Video Data Steganography
Based on Discrete Cosine Transform Method

A THESIS SUBMITTED TO THE
COLLEGE OF SCIENCE, UNIVERSITY OF BAGHDAD IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER SCIENCE IN
Physics (Remote Sensing)

BY

Mohammed Abd Al-Hassan Hussein
B. Sc. (Physics Science), 2010

Supervised by

Prof. Dr. Alaa S. Mahdi
Ass. Prof. Dr. Ali Hassan Khidhir

2014 1435
بسم الله الرحمن الرحيم

الَّذِي جَعَلَ لَكُمُ الْأَرْضَ فَرَاشًا وَالسَّمَاءَ بِنَاءً وَأَنزَلَ مِنَ السَّمَاءِ مَاءً فَأَخَرَجَ بِهِ مِنَ الثَّمَرَاتِ رِزقًا لَكُمْ فَلا تَجَاعَلُوا لِلَّهِ أَنْدَادًا وَأَنْتُمْ تَعَلَّمُونَ

صدق الله العظيم

الآية (22) سورة البقرة
Dedication

TO / My Family & / My Friends

with all my love and respect

Mohammed
2014
"Video data steganography based discrete cosine transform method"

The preparation of this thesis was made under our supervision at the College of Science, University of Baghdad in partial fulfillment of the requirements for the Degree of Master Science in Physics.

Signature: 
Signature:

Title: Professor 
Title: Ass. Professor

Name: Dr. **Alaa S. Mahdi Khidhir**
Name: Dr. **Ali Hassan**

Supervisor
Supervisor

Date: / / 2014
Date: / / 2014

Approved by the Head of Department of Physics

Signature:

Title: Professor

Name: Dr. **Raad M.S. Al Haddad**

Head of the Department of Physics

Date: / / 2014
Acknowledgment

At the beginning thanks to great Allah who gave me the reality and strength to accomplish this work.

I would like to extend my thankful, respection and appreciation to my supervisor Dr. Alaa S. Mahdi who have given me their advice and their important guidance and appreciable opinions which all made my study easy through this work.

My great thanks directed to Dr. Ali Hassan for his assistance, my thanks directed to all people that help me to complete my work Also I would like to express my thanks to the head of Physics Department of Baghdad University Dr. Raad M.S. Al Haddad.

Very much thanks to my Friends for their love and encouragement.

Finally, My deep thanks directed to my family, Father and Mother, Sisters and Brothers, for their love and great supports in all work steps.

Mohammed
2014
Abstract

The secure data transmission over internet is achieved using steganography. It is the art and science of concealing information in unremarkable cover media so as not to arouse an observer's suspicion.

In this research the proposed system is designed to hide video (image, audio) by using discrete cosine transform (DCT) method and discrete wavelet transform (DWT) method and Also, the Principal Components Analysis (PCA) and (DWT) methods were used to hide the data. After cutting up the video to frames by using Ulead video studio 9 program.

This program have been cutting up video to 20 frame in one second. The system will embed the (input) secret data (image color ,audio) inside a cover frame, the secret data apply it discrete cosine transformation (DCT) method and the cover frame is decomposing into four parts Horizontally and vertically low pass( LL), Horizontally low pass and vertically high pass(LH), Horizontally high pass and vertically low pass (HL),and Horizontally and vertically high pass (HH ) by using discrete wavelet transformation (DWT) method and the secret data hidden in the part (HH) in segment Least Significant Bit (LSB) of cover image. and produce (output) stego-image.

The stego key uses for extraction the data hidden (secret data) from stego cover through use the process embedding inverse.

Apply the equation of each Peak Signal to Noise Ratio (PSNR), Mean square error (MSE) and Bit Error Ratio (BER) on image used as a cover before and after the data hiding so that evaluated quality of the image and the quality of effect. Our proposed system are implement using by MATLAB ver. 7.6 program.
# List of Contents

<table>
<thead>
<tr>
<th>Subjects</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgement</td>
<td>i</td>
</tr>
<tr>
<td>Abstract</td>
<td>ii</td>
</tr>
<tr>
<td>List of contents</td>
<td>iii</td>
</tr>
<tr>
<td>List of Figures</td>
<td>vi</td>
</tr>
<tr>
<td>List of Tables</td>
<td>viii</td>
</tr>
<tr>
<td>List of Abbreviation</td>
<td>ix</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter One</th>
<th>General Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.2 History of Steganography</td>
<td>2</td>
</tr>
<tr>
<td>1.3 General of Steganography</td>
<td>4</td>
</tr>
<tr>
<td>1.4 Goal of the Steganography</td>
<td>6</td>
</tr>
<tr>
<td>1.5 Uses of Steganography</td>
<td>7</td>
</tr>
<tr>
<td>1.6 Steganography vs. Digital Watermarking</td>
<td>8</td>
</tr>
<tr>
<td>1.7 Difference between Steganography and Cryptography</td>
<td>10</td>
</tr>
<tr>
<td>1.8 Literature Review</td>
<td>11</td>
</tr>
<tr>
<td>1.9 The Aim of Thesis</td>
<td>14</td>
</tr>
<tr>
<td>1.10 The Thesis Layout</td>
<td>14</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter Two</th>
<th>Steganography and Images Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Introduction</td>
<td>16</td>
</tr>
<tr>
<td>2.2 Image processing</td>
<td>16</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>2.3</td>
<td>The Steganography</td>
</tr>
<tr>
<td>2.4</td>
<td>Types of Steganography</td>
</tr>
<tr>
<td>2.4.1</td>
<td>The Pure Steganography</td>
</tr>
<tr>
<td>2.4.2</td>
<td>The Secret key Steganography</td>
</tr>
<tr>
<td>2.4.3</td>
<td>The Public key Steganography</td>
</tr>
<tr>
<td>2.5</td>
<td>The Types of Cover</td>
</tr>
<tr>
<td>2.5.1</td>
<td>The Hiding in Text</td>
</tr>
<tr>
<td>2.5.2</td>
<td>The Hiding in Image</td>
</tr>
<tr>
<td>2.5.3</td>
<td>The Hiding in Audio</td>
</tr>
<tr>
<td>2.5.4</td>
<td>The Hiding in video</td>
</tr>
<tr>
<td>2.5.5</td>
<td>The Hiding in Protocol</td>
</tr>
<tr>
<td>2.6</td>
<td>The Famous Type of Steganography Methods</td>
</tr>
<tr>
<td>2.6.1</td>
<td>Least Significant Bit (LSB) insertion</td>
</tr>
<tr>
<td>2.6.2</td>
<td>Masking and filtering</td>
</tr>
<tr>
<td>2.6.3</td>
<td>Transform techniques</td>
</tr>
<tr>
<td>2.6.3.1</td>
<td>Transform techniques in DCT</td>
</tr>
<tr>
<td>2.6.3.2</td>
<td>Transform techniques in DWT</td>
</tr>
<tr>
<td>2.7</td>
<td>Digital Image</td>
</tr>
<tr>
<td>2.7.1</td>
<td>Types of Digital Image</td>
</tr>
<tr>
<td>2.7.1.1</td>
<td>Gray – Scale Image</td>
</tr>
<tr>
<td>2.7.1.2</td>
<td>Binary Image</td>
</tr>
<tr>
<td>2.7.1.3</td>
<td>The Color Image</td>
</tr>
<tr>
<td>2.7.1.4</td>
<td>Multi-spectral Image</td>
</tr>
<tr>
<td>2.7.2</td>
<td>Types of Image Depths</td>
</tr>
<tr>
<td>2.7.3</td>
<td>Types of BMP Files</td>
</tr>
<tr>
<td>Chapter Three</td>
<td>The System Implementation</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>3.1</td>
<td>Introduction</td>
</tr>
<tr>
<td>3.2</td>
<td>Step of system</td>
</tr>
<tr>
<td>3.3</td>
<td>Secret data (Image, audio) &amp; Cover video frame</td>
</tr>
<tr>
<td>3.4</td>
<td>Steganography using DCT &amp; DWT</td>
</tr>
<tr>
<td>3.4.1</td>
<td>Stego Image</td>
</tr>
<tr>
<td>3.4.2</td>
<td>Extraction process</td>
</tr>
<tr>
<td>3.5</td>
<td>Steganography using PCA &amp; DWT</td>
</tr>
<tr>
<td>3.6</td>
<td>The Resultants Images Quality Investigation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter Four</th>
<th>Results and discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Introduction</td>
</tr>
<tr>
<td>4.2</td>
<td>The results of Image Data using (DCT &amp; DWT)</td>
</tr>
<tr>
<td>4.3</td>
<td>The results of Image Data using (PCA &amp; DWT)</td>
</tr>
<tr>
<td>4.4</td>
<td>The results of Audio Data (DCT &amp; DWT)</td>
</tr>
<tr>
<td>4.5</td>
<td>Images Quality Investigation Methods</td>
</tr>
<tr>
<td>4.6</td>
<td>Result Discussions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter Five</th>
<th>Conclusions &amp; Recommendations For Future Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Conclusions</td>
</tr>
<tr>
<td>5.2</td>
<td>Recommendations For Future Works</td>
</tr>
</tbody>
</table>

