REPUBLIC OF TURKEY
SİİRT UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

STILL IMAGE STEGANOGRAPHY DETECTION BASED ON MACHINE LEARNING TECHNIQUES

MASTER DEGREE THESIS

ISAMADEEN ABDOLMUGHITH KHALIFA KHALIFA
163111007

Department of Electrical and Electronics Engineering

Supervisor: Assoc. Prof. Dr. Musa ATAŞ
Co-Supervisor: Asst. Prof. Dr. Eng. Subhi R. M. ZEEBAREE

JUNE– 2019
SIIRT

THESIS ACCEPTANCE AND APPROVAL

This thesis entitled as". Prepared by "**STILL IMAGE STEGANOGRAPHY DETECTION BASED ON MACHINE LEARNING TECHNIQUES**", prepared by Isamadeen Abdolmughith Khalifa Khalifa under the supervision of Assoc. Prof. Dr. Musa ATAŞ has been accepted as thesis study on the data 21/06/2019, as a Master degree in the Department of Electrical and Electronic Engineering at Siirt University, with majority votes by the jury below.

Jury Members **Signature**

President
Assoc. Prof. Dr. İbrahim Berkan AYDİLEK ....

Supervisor
Assoc. Prof. Dr. Musa ATAŞ ....

Member
Assist. Prof. Dr. Melih KUNCAN M. Kuncan ....

I confirm the above results.

Assoc. Prof. Dr. Fevzi HANSU
Director of the Graduate School of
Natural and Applied Sciences

ACKNOWLEDGMENT

First of all, thanks to ALLAH for giving me the strength and confidence to achieve my wishes. I would like to express my gratitude and appreciation to my supervisor's Assoc. Prof. Dr. Musa Ataş, and Asst. Prof. Dr. Eng. Subhi R. M. Zeebaree for guiding me throughout implementing this valuable study. Also, I extend my gratitude to lecturers of the Department of Engineering at Siirt University, for their inspiration and valuable suggestions throughout studying my courses. Asst. Prof. Dr. Yılmaz Kaya, and Asst. Prof. Dr. Volkan Müjdat Tiryaki. Furthermore, I want to convey my special thanks and appreciations to my cousin Farhad M. Khalifa for continuous help. Also, I don't forget to thanks to my parents, and all my brothers, sisters, and special thanks to my family to support me at all times.

2019
Isamadeen Abdolmughtih Khalifa Khalifa

THESIS NOTIFICATIONI hereby declare that this paper is my unique authorial work, which I have worked out on my own. Every information bases, references, and literature used or excerpted through an explanation of this work are correctly cited and listed incomplete reference to the owing cause.

Signature

Isamadeen Abdolmughith Khalifa Khalifa

Note: In this thesis, the use of original and other source notifications, tables, figures and photographs without reference, it is subject to the provision of law No. 5846 on Intellectual and Artistic Works.

CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

ABBREVIATIONS AND SYMBOL LISTS

Abbreviation	Explanation
TP	**:** True Positive
TN	**:** True Negative
FP	**:** False Positive
FN	**:** False Negative
LSB	**:** Least Significant Bit
DWT	**:** Discrete Wavelet Transform
CWT	**:** Continuous Wavelet Transform
LBP	**:** Local Binary Pattern
DCT	**:** Discrete Cosine Transform
ANN	**:** Artificial Neural Network
FLD	**:** Fisher Linear Discriminant
SVM	**:** Support Vector Machines
IQMs	**:** Image Quality Metrics
MBDCT	: Multi-Size Block Discrete Cosine Transform
ELM	: Extreme Learning Machine
CGCM	**:** Colors Gradient Co-Occurrence Matrix
GLCM	**:** Gray Level Co-Occurrence Matrix
DFT	**:** Discrete Fourier Transform
BPNN	**:** Backpropagation neural network
CODFT	**:** Co-Occurrence Matrix Discrete Fourier Transform
CODCT	**:** Co-Occurrence Matrix Discrete Cosine Transform
CM	**:** Co-Occurrence Matrix
BPP	**:** Bit per Pixel

Symbol	Description
a	: Constant
b	: Scaling
g[n]	: Low Pass Filter
h[n]	: High Pass Filter
X1, H [n]	: High pass filter Output
X1, H [n]	: Low pass filter Output
ψ	: Mother wavelet
d[n]	: High pass filter produces
s[n]	: Low pass filter produces
m_{pq}	: Central Moments
$[\ \phi 1 \ldots \phi 7\ ]$	: Seven moments

ÖZET

YÜKSEK LİSANS TEZİ

MAKİNE ÖĞRENMESİ TEKNİKLERİ TABANLI HAREKETSİZ GÖRÜNTÜ STEGANOGRAFİ TESPİTİ

Yüksek Lisans Tezi

Isamadeen Abdolmughith Khalifa KHALIFA

Siirt Üniversitesi Fen Bilimleri Enstitüsü
Elektrik-Elektronik Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Musa ATAŞ

II. Danışman: Asst. Prof. Dr. Eng. Subhi R. M. ZEEBAREE

Haziran 2019, 53 sayfa

Son yirmi yılda steganaliz bilimi, dijital bilgisayar dosyalarındaki veri gizliliğinin yanlış kullanılması ile geride bırakılan güvenlik risklerini en aza indiren verimli bir araştırma alanı haline geldi. Gizli yazının yayılması arttıkça, steganalize olan ihtiyaç ortaya çıktı ve yasadışı gizli iletişimleri engellemek için büyük ölçüde gerekli hale geldi. Bu tez, eş oluşum matrisini, frekans alanı dönüşümlerini, ilk üç momenti ve Geri Yayılımlı Sinir Ağlarını (GYSA) kullanarak hareketsiz görüntülerdeki gizli bilgileri tespit etmek için bir steganaliz sistemi sunmaktadır. İlk olarak, eş-oluşum matrisi, gizli bilginin taşıyıcısı olduğundan şüphelenilen giriş görüntüsü için hesaplanır. İkinci olarak, 12 alt bantla sonuçlanan üç Ayrık Dalgacık Dönüşümü (ADD) seviyesi uygulanır. Ardından, orijinal görüntü ile birlikte bu alt bantlar, 13 alt bant üretmek için Ayrık Fourier Dönüşümü (AFD) veya Ayrık Kosinüs Dönüşümü (ACD) tarafından işlenir. Bundan sonra, ilk üç momentten 39 elemanlı özellik vektörü hesaplanır. Son olarak görüntünün gizli bilgi içerip içermediğini belirlemek için bir GYSA sınıflandırıcısı kullanılır. Önerilen yaklaşım, eş-oluşum matrisi ve onsuz olarak her biri bir kez AFD ve bir kez de ACD kullanılarak test edilmiştir. Elde edilen sonuçlar önceki çalışmalara göre AFD ile birlikte eş-oluşum matrisini kullanmanın en yüksek performansa sahip olduğunu göstermiştir.

Anahtar kelimeler: Ayrık Dalgacık Dönüşümü, Ayrık Fourier Dönüşümü, Ayrık Kosinüs Dönüşümü, Eş Oluşum Matrisi, Geri Yayılımlı Sinir Ağları, Görüntü, Steganaliz.

ABSTRACT

M.Sc. Thesis

STILL IMAGE STEGANOGRAPHY DETECTION BASED ON MACHINE LEARNING TECHNIQUES

Isamadeen Abdolmughith Khalifa KHALIFA

The Graduate School of Natural and Applied Science of Siirt University
The Degree of Master of Science
In Electrical-Electronics Engineering

Supervisor: Assoc. Prof. Dr. Musa ATAŞ

Co-Supervisor: Asst. Prof. Dr. Eng. Subhi R. M. ZEEBAREE

June 2019, 53 pages

In the last two decades, steganalysis has become a fertile research area to minimize the security risks left behind by misuse of data concealment in digital computer files. As the propagation of hidden writing increased, the need for the steganalysis emerged and grew to a large extent necessary to deter illicit secret communications. This thesis introduces a steganalysis system to detect hidden information in still images through using co-occurrence matrix, frequency domain transforms, the first three moments, and Back Propagation Neural Network (BPNN). Firstly, the co-occurrence matrix is calculated for the input image, which suspected to be a carrier of hidden secret information. Second, three levels of Discrete Wavelet Transform (DWT) are applied resulting in 12 subbands. Then, those subbands along with the original image are transformed by Discrete Fourier Transform (DFT) or Discrete Cosine Transform (DCT) to produce 13 subbands. After that, the first three moments are calculated resulting feature vector with 39 feature. Finally, a BPNN is used as a classifier to determine whether the image is containing hidden information or not. The proposed approach is tested with and without co-occurrence matrix, each of them once using DFT and another time using DCT. The results showed that using the co-occurence matrix with DFT has the highest performance compared to previous studies.

Keywords: BPNN, Co-Occurrence matrix, DCT, DFT, DWT, Image, Steganalysis.

1. INTRODUCTION

Due to the tremendous development in the field of digital technology, the Internet, communications, and personal privacy has become more easily violated. There was a need to preserve the confidentiality of personal data when it was transmitted to prevent hackers from accessing it. The beginning of the last decade of the last century saw the emergence of the forefront of research on writing about hidden writing. Although hidden writing generally has deep roots in history, various methods of performing hidden writing have used, some primitive.

The end of the same decade saw the emergence of the first research that attempts to detect hidden writing in digital media. It was the beginning of the science of Steganalysis, the door opened widely for researchers to engage in the fields of hidden writing and steganalysis which become a fertile field of scientific research fields and produced countless methods. In this chapter, some of the key terms will be thoroughly identified and then some topics will be explained like hiding information, the dangers of hidden writing, the need to steganalysis, the importance of this research and its purpose, and the research plan for the remaining chapters.

1.1. Terminologies

Some terms need to know to delve into the subject of steganalysis. In the following illustrates these terminologies.

- Steganography

It is the art and science of hiding important secret data in an innocuous vector in a manner that conceals the existence of hidden data without causing suspicion to keep the communication between the two parties secret (Li et al., 2011). Steganography is a Greek word composed of two parts, the first "Steganos" which means hidden, covered or secret, and the second "Graphy" which means writing or drawing, so literally means hidden writing, covered writing, or confidential writing (Kobsi and Merouani, 2007).

- Steganalysis

Steganalysis is the technique and science that is used to decide if the messages are involved in the image or not by the steganography algorithm. Steganalysis system is utilized to find, extract, disable or change the message before arriving at the recipient (Bachrach and Shih, 2011).

The steganalysis art plays a major role in selecting traits or features that may characterize the typically embedded cover, while science helps to test the features chosen in a documented manner to determine whether or not there is hidden information (Kobsi and Merouani, 2007).

- Secret massage

Is the confidential information that is to be hidden by the steganography algorithm, whether inside the image, audio or video, also called payload (Hariri et al., 2011).

- Cover

The cover is the media or digital files used to include and hide the data to hidden, also called “Carrier” or “Host”, the cover can be text image, video, audio file, or other computer files (Gope et al., 2010). Figure 1.1 shows a simple illustration of stego media.

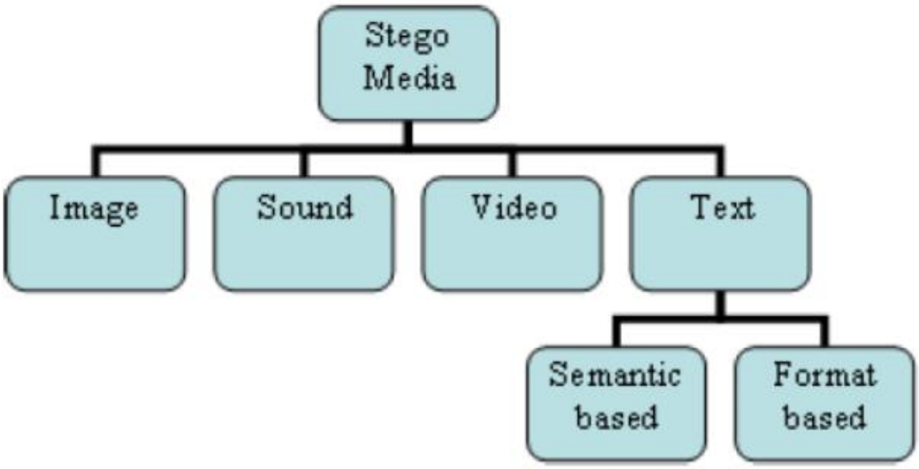


Figure 1.1. A simple illustration of stego media (Odeh and Elleithy, 2012).

- Stego-cover

It is the digital file after the message is hiding and merging it using the inclusion algorithm (Gope et al., 2010). The file quality usually decreases after the data is hidden, but make the hidden connection. The embedded cover must be indistinguishable from the original cover (Xie et al., 2011).

- Positive class

  It is an embedded image.

- Negative class

  It is the non-embedded image.

- True positive (TP)

  It can say that the situation is true positive if the result of examining the test image correct detected as an embedded image during the test.

- True negative (TN)

  It can say that the situation is true negative if the result of examining the test image correct detected as the non-embedded image during the test.

- False positive (FP)

  It can say that the situation is false positive if the result of examining the test image incorrect detected as the embedded image during the test.

- False negative (FN)

  It can say that the situation is false negative if the result of examining the test image incorrect detected as the non-embedded image during the test.

1.2. Steganography

The development of Internet and communication technology has helped to transmit data. For the reason opened communication there are dangers to the security of information and existence of a forbidden data. Steganography is the technique of hiding and transfers the data over a transporter which can be any digital file, for example, an image, text, video, audio, etc. through these transporters. Digital images are the more used in the hiding of information because they are widely used on the internet and they include a big number of redundant bits (Desai and Patel, 2016).

Since a long time ago there are hidden communications. There are two technics of hiding communication cryptography and steganography using image or text or video (Green et al., 2015).

The word steganography initially gotten from Greek words which mean "Covered Writing" It has utilized in different forms for a great many years. In the fifth century, BC Histaiacus shaved a slave's head, tattooed a message on his skull, and the slave sent with the letter after his hair became back. In Saudi Arabia at the King Abdul-Aziz City of science and innovation, a project was started to convert into English some old Arabic original copies about secret writing which are accepted to have been written1200 years ago. Some of these compositions found in Turkey and Germany (Cheddad et al., 2010).

Sometimes there is confusion between steganography and cryptography. But it is different. Steganography hides the presence of a message while cryptography hides of a message contain by the mix-up. Steganography science is an essential need due to the loss of privacy in today. Steganography allows people to communicate without the interference of others. Steganography techniques have been in increasing speed as its effectiveness in forbidding others from trying for decode a secret data hidden in the cover medium. For image-based steganography, many methods suggested but the most important and active method is the Least Significant Bit (LSB) to hide the secret data replaces the Least Significant Bit of pixels selected.

The confidential data embeds within a pixel of a cover image by the Least Significant Bit technique (LSB) directly. Each pixel of an image we can take the benefit from it at each pixel is of eight bits that store the value of color in each image. In each color pixels value changing by the Least Significant Bit to hide data. It can be replaced bit with a bit without changing the color value (Yadav et al., 2013).

Hiding information in the computer field is increasingly common in image and audio files in addition to other types of data Programs easy to download and easy to use and it’s free for steganography (Geetha and Kamaraj, 2010). Steganography technique of commercialization and application has spread widely in recent years due to International interest in research and development (Pevný, 2008).

