer S. Atia ,2018)

1- **Substitution Techniques**: These techniques replace parts of the covering with the secret message.
2- **Spread Spectrum Techniques**: Spread spectrum techniques include the secret message based on the spread spectrum techniques used in digital communications.
3- **Statistical Techniques**: The information are being ensured by changing some of the statistical properties of the cover.
4- **Distortion Techniques**: The information is ensured by distorting the signal and measuring the deviation from the original cover in the retrieval process.
5- **Cover Generation Techniques**: The information is ensured by creating a cover (Falih Hassan Owaid,2015).

2.6.1 Substitution Techniques

Making a slight change in the parts of multimedia is not perceived by human sensory means such as hearing and sight. Thus, this non-perception feature is taken as an

advantage to hide data in multimedia by replacing parts of the data of these media with the data to be hidden, as well as the advantage of the unused places from these media to hide the secret message (Kartik & Ashutosh & Tanay and Ashish Khanna ,2019).

1- Least Significant Bit

The substitution techniques in the binary cell are the least important of the commonly used and widespread concealment techniques, and this is due to the fact that its application is very easy. These techniques are characterized by high concealment ability (transparency) and large storage capacity. A large amount of information can be hidden with little cover effect and is relatively unaware. However, with its disadvantage, it is easy to be subject to attacks, for example, the process of converting an image from GIF or BMP format with a loss compressed format such as JPEG which leads to the destruction of the information hidden in the image using this technique (GeethaVani L K Sathya Suneetha S. Susmitha,2016).

When applying LSB technology to an image-type concealment, the least significant binary cell for some or all of the data of this image is replaced by one of the binary cells of the security message. When the color image has a representation (24-bit), a binary cell can be concealed in red, a binary cell in green and a binary cell in blue color, that is, one pixel hides three binary cells of the secret message. For example, in an image of size (600 *800), it is possible to hide (800 * 600 * 3 = 1,440,000 Bits) or (180,000 Bytes) of the secret message (GeethaVani L K Sathya Suneetha S. Susmitha,2016).

Suppose we have three light spots from a color image with a representation of 24 binary cells whose binary representation starts from the left as shown in Table (2-1):

Table (2-1): Three light spots from a color image

	Blue	***Green***	***Red***
The first light point	**11001000**	**11101001**	**00100111**
The second light point	**11101001**	**11001000**	**00100111**
The third light point	**11101001**	**00100111**	**11001000**

When the number 198 with binary representation includes 11000110 in the binary cell of least significance in the previous light points, the result is (Ahmed Saadi, 2019) as shown in table (2-2):

Table (2-2): The previous light points

	Blue	***Green***	***Red***
The first light point	**11001000**	**11101001**	**00100111**
The second light point	**11101001**	**11001000**	**00100110**
The third light point	**11101001**	**00100111**	**11001001**

The underlined binary cells are the only cells that have changed in the light points that were used in the concealing process, and the main benefit of the LSB technique is to hide a relatively large amount of information without noticing a noticeable change in the cover (Ahmed Saadi, 2019).

2- Unused or Reserved Space in Computer Systems

This space is used to hide confidential information. The way the operating system stores files on the hard disk is that it produces an unused space, this space is reserved for stored files, and the space resulting from the storage process is called Slack Space. For example, the operation system in Windows 95 organizes the Format of the hard disk using the Fat16 partition, and the size of the cluster is 32KB, which means that the smallest file gives a size of 32KB. A file whose size is 1KB, the operating system reserves 32KB of space for it, and the actual size used is 1KB, with the rest of the size being 31KB, and this space can be used to hide confidential information (Hamid Mohammed and, Zena Ahmed, 2018).

One more technique in the use of reserved spaces is the Files Header, such as images and audio files, and these techniques are considered inefficient due to the small size of these spaces and the ease of being detected.

3- Concealment in Unused Spaces in Network Protocols

Network protocols have properties that can be used to hide information, for example TCP/IP protocols contain unused or reserved spaces (Deepesh Rawat, Vijaya Bhanda, 2013). These spaces are exploited to hide confidential information.

There are three unused binary cells requirements in the IP Header that can be used to hide confidential information which are:

1. The two least important binary cells in the Type of Services field.
2. Don't Fragment (DF).
3. The TCP header contains 6 binary cells after the Header Length field, which can be used to hide confidential information (Kanar M. Sami,2019).

2.6.2 Spread Spectrum Techniques

Spread spectrum techniques are widely used today, especially in commercial and military communications. Modern concealing systems use these techniques to broadcast a secret narrow-band signal over a large-band (cover) signal.

The main benefit of using Spread Spectrum Techniques in overwriting is the power towards modifications and attacks against the cover. Since the hidden information is spread across the cover, it is difficult to completely remove that hidden information without completely destroying the cover. Spread spectrum techniques frequently use an audio file type cover (Sabah, 2016) .

2.6.3 Statistical Techniques

Statistical concealing techniques include information by changing some of the statistical properties of the cover and using Hypothesis Testing assumptions in the process of retrieving confidential information. In order to build a statistical concealing system, the cover is divided into a group of discrete blocks Bi of a certain size, and the block is modified if the binary value of the secret message is "1" until this changes the statistical properties of that block. However, if the binary value of the secret message is "0", then the block is left unaltered and a specific binary number is detected by the default check function F (Bi) that distinguishes modified blocks from unmodified blocks (Sabah A. Gitaffa,2016) as shown folloing equation .

$$F\ (Bi) = \begin{cases} Modified\ Block\ in\ the\ Process\ of\ Embedding \\ Unmodified\ Block\ in\ the\ Process\ of\ Embedding \end{cases} \quad (2\text{-}8)$$

Statistical concealing techniques are difficult to apply due to the difficulty of finding a good statistical function H (Bi) that distinguishes the modified and unmodified cover masses (Jinan, 2017).

2.6.4 Distortion Techniques

In comparison with substitution systems, jamming techniques require recognizing the original cover in the process of retrieving the secret message. The sender applies a series of modifications to the cover to hide the secret message, so this sequence of modifications is chosen in a way that is identical to the secret message. After that, the recipient begins measuring the differences between the message and the original cover in order to retrieve the secret message. Such kind of systems are not useful, because the recipient must reach the original cover, and if the hackers can access the covers, they can easily detect the modifications of the cover, and have the evidence that there is a secret communication (Al-Asadi, 2013).

Most obfuscation-type concealing methods are based on a text file-type cover, and among the widespread obfuscation techniques are (Dahoos, 2014):

1- Line - Shift Coding

This easy-to-implement method works by shifting lines up or down to a certain amount. This method is visible to the reader, that is, it can be easily detected by careful examination of the text. It can be broken by automatic measurements of the number of pixels between lines or by reshaping the text. By discovering the lines that have been removed, the hidden message can be known (Singh, 2015).

2- Word - Shift Coding

This method is similar to the previous one, except that the words are shifted horizontally to the right or to the left, and this shift depends on the binary cells (Bits) of the secret message. This method is more difficult to see than the previous method, but the spaces between the words must appear natural to prevent suspicion, as shown in Figure (2-3) (Srikanth. V,2016).

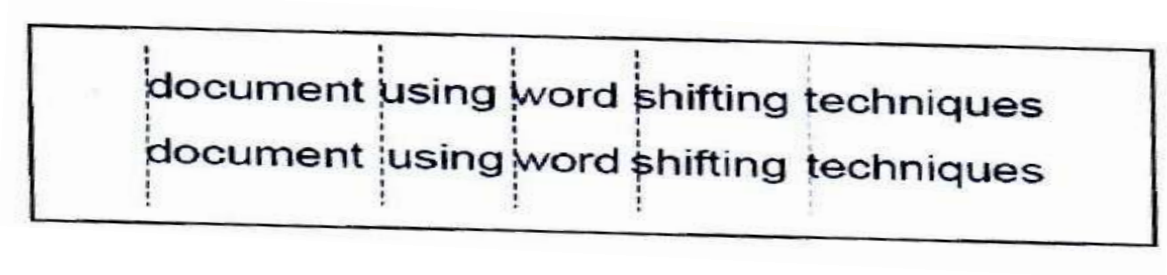


Figure (2-3): Word - Shift Coding.

2.6.5 Cover Generation Techniques

Unlike all the concealment methods that were presented previously, the confidential information is added to the cover through the implementation of the embedding algorithm. In addition, Cover Generation Techniques implement concealment by creating a digital material that is a cover in the concealment process of confidential communication. Examples of these techniques are: automatic production of English texts (Karthikeyan B, Asha S, Poojasree B,2019).

2.7 Hiding Data in Image

In the software of the computer, the image is represented as a matrix of luminous intensity values. The luminous intensity designates a point of light on the screen as a pixel. It is possible to represent each point of light using one binary cell (1bit), and represent it using one octet (8 bits) 1Byte and three octet blocks (3Bytes) (24 bit).

In the representation of (24 bits), the intensity of the illumination embodies the intensity of a color from the three main colors, red R, green G, and blue B. By merging the intensity of the three illuminations, the required color (RGB) is formed, and thus (2) 16,777,216 colors are provided. and the three-color ratios represent the true color of a point light on the screen. This representation is called True Color Representation (Jinan N. Shehab,2017).

Moreover, the values of the image matrix in the representation by using one octet block do not represent the true color values, but rather an entry for a site address in the Palatte (color palette) located in the header of the image file. Therefore, this representation is called the pseudo color representation. The number of entries in the color palette is 256 entries, thus providing (2) 256 colors in this representation. Thus, the organization of the color palette in color images in this representation does not depend on the sequence of color gradations on a regular basis. However, in gray images, the organization of the color palette is regular and has regular gray gradations which is regarded as one of the most important techniques used for concealing inside the image (Tawfiq A. Al-Asadi,2013).

2.7.1 Hiding in Least Signified Bit

This technique is one of the most well-known techniques and is characterized by ease of implementation, but it is more vulnerable to be attacked. In this method, the following characteristics on the image are noticeable:

A. True Color

The change of the least important cell for each color increases or decreases that color by one amount within the gradations of that color (256 color gradations), and this change cannot be perceived by the human eye (Zainb Bakar Dahoos,2014)،

B. Pseudo color

1. A Color Image: Due to the difference in the sequences of entries for the color palette, changing the least important binary cell of the image data leads to an increase or decrease in the value of the color palette input index by one amount. Thus, it another color is indicated which may be completely different from the original color, which in turn leads to the destruction of the original image and the distortion of its features. Figure (2-4) shows a color palette of a color image with representation (8bits) before and after concealing in one binary cell (Ashwini Palimkar, Dr.S.H. Patil,2014).

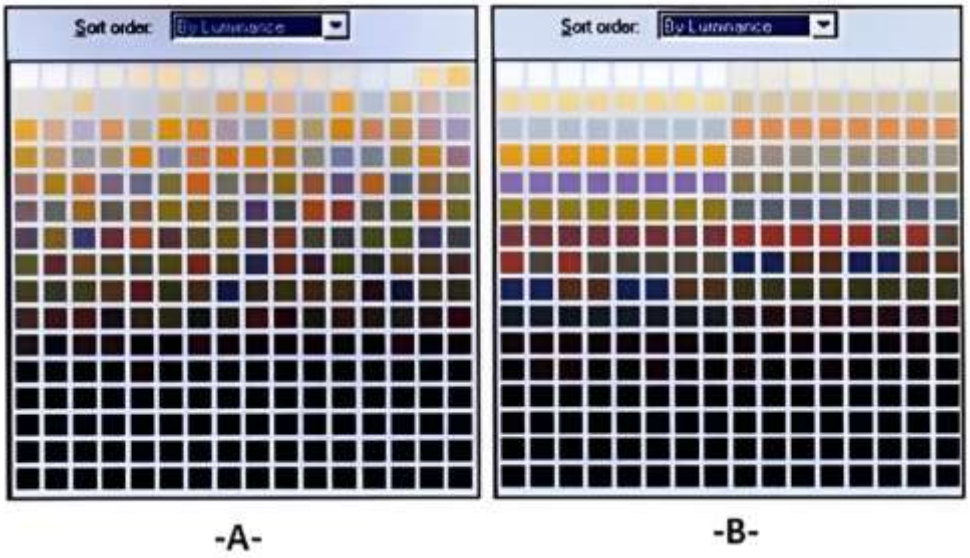


Figure (2-4): A color Palette of a Colored Image, A- before Concealing, B - After Concealing.

