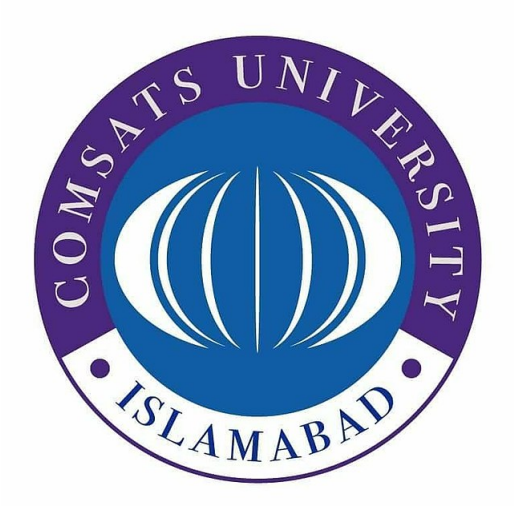
COMSATS University Islamabad Attock Campus

Department Of Electrical And Computer Engineering

June 2022



Digital Image Water Marking

Digital Signal Processing- CPE324

Submitted by:

Ammar (FA19-BCE-001)

Shayan Shahid (FA19-BCE-012)

Sadaqat Ullah (FA19-BCE-023)

Submitted To

Mr.Muhammad Abdul Rehman Chaudary

ABSTRACT

Keywords - Digital Image Processing , Digital Water Marking, Least Significant Bit, Signals Processing

With the rapid growth and internet and networks techniques, multimedia data transforming and sharing is common to many people. Multimedia data is easily copied and modified, so necessarily for copyright protection is increasing. It is the imperceptible marking of multimedia data to brand ownership. Digital watermarking has been proposed as technique for copyright protection of multimedia data. Digital watermarking invisibly embeds copyright information into multimedia data. Thus, digital watermarking has been used for copyright protection, finger protection, fingerprinting, copy protection, and broadcast monitoring. Common types of signals to watermark are images, music clips and digital video. The application of digital watermarking to still images is concentrated here. The major technical challenge is to design a highly robust digital watermarking technique, which discourages copyright infringement by making the process of watermarking removal tedious and costly.

Contents

List of Figures

Chapter 1

INTRODUCTION

1.1 Digital Image Processing

Digital Image Processing (DIP) deals with manipulation of digital images through a digital computer. It is a subfield of signals and systems but focuses particularly on images. DIP focuses on developing a computer system that is able to perform processing on an image. The input of that system is a digital image and the system process that image using efficient algorithms, and gives an image as an output.

Figure 1.1: Working Of DIP

The digital image processing deals with developing a digital system that performs operations on an digital image.

1.2 What Is An Image?

An image is nothing more than a two dimensional signal. It is defined by the mathematical function f(x,y) where x and y are the two coordinates horizontally and vertically. The

value of f(x,y) at any point is gives the pixel value at that point of an image.

Figure 1.2: Normal Image

The above figure is an example of digital image which is nothing but a two-dimensional array of numbers ranging between 0 and 255.

1.3 Relation Between A Signal And Image

In physical world, any quantity measurable through time over space or any higher dimension can be taken as a signal. A signal is a mathematical function, and it conveys some information. A signal can be one dimensional or two dimensional or higher dimensional signal. One dimensional signal is a signal that is measured over time. The common example is a voice signal. The two-dimensional signals are those that are measured over some other physical quantities. The example of two-dimensional signal is a digital image.

1.3.1 Relationship

Since anything that conveys information or broadcast a message in physical world between two observers is a signal. That includes speech or (human voice) or an image as a signal. Since when we speak, our voice is converted to a sound wave/signal and transformed with respect to the time to person we are speaking to. Not only this, but the way a digital camera works, as while acquiring an image from a digital camera involves transfer of a signal from one part of the system to the other.

1.4 Digital Image

Since capturing an image from a camera is a physical process. The sunlight is used as a source of energy. A sensor array is used for the acquisition of the image. So, when the sunlight falls upon the object, then the amount of light reflected by that object is sensed by the sensors, and a continuous voltage signal is generated by the amount of sensed data. In order to create a digital image, we need to convert this data into a digital form. This involves sampling and quantization. The result of sampling and quantization results in a two-dimensional array or matrix of numbers which are nothing but a digital image.

1.5 Why Digital Image Processing

Digital information and data are transmitted more often over the internet now than ever before. The availability and efficiency of global computer networks for the communication of digital information and data have enhanced the popularity of digital media. Hence, information security is becoming more and more important for information intercommunication and transmission among people. In order to secure information against unauthorized illegal access, diverse methods such as symmetric and asymmetric encryption systems are used.

Traditionally, protection of digital data has been provided by a variety of encryption methods. However, encryption alone does not provide an adequate solution as it only provides for robust delivery of the content. Once the content is decrypted, it is no longer protected and the content may be illegally replicated or copied without any prevention. Thus, piracy in the presence of internet and computers is a major concern. To deal with piracy and counterfeiting of the multimedia data, digital watermarking technique has an edge over the other available techniques. Thus, last decades gaining attention on watermarking schemes.