Although steganography has big benefits in the security field and saves personal privacy, but everything has a negative side. There may be a danger to commercial activities and national security. For commercial spies or traitors maybe some of them abuse this technique for illegal activities. They may steal commercial secrets or technical messages and give them to competitive using steganography technique for large sums of money (Geetha and Kamaraj, 2010).

Figure 1.2. is a simple illustration to hide the writing in the picture where the message M is embedded in the cover image by the steganography algorithm. The result of the image which contains the letter M appeared to be like the cover of the original image and called that Stego image.

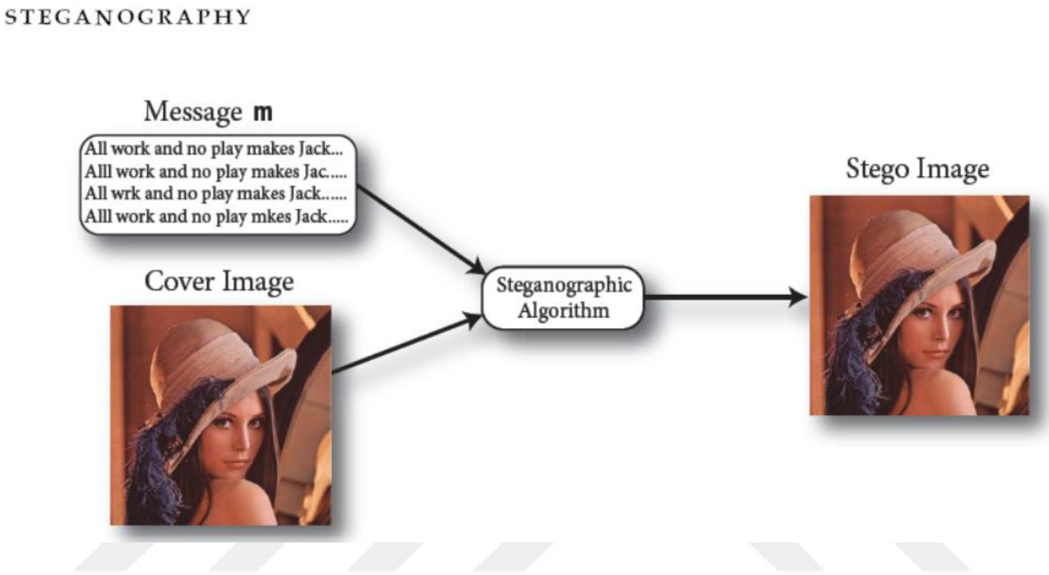

STEGANOGRAPHY
Message m
All work and no play makes Jack...
Alll work and no play makes Jac.....
All wrk and no play makes Jack......
Alll work and no play mkes Jack.....
Cover Image
Steganographic Algorithm
Stego Image

Figure 1.2. A simple illustration of steganography for an image (Miche, 2010).

1.3. Steganography Risks

Hiding information in digital computer files is becoming increasingly common. Free hidden writing software has become easy to download and easy to use (Kang, 2011). International attention has been growing in recent years to research and develop steganography techniques and applied them commercially (Pevný, 2008).

Although steganography has significant benefits in protecting rights intellectual property and the keeping of personal privacy, everything has a negative and positive effects. Hidden writing   perhaps occur the negative effects from a personal, business, and security perspective information. Some who have hidden motives perhaps misuse this technique for planning illegal activities to avoid the application of the law.

For example, some person may steal commercial messages or technical messages, and they deliver them to competitors using steganography techniques opposite large sums of money (Geetha and Kamaraj, 2010). In 2007 there was a case of commercial intrusion, leaked confidential information to a competitor company, used a hidden writing tool to hide the information in pictures and music files. Although the perpetrator of the work arrested in this case, it gives an idea of the vast space in which hidden writing can apply (Badr et al., 2014).

There are concerns that hidden writing techniques create a potential threat to information security. Because hidden writing ensures the confidentiality of additional information that is almost undetectable in digital products, the possibility of clandestine dissemination of information and malware is very large.

Current concerns also include the use of internet hackers and confidential communications to spy on sensitive data that are vulnerable to protection and disclosure of government secrets that have access to these secrets. Concerns also relate to the use of secret communications for criminal activities, such as cheat and the steal of financial or identity information, by hackers (Pevný, 2008).

1.4. The need for steganalysis

Misuse of hidden writing poses real risks at various levels. As the propagation of hidden writing increased, the need for the steganalysis emerged and grew to a large extent necessary to deter illicit secret communications. Steganalysis tools are very important for internet security professionals. Law enforcement agencies need good programs that can identify suspicious files on the computer or on the web (Davidson et al., 2005).

1.5. Steganalysis

Steganalysis is the art of seeing or detecting something invisible to separate the images that contain the hidden data or the secret messages from the clean images which have not to include the hidden data or the secret messages. Without existence, any information about the steganography algorithm the goal of this system is to collect any evidence about the presence of secret data (Kaur and Kaur, 2014).

Steganalysis stands against steganography, it attacks data hiding techniques. Law enforcement agencies and media are very interested in steganalysis and steganography techniques. The criminals can be misapplied steganography to plan criminal activities by insert the secret text in video, audio or images and send them to public sites. To overcome these types of problems, as it is tough to note and trace the recipient of the message, there is a need for breaking steganography. Steganalysis is a technique and science to breach steganography (Desai and Patel, 2016).

Steganalysis can be an active element to judge the safety performance of steganography techniques (Xuan et al., 2005). While steganography does modify statistical properties of images, may be taken the unnatural distortion. Can use tools to separate the main contains from media with the covered message, designed to detect hidden information (Al Bouna et al., 2015).

The steganalysis study aims to find adequate guides to the embedded message to cut the security of its transporter. Several features extracted from the main part and stego media, in most of the techniques to training the classifiers, which are applied to take the decisions main or stego for fishy media. The focal point of the proposed work regards picture steganography.

There are different techniques to distinguish whether there are hidden messages in pictures. In general, embedding of secret message in the pictures using steganography methods produces apparent artifacts. In unlocking channel such as the internet, to check the presence of a secret message, it is very difficult to perform optical testing on many images. Therefore the growth of methods to automate the detection process will be very useful to the steganalysis works (Suryawanshi and Mali, 2016).

The technique of steganalysis discovers the presence of hidden writing within a digital medium voice, video or image. It is very important to develop this technique. Documents that contain hidden writings called the cover documents and the documents that do not include hidden writings called clean documents. Again, the concept of steganalysis is very different from the concept of cryptanalysis (as cryptography is different from steganography).

In cryptanalysis, the objective is to break the code and then get the encrypted message. The steganalysis is not intended to get the hidden message in the cover, the main objective is whether there is a message hidden in the digital medium or not (Miche, 2010).

Steganalysis usually performed by one of these methods, signature analysis, and blind detection. In the signature analysis, the method of steganography is known beforehand. It making detection easier, the embedding algorithm always leaves a partial signature, which can track for detection, On the contrary, the method of blind detection does not know the method of concealment, although this disclosure is clear that this technique is the most used, it is more difficult to implement (Luo et al., 2008).

In a simplified way in this picture Figure 1.3 has been clarified the classical steganalysis process a suspicious image is processed by steganalysis to separate it to genuine or stego.

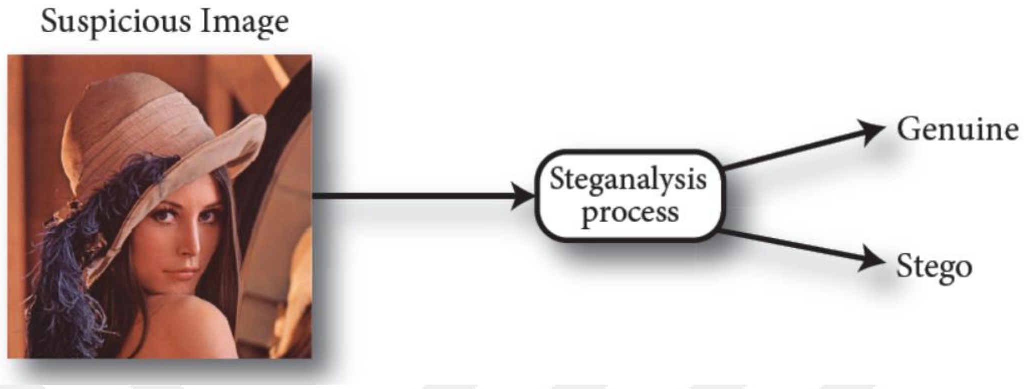


Figure 1.3. The classical steganalysis process (Miche, 2010).

A suspicious image was identified using steganalysis as a real form. In other words, steganalysis is the treatment against information hiding methods, for detection and extraction, destruction and processing of hidden data in a stego object, Figure 1.4 displays steganalysis, and steganography processes.

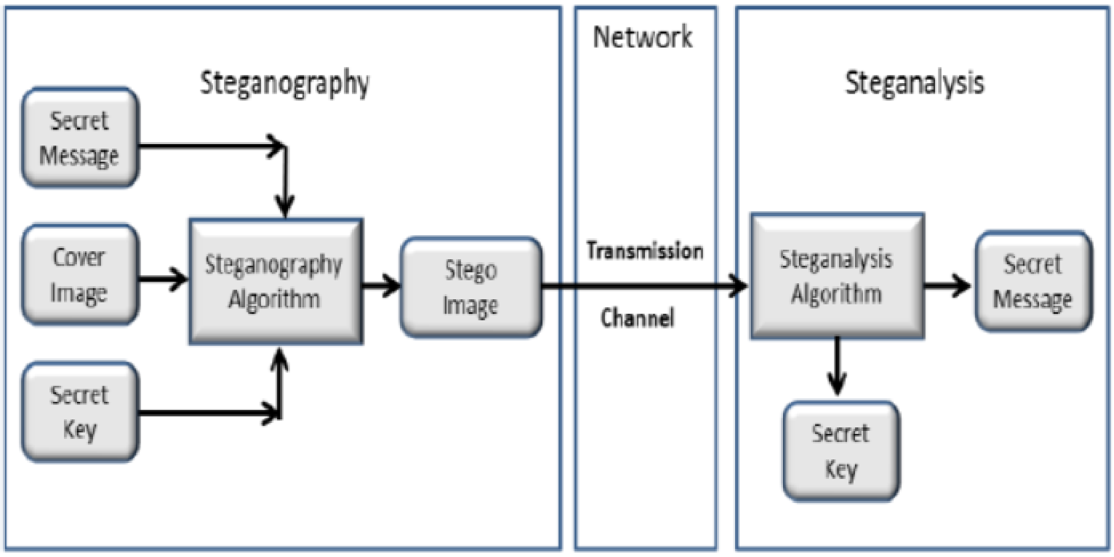


Figure 1.4. Steganography and Steganalysis Processes (Badr et al., 2014).

1.5.1. Steganalysis Techniques/Types

Steganalysis method can be categorized as follows:

1. Targeted Steganalysis

The technique of targeted steganalysis works on a specific type of hidden information planner and sometimes restricted to a particular kind of image.

2. Blind Steganalysis

To the work on all types of embedding methods and image formats, for these reasons, the blind steganalysis method is prepared.

3. Quantitative Steganalysis

The method of quantitative steganalysis differs from the qualitative steganalysis method. It predicts the length of the hidden information that has embedded in the medium of the cover.

4. Forensic Steganalysis

At last, the forensic steganalysis goes behind the discovery stage of the classical steganalysis getting the real steganography. There are several potential details which the spy might want to get about the message (Miche, 2010).

1.5.2. Common steganalysis approaches

Generally, a large number of binary cells are used to cover the secret message. A hiding process may leave a trace or imprint marks on the cover. Any deformation in the properties of the cover image enables the classifier to detect the hidden message. In some steganalysis techniques, we must have the original cover beside with the included cover to comparative analysis, as follows some common steganalysis technics (Chandrababu, 2009).

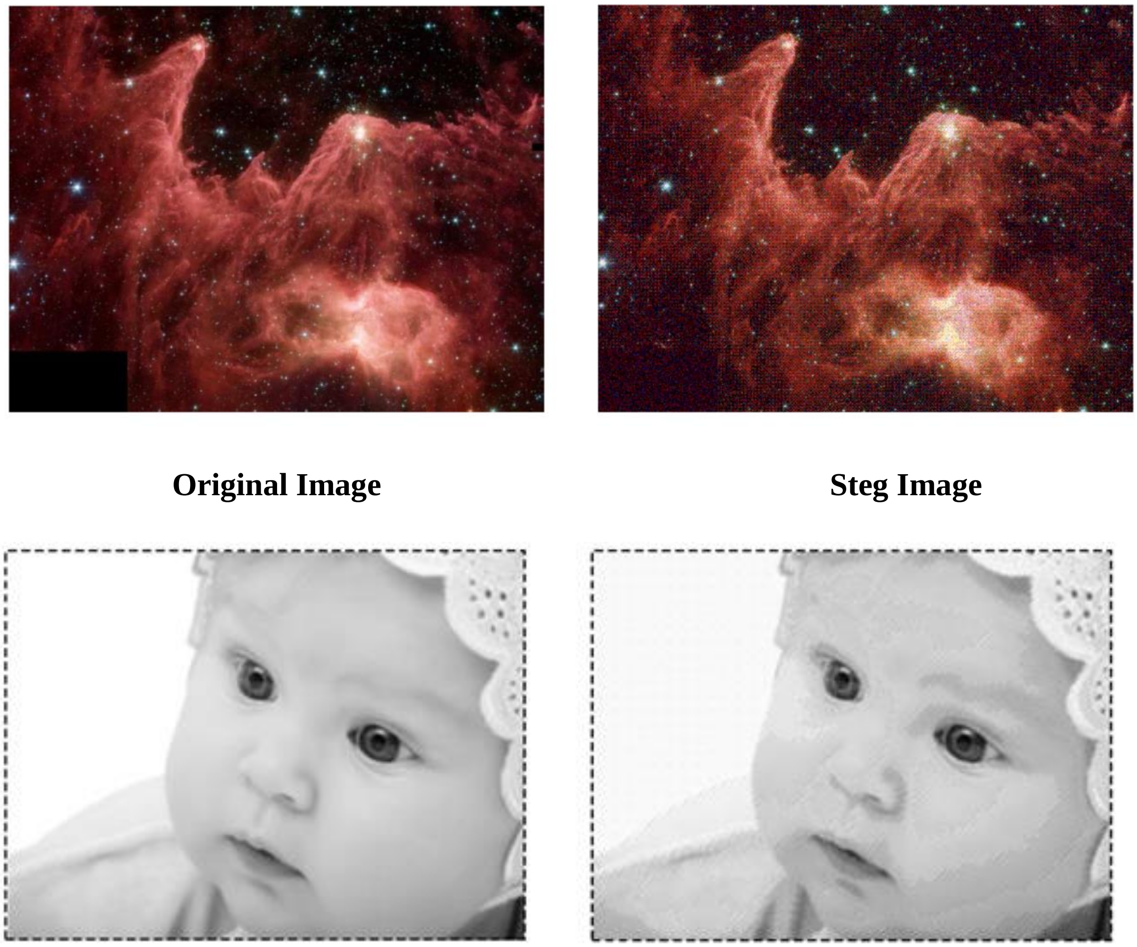
1. Visual detection

Maybe it is enabled to distinguish or detect secret data in stego images, by looking at the repetitive models. These repetitive models might detect the identification or signature of a steganography tool or secret data. Even small deformation can distinguish or detect the existence of secret data (Richer, 2003).