2. A Gray Image: Changing the least significant binary cell increases or decreases the value of the color palette input index by one amount, that is, shifting of one color in the color palette, and this change is imperceptible to the human eye (Alyaa Hasan Zwiad, 2018).

2.8 Watermark

It is an image recognizable by the pattern in the paper which shows different shades of light and darkness when seen in light (when viewed in reflected light or on a dark background), and is caused by differences in thickness or density of the paper in different

areas of it. There are two main ways to produce watermarks in paper; the winding process, or by using a more complex cylindrical mold (Ahmed Saadi Abdullah, 2019).

Watermarks vary greatly in their visible appearance. Although some of them are crystal clear, there are some that require greater study and observation. Banknotes, passports, postage stamps, and other papers frequently have watermarks applied as security features to deter forgery. A watermark is very useful in studying paper because it can be used to identify sizes, brands, locations and quality of paper (Qasim Mohammed, 2020). Encoding digital music, video, digital photos or any other digital file is called digital watermark.

2.9 Types of Watermarks

There are many places where you can apply a watermark, whether visible or invisible, such as your official signature where it can be added as a distinctive mark to your photos or designs so that customers can track your work through it. Faults if misused, may cause a distraction or shift in the focus of the image.

Watermarks can be divided into two types, the first is visible and the second is invisible. The visible can be seen easily, and is also known as the *public watermark*, while the invisible is known as the *secret watermark.*

2.9.1 Visible Watermark

Most of the time, a visual watermark takes the form of a semi-transparent image embedded in the original image. It may contain a logo or a name denoting the photographer or the name of the company that owns the copyright to the image, as well as other elements such as the date and copyright symbol (Qasim Mohammed, 2020). However, its presence never affects the main content so you can still see the main image without distortion.

2.9.2 Invisible Watermark

Regarding the invisible (secret) watermark, it is integrated into the image and remains invisible through regular viewing, and you can only view it through specialized programs. It has several types, and hereunder are some of them (Qasim Mohammed Hussein, 2014):

- A type which may come within the image but with a transparency so high that it may not be noticeable.
- A spatial watermark, one that only appears when printed because it is of a specific color spectrum.
- A custom frequency watermark, which is applied to a specific frequency and can only be seen when that frequency is separated.

2.9.3 Comparison Between Watermark & Steganography

Watermarks and covered writing are two types of subdomains that are important for hiding information and closely related to each other but with a difference in basic characteristics, requirements and design which leads to different technique solutions.

The main purposes of the use of watermark is to disseminate intellectual property rights, to protect copyrights from illegal publication and to prevent forgery of various kinds. It is used in applications with security purposes such as cards and confidential communications (Ministry of Defense and Secret Intelligence applications). On the other hand, a watermark is hardened against attempts to remove embedded data. Information embedded by watermark systems is always linked to a digital object whose holder's ownership is protected while covered writing systems are used to conceal any information and send it in a confidential manner that cannot be distinguished from such data. In addition, the hardening criteria are different since the watermark focuses on how to prevent the removal of data embedded by the intruder while in covered writing it is less hard against attacks because it is primarily concerned with impeding the detection of the presence of the hidden message by the illegal person (Khalil Ibrahim & Alsaif Meaad, 2013). Moreover, the secret connection in watermark systems is from point to point, while in book systems its cover is from point to point.

Digital watermarking technology is an important branch in the field of information security and is the best way to determine the reliability of information and property rights. It has attracted noticeable attention, occupied important and effective space within the field of research, marketing and development, and is necessary for the purpose of addressing the challenges faced by the rapid spread of digital media.

Recently, watermark technology has attracted much attention and is used by various (DRMs) to achieve rights management that supports copyright information (Qasim

Mohammed, 2020). There are many differences between watermark and covered writing as shown in Table (2-3).

Table (2-3): The differences between watermark and covered writing

T	Covered writing	Watermark
1	Used for covert purposes (concealment)	Used to prove ownership
2	It does not affect the entity that contains it	A change in the cap
3	Data volume can be large	Data that can be included is few
4	It is less hard	It must be strong (featured by hardness)

2.10 Digital Images

Digital Images in general are computer files of a specific storage nature that contain the characteristics of the natural image in two frames. The first is the spatial frame, which is represented by two-dimensional matrix elements. The second is the color frame, represented by the matrix element, and which contains the value of the color gamut of the corresponding point in the natural image. Each element is called *Name* (picture element), i.e. (pixel) (Amer A. Al-Lehiebe, 2015).

These files are created either by doing a numbering *digitization* of the original images taken with the ordinary camera using a digitizer, the most common type of which is the scanner, or the images are taken directly using the digital camera. The digital images contain information regarding the original image in terms of:

(1) The gradation of color points,

(2) The nature of the forms contained in the original image.

After the image is converted into a digital form, it is possible to perform many operations on it such as improving, reformulating and distinguishing forms, re-sizing, and

performing operations of a statistical nature. Digital images are classified in terms of color representation and use into four basic types, namely (Binary images, gray scale images, multispectral images, and color images). The color image is to be explained due to its relevance to the research topic (Amer A. Al-Lehiebe, 2015).

2.11 Image Analysis

Image analysis is the process of changing picture data to home in on particulars that will aid in the resolution of a computer imaging task.

Data reduction is the initial step in the analysis of photographs. As we have seen, images may contain hundreds or even thousands of bytes of information. While attempting to address a particular computer imaging problem, the process of image analysis significantly relies on identifying which data is relevant, as most of the information is often redundant. (2015) Abdallah H. Muhammad.

The image analysis process can be divided into three major stages:

1. Preprocessing

2. Data Reduction

3. Features Analysis

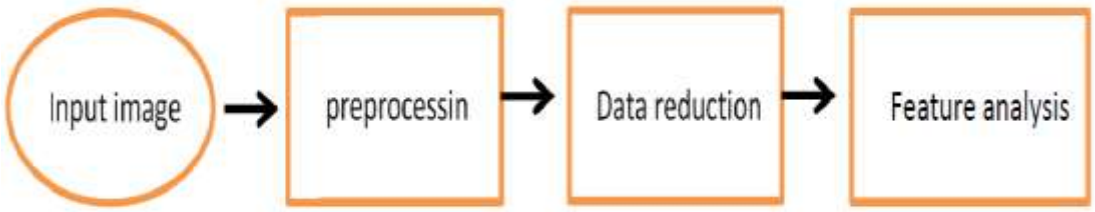


Figure (2-5): Image Analysis.

a. Preprocessing:

It is a tool for removing unneeded or irritating visual elements. The following are potential instances of additional preprocessing steps: During the taking of an image, "noise" may appear (Ayman Mudheher, 2018):

a) Quantification in space or on a scale of gray (reducing the number of bits per pixel or the image size).

b) Identifying good targets for further investigation.

b. Data Reduction:

After the geographic data is either decreased in size or translated to the frequency domain, features are extracted for analysis.

c. Features Analysis:

The features obtained through data reduction are reviewed to determine their suitability for use inside the application.

For further examination, the image can subsequently be segmented in the spatial domain or digitally translated into the frequency domain. After these steps, we may decide to add an image filter. By further reducing the data, this method of filtering allows us to obtain the features we may need for analysis. (Muhammad Abdullah ibn Abdullah, 2015).

2.11.1 Image Representation

It is evident that the human visual system obtains its information from the optical image, which consists of spatially distributed light energy (HVS). Due to the fact that cameras acquire, track, and display optical images, we continuously interact with them. As we all know, the electrical analog signals utilized to represent these optical images as video data are sampled to form the digital image I. (r, c).

The digital picture I (r, c) is represented by a two-dimensional array of data, with each pixel value representing the brightness of the image at that particular location (r, c). A vector represents a single row (or column) of a two-dimensional array in linear algebra, such as our image model I. (r, c). Reference: (Kamal deep Joshi, 2018) (Kamal deep Joshi, 2018).

The image types consideres are:

1- Binary Images

2- Gray Scale Images

3- Color Images

4- Multispectral Images

Because binary images only allow for two possible values, often black and white or (0) and (1), they are the most basic sort of image (1). As each pixel may be represented by a

single binary digit, binary images are also known as one-bit-per-pixel images. When just high-level shape or contour information is required for a particular job, these images are frequently employed in computer vision applications (Kamal deep Joshi, 2018). To demonstrate this, we may employ optical character recognition to detect distortion in manufactured objects (OCR).

The figure (2-6) demonstrates a popular approach for converting grayscale images to binary images: applying a threshold value that assigns "1" to anything that falls above it and "0" to everything that falls below it.

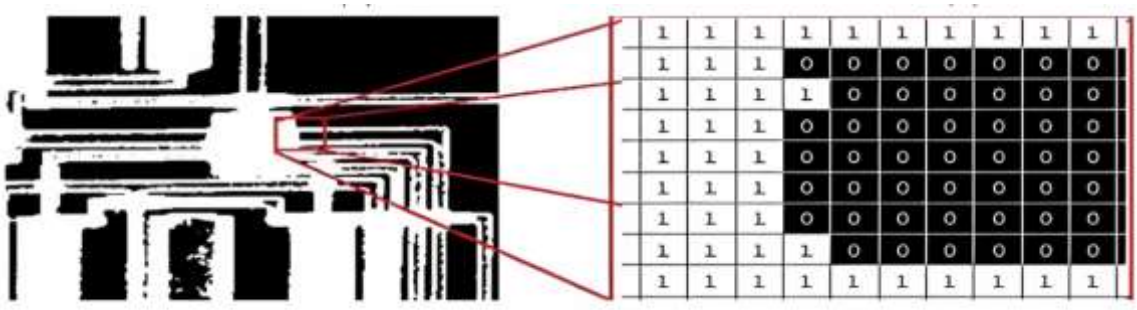


Figure (2-6): Binary Image (Ahmed S. Abdullah, 2015).

2.11.2 Gray Scale Images

Monochromes are images that include only one color. Without color information, they just have brightness information. There are a multitude of brightness levels available. The standard image uses 8 bits per pixel, which provides a range of grayscale values (0–255). The byte, which consists of 8 bits of data, is the globally accepted unit for digital computers, which is why the 8-bit representation is so prevalent. Haleem Jamil; Jamil Muhammad; Jamil Khan Muhammad; Khan Muhammad; 2014.

2.12 Color Image

A color image can be faked by separating monochrome image data into three bands, with each band representing a different color. Digital image files provide brightness information for each spectral band.

As depicted in Figure 1, the brightness information for a specific color is presented on the screen based on the image elements that release light energy corresponding to that color (1-6). (Deepali Singla and MamtaJuneja, 2014).

Typically, color images are represented as RGB images, which consist of red, green, and blue channels and adhere to the 8-bit monochrome standard. A equivalent color image with 8 bits per color channel would have 24 bits per pixel (red, green and blue). Figure 2-7 depicts what a typical RGB color picture looks like.

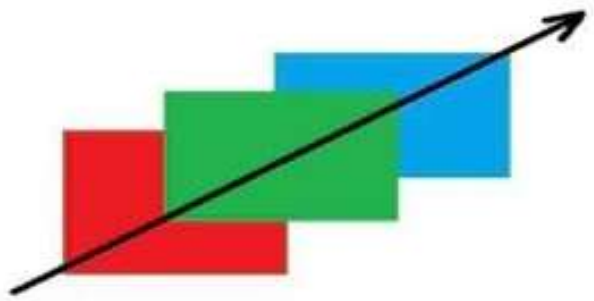


Figure (2-7): Color Image (red, green and blue).

In addition to the more prevalent arrow and column nomenclature, the red, green, and blue values of a single pixel can also be discussed as a color pixel vector (R, G, B).

2.13 Multispectral Images

To create a multispectral image, information about a picture is acquired at multiple frequencies across the electromagnetic spectrum. Multispectral photos contain data that is generally invisible to the naked eye (Deepali Singla and MamtaJuneja, 2014). Moreover, information from other spectrum, such as acoustic or radar waves, can be provided. Figure 2-8 illustrates a photograph taken from space, but comparable images can also be captured using satellites, sonar systems, and medical diagnostic imaging instruments.

Figure (2-8): Multispectral Images.

2.13.1 Image Color

This type of image is capable of covering the full range of colors perceived by the human eye with 32-bit spread. Each image unit is represented by (4-byte) which is similar to (24-bit), but with the addition of a fourth byte representing the degree of transparency (transparency) of the image unit. If the value of (byte) is (256), it means that the color is completely dulled, but if the value is zero it means that it is completely transparent. The shape can be seen as (1-9) which represents a color image (Aymen Mudheher, 2018).