Reference 65
Appendix 72
### List of Figures

<table>
<thead>
<tr>
<th>No.</th>
<th>Subject</th>
<th>page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>General Steganography System</td>
<td>5</td>
</tr>
<tr>
<td>2.1</td>
<td>The Steganography Types and Categories</td>
<td>19</td>
</tr>
<tr>
<td>2.2</td>
<td>The Discrete Cosine Transform of an image</td>
<td>25</td>
</tr>
<tr>
<td>2.3</td>
<td>Discrete Wavelet Transform on image</td>
<td>27</td>
</tr>
<tr>
<td>2.4</td>
<td>The Gray scale image</td>
<td>29</td>
</tr>
<tr>
<td>2.5</td>
<td>The Binary image</td>
<td>29</td>
</tr>
<tr>
<td>2.6</td>
<td>The RGB System of Color Image</td>
<td>30</td>
</tr>
<tr>
<td>3.1</td>
<td>The System Block Diagram</td>
<td>35</td>
</tr>
<tr>
<td>3.2</td>
<td>The block diagram of the encoder for the suggested image hiding system</td>
<td>36</td>
</tr>
<tr>
<td>3.3</td>
<td>The cover color image</td>
<td>37</td>
</tr>
<tr>
<td>3.4</td>
<td>The DWT on the cover color image</td>
<td>38</td>
</tr>
<tr>
<td>3.5</td>
<td>Part (HH) of cover image in binary system</td>
<td>39</td>
</tr>
<tr>
<td>3.6</td>
<td>The Displayed Audio Data</td>
<td>39</td>
</tr>
<tr>
<td>3.7</td>
<td>Audio file in system binary</td>
<td>40</td>
</tr>
<tr>
<td>3.8</td>
<td>The secret color image</td>
<td>40</td>
</tr>
<tr>
<td>3.9</td>
<td>The secret gray image</td>
<td>41</td>
</tr>
<tr>
<td>3.10</td>
<td>The DCT on The secret gray matrix image</td>
<td>41</td>
</tr>
<tr>
<td>3.11</td>
<td>The DCT gray data image in system binary</td>
<td>42</td>
</tr>
<tr>
<td>3.12</td>
<td>The LSB modification procedure for image Steganography</td>
<td>43</td>
</tr>
<tr>
<td>3.13</td>
<td>The DWT image stego file</td>
<td>43</td>
</tr>
<tr>
<td>3.14</td>
<td>The stego image</td>
<td>44</td>
</tr>
<tr>
<td>3.15</td>
<td>The block diagram for extraction for the suggested image hiding system</td>
<td>45</td>
</tr>
<tr>
<td>3.16</td>
<td>The Stego image</td>
<td>46</td>
</tr>
<tr>
<td>3.17</td>
<td>The DWT on stego image</td>
<td>47</td>
</tr>
<tr>
<td>3.18</td>
<td>Convert part HH stego image in system binary</td>
<td>47</td>
</tr>
<tr>
<td>3.19</td>
<td>The data image extract from type DCT</td>
<td>48</td>
</tr>
<tr>
<td>3.20</td>
<td>Image data gray color</td>
<td>48</td>
</tr>
<tr>
<td>3.21</td>
<td>The color data image extract original</td>
<td>49</td>
</tr>
<tr>
<td>3.22</td>
<td>The audio data file extract original</td>
<td>49</td>
</tr>
<tr>
<td>4.1</td>
<td>Origin Data and Cover Images in Real Spatial Size</td>
<td>54</td>
</tr>
<tr>
<td>4.2</td>
<td>Origin Data and Cover Images Gray Mode</td>
<td>54</td>
</tr>
<tr>
<td>4.3</td>
<td>Example of DCT Data</td>
<td>55</td>
</tr>
<tr>
<td>4.4</td>
<td>Example of Normalized Data</td>
<td>56</td>
</tr>
<tr>
<td>4.5</td>
<td>The DWT Merge Image</td>
<td>56</td>
</tr>
<tr>
<td>4.6</td>
<td>The Four Components Images of DWT</td>
<td>57</td>
</tr>
<tr>
<td>4.7</td>
<td>The Final Resultant Image From The Cover</td>
<td>57</td>
</tr>
<tr>
<td>4.8</td>
<td>The Forward PCA Transformation Components</td>
<td>58</td>
</tr>
<tr>
<td>4.9</td>
<td>The Final Resultant color Image From The Cover</td>
<td>59</td>
</tr>
<tr>
<td>4.10</td>
<td>Example of Origin Audio File Data Value</td>
<td>60</td>
</tr>
</tbody>
</table>
## List of Tables

<table>
<thead>
<tr>
<th>No.</th>
<th>Subjects</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Comparison between steganography and cryptography.</td>
<td>10</td>
</tr>
<tr>
<td>2.1</td>
<td>BMP file, which can be divided into Header, Palette, and Data.</td>
<td>32</td>
</tr>
<tr>
<td>2.2</td>
<td>The Steganalysis attacks.</td>
<td>33</td>
</tr>
<tr>
<td>4.1</td>
<td>The Eigen Values of Forward PCA Transform.</td>
<td>58</td>
</tr>
<tr>
<td>4.2</td>
<td>The PSNR for PCA &amp; DWT.</td>
<td>59</td>
</tr>
<tr>
<td>4.3</td>
<td>The Values of BER for Stego Methods.</td>
<td>62</td>
</tr>
</tbody>
</table>
## List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU</td>
<td>Audio Units</td>
</tr>
<tr>
<td>BER</td>
<td>Bit Error Ratio</td>
</tr>
<tr>
<td>BLSDCT</td>
<td>Bit Length Significant Discrete Cosine Transform</td>
</tr>
<tr>
<td>BMP</td>
<td>Bitmap Picture</td>
</tr>
<tr>
<td>BPP</td>
<td>Bit Per Pixel</td>
</tr>
<tr>
<td>DC</td>
<td>Discrete cosine</td>
</tr>
<tr>
<td>DCT</td>
<td>Discrete Cosine Transform</td>
</tr>
<tr>
<td>DFT</td>
<td>Discrete Fourier Transform</td>
</tr>
<tr>
<td>DWT</td>
<td>Discrete Wavelet Transform</td>
</tr>
<tr>
<td>GIF</td>
<td>Graphics Interchange Format</td>
</tr>
<tr>
<td>HH</td>
<td>Horizontally and vertically high pass</td>
</tr>
<tr>
<td>HL</td>
<td>Horizontally high pass and vertically low pass</td>
</tr>
<tr>
<td>HTML</td>
<td>Hyper Text Markup Language</td>
</tr>
<tr>
<td>IDCT</td>
<td>Inverse Discrete Cosine Transform</td>
</tr>
<tr>
<td>JPEG</td>
<td>Joint Photographic Experts Group</td>
</tr>
<tr>
<td>LH</td>
<td>Horizontally low pass and vertically high pass</td>
</tr>
<tr>
<td>LL</td>
<td>Horizontally and vertically low pass</td>
</tr>
<tr>
<td>LSB</td>
<td>Least Significant Bit</td>
</tr>
<tr>
<td>MP3/ MPEG</td>
<td>Moving Picture Expert group audio layer3</td>
</tr>
<tr>
<td>MSE</td>
<td>Mean square error</td>
</tr>
<tr>
<td>PCA</td>
<td>Principal Components Analysis</td>
</tr>
<tr>
<td>Pixel</td>
<td>Picture Element</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>PSNR</td>
<td>Peak Signal to Noise Ratio</td>
</tr>
<tr>
<td>RGB</td>
<td>Red, Green, and Blue</td>
</tr>
<tr>
<td>SSIM</td>
<td>Structural similarity index</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol /Internet Protocol</td>
</tr>
<tr>
<td>WAV</td>
<td>Waveform audio format</td>
</tr>
<tr>
<td>YIQ</td>
<td>Luminance (Y) and chrominance (I and Q)</td>
</tr>
</tbody>
</table>
Chapter One

General Introduction

1.1 Introduction

In early days of computer (1940), data security was not an important matter. Computers weren't connected as a network, and in order to steal data from computer, it was necessary to inter to the computer room itself, and the security was on the building rather than data or computer, [1]. In 1980, a new type of criminals (Hackers) arises, this phrase was used for all computer users and then for information robbers. Many of hackers steal data for challenge only, but some of them for other purposes (financial, competition, etc.). Data threats are existent even in minicomputer systems, and they increase whenever the financial processes increase.

Computer networks becomes the most important tool and mean in data communications today, we need to communicate with the other people in order to send or receive messages (data), in fast, quick, secure, and cheap way. In general, data in computer system are in danger from many threats, including indiscriminate searching, leakage inference and accidental distortion,[1]. In this era of emerging technologies, electronic communication has become an integral and significant part of everyone's life because it is simpler, faster and more secure. With adoption of electronic communication on such a large scale, it has become necessary to devise ways to transmit information secretly.

Although people have hidden secrets in plain sight now called steganography throughout the ages, the recent growth in computational power and technology has propelled it to the forefront of today’s security techniques, [2]. Steganography is the branch of science which deals
with embedding secret message on the transmitter side and retrieving it successfully on the receiver side. Whether it is about copyright protection for piracy prevention or private personal communication, steganography is the emerging technique which would be the solution to such issues. Strictly speaking, steganography is not only authentication provider through watermarking but a door to confidential communication as well.

Steganography is an art of hiding some secret message in another message without letting anyone know about presence of secret message except the intended receiver. The message used to hide secret message is called host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as stego message. In other words, stego message is combination of host message and secret message. Steganography is often mixed up with cryptography. Cryptography changes representation of secret message being transmitted while steganography hides presence of secret message, [2]. Steganography can be applied to different type of media including text, audio and video. files are considered to be excellent carriers for the purpose of steganography due to presence of redundancy,[3].

1.2 History of Steganography
Throughout history, the people have tried to find methods to hide information. In fact, they have used a multitude of such techniques and variations. David Kahn provides a very interesting history in the book named the Code breakers. There is also Bruce Norman who recounts numerous tales of cryptography and steganography during wars in the book Secret Warfare : The Battle of Codes and Ciphers, [4]. One of the first documents describing steganography is from the Histories of Herodotus, the father of history, in which he gives several cases of such activities. A man named Harpagus killed a hare and hid a message
in its belly. Then he sent the hare with a messenger who pretended to be a hunter, [4].

To inform his friends that it was time to begin a revolt against the Medes and the Persians, Histiaeus shaved the head of one of his trusted slaves, tattooed the message on his head and waited till his hair grew back. After that, he sent him along with the instruction to shave his head and his friends received the message, [4,5].

Another technique was using the tablets covered by wax. Herodotus also tells about Demeratus, who wanted to report from the Persian court back to his friends in Greece that Xerxes the Great was about to invade them. He hid this by hiding the messages under writing tablets. In that period the writing tables were usually two pieces of wood covered with wax, hinged as a book. One wrote on the wax, the recipient melted the wax and reused the tablet. The technique that Demeratus used was to remove the wax, to write his message on the wood and then to re-cover the wood with wax. The tablets were sent then as apparently blank tablets to Greece. In the beginning, this thing worked, but after a while a woman named Gorgo guessed that may be the wax hides something, so she removed the wax and became the first woman cryptanalyst, [4,5].

Ancient Romans used to write between lines using invisible inks made from fruit juices, milk and urine. They were made visible when heat was applied to the writing. During World War II invisible inks were also used to send secret messages, [6]. In the mid-90s a number of the older techniques of hiding messages inside other messages and even images became more popular with the advent of modern software and powerful computers.
Regardless of the technique used, the key similarity in all cases was that messages were hidden in plain view. In the digital world of today, namely 1992 to present, Steganography is being used all over the world on computer systems. Many tools and technologies have been created that taken advantage of old steganographic techniques such as null ciphers, coding in images, audio, video and microdot, [7].

Classical Steganography concerns itself with ways of embedding a secret message (which might be a copyright mark, or a covert communication, or a serial number) in a cover message (such as a video film, an audio recording, or computer code), [6].

1.3 The General Steganography Systems

When a steganography system is developed, it is important to consider what the most appropriate cover Work should be, and also how the stegogramme is to reach its recipient. With the Internet offering so much functionality, there are many different ways to send messages to people without anyone knowing they exist. For example, it is possible that an image stegogramme could be sent to a recipient via email. Alternatively it might be posted on a web forum for all to see, and the recipient could log onto the forum and download the image to read the message. Of course, although everyone can see the stegogramme, they will have no reason to expect that it is anything more than just an image.

In terms of development, Steganography is comprised of two algorithms, one for embedding and one for extracting. The embedding process is concerned with hiding a secret message within a cover Work, and is the most carefully constructed process of the two. A Steganographic algorithm combines the cover message with the embedded message, which is something to be hidden in the cover. The algorithm may, or may
not, use a Steganographic key (stego key), which is additional secret data that may be needed in the hidden process. The same key (or related one) is usually needed to extract the embedded massage again. The output of the Steganographic algorithm is the stego message. The cover massage and stego message must be of the same data type, but the embedded message may be of another data type. The receiver reverses the embedding process to extract the embedded message, [8]. A general Steganography system is shown in Figure (1-1).