The technique of Digital Image watermarking using MATLAB is inserting an information to an image, then it can be further detected (or) extracted for different purposes which contain authentication and identification purposes. The important aspect of watermarking is the method of hiding a message on a video (or) audio with data for the need to generate new data. The date cannot be replaced (or) remove a new data with the real one. Watermarking is a method to protect the data and to authenticate the digital content. Wa-

termarking is required due to the emergence of usage of internet in one's day to day life. As the usage of digital content is growing rapidly, there are many instances where data is insecure. Watermarking is a process to hide data for authorization purpose. Watermarking is the best way to secure the digital content. Watermarking can be done by various methods. Least Significant Bit Watermarking (LSBW) method is one of them. In this method, the pixel values of the image are converted in to binary and the information is concealed in the bits of the pixel values. A digital watermark added to a photo, is more or less visible information in the form of a text or some other photo/image that has been added to the original photo. The added information can be more or less transparent to make it either easy or hard to notice the watermark. Typical applications of digital watermarking can include broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control legacy enhancement and content description.

1.6 History Of Watermarking

The term "Digital Watermark" was coined by Andrew Tirkel and Charles Osborne in December 1992. Two basic methods of information hiding are cryptography and stenography. The term stenography means cover writing and cryptography means secret writing. Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the plain text and disguised message is called cipher text. The process of converting a plain text to a cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption. Encryption protects contents during the transmission of the data from the sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected and is in the clear. Watermarking techniques are particular embodiment's of stenography. The use of watermarks is almost as old as paper manufacturing.Our ancients poured their half-stuff slurry of fiber and water on to mesh molds to collect the fiber, then dispersed the slurry within deckle frames to add shape and uniformity, and finally applied great pressure to expel the water and cohere the fiber. This process hasn't changed too much in 2000 years. One by-product of this process is the watermark the technique of impressing into the paper a form of image, or

text derived from the negative in the mold, as the paper fibers are squeezed and dried. The digitization of our world has expanded our concept of watermarking to include immaterial digital impressions for use in authenticating ownership claims and protecting proprietary interests. However, in principle digital watermarks are like their paper ancestors. They signify something about the token of a document or file in which they inherit. Whether the product of paper press or discrete cosine transformations, watermarks of varying degree of visibility are added to presentation media as a guarantee of authenticity, quality ownership and source.

1.7 Watermarking

The digital watermarking or watermarking explains the ways and mechanisms to hide the data and the data can be a number or text, in digital media, it may be a picture or video. The watermarking is a message that can be embedded into the digital data like video, pictures, and text and the embedded data can be extracted later. The stenography is also another form of watermarking and in this, the messages are hidden in the content without making the people to note its presence. The Indian currency is a good example of watermarking and in the general watermarking procedure the genuine image undergoes the embedding procedure along with the watermark and the output generated will be a watermarked image.

1.8 Framework For Watermarking

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. In general, any watermarking scheme (algorithm) consists of three parts:

- The watermark
- The encoder (marking insertion algorithm)

Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark into the object.

The verification algorithm authenticates the object determining both the owner and the integrity of the object.

1.9 Types Of Digital Watermark

Watermarks and watermarking techniques can be divided into various categories in various ways. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows:

1. Image Watermarking
2. Video Watermarking
3. Audio Watermarking
4. Text Watermarking

According to Human Perception, the watermarking techniques can be divided into three types

1. Visible Watermark
2. Invisible Watermark
3. c) Dual Watermark

Visible watermark is a translucent overlaid into an image and is visible to the viewer. Visible watermarking is used to indicate ownership and for copyright protection. Whereas an invisible watermark is embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed. Invisible watermark is used as evidence of ownership and to detect misappropriated images. Dual watermark is the combination of visible and invisible watermark. An invisible watermark is used as a backup for the visible watermark.

1.10 Applications

Visible watermarks can be used in following cases 1. Visible watermarking for enhanced copyright protection. In such situations, where images are made available through Internet and the content owner is concerned that the images will be used commercially (e.g.

imprinting coffee mugs) without payment of royalties. Here the content owner desires an ownership mark, that is visually apparent, but which doesn't prevent image being used for other purposes (e.g. scholarly research). 2. Visible watermarking used to indicate ownership originals. In this case, images are made available through the Internet and the content owner desires to indicate the ownership of the underlying materials (library manuscript), so an observer might be encouraged to patronize the institutions that owns the material.

1.10.1 Invisible Robust Watermark

Invisible robust watermarks find application in following cases.

- Invisible Watermarking to detect misappropriated images. In this scenario, the seller of digital images is concerned, that his, fee-generating images may be purchased by an individual who will make them available for free, this would deprive the owner of licensing revenue.
- Invisible Watermarking as evidence of ownership. In this scenario, the seller the digital images suspects one of his images has been edited and published without payment of royalties. Here the detection of the seller's watermark in the image is intended to serve as evidence that the published image is property of seller.

1.10.2 Invisible Fragile Watermark

Following are the applications of invisible fragile watermarks.

Invisible Watermarking for a trustworthy camera.In this scenario, images are captured with a digital camera for later inclusion in news articles. Here, it is the desire of a news agency to verify that an image is true to the original capture and has not been edited to falsify a scene. In this case, an invisible watermark is embedded at capture time its presence at the time of publication is intended to indicate that the image has not been attended since it was captured. Invisible Watermarking to detect alternation of images stored in a digital library. In this case, images (e.g. human fingerprints) have been scanned and stored in a digital library the content owner desires the ability to detect any alteration of the images, without the need to compare the images to the scanned materials.