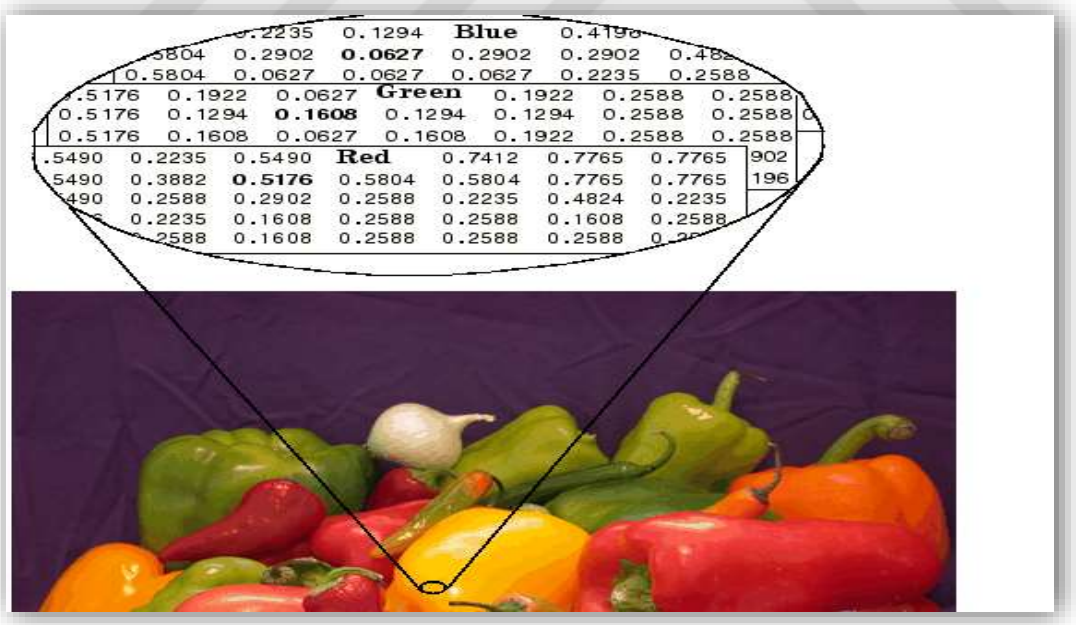


Figure (2-9): A Color Image.

3.MATERIALS AND METHOD

In this chapter, the proposed algorithm is addressed and illustrated through texts that are included in all types of images. This algorithm relies on embedding data directly within the image The experiments conducted used more than 500 characters within images where the point is divided into two sections.

The methodology employed in this thesis is founded upon conducting experimental procedures involving the incorporation of a confidential message or data into a cover image through the utilization of the Least Significant Bit (LSB) method. Subsequently, the resulting Stego image is subjected to an assault, followed by an assessment of the integrity of the Stego data subsequent to the attack. The experimental data included in this study is derived from publicly available image datasets that have been developed through rigorous academic research. The model under consideration has been implemented within the MATLAB environment. The execution of the suggested model is partitioned into three distinct modules: The concept of embedding involves the process of storing a confidential message within a designated cover image, while also performing checksum computation. On the other hand, an attack refers to the act of changing the Stego image by randomly substituting bits. The ASCII code is a character encoding standard that represents text in computers and other devices. This process involves the extraction of a concealed message, as well as the verification of its integrity.

3.1 Explanation of the proposed method

1- Read the color image in the program used.

2- Divide the color image into three layers (blue, green, and red) to include the secret data in the high-contrast bits.

3- Each layer of the color image consists of 256 bits. We choose the most contrast layer, to hide it in the high contrast. The high contrast layer is determined and put the secret data in the most contrast layer and bits.

4- After selecting the most contrast layer, we select two options: the first option is to put a cover message in the front of the image, the second one is to specify the hiding place, either in the form of a picture within a picture, a video clip, or an audio message, we hide a secret message in the form of a text.

5- After selecting the hiding topics and the cover letter, we include the message.

6- In the process of embedding the message, we apply it to the embedding code that we relied on in the methodology at the beginning. After all the commands that we have done, this paragraph for embedding only. We read the secret message, and then we encrypt it. We encrypt it again, and after completing the concealment and encryption twice by the (Ascll code) way that contains the encrypted message, and converting the encrypted message into the bit numbers in the color image.

$$\boldsymbol{Cipher\ text} = (\boldsymbol{Plain\ text} + \boldsymbol{Key}) \qquad \textbf{(1)}$$

Where

Cipher text is the encrypted text

Plain text is the explicit text to be kept confidential and sent

Key encryption, which is found based on the chromatic values of the color layers.

- Let the message contain the word ('THOLFEKAR')
- Convert the character to ASCII code (‘THOLFEKAR') => (' 65 72 77 69 68')
- Encryption key is selected using the value of pixel in the second layer or the third layer.

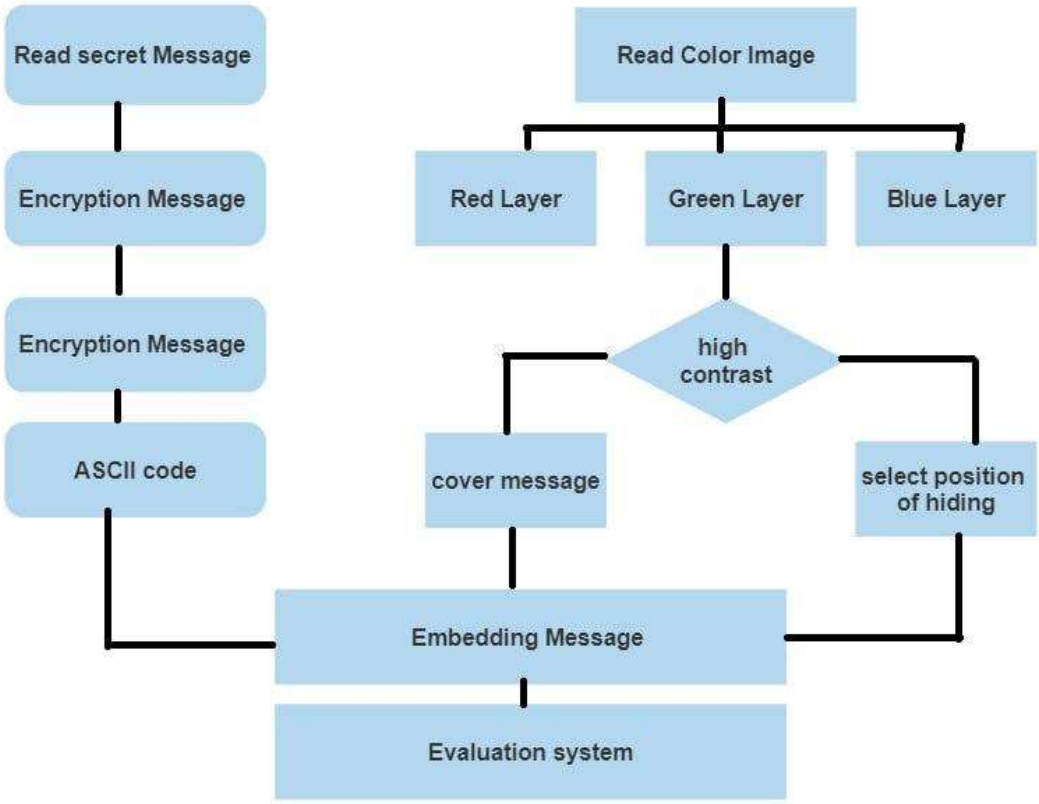


Figure (3-1): Proposed Algorithm in this study.

This algorithm has the advantage of increasing the volume of data that can be hidden, the possibility of retrieving the written text without errors, as well as giving a higher degree of reliability to ensure the integrity of image before retrieving its contents. The data within the image have been randomly embedded which has earned it higher security and resistance to extraction by saboteurs. The new algorithm is compared with other algorithms and the results demonstrate the new algorithm's ability to hide and retrieve data, the high storage capacity and not being visible or detected by electronic methods.

3.2 The main functional points of the proposed method

The primary aim of the proposed study is to augment the security measures employed for transmitting secret messages across communication networks by integrating many functional aspects.

1. In order to mitigate potential attacks from adversaries, it is advisable to conceal the confidential message behind a grayscale image before transmitting it across a communication channel.
2. One potential countermeasure to thwart an attacker's attempt to uncover a secret message, following its detection by an analytical tool, involves the incorporation of fake data with the intention of inducing confusion.
3. The objective of the embedding procedure is to produce a stego image that possesses a reduced likelihood of being detected, as per the criteria of non-visual perceptibility and the PSNR measure.
4. Incorporate a checksum into the steganographic image during the process of embedding, and subsequently compute a second checksum during the process of extraction. Checksums are employed for the purpose of identifying any alterations that may have taken place, through the process of comparing the two checksums.
5. In the absence of any attacks, the recovered secret file must possess same contents and format as the original secret file.
6. Conduct an offensive operation aimed at inducing alterations in the Stego picture that necessitate identification during the subsequent extraction procedure.
7. The secret message should be extracted and its integrity should be verified through the process of checksum comparison.

8. In the event of an identified attack, the process involves determining the altered secret image bytes by means of a comparative analysis between the data bit pair and the decoy bit pair within each byte.

3.3 Design considerations for the proposed model

1. Grayscale cover images are employed for the purpose of concealing covert multimedia files and decoy data, so serving to obfuscate the genuine information and perplex potential attackers. The concealment capacity will constitute 50% of the available data space allocated for the steganographic image. Within this capacity, 25% will be utilized for the purpose of embedding the confidential message, while the remaining 25% will be dedicated to storing decoy data, which will serve the purpose of verifying the integrity of the concealed information. In order to prevent noticeable visual distortion, the right half of the stego pictures will contain two bits of actual confidential data and two bits of decoy data, while the left half of the byte will remain unaltered.
2. In the process of embedding, the hidden multimedia file will be interpreted as a sequential series of bytes, irrespective of its specific file format.
3. The grayscale cover image will be partitioned vertically into four segments, with each segment containing two bits, in order to conceal the hidden multimedia content.
4. The 2-bit segments of the confidential message will be substituted for the least significant 2 bits of the byte in the steganographic image. The two least significant bits (LSB) of each byte will be allocated for storing two-bit segments of the decoy data. This decoy data will consist of an inverted replica of the original secret data fragment.
5. When doing a comparison between the cover picture and the stego image, it is imperative that the Peak Signal-to-Noise Ratio (PSNR) findings obtained be consistent with those generated by widely regarded standard image comparison tools, such as Imagemagick.
6. The formula for determining the maximum hiding capacity (HC) of a grayscale cover picture when utilizing the 2-LSB (Least Significant Bit) method is given by HC = (width x height) / 4.

3.4 Region of Interest Image

While conducting image analysis, the "region of interest" is the area of the image that requires further examination (ROI). For this aim, image geometry techniques that adjust the image's x, y, and z coordinates are required. Among the several subjects covered in this text are operations on the geometry of images, such as resizing (Crop, Zoom, Enlarge, Shrink, Translate, Rotate).

Cropping an image refers to selecting a small portion of a photograph (often called a sub-image) and removing it from the larger original.

1-ZeroOrder Hold: is performed by repeating previous pixel values, thus creating a blocky effect.

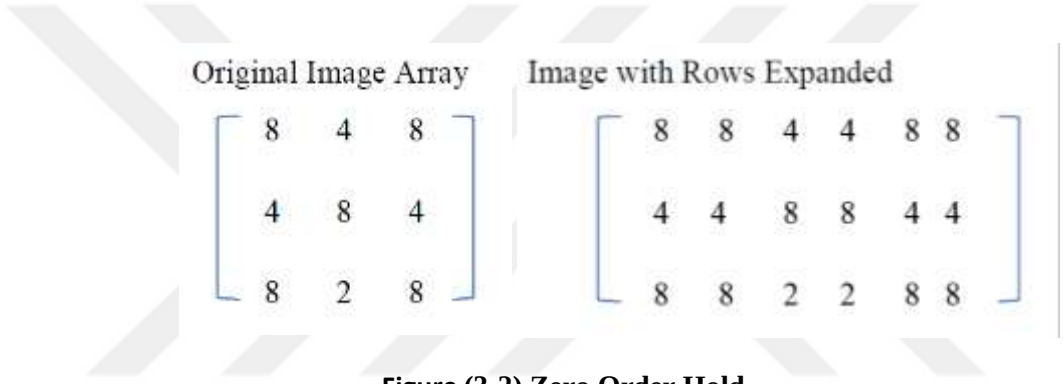


Figure (3-2) Zero Order Hold.