This method can be use JPGand BMP or other image formats. When the image file contains confidential data, the distortion may appear, be visible, and may be diagnosed with the naked eye. Distortions or visual patterns of the human eye are the objects of the detector. The standard for diagnosing such patterns is to compare the cover size with the original coverage and visual differences. Accurate ultrasonography observed when the lid compared with the built-in cover.

These minor distortions may pass without be noted without assistance such comparison. For example, distortions that enter into the voice may the noise generated by the clamping process is distorted by JPG but this noise is highlighted in the cover embedded when compared with the vertical cover. Such noise may be acceptable as an integral part of the sound is not used for comparison with the cover and passes without notice (Johnson and Jajodia, 1998).

With a simple concept of visual detection, compare the image with the original image to see if there is a difference between the two images (Rasool, 2017). Figure 1.5 shows an example of visual detection.



Original Image **Steg Image**

Original Image **Steg Image**

Figure 1.5. Visual steg detection example (Chandrababu, 2009).

2. Audible Detection

In order to determine the secret inclusion in this method the distortion in the WAV and MPEG files must be taken into account.

3. Structural Detection

In this method, the detection performed by comparing the properties of the embedded cover file and its contents with the properties of the original cover file and its contents. The characteristics that are likely to be changed include:

- Disagreement in image sizes.
- Disagreement in dates or times.
- A change of the content file.

A modification in the checksum values (Chandrababu, 2009).

4. Statistical Detection

This method of detection is also known as histogram analysis. This method analyzes the changes in the image point patterns of the embedded cover. In particular, we work on the least significant bits. Most steganalysis algorithms and tools fall within this type of steganalysis techniques (Chandrababu, 2009).

5. Signature Tracing

This method depends on signatures that lag behind the embedded cover during the embedding process. You can find clear and repetitive patterns in the cover that included the original cover image and note the differences between them. By replicating comparisons of a number of images, these patterns begin to appear as possible signatures for data hiding programs and tools.

1.6. Wavelet

Some basics are needed to understand wavelet. The signals that are coming from the source are usually on the timescale. Examples of this are biomedical signals, sinusoidal signals, and other signals, which of these signals can be processed in the time domain and can be processed by converting them to the frequency domain using mathematical conversion equations. Fourier transformations are one of the most popular conversion equations to convert signals from time domain to frequency domain and without losses.

When the signal drawn on the time domain, we use the time on the x-axis and the amplitude on the y-axis. The hidden information in the message cannot be detected in the time domain. In this case, required to transform into the frequency domain. The frequency on the x-axis in the frequency domain and amplitude on the y-axis can be considered the wavelet transform as a mathematical tool to transfer the signal from a time scale to various form (Yan et al., 2014).

Where the use of wavelet in processing of digital signal and images. The use of the wavelet for this purpose is a modern development, although the theory is not new, similar to the theory of Fourier. The wavelet term was depended to express the concept of a short signal or shortwave (Domingues et al., 2005).The wavelet transform can be classified as Continuous Wavelet Transform (CWT) and Discrete Wavelet Transform (DWT).

1.6.1. Continuous Wavelet Transform (CWT)

Equation (1.1) depicts the continuous wavelet transform

$$Xw(a,b) = 1/\sqrt{b}\int_{-\infty}^{\infty} x(t)\psi\left(t-\frac{a}{b}\right)dt \tag{1.1}$$

Where x(t) is the input, ψ(t) is the wavelet function, the constant *a* is the place supposed through a real number and *b* is a scaling supposed through any positive real number. There are many kinds of wavelets function that can be applied.

1.6.2. Discrete wavelet transform (DWT)

The block diagram of discrete wavelet transforms is shown in Fig 1.6

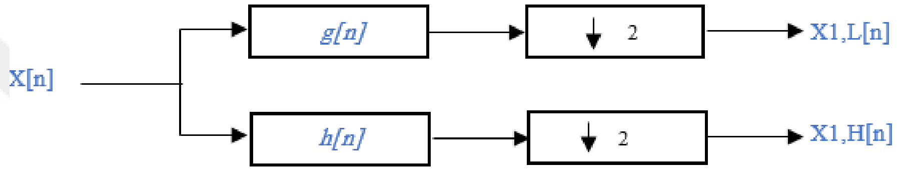


Figure.1.6. The discrete wavelet transform block diagram(Balakrishnan, 2013).

x[n] is the input, g[n] is a low pass filter, h[n] is the high pass filter 2 is the sampling factor, X1, H[n] is the high pass filter output, X1, L[n] low pass filter output. g[n] is the same wave function in the continuous wavelet transform, and h[n] is simply such as scaling function in the constant wavelet transform (Balakrishnan, 2013).

1.7. Problem statement

Security concerns have increased in recent decades due to the evolution of information technology and the penetration of these technologies into all the details of our daily lives. These concerns have led to the appearance of technology to hide information in images and multimedia to protect privacy. However, misuse of this technology has shown serious security concerns to exploit this technology by terrorists and information thieves from corrupt employees in companies to leak sensitive data, so it is necessary to develop detection techniques against hiding information. This research looks about an efficient way to solve this problem and detect the hidden information.

1.8. Research aim

The research aims to find more efficient methods in the field of steganalysis on the passive side. It aims to build a system capable of detecting the existence of secret data hidden by the algorithms of steganography in color images or shooting reliably. This is done in order to detect the secret communication between unwanted suspects and other destinations such as infiltrating business secrets from a particular institution or sending sensitive information from spy clients.

1.9. Thesis outline

This thesis is organized in five chapters. Chapter 1 presents the entire work and provides an overview of the topics discussed here. Chapter 2 is about literature review and the previous works. Methodology and the proposed model is introduced in Chapter 3. Implementation and results of the proposed system is provided in Chapter 4. Conclusions and future works are drawn in Chapter 5.

2- LITERATURE REVIEW

Trivedi and Chandramouli (2003), presented a method to analyze concealment by exploiting the sudden change in data due to Sequential Steganography. They used extremely effectively spread spectrum steganography technique to find length and locations of secret messages. The method of locating the hidden message and its length using sequential hiding algorithms presented the analytic derivations of cases when hiding coefficients are fully or partially known (Trivedi and Chandramouli, 2003).

Berg and et al. (2003), proposed a method of concealment analysis using machine learning techniques. The researchers used machine learning algorithms to distinguish images into a cover and an embedded cover based on characteristics taken from these images. The machine was pre-programmed to be able to distinguish this image. The algorithm they used was novel, and they also claimed that more sophisticated algorithms could be better detected in steganalis (Berg et al., 2003).

Shaohui et al. (2003), proposed a new method of detecting secret message, using transformations to the frequency band. After that obtaining some statistical characteristics to present them based on the neural network to obtain statistics features of images to identify the underlying hidden data. At the first, extract features of image embedded secret message, and delivered to the neural network to get output. The back propagation artificial neural network used to distinguish whether the image contained confidential data or not (Shaohui et al., 2003).

Lafferty and Ahmed (2004), introduced the texture base steganalysis system using a Local Binary Pattern (LBP) texture operator to examine the patterns of neighboring cells across color levels, causes disturbances in the relationships between neighboring pixels. A method for steganalysis using LBP texture process to examine the pixel texture samples presented.

Some statistical properties extracted to form the input vector for the neural network. Statistical characteristics included the values of the delta change of the histogram of the (LBP) factor as well as the first level statistics (Mean, Variance, Entropy) derived from the histogram (Lafferty and Ahmed, 2004).

Trivedi and Chandramouli (2005),introduced the method of detecting the secret key in the inclusion of secret data using sequential hiding algorithms, A theory developed for detecting sudden, jumps in the statistics of the stego signal through steganalysis. Efficiency of the system depends on the nature of the hiding. In the case of hiding in the low frequency of DCT, the system is inefficient. It is shown extensive experimental results are to demonstrate the strengths and weaknesses of the suggested steganalysis algorithm (Trivedi and Chandramouli, 2005).

Ambalavanan and Chandramouli (2005), presented a method of analysis of hidden message guessing based on Bayes theory, by forming a random Markov image, and using symmetry between images and automated statistical systems. Where has dealt only with the detection of a secret message and estimation of some of its parameters this method attempts to connect the cover image with the embedded cover by a function of the probability (Ambalavanan and Chandramouli, 2005).

Davidson et al. Presented (2005), an automatic classifier artificial neural networks to differentiate images that have hidden data and clean based on multiple properties derived from wavelet transformations (Davidson et al., 2005).

Xuan et al. (2005), Proposed a general blind image steganalysis system in which the statistical moments of characteristic functions of the prediction-error picture, they used the artificial neural network as a classifier, the test picture, and their wavelet subbands chosen as features. The performance of the proposed steganalysis system is significantly better than the previous techniques (Xuan et al., 2005).

Kumar and Reddy (2007), proposed a comparative study of three techniques of steganalysis. He investigated and compared the performance of each technique in the detection of methods of inclusion. A procedure may help a legitimate examiner to decide on the methods of detection to achieve better results in terms of time and accuracy.

The steganalysis techniques which compared and analyzed are aimed to detect the secret message in JPEG images. Steg detect, DA (FLD) Discriminant Analysis based on Fisher Linear Discriminant classification, DA (SVM) Discriminant Analysis established on Support Vector Machines, and Breaking F5. Both DA (FLD) and DA (SVM) are classification techniques. The detection logic in both is the same, i.e., the features used for the classification are the same, and only the methods used for the classification are various (Reddy and Kumar, 2007).

Zhang et al. (2008), Processed the blind image steganography detection, this paper suggests a new detection model. Image steganography detection can be treated as a two-class pattern recognition problem, which builds the model using moment features, also some image quality metrics (IQMs) extracted from the given test image and properties derived from Multi-Size Block Discrete Cosine Transform (MBDCT) and then used artificial neural networks Specifically the Back Propagation Algorithm, is a classification of these properties (Zhang et al., 2008).

Nissar and Mir (2010), presented a papering which they distinguished and gave an account of the different approaches that have been suggesting for steganalysis. Categorized and presented different methods proposed for the system of steganalysis. Some promising methods of statistical steganalysis (Nissar and Mir, 2010).

Thiyagarajan et al. (2011), He was proper interested in global image steganalysis approach which used RGB to HSI color model conversion. Any global Steganalysis algorithm developed should be tested with different Stego-images to prove its efficiency. The developed global Steganalysis algorithm tested in Stego-image database which obtained by implementing different RGB Least Significant Bit steganography algorithms. Suggested using the color conversion system model and visual perception to distinguish between the stego and the cover image, this is in order to develop the steganalysis algorithm (Thiyagarajan et al., 2011).

Gong and Wang (2012), proposed the steganography detection algorithm based on colors gradient co-occurrence matrix (CGCM) to the GIF images. (CGCM) Is built with colors and gradient matrix of the GIF image, and 27-dimensional statistical features of (CGCM), Which are between adjacent pixels are sensitive to the color relationship and break the image texture, are extracted. Support vector machine (SVM) methods make the 27-dimensional statistical features to steganalysis secret message in GIF images. Experimental results mention that the suggested algorithm is effectively more than several GIF steganography algorithms and steganography tools (Gong and Wang, 2012).

Aljarf et al. (2013), Proposed a steganography detection system for both color and gray images based on four features which are homogeneity, correlation, contrast, and energy, using grey images for steganography has many limitations. A developed detection system presented in this paper. The first side of work involves making a set of step images. These Stego-images have various image file style. So, these stego-images have been done using three steganography tools: S-Tools, F5 algorithm, and open stego.

The make Stego-images are utilized to train the detection system in the next step. However, the second side of the work involves detecting the secret message. So the co-occurrence matrix makes for all images, in order to do detect the hidden data. A number of image features extracted from the matrix. These features are necessary to distinguish between the Stego images and the clean images (Aljarf et al., 2013).

Bhasin and Bedi (2013), proposed a novel blind steganalysis operation, for colored JPEG images. They distinguished the images into clean images or stego images, Extreme Learning Machine (ELM) has used. The images contain 810 features this feature set used for classification. First 405 features applied to correlations among JPEG coefficients of the image are based on Markov random process. To get the remaining 405 features calibration is applied to these Markov features. These standardized features are the variance between Markov features of a reference image and the Markov features of the image. It obtained by decompressing, cropping and recompressing the image.

The experimental outcome shows that our proposed ELM based steganalysis method outperforms another SVM based steganalysis process, in terms of the percentage of correctly distributing images and in terms of time taken for both testing and training. Due to the fast learning time of ELM makes the fast speed of the proposed method is useful for real-time steganalysis (Bhasin and Bedi, 2013).

Kaur and Kaur (2014), made a review of various steganalysis techniques. Steganography and steganalysis have developed. Steganography and steganalysis received a great deal of attention from law enforcement and the media. Many robust and strong methods of steganalysis and steganography, can be considering the methods of steganalysis that are to use for this operation. This paper giving several ideas about steganalysis and its method (Kaur and Kaur, 2014).

Eichkit et al. (2015), explain how gray level co-occurrence matrix can be suitable, to do on 3D images of seismic data. (GLCM) can supply important insight into the subsurface during attribute analysis. Many authors have shown the GLCM is a beneficial tool for the description of seismic face. Because (GLCM)-based attributes can be calculated in various directions, it can be used to determine directional variations in seismic data. It opens the door to distinguish between sedimentary face and sample of fracturing, involving the delineation of fractured zones and their strike and dip (Eichkitz et al., 2015).

Di Ruberto et al. (2015), for medical color image classification proposed various color space. They started by decomposing the color image to the three channels Ch1, Ch2, and Ch3, obtaining three various images. To extend the classical grey level texture features to color texture features. Use the classical implementation and pass to them every time a different color channel, it most intuitive way to take into account color information for the computation of texture feature.

The results of the collection is a feature vector nine time larger from the classical feature vector, consist of three inter-channel feature vector (Ch1, Ch1), (Ch2, Ch2) and (Ch3,Ch3) and six inter-channels feature vector (Ch1, Ch2), (Ch2, Ch1), (Ch1, Ch3), (Ch3, Ch1), (Ch2, Ch3) and (Ch3, Ch2). The combination did not involve the three channels as one vector (Di Ruberto et al., 2015).

Desai and Patel (2016), has made a review of various steganalysis algorithms. Performance of any image steganalysis algorithm based on the sensitivity of features and amount of secret data in an image. Image steganalysis finds its application in the field of digital investigation. Evaluate the performance of (DWT) feature based steganalysis algorithms against various state-of-art steganography methods and variable message embedding rates is the goal of this paper. The classification and feature selection are the two main steps of the steganalysis algorithm. and also has made the comparative performance of individual algorithms to various classification methods. Where the evaluated against Stego images generated by steganography tools available for data hiding methods like LSB, blind hide, DBS, hide seek, DFF and F5 (Desai and Patel, 2016).

Rasool, (2017) presented a steganalysis model to detect the presence of secret data in RGB color images. Where uses statistical texture features and machine learning techniques. The work analyzes features of an RGB image as a composite unit, also analyzing individual color channels and dual combinations of the channels. The feature set used in this thesis consists of 26 features per channel, which involves the Gray Level co-occurrence Matrix (GLCM) features of contrast, correlation, homogeneity and energy, calculated for 2-bit, 3-bit half-bytes and full bytes fragments of individual channels, skewness of full bytes and half-bytes, entropy of full bytes and half-bytes, and also statistical features.