![Steganography System Diagram](image)

**Figure (1-1): General Steganography System[9]**

where:

\[ f_E : \text{Steganographic function “embedding”} \]

\[ f_E^{-1} : \text{Steganographic function “extraction”}. \]

Emb: is the message to be hidden.

cover: is the cover data in which secret data is hidden.

stego: is the cover data with secret data embedded.

Key: is the parameter of \( f_E \).[9]
1.4 Goal of the Steganography

In an ideal world we would all be able to openly send encrypted email or files to each other with no fear of reprisals. However there are often cases when this is not possible, either because you are working for a company that does not allow encrypted email or perhaps the local government does not approve the encrypted communication (a reality in some parts of the world). This is where steganography can come into play. Steganography hides the existence of a message by transmitting information through various carriers. Its goal is to prevent the detection of a secret message. There are many reasons why steganography is used, and it is often used in significant field. It can be used to communicate with complete freed on even under condition that are censured or monitored. It can also be used to protect private communications where the use of the cryptography is normally not allowed or would raise suspicion, [6].

The primary goal of steganography is to avoids drawing suspicion to the transmission of the hidden message. If suspicion is raised, then the goal is defeated. Furthermore, actual detection of an embedded message renders the primary goal of steganography useless, [10]. The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being in a way that does not allow any enemy to even detect that there is a second secret discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide, [6].
1.5 The uses of Steganography

1- Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.

2- It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside.

3- Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. The main difference is on intent, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, steganographic methods can be used to hide this.

4- E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric fingerprint scanning, combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open ecommerce transaction verification.

5- Paired with existing communication methods, steganography can
be used to carry out hidden exchanges. Governments are interested in two types of hidden communications: those that support national security and those that do not. Digital steganography provides vast potential for both types. Businesses may have similar concerns regarding trade secrets or new product information.

6-The transportation of sensitive data is another key use of steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites, [11,12].

1.6 Steganography vs. Digital Watermarking

Information hiding is a recently rapidly developed technique in the field of information security and has receive significant attention from both industry and academia. It contains two main branches:

Digital Watermarking and Steganography. The former is mainly used for copyright protection of electronic products. While steganography, as a new way of covert communication, the main purpose is to convey data secretly by concealing the very existence of communication,[13].

Modern steganography studies the encoding and the detection of secret messages transmitted over digital communication platforms. Steganographic methods hide the presence of an arbitrary digital message by encoding it into other digital media, thus making its discovery by potential investigators very difficult. Steganography implies that the message to be transmitted is not visible to the informal eye,[16]. The importance of steganography was recently reconsidered by governments with regard to Internet security,[17].
Watermarking is the process of embedding a message on a host signal.

The Watermarking is used to embed a distinguishable symbol such as signature, logo of the organization or any trademark into host signals to recognize the ownership of the signals,[15]. Watermarking is to concentrate to get high robustness against attacks and also to ensure that the embedded information can be successfully extracted from the watermarked signals,[16]. Watermarking, as opposed to steganography, has the additional requirement of robustness against possible attacks.

A watermark can be either visible or invisible. Using digital watermarking, copyright information can be embedded into the multimedia data. This is done by using some algorithms. Information such the serial number, images or text with special significance can be embedded. The function of this information can be for copyright protection, secret communication, authenticity distinguish of data file, etc, [14].

Digital watermarking, on the other hand, focuses mainly on the protection of intellectual property rights and the authentication of digital medi,[18]. Similar to steganographic methods, digital watermarking methods hide information in digital media. The difference consists in the purpose of the hidden information – it pertains to the digital medium itself and contains information about its author, its buyer, the integrity of the content, etc. Digital watermarking methods help keeping track of the quick and inexpensive distribution of digital information over the Internet. They provide new ways of ensuring the adequate protection of copyright holders in the intellectual property distribution process, [19].
1.7 Difference between Steganography and Cryptography

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Therefore, the definition of breaking the system is different, [20]. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system need the attacker to detect that steganography has been used and he is able to read the embedded message. The following table has shown the comparison between Cryptography and Steganography, [20,21].

Table ( 1-1) Comparison Between Steganography and Cryptography

<table>
<thead>
<tr>
<th></th>
<th>Steganography</th>
<th>Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unknown message passing.</td>
<td>Known message passing.</td>
</tr>
<tr>
<td>2</td>
<td>Little known technology.</td>
<td>Common technology.</td>
</tr>
<tr>
<td>3</td>
<td>Steganography is hiding the message in another median so that nobody will notice the message.</td>
<td>The encrypted latter could be seen by anyone but cryptography message not understandable.</td>
</tr>
<tr>
<td>4</td>
<td>The end result in steganography hiding is the stego-media.</td>
<td>The end result in cryptography is the cipher text.</td>
</tr>
<tr>
<td>5</td>
<td>The goal of a secure steganography methods is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data.</td>
<td>The goal of a secure cryptography is to prevent an interceptor from gaining any information about the plaintext from the intercepted cipher text.</td>
</tr>
<tr>
<td>6</td>
<td>Steganography can be used in conjunction with cryptography by hiding an encrypted message .</td>
<td>Steganography cannot be used to adapt the robustness of cryptography system.</td>
</tr>
</tbody>
</table>
1.8 Literature Review

In 1998, Westfeld and Wolf, [22], presented a steganographic system based on DCT, which embeds a secret message in a video stream. The proposed system reproduced these effects artificially; the signal changes imperceptibly. A direct comparison with the original allows differentiation, but this still does not enable the observer to discern between the original and the altered signals. Furthermore, the sender merely transmits the changed frames.

In 2004, Al-Khzraji, [23], Design stego-system uses the transform domain in the steganography process to increase the robustness by inserting the low frequency component of the signature image in the high frequency component of the host image, using Haar-Wavelet Transform. the stego-key is used, in which the LL normalized coefficients were inserted in an inverse order at the HH-location of the host image. image. The imperceptibility of the resulted stego-image is assessed by using PSNR measure. The stego-image, under certain parameters selection, has excellent quality (PSNR above 30 dB). In the other hand, the reconstructed image has an acceptable quality but not the same as of the stego-image.

In 2004, AL Kubaisi, [6], design a system that reads a color BMP image (8 and 24 bits) and hide data of another color BMP image (8 and 24 bits) in the band of RGB was suggested and tested. first apply the discrete cosine transform (DCT) on the partitioned blocks (size 8*8) of the image. Then, the significant coefficients (low frequency) are separated from the insignificant coefficients (high frequency). The significant coefficients of the secret image are down scaled by using the root mean square function. After that the system will replace the insignificant DCT coefficients of the cover image by the down-scaled significant coefficient of the secret image.
to produce stego-cover DCT coefficients, these coefficients are send to Inverse discrete cosine transform (IDCT) to produce the stego cover image. Finally, the test results indicate that the performance of the suggested hiding system is good.

In 2006, Chen and Lin, [24], presented a new steganography technique which embeds the secret messages in frequency domain. According to different users’ demands on the embedding capacity and image quality, the proposed algorithm is divided into two modes and 5 cases. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform (DWT). Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality. Some basic mathematical operations are performed on the secret messages before embedding.

In 2009, Ahmed Tariq Sadiq et al., [25], presented a new technique for hiding text in a bitmap images will be present. The technique based on using an index of the dictionary representing the characters of the secret messages instead of the characters themselves. The technique uses multiple frequency domains for embedding these indexes in an arbitrary chosen bitmap image. By using discrete cosine transform DCT, discrete wavelet transform DWT, and a combination of both of them. A software package for implementing this technique are built and them got very good results in terms of capacity of hiding, imperceptibility which are the most two important properties of steganography, the time of hiding the text, and the security issues.

In 2010, Ekta Walia et al., [26], provides analysis of Least Significant Bit (LSB) based steganography and Discrete Cosine Transform (DCT) based steganography. LSB based steganography insets the text message in LSBs of digital data. Converting an image from a format like BMP or GIF which reconstructs the original
message exactly to a JPEG which does not and then back could destroy the information hidden in the LSBs. DCT based steganography embed the text message in LSBs bits of the discrete cosine (DC) coefficient of digital picture. When information is hidden inside video, the program hiding the information usually performs the DCT. DCT slightly changes each of the images in the video. PSNR ratio shows that PSNR ratio of DCT based steganography scheme is high as compared to LSB based steganography scheme for all types of images.

In 2010, K. B. Shiva Kumar et. al., [27], propose Bit Length Replacement Steganography Based on DCT Coefficients (BLSDCT). The cover image is segmented into 8*8 blocks and DCT is applied on each block. The numbers of payload MSB bits are embedded into DCT coefficients of the cover image based on the values of DCT coefficients. It is observed that the proposed algorithm has better PSNR, Security and capacity compared to the existing algorithm.

In 2011, A. A. Al-Saffar, [28], present a algorithm for Steganography using DCT for cover image and DWT for hidden image with an embedding order key is proposed. For more security and complexity the cover image convert from RGB to YIQ, Y plane is used and divided into four equally parts and then converted to DCT domain. The four coefficient of the DWT of the hidden image are embedded into each part of cover DCT, the embedding order based on the order key of which is stored with cover in a database table in both the sender and receiver sender. Experimental results show that the proposed algorithm gets successful hiding information into the cover image.

In 2012, Gurmeet Kaur and Aarti Kochhar, [29], presented a algorithm for Steganography using DCT for cover image and DWT for hidden image with an embedding order key is proposed. same the
work above [28] but result as a comparative analysis is made to
demonstrate the effectiveness of the proposed methods. The
effectiveness of the proposed methods has been estimated by
computing Mean Square Error (MSE) and Peak Signal to Noise Ratio
(PSNR), Processing time, security. The analysis shows that the BER
and PSNR is improved in the LSB Method but security sake DCT is
the best method.

1.9 The Aim of Thesis

The aim of this work is to design a system that hides the video
data (color images and audio) through another color image using the
steganography methods. DCT and PCA method apply on secret image and
DWT method apply on cover frame. The hiding information is manipulated
in such a way to keep a host image without any noticeable change.

1.10 The Thesis Layout

This thesis has been arranged in five chapters, as in the following details.

Chapter One: "General Introduction", History of Steganography,
General of Steganography Systems, Goal of steganography, Uses of
Steganography, Steganography vs. Digital Watermarking, Difference
between Steganography and Cryptography, Literature Review, Aim of

Chapter Two:" Steganography and Images Processing", Introduction,
Steganography, Types of Steganography, Types of Cover, Digital Image,
Steganalysis.
Chapter Three: "The mechanisms used in the research", Introduction, the layout of the suggested hiding system is given, Step of system, Embedding Process, Extraction process.

Chapter Four: "Results and Discussion", Introduction, the steganography procedures and result discussions.

Chapter five: "Conclusions and Future Work", This chapter containing the conclusions and the Suggestion for future work.
Chapter Two

Steganography and Images Processing

2.1 Introduction

The appearance and the widely usage of the Internet is considered to be one of the major events of the last years, information become available on-line, all users who have a computer can easily connect to the Internet and search for the information they want to find. The result is that everybody can read the latest news on-line and also consult digital libraries, read about firms, universities, cultural events, exhibitions, etc. but also the companies can sell their products through the Internet, using electronic commerce, [5].