In zero order hold, the output image size is double the original image size with (2n * 2n), which (n x n) is the dimension of image.

Figure (3-3) Zero Order Hold.

Once a sub-image has been extracted from the main image through cropping, it is possible to enhance its size by means of enlargement, so allowing for closer examination. The process of zooming can be executed by many methods, as seen in Figure 3.2.

Figure (3-4): Original image zoom process.

2-First Order Hold: is performed by finding linear interpolation between adjacent pixels, finding the average value between two pixels and using that as the pixel value between those two. We can do this for the first rows as follows:

Original Image Array

$$\begin{bmatrix} 8 & 4 & 8 \\ 4 & 8 & 4 \\ 8 & 2 & 8 \end{bmatrix}$$

Image with Rows Expanded

$$\begin{bmatrix} 8 & 6 & 4 & 6 & 8 \\ 4 & 6 & 8 & 6 & 4 \\ 8 & 5 & 2 & 5 & 8 \end{bmatrix}$$

Figure (3-5) First Order Hold

The first two pixels in the first row are averaged (8+4)/2=6, and this number is inserted between those two pixels. This is done for every pixel pair in each row.

Next, take the results and expand the columns in the same way as follows: Image with rows and columns expanded

$$\begin{bmatrix} 8 & 6 & 4 & 6 & 8 \\ 6 & 6 & 6 & 6 & 6 \\ 4 & 6 & 8 & 6 & 4 \\ 6 & 5.5 & 5 & 5.5 & 6 \\ 8 & 5 & 2 & 5 & 8 \end{bmatrix}$$

Figure (3-6) First Order Hold

This method allows us to enlarge an N×N sized image to a size of (2N-1) × (2N-1) and is repeated as desired.

From this method we conclude the process of enlarging the image in different and many ways as shown in the figure (3.7).

Figure (3-7): Image zoom process.

3- Convolution: this process requires a mathematical process to enlarge an image.

This method requires two steps:

1. Extending the image by adding rows and columns of zeros between the existing rows and columns.

2. Performing the convolution.

The image is extended as follows:

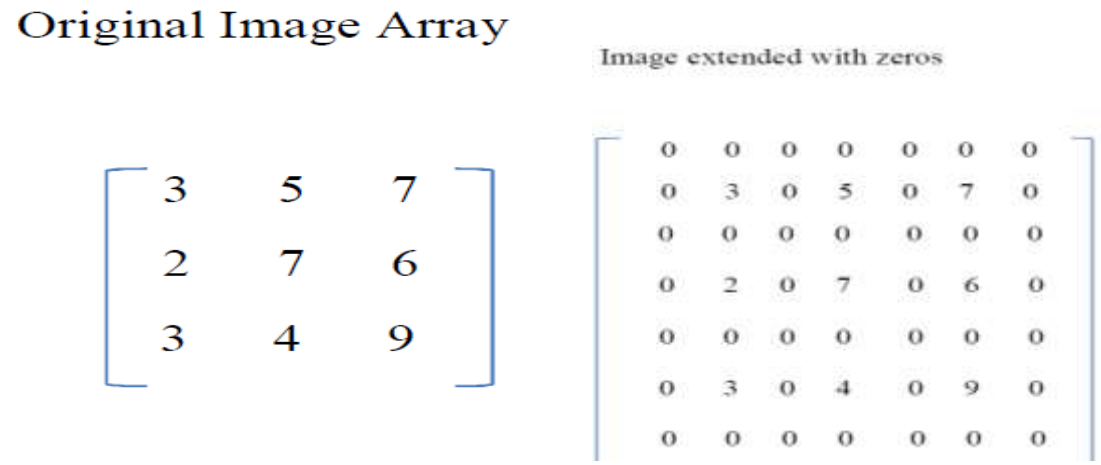


Figure (3-8) Convolution

Next, we use a convolution mask, which is a slide across the extended image, and perform simple arithmetic operations at each pixel location. **Note** that for this mask we need to put the result in the pixel location corresponding to the lower-right corner because there is no center pixel.

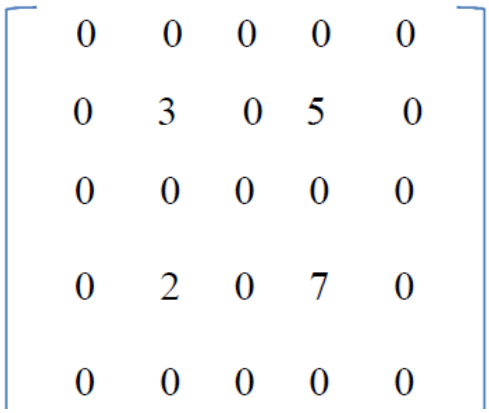


Figure (3-9) Convolution

A. Performing the convolution:

1) 1*0 + 1*0 +1*0 +1*3 =3

2) 1*0 + 1*0 +1*3 +1*0 =3

3) 1*0 + 1*0 +1*0 +1*5 =5

4) 1*0 + 1*0 +1*5 +1*0 =5

5) 1*0 + 1*3 +1*0 +1*0 =3

6) 1*3 + 1*0 +1*0 +1*0 =3

7) 1*0 + 1*5 +1*0 +1*0 =5

8) 1*5 + 1*0 +1*0 +1*0 =5

9) 1*0 + 1*0 +1*0 +1*2 =2

10) 1*0 + 1*0 +1*2 +1*0 =2

11) 1*0 + 1*0 +1*0 +1*7 =7

12) 1*0 + 1*0 +1*7 +1*0 =7

13) 1*0 + 1*2 +1*0 +1*0 =2

14) 1*2 + 1*0 +1*0 +1*0 =2

15) 1*0 + 1*7 +1*0 +1*0 =7

16) 1*7 + 1*0 +1*0 +1*0 =7

Then, we enlarge image by convolution mask for zero order hold:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 3 & 5 & 5 \\ 0 & 3 & 3 & 5 & 5 \\ 0 & 2 & 2 & 7 & 7 \\ 0 & 2 & 2 & 7 & 7 \end{bmatrix}$$

Figure (3-10) enlarge image by convolution mask for zero order hold.

3.5 Convolution mask for order hold

For each iteration, the image mask must be layered on the convolution result, the coincident values must be multiplied, and the sum must be calculated.

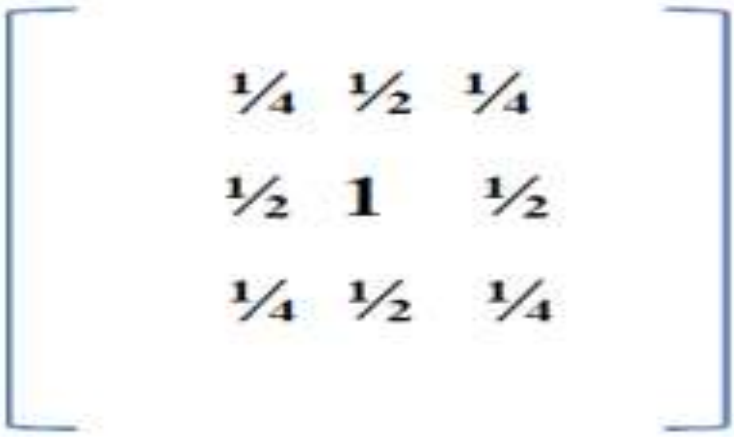


Figure (3-11) Convolution mask for order hold.

This operation is comparable to locating the vector inner product of the mask with a supporting sub-image. By superimposing a mask on the sub-image, the vector inner product is determined. The results of multiplying the coinciding terms are then added together. For instance, if we superimpose the mask on the upper left corner of the image, we receive (reading vertically from right to left):

1/4(0) +1/2(0) +1/4(0) +1/2(0) +1(3) (3) (3) (3) +1/2(0) + 1/4(0) (0) +1/2(0) +1/4(0) =3

Nothing will alter the existing values of the image. By advancing the mask by one pixel, a second set of processes is triggered:

1/4(0) +1/2(0) (0) +1/4(0) (0) (0) (0) +1/2(3) +1(0) (0) (0) (0) +1/2(5) + 1/4(0) (0) (0) +1/2(0) +1/4(0) =4

This computation is based on the median of the two properties in the region. From the beginning of the process through the end of the row, the operation's outcome is always placed in the mask's center cell.

The technique is repeated row by row after shifting the mask down one row at the end of the row. Convolution is the process of sliding, multiplying, and summing across a whole image.

As shown in Figure (3.4), the convolution method necessitates that the output image be stored in a buffer, a distinct array of images, to prevent the existing values from being overwritten.

b. Performing the convolution:

1) [1/4 *0 +1/2 *0 +1/4 *0 +1/2 *0 +1*3 +1/2 *0 +1/4 *0 +1/2 *0 +1/4 *0] = 3

2) [1/4 *0 +1/2 *0 +1/4 *0 +1/2 *3 +1*0 +1/2 *5 +1/4 *0 +1/2 *0 +1/4 *0] = 1.5 + 2.5 = 4

3) [1/4 *0 +1/2 *0 +1/4 *0 +1/2 *0 +1*5 +1/2 *0 +1/4 *0 +1/2 *0 +1/4 *0] = 5

4) [1/4 *0 +1/2 *3 +1/4 *0 +1/2 *0 +1*0 +1/2 *0 +1/4 *0 +1/2 *2 +1/4 *0] = 1.5 + 1 = 2.5

5) [1/4 *3 +1/2 *0 +1/4 *5 +1/2 *0 +1*0 +1/2 *0 +1/4 *2 +1/2 *0 +1/4 *7] = 0.75 + 1.25 +0.5 +1.75 = 4.25

6) [1/4 *0 +1/2 *5 +1/4 *0 +1/2 *0 +1*0 +1/2 *0 +1/4 *0 +1/2 *7 +1/4 *0] = 2.5 + 3.5 = 6

7) [1/4 *0 +1/2 *0 +1/4 *0 +1/2 *0 +1*2 +1/2 *0 +1/4 *0 +1/2 *0 +1/4 *0] = 2

8) [1/4 *0 +1/2 *0 +1/4 *0 +1/2 *2 +1*0 +1/2 *7 +1/4 *0 +1/2 *0 +1/4 *0] = 1 + 3.5 = 4.5