1.11 Attacks On Watermark

A watermarked image is likely to be subjected to certain manipulations, some intentional such as compression and transmission noise and some intentional such as cropping, filtering, etc. They are summarized below Lossy Compression:

Many compression schemes like JPEG and MPEG can potentially degrade the data's quality through irretrievable loss of data.

- Geometric Distortions: Geometric distortions are specific to images and videos and include such operations as rotation, translation, scaling and cropping. Common Signal Processing Operations: They include the followings.
- D/A conversion
- A/D conversion
- Re sampling
- Re quantization
- Dithering distortion
- Re compression
- Linear filtering such as high pass and low pass filtering
- Non-linear filtering such as median filtering
- Color reduction
- Addition of a constant offset to the pixel values
- Addition of Gaussian and Non Gaussian noise
- Local exchange of pixels
- Other intentional attacks:
- Printing and Re scanning
- Watermarking of watermarked image (re watermarking)

- Collusion: A Number of authorized recipients of the image should not be able to come together (collude) and like the differently watermarked copies to generate an un-watermarked copy of the image (by averaging all the watermarked images).
- Forgery: A Number of authorized recipients of the image should not be able to collude to form a copy of watermarked image with the valid embedded watermark of a person not in the group with an intention of framing a 3rd party.
- IBM attack: It should not be possible to produce a fake original that also performs as well as the original and also results in the extraction of the watermark as claimed by the holder of the fake original.

Chapter 2

METHODOLOGY

2.1 Encoding Process

The figure illustrates the encoding process.

Let us denote an image by I, a signature by S = { sr, sR, . . . — the watermarked image by I'. E is an encoder function, it takes an image I and a signature S, and it generates a new image which is called watermarked image I', i.e. E (I, S) = I'.

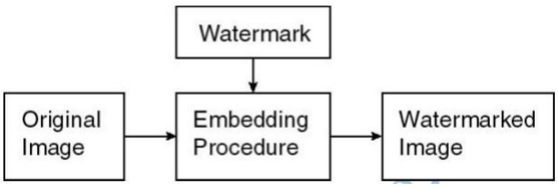


Figure 2.1: Flow Diagram From Encoding Process

2.2 System Design

Visible watermark is a translucent overlaid into an image and is visible to the viewer. Visible watermarking is used to indicate ownership and for copyright protection. Whereas an invisible watermark is embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed. Invisible watermark is used as evidence of ownership and to detect misappropriated images. Dual watermark is the combination of visible and invisible watermark. An invisible watermark is used as a backup for the visible

watermark. According to Working Domain, the watermarking techniques can be divided into two types a) Spatial Domain Watermarking Techniques b) Frequency Domain Watermarking Techniques In spatial domain techniques, the watermark embedding is done on image pixels while in frequency domain after marking techniques the embedding is done after taking image transforms. Generally frequency domain methods are more robust than spatial domain techniques. According to the watermarking extraction process, techniques can be divided into three types

- Non-blind
- Semi-blind
- Blind

Non-blind watermarking schemes require original image and secret key for watermark detection whereas semi-blind schemes require secret key and watermark bit sequence for extraction. Blind schemes need only secret keys for extraction.

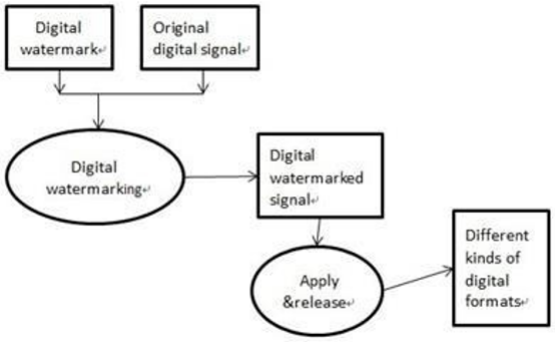


Figure 2.2: General System Model

2.3 Implementation

A watermarking system has a number of requirements. Obviously, different applications have different concerns therefore, there is no set of properties that all watermarking systems have to satisfy. This section highlights the common evaluation methods used for watermarking systems and indicates when they are important. Invisibility:The best way to evaluate invisibility is to conduct subject tests where both original and watermarked

signals are presented to human subjects. However, due to the high volume of test images, subject tests are usually impractical. The most common evaluation method is to compute the peak signal-to-noise ratio (PSNR) between the host and watermarked signals. PSNR is defined as follows:

$$PSNR = 10log10/2552MSE \tag{2.1}$$

and

$$MSE = 1nXni = 1(ImaiAIw(i))2 \tag{2.2}$$

where Im and Iw are the original and watermarked images, respectively, n is the total number of pixels, and 255 refers to the highest possible image level in an 8-bit image. In general, the higher the PSNR, the better the signal quality.

Effectiveness: Digital watermarking systems have a dependence on the input signal. Effectiveness refers to whether it is possible to detect a watermark immediately following the embedding process. Although 100% effectiveness is ideal, it is often not possible to achieve such a high rate. For example, watermarking of a completely random signal is very difficult because of the lack of redundancies. **Efficiency:** Efficiency refers to the embedding capacity. For images, it is usually expressed in bits of information per pixel (bpp). A 512 x 512 image with 16 KB of embedded data has an embedding capacity of 0.5 bpp. The desired size of the watermark is application dependent. **Robustness:** Robustness is one of the most commonly tested properties in digital watermarking systems. In many applications, it is unavoidable that the watermarked signal would be distorted before it reaches the detector. Robustness refers to the ability for the detector to detect the watermark after signal distortion, such as format conversion, introduction of transmission channel noise and distortion due to channel gains. Security One of the major goals of a digital watermarking system is to protect digital content from illegal use and distribution. However, the protection is diminished if the attackers can estimate, remove, or insert a watermark.

