INDEX

Chapter I

INTRODUCTION

The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Applications include electronic advertising, real time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is the protection of the rights of all participants. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest towards developing new copy deterrence and protection mechanisms. One such effort that has been attracting increasing interest is based on digital watermarking techniques. Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content. The recent growth of networked multimedia system has increased the need for the protection of digital media. This is particularly important for the protection and enforcement of intellectual property rights. Digital media includes text, digital audio, images, video and software. Many approaches are available for protecting digital data; these include encryption, authentication and time stamping. One way to improve one's claim of ownership over an image, for instance, is to place a low- level signal directly into the image data. This signal, known as a digital watermark, uniquely identifies the owner and can be easily extracted from the image.

1.1 Digital Watermarking

Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible. A digital watermark is a message which is embedded into digital content (video, images or text) that can be detected or extracted later. Moreover, in image the actual bits

representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. Watermarking is the insertion of imperceptible and inseparable information into the host data for data security & integrity.

With the increasing use of the internet, copyright protection for the multimedia data has turned into a vital issue. For reliable communication the security of the data is the prime concern. Traditionally the cryptographic techniques were used for providing the security to the information but this theory has its own limitation. So to resolve the problem of the traditional technique the analyst has been focusing on the study of the digital watermarking technology. It increases the security of the data and protects the information from unauthorized access. Watermark information can be patent information, authentication information in order to determine the copyright owner of the digital works, it also certify the reliability and probity of the multimedia works .

A digital watermark is insertion of an impalpable signal into information, like sound, video and pictures, for an assortment of purposes, including inscribing and copyright control. It is basically used for the identification of the ownership of the copyright of an image. Digital watermarking is a code that is embedded in the image .it is very similar to the steganography as in both the information is embedded inside the cover message with less or no degradation of the cover - object. In steganographic systems the large amount of data is embedded which results in the secure data transmission without the degradation of the cover objects and in the watermarking systems the large amount of the data is embed that can't be extracted or diversified without making the cover object entirely unusable .Many image watermarking techniques are used for process of watermarking techniques like DCT, DWT, LSB etc.

1.1.1 Digital watermarking Definition

A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked.

Digital watermarking techniques derive from steganography, which means covered writing (from the Greek words stegano or "covered" and graphos or "to write"). Steganography is the science of communicating information while hiding the existence of the communication. The goal of steganography is to hide an information message inside harmless messages in such a way that it is not possible even to detect that there is a secret message present. Both steganography and watermarking belong to a category of information hiding, but the objectives and conditions for the two techniques are just the opposite. In watermarking, for example, the important information is the "external" data (e.g., images, voices, etc.). The "internal" data (e.g., watermark) are additional data for protecting the external data and to prove ownership. In steganography, however, the external data (referred to as a vessel, container, or dummy data) are not very important. They are just a carrier of the important information. The internal data are the most important. On the other hand, watermarking is not like encryption. Watermarking does not restrict access to the data while encryption has the aim of making messages unintelligible to any unauthorized persons who might intercept them. Once encrypted data is decrypted, the media is no longer protected. A watermark is designed to permanently reside in the host data. If the ownership of a digital work is in question, the information can be extracted to completely characterize the owner.

1.1.2 History of Digital Watermarking

The idea of hiding data in another media is very old, as described in the case of steganography. Nevertheless, the term digital watermarking first appeared in 1993, when Tirkel et al. (1993) presented two techniques to hide data in images. These methods were based on modifications to the least significant bit (LSB) of the pixel values.

1.2 Effective Watermarking

It is desired that watermarks survive image-processing manipulations such as rotation, scaling, image compression and image enhancement, for example. Taking advantage of the discrete wavelet transform properties and robust features extraction techniques are the new trends that are used in the recent digital image watermarking methods. Robustness against geometrical transformation is essential since image-publishing applications often apply some kind of geometrical transformations to the

image, and thus, an intellectual property ownership protection system should not be affected by these changes.

1.2.1 Visible vs. Invisible Watermarks

Digital watermarking is divided into two main categories: visible and invisible. The idea behind the visible watermark is very simple. It is equivalent to stamping a watermark on paper, and for this reason its sometimes said to be digitally stamped. An example of visible watermarking is provided by television channels, like BBC, whose logo is visibly superimposed on the corner of the TV picture. Invisible watermarking, on the other hand, is a far more complex concept. It is most often used to identify copyright data, like author, distributor, and so forth.

Though a lot of research has been done in the area of invisible watermarks, much less has been done for visible watermarks. Visible and invisible watermarks both serve to deter theft but they do so in very different ways. Visible watermarks are especially useful for conveying an immediate claim of ownership (Mintzer, Braudaway & Yeung, 1997). Their main advantage, in principle at least, is the virtual elimination of the commercial value of a document to a would-be thief, without lessening the document's utility for legitimate, authorized purposes. Invisible watermarks, on the other hand, are more of an aid in catching a thief than for discouraging theft in the first place (Mintzer et al., 1997; Swanson et al., 1998).