The features applied to single channels, and the single channel features merged into dual and three-channel image feature sets. The Support Vector Machine (SVM) algorithm is the machine learning binary classifier that selected for this work. Also datasets created from the clean images datasets, which were involved with hidden data using 2LSB and 4LSB stenography method (Rasool, 2017).

Zeng et al. (2017), proposed a general hybrid deep-learning framework for JPEG steganalysis. The proposed structure includes two-phase. The first stage is hand-crafted, corresponding to the quantization, convolution, and truncation of the rich models. The other phase is a compound neural network in which the parameters are learned in the training procedure (Zeng et al., 2017).

3. MATERIALS AND METHODS

In this chapter, to investigate from the aim of the research, this work is followed by an empirical approach. Where the detection of secret data in the image requires the analysis of relevant data about the image as necessary to improve detection performance.

3.1 Summary of the Proposed Model

The suggested model goals to uncover the presence of a secret message that has embedded into a cover image. Where the reveal task established on previous training of the classifier on the features of a dataset of Stego and clean images, by using supervised learning methods.

The statistical features of the suggested model consist of: Passing the input images to co-occurrence matrix features of contrast, on three levels (DWT) using haar wavelet. After that histogram is taken for each subband, passing from (DFT) and through (1st, 2nd and3rd) order moments. Using (BPNN) to classify the image into stego or clean.

3.2 Artificial Neural Networks ANNs

The artificial neural network is a widely distributed processor it consists of easy processing units. Which have a natural tendency to store experimental knowing and make it ready for usage? It is similar to the brain from two sides:

1-The acquisition of knowledge through the network takes of its environment through learning operation.

2- To store the acquired knowledge are utilized Interneuron connection force, known as synaptic weights (Collins and Tissot, 2016). The following picture shows you the neuron in the simplest cases: Figure 3.1 and Figure 3.2.

The artificial neural network is signal processing systems are trying to simulate the behavior of information processing methods. With a mathematical model of neurons interconnected in the network. And is a study of networks of adaptable nodes that store experimental knowledge acquired from a learning process from previous models and make knowledge usable (Collins and Tissot, 2007).

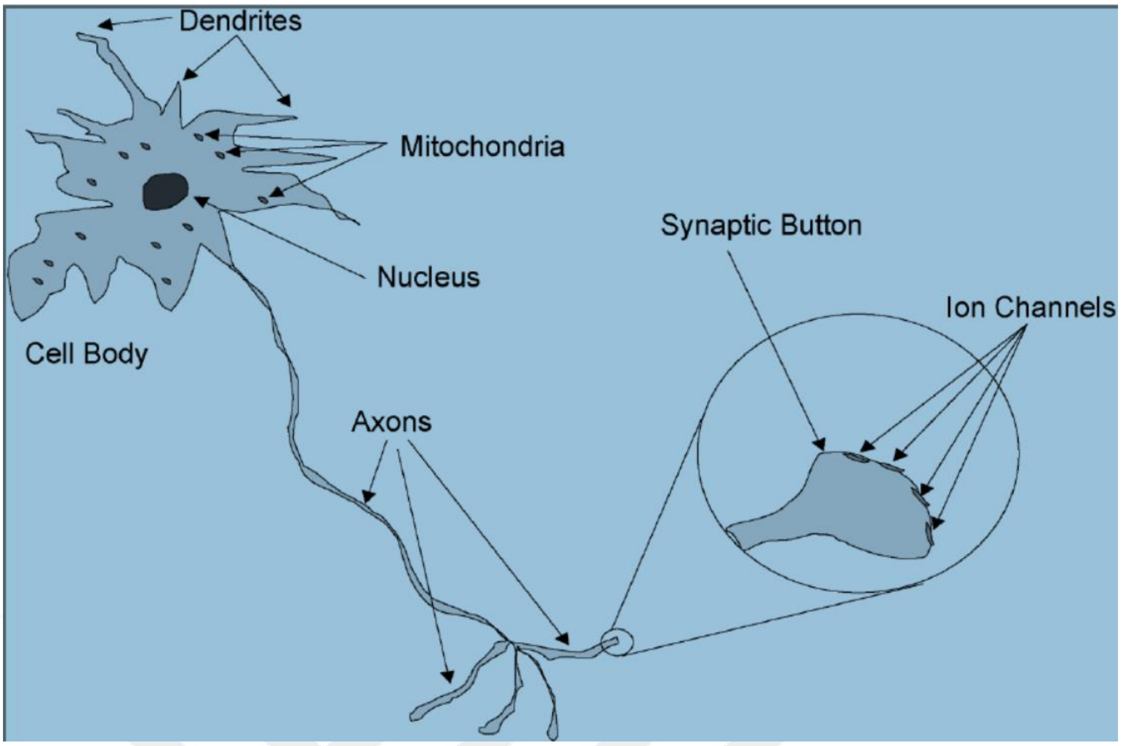


Figure 3.1. A neuron cell (Priddy and Keller, 2005)

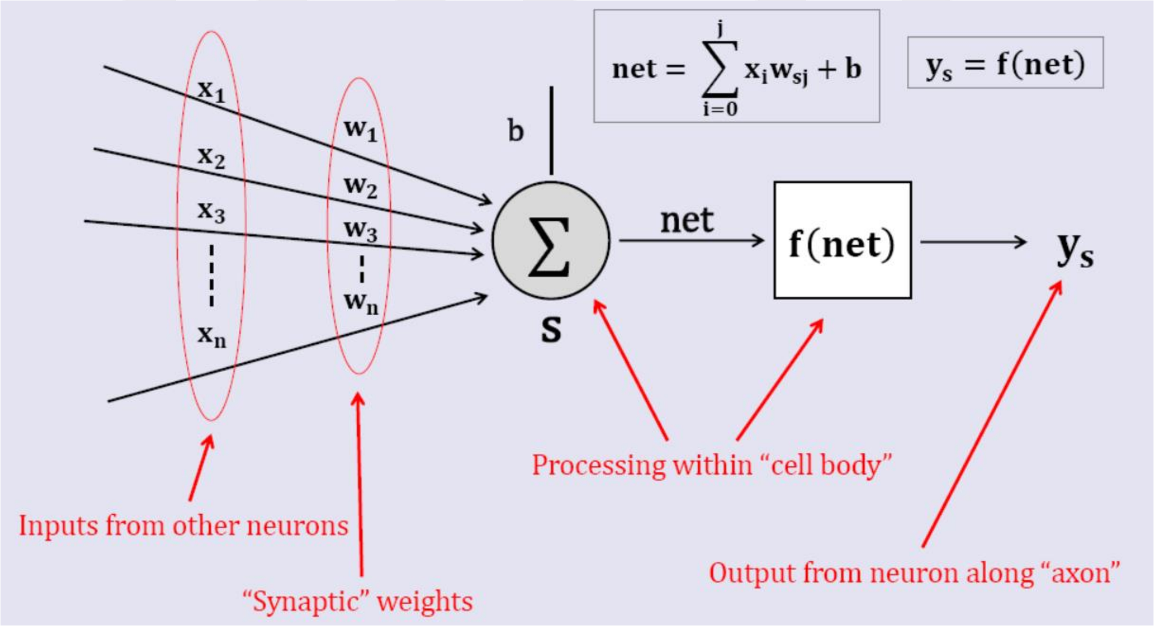

x_1
x_2
x_3
x_n
w_1
w_2
w_3
w_n
b
$\text{net} = \sum_{i=0}^{j} x_i w_{sj} + b$
$y_s = f(\text{net})$
Σ
S
net
f(net)
y_s
Processing within "cell body"
Inputs from other neurons
"Synaptic" weights
Output from neuron along "axon"

Figure 3.2. The Biological Neural Network: Single Artificial Neuron (Priddy and Keller, 2005).

This cell. Which you see above, starts its work when you receive the signal that comes from another cell. The neuron receives that signal through the dendrites. When the cell receives the signal, if the signal is within that range, the cell is conducting a fire, meaning that this cell also sends a signal to the rest of the cells in the neural network, and the transmission channel is as clear in the axon image, cells interconnected from one another the synapses.

3.2.1. Solving Problems with Neural Networks

Why all this trouble? Why do we want to emulate this neural network? What is the benefit of the simulation process? Perhaps these questions are in the mind of man, one of the most important reasons is to improve your ability to solve problems, and to understand what can do with ANN and things that cannot do ANN.

As a programmer, you have to specify when to use purely programming methods such as function and when to use methods dedicated to a particular type of problem ANN, therefore, increase your productivity with minimal losses.

There are some problems where you should use neural networks and some problems that you should use other ways. When you have a task, there were clear steps to solve this problem. This problem is not within the ANN, solve it in any other way, for example, you have a task requires that the program is constant never change, for example, to search or arrange, here of course also ANN Suitable for the whole and may lead to undesirable results. Programs that do not have a clear algorithm to solve are a good indicator of how to choose ANN as a way to solve. Pattern recognition also gives you a certain pattern (image, sound file, numbers), and your program recognizes this pattern trained.

Another type of problem that ANN offers is an excellent solution, optimization issues. Here, you can choose the best way to perform a task. For example, the problem of the seller who wants to visit several cities and wants to choose the shortest route that leads to the travel salesman problem, of course, this problem can be solved using traditional methods but taking a long time, will not come out the perfect solution.

Another type of problem is near to recognizing the style is a classification in this type of issues you have a set of patterns (images, sound, etc.) and you want to divide them into groups, each style goes to the appropriate section (Heaton, 2008).

3.2.2. Neural Network Components

1- Input layer: It receives data from its various sources so that each entry represents one characteristic and contains a number of processing elements equal to the number of independent variables that are considered inputs for the model (Heaton, 2008).

2- Hidden layer: The process of detecting and distinguishing the properties, the classification, and analysis of inputs by giving specific weights. Each it uses an analytical function to adjust those weights Based on the comparison of the target results depends on the selection of the number of treatment elements in that layer on the trial and error and to achieve the best performance of the network (Heaton, 2008).

3- Output layer: it sends the results generated in the previous stage to the user and contains that layer on one or more treatments, we derive the value of the final output of the neural network (Heaton, 2008).

4- Processing elements: Are processing units in which calculations made in which weights calculated and obtained the appropriate reaction for each input of the network (Ng, 2003).

5- Connection nodes: connect the processing elements in the different layers together. The structure of the neural network formed. Each component performs calculations independently of other processing elements, but all elements of the processing do so simultaneously, and each node helps communicate the different values between the structure of the network until it is done the interaction and integration among them in order to achieve the best performance of the network.

6- Weights: The weights expresses the relative importance of each input to the treatment element. It determines the strength of the relationship between the two treatment elements. It also shows the effectiveness of the communication between the input and the operating area. The weights used when performing the calculations to reach the actual outputs.

7- Summation function: This function calculates the relative weights of all inputs to the processing elements by multiplying each input with its weight.

8-Transfer function: It is a mathematical Equation formula that determines the output quality of the operating elements taking consider the quality of inputs and weighted weights (Collins and Tissot, 2016).

9-Learning rate: Determines the value of correction on which the adjustment is made in the weights during the neuron training process. The learning rate is a small value that increases with the learning times until we access the optimal solution, while at the same time reduce the error (Heaton, 2008).

3.2.3. Types of the neural network

Perceptron: It is one of the oldest and easiest types of neural network, it is a simplified form of the Feed-Forward Neural Network where there is one type that contains a (single layer) the other contains more than one layer (Multi-Layer Perceptron). In generally the task of this model is classification. The Single Layer Perceptron is called a linear classifier, meaning that the network resolves linearly separable problems (Alpaydın, 2010).

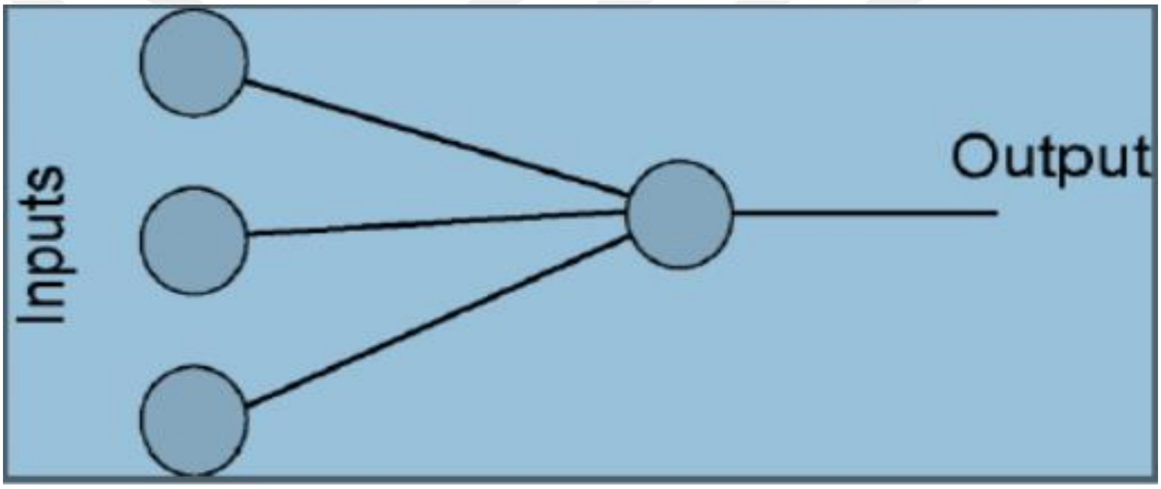


Figure 3.3. Single layer neural network. (Priddy and Keller, 2005).

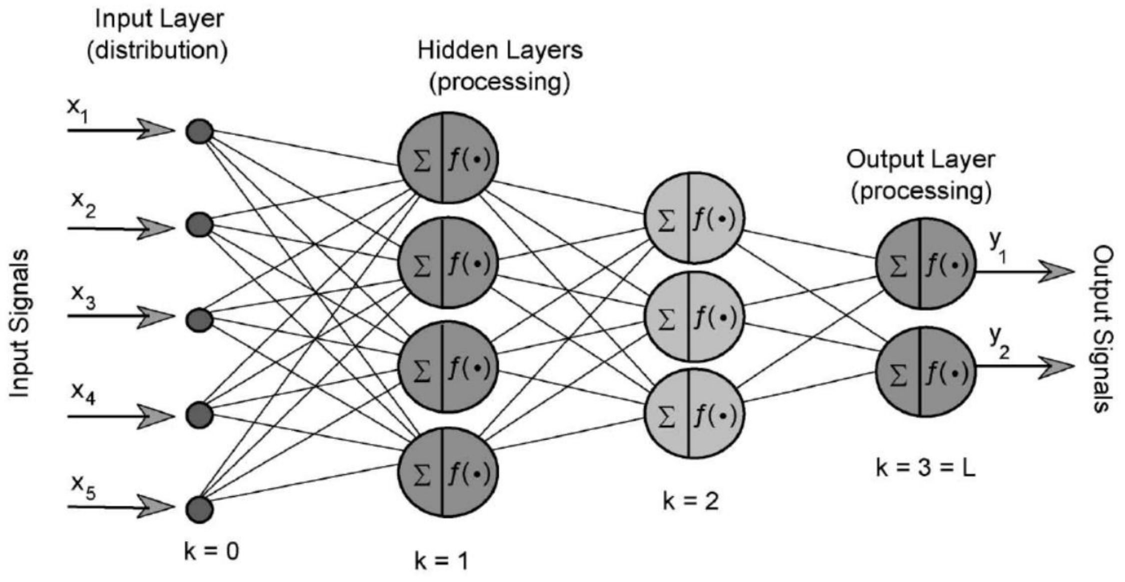


Figure 3.4 multi-layer neural network. (Priddy and Keller, 2005)

Feedforward neural networks: They are networks that are free of a closed loop of interconnections between their constituent units. These networks are the most used neural networks. The network consists of at least two layers, often with hidden layers between the input layer and the layer Outputs, and arithmetic moves in one direction forward from the input layer to the output layer across the hidden layers the most important one of them:

Backpropagation feedforward neural network: is a type of network that trains by supervised and uses in many fields. The idea of reverse propagation of the training of multilayered neural networks came after single layer neural networks. This network has given the extensive field of training. Training of this network in reverse propagation involves three stages:

1-Front feeding stage for input patterns.