2.4 Desired Characteristics

The desired characteristics of the watermarks are listed below.

- **Difficult to notice:** The invisible watermarks should not be noticeable to the viewers nor should the watermark degrade the quality of the content. Ideally, it should

be imperceptible . However, if a signal is truly imperceptible, then perceptual based lossy compression algorithm should, in principle, remove such signal. Of course, a just noticeable difference (JND) is usually observed by comparing two signals, e.g. compressed and uncompressed or watermarked and original.

- **Robustness:** In general, a watermark must be robust to transformations that include common signal distortions as well as D/A and A/D conversions and loss compression. Moreover, for images and video, it is important that the watermark survive geometric distortions such as translation, scaling and cropping etc. It has been argued that robustness can only be attained if watermark is placed perceptually significant regions of an image. But it has been already mentioned that watermark should be imperceptible, which is possible if watermark is plated in perceptually insignificant regions of an image. They are two conflicting requirements. It should be noted robustness actually comprises two separate issues: Whether or not the watermark is still present in the data after distortion and whether the watermark detector can detect it. It should also be noted that ability to embed robust watermarks in digital images does not necessarily imply the ability to establish ownership, unless certain requirements are imposed legally on the watermarking scheme.

- **Tamper-resistance:** As well as requiring the watermark to be robust to legitimate signal distortions, a watermark may also be subjected to signal processing that is solely intended to remove the watermark. It is important that a watermark be resistant to such tampering. There are a number of possible ways this may be achieved:

- **Private Watermark:** A private watermark where either the decoder requires knowledge of the un-watermarked content or the pseudo-random noise sequence that constitutes the watermark is only known to sender and receiver, are inherently more tamper resistant than public watermarks in which every body is free to decode the watermark

- **Asymmetric encoder/decoder:** If removal of a public watermark requires inverting the encoding, then it is highly desirable to make the encoder as complex as possible, especially if the watermark is only to be applied once. However if decoders must run in real time, then it is necessary for the decoding process to be simpler than encoding.

- **Bit-rate:** The bit rate of a watermark refers to them amount of information a watermark can encode in a signal. This is especially important for public watermarks. Low bit-rate watermarks are more robust .

- **Modification and Multiple Watermarks:** In some circumstances, it is desirable to alter the watermark after insertion. For example, in the case of digital video discs, a disc may be watermarked to allow only a single copy. Once this copy has been made, it is then necessary to alter the watermark on the original disc to prohibit further copies. Changing a watermark can be accomplished either (a) removing the 1st watermark and then adding a new one or (b) inserting a 2nd a watermark such that both are readable, but are overrides the other.

- **Scalability:** It is well known that computer speeds are approximately doubling every eighteen months, so that what looks computationally unreasonable today may very quickly become a reality. It is therefore, very desirable to design a watermark whole decoder is scalable with each generation of computers. Thus, for example, the first generation of decoder might be computationally inexpensive but might not be as reliable as next generation decoders that can afford to expend more computation to deal with issues such as geometric distortions.

- **Unambiguous:** Retrieval of watermark should unambiguously identify the owner. The watermark should not need any interpretation as looking into the database of codes to interpret the watermark unless a standard body maintains it internationally.

- **Universal:** The same digital watermark should apply to all three media under consideration. This is potentially helpful in the watermarking of multimedia products. Also, this feature is conducive to implementation of audio/image/video watermarking algorithm on common hardware.

- **Minimum alternation of pixels:** While watermarking high quality image and art works the amount of pixel modification should be minimum. Minimum Human intervention: Insert of watermark should require little human intervention or labor.

2.5 Working

The idea behind this watermarking technique is the following: if you see image as a matrix NxM (where N and M are the dimension of the image) you can represent the value of the pixel in the position (i,j) as a binary number; this binary can be then divided in all of its bit, so that you will have a most significant bit (the one that contains quite a lot of information, and a least significant bit that contains few information).

User is asked which bit plane they want to hide the image in. The image to be hidden is read and its size is found out so that its size is compared with the watermarked image. They both should be of the same size. Watermark is inserted to the selected bit plane of the cover image.