1.2.2 Watermarking Classification

There are different classifications of invisible watermarking algorithms. The reason behind this is the enormous diversity of watermarking schemes. Watermarking approaches can be distinguished in terms of watermarking host signal (still images, video signal, audio signal, integrated circuit design), and the availability of original signal during extraction (non-blind, semi-blind, blind). Also, they can be categorized based on the domain used for watermarking embedding process, as shown in Figure 1. The watermarking application is considered one of the criteria for watermarking classification. Figure 2 shows the subcategories based on watermarking applications.

1.2.3 Digital Watermarking Algorithms

Current watermarking techniques described in the literature can be grouped into three main classes. The first includes the transform domain methods, which embed the data by modulating the transform domain signal coefficients. The second class includes the spatial domain techniques. These embed the watermark by directly

modifying the pixel values of the original image. The transform domain techniques have been found to have the greater robustness, when the watermarked signals are tested after having been subjected to common signal distortions. The third class is the feature domain technique. This technique takes into account region, boundary and object characteristics. Such watermarking methods may present additional advantages in terms of detection and recovery from geometric attacks, compared to previous approaches.

- Spatial domain techniques
- Transform domain techniques
- Feature domain techniques

Spatial Domain Techniques

This section gives a brief introduction to the spatial domain technique to gives some background information about watermarking in this domain. Many spatial techniques are based on adding fixed amplitude pseudo noise (PN) sequences to an image. PN sequences are used as the "spreading key" when considering the host media as the noise in a spread spectrum system, where the watermark is the transmitted message. In this case, the PN sequence is used to spread the data bits over the spectrum to hide the data.

Transform Domain Techniques

Many transform-based watermarking techniques have been proposed. To embed a watermark, a transformation is first applied to the host data, and then modifications are made to the transform coefficients. In this section, the state of the art of the current watermarking algorithms using the transform domain is presented. The section has three main parts, including discussions of waveletbased watermarking, DCT-based watermarking and fractal domain watermarking.

Digital Watermarking Using Wavelet Decomposition

This algorithm can easily be built into video watermarking applications based on a 3-D wavelet transform due to its simple structure. The hierarchical nature of the wavelet representation allows multi-resolutional detection of the digital watermark, which is a Gaussian distributed random vector added to all the high pass bands in the wavelet domain.

1.2.4 Digital Watermarking and Watermarking Attacks

Digital watermarking was claimed to be the ultimate solution for copyright protection over the Internet when the concept of digital watermarking was first presented. However, some problems related to robustness and security of watermarking algorithms to intentional or unintentional attacks still remain unsolved. These problems must be solved before digital watermarking can be claimed to be the ultimate solution for copyright ownership protection in digital media. One of these problems is the effect of geometrical transformations such as rotation, translation and scaling on the recovery of the watermark. Another is the security of the watermarking algorithm when intentional attackers make use of knowledge of the watermarking algorithm to destroy or remove the watermark.

1.2.5 Watermarking Standardization Issue

The most important question about watermarking technology is whether watermarking will be standardized and used in the near future. There are several movements to standardize watermarking technology, but no one standard has prevailed at this moment in time. Some researchers have been working to develop a standardized framework for protecting digital images and other multimedia content through technology built into media files and corresponding application software. However, they have lacked a clear vision of what the framework should be or how it would be used.

In addition, there was a discussion about how and whether watermarking should form part of the standard during the standardization process of JPEG2000. The requirements regarding security have been identified in the framework of JPEG2000. However, there has been neither in-depth clarification nor a harmonized effort to address watermarking issues. It is important to deduce what really needs to be standardized for including the watermarking concept in JPEG2000 and to what extent. The initial drafts of the JPEG2000 standard did not mention the issue of watermarking. However, there is a plan to examine how watermarking might be best applied within JPEG2000. The features of a given watermarking scheme are likely to offer designers an opportunity to integrate watermarking technology into JPEG2000 for different application such as distributing images on the Internet. Also, standardization of digital watermarking will influence the progress in imaging standards of JPEG2000 where the data security will be part of this standard.

Therefore, the likelihood is that watermarking technology will be used in conjunction with JPEG2000 (Clark, 2000).

1.2.6 Future Highlights

Nevertheless, the future seems bright for digital watermarking. Many companies have already been active in digital watermarking research. For example, Microsoft has developed a prototype system that limits unauthorized playback of music by embedding a watermark that remains permanently attached to audio files. Such technology could be included as a default playback mechanism in future versions of the Windows operating system. If the music industry begins to include watermarks in its song files, Windows would refuse to play copyrighted music released after a certain date that was obtained illegally. Also, Microsoft Research has also invented a separate watermarking system that relies on graph theory to hide watermarks in software. Normally the security technology is hack able. However, if the technology is combined with proper legal enforcement, industry standards and respects of the privacy of individuals seeking to legitimately use intellectual property, digital watermarking will encourage content creators to trust the Internet more. There is a tremendous amount of money at stake for many firms. The value of illegal copies of multimedia content distributed over the Internet could reach billions of dollars a year. It will be interesting to see how the development and adoption of digital watermarking plays out. With such high stakes involved for entertainment and other multimedia companies, they are likely to keep pushing for (and be willing to pay for) a secure technology that they can use to track and reduce copyright violation and capture some of their foregone revenues. Finally, it is expected that a great deal of effort must still be put into research before digital image watermarking can be widely accepted as legal evidence of ownership.