2-The stage of computation and the backpropagation of the output errors.

3-Weights tuning stage.

After these three stages, the network testing stage begins.

3.2.4. Artificial neural networks training

Learning in neural networks produces new data in the network as a result of weight change. The network trains a set of inputs to provide the required output and training is achieving sequentially on the input vector when the network weights change according to specific laws. During training, the network weights gradually approach the ideal values, and the input works to show the desired output. The training of the artificial neural network is two types.

Supervised Training: In this type the information is displayed in the input pattern, the target pattern, and uses the network the difference between the two forms in calculating the error function that is used to adjust the value of weights in order to reduce the difference between the two forms the process of learning done in several stages.

Unsupervised training: it means that the network has some information during the training. It only has inputs and weights and has no knowledge of output result for comparison. Cohen and others discovered this type of training. The training group consists of the input vector and the training algorithm to change the network weights to produce the fixed output vector, as the input applied to the specific output.

3.3. Structure of the Proposed System

The method used to detect hidden data in images depends on the extraction of certain characteristics of the images to determine whether they contain secret data or not. And then classify that characteristics to determine the extent to which these images include hidden data. In this study used multiple methods in extracting features from images to use in the discovery of hidden data in those images and used the back propagation neural network (BPNN) to classify these properties. The following sections illustrate these methods.

3.3.1. Structure of DFT

When inserting the image into the system, it is applied to three levels of discrete wavelet transform (DWT) using the Haar filter. For each level 4 sub bands, the total is 12 sub bands, and the original image is added it, to be 13 sub bands after then the histogram is calculated for each sub band then discrete Fourier transform (DFT) is applied to each histogram and applied the equations of the first three moments from the seven-moment equations. The vector result is 39 elements. Sends to the classified (BPNN) to determine if the image is clean or contains a hidden.

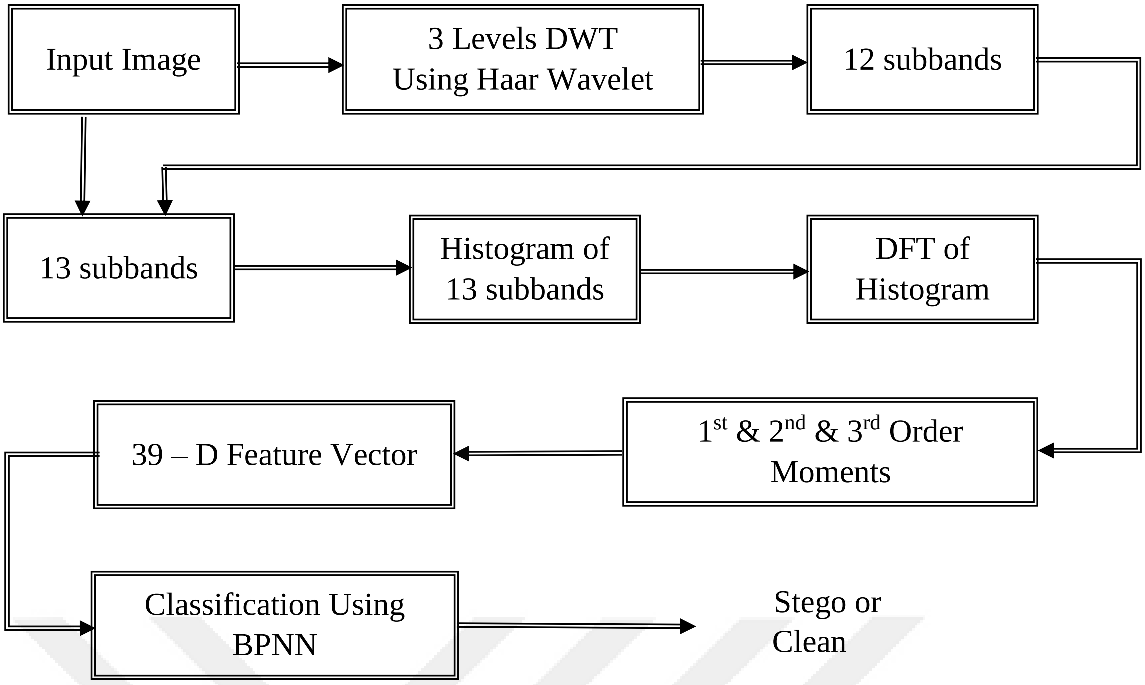


Figure 3.5. Structure of DFT

3.3.2. Structure of CODFT

In this system, it has the same steps as in the (DFT) system except that before the beginning inserting the image to the system. Must be taken the co-occurrence matrix for the image and then pass on the system.

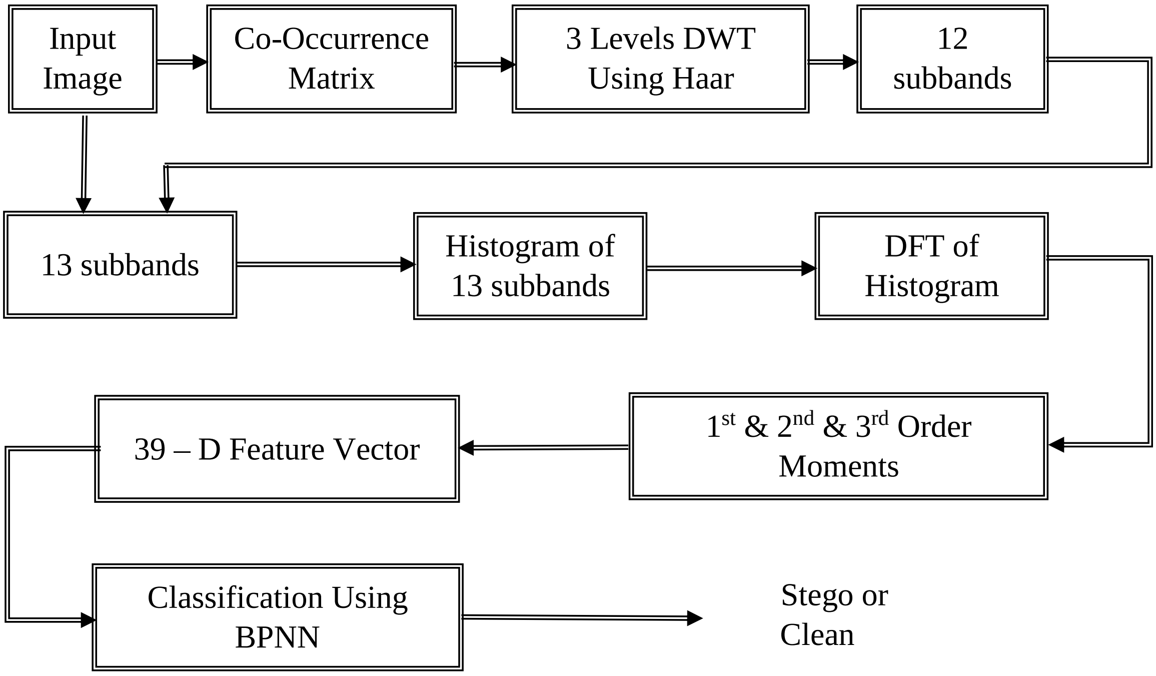


Figure 3.6. Structure of CODFT

3.3.3. Structure of DCT

In this system, it has the same steps as in the (DFT) system except that instead of the (DFT) it uses (DCT).

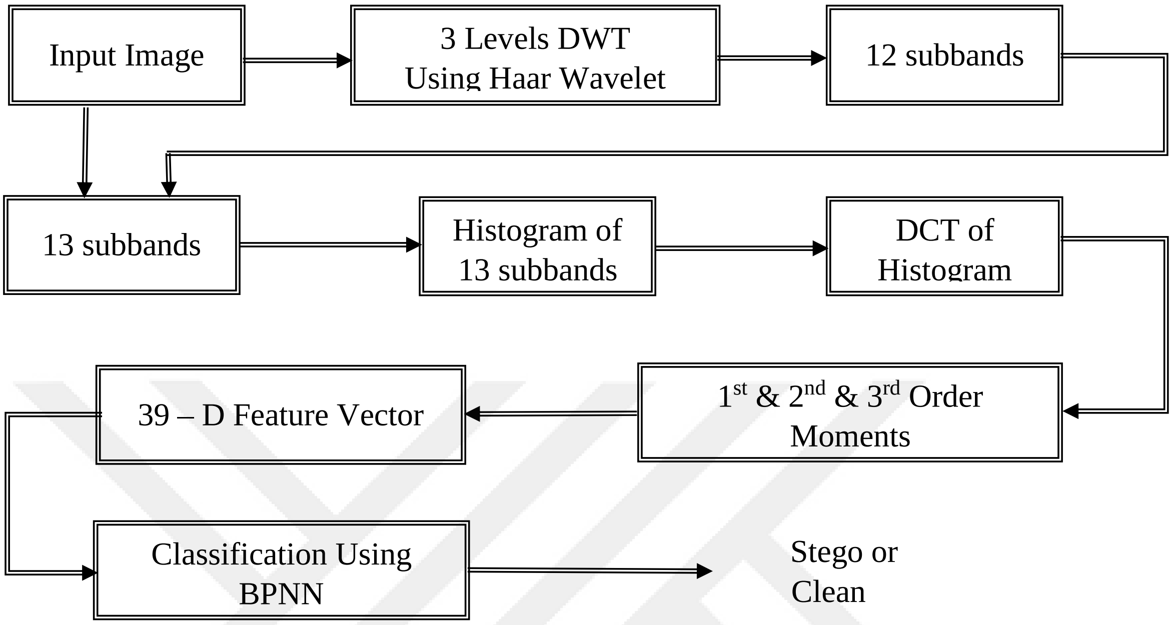


Figure 3.7. Structure of DCT

3.3.4. Structure of CODCT

In this system, it has the same steps as in the (DCT) system except that before the beginning inserting the image to the system. Must be taken the co-occurrence matrix for the image and then pass on the system.

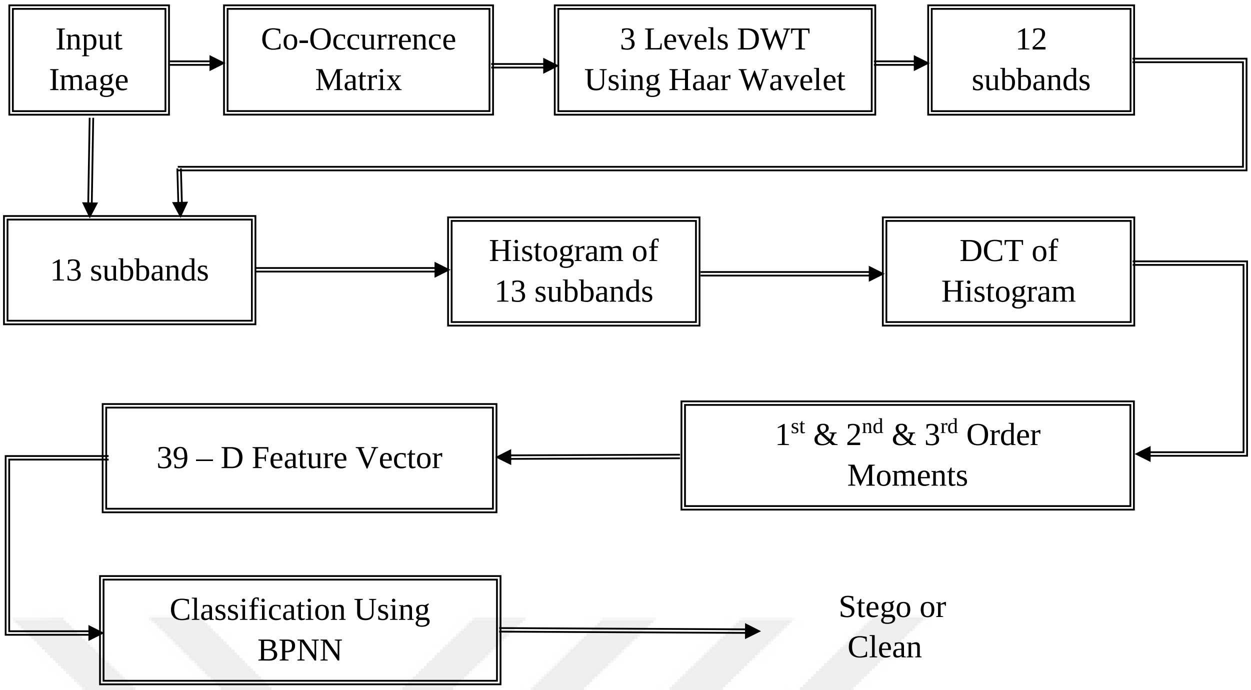


Figure 3.8. Structure of CODCT

3.4. Feature Extraction

The following sections discuss the concepts used to extract properties from images to determine whether they contain hidden data.

3.4.1. Data Set for Input Images

Where the use of different algorithms to hide certain information within the images, each algorithm has characteristics and features, disadvantages and the method of working varies from one method to another, in information-hiding algorithms, it is always intended not to show deformation in the built-in cover.

The distortions are not visible to the human eye. The best way to accomplish that by taking a wide variety of cover images that do not include hidden data to get the most natural patterns to distribute the colors of the image expected to be repeated in natural images. As well as a variety of embedded cover images that contain hidden data to obtain patterns of distortions by including hidden data, and then draw certain characteristics of these images to distinguish them using artificial neural networks, as the neural networks can distinguish patterns that appear to be intangible.

That's hard to do is the vast amount of images available on the Internet (the medium where such hidden messages exchanged). Since the number of image data is large, the diversity and nature of the images are very large, the diversity of natural color distribution patterns is also enormous. It is very difficult to determine the pattern of data distribution in images whether the distribution pattern is normal (that is, the image is clean and has not modified), or that the distribution pattern is similar to the data distribution in the embedded cover (i.e., the image contains hidden data).

The challenge is how to find a mechanism to extract certain characteristics that can distinguish natural patterns of data distribution from unnatural patterns. Methods of hiding information are many and varied, so it is difficult for the concealer analyzer to attack all the algorithms and methods of concealment common at the same time, the researcher in this area must determine the general specifications of the method of concealment that will attack.