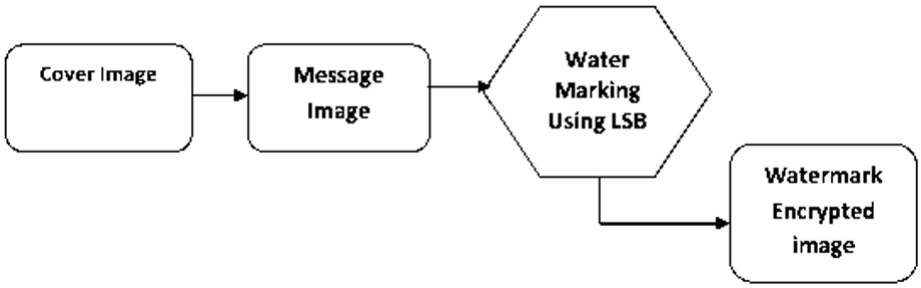


Figure 2.3: LSB Watermarking

2.6 Block Diagram

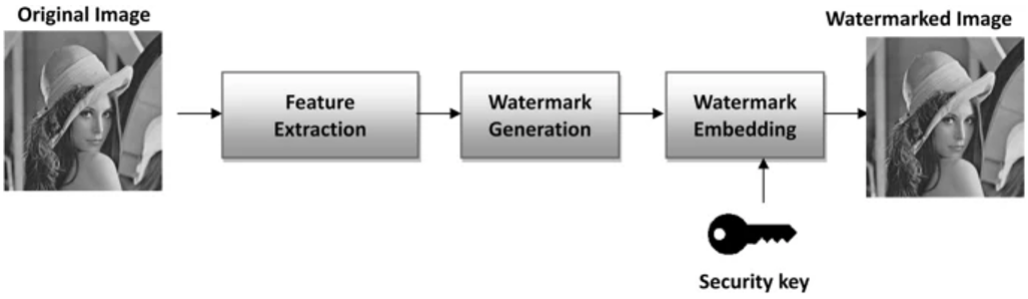


Figure 2.4: Block Diagram Of The Proposed Model

2.7 Flow Chart

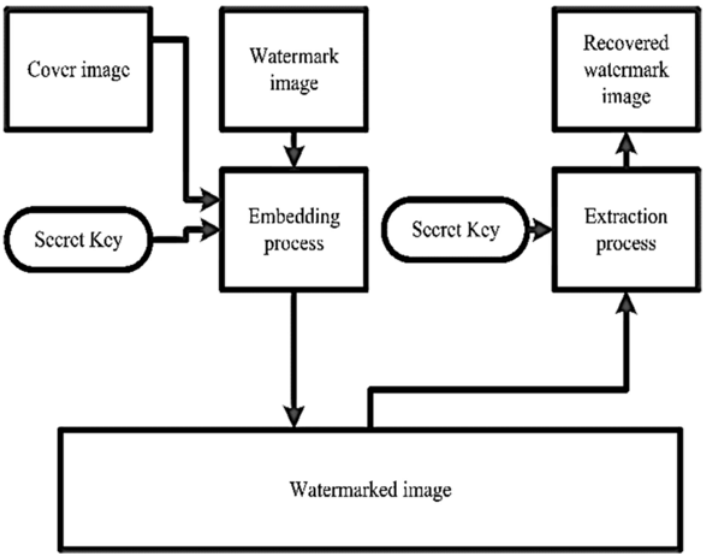


Figure 2.5: Flow Chart Of The Proposed Model

2.8 Code

```
clc % Clear the command window
close all; % Close all figures (except those of imtool.)
imtool close all; % Close all of imtool figure
clear; % Erase all existing variable
workspace; % Make sure the workspace panel is showing
fontSize = 12;
%C:\Program Files\MATLAB\R2018a\toolbox\images\imdata
% Read in the image what will have another image hidden
    into it
baseFileName='pout.tif';
%baseFileName='Cameraman.tif';
folder=fullfile(matlabroot,'\toolbox\images\imdemos');
% Get the full fileName, with path prepended
fullFileName=fullfile(folder,baseFileName);
if ~exist(fullFileName,'file')
```

```
% Didn't find it there. check the search path for it
fullFileName=baseFileName;
if ~exist(fullFileName,'file')
% Still didn't find it. Alert user
errorMessage=sprintf('Error: does not exist', fullFileName)
    ;
uiwait(warndlg(errorMessage));
return;
end
end
originalImage=imread(fullFileName);

%Get the number of row and column in the original image
[visibleRows,visibleColumns,numberOfColorChannels]=size(
    originalImage);
if numberOfColorChannels > 1
% If it's color, extract the image
originalImage=originalImage(:,:,1);
end

% Display the original gray scale image
subplot(3,2,3)
imshow(originalImage,[]);
title('Original Grayscale Starting Image','FontSize',
    fontSize);
% Enlarge figure to full screen
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
set(gcf,'name','Demo by ImageAnalyst','numbertitle','off')

% Read the image message you want to hide in the cover
    image
baseFileName='cameraman.tif';
```

```
43 %%baseFileName='moon.tif';
44 % Get the full FileName with path pepended.
45 fullFileName=fullfile(folder,baseFileName);
46 if ~exist(fullFileName,'file')
47 % Didn't find it there. check the search path for it
48 fullFileName=baseFileName;
49 if ~exist(fullFileName,'file')
50 % Still didn't fint it. Alert the user
51 errorMessage=sprintf('Error: does not exist', fullFileName)
      ;
52 uiwait(warndlg(errorMessage));
53 return;
54 end
55 end
56 hiddenImage=imread(fullFileName);
57 %Get the number of row and column in the original image
58
59 [hiddenRows,hiddenColumns,numberOfColorChannels]=size(
      hiddenImage);
60 if numberOfColorChannels > 1
61 % If it's color, extract the red channel
62 hiddenImage=hiddenImage(:,:,1);
63 end
64 %Display the image that we want to hide
65 subplot(3,2,1);
66 imshow(hiddenImage,[]);
67 title('Image to be Hidden','FontSize',fontSize)