In the last few years, there was a rapidly growing interest in ways to hide information in other information. The fact that an unlimited number of perfect copies can be illegally produced led people to study ways of embedding hidden copyright information and serial numbers in audio and video data; therefore people motivated to study and find methods for communicating secretly, [5].

2.2 Image processing

Image Processing is a technique to enhance raw images received from cameras/sensors placed on satellites, space probes and aircrafts or pictures taken in normal day-to-day life for various applications. Various techniques have been developed in Image Processing during the last four to five decades. Most of the techniques are developed for enhancing images obtained from unmanned spacecrafts, space probes and military reconnaissance flights. Image Processing systems are becoming popular due to easy availability of powerful personnel computers, large size memory devices, graphics software's etc.
Image Processing is used in various applications such as:
( Remote Sensing , Medical Imaging , Film industry ,..etc )
The common steps in image processing are image scanning, storing, enhancing and interpretation. There are two methods available in Image Processing:
Analog Image Processing refers to the alteration of image through electrical means. The most common example is the television image,[45].

Digital Image Processing In this case, digital computers are used to process the image. The image will be converted to digital form using a scanner – digitizer and then process it. It is defined as the subjecting numerical representations of objects to a series of operations in order to obtain a desired result. It starts with one image and produces a modified version of the same. It is therefore a process that takes an image into another.

The term digital image processing generally refers to processing of a two-dimensional picture by a digital computer. In a broader context, it implies digital processing of any two-dimensional data. A digital image is an array of real numbers represented by a finite number of bits, The principle advantage of Digital Image Processing methods is its versatility, repeatability and the preservation of original data precision,[47].

2.3 The Steganography

Steganography is a type of hidden communication process that literally means “covered writing” (according to the Greek, the words stegano or “covered” and graphs or “to write” ). The goal of steganography is to hide an information message inside harmless cover medium in such a way that it is not possible even to detect that there is a secret message, [30].

Oftentimes throughout history, encrypted messages have been intercepted but have not been decoded. While this protects the
information hidden in the cipher, the interception of the message can be just as damaging because it tells an opponent or enemy that someone is communicating with someone else. Steganography takes the opposite approach and attempts to hide all evidence that communication is taking place, [31].

Essentially, the information-hiding process in a Steganographic system starts by identifying a cover medium’s redundant bits (those that can be modified without destroying that medium’s integrity or the origin data values). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography’s goal is to keep its mere presence undetectable. But, the steganographic systems, because of their invasive nature, leave behind detectable traces in the cover medium through modifying its statistical properties. Therefore, eavesdroppers can detect the distortions in the resulting stego medium’s statistical properties. The process of finding these distortions is called Statistical Steganalysis calculations, [32].

2.4 Types of Steganography

According to the embedding technique, steganography can be classified into three main types, see figure (2-1). The public goal of them is to embed a secret message in a digital cover by using a private technique for each of them. They try to make stego-project and innocent cover perceptually similar, [1] they are:-
2.4.1 The Pure Steganography

Pure steganography algorithms hide information in a digital cover without using any types of key, [1]. This method of Steganography is the least secure means by which to communicate secretly because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message,[33]. In this approach stegobject contains the cover and the hidden message only, [34].

the embedding process can be described as a mapping:

\[ E : C \times M \rightarrow C \quad \text{... 2.1} \]

Where \( C \) is the set of possible covers and \( M \) is the set of possible messages. The extraction process consists of the mapping.

\[ D : C \rightarrow M \quad \text{... 2.2} \]

and extracting the secret message out of a cover, [6].
2.4.2 The Secret Key Steganography

This technique uses a type of hiding key, which is called the secret key, [1]. The stegobject contains the cover, hidden message and the secret key. Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a stego-key, which makes it more susceptible to interception. The benefit to Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message, [33,34].

The mapping process could be written as follows:

\[ E_k : C \times M \times K \rightarrow C \quad \ldots 2.3 \]

and

\[ D_k : C \times K \rightarrow M \quad \ldots 2.4 \]

with the property that

\[ D_k(E_k(c,m,k), K) = m \]

For all \( c \in C \) and \( k \in K \), is called a secret key steganography system, [6].

2.4.3 The Public key Steganography

This technique uses two types of key to embed the secret message into the cover. The first key is called the private key, and the second key is called public key. The stegobject contains the cover, hidden message, private key, and the public key, [1]. The sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a more robust way of implementing a steganography system because it can utilize a much more robust and researched technology in Public Key Cryptography, [33,34].
2.5 The Types of Covers

There are many types of cover in which information are embedded. Some of which are public, another are not. always, steganography users discover new types of cover, therefore, types of cover cannot be enumerated. In every day we expect a new type of cover. Figure ( 2-1) shows the main categories of file formats that can be used for steganography.

2.5.1 The Hiding in Text

Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word of the previous sentence, you will see that it is possible and not very difficult. Hiding information in plain text can be done in many different ways, [35]. Many techniques involve the modification of the layout of a text, rules like using every n-th character or the altering of the amount of white space after lines or between words, [35]. Invisible inks prove to be a popular medium. Computers bring more capability to information hiding. The layout of a document may also reveal information. Documents may be marked identified by modulations in the positions of lines and words. Adding spaces and "invisible" characters to text provides a method to pass hidden information. An Interesting way to see this is to add spaces and extra line breaks in an HTML file. Web browsers ignore these "extra" spaces and lines, but revealing the source of the web page displays the extra characters. For an additional text-based hiding techniques and an algorithm for mimicking the statistical distribution of text to pass information see, [36]. The last technique was successfully used in practice and even after a text has been printed and copied on paper for ten times, the secret message could still be retrieved. Another possible way of storing a secret inside a text is using a publicly available cover source, a
book or a newspaper, and using a code which consists for example of a combination of a page number, a line number and a character number. This way, no information stored inside the cover source will lead to the hidden message. Discovering it relies solely on gaining knowledge of the secret key, [35].

2.5.2 The Hiding in Image

Image can be considered as a great media used to hold information by using steganography techniques huge data contained in images give a good area to hide information in it. Image view may take the detector attention away from the hidden information, which give another reason to hide information in image. This approach of steganography is the specified approach of this thesis, there for it will be explained in some details.

2.5.3 The Hiding in Audio

In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files, [37]. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information. The list of methods that are commonly used for audio steganography are listed and discussed below, [37].
Chapter 2  Steganography and Images Processing

1- LSB coding  
2- Parity coding  
3- Phase coding  
4- Spread spectrum  
5- Echo hiding  

2.5.4 The Hiding in video

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information, [37]. In this research will be hidden data in images after cutting up video to frames.

2.5.5 The Hiding in Protocol

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission, [38]. In the layers of the OSI network model there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a Transmission Control Protocol /Internet Protocol (TCP/IP) packet in some fields that are either optional or are never used, [38].

2.6 The Famous Type of Steganography Methods

There are several types of image steganography, [1]. The most popular methods are:

2.6.1 Least Significant Bit (LSB) insertion

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic
techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small, [20]. For example, if we consider image steganography then the letter A can be hidden in three pixels (assuming no compression). The original raster data for 3 pixels (9 bytes) may be;

(00100111 11101001 11001000)  
(00100111 11001000 11101001)  
(11001000 00100111 11101001) 

The binary value for A is 10000001. Inserting the binary value for A in the three pixels would result in

(00100110 11001000 11101000)  
(00100110 11001000 11101000)  
(11001000 00100111 11101001) 

The underlined bits are the only three actually changed in the 8 bytes used. On average, LSB requires that only half the bits in an image be changed. You can hide data in the least and second least significant bits and still the human eye would not be able to discern it. The resultant image for the above data insertion and the original cover image are given below, [37].

2.6.2 Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level, [20].
2.6.3 Transform techniques

Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants, [20]. In this research will be use techniques (DCT and DWT) as following:

2.6.3.1 Transform techniques in DCT

This method is used, but similar transforms are for example the Discrete Fourier Transform (DFT). These mathematical transforms convert the pixels in such a way as to give the effect of “spreading” the location of the pixel values over part of the image, [39]. It transforms a signal or image from the spatial domain to the frequency domain, figure (2-2). It can separate the image into high, middle and low frequency components, by grouping the pixels into 8×8 pixel blocks and transforming the pixel blocks into 64 DCT, [40].

![Figure (2-2): The Discrete Cosine Transform of an image](image-url)
Chapter 2  Steganography and Images Processing

The general equation for a 1D (N data items) DCT is defined by the following equation:

\[ t(k) = c(k) \sum_{n=0}^{N-1} s(n) \cos \left( \frac{2n+1}{2N} \right) k \], \hspace{1cm} 2.5

where \( s \) is the array of \( N \) original values, \( t \) is the array of \( N \) transformed values, and the coefficients \( c \) are given by, [6]:

\[ c(0) = \sqrt{1/N} \quad , \quad c(k) = \sqrt{\frac{2}{N}} \quad \text{for} \quad 1 \leq k \leq N-1 \quad \text{... 2.6} \]

The general equation for a 2D (N by M image) DCT is defined by the following equation:

\[ t(i, j) = c(i, j) \sum_{m=0}^{W-1} \sum_{n=0}^{H-1} s(m, n) \cos \left( \frac{2m+1}{2W} \right) i \cos \left( \frac{2n+1}{2H} \right) j \], \hspace{1cm} 2.7

with an analogous notation for \( s, t \) \( w \) is the block width, \( H \) is the block height (in our case \( W = H = N = 8 \) and the \( c(i, j) \) given by, [6].

\[ c(0, j) = \sqrt{\frac{1}{N}}, c(i, 0) = \sqrt{\frac{1}{N}} \quad \text{and} \quad c(i, j) = \sqrt{\frac{2}{N}} \quad \text{for} \quad \text{both} \quad i \quad \text{and} \quad j \neq 0 \quad \text{... 2.8} \]

There are some simple functions to compute the IDCT, as the following:

The One-Dimensional (1-D) Inverse Discrete Cosine Transform, IDCT is defined by, [6]:

\[ s(n) = \sum_{k=0}^{N-1} c(k) t(k) \cos \left( \frac{2n+1}{2N} \right) k \], \hspace{1cm} 2.9

The Two-Dimensional (2-D) Discrete Cosine Transform is defined by, [6]:

\[ s(m, n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} c(i, j) t(i, j) \cos \left( \frac{2m+1}{2N} \right) i \cos \left( \frac{2n+1}{2N} \right) j \], \hspace{1cm} 2.10
2.6.3.2 Transform techniques in DWT

This is another frequency domain in which steganography can be implemented. DCT is calculated on blocks of independent pixels. DWT applies on entire image. DWT offers better energy. DWT splits component into numerous frequency bands called sub bands known as:

- LL – Horizontally and vertically low pass
- LH – Horizontally low pass and vertically high pass
- HL - Horizontally high pass and vertically low pass
- HH - Horizontally and vertically high pass

Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three parts without making any alteration in LL sub band, figure (2-3). As other three sub-bands are high frequency sub-band they contain insignificant data. Hiding secret data in these sub-bands does not degrade image quality that much, [41].