1.3 Purpose of the study

The purpose of this project is to make software through which we can perform basic image operations on the desired images and also can encrypt messages or hide the messages for the purpose of security. Through steganography we are encrypting the messages whereas cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the

contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Thus image steganography is a better approach than cryptography. Purpose of watermarking is to make the quality of an image better so that the required operations can be easily performed on it. Image steganography is performed on the desired formats which are suitable. One can use this software for performing simple image operations on the images and encrypt the desired message which is to be sent to another person by preventing its security. This software performs image operations with message encryption.

1.4 Objective

Digital watermarking hides, in digital images, the information necessary for ownership identity to offer copyright Protection and authentication. Robustness, even if recognized as a key property of the digital watermarking, is not considered enough to prove the ownership of the image. The aim of inversion attacks is to create ambiguities about the authorship of an image. To thwart inversion attacks with otherwise robust watermarking schemes, non-invertibility of watermarking has often been stressed. Digital watermarking is applied to protect the copyright of the digital media which unlike the analog media can be stored, duplicated, and distributed without loss of fidelity. Unauthorized copy of digital documents has been a subject of concern for many years especially with respect to their authorship claims. Digital watermarking, by hiding certain information in the original data provides a solution digital watermarking technology can effectively compensate for the deficiencies of the security and protection application of traditional information security technology. Digital watermarking prevents illegal duplicating, interpolating and distributing the digital content technically.

Chapter II

Literature Review

[1] In First survey learn to Comparison of Digital Watermarking with Other Techniques of Data Hiding", , the author name is, K.Sridhar, Dr. Syed Abdul Sattar , Dr. M Chandra Mohan International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (1) , 2014, 350-353 describe the four algorithms appear under the following headings in his thesis: developed a novel semi-fragile watermarking technique to embed the proposed robust digital signatures. They have implemented a unique Self- Authentication-and-Recovery Images (SARI) system, which can accept quantization-based lossy compression to a determined degree without any false alarms and can sensitively detect and locate malicious manipulations [13]. Chun-Shien Lu et al. [2001] they propose a novel multipurpose watermarking scheme, in which robust and fragile watermarks are simultaneously embedded, for copyright protection and content authentication. By quantizing a host image's wavelet coefficients as masking threshold units (MTUs), two complementary watermarks are embedded using cocktail watermarking and they can be blindly extracted without access to the host image. For the purpose of image protection, the new scheme guarantees that, no matter what kind of attack is encountered, at least one watermark can survive well. On the other hand, for the purpose of image authentication, our approach can locate the part of the image that has been tampered with and tolerate some incidental processes that have been executed [14].

[2] In second survey learn the paper title is "Performance Comparison of Digital Image Watermarking Techniques, the author name is Namita Chandrakar, Jaspal Bagga A Survey", International Journal of Computer Applications Technology and Research Volume 2- Issue 2, 126 - 130, 2013 in this paper, they present an overview and summary of recent developments on this important topic, and discuss important issues such as robustness and data hiding capacity of the different techniques [15]. P.Tay et al. [2002], in this paper they propose a novel image watermarking scheme. This technique uses a 2-D discrete wavelet transform to decompose an image into various frequency channels. A scaled image is used as watermark and inserted into a mid- frequency wavelet channel.

The watermark embedded image is produced by taking the inverse 2- D discrete wavelet transform of the altered wavelet decomposition. The image size, the non-zero scaling factor, the channel in which the watermark is inserted, and the wavelet transform filters can be used as security keys for the extraction of the inserted watermark. The propose watermark extraction technique is independent of the original image [16].

[3] Prabhishek Singh [2017], in this paper they introduce two spatial methods in order to embed watermark data into fingerprint images, without corrupting their features. The first method inserts watermark data after feature extraction, thus preventing watermarking of regions used for fingerprint classification. The method utilizes an image adaptive strength adjustment technique which results in watermarks with low visibility. The second method introduces a feature adaptive watermarking technique for fingerprints, thus applicable before feature extraction. For both of the methods, decoding does not require original fingerprint image. most of the published spatial watermarking method the proposed methods provide high de accuracy for fingerprint images. High data hiding decoding performance for color images is also observed [17].

[4] J.J.K. O Ruanaidh et al. [2016] discuss the watermarking digital images for copyright protection. They have demonstatrated a solution to one of the key problems in image watermarking, namely how to hide robust invisible labels inside grey scale or colour digital images. An invisible mark embedded in a digital image which may be used for Copyright protection. The embedded marks are designed to be unaffected by any combination of rotation, scale and translation transformations. The original image is not required The thesis concludes with a discussion of the advantages and disadvantages of the techniques proposed and the future directions of research.

[5] Juan R. Hernandez et al. [2019] addresses the problem of the performance analysis of image watermarking systems that do not require the availability of the original image during ownership verification. They focus on a statistical approach to obtain models that can serve as a basis for the application of the decision theory to the design of efficient detector structures. Special attention is paid to the possible nonexistence of a statistical description of the original image.