68 % the threshold is simply to generate a binary image to be
      hidden.
69 thresholdValue = 70;
70 binaryImage = hiddenImage < thresholdValue; % Now we have a
       binary image.
```

```
71 % Display the binary image.
72 subplot(3, 2, 2);
73 imshow(binaryImage, []);
74 caption = sprintf('Hidden Image Threshold at %d',
       thresholdValue);
75 title(caption, 'FontSize',fontSize);
76
77 % Get the bit plane to hide the binary image in.
78 % Since it's binary it can be storen in a single bit plane.
79 prompt = 'Enter the bit plane you want to hide the image in
       (1 - 8) ';
80 dialogTitle = 'Enter bit plane to replace';
81 numberOfLines = 1;
82 defaultResponse = {'6'};
83 bitToSet = str2double(cell2mat(inputdlg(prompt, dialogTitle
       , numberOfLines,defaultResponse)));
84 % If image to be hidden is bigger than the orignal image,
       scale it down.
85 if hiddenRows > visibleRows || hiddenColumns >
       visibleColumns
86     amountToShrink = min([visibleRows / hiddenRows,
           visibleColumns / hiddenColumns]);
87     binaryImage = imresize(binaryImage, amountToShrink);
88     % Need to update the number of rows and columns.
89     [hiddenRows, hiddenColumns] = size(binaryImage);
90 end
91
92 % Title the hiddenimage,if it's smaller, so that it will
       cover the orignal image.
93
94 if hiddenRows < visibleRows || hiddenColumns <
       visibleColumns
```

```
95      watermark = zeros(size(originalImage), 'uint8');
96      for column = 1:visibleColumns
97          for row = 1:visibleRows
98              watermark(row, column) = binaryImage(mod(row,
                    hiddenRows)+1, mod(column,hiddenColumns)+1);
99          end
100     end
101     % Crop it to the same size as the orignal image.
102     watermark = watermark(1:visibleRows, 1:visibleColumns);
103 else
104     % Watermark is the same size as the orignal image.
105     watermark = binaryImage;
106 end
107 % Display the threshold binaryImage - the watermark alone.
108 subplot(3, 2, 4);
109 imshow(watermark, []);
110 caption = sprintf('Hidden Image\nto be inserted into Bit
      Plane %d', bitToSet);
111 title(caption, 'FontSize', fontSize);
112
113 % Set the bit of orignalImage(a copy, actual) to the value
      of watermark.
114 watermarkedImage = originalImage; %Initialize
115 for column = 1 : visibleColumns
116     for row = 1 : visibleRows
117         watermarkedImage(row, column) = bitset(
              originalImage(row, column), bitToSet, watermark(
              row, column));
118     end
119 end
120 % Display the final watermarked image.
121 subplot(3, 2, [5,6]);
```

```
122 imshow(watermarkedImage, []);
123 caption = sprintf('Final Watermarked Image');
124 title(caption, 'FontSize', fontSize);
```