From this point of view, it suggested in this part of the research that the system is trained and tested on a method of concealment of acceptable specifications that mimics the effect of most of the most common types of concealment. So suppose the following:

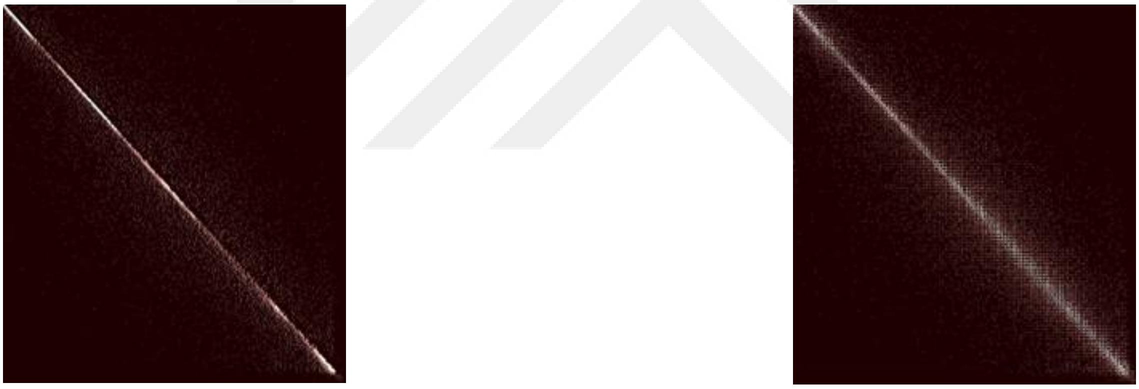
1- Non-pressed images were selected.
2- The selected images are varied in their content patterns and are statistically independent.
3- There is no prior information on the statistical characteristics of pixels of the images that can use in the detection process, such as a particular statistical histogram.
4- All cells are available for concealment, meaning that the transmitter not restricted by hiding in specific areas of the image.
5- The stenography algorithm used is the least significant bit (LSB).

In this thesis, the data set obtained from taking pictures of different patterns, actually, at first, they are clean images without hidden data or secret message, but by the used least significant bit algorithm, the secret message embedded in those images.

3.4.2 Co-Occurrence Matrix

Co-Occurrence Matrix (CM) Symmetry Matrix The image of the adjacent pixels examined. This process calculates the number of times a sequence of two specific color values occurs in the entire image space. It creates a 256x256 synchronous occurrence matrix. Each element in this matrix represents the number of times of two color values. The first value is equal to the row directory value for that element, the value of the column directory for the same item. For example, if CM (85, 83) = 62 means that the value of the item in row 85 and column 83 of the CM is 62, this means that the number of times the value 85 is received immediately before the value 83 is 62 times in full Image space. The result is a 256 x 256 matrix with each element representing the number of times the row directory is synchronized with the column directory for that element since the row directory is directly in front of the column directory.

It is important to note that in the case of clean images, the high values of Repetition concentrated in the main diameter of and around the co-occurrence matrix. Because the values of adjacent images cells are equal or very close to each other in most areas of the image. But hiding data inside the image dissipates this harmony, between the adjacent points in the image, and this is evident when comparing the co-occurrence matrix of the cover with the co-occurrence matrix of the same image without hidden data, as we see the breadth of the area where the high-frequency values centered around the main diameter of the matrix (Sebastian et al., 2012). Figure 3.9 shows the co-occurrence of a picture before and after data is hidden.



Before hidden

After hidden

Figure 3.9. Co-Occurrence Matrix before and after hidden (Hasson, and Khalifa, 2012).

3.4.3. Discrete Wavelet Transform (DWT) Using Haar Wavelet

Where discrete wavelet transforms working to analyze the signal of input with the different resolutions at the different frequencies through resolving the signal to approximation and allocate information. The discrete wavelet transform utilizes two sets of function scaling and wavelet. While the signal is decomposed into different frequencies, obtained during the sequential high pass and low pass filtering of the time domain signal.

Figure 3.1 shows a three-level wavelet analysis of the signal x[n] utilize the high pass filter g0[n] and low pass filter h0[n]. It is known as tree decomposition. At each level, the low pass filter produces s [n]. The high pass filter produces d[n].

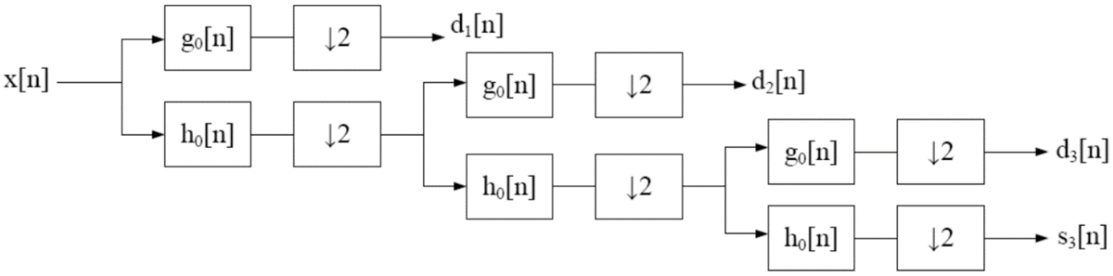


Figure 3.10. Three level wavelet decomposition tree (Balakrishnan, 2013).

The picture is analyzing to 4 subbands, one LL and other sub bands HL, LH and HH, The following level decomposition is continuous by the LL sub band. The procedure repeated for the required number of levels, Figure 3.2 and Figure 3.3 shows the three-level 2-D DWT analysis of an image (Balakrishnan, 2013).

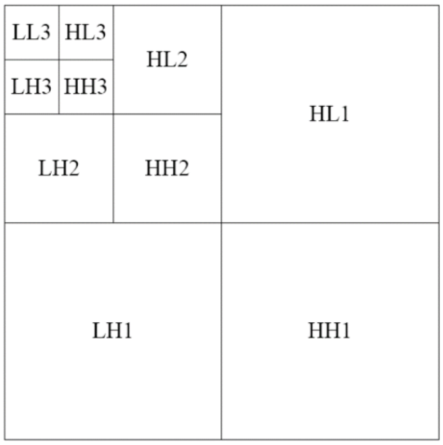


Figure 3.11. Three level 2-D DWT decomposition of an image (Balakrishnan, 2013).

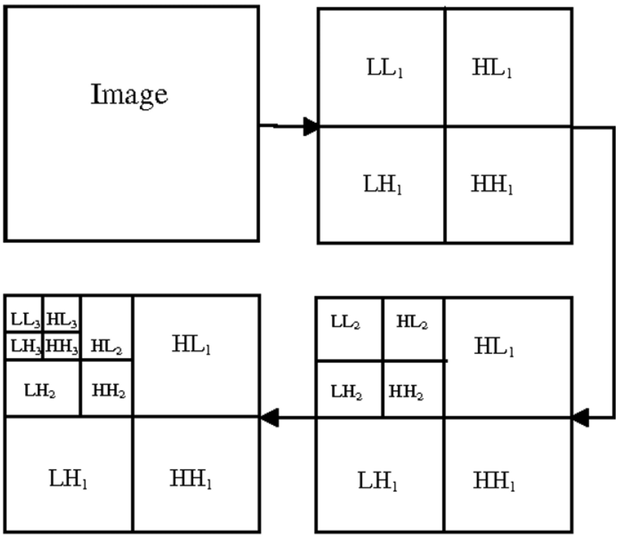


Figure 3.12. Three level 2-D DWT decomposition of an image (Balakrishnan, 2013).

Based on the above and since it consists of three levels. The image takes 12 subbands and with adding the original image to it has become 13 sub bands.

3.4.4. Histogram

The histogram is an image enhancement technique. It is a function to describe the distribution of light levels in the image. It usually used to make picture characteristics clearly for viewing and analysis. The main objective of optimization techniques is a specific image processing.

Where the result is more appropriate than the original images. For a specific application, optimization used as a preliminary processing phase in applications that rely on computer vision before being processed in subsequent stages. When the image has a histogram collected at the lower end (left side) to the extent of the levels, they are dark, when the histogram collected at the upper end (right side) to the extent of the levels, they are light or white. The histogram can be modified using the conversion function it works to extend the histogram, (Yang et al., 2016). As shown in Figure 3.13 and Figure 3.14

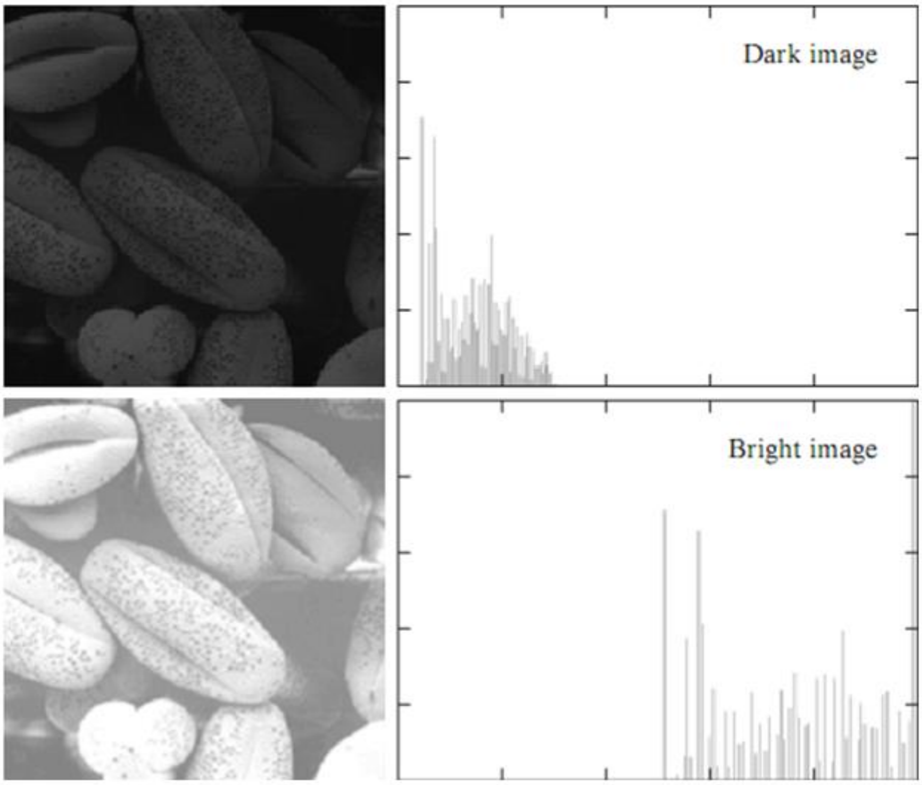


Figure 3.13. Histogram of dark and bright images (Yang et al., 2016).

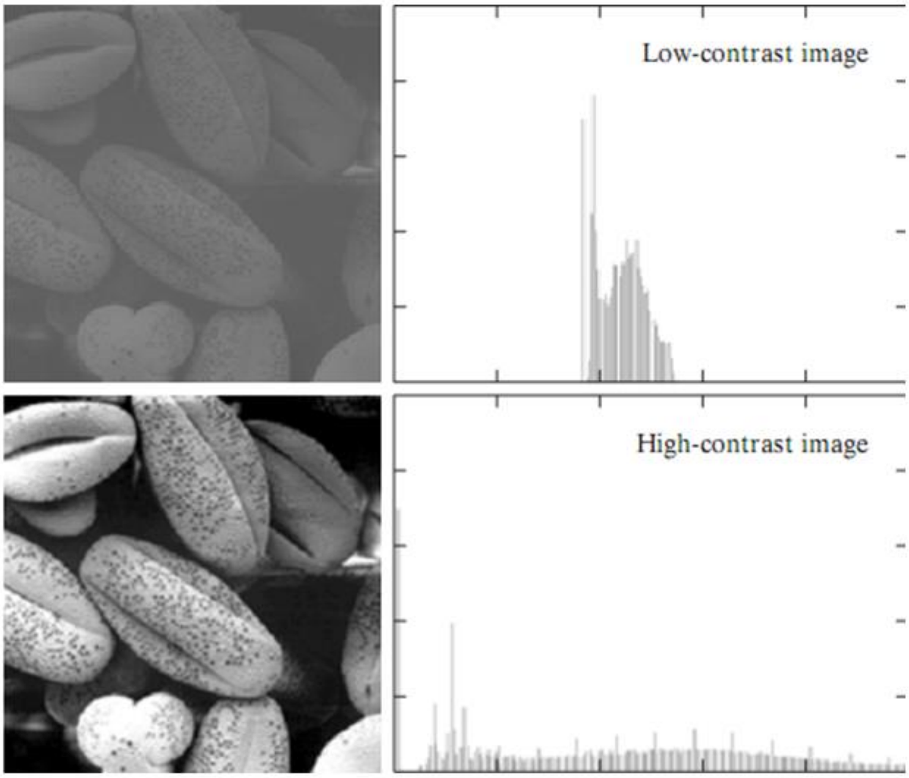


Figure 3.14. Histogram of low and high contrast images (Yang et al., 2016).

The histogram helps to detect hidden data using histogram change, where the focus on the feature extraction based on the histogram of the wavelet sub bands and the statistical moment for the properties wavelet (Hyun et al., 2010).

3.4.5. Discrete Fourier Transform

Is the process of converting the signal from the time domain to the frequency domain so that it carries the discrete signal of value and phase, Fourier analysis is the signal process to find their reality and be the difference between the (sin) and (cos) angle of 90 degrees and also the same angle between real and imaginary. In the frequency domain, the input must be a sine function it gives value and phase. Which returns the signal to the original is Fourier series and Fourier transform.

Where the origin of any signal is an exponential function and their derivatives (sin) and (cos). The target to the convert of the time domain to another domain is:
1-Extract information not existed in the time domain.

2-Find value and phase of the signal.

3-Get rid of the convolution.

When the signal is long the sampling process is all incorrect and to deal with it by taking part in it. Fourier Transform is an important tool in image processing. It is utilized to analyze the image in its (sin) and (cos) components. The result of the conversion represents the picture in the Fourier or frequency domain, while the image input is equal to the spatial domain.

In the Fourier domain image, represent every point a special frequency included in the spatial domain image. Fourier transform utilized in many usages, like image processing, image filtering, and image pressure.

For dealing with digital images only, it is enough to talk about a discrete Fourier transform. Is taking samples of the Fourier transform, not all frequencies that make up the image. Can be a set of samples which is big enough to describe the spatial domain image. The number of frequencies matches to the number of pixels in the particular domain image. The image in the Fourier and spatial domain are of the same size.

The discrete Fourier transform depends on a Fourier series utilized to represent the cyclic signal uninterruptible time. Fourier series is the basis of the Fourier transform it states that any periodic function can express as the sum of sine or cosine from various frequencies multiplied by various coefficients. Where a discrete Fourier transform analyzes the image into the sin and cos function. Utilize an inverse discrete Fourier transform. Any image can convert to the spatial domain for its return to normal (Bachrach and Shih, 2013).

3.4.6. First Three Order Moments

The moment is one of the first methods adopted to achieve the constant discrimination of two-dimensional model images. It also based on the method of algebra using a non-linear equation of the values that represent algebraic moments, a property required for stability when translating the image, modify the size (zooming) and rotation, translation, and scaling values are the best measure for identifying Arabic, English characters and digital images.

The seven moments considered the constant factors of any image as it does not change and is not affected when the rotation and translation and the scaling and this type of moment better suited different methods of discrimination because of their fixed properties (Xuan et al., 2005).