![Figure (2-3): Discrete Wavelet Transform on image](image_url)
2.7 Digital Image

An digital image is a two – dimensional matrix of the intensity values, each element in this matrix is called pixel. Pixel values (intensities) determine image colors in the pixel. Images can be classified according to the color of the image, or to the bits required to represent a pixel (depth). Moreover, there are other classifications of images according to other features, which can be found in, [1].

2.7.1 Types of Digital Image

There are four main types of images according to the range of the image colors, some of the them has an inner classification, these types are:

2.7.1.1 Gray – Scale Image

It is also known as an intensity, gray scale, or gray level image. Array of class uint8, uint16, single, or double whose pixel values specify intensity values, [42]. The pixel values of binary image can be expanded to (0-256) range, in which there are 256 color available, White, Black, and 254 levels of gray color. This image may give a good view when color details are not needed, or less storage area are available, see figure (2-4). If the color levels are of another color(Red, Green, or Blue), then the image is called Monochrome image, [1]. Binary image can be derived from gray scale image, by determining a threshold and setting any value greater than threshold to (255) and the other to (0).
2.7.1.2 Binary Image

In this types of images, there are only two colors white and black, each pixel value is either (1) for white, or (0) for black. Binary image shows the boundaries of the objects in the image, without any inner detail, see figure (2-5). Binary images can be used in monitor controlling of industrial production lines, edge detection in image enhancement applications, and many other applications, [1].
2.7.1.3 The Color Image

It is known as an RGB image, a true color image is an image in which each pixel is specified by three values one each for the red, blue, and Green components of the pixel scalar, [42]. There are three essential colors Red (R), Green (G) and Blue (B), i.e. any color can be produced by mixing them. Instead of storing huge number of colors, computers store three values for each pixel R, G, and B respectively and generate colors by displaying these values on the monitor at the same time, see figure (2-6). This system is called RGB system, [1].

2.7.1.4 Multi-spectral Image

This form of image typically contains information outside the normal human perceptual range. This may include infrared, ultraviolet, acoustic, or radar images are not images in the usual sense because information represented is not directly visible by the human visual system. It can be displayed as a visual form by mapping the different spectral bands to RGB system, [1].

Figure (2-6): The RGB System of Color Image
2.7.2 Types of Image Depths

There are many types of images according to the depth bit per pixel (BPP), [1], and for each BPP there are \(2^{\text{BPP}}\) colors range in the image. The most used forms in windows applications are:

- Binary image (1BPP)
- Gray scale image (8BPP)
- 16 Colors image (4BPP)
- 256 Colors image (8BPP)
- True colors (24BPP)

2.7.3 Types of BMP Files

BMP file can be divided into three parts Header, Palette, and Data, [1]. All BMP files consist of headers and data, but only some of them consist of palettes. BMP header contains the image features like file identification (BM), file size, data size, image height, image width, ... etc, the header size is 54 bytes. The palette is a table that contains image colors, i.e. the pixel value refers to a position in the palette, which represents the color of the pixel as shown in Table (2-1). Data contain two values the pixel position in the file, and the values of the pixels, which represent palette position, or the color value in the files that does not contain palette. In true color image, there is no palette, instead each pixel is represented by 3 bytes (24 bits), a byte for each color (R G B). In this form a huge number of colors can be produced, i.e. for each byte there are 256 levels of the color, and by mixing them we can obtain 16777216 colors \((256*256*256)\), which can give more color details. A digital image is a rectangular array of pixels sometimes called a bitmap, [43].
Table (2-1) BMP file, which can be divided into Header, Palette, and Data

<table>
<thead>
<tr>
<th>Palette No.</th>
<th>Red</th>
<th>Green</th>
<th>Blue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20</td>
<td>75</td>
<td>35</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>20</td>
<td>32</td>
</tr>
<tr>
<td>3</td>
<td>120</td>
<td>130</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>220</td>
<td>10</td>
<td>230</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>0</td>
<td>190</td>
</tr>
<tr>
<td>6</td>
<td>225</td>
<td>220</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BM 1024 15 64 54 .....</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.8 The Steganalysis

Modern steganography’s goal is to keep its mere presence undetectable, but steganographic systems—because of their invasive nature—leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is; modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium’s statistical properties. The process of finding these distortions is called statistical steganalysis,[44].

Steganalysis is the art of discovering and rendering useless such covert message, or the attacks against hidden data, [1]. Steganalysis involves two aspects, detection and distortion of embedded message. Detection requires that the analyst observe various relationships between combination of steganalysis elements, these elements are cover, message, stegobject, and stegotool. Distortion attack requires that the analyst
manipulate the stegobject to render the embedded information useless or remove it altogether, [1].

Attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling or destroying hidden information. An attacker may also embed counter-information over the existing hidden information. Due to space limitations we will look at two methods: detecting messages or their transmission and disabling embedded information. These approaches (attacks) vary depending upon the methods used to embed the information in to the cover media,[36].

There are many methods of detecting steganography signature (a sign to the steganography existence ), they are based on combination of steganography elements known by steganalyst . They can be explained as given in table (2-2), [1,36].

**Table (2-2) The Steganalysis Attacks**

<table>
<thead>
<tr>
<th>No.</th>
<th>Attack</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sego-only</td>
<td>Only the stegobject is available for attacker.</td>
</tr>
<tr>
<td>2</td>
<td>Known cover</td>
<td>The original cover and stegobject are both available.</td>
</tr>
<tr>
<td>3</td>
<td>Known message</td>
<td>At some point, the attacker may know the hidden message. Analyzing stegobject patterns that corresponds to the hidden message may be beneficial for future attacks against that system. Even with the message, this may be very difficult and may even be considered as equivalent to the stego- only attack.</td>
</tr>
<tr>
<td>4</td>
<td>Chosen stego</td>
<td>The steganography tools and the stegobject are both known.</td>
</tr>
<tr>
<td>5</td>
<td>Chosen message</td>
<td>The steganalyst generates stegobject from some stegotools and a chosen message. The goal in this attack is to determine corresponding patterns in the stegobject that may point to the use of specific stegotool.</td>
</tr>
<tr>
<td>6</td>
<td>Known attack</td>
<td>The stegotool is known and both the original cover and stegobject are available.</td>
</tr>
</tbody>
</table>
Steganalysis depends on some features or modifications that may results from stego-tool executing, [1]. They may output a signature of stego-tool that used in hiding technique, they can be listed as:-

1- Obvious modification on the original innocent cover.
2- Perceptible differences in the image colors.
3- Repetitive patterns.
4- Probability distribution and hypothesis testing.
Chapter Three

The System Implementation

3.1 Introduction

The proposed system is designed to hide the video (image and audio) using discrete cosine transformation (DCT) method and discrete wavelet transformation (DWT) method. Also, the Principal Components Analysis (PCA) and (DWT) methods were used to hide the data. The video was divided into multi frames using the Ulead video studio 9 program. This program have been cutting up the video into 20 frame per second. The system will embed the (input) secret image (color, audio) color inside a cover (image). The secret images transform to another image by applying the (DCT or PCA) methods, where, the cover reconstructed using the discrete wavelet transformation method (DWT) and produce (output) stego-image.

3.2 The System Steps

The designed and implemented system does two main functions, Embedding and Extraction. These two functions involved several sub functions to complete the job, which can be shown as figure (3-1).

![Figure (3-1): The System Block Diagram](image)
3.3 Secret Data (Images, Audio) & Cover video frame

The secret data are color images of (JPG) format file and audio. The cover data was a gray image used as cover to hide the data. The Steganography was implemented using the following two main methods. These methods were evaluated using four written Matlab program.

3.4 Steganography using DCT & DWT

The process of embedding a data to be put inside the cover to hide the data you want to hide is the image of the cover is also a picture of the method used in this research are shown in the following chart, figure (3-2).

Figure (3-2): The block diagram of the encoder for the suggested data hiding system
The embedding module is used to hide secret image inside a cover. The embedding process implies the following operations:

1. Load the secret (image, audio). The selection is performed by choosing an image color of type JPG and audio of type WAV.
2. Load the cover video frame. The selection is performed by choosing an image color of type JPG.
3. Apply the DWT on the cover image.
4. Apply the DCT on the secret (image, audio).
5. Hiding the secret DCT data in the DWT of the cover (image) in part HH to produce the stego-cover.
6. Apply the IDWT on the resulted stego-cover to produce the stego-image.
7. Save the stego-image as the color image.

In the following a list of algorithms used to handle the processes involved in the hiding:

Step 1: Read the color image as a cover, figure (3-3).

![The Cover Color Image](image-url)

**Figure (3-3):** The cover color image
**Step 2:** Apply equation discrete wavelet transformation (DWT) to the image used as a cover and when viewing the image will split the picture into four parts, the first part (LL) and second part (LH) and three part (HL) and four part (HH) and we are hiding the image you want to hide inside the (HH ). The following figure shows the image after applying the conversion DWT, figure (3-4).

![The DWT cover image](image)

**Figure (3-4): The DWT on the cover color image**

**Step 3:** converting the part (HH) into the binary system and then hide the images in the least significant bits (LSB) method. The figure (3-5) show the part (HH) in system binary and show location LSB whose in hide data.
Step 4: Read the Audio file as a data secret can be displayed using the windows media player as shown in figure (3-6).

Figure (3-6): The Displayed Audio Data

Step 5: Apply equation discrete cosine transformation (DCT) on the audio file and converting it to binary system then hide the audio data in the least significant bits in the segment cover image The following figure shows the audio file of binary system and show locations audio data, figure (3-7).
Figure (3-7): Audio File in Binary System

Step 6: Read the secret color image, figure (3-8).

Figure (3-8): The secret color image

Step 7: Convert the secret color image into gray image, figure (3-9).
Step 8: Apply the discrete cosine transformation (DCT) on the image used to hide where the image to transform it into a gray image and then apply the normal conversion (DCT). After that transform it to the binary system in order to do their hiding inside the cover. Figure(3-10), represent the matrix image after applying the conversion DCT.

Figure (3-10): The DCT on The secret gray matrix image
Step 9: The process of substitution (Insertion) in this process we hid the secret data (i.e., the image and audio you want to hide them) within images used as a cover and hide the data in part (HH) of the image cover then hide the secret data in the least significant bits in the image cover through this process we specify the location from which starts the process of replacing bits of the image you want to hide in bits image cover any mean in the site we put the image data inside the cover, which named key (K) through which we can retrieve the data. Upon completion we will get a data inside the cover image. The following figures (3-11) & (3-12) shows the image file after LSB modification procedure for image Steganography.

Figure (3-11): The DCT gray data image in system binary
Step 10: In this step viewing result stego file image, figure (3-13).

Figure (3-12): The LSB modification procedure for image Steganography

Figure (3-13): The DWT image stego file
Step 11: In this step, the inverse of the discrete wavelet transform (IDWT) on the resulting stego file image was applied, figure (3-14).

![The Stego Image](image)

**Figure (3-14): The stego image**

Step 12: save stego file image.

3.4.1 The Stego Image

Stego result image put in place the image in the video you want to send it (with image we have cut it to a frame of the video), with same and which containing data (image, audio) so that can send into receiver.

3.4.2 Extraction process

The extraction process used to create the hide data from the stego image. The figure (3-15) show block diagram the step extraction.
The extraction algorithm is used to extract secret data from the stego image. The extraction operation involved different steps:

1- Read stego image.