[6] Ingemar J. Cox et al. [2012] describe a number of applications of digital watermarking and they examine the common properties of robustness, tamper resistance, fidelity, computational cost and false positive rate. They observe that these properties vary greatly depending on the application. Consequently, they conclude that evaluation of a watermarking algorithm is difficult without first indicating the context in which it is to be applied.

[7] Jian Zhao et al. such types of content authentication. Also, they have [1998] describe digital watermark for copyright developed a novel semi-fragile watermarking [1998] describe digital watermark for protection, digital watermark for hidden annotation, digital watermark for proving authenticity, steganographic communication, functions and technical requirements [7].

[8] M. Barni et al. [1998] derived a new watermarking algorithm for digital images is presented the method, which operates in the frequency domain, embeds a pseudo-random sequence of real numbers in a selected set of DCT coefficients. After embedding, the watermark is adapted to the image by exploiting the masking characteristics of the human visual system, thus ensuring the watermark invisibility [8].

[9] Nasir Memon et al. [1998] describe protecting digital media content and Watermark insertion integrates the input image and a watermark to form the output watermarked image. Watermark extraction uncovers the watermark in watermarked images, a technique usually applicable in verification watermarks [9].

[10] A.Z.Tirkel et al. [2015] discuss the feasibility of coding a robust, undetectable, digital watermark on a standard 512*512 intensity image with an 8 bit gray scale image. The watermark is capable of carrying such information as authentication or authorisation codes, or a legend essential for image interpretation derives copyright protection is a very important subject but not the only one in which watermarking appears as one of the very promising solutions. In this communication, they have attempted to go back to the early beginning of this exciting new research field, make an overview of its history, discuss the applications and stakes involved, classify the proposed methods, present the problems and benchmarking tools and finally, try to peak into the future [18]. Saraju P. Mohanty et al. [2003], in this paper, they develop hardware system

that can insert both robust and fragile invisible watermarks in images. The hardware module can be easily incorporated into a JPEG encoder to develop a secure JPEG encoder. A prototype chip is implemented using 0.35p CMOS technology. According to them, this is the first watermarking chip implementing both invisible-robust and invisible-fragile watermarking capabilities [19]. Chang-Chou Lin et al. [2004], they

[11] work a novel approach to secret image sharing based on a ok; nP-threshold scheme with the additional capabilities of steganography and authentication is an proposed [20].

[12] Vidyasagar M. Potdar et al. [2005] present a detailed survey of existing and newly proposed steganographic and watermarking techniques. The complementary role of watermarking with respect to medical information security and management. The issues related to image watermarking benchmarking and scenarios based on digital rights management requirements. A new robust digital image watermarking algorithm based on Joint DWT-DCT Transformation is proposed. Two modified image adaptive watermarking techniques based on multi-scale morphological segmentation are presented by to present a survey on different types of digital watermarks and methods to do image watermarking.

[13] The main reason for development of digital watermarking research is the endeavor for coming up ith innovations to protect intellectual properties of e digital world. This is because the recent technological advancement in generation, storage, and communication of digital content has created/generated problems like copying the digital contents without any constraints, forgery, and editing without any prohibitive professional efforts. The absence of protecting techniques makes it doubtful to use the digital communication system in medical, business, and military applications. Watermarking is one of the most common solutions to make the data transferring

[14] secure from the illegal interference.

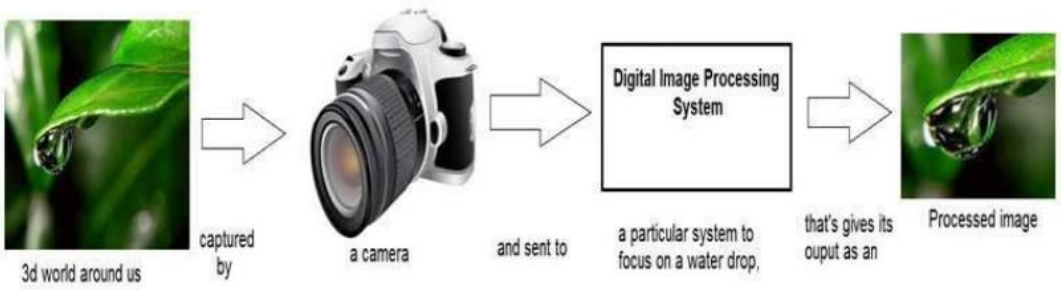
Chapter III

METHODOLOGY

3.1 Proposed Work

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark .For visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. Fig 1.1. Watermark and image The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals.

Digital Watermarking (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.



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

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

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

Relationship Between A Signal And Image

Signal

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.

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.

How A Digital Image Is Formed

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 an two dimensional array or matrix of numbers which are nothing but a digital image.

Why Digital Watermarking Required

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.

3.2 General 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)
- The decoder and comparator (verification or extraction or detection 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.

3.2.1 Encoding Process:

The figure illustrates the encoding process.