A set of fixed moments that have a desirable property is derived from being constant under rotation, translation, and scaling.

$$m_{pq} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x^{p} y^{q} f(x,y)\,dx\,dy \qquad (3.1)$$

Where (x, y) represents coordinates the unit of the image respectively.

Moments m_{pq} projection of image f(x,y)to the basis $x^{p}y^{q}$.

f(x,y): piecewise continuous function with nonzero values in a portion of the plane=image.

$$\mu_{pq} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} (x-\bar{x})^{p} (y-\bar{y})^{q} f(x,y)\,dx\,dy \qquad (3.2)$$

$$\bar{x} = \frac{m_{10}}{m_{00}}, \bar{y} = \frac{m_{01}}{m_{00}} \qquad (3.3)$$

$$\mu_{pq} = \sum_{x}\sum_{y} (x-\bar{x})^{p} (y-\bar{y})^{q} f(x,y) \qquad (3.4)$$

$$\eta_{pq} = \frac{m_{10}}{m_{00}^{\gamma}} \qquad (3.5)$$

$$\gamma = \frac{1}{2}(p+q)+1 \qquad (3.6)$$

Seven invariant moments can be derived from the second and third moments and giving the following:

$$\Phi_1 = \eta_{20} + \eta_{02} \tag{3.7}$$

$$\Phi_2 = (\eta_{20} + \eta_{02})^2 + 4\,\eta_{11}{}^2 \tag{3.8}$$

$$\Phi_3 = (\eta_{30} + 3\eta_{12})^2 + (\,3\eta_{21} - \eta_{03})^2 \tag{3.9}$$

$$\Phi_4 = (\eta_{30} + \eta_{12})^2 + (\,\eta_{21} - \eta_{03})^2 \tag{3.10}$$

$$\Phi_5 = (\eta_{30} - 3\eta_{12})(\eta_{30} + \eta_{12})[(\eta_{30} + 3\eta_{12})^2 - 3(\,\eta_{21} + \eta_{03})^2],\ +(3\eta_{21} + \eta_{03})(\eta_{21} + \eta_{03})[3(\eta_{30} + \eta_{12})^2 - (\,\eta_{21} + \eta_{03})^2] \tag{3.11}$$

$$\Phi_6 = (\eta_{20} - \eta_{02})[(\eta_{30} + \eta_{12})^2 - (\,\eta_{21} + \eta_{03})^2], +4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03}), \tag{3.12}$$

$$\Phi_7 = (3\eta_{21} - \eta_{03})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\,\eta_{21} + \eta_{03})^2],\ +(3\eta_{12} + \eta_{30})(\eta_{21} + \eta_{03})[3(\eta_{30} + \eta_{12})^2 - (\,\eta_{21} + \eta_{03})^2] \tag{3.13}$$

Where these seven moments don't change with rotation, translation, and scaling. In this thesis only used the first three moments.

3.5. Classification Using BPNN

The backpropagation neural network (BPNN) system used in the proposed system. For decision-making to a classification of the image to clean or Stego by feeding the 39 properties previously extracted as mentioned in the previous sections. The cell target is one element with two values zero means (clean) or one means (Stego) the (BPNN) used in this work is illustrated in Figure 3.15.

The input layer consists of 39 neurons that receive the extracted properties, while two hidden layers, the first containing 60 neurons, the second containing 30 neurons, and the transfer function used in them are Logsig. These values determined for the number of neurons and the transfer function based on the principle of experiment and error. The output layer consisted of a single neuron and used the function pureline as a transfer function. As the goals either zero means clean or one and mean stego.

The network is trained using the number of training pairs (input and target) and then testing the network using test pairs. After completing the training process, weights and parameters of the trained network stored in a file for later use to estimate the extent to which images contain hidden data.

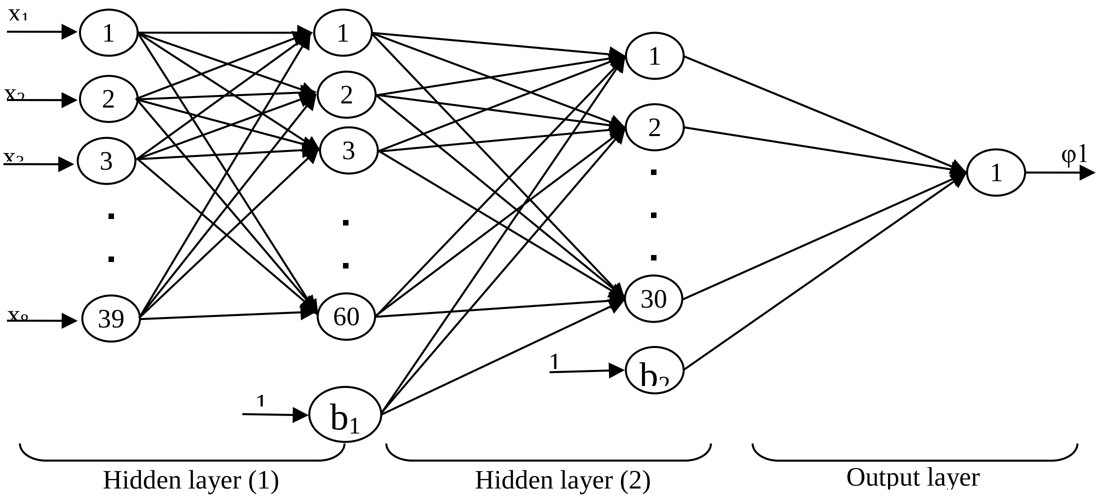


Figure 3.15. The (BPNN) architecture used in the proposed system

4. FINDINGS AND DISCUSSION

This chapter discusses how the proposed system implemented and what results produced after the execution of the system.

4.1 Introduction

It sets of functions which built in the Matlab v. 8.5.0.197613 (R2015a). For the application of work, as known, this language supports image processing and also supports artificial intelligence techniques and artificial neural networks in particular. This chapter reviews the results obtained from the application of the hidden data detection system and discusses these results and compares them with the results of previous work in the same field.

4.2 Implementation

It takes a bunch of gray images, not compressed, the content of these images varied. The images were collected randomly and were not categorized, sorted or modified. The collection contained 110 cover images (no hidden data). 110 images of an embedded cover (containing hidden data), data hidden at varying rates (1bpp, 0.1bpp, 0.2bpp, and 0.5bpp), a separate network is trained for each percentage of hiding, as well as for each of the methods mentioned in Sections 4.4.1 to 4.4.4.

This group of images random assigned to a training group of 70% of the group of images and a 30% test group of the remaining images. The total number of images for the training set for each image covered and the embedded cover is 77 for the cover images and 77 for the embedded cover images. The number of images for the test set for each of the images covers, and embedded cover images, 33 cover images, and 33 embedded cover images. Figure 4.1 shows some gray image models used in the proposed system training and testing.

Figure 4.1. Some images used to train and test to proposed system.

4.3 Obtained Results

After training the hidden detection system using the training data from the database illustrated in Section 4.2, the system tested using the test data (which included 33 cover images and the same embedded cover images) from the same database. The test results based on the method used, as the following sections.

4.3.1. Results of DFT

After training the neural network by using the dataset illustrated previously by different data hiding percentages (0.1 bpp, 0.2 bpp, 0.5 bpp, and 1bpp) for the system that used (DFT) that illustrated in Section 3.4.1 and the result as the following Table 4.1.

a) Results of DFT 0.1 bpp

b) Results of DFT 0.2 bpp

c) Results of DFT 0.5 bpp

d) Results of DFT 1 bpp

Table 4.1. Results of the DFT method.

Hiding Ratio	TP	TN	FP	FN	Detection Rate
0.1bpp	27	20	6	13	71.2121%
0.2bpp	22	19	11	14	62.1212%
0.5bpp	30	21	3	12	77.2727%
1bpp	31	23	2	10	81.8182%

4.3.2. Results of CODFT

After training the neural network by using the dataset illustrated previously by different percentages (0.1 bpp,0.2 bpp,0.5 bpp,1bpp) for the system that used (CODFT) that illustrated in Section 3.4.2 and the result as the following Table 4.2.

a) Results of CODFT 0.1 bpp

b) Results of CODFT 0.2 bpp

c) Results of CODFT 0.5 bpp

d) Results of CODFT 1 bpp

Table 4.2. Results of CODFT method

Hiding Ratio	TP	TN	FP	FN	Detection Rate
0.1bpp	21	29	12	4	75.7576%
0.2bpp	29	24	4	9	80.3030%
0.5bpp	27	27	6	6	81.8182%
1bpp	30	20	3	13	75.7576%

4.3.3. Results of DCT

After training the neural network by using the dataset illustrated previously by different percentages (0.1 bpp,0.2 bpp,0.5 bpp,1bpp) for the system that used (DCT) that illustrated in Section 3.4.3 and the result as the following Table 4.3.

a) Results of DCT 0.1 bpp

b) Results of DCT 0.2 bpp

c) Results of DCT 0.5 bpp

d) Results of DCT 1 bpp

Table 4.3. Results of the DCT method

Hiding Ratio	TP	TN	FP	FN	Detection Rate
0.1bpp	15	29	18	4	66.6667%
0.2bpp	17	30	16	3	71.2121%
0.5bpp	28	12	5	21	60.6061%
1bpp	15	29	18	4	66.6667%

4.3.4. Results of CODCT

After training the neural network by using the dataset illustrated previously by different percentages (0.1 bpp,0.2 bpp,0.5 bpp,1bpp) for the system that used (CODCT) that illustrated in section (3.4.4) and the result as the following table 4.4.

a) Results of CODCT 0.1 bpp

b) Results of CODCT 0.2 bpp

c) Results of CODCT 0.5 bpp

d) Results of CODCT 1 bpp

Table 4.4. Results of CODCT method

Hiding Ratio	TP	TN	FP	FN	Detection Rate
0.1bpp	28	20	5	13	72.7273%
0.2bpp	30	21	3	12	77.2727%
0.5bpp	24	29	9	4	80.3030%
1bpp	16	30	17	3	69.6970%

4.4 Discussion of the Obtained Results

The following few sections discuss the experimental result of the proposed system. Figure 4.2 shows a bar chart that illustrates the results of the proposed system grouped by embedding ratio, and Figure 4.3 views the results of the proposed system grouped by steganalysis method.

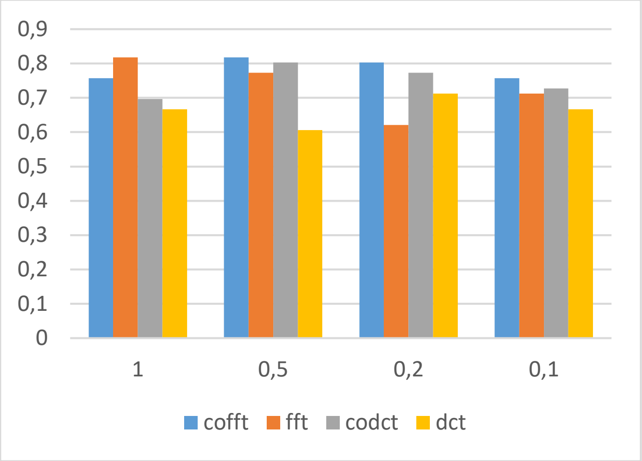


Figure 4.2. Results of proposed system grouped by embedding ratio.

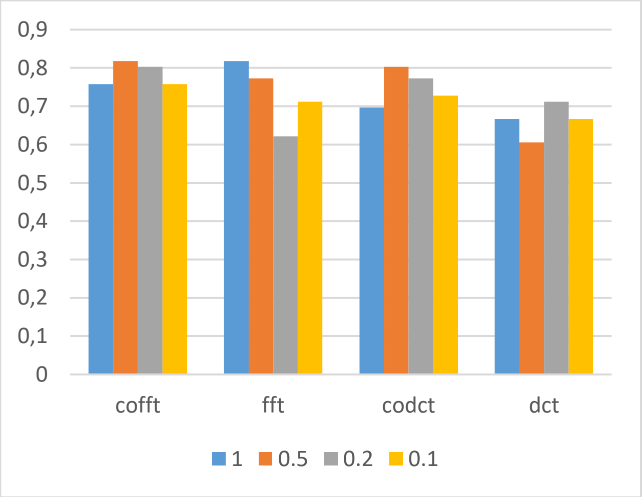


Figure 4.3. Results of proposed system grouped by steganalysis method.

4.4.1. Discussion of DFT Results

Based on the Equation 4.1. as shown in the Table 4.1. for the ratio hidden (0.1 bpp) the detection rate is (71.2121%) and has obtained by the equation shown in the following, and so there is no big difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, they are a medium ratio to the rest of the cases.

$$Detection\ Rate = \frac{TP + TN}{TP + TN + FP + FN} \times 100\ \% \tag{4.1}$$

For the ratio hidden (0.2 bpp) the detection rate is (62.1212%), and so there is no big difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, they are the lowest ratio of rest the cases.

For the ratio hidden (0.5 bpp) the detection rate is (77.2727%), and so there is no big difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, they are better from the first two cases.

For the ratio hidden (1 bpp) the detection rate is (81.8182%), and so there is no big difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, they are best from all other cases, and here it shows that the best performance is when the hidden ratio is 1bpp.

4.4.2. Discussion of CODFT Results

As shown in the table 4.2 at the ratio hidden (0.1 bpp) the detection rate is (75.7576%), and so there is no big difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, it became better due to the co-occurrence matrix add to the system.

For the ratio hidden (0.2 bpp) the detection rate is (80.3030%), and so there is no big difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, large differences occur with the co-occurrence matrix add to the system in this case and consider that enhance for this case.

For the ratio hidden (0.5 bpp) the detection rate is (81.8182%), and so there is no difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, better from all cases with the co-occurrence matrix add to the system in this case and that is the best performance.

For the ratio hidden (1 bpp) the detection rate is (75.7576%), and so there is no big difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, In this case, the ratio decreased with the co-occurrence matrix add to the system in this case.

4.4.3. Discussion of DCT Results

As shown in the Table 4.3 at the ratio hidden (0.1 bpp) the detection rate is (66.6667%), and so there is a big difference between the true positive (TP) and true negative (TN), and that's a no good thing. As for the detection ratio, it less than the other first two cases in this system.

For the ratio hidden (0.2 bpp) the detection rate is (71.2121%), and so there is a big difference between the true positive (TP) and true negative (TN), and that's a no good thing. As for the detection ratio, it less than the previous case in this system.

For the ratio hidden (0.5 bpp) the detection rate is (60.6061%), and so there is a big difference between the true positive (TP) and true negative (TN), and that's a no good thing. As for the detection ratio, it less than all the previous case in this system.

For the ratio hidden (1 bpp) the detection rate is (66.6667%), and so there is a big difference between the true positive (TP) and true negative (TN), and that's a no good thing. As for the detection ratio, it less than all the previous case in this system.

4.4.4. Discussion of CODCT Results

As shown in the Table 4.4 for the ratio hidden (0.1 bpp) the detection rate is (72.7273%), and so there is no big difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, it became better due to the co-occurrence matrix add to the system.

For the ratio hidden (0.2 bpp) the detection rate is (77.2727%), and so there is no big difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, it became better due to the co-occurrence matrix add to the system.

For the ratio hidden (0.5 bpp) the detection rate is (80.3030%), and so there is no big difference between the true positive (TP) and true negative (TN), and that's a good thing. As for the detection ratio, it became better due to the co-occurrence matrix add to the system.