2- Apply DWT on stego image.

3- Extract the secret data (image, audio) from the stego image.

4- Commonalty data image after extract to get hide image.

5- Commonalty data audio after extract to get hide audio.
6- Apply IDCT on image after commonalty to reconstruct the secret image.

7- Save secret image.

In the following a list of algorithms used to handle the processes involved in the extraction:

Step 1: Load stego image, figure (3-16).

![Figure (3-16): The Stego image](image)

Step 2: Apply equation discrete wavelet transformation (DWT) on the stego image and when viewing the image will split the picture into four parts, the first part (LL) and second part (LH) and three part (HL) and four part (HH) and extraction the hidden image data from the part (HH), figure (3-17).
Figure (3-17): The DWT on stego image

Step 3: Converting the part (HH) into the binary system and then extraction the image data from the least significant bits (LSB), figure (3-18).

Figure (3-18): Convert part HH stego image in system binary

Step 4: Retrieve the Secret data hidden from cover by reversing the process of inclusion and learning key (K) whose from through knowledge of the site from which we have included the secret data.
Step 5: Compile the image data retrieve hidden and return it to their proper positions will get a picture of the type (DCT), figure (3-19).

**Figure (3-19): The data image extract from type DCT**

Step 6: Apply the inverse discrete cosine transformation (IDCT) on the resulting image retrieval process (DCT) to get on image hiding but will be image gray color, figure (3-20).

**Figure (3-20): Image data gray color**
Step 7: Convert gray image to color image, figure (3-21).

![The Color Image](image)

Figure (3-21): The color data image extract original

Step 8: Compile the audio data retrieve hidden and return it to their proper positions will get audio file of the type (WAV).

![The audio data file extraction](image)

Figure (3-22): The audio data file extract original

Step 9: Save image color and audio file.
3.5 Steganography using PCA & DWT

Principal Component Analysis (PCA) is a variable reduction procedure. It is useful when the obtained data is of a number of variables (possibly a large number of variables), and that there is some redundancy in those variables. In this case, redundancy means that some of the variables are correlated with one another, possibly because they are measuring the same construct. Because of this redundancy, it should be possible to reduce the observed variables into a smaller number of principal components (artificial variables) that will account for most of the variance in the observed variables, [46].

The data (color image only) is of three bands, with high correlation values between them. The PCA kernel was applied to the data color image, therefore, the output result is three PCs bands and three Eigen values of 8 bit representation. For the purpose of compression and program result evaluation, the first PC will be use only with the three Eigen values i.e. for binary transformation. The PCA kernel was used instead of the DCT and all the above steps are the same. Also, in data extraction after stegano process, the extract first PC and the three Eigen values can be use to extract the three data band through the inverse PCA.

3.6 The Resultants Images Quality Investigation

Digital images are subject to a wide variety of distortions during acquisition, processing, compression, storage, transmission and reproduction, any of which may result in a degradation of visual quality. The objective methods for assessing perceptual image quality traditionally attempted to quantify the visibility of errors (differences) between a resultants image and a reference image using a variety of known properties of the human visual system, [46].
The Subjective image quality methods depend on some mathematical and statistical calculation between the origin images and process results. The first method is peak signal-to-noise ratio (PSNR), the term (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale. The mathematical representation of the PSNR is as follows, [46].

\[
PSNR = 20 \log_{10} \left( \frac{MAX_f}{\sqrt{MSE}} \right) \quad \text{... 3.1}
\]

where the MSE (Mean Squared Error) is:

\[
MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (f(i,j) - g(i,j))^2 \quad \text{... 3.2}
\]

And,

\( f \): represents the matrix data of our original image.

\( g \): represents the matrix data of our resultant image in question.

\( m \): represents the numbers of rows of pixels of the images and i represents the index of that row.

\( n \): represents the number of columns of pixels of the image and j represents the index of that column.

\( MAX_f \): is the maximum signal value that exists in our original “known to be good” image.

In computing the MSE between two identical images, if the value equal to zero and hence the PSNR will be undefined (division by zero). The main limitation of this metric is that it relies strictly on numeric comparison and does not actually take into account any level of
biological factors of the human vision system such as the structural similarity index. (SSIM) For color images, the MSE is taken over all pixels values of each individual channel and is averaged with the number of color channels. Another option may be to simply perform the PSNR over a converted luminance or grayscale channel as the eye is generally four times more susceptible to luminance changes as opposed to changes in chrominance. This approximation is left up to the experimenter. So, the minimum value of PSNR represent best result, [46].
Chapter Four

Results And Discussion

4.1 Introduction

The results of the steganography methods will be introduce and analysis in this chapter, two types of data have been used (images and audio), where the cover used type was video frame. The two main transformations (DCT, & PCA) were applied for the data, that yield four programmes to evaluate the results. The program written using the Matlab facilities (standard functions and adaptive others). The used images data were extracted from a video file format, the extraction process was evaluated using a special program. The extracted frames of images holds the JPEG extensions, while the used audio file format is wave.

The sequence of images is band to band color (3-bands), of 8-bit representations, i.e. gray levels are (0-255). The spatial dimensions of each band are 208 (No. of columns), and 160 (No. of rows). these dimensions were selected for decrease the times of running of programs. Also, for image quality investigations, two main methods were used to compare between the origin and steganography data. This was accomplished through written sub-programs in Matlab facilities.

4.2 The Results of Image Data using (DCT & DWT)

The first; written programs is use the discrete cosine transform applies to the data which is color frame image, and discrete wavelet transform, applies for the cover image. The origin data and cover images shown in figure (4-1) with real spatial sizes.
Origin Data  

Cover Image

Figure (4-1): Origin Data and Cover Images in Real Spatial Size

In each method, the output image from the program will be represented and compared with the origin data.

The following images represent the results of programming steps that were written in chapter three. In order to apply the transformation, both the data and cover were converted into gray scale images by converting the three bands data into single band, figure (4-2).

Origin data  

Cover image

Figure (4-2): Origin Data and Cover Images Gray Mode
The discrete cosine transform DCT yield a minus image values, these values affected the transformation into binary bits image. i.e, the binary image production is not correct in values. In order to avoid this affect, a linear normalization process will be apply to extract the DCT result values, the new range data is (0-255). This process dose not effected the data quality and data texture because its simple process and can be reversed exactly using the max. and min. values of origin data after DCT, figure (4-3), and figure (4-4) shown example of DCT data and normalized data respectively from the Matlab commands window.

![Figure (4-3): Example of DCT Data](image-url)
Chapter 4
Results And Discussion

Figure (4-4): Example of Normalized Data

The DWT was applied to the cover image to yield the four sub-images that will be evaluated also in the same program. The DWT based on the gray level of 255, figures (4-5), (4-6) illustrate the four components images of DWT merge and separately. The HH sub-image was used to cover the data in the steganography model.

Figure (4-5): The DWT Merge Image
After applying the steganography, the final resultant image from the cover will be illustrated in the figure (4-7). This image will be compared with the original one, figure (4-2, left) using the subjective PSNR method.

**Figure (4-7): The Final Resultant Image From The Cover**

The PSNR value for the first method is $3.1 \times 10^3$ which was created between the origin image and the resultant image from the stego process. In previous work, the process was applied on the gray image, also, the method can be applied for each band if the transformation is applied for another band. i.e. the specific program must be applied for each band separately, the written subroutine is indicated in appendix A.

### 4.3 The Results of Image Data using (PCA & DWT)

In this method, the principal component analysis was applied to the data image, in this process the data must be multi bands. The condition of multi-dimensional data is necessary due to the PCA kernel requirement. In the forward PCA process, the first PC and the $n$ Eigen values are
require to extract the all inverse bands, where, the \( n \) is the total No. of bands, the third forward PCs are shown in figure (4-8). Also, table (4-1) represent the Eigen values of forward PCA transform.

![Forward PCA Transformation Components](image)

**Table (4-1) The Eigen Values of Forward PCA Transform**

<table>
<thead>
<tr>
<th>Eigen Value 1</th>
<th>Eigen Value 2</th>
<th>Eigen Value 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.8720</td>
<td>0.1236</td>
<td>0.0069</td>
</tr>
</tbody>
</table>

From the Eigen values, the PC1 holds 87% of the all bands data, where the PC2, & PC3 can be considered as noise. That forward PCA transform kernel was performed through written program. In fact, the first principal components was used into the steganography kernel, i.e. apply the same steps after DCT of the above method. So, the hidden image is the first PC1 only which was covered by the LL part of DWT (applied to the cover image). In order to extract the final resultant bands images, the first PC and the three Eigen values in table (4-1) were used to produce the three bands of data using the inverse PCA transform kernel, it was performed in the same program. Figure (4-9) represent the final
resultant images. The adaptive techniques in this method is the capability of use multi dimensional data say \( n \) bands and hide them in the steganography kernel in low size of data, the total size equal to the \( 1/n \) plus the bits requirement of the Eigen values numbers. This PCA adaptive technique represent a new combination of image processing steganography and image compression. Since many secrete processing were associated with the data transmission and communications, therefore, the data size reduction is more important and useful. This is represent an evidence to use the PCA transform which is essential in image compression.

![The Final Resultant Color Image From The Cover](image)

**Figure (4-9): The Final Resultant Color Image From The Cover**

The PSNR value for the second method was calculated between the origin image and the resultant image from the stego process. The process was applied for each band of the two images respectively, table (4-2) show the PSNR for each band, the written subroutine is indicate in appendix B.

**Table (4-2) The PSNR for PCA & DWT**

<table>
<thead>
<tr>
<th>PSNR Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{Band 1} )</td>
</tr>
<tr>
<td>3.2E+3</td>
</tr>
</tbody>
</table>
4.4 The Results of Audio Data (DCT & DWT)

The third method is the steganography of an audio file of wave format performed with the DCT and DWT techniques. The file has been readied using the Matlab wave read facility. The value of the data is determined between the (-1) and (1), therefore, a linear normalized process was applied to convert the audio data value between (0) and (255), figure (4-10), show some of origin audio file data value.

![Command Window](image)

![Figure (4-10):Example of Origin Audio File Data Value](image)

Therefore, the DCT transform will be apply to the normalized audio data in the same way of the first method and in the same cover image. In order to extract the audio file after the stego process from the cover image, a renormalized process will be apply using the values between (-1) to (1). The PSNR investigation between the origin audio file and the final
stego file was applied for a part of the file due to the file large of the input audio. The value of PSNR is 3.14E+3.

4.5 Images Quality Investigation Methods

The PSNR and BER (Bit Error Rate) are use to investigate the quality of resultant images. The first criteria was discussed in chapter three, where, the second BER can be assume as is the number of bit errors divided by the total number of transferred bits during a studied time interval. In digital transmission, the number of bit errors is the number of received bits of a data stream over a communication channel that have been altered due to noise, interference, distortion or bit synchronization errors. The BER is a unitless performance measure, often expressed as a percentage. The bit error probability $p_e$ is the expectation value of the BER. The BER can be considered as an approximate estimate of the bit error probability. This estimate is accurate for a long time interval and a high number of bit errors.