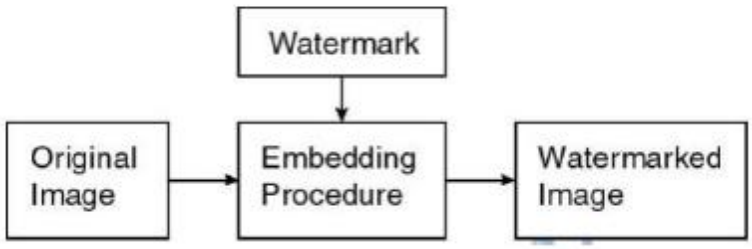


Fig. 3.1 Block diagram of the system

Let us denote an image by I, a signature by S = { si, s2, ... } 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'.

3.2.2 Decoding Process

A decoder function D takes an image J (J can be a watermarked or unwatermarked image, and possibly corrupted) whose ownership is to be determined and recovers a signature S' from the image. In this process, an additional image I can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels. Mathematically,

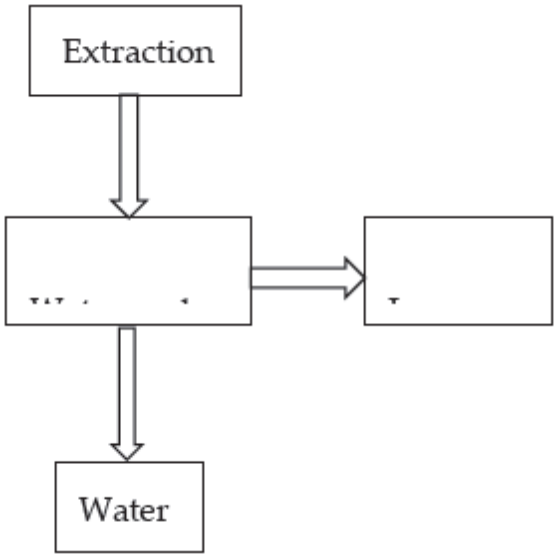


Figure 2.2Decoding Process

Depending on the way the watermark is inserted and depending on the nature of the watermarking algorithm, the method used can involve very distinct approaches.

In some watermarking schemes, a watermark can be extracted in its exact form, a procedure we call watermark extraction. In other cases, we can detect only whether a specific given watermarking signal is present in an image, a procedure we call watermark detection. It should be noted that watermark extraction can prove ownership whereas watermark detection can only verify ownership.

3.3 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 ater 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.

3.4 Methodology For 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 /2552 MSE and

MSE = 1 n Xn i=1 (Im(i) - Iw(i))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.

3.5 Types Of Digital Watermarks

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:

a) Image Watermarking

b) Video Watermarking

c) Audio Watermarking

d) Text Watermarking

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

a) Visible Watermark

b) Invisible Watermark

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.

Figure 3.4 Visible Watermarking

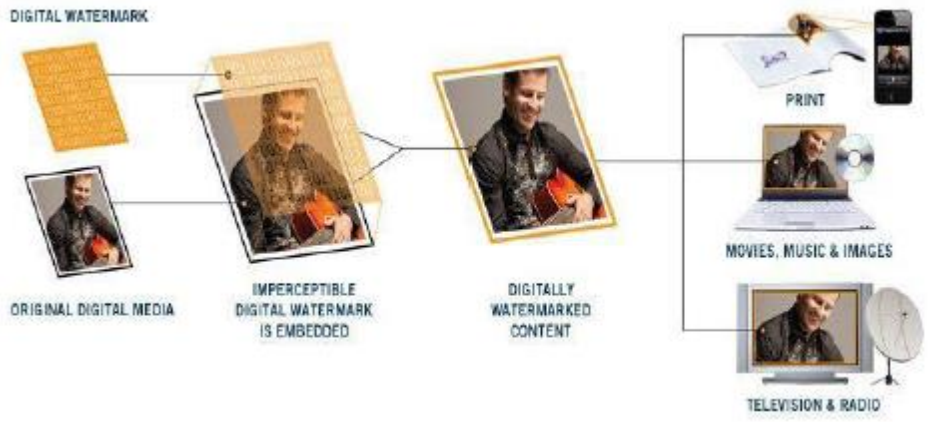


Figure 3.5 Invisible Watermarking

Application of digital watermarks visible watermark:

Visible watermarks can be used in following cases

- 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).
- 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.

Invisible robust watermarks:

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.

Invisible fragile watermarks:

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.

Attacks On Watermarks

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
- Resampling
- Requantization
- Dithering distortion
- Recompression
- 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

3.6 Desired Characteristics Of Watermarks

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.