9) [1/4 *0 +1/2 *0 +1/4 *0 +1/2 *0 +1*7 +1/2 *0 +1/4 *0 +1/2 *0 +1/4 *0] =

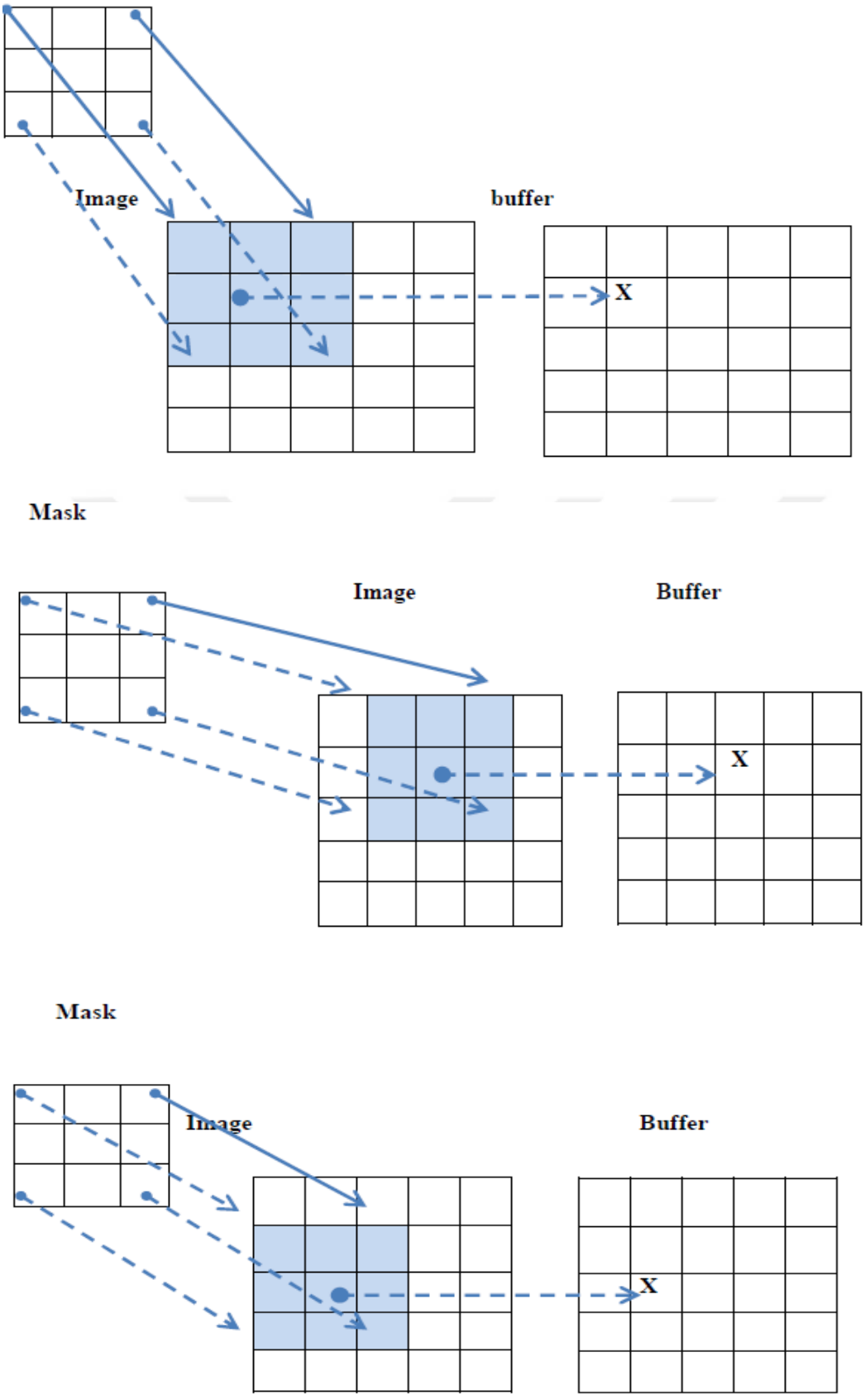


Figure (3-12): multiplying and summing are called convolution.

4. RESULTS AND DİSCUSSİON

In this chapter we will discuss and apply the proposed adopted algorithm (Matlab,2020) in the design and implementation of the algorithm.

The algorithm was applied to different types of images in terms of their size and formula, where the algorithm was studied on a natural, and personal images of different sizes.

The effect of the algorithm was also studied in the concealment of texts of different lengths. Thus, there was the reliance on one of the encryption methods to encrypt the text to be hidden before the concealment process, in order to increase the hardness in breaking or detecting the hidden text.

4.1 Proposed algorithm for Inclusion

In this section the algorithm adopted to hide the information is to be discussed as follows:

4.1.1 Read the colored image

Read the colored image by uploading it from the computer (4-1).

Figure (4 - 1): The Colored Image (Original).

The image is then dismantled into the original layers of red, green and blue, since the original image consists of 24 bits. If the image is divided into the basic layers, each type will consist of 8 bits.

4.1.2 Calculation of Image Variation

The color image is divided into the basic layers and the variance is then calculated for each of the three layers. After the image is calculated, the high contrast layer or the other layers are used, and the values in the pixel can be used as keys in the process of encrypting the text to be sent.

4.1.3 Encrypting the Message

In order to increase the security of the sent data, there must be a range of ways that help to communicate information to the intended party only. If the unauthorized party accesses this data, it becomes necessary to find a set of solutions that help maintain the security of the data in this induction. The proposed encryption algorithm is used against the values of the less varied color layers.

Figure (4 - 2) explains the method with following steps:

179	180	183	183	183	177	165	147
182	183	186	185	183	175	160	136
180	182	183	183	181	172	158	123
179	179	180	178	176	162	140	107
176	176	174	169	164	148	126	96
168	168	164	158	151	136	115	86
159	156	152	146	142	128	107	73

170	172	175	176	178	179	178	178
170	172	175	176	178	177	179	179
169	171	174	175	175	177	181	182
170	171	172	173	175	179	181	183
170	171	172	173	175	179	183	184
170	172	173	173	175	178	184	186
171	171	172	173	176	177	183	186

Figure (4 - 2): Segment of low and medium contrast layers.

4.1.4 Embedding Process

After the image has been dismantled and the layer with the highest variation and the encrypted text is included in this paragraph confidential data in the layer with the highest variation.

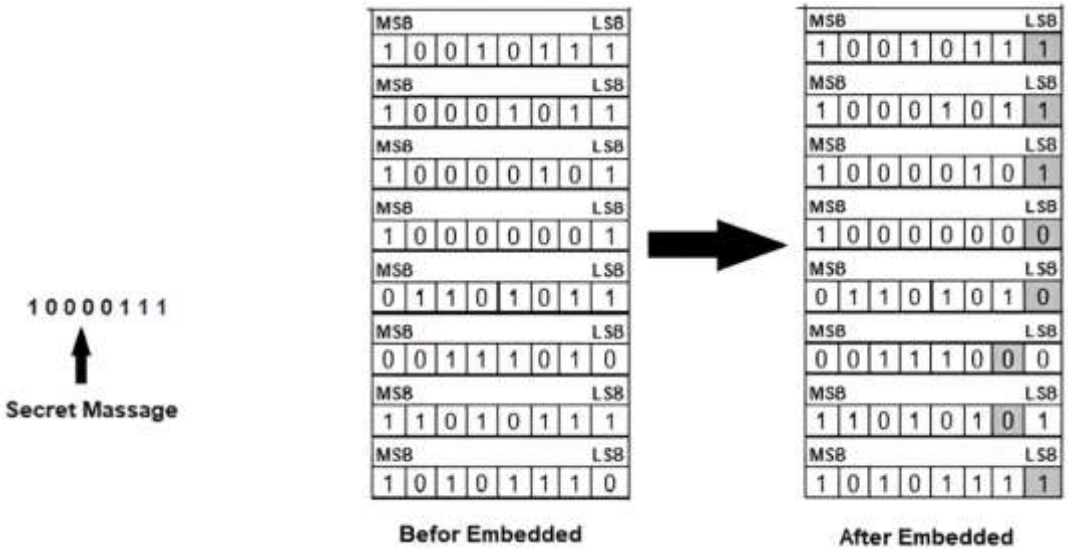


Figure (4 - 3): Embedding stage with encrypted text.

4.1.5 PSNR

PSNR, or peak Signal to Noise Ratio, measures the similarity between two images. We determine the greatest difference between the two photos. Whenever possible, the PSNR of a steganography approach should be maximized.

4.1.6 Signal-to-noise ratio

A high signal-to-noise ratio (S/N or SNR) is required for effective discrimination between diverse output streams. This ratio measures the desired signal's intensity in comparison to the noise's (unwanted signal). A higher signal-to-noise ratio (SNR) suggests a crisper transmission by having more valuable data (signal) than distracting noise (Noise). In extremely high SNR outputs, a signal-to-noise ratio (SNR) of 100 dB, for example, is superior to an SNR of 70 dB.

4.1.7 Application of the System to a Group of Images

The findings depicted in Figure 4-4 The original image is displayed subsequent to its integration into the hostgram. One key benefit of employing steganography for data concealment, as opposed to encryption, lies in its capacity to obfuscate the presence of confidential information within a file or other medium containing the concealed text.

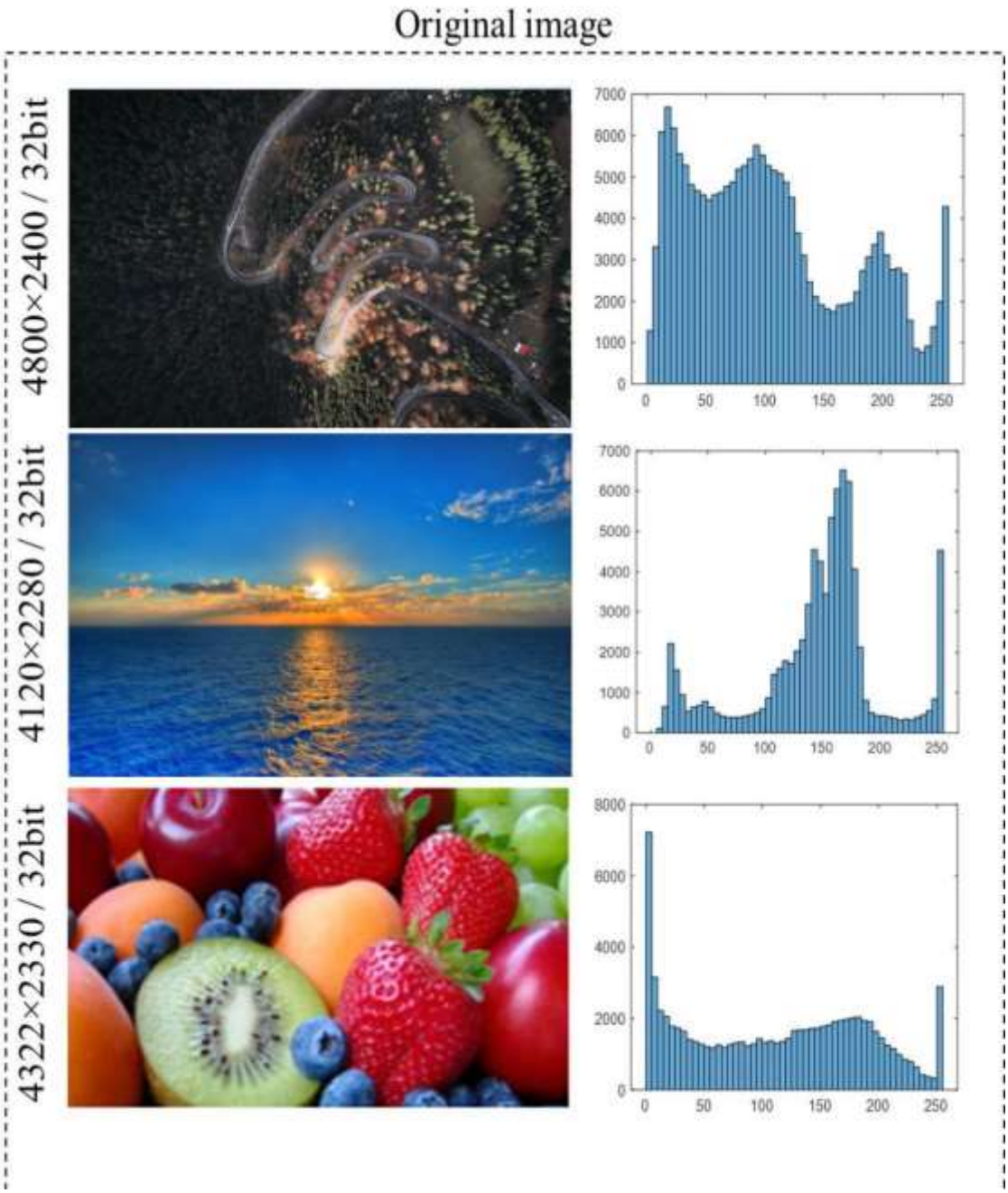


Figure (4 - 4): Original images with their histogram.

In Figure 4-5, concealing techniques were applied, resulting in a visually apparent alteration in the disparity between the modified photographs and their original counterparts. One of the main benefits associated with the utilization of steganography for concealing data, as opposed to encryption, lies in its capacity to obfuscate the presence of sensitive information embedded inside a file or other form of material that carries the concealed text.