As an example, assume this transmitted bit sequence:

0 1 1 0 0 0 1 0 1 1,

And the following received bit sequence:

0 0 1 0 1 0 1 0 0 1,

The number of bit errors (the underlined bits) is in this case 3. The BER is 3 incorrect bits divided by 10 transferred bits, resulting in a BER of 0.3 or 30%. In a communication system, the receiver side BER may be affected by transmission channel noise, interference, distortion, bit synchronization problems, attenuation, wireless multipath fading, etc. In the present works, the bit errors or noise were introduce from the transformations and steganography processing methods.
The BER value for the above three methods are illustrate in the table (4-3).

**Table (4-3) The Values of BER for Stego Methods**

<table>
<thead>
<tr>
<th>DCT, Image</th>
<th>DCT, Audio</th>
<th>PCA, Image</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Band1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Band2</td>
</tr>
<tr>
<td>0.82</td>
<td>0.78</td>
<td>Band3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.85</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.81</td>
</tr>
</tbody>
</table>

**4.6 Result Discussions**

The above results were represent the core of this thesis in concerting with the steganography methods for digital data. The following can be achieved;

1- All methods holds error in the resulting data due to the data transformation and processing.

2- The DCT stego method hold many minus values, therefore, a normalization process was applied.

3- The DCT stego method deal with single band only, therefore, to overcome all data bands, the program must be rerun.

4- In the PCA stego method, there are no minus values in the processing steps.

5- Also, the PCA stego method, can be apply for multi dimension data as well as the value for high compression factor.
In this chapter, the works conclusion and the recommendation future work will be introduce;

5.1 Conclusions

The three methods that been used are DCT, PCA, and DWT for the secret image and cover frame to create steganography image. The DCT stego method hold many minus values, therefore, a normalization process was applied to this method. The DCT stego method deal with single band only, therefore, to overcome all data bands, the program must be rerun.

In the PCA stego method, there are no minus values in the processing steps. Also, the PCA stego method, can be apply for multi dimension data as well as the value for high compression factor.

All methods holds error in the resulting data due to the data transformation and processing, and the errors value different from method to another. The tested results indicate that the considered hiding method has an acceptable performance, and the produced stego-images are not so different from the original secret image to the human eye. The evaluation methods was given by using scale PSNR and BER for three methods above. The best result for three methods above was by using DCT on secret image and DWT on cover frame to acquirement good values PSNR and BER. On other hand, using PCA and DWT on secret image and cover frame given good values.
5.2 Recommendations For Future Works

1. In future, its recommended to use real time data transfer channels with steganography methods.

2. The user can use another image processing methods, such as co-occurrence matrix analysis.

3. Also, the processing of binary transformations can be adaptive in many ways in order to increase the security of data transfer.

4. Using another technique of steganography in order to decrease the amount of resulting hidden data.

5. Can uses method PCA on both the cover frame and secret image.
References


<table>
<thead>
<tr>
<th>Reference</th>
<th>Reference</th>
</tr>
</thead>
</table>


Appendix A,

The Subroutine of Image Data using (DCT & DWT)

clear all
path='D:\161.jpg';% Data
co= imread(path);
figure;%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%% imshow(co);%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% 
%%%%
title('The Color Data Image')
I= rgb2gray(co);% convert to gray
J = dct2(I); % Forward Descrete Cosine Transfom

%% Normalazation process
% % mn1=min(J);
% % mn2=min(mn1);
% % mx1=max(J);
% % mx2=max(mx1);
% % b1=255/(mx2-mn2);
% % a1=255-(mx2*b1);
% % for i1=1:160;
% %     for k1=1:208;
% %         J3(i1,k1)=(a1+(b1*J(i1,k1)))
% %     end
% % end
% % figure;
% % J4=uint8(J3-1);
% % imshow(J4);%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% 
%%%%
title('The Normalized Inverse Descrete Cosine Transform  Image')

yu=idct2(J); % Inverse Descrete Cosine Transfom
yu1=uint8(yu-1);
figure;
imshow(yu1);

% The Inverse Discrete Cosine Transform Gray Data Image

figure;
imshow(yu1);

title('The Inverse Discrete Cosine Transform Gray Data Image')

imageDCE=(J); % Data gray
% [r c]=size(imageDCE);
% convert image to from Decimal to binary
imageBIN=dec2bin(J3,8); % cover it to one col 8bit and row=r*c
imageBIN(:,8)=0;
subplot(1,2,1);
figure;

figure;
imshow(J);

title('The DCT Gray Data Image')

imwrite(J,'D:\newdct1.jpg')

path='D:\106.jpg';

The Cover Image
x=imread(path);
x=rgb2gray(x);
figure;
imshow(x);

title('The Cover Gray Image')
x1=double(x)+1;

% The current extension mode is zero-padding (see dwtmode).
% Load original image.
% load woman;
% X contains the loaded image.
% map contains the loaded colormap.
ncol = 255; % size(map,1);
% Perform single-level decomposition
% of X using db1.
[cA1,cH1,cV1,cD1] = dwt2(x1,'db1');
% Images coding.
cod_x = wcodemat(x1,ncol);
cod_cA1 = wcodemat(cA1,ncol);
cod_cH1 = wcodemat(cH1,ncol);
cod_cV1 = wcodemat(cV1,ncol);
cod_cD1 = wcodemat(cD1,ncol);
dec2d = [...
    cod_cA1, cod_cH1; ...
    cod_cV1, cod_cD1 ...
];
cod_cA11 = uint8(cod_cA1 - 1);
cod_cH11 = uint8(cod_cH1 - 1);
cod_cV11 = uint8(cod_cV1 - 1);
cod_cD11 = uint8(cod_cD1 - 1);
dec2d1 = uint8(dec2d - 1);
figure;
imshow(cod_cA11); % LL
figure;
imshow(cod_cH11);
figure;
imshow(cod_cV11);
figure;
imshow(cod_cD11); % HH
figure;
imshow(dec2d1);%%%%%%%

%%% use LL to convert to binary iamge
x2=double(cod_cA11)+1;
[row col]=size(x2);
zoom=2;
zr=zoom*row;
zc=zoom*col;
for i=1:zr;
    y=i/zoom;
    mapi=round(y);
    if mapi==0;
        mapi=1;
    end
    for j=1:zc;
        z=j/zoom;
        mapj=round(z);
        if mapj==0;
            mapj=1;
        end
        im_zoom(i,j)=x2(mapi,mapj);
    end
end
J1=idct2(J);

New_cover=uint8(im_zoom-1);
figure;
imshow(New_cover);%%%%%%%
title('The New Cover Image')
for i=1:160;
    for j=1:208;
        steco_image(i,j,1)=im_zoom(i,j); % Cover
        steco_image(i,j,2)=im_zoom(i,j); % Cover
    end
end
steco_image(i,j,3)=J1(i,j);  % Data  
final_image(i,j)= steco_image(i,j,3);
end
end
New_Data=uint8(steco_image-1);
figure;
imshow(New_Data);
title('The New Srtego Image')

New_final=uint8(final_image-1);
figure;
imshow(New_final);
title('The New Final Srtego Image')

%PEAK SIGNAL TO NOISE RATIO CALCULATION
origin=double(I)+1;
y1=0;
for i=1:160;
    for j=1:208;
        y1=y1+( origin(i,j)-final_image(i,j) )^2;
    end
end
res=y1/(160*208)
figure;
plot (origin,final_image)

% % imageBIN_Cover_LL=dec2bin( x2,8);% SIZE 80 X 104
% % I=double(I)+1;
% % imageBIN_Data=dec2bin( J,8); % SIZE 160 X 208
% % for i=1:2:33280;
% %    cov(i)=imageBIN_Cover_LL(i);
% %    cov(i+1)=imageBIN_Cover_LL(i);
% % end
% %
% % result=cov;
% % for k=1:33280;
% % dat(k)=imageBIN_Data(k);
% % stegano_image(k)=cov(k)+dat(k);
% % end

% % %%%DENORMALIZED PROCESS
% % a2=mn2;
% % b2=(mx2-mn2)/1023;
% % for i1=1:160;
% % for k1=1:208;
% % J4(i1,k1)=(a2+(b2*J3(i1,k1)));  
% % end
% % end
% % yu2=uint8(J4-1);
% % figure;
% % imshow(J4);%%%%IMSHOW(J4)
% % title('The DENormalized Inverse Discrete Cosine Transform Image')
% 
% ri=bin2dec(imageBIN_Cover_LL);
% %
% % i1=0;
% % for i=1:80;
% % for j=1:104;
% % i1=i1+1;
% % ri1(j,i)=ri(i1);
% % end
% % end
% % ri2=uint8(ri1-1);
% % figure;
% imshow(ri2);
%%%title('The DEwavlet Cover Image')
Appendix B, The Subroutine of Image Data using (PCA & DWT)

clear all
path='D:\161.jpg';% Data
co= imread(path);
figure;%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    imshow(co);%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
title('The Color Data Image')
    I= rgb2gray(co);% convert to gray
    J = dct2(I); % Forward Descrete Cosine Transfom
    yu=idct2(J); % Inverse Descrete Cosine Transfom
    yu1=uint8(yu-1);
    figure;
    %
    imshow(yu1);%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    title('The Inverse Descrete Cosine Transform Gray Data Image')

% PRINCIPAL COMPONENTS ANALYSIS
d1 = double(co) + 1;
x=160;%256;%915;
y=208;%881;
nob=3;
i1=0;
for i=1:x;
    for j=1:y;
        i1=i1+1;
        for k=1:nob;
d2(i1,k)=d1(i,j,k);
end
d1(i,k);
end end
end
s1=0;
s2=0;
s3=0;
for i=1: x*y;
    s1=s1+d2(i,1);
    s2=s2+d2(i,2);
    s3=s3+d2(i,3);
end
m1=s1/(x*y);
m2=s2/(x*y);
m3=s3/(x*y);
for i=1 :x*y;
    d3(i,1)=d2(i,1)-m1;
    d3(i,2)=d2(i,2)-m2;
    d3(i,3)=d2(i,3)-m3;
end
d4=d3';
d5=d4*d3;
acc=0.000003;
sss=0;
for i=1:3;
    for j=1:3;
        if i==j
            sss=sss+d5(i,j);
        end
    end
end
uo1=[1 1 1 ];
for ic1=1:100;
    u11=uo1*d5;
ma11=max(u11);
u11=u11/ma11;
u21=u11*d5;
ma21=max(u21);
u21=u21/ma21;
    if ((u21-u11)<=acc*[1 1 1]);
        u31=u21*d5;
        L1=max(u31);
        S1=sum(u31.^2);
        n11=(L1/S1)^0.5;
        v1=u31*n11;
    break,
    else
        u01=u21;
    end
end
lem1=L1/sss;
Eigen1=lem1
vv1=v1';
vvv1=vv1*v1;
dw=d5-vvv1;%new var-covar matrix
d55=dw;
uo2=[1 1 1];
for ic2=1:100;
    u12=uo2*d55;
    ma12=max(u12);
    u12=u12/ma12;
    u22=u12*d55;
    ma22=max(u22);
    u22=u22/ma22;
    if ((u22-u12)<=acc*[1 1 1]);
        u32=u22*d55;
        L2=max(u32);
        S2=sum(u32.^2);
n12=(L2/S2)^0.5;
v2=u32*n12;
break,
else
    uo2=u22;
end
end
lem2=L2/sss;
Eigen2=lem2
vv2=v2';
vvv2=vv2*v2;
dw1=d55-vvv2;% new var-covar matrix
d555=dw1;
uo3=[1 1 1 ];
for ic3=1:100;
    u13=uo3*d555;
    ma13=max(u13);
    u13=u13/ma13;
    u23=u13*d555;
    ma23=max(u23);
    u23=u23/ma23;
    if ((u23-u13)<=acc*[1 1 1 ]); u33=u23*d555;
    L3=max(u33);
    S3=sum(u33.^2);
    n13=(L3/S3)^0.5;
    v3=u33*n13;
    break,
else
    uo3=u23;
end
end
lem3=L3/sss;
Eigen3=lem3
vv3=v3';
vvv3=vv3*v3;