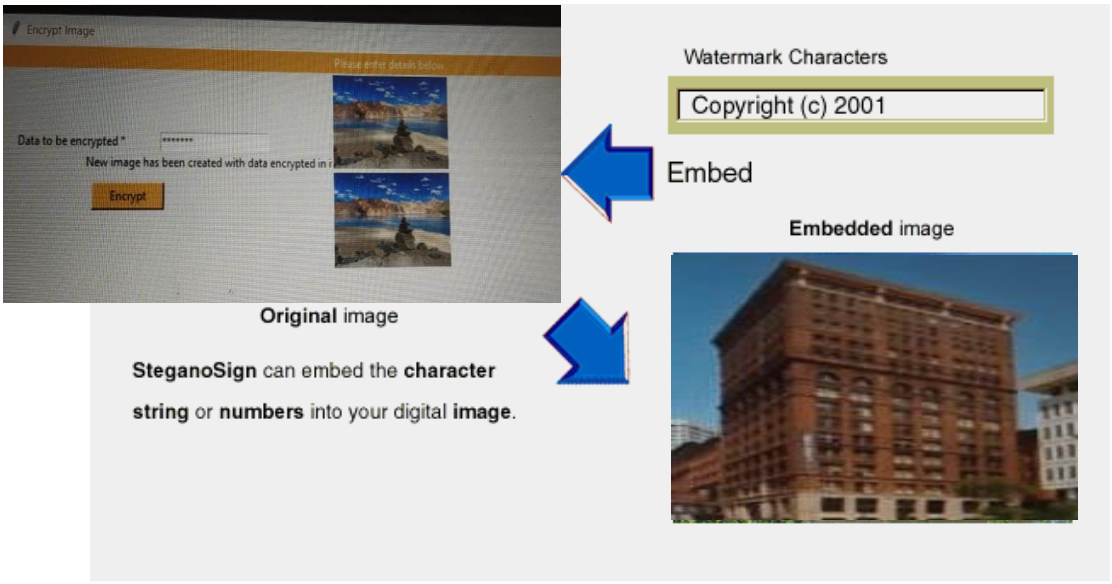
  It should also be noted that ability to embed robust watermarks in digital images does not necessarily imply the ability to establish ownership, unless certain requirements are imposed legally on the watermarking scheme.
- Tamper-resistance: As well as requiring the watermark to be robust to legitimate 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

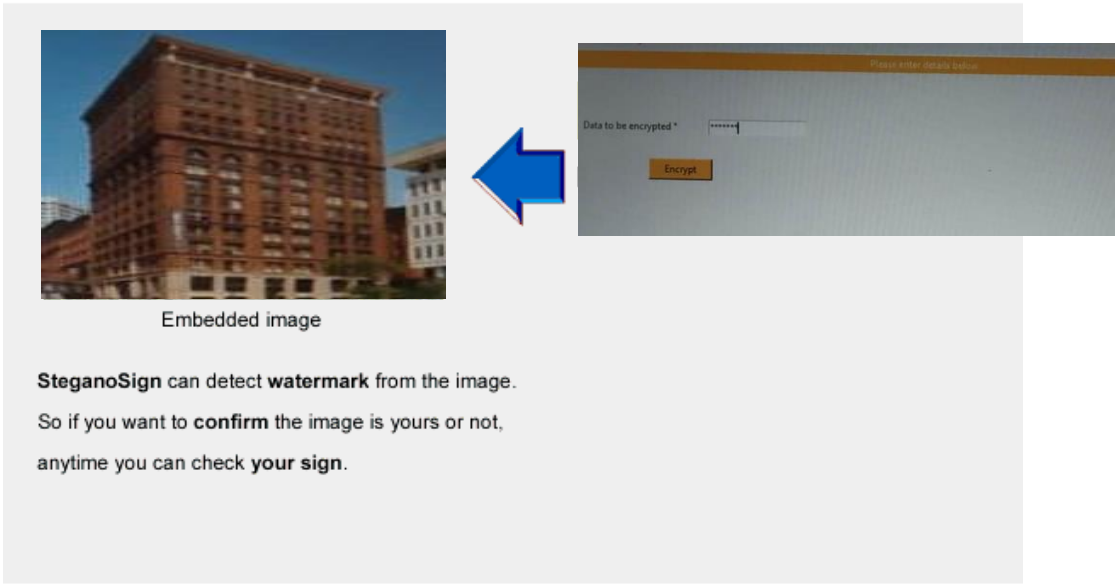
- Asymmetric encoder/decoder: If removal of a public watermark requires inverting the encoding, then it is highly desirable to make the encoder as complex as possible, especially if the watermark is only to be applied once. However if decoders must run in real time, then it is necessary for the decoding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