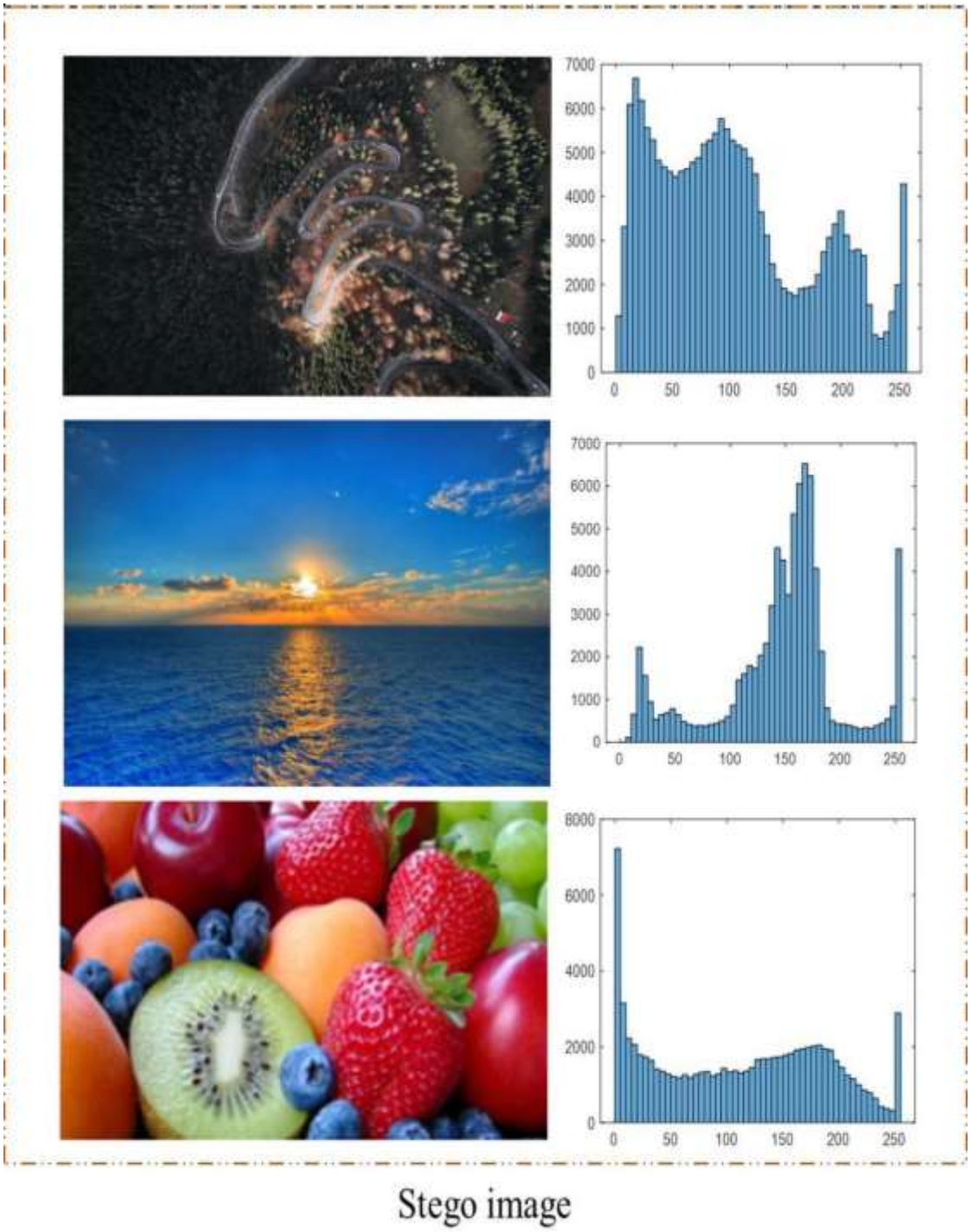


Figure (4-5): Stego images with their histogram.

4.2 Results after application

As depicted in Table 4-1, a collection of photographs with varying formats and dimensions is subjected to encryption through the concealment algorithm, resulting in the encryption of information inside the images. In the initial image, the quantities of characters employed are (100, 200, 300, 400, 500) in a sequential manner. Correspondingly, the resultant outcomes (PSNR, SNR) exhibit a declining trend as the quantity of characters employed grows. This indicates that there is a reverse proportion in the encryption between the number of characters used and the output results (PSNR, SNR). This applies to all images on which the encryption algorithm has been applied and which are of different sizes and formulas. The algorithms were applied to a median contrast layer:

Table (4-1): A group of (15) images.

Image	No. Character	HIGH – CONTRAST		Shannon entropy – Original image	Shannon entropy – Encrypted image
		PSNR	SNR		
Image 1	100	75,6007	72,2465	7.344054	8.001004
	200	72.5461	69.1919	7.403208	7.995966
	300	70.7377	67.3835	7.324465	8.064018
	400	69.4865	66.1323	7.330545	7.999679
	500	68.4193	65.0651	7.397676	8.044635
Image 2	100	81.6268	76.0509	7.319968	8.072581
	200	78.8370	73.2611	7.345314	8.048303
	300	77.0572	71.4814	7.33104	8.057875
	400	75.6793	70.1035	7.318151	7.994308
	500	74.7437	69.1679	7.336677	8.011422
Image 3	100	73.4682	64.4764	7.32171	8.027749
	200	70.4250	61.4332	7.41035	7.991221
	300	68.8347	59.8429	7.410755	8.064644
	400	67.3821	58.3902	7.357137	8.065236
	500	66.5027	57.5108	7.373024	8.048739

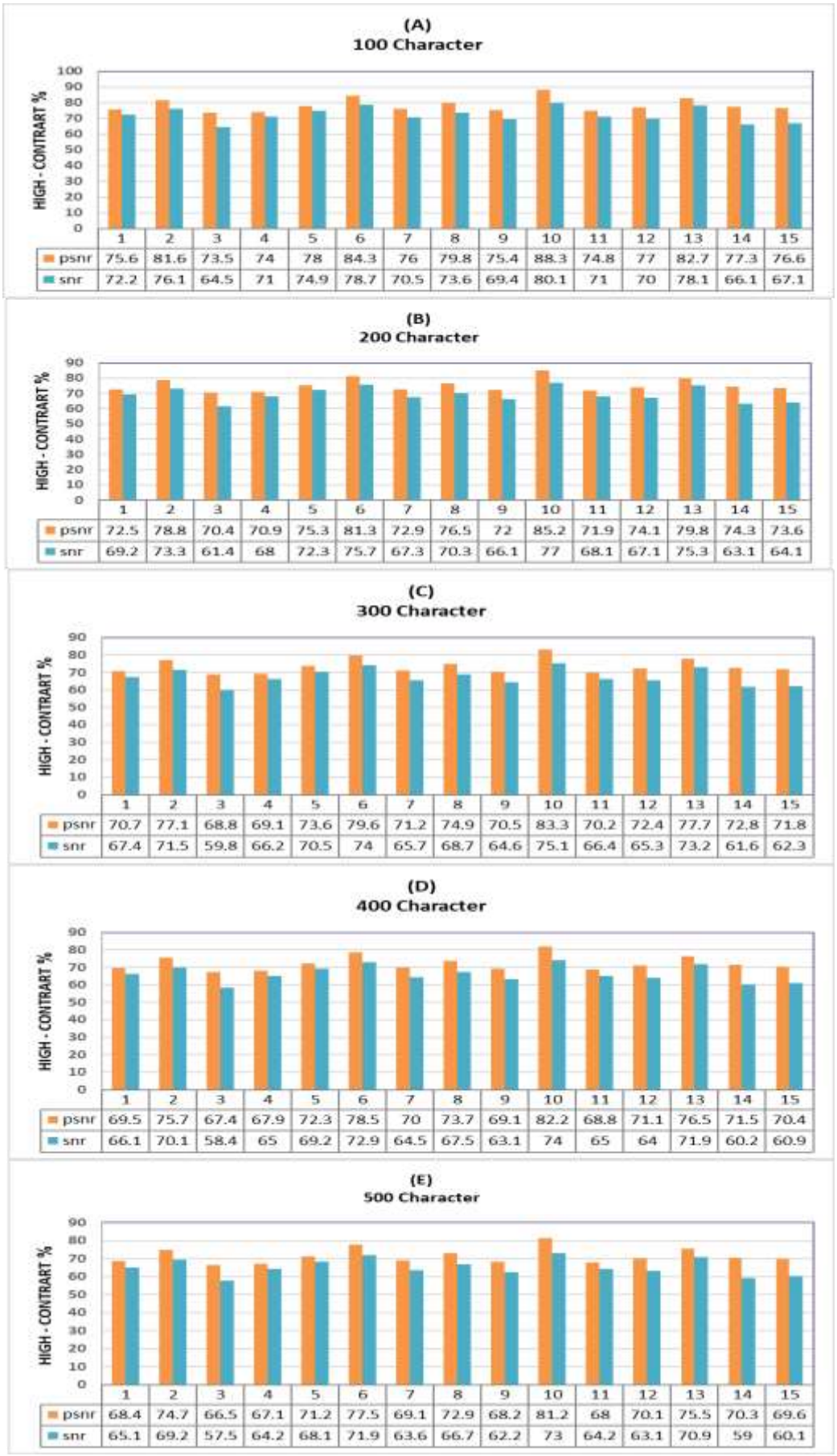
Image 4	**100**	**73.9513**	**71.0256**	**7.314774**	**8.000399**
	200	**70.9083**	**67.9826**	**7.369075**	**7.995802**
	300	**69.0935**	**66.1678**	**7.408466**	**8.006209**
	400	**67.9472**	**65.0215**	**7.326318**	**8.03022**
	500	**67.0814**	**64.1557**	**7.347816**	**8.050817**
Image 5	**100**	**77.9559**	**74.8731**	**7.340205**	**8.053453**
	200	**75.3375**	**72.2547**	**7.372968**	**8.069775**
	300	**73.6161**	**70.5333**	**7.361407**	**8.077783**
	400	**72.2852**	**69.2024**	**7.372767**	**8.039506**
	500	**71.2025**	**68.1197**	**7.411487**	**7.98953**
Image 6	**100**	**84.3430**	**78.7440**	**7.398539**	**8.06558**
	200	**81.2536**	**75.6546**	**7.345135**	**8.024851**
	300	**79.6469**	**74.0480**	**7.364594**	**8.081349**
	400	**78.4520**	**72.8531**	**7.345994**	**8.046212**
	500	**77.5159**	**71.9170**	**7.327367**	**7.991876**
Image 7	**100**	**76.0477**	**70.5262**	**7.390134**	**8.037793**
	200	**72.8623**	**67.3408**	**7.341286**	**8.025173**
	300	**71.1731**	**65.6515**	**7.386193**	**8.074644**
	400	**70.0271**	**64.5056**	**7.348229**	**8.047507**
	500	**69.1016**	**63.5800**	**7.408733**	**7.992594**
Image 8	**100**	**79.8283**	**73.6204**	**7.314332**	**8.047667**
	200	**76.4930**	**70.2852**	**7.394109**	**8.008557**
	300	**74.9319**	**68.7240**	**7.393605**	**8.084496**
	400	**73.7429**	**67.5350**	**7.38379**	**8.021732**
	500	**72.8868**	**66.6789**	**7.366298**	**8.000184**
Image 9	**100**	**75.3630**	**69.4142**	**7.379374**	**8.025849**
	200	**72.0414**	**66.0925**	**7.386938**	**8.011069**
	300	**70.4989**	**64.5501**	**7.377676**	**8.03436**
	400	**69.0750**	**63.1261**	**7.371543**	**8.001362**
	500	**68.1715**	**62.2226**	**7.342938**	**8.084129**
Image 10	**100**	**88.2775**	**80.0698**	**7.391047**	**8.038773**
	200	**85.1803**	**76.9726**	**7.315996**	**8.007923**
	300	**83.3167**	**75.1090**	**7.321607**	**8.071039**

	400	**82.1700**	**73.9623**	**7.384506**	**8.074646**
	500	**81.1837**	**72.9760**	**7.375198**	**8.061115**
Image 11	**100**	**74.8380**	**71.0335**	**7.385658**	**7.996442**
	200	**71.8699**	**68.0655**	**7.376154**	**7.995752**
	300	**70.1553**	**66.3508**	**7.31215**	**8.012092**
	400	**68.8490**	**65.0446**	**7.327113**	**8.045797**
	500	**67.9959**	**64.1914**	**7.41197**	**8.06838**
Image 12	**100**	**76.9766**	**69.9704**	**7.410246**	**8.060015**
	200	**74.1465**	**67.1402**	**7.34538**	**7.994891**
	300	**72.3541**	**65.3478**	**7.331648**	**7.988761**
	400	**71.0507**	**64.0443**	**7.335097**	**7.993478**
	500	**70.0581**	**63.0518**	**7.404775**	**8.086217**
Image 13	**100**	**82.7140**	**78.1353**	**7.343659**	**8.061204**
	200	**79.8358**	**75.2571**	**7.383855**	**8.079126**
	300	**77.7475**	**73.1688**	**7.353517**	**8.067652**
	400	**76.4568**	**71.8781**	**7.393521**	**8.007982**
	500	**75.4995**	**70.9208**	**7.355091**	**8.022305**
Image 14	**100**	**77.3078**	**66.0743**	**7.379344**	**8.04607**
	200	**74.3247**	**63.0911**	**7.349026**	**8.083936**
	300	**72.8046**	**61.5711**	**7.37835**	**8.051706**
	400	**71.4810**	**60.2475**	**7.377092**	**8.061545**
	500	**70.2771**	**59.0436**	**7.326229**	**8.08236**
Image 15	**100**	**76.5711**	**67.0786**	**7.344054**	**8.001004**
	200	**73.5833**	**64.0908**	**7.403208**	**7.995966**
	300	**71.7924**	**62.2999**	**7.324465**	**8.064018**
	400	**70.4121**	**60.9195**	**7.330545**	**7.999679**
	500	**69.6403**	**60.1477**	**7.397676**	**8.044635**

4.2.1 Result Charts (PSNR, SNR)

The subsequent charts present a comparison of the results as depicted in Table (4-1) pertaining to the quantity of pictures, which is 15, together with their corresponding values of PSNR and SNR. Each chart in the study displays character values within the image, which are categorized into five graphs based on the characters examined: 500, 400, 300, 200, and 100.