% Computing Scalar Multipler
w1=v1/L1;
w2=v2/L2;
w3=v3/L3;

for i=1:x*y;
    for j=1:3;
        y1(i)=w1(j)*d3(i,1);
y2(i)=w2(j)*d3(i,2);
y3(i)=w3(j)*d3(i,3);
    end
end

% Forward Transform
for i=1:x*y;
    z(i,1)=fix(m1+y1(i)*v1(1)+y1(i)*v1(2)+y1(i)*v1(3));
z(i,2)=fix(m2+y2(i)*v2(1)+y2(i)*v2(2)+y2(i)*v2(3));
z(i,3)=fix(m3+y3(i)*v3(1)+y3(i)*v3(2)+y3(i)*v3(3));
end

i1=1;
i2=0;
for i=1:x*y;
    i2=i2+1;
z1(i1,i2)=z(i,1);
    if i2==y;
        i1=i1+1;
i2=0;
    end
end
\texttt{ma1}=\text{max}(z1); \\
\texttt{maa1}=\text{max}(ma1); \\
\texttt{mi1}=\text{min}(z1); \\
\texttt{mii1}=\text{min}(mi1); \\
\text{for } i=1:x; ; \\
\hspace{10pt} \text{for } j=1:y; \\
\hspace{20pt} z1(i,j)=255*((z1(i,j)-\text{mii1)/(maa1-mii1)}; \\
\hspace{10pt} \text{end} \text{ end} \\
\texttt{i1}=1; \\
\texttt{i2}=0; \\
\text{for } i=1:x*y ; \\
\hspace{10pt} \texttt{i2}=i2+1; \\
\hspace{10pt} z2(i1,i2)=z(i,2); \\
\hspace{10pt} \text{if } \texttt{i2}\text{=}\text{y}; \\
\hspace{20pt} \texttt{i1}=i1+1; \\
\hspace{20pt} \texttt{i2}=0; \\
\hspace{10pt} \text{end} \text{ end} \\
\texttt{ma2}=\text{max}(z2); \\
\texttt{maa2}=\text{max}(ma2); \\
\texttt{mi2}=\text{min}(z2); \\
\texttt{mii2}=\text{min}(mi2); \\
\text{for } i=1:x; ; \\
\hspace{10pt} \text{for } j=1:y; \\
\hspace{20pt} z2(i,j)=255*((z2(i,j)-\text{mii2)/(maa2-mii2)}; \\
\hspace{10pt} \text{end} \text{ end} \\
i1=1; \\
i2=0; \\
\text{for } i=1:x*y ; \\
\hspace{10pt} \texttt{i2}=i2+1; \\
\hspace{10pt} z3(i1,i2)=z(i,3);
if i2==y;
    i1=i1+1;
    i2=0;
end

ma3=max(z3);
maa3=max(ma3);
mi3=min(z3);
mii3=min(mi3);
for i=1:x;;
    for j=1:y;
        z3(i,j)=255*((z3(i,j)-mii3)/(maa3-mii3));
    end
end

z11=uint8(z1-1);
figure;
imshow(z11);
title('First Forward PC Image');

z22=uint8(z2-1);
figure;
imshow(z22);
title('Second Forward PC Image');

z33=uint8(z3-1);
figure;
imshow(z33);
title('Third Forward PC Image');

for i=1:x*y;
    zr(i,1)=fix(m1+y1(i)*v1(1)+y1(i)*v2(1)+y1(i)*v3(1));
    zr(i,2)=fix(m2+y2(i)*v1(2)+y2(i)*v2(2)+y2(i)*v3(2));
    zr(i,3)=fix(m3+y3(i)*v1(3)+y3(i)*v2(3)+y3(i)*v3(3));
end
i1=1;
i2=0;
for i=1:x*y
    i2=i2+1;
zr1(i1,i2)=zr(i,1);
if i2==y;
i1=i1+1;
i2=0;
end
end
mar1=max(zr1);
maar1=max(mar1);
mir1=min(zr1);
miir1=min(mir1);
for i=1:x;
    for j=1:y;
        zr1(i,j)=255*((zr1(i,j)-miir1)/(maar1-miir1));
    end
end
i1=1;
i2=0;
for i=1:x*y
    i2=i2+1;
zr2(i1,i2)=zr(i,2);
if i2==y;
i1=i1+1;
i2=0;
end
end
mar2=max(zr2);
maar2=max(mar2);
mir2=min(zr2);
miir2=min(mir2);
for i=1:x;
for j=1:y;
    zr2(i,j)=255*((zr2(i,j)-miir2)/(maar2-miir2));
end
end
i1=1;
i2=0;
for i=1:x*y;
    i2=i2+1;
    zr3(i1,i2)=zr(i,3);
    if i2==y;
        i1=i1+1;
        i2=0;
    end
end
mar3=max(zr3);
maar3=max(mar3);
mir3=min(zr3);
miir3=min(mir3);
for i=1:x;
    for j=1:y;
        zr3(i,j)=255*((zr3(i,j)-miir3)/(maar3-miir3));
    end
end
zr11=uint8(zr1-1);
figure;
imshow(zr11);
title('First Inverse PC Image');
zr22=uint8(zr2-1);
figure;
imshow(zr22);
title('Second Inverse PC Image');
zr33=uint8(zr3-1);
figure;
imshow(zr33);
title('Third Inverse PC Image');

for i=1:x;;
    for j=1:y;
        stego(i,j,1)=zr1(i,j);
        stego(i,j,2)=zr2(i,j);
        stego(i,j,3)=zr3(i,j);
    end
end

stego1=uint8(stego-1);
figure;
imshow(stego1);
title('The Final Stego Color Image');

for i=1:160;
    for j=1:208;
        y1=y1+(d1(i,j,1)-stego(i,j,1))^-2;
    end
end

res=y1/(160*208)
% figure;
% plot (d1, stego)

path='D:\106.jpg';

The Cover Image
x=imread(path);
x=rgb2gray(x);
figure;
imshow(x);
title('The Cover Gray Image')
x1=double(x)+1;

nbcol = 255;% size(map,1);
[cA1,cH1,cV1,cD1] = dwt2(x1,'db1');

% Images coding.
cod_x = wcodemat(x1,nbcol);
cod_cA1 = wcodemat(cA1,nbcol);
cod_cH1 = wcodemat(cH1,nbcol);
cod_cV1 = wcodemat(cV1,nbcol);
cod_cD1 = wcodemat(cD1,nbcol);

dec2d = [...
    cod_cA1,    cod_cH1;    ...
    cod_cV1,    cod_cD1 ...
];

cod_cA11=uint8(cod_cA1-1);
cod_cH11=uint8(cod_cH1-1);
cod_cV11=uint8(cod_cV1-1);
cod_cD11=uint8(cod_cD1-1);
dec2d1=uint8(dec2d-1);

figure;
imagesc(cod_cA11);% LL

figure;
imagesc(cod_cH11);

figure;
imagesc(cod_cV11);

figure;
imagesc(cod_cD11);% HH

figure;
imagesc(dec2d1);% use LL to convert to binary image

x2=double(cod_cA11)+1;
[row col]=size(x2);
zoom=2;
zr=zoom*row;
zc=zoom*col;
for i=1:zr;
    y=i/zoom;
    mapi=round(y);
    if mapi==0;
        mapi=1;
    end
    for j=1:zc;
        z=j/zoom;
        mapj=round(z);
        if mapj==0;
            mapj=1;
        end
        im_zoom(i,j)=x2(mapi,mapj);
    end
end
J1=idct2(J);

New_cover=uint8(im_zoom-1);
figure;
imshow(New_cover);title('The New Cover Image')
for i=1:160;
    for j=1:208;
        steco_image(i,j,1)=im_zoom(i,j); % Cover
        steco_image(i,j,2)=im_zoom(i,j); % Cover
        steco_image(i,j,3)=J1(i,j); % Data
    end
end
New_Data=uint8(steco_image-1);
figure;
imshow(New_Data);%

title('The New Srtego Image')
الملخص

تنتقل البيانات الأمنة خلال شبكة الإنترنت باستخدام عملية الإخفاء. وهو علم إخفاء المعلومات باستعمال غطاء غير معلم إذا لا يثير شكوك أي الآخرين.

في هذا البحث، النظام المقترح صمم لإخفاء بيانات الفيديو (صورة، صوت) باستخدام طريقة تحويل جيب التمام المتقطع (DWT) وطريقة التحويل الموجي المتقطع (DCT) وأيضاً طرق تحليل المكونات الرئيسي (PCA) و (DWT) لتُستخدم لإخفاء البيانات.

بعد تقطيع الفيديو إلى الإطارات باستخدام البرنامج Ulead video studio 9 إذا يقوم بتفطير الفيديو إلى 20 إطار في الثانية الواحدة. النظام المستخدم سيُっぱَن (إخفاء) بيانات سريّة (صورة ملونة، صوت) داخل الصورة الملونة المستخدمة لغطاء الصورة السريّة وتطبيق عليها طريقة تحويل (DCT) النطاق المستخدمة لغطاء تتجزأ إلى أربعة أجزاء (LL, LH, HL, HH) ومعتمد إخفاء الصورة السريّة. في جزء (HH) أي في قطع البت الأوّل رتبة (DWT) من صورة الغطاء. سوف نحصل على ناتج صورة stego عن طريق مفتاح stego يمكن استرجاع البيانات المخفية (بيانات سريّة) من غطاء وذلك عن طريق استعمال معكوّس عملية التضمين.

طبقت كل من MSE وBER، PSNR على الصورة المستخدمة كغطاء قبل وبعد إخفاء البيانات فيها لتقسيم نوعية الصورة بعد الإخفاء وقيمة تأبيثًا لأن الطرق المقترحة قد نفّذت باستعمال برنامج MATLAB ver. 7.6.
إخفاء بيانات الفيديو المستندة على طريقة تحويل جيب تمام المقطع

رسالة مقدمة
إلى كلية العلوم / جامعة بغداد كجزء من مطالب دبلوم درجة الماجستير في الفيزياء (التحسس النائي)

من قبل
محمد عبد الحسن حسين
بكالوريوس فيزياء، 2010

إشراف
أ.د. علاء سعود مهدي
أ.م.د علي حسن خضر

2014 1435