Chapter IV

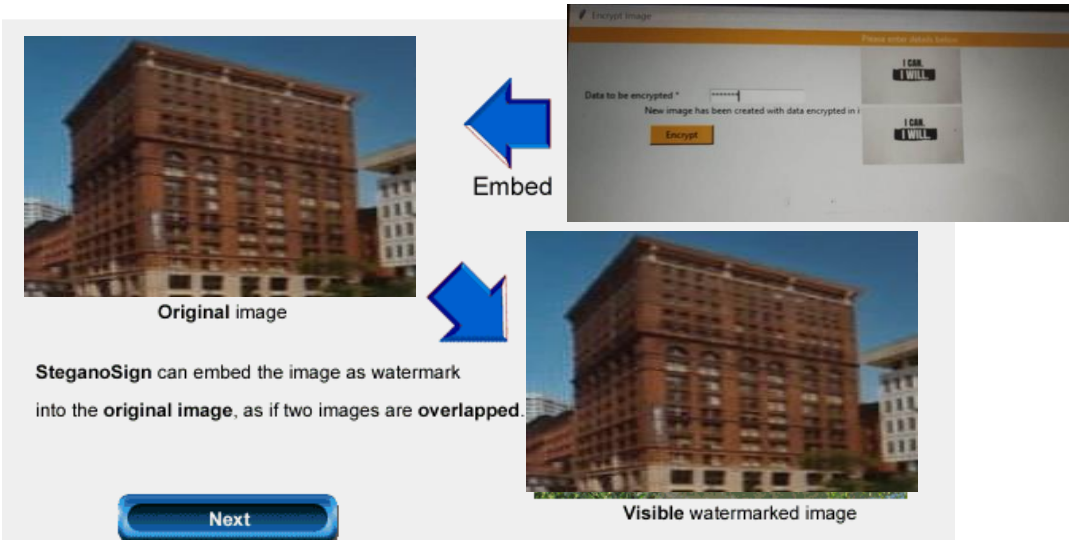
RESULTS ANALYSIS

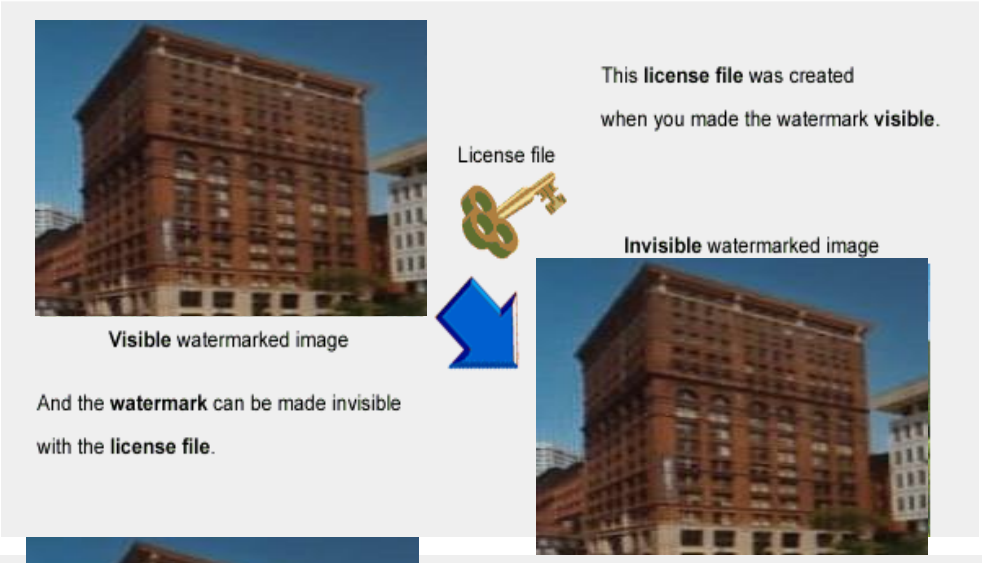
4.1 Invisible Watermarking Process

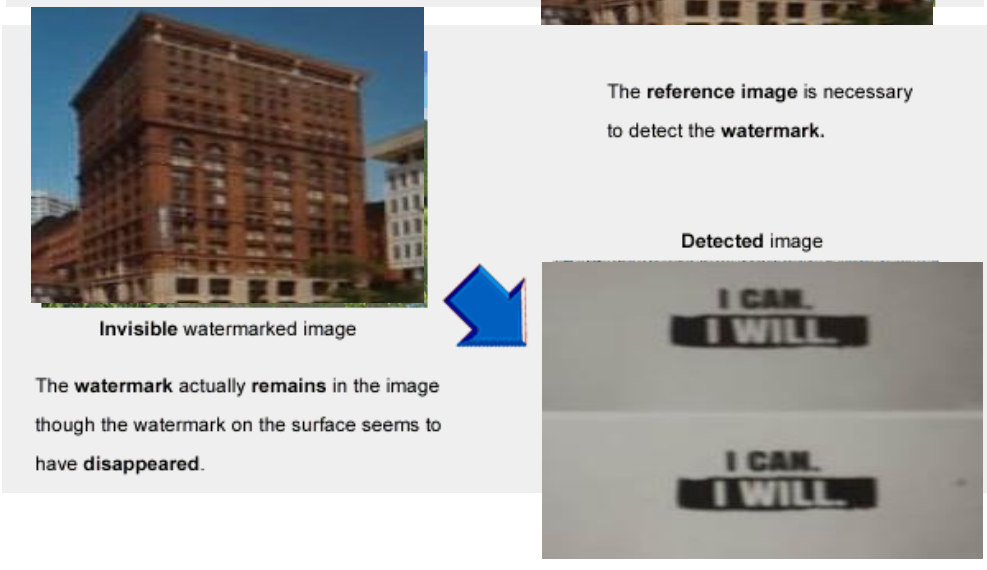




4.2 The Visible Watermarking Process







Chapter V

IMPLEMENTATION OF THE SYSTEM

In visible watermarking of images, a secondary image, the watermark, is embedded on a primary image such that the watermark is intentionally perceptible to a human observer whereas in the case of invisible, the embedded image data that is not perceptible, but may be extracted by a computer program.