2.9 Output

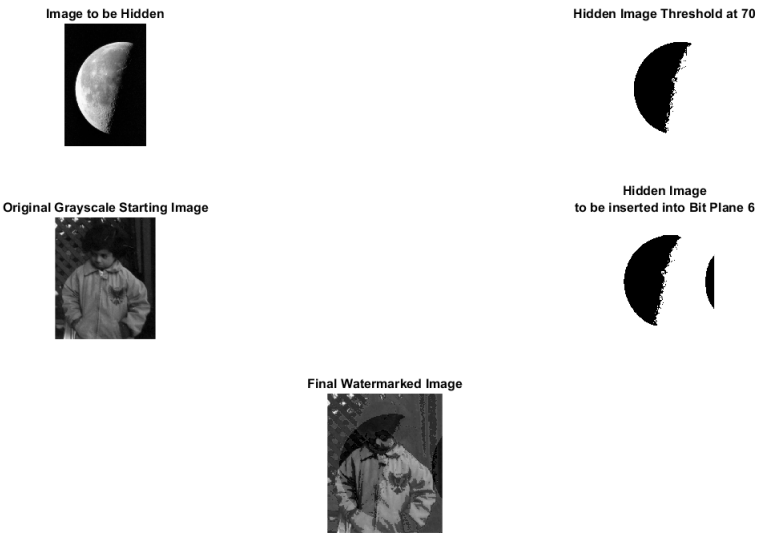


Figure 2.6: Output Of Test Run 1

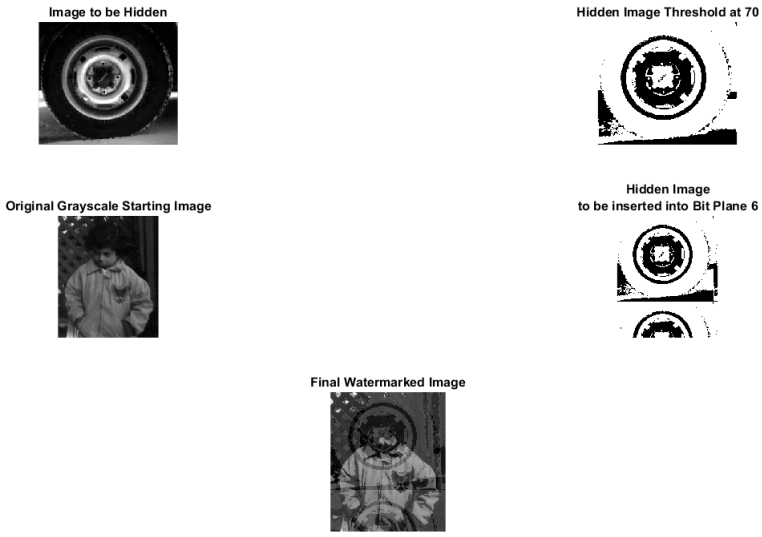


Figure 2.7: Output Of Test Run 2

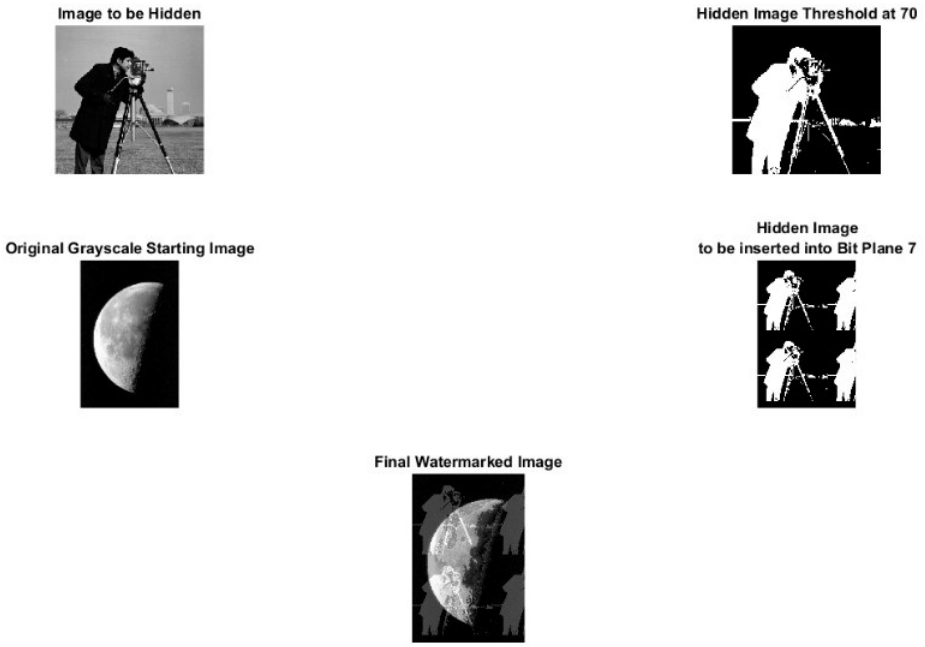


Figure 2.8: Output Of Test Run 3

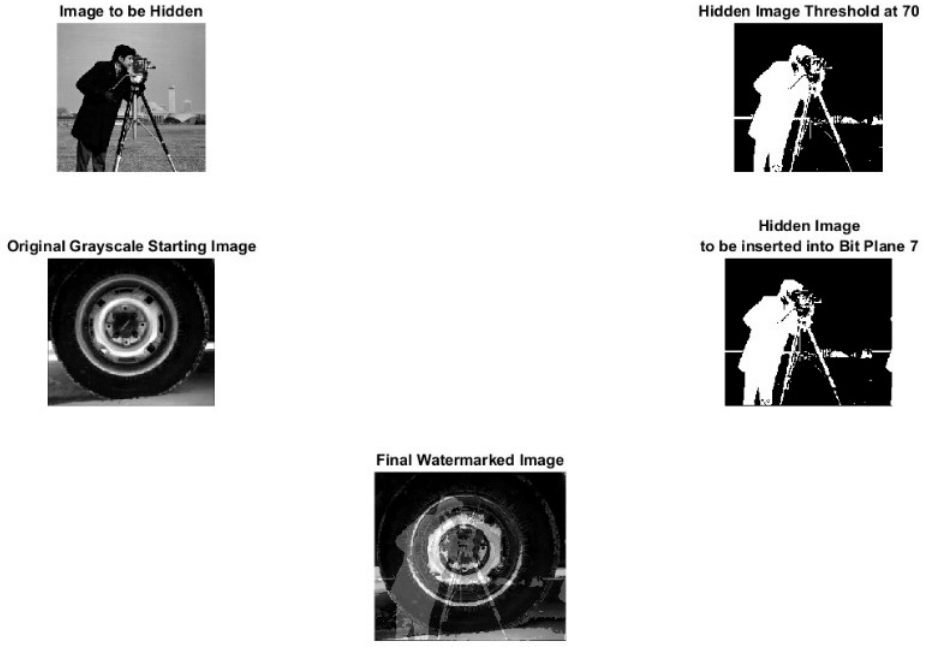


Figure 2.9: Output Of Test Run 4

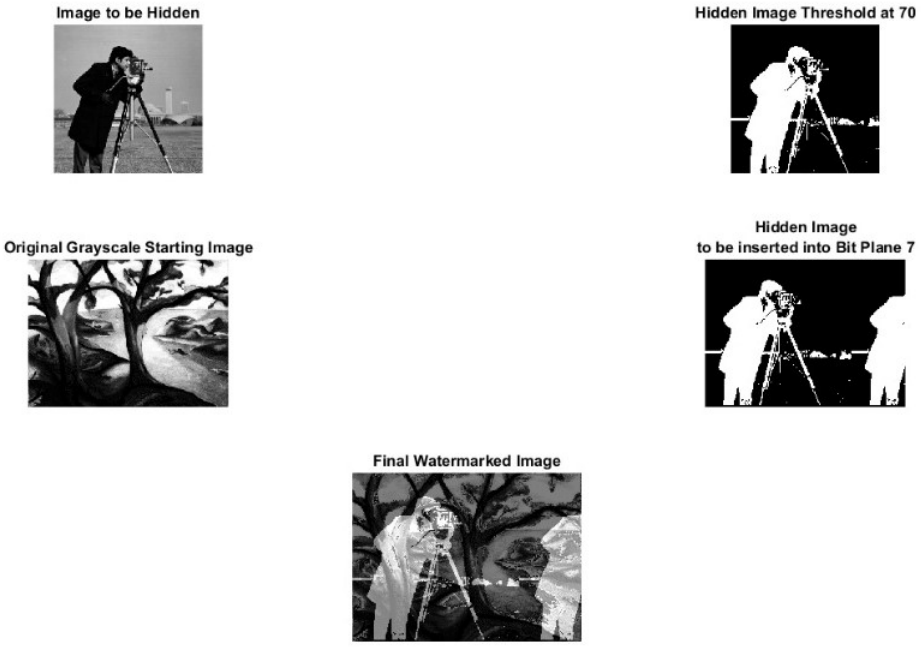


Figure 2.10: Output Of Test Run 5

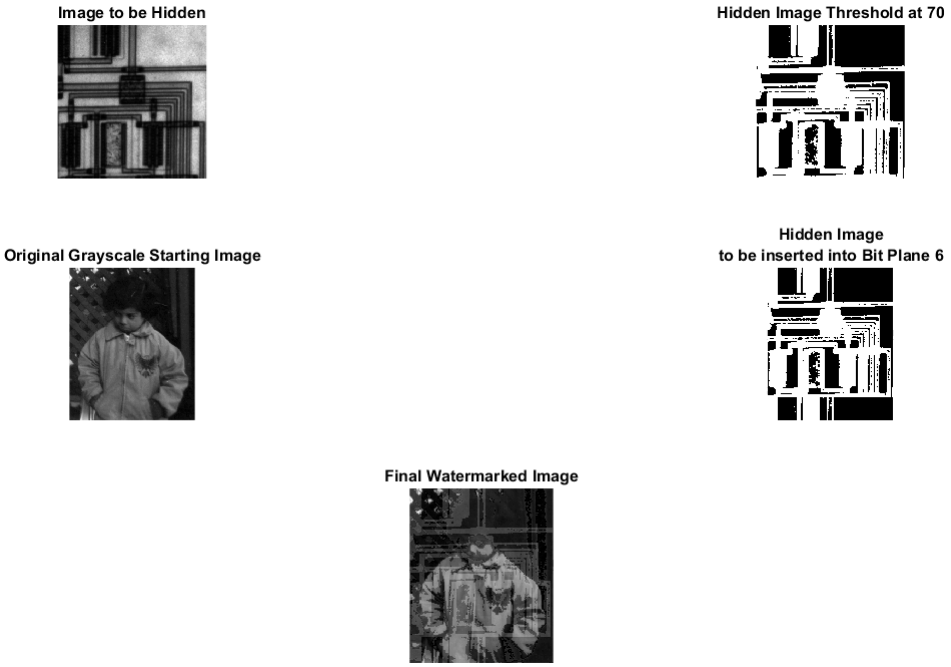


Figure 2.11: Output Of Test Run 6

Chapter 3

CONCLUSION

3.1 Objectives

To watermark an image by hiding another image in a certain bit plane called ”LSB Watermarking”. A watermark is a visible embedded overlay on a digital photo consisting of text, a logo, or a copyright notice. The purpose of a watermark is to identify the work and discourage its unauthorized use.

3.2 Results And Discussion

In Chapter 2 section output Fig.[2.6,2.7,2.8,2.9,2.10,2.11] represent that there will be two images provided as input one the image to use as water mark and second the image to be water marked. As the algorithm run well get our result image in the end and title Water Marked image.

3.3 Limitations Of System

The image provided water marking image should be with following properties

- Resolution 512x512
- Gray-scale
- Format: Name.tif

The Image to be water marked can of any size preferable size less than 3mb and it should be .tif format as well.

3.4 Conclusion