In the Figure (4 - 6) form (A)(100) characters were used and hidden inside the image and compared (PSNR, SNR) per (15) image and results are shown as in the attached table, and shape (B) (200) characters were used, and the shape (C) we used (300) characters, and the shape (D) (400) characters were used, and the form (E) we used (500) characters as well, we did in these tables comparison (PSNR, SNR) and showed its proportion and the more we increase the characters to hide the lower the ratio (PSNR, SNR).



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
psnr	75.6	81.6	73.5	74	78	84.3	76	79.8	75.4	88.3	74.8	77	82.7	77.3	76.6
snr	72.2	76.1	64.5	71	74.9	78.7	70.5	73.6	69.4	80.1	71	70	78.1	66.1	67.1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
psnr	72.5	78.8	70.4	70.9	75.3	81.3	72.9	76.5	72	85.2	71.9	74.1	79.8	74.3	73.6
snr	69.2	73.3	61.4	68	72.3	75.7	67.3	70.3	66.1	77	68.1	67.1	75.3	63.1	64.1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
psnr	70.7	77.1	68.8	69.1	73.6	79.6	71.2	74.9	70.5	83.3	70.2	72.4	77.7	72.8	71.8
snr	67.4	71.5	59.8	66.2	70.5	74	65.7	68.7	64.6	75.1	66.4	65.3	73.2	61.6	62.3

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
psnr	69.5	75.7	67.4	67.9	72.3	78.5	70	73.7	69.1	82.2	68.8	71.1	76.5	71.5	70.4
snr	66.1	70.1	58.4	65	69.2	72.9	64.5	67.5	63.1	74	65	64	71.9	60.2	60.9

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
psnr	68.4	74.7	66.5	67.1	71.2	77.5	69.1	72.9	68.2	81.2	68	70.1	75.5	70.3	69.6
snr	65.1	69.2	57.5	64.2	68.1	71.9	63.6	66.7	62.2	73	64.2	63.1	70.9	59	60.1

Figure (4 - 6): Result Charts (PSNR, SNR).

4.3 Results After Applying High-Resolution Images

Regarding Table 4-2, a collection of high-resolution photographs is utilized. The concealing algorithm is employed to encrypt the data, which is then embedded into the images, as depicted in the initial image. The number of characters utilized are as follows: 100, 200, 300, 400, and 500, in sequential order. The obtained output results, specifically the peak signal-to-noise ratio (PSNR) and signal-to-noise ratio (SNR), exhibit a modest increase compared to the medium-resolution photos used as input. This observation suggests that there is a positive correlation between the size of the image and the effectiveness of the hiding and encryption procedures. A limited number of five photos are utilized in order to derive additional findings. The uploaded photographs possess much higher resolution compared to the images (15) documented in Table No. (4-1). This phase was undertaken to examine potential disparities in data hiding inside photographs, specifically comparing medium-resolution photos to high-resolution images. The results obtained from this test were favorable, indicating that larger images yield superior outcomes.

The algorithms were applied to a set of high-resolution images:

Table (4-2): A group of (5) images.

Image	No. Character	HIGH – CONTRAST		Shannon entropy – Original image	Shannon entropy – Encrypted image
		PSNR	SNR		
Image 1	100	95.2174	83.2355	7.402661	8.032437
	200	91.9788	79.9969	7.367333	8.080775
	300	90.4911	78.5092	7.3431	7.989907
	400	89.1057	77.1238	7.327723	8.034199
	500	88.2255	76.2436	7.321089	8.08474
Image 2	100	96.2857	89.6811	7.388206	8.049291
	200	93.1995	86.5949	7.384608	8.064903
	300	91.4999	84.8953	7.314224	8.011289
	400	90.3423	83.7378	7.332829	8.040719
	500	89.3135	82.7089	7.411067	8.005636

Image 3	**100**	**80.4693**	**67.7740**	**7.323449**	**8.033943**
	200	**77.6356**	**64.9403**	**7.37536**	**8.074222**
	300	**75.7332**	**63.0379**	**7.350344**	**8.071723**
	400	**74.5361**	**61.8408**	**7.317718**	**8.044986**
	500	**73.6116**	**60.9163**	**7.325546**	**8.031734**
Image 4	**100**	**80.0720**	**73.9271**	**7.390128**	**8.082295**
	200	**76.9622**	**70.8173**	**7.339546**	**8.052922**
	300	**75.2626**	**69.1177**	**7.407314**	**8.019006**
	400	**74.0851**	**67.9402**	**7.388102**	**8.050577**
	500	**73.0157**	**66.8708**	**7.382864**	**8.03546**
Image 5	**100**	**87.2203**	**76.7082**	**7.37578**	**8.054582**
	200	**84.1087**	**73.5966**	**7.397815**	**8.085982**
	300	**82.4615**	**71.9494**	**7.36748**	**8.078208**
	400	**81.2868**	**70.7747**	**7.339402**	**8.046878**
	500	**80.3420**	**69.8299**	**7.402066**	**7.999424**

4.3.1 Result Charts (PSNR, SNR)

The comparison of the results depicted in the charts is presented in Table (4-1), which includes the quantities of images (5) and the corresponding values of peak signal-to-noise ratio (PSNR) and signal-to-noise ratio (SNR). Within each chart, the values of the characters depicted in the image are segregated into five distinct graphs based on the characters that were examined in the present study, specifically denoted as (100, 200, 300, 400, and 500).

In Figure (4-4) (A) (100) the characters within the image were used and concealed and compared (PSNR, SNR) per (5) image and results shown as in table (4-2) Annex and shape (B) (200) letter, shape (C) we used (300) letters, use shape (D) (400), shape (e) We used (500) letters as well, we did this in comparing these tables (PSNR, SNR) and showed its ratio and the more letters we increased to hide the lower ratio (PSNR, SNR) In these charts we used (5) high resolution image.

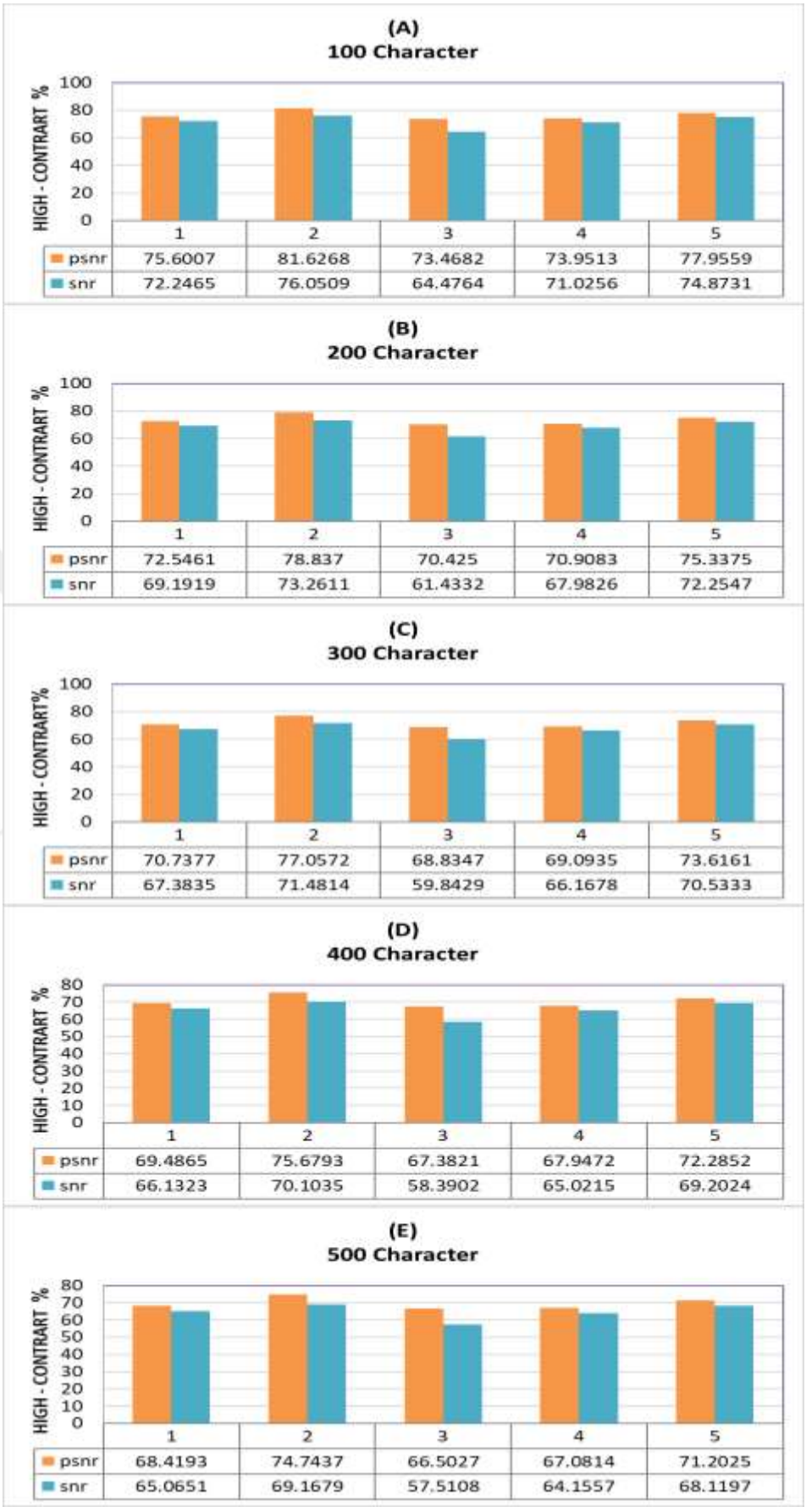


Figure (4-7): Result Charts (PSNR, SNR) High-Resolution Images

4.4. Comparison with Related Work

In their study, Arun and Nivek (2015) put out a novel encryption technique that involves a two-phase process for encrypting a given text into an image. During the initial stage, the plaintext of the text message is converted into an image by employing the Modulo 256 technique. Subsequently, in the second stage, the pixels of the resulting image are encrypted using the AES encryption algorithm. The use of a composite database is unnecessary within this protocol, as the encryption key produced by the Advanced Encryption Standard (AES) is transmitted alongside the image to the recipient.

In the proposed algorithm, the text undergoes a two-stage encryption process before being converted into a code and concealed within the pixels. This encryption procedure is necessary prior to listing in order to prevent unauthorized parties from gaining knowledge of the listing process, which would compromise the encryption mechanism and compromise the security of the information.

Panchami, Paul, and Wahi (2014) developed a text encryption strategy that relies on the utilization of Unicode and the RGB model. In the proposed approach, the initial step involves encrypting a text message into Unicode utilizing the Unicode Model. Subsequently, the Unicode representation is transformed into RGB color values. If two neighboring letters generate the same color, they are altered to a distinct hue. The current moment is employed as a means of preserving and employing a personal encryption key, denoted as K2.

The proposed methodology highlights the significance of implementing an encryption procedure prior to inclusion. This is crucial as the unauthorized party's knowledge of the inclusion method could lead to encryption issues, hence compromising the security of the information.

In 2016, a cohort of scholars disseminated their research outcomes, following an extensive examination of the impact of digital color schemes on the data embedding technique. Ahmed (2019) conducted a study to investigate the influence of color layers on the concealing of information. The study included nine distinct color systems and using the least significant bit approach to evaluate the effectiveness of concealment, utilizing metrics such as mean square error and peak signal-to-noise ratio. The presented

methodology technique highlights the necessity of implementing an encryption procedure prior to the inclusion process. This is crucial because if an unauthorized party becomes aware of the method employed during the inclusion process, it will offer a challenge to the encryption mechanism and compromise the security of the information. By including encryption, the overall security of the data will be strengthened.