For the ratio hidden (1 bpp) the detection rate is (69.6970%), and so there is a big difference between the true positive (TP) and true negative (TN), and that's no good thing. As for the detection ratio, it became better due to the co-occurrence matrix add to the system. In general, all the obtained results have been better when the co-occurrence matrix added to the system.

4.5 **Comparison with Previous Works**

The results has been compared with these three papers

1-(Shi et al., 2005).

2-(Xuan et al., 2005).

3-(Shi et al., 2005).

Table 4.5.. Accuracy comparison with previous works

Steganalysis Method	**Embedding Rate = 1 bpp**	**Embedding Rate = 0.5 bpp**	**Embedding Rate = 0.2 bpp**
18-D DWT features [1]	61.67 %	60 %	60 %
39-D DWT features [2]	60 %	60 %	63.33 %
78-D DWT features [3]	46.67 %	53.33 %	51.67 %
Proposed CoDFT	75.76 %	81.82 %	80.3 %
Proposed DFT	81.82 %	77.27 %	62.12 %
Proposed CoDCT	69.7 %	80.3 %	77.27 %
Proposed DCT	66.67 %	60.61 %	71.21 %

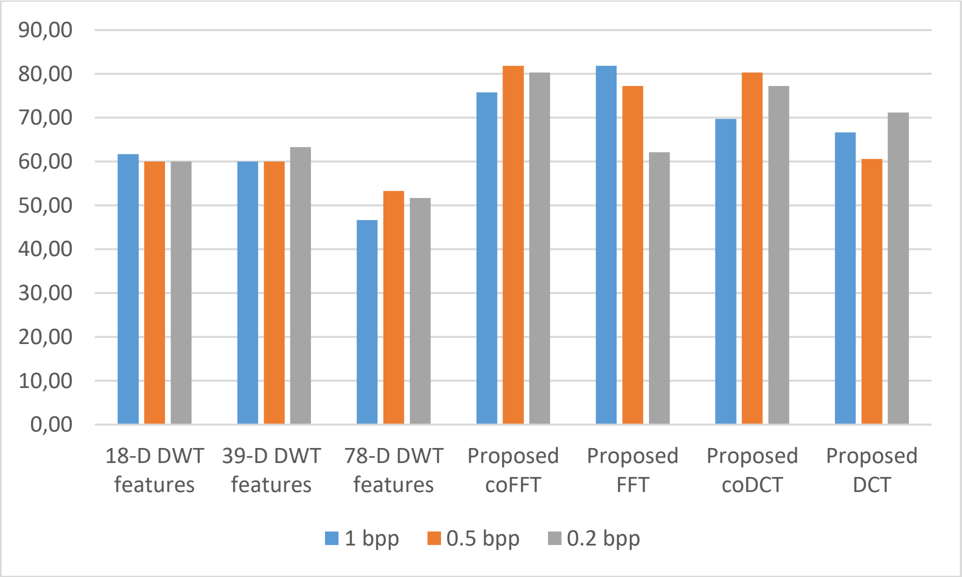


Figure 4.4. Accuracy comparison with previous steganalysis method.

5. CONCLUSIONS AND SUGGESTIONS

In the following two sections illustrate the conclusion of this work is and the suggestion made for future work.

5.1 Conclusions

The regularity of the relationship between adjacent image cells in most picture areas provides the appropriate ground for constructing a detection system based on the nature of this relationship to determine whether the image is a cover or Stego-cover. Depending on the relationship between the adjacent image points, using the co-occurrence matrix, enabled the steganalysis to detect the hidden.

The diversity of large data within the supplied database occur Conflicts and inconsistencies, the existence of these conflicting and abnormal data confuse the work of the detection system and make the arrival of the situation of stability difficult.

The relationship between system performance and the hidden ratio is an inverse relationship in CoDFT, CoDCT, and DCT. The lower the percentage of hidden message, be more efficient the system.

The relationship between system performance and the hidden ratio is a positive relationship in DFT, as the greater the percentage of hidden message, be more efficient the system.

5.2 Suggestions for Future Works

Procedure an image texture-based automatic classification .to distinguish images in different combinations. To increase system efficiency when used on sets of images with similar data structures.

Try to find some characteristics of image texture that affect the way the distribution of image cells and adopt it the input to the neural network as well as the cells adjacent to the image of the cell to estimate their original value.

It is recommended to use DFT to detect hidden information in high density in images. The rest of the methods tested in this work is recommended to detect hidden information with less intensity in images. It is efficient.

6. REFERENCES

Al Bouna, B., Couchot, J. F., Couturier, R., Fadil, Y. A., Guyeux, C. 2015. Performance Study of Steganalysis Techniques. *International Conference on Applied Research in Computer Science and Engineering*, 1-7.

Aljarf, A., Amin, S., Filippas, J., Huttelworth, J. 2013. Develop a Detection System for Grey and ColourStego Images. *International Journal of Modeling and Optimization, 3*(5), 458-461.

Ambalavanan, A. and Chandramouli, R. 2005. A bayesian image steganalysis approach to estimate the embedded secret message. *Proceedings of the 7th workshop on Multimedia and security - MM and Sec '05*, 33-38.

Ayodele, T. O. 2010. Introduction to machine learning. *In New Advances in Machine Learning. IntechOpen*, 1-366.

Badr, S. M., Ismaial, G., Khalil, A. H. 2014. A Review on Steganalysis Techniques: From Image Format Point of View. *International Journal of Computer Applications, 102*(4), 11-19.

Balakrishnan, P. 2013. Design and Implementation of Lifting Based Daubechies Wavelet Transforms Using Algebraic Integers. *Doctoral dissertation, University of Saskatchewan*, 1-79.

Berg, G., Davidson, I., Duan, M. Y., Paul, G. 2003. Searching for Hidden Messages: Automatic Detection of Steganography. *IAAI 2003*, 51-56.

Bhasin, V. and Bedi, P. 2013. Steganalysis for JPEG images using extreme learning Machine. *In 2013 IEEE International Conference on Systems, Man, and Cybernetics* (pp. 1361-1366). IEEE.

Chandrababu, A. 2009. Using an Ariticial Neural Network to Detect the Presence of Image Steganography. *Doctoral dissertation, University of Akron, 1*(6), 1-65

Cheddad, A., Condell, J., Curran, K. Mc Kevitt, P. 2010. Digital image steganography: Survey and analysis of current methods. *Signal processing, 90*(3), 727-752.

Collins, W. and Tissot, P. 2007. Use Of An Artificial Neural Network To Forecast Thunderstorm Location. *NOAA/National Weather Service*, 1-9.

Collins, W. G. and Tissot, P. 2016. Thunderstorm Predictions Using Artificial Neural Networks. *In Artificial Neural Networks-Models and Applications*, 252-287.

Davidson, J., Bergman, C., Bartlett, E. 2005. An artificial neural network for wavelet steganalysis. *International Society for Optics and Photonics, 5916*(515), 1-10.

Desai, M. B. and Patel, S. V. 2016. Performance analysis of image steganalysis against message size, message type and classification methods. *International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT),* 295-302.

Di Ruberto, C., Fodde, G., Putzu, L. 2015. On different colour spaces for medical colour image classification. *International Conference on Computer Analysis of Images and Patterns*, 477-488.

Domingues, M. O., Mendes Jr, O., Da Costa, A. M. 2005. On wavelet techniques in atmospheric sciences. *Advances in Space Research, 35*(5), 831-842.

Eichkitz, C. G., Davies, J., Amtmann, J., Schreilechner, M. G., de Groot, P. 2015. Grey level co-occurrence matrix and its application to seismic data. *First break, 33*(3), 71-77.

Geetha, S. and Kamaraj, N. 2010. Optimized image steganalysis through feature selection using MBEGA. *International Journal of Computer Networks & Communications (IJCNC), 2*(4), 161-175.

Geetha, S. and Kamaraj, N. 2010. Optimized image steganalysis through feature selection using MBEGA. I*nternational Journal of Computer Networks & Communications (IJCNC), 2*(4), 161-175.

Gong, R. and Wang, H. 2012. Steganalysis for GIF images based on colors-gradient co-occurrence matrix. *Optics Communications, 285*(24), 4961-4965.

Gope, P., Kumar, A., Luthra, G. 2010. An enhanced JPEG steganography scheme with encryption technique. *nternational Journal of Computer and Electrical Engineerin, 2*(5), 924-930.

Green, J., Levstein, I., Boggs, C. R. J., Fenger, T. 2015. Steganography Analysis: Efficacy and Response-Time of Current Steganalysis Software. *J Comput Sci*, 28.

Hariri, M., Karimi, R., Nosrati, M. 2011. An introduction to steganography methods. *World Applied Programming, 1*(3), 191-195.

Hasson, S. O. and Khalifa, F. M. 2012. Steganalysis Using KL Transform and Radial Basis Neural Network. *AL-Rafidain Journal of Computer Sciences and Mathematics,, 9*(1), 47-58.

Hyun, S. H., Park, T. H., Jeong, B. G., Kim, Y. S., Eom, I. K. 2010. Feature Extraction for Steganalysis using Histogram Change of Wavelet Subbands. *The 25th International Technical Conference on Circuits/Systems, Computers and Communications*(2), 4-7.

Heaton, J., 2008. *Introduction to Neural Networks for Java* (Vol. 99). St. Louis: Heaton Research, Inc.

Johnson, N. F and Jajodia, S. 1998. Steganalysis of images created using current steganography software. *International Workshop on Information Hiding*, 273-289.

Kang, L.C. 2011. steganalysis of binary images. *Department of Computing Faculty of Science, Macquarie University Australia*, 1-160.

Kaur, M. and Kaur, G. 2014. Review of various steganalysis techniques. *International Journal of Computer Science and Information Technologies, 5*(2), 1744-1747.

Kobsi, N. and Merouani, H. F. 2007. Neural network based image steganalysis: a comparative study. In Neural Networks for Signal Processing. *Proceedings of the 1994 IEEE Workshop*, 423-430.

Lafferty, P. and Ahmed, F. 2004. Texture-based steganalysis: results for color images. *International Society for Optics and Photonics, 5561*, 145-152.

Li, B., He, J., Huang, J., Shi, Y. Q. 2011. A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing, 2,* 142-172.

Luo, X. Y., Wang, D. S., Wang, P. Liu, F. L. 2008. A review on blind detection for image steganography. *Signal processing, 88*(9), 2138-2157.

Bachrach, M., and Frank, Y. Shih. 2011. Image steganography and steganalysis. *Wiley Interdisciplinary Reviews: Computational Statistics*, *3*(3), 251-259.

Miche, Y. 2010. Developing fast machine learning techniques with applications to steganalysis problems. *Aalto University School of Science and Technology*, 1-134.

Ng, G. W. 2003. Intelligent systems–fusion, tracking and control. England: DSO *National Laboratories and National University of Singapore*.

Nissar, A. and Mir, A. H. 2010. Classification of steganalysis techniques: A study. *Digital Signal Processing: A Review Journal, 20*(6), 1758-1770.

Odeh, A. and Elleithy, K. 2012. Steganography in arabic text using zero width and kashidha letters. *International Journal of Computer Science & Information Technology (IJCSIT), 4*(3), 1-11.

Pevný, T. 2008. Kernel methods in steganalysis. *State University of New York at Binghamton,Thomas J. Watson School of Engineering and Applied Science, Department of Computer Science.*, 1-128.

Priddy, K. L. and Keller, P. E. 2005. Artificial neural networks: an introduction. *SPIE press, 68,* 1-180.

Rasool, Z. I. 2017. The Detection of Data Hiding in RGB Images Using Statistical Steganalysis. *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), 4*(8), 1-94.

Reddy, P. and Kumar, S. 2007. Steganalysis techniques: A comparative study. *University of New Orleans Theses and Dissertations*, 1-50.

Richer, P. 2003. Steganalysis: Detecting hidden information with computer forensic analysis. *SANS Institute InfoSec Reading Room*, 1-12.

Sebastian, V., Unnikrishnan, A., Balakrishnan, K. 2012. Gray level co-occurrence matrices: generalisation and some new features. *nternational Journal of Computer Science, Engineering and Information Technology (IJCSEIT), 2*(2), 151-157.

Shaohui, L., Hongxun, Y., Wen, G. 2003. Neural network based steganalysis in still images. *International Conference on Multimedia and Expo. ICME'03, 2,* II-509.

Suryawanshi, G. R. and NMali, S. 2016. Universal steganalysis using IQM and multiclass discriminator for digital images. *Signal Processing, Communication, Power and Embedded System (SCOPES)*, 877-881.

Thiyagarajan, P., Aghila, G., Venkatesan, V. P. 2011. Steganalysis using color model conversion. *An International Journal (SIPIJ), 2*(4), 201-211.

Trivedi, S. and Chandramouli, R. 2003. Active steganalysis of sequential steganography. *International Society for Optics and Photonics, 5020*, 123-131.

Trivedi, S. and Chandramouli, R. 2005. Secret key estimation in sequential steganography. *IEEE Transactions on Signal Processing, 53*(2), 746-757.

Xie, C., Cheng, Y and Chen, Y. 2011. An active steganalysis approach for echo hiding based on Sliding Windowed Cepstrum. *Signal Processing, 91*(4), 877-889.

Xuan, G., Shi, Y. Q., Gao, J., Zou, D., Yang, C., Zhang, Z., Chen, W. 2005. Steganalysis Based on Multiple Features Formed by Statistical Moments of Wavelet Characteristic Functions. *International Workshop on Information Hiding*, 262 - 277.

Yadav, P., Mishra, N., Sharma, S. 2013. A secure video steganography with encryption based on LSB technique. *In 2013 IEEE International Conference on Computational Intelligence and Computing Research*, 1-5.

Yan, R., Gao, R. X., Chen, X. 2014. Wavelets for fault diagnosis of rotary machines: A review with applications. *Signal processing, 96*, 1-15.

Yang, J., Zhong, W., Miao, Z. 2016. On the Image enhancement histogram processing, I*n 2016 3rd international conference on informative and cybernetics for computational social systems*, 252-255.

Zeng, J., Tan, S., Li, B., Huang, J. 2017. Large-scale JPEG image steganalysis using hybrid deep-learning framework. *IEEE Transactions on Information Forensics and Security, 13*(5), 1200-1214.

Zhang, Z., Bian, Y., Ping, X. 2008. Image blind forensics using artificial neural network, *In 2008 International Conference on Computer Science and Software Engineering*, 4, 847-850.

CURRICULUM VITAE

PERSONAL INFORMATION

Name and surname	: Isamadeen Abdolmughith Khalifa Khalif
Nationality	: Iraq
Birthplace and Date	:1 January 1975
Telephone	: 05382573409- 009647504843801
Email	: isamadeen.khalifa@dpu.edu.krd , isamadeen4@gmail.com

EDUCATION

At 8.2.2016 I started to study in Turkey M.Sc. in computer engineering in department of electrical and electronic engineering at Siirt University.

DEGREE	**INSTITUTE**	**YEAR GRADUATION**
High school	Mosul high school	1995
Diploma	Mosul Technical Institute	1998
B. Eng.	Technical Engineering College of Mosul	2003
M.Sc.	Siirt University	2019

RESEARCH INTERESTS

M.Sc. Still image Steganography Detection Based on Machine learning.

FOREIGN LANGUAGE

Kurdish, Arabic and English.