Finally, we can conclude that Watermarking using LSB is the easy to understand and best method for encryption of data. In open networks, to securely transmit data Encryption and Decryption is used. To protect confidential image data from unauthorized access as each type of data has its own features, different techniques should be used. Watermarking is one of them. We can secure our data by watermarking an image to the cover image by the procedure explained above called LSB watermarking. Since the image consisting of pixels can be represented as binary value whose MSB contains all the information and LSB contains least data so changing the least significant bit does not affect the overall image. In LSB watermarking LSB is changed and as a result we get a watermarked image. Watermarking procedure can be used to secure date in various fields.

Bibliography

[1] https://www.mdpi.com/2078-2489/11/2/110/htm: :text=Digital%20image%20watermarking%20is%20a,of%20the%20image%20%5B1%5D..

[2] https://asp-eurasipjournals.springeropen.com/articles/10.1186/1687-6180-2014-135

[3] https://encyclopedia.pub/entry/680

[4] https://www.geeksforgeeks.org/digital-watermarking-and-its-types/

[5] https://www.sciencedirect.com/topics/engineering/digital-watermarking

[6] https://www.youtube.com/watch?v=WvRBKn8-JJA

[7] https://www.sciencedirect.com/topics/engineering/image-watermarking

[8] https://www.youtube.com/watch?v=BQb01Mmuqrk

[9] http://www.computerscijournal.org/vol9no1/digital-image-watermarking-an-overview/

[10] https://link.springer.com/chapter/10.1007/978-3-319-57699-2_1