Table (4-3): Comparison with related work.

Ref.	Average of Shannon Entropy		Average of PNSR	
	Original images	***Encrypted images***	***Original images***	***Encrypted images***
Arun and Nivek (2015)	**8.064471**	**7.61741**	**86.54839**	**88.30093**
Panchami, Paul, and Wahi (2014)	**8.077734**	**7.752229**	**86.62732**	**88.25086**
Ahmed, 2019	**8.033821**	**7.627919**	**85.35463**	**88.31042**
Current study	**7.994651**	**7.31935**	**80.52012**	**88.28323**

5.CONCLUSION AND FUTURE WORK

5.1 CONCLUSIONS

This thesis introduces a security enhancement approach that aims to safeguard confidential information buried within cover images through the utilization of the steganography technique. The proposed scheme is developed using Matlab.

Data concealment is very useful, especially in the event that sending encrypted messages may raise doubts as in countries experiencing the suppression of freedom of expression, where images are circulated very normally while information within them is hidden and dismantled by a particular algorithm. After studying and experimenting the following conclusions are reached:

1.The efficacy of using a larger image as a cover is enhanced since it minimizes the impact of including additional info on the image.

2.The utilization of colored images in the embedding process is preferable over grey-graded images due to the enhanced security of color image data compared to grey image data.

3.The strength of the inclusion process can be enhanced by preceding it with an encryption process. In the event that an unauthorized party gains knowledge of the inclusion process methodology, they will confront the encryption challenge, thereby increasing the security of the information.

4.The utilization of keyword incorporation inside photo layers is superior than the implementation of a static key.

5.Utilizing the RGB color value with integrated message encryption techniques has a number of advantages. It may be used as a stand-alone method, for instance, to encrypt text and picture data both offline and online.

5.2 Future Work

1-Non-RGB color systems can be used and the characteristics of these colors can be used to increase the security of the data to be included.

2- Data can be included based on video and used as cover in the process of embedding information.

3-Two encryption methods can be used so that the information is safer because the attacker or the unauthorized party will have three encryption and embedding challenges.

4- The transformation of a picture from the spatial domain to the frequency domain allows for its concealment inside the frequency field.

5- The volume of data to be hidden can be changed and the power of the system selected.

6- Images of text or audio allowance can be concealed or the efficiency of the system selected.

6. REFERENCES

1 Abdullah. Muhammad, “Hiding the Text in Image of Variable Size”, Diyala Journal for Pure Science, Volume: 11 Issue: 2 Pages: 44-55,2015.

2 Ahmed S. Abdullah." Text Hiding Based on Hue Content in Hsv Color Space ", International Journal of Emerging Trends & Technology In Computer Science (Ijettcs), Volume 4, Issue 2, March-April 2015.

3 Ahmed Saadi Abdullah.” Improving Message Embedding by Using Some Attributes of Color Image”, Raf. J. of Comp. & Math’s., Vol. 13, No.2, 2019.

4 Alanazi, N., Khan, E., Gutub, A.: Functionality-improved Arabic text steganography based on unicode features. Arabian J. Sci. Eng. 45(12), 11037–11050 (2020).

5 Ali Fattah Dakhil,” Steganography: Applying LSB Algorithm to Hid Text in Image”, Journal of AL-Qadisiya for computer science and mathematics Vol.9 No.1 Year 2017.

6 Ali Nasser Hussain, Enricher MH awes Zghairb,” Efficient Text Message Hidden Technique Using YIQ Model”, JOURNAL OF MADENAT ALELEM COLLEGE, Volume: 9 Issue: 1 Pages: 217-228, 2017.

7 Allen Tom, Anu V Thomas, Jerin Jose, Maria, P. Darsana,” Hiding Host Image using a Cover Image”, International Journal of Engineering Research & Technology,2015.

8 Alyaa Hasan Zwiad,” Proposal Compression Algorithm to Hide Multiple Text Images Based on Bit Plane Slicing”, Iraqi Journal of Information Technology. V.8 N.4. 2018.

9 Amer A. Al-Lehi be,” Ciphered Text Hiding in an Image using RSA algorithm. Of College Of Education For Women, volume 26, issue 3 , 2015.

10 Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh,” Steganography in Images Using LSB Technique, International Journal of Latest Trends in Engineering and Technology,2015.

11 Arun, M., S. MohamedAzarudeen, and T. N. Nivek. "AES based Text to Pixel Encryption using Color Code Conversion by Modulo Arithmetic." International Journal of Recent Research in Science, Engineering and Technology 1.3 (2015): 37-42.

12 Ashwini Palimkar, Dr.S.H. Patil," Using SBR Algorithm to Hide the Data into The JPEG Image",

13 Ayman Mudheher Badr, &Mohamed laythtalal and Ghassan Sabehc," Image in Image Steganography based on modified Advanced Encryption Standard and Lest Significant Bit Algorithms", Journal of University of Babylon for Pure and Applied Sciences. (26), No. (8): 2018.

14 Azal Habeeb," A NEW METHOD FOR HIDING TEXT IN A DIGITAL IMAGE", JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY, Vol. 55 No. 2,2020.

15 Deepali Singla and Dr. Mamta Juneja," New Information Hiding Technique using Features of Image", JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE, VOL. 6, NO. 2, MAY 2014.

16 Deepesh Rawat, Vijaya Bhandal, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications, Volume 64– No.20, February 2013.

17 Dr. Yossra H. Ali Ahmed Y. Yousif Tayseer S. Atia," Distributed AMELSB Replacement Method for Text Hiding",", Iraqi Journal of Information Technology, volume 2, issue 2, 2018.

18 Falih Hassan Owaid," INFORMATION HIDING USING STAGAEROGRAPHS SYSTEM USING LSB-TECHNIQUE", Journal of Baghdad College of Economic sciences University, Issue: 38 Pages: 376-394, 2015.

19 Geetha ani L K Sathya Suneetha S. Susmitha," Embedding Audio in Image for Hiding Information Using MSB Technique", Volume 6, Issue 6, June 2016

20 Gutub, A., Al-Ghamdi, M.: Hiding shares by multimedia image steganography for optimized counting-based secret sharing. Multimed. Tool. Appl. 79(11–12), 7951– 7985 (2020).

21 Hamid Mohammed Farhan, Zena Ahmed Alwan," Improved method using a two Exclusive-OR to binary image in RGB color image steganography", International Journal of Engineering & Technology,2018.

22 Hayder I. Hendi, Shaker K. Ali," PROPOSED METHOD OF INFORMATION HIDING IN IMAGE", Journal of Kufa for Mathematics and Computer, Vol.2, No.1, may 2014.

23 Hazim Noman Abed, Noor Hasan Hasson, Ahmed Luay Ahmed, Ismael Salih Albayaty “Hiding Information in an Image Based on Bats Algorithm”, Iraqi Journal of Information Technology, volume 8, issue 2, 2018.

24 Hussein L. Hussein, Ahmed A. Abbas, Sinan A. Naji, Salam Al-augby and Jasim H. Lafta,” Hiding text in gray image using mapping technique,” IOP Conf. Series: Journal of Physics,2018.

25 International Journal of Security (IJS), Volume (8), Issue (2), 2014.

26 Jamila HarbiS,” New Method of Image Hiding”, Iraqi Journal of Information Technology, Vol.6 No.2, may 2014.

27 Jinan N. Shehab, Haraa Raheem Hatem, Omar Abdul Kareem Mahmood, “HIDING (1-8) MULTIMEDIA FILES IN ONE COLOR IMAGE”, Diyala Journal of Engineering Sciences. 10, No. 3, September 2017.

28 Joshy, Amal, et al. "Text to image encryption technique using RGB substitution and AES." 2017 International Conference on Inventive Computing and Informatics (ICICI). IEEE, 2017.

29 Kamal deep Joshi, Swati Gill, and Rajkumar Yadav, “A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image”, Journal of Computer Networks and Communications, 2018.

30 Kanar M. Sami,” Embedding Data in Personal Image by Using Mosaic Image”, Journal of Education and Science. 28, No.4, 2019.

31 Karthikeyan B, Asha S, Poojasree B,” Gray Code Based Data Hiding in an Image using LSB Embedding Technique”, Volume-8, Issue-1, May 2019.

32 Kartik Sharma, Ashutosh Aggarwal, Tana Singhania, Deepak Gupta, Ashish Khanna, “Hiding Data in Images Using Cryptography and Deep Neural Network”, Journal of Artificial Intelligence and Systems, 2019.

33 Khalil Ibrahim Alsaif, Meaad M. Salih," Contourlet Transformation for Text Hiding In Hsv Color Image ", International Journal Of Computer Networks And Communications Security, Vol. 1, No. 4, September 2013.

34 Khan Muhammad, Jamil Ahmad, Haleem Farman and Muhammad Zubair, “A Novel Image Steganographic Approach for Hiding Text in Color Images Using HSI Color Model”, Middle-East Journal of Scientific Research 22 (5), 2014: 647-654, 2014.

35 KI Al-Saif, AS Abdullah," Color image enhancement based on contourlet transform coefficients", Australian Journal of Basic and Applied Sciences, 2013.

36 Mamta Juneja and Parvinder Singh Sandhu," A New Approach for Information Security using an Improved Steganography Technique", J Inf Process Syst, Vol.9, No.3, September 2013.

37 Nada Qasim Mohammed, Qasim Mohammed Hussein, Mohammed Sh. Ahmed."Suitability of Using Julia Set Images as a Cover for Hiding Information", Al-Mansour International Conference on New Trends in Computing, Communication, and Information Technology, IEEE Xplore, 2018.

38 Omar Younis Abdul Hameed." Hiding A Secret Watermark in Image Using Intelligent Water Drops Algorithm", Diyala Journal for Pure Science, volume 13, issue 2, 2017.

39 Omar Younis Abdulh ameed." Hiding a Secret Information in Image Using Gravitational Search Algorithm", Diyala Journal for Pure Science, volume 14, issue 1, 2018.

40 Panchami, V., Paul, V., & Wahi, A. (2014). A new color oriented cryptographic algorithm based on unicode and RGB color model. International Journal of Research in Engineering and Technology (IJRET), 3, 82-87.

41 Qasim Mohammed Hussein, Hiding Message in Color Image Using Auto Key Generator, 3rd International Conference on Advanced Computer Science Applications and Technologies, Amman, Jordan, 2014.

42 Qasim Mohammed Hussein," New Metrics for Steganography Algorithm Quality", International Journal of Advanced Science and Technology, Vol. 29, No.02, (2020).

43 Sabah A. Giraffa," IMPLEMENTATION OF HIDING SECURED FINGERPRINT IN FACE IMAGE FOR BIOMETRIC APPLICATIONS", Vol. 20, No.1, January 2016.

44 Srikanth. V," Secret Image Hiding in an Enhanced Steganography Approach using IWT", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 5, Issue 4, April 2016.

45 Suhaila Mohammed, Shaymaa Ahmed, Ghusoon Mohammed, and Dhuha Abdul-Jabbar," Block-based Image Steganography for Text Hiding Using YUV Color Model and Secret Key Cryptography Methods", Australian Journal of Basic and Applied Sciences, 11(7) May 2017.

46 Tawfiq A. Al-Asadi,” Sound file hiding in fingerprint image”, Journal of University of Babylon,2013.

47 Wejdan A. Amer,” Efficient text in image hiding method based on LSB method principle”, Iraqi Journal of Science, Vol. 57, No.2,2016.

48 Zainab Bakar Dahoos,” Hide Encoded Text Within the Image by Using the Third Least Significant Bit”, Journal of University of Thi-Qar Vol.9 No.4 Dec. 2014.

7. CURRICULUM VITAE

Student Information	
Name/Surname:	Thulfiqar Muayad Hameedi
Nationality:	Iraq-Salah alddin-Tikrit
Orcid No:	0000-0001-8011-8524

School Information	
Undergraduate Study	
University	Tikrit University
Faculty	Computer Science and Mathematics
Department	Computer Science
Graduation Year	2017
Graduate Study	
University	Kırşehir Ahi Evran University
Institute	Graduate School Of Scıence
Department	Department Of Advanced Technologıes
Graduation Year	2023

Articles and Papers Produced from the Thesis