Some of the desired characteristics of visible watermarks are listed below A visible watermark should be obvious in both color and monochrome images.

- The watermark should spread in a large and important area of the image in order to prevent its deletion by clipping.
- The watermark should be visible yet must not significantly obscure the image details beneath it.
- The watermark must be difficult to remove, rather removing a watermark should be more costly and labor intensive than purchasing the image from the owner.
- The watermark should be applied automatically with little human intervention and labor.

5.1 Proposed Watermarking Technique With OPENCV

The steps for watermark insertion using Transparent Overlay using opencv are described below.

• In order to construct a transparent overlay, two images are required:

1. Original image.

2. An image(watermark) containing what we want to "overlay" on top of the first using some level of alpha transparency.

- This watermark is a PNG image with four channels: a Red channel, a Green channel, a Blue channel, and an Alpha channel used to control the transparency of each of the pixels in the image.
- Values in our alpha channel can range [0, 255], where a value of 255 is 100% opaque (i.e., not transparent at all) while a value of 0 is 100% transparent.
- Once we actually overlay the watermark on our image, the watermark will be semi¬transparent, allowing us to (partially) see the background of the original image.

5.2 Creating A Watermark Using OPENCV

- Open up a new file, name it watermark_dataset.py
- Import required Python packages. We'll be making use of the packages like imutils,argparse,cv2,os,numpy.
- Parsing our required command line arguments we require three command line arguments and can supply two additional (optional) ones.
- --watermark : Here we supply the path to the image we wish to use as the watermark. We presume that (1) this image is a PNG image with alpha transparency and (2) our watermark is smaller (in terms of both width and height) then all images in the dataset we are going to apply the watermark to.
- --input : This is the path to our input directory of images we are going to watermark.
- --output : We then need to supply an output directory to store our watermarked images.
- --alpha : The optional --alpha value controls the level of transparency of the watermark. A value of 1.0 indicates that the watermark should be 100% opaque (i.e., not transparent). A value of 0.0 indicates that the watermark should be 100% transparent.
- --correct : Finally, this switch is used to control whether or not we should preserve a "bug" in how OpenCV handles alpha transparency.
- Now that we have parsed our command line arguments, we can load our watermark image from disk
- The cv2.imread function loads our watermark image from disk using the cv2.IMREAD_UNCHANGED flag — this value is supplied so we can read the alpha transparency channel of the PNG image (along with the standard Red, Green, and Blue channels).
- The spatial dimensions (i.e., height and width) of the watermark image is taken.
- To ensure that each of the Red, Green, and Blue channels respected the alpha channel, the bitwise AND is taken.
- Start looping over each of the images in our --input directory. For each of these images, we load it from disk and its width and height is taken.

- It's important to understand that each image is represented as a NumPy array with shape (h, w, 3), where the 3 is the number of channels in our image — one for each of the Red, Green, and Blue channels, respectively.
- However, since we are working with alpha transparency, we need to add a 4th dimension to the image to store the alpha values. This alpha channel has the same spatial dimensions as our original image and all values in the alpha channel are set to 255, indicating that the pixels are fully opaque and not transparent.
- Construct the overlay for our watermark. Again, the overlay has the exact same width and height of our input image.
- Finally, we construct our watermarked image by applying the cv2.addWeighted function.
- The output image are taken and written to the --output directory.

5.3 Implementation For Watermarking An Image:

```
# USAGE
#python watermark_dataset .py--watermark
pyimagesearch_watermark.png --input input --output output # import the necessary packages
from imutils import paths

import numpy as np
import argparse import cv2 import os
# construct the argument parse and parse the arguments ap = argparse.ArgumentParser()
ap.add_argument("-w", "--watermark”, required=True,
help=”path to watermark image (assumed to be transparent PNG)")
ap.add_argument("-i", "--input", required=True, help="path to the input directory of images")
ap.add_argument("-o", "--output", required=True, help="path to the output directory")
ap.add_argument("-a", "--alpha", type=float, default=0.25,
help="alpha transparency of the overlay (smaller is more transparent)")
ap.add_argument("-c", "--correct", type=int, default=1, help="flag used to handle if bug is displayed or not")
```

```
args = vars(ap.parse_args()) alpha=args["alpha"] beta= 1-args["alpha"] print("alpha"
+ str(alpha)) print("beta" + str(beta))
#       load the watermark image, making sure we retain the 4th channel
#       which contains the alpha transparency
watermark = cv2.imread(args["watermark"], cv2.IMREAD_UNCHANGED)


(wH, wW) = watermark.shape[:2]
#       split the watermark into its respective Blue, Green, Red, and
#       Alpha channels; then take the bitwise AND between all channels
#        and the Alpha channels to construct the actaul watermark
#        NOTE: I'm not sure why we have to do this, but if we don't,
#       pixels are marked as opaque when they shouldn't be if args["correct”] > 0:
(B, G, R, A) = cv2.split(watermark)
B = cv2.bitwise_and(B, B, mask=A)
G = cv2.bitwise_and(G, G, mask=A)
R = cv2.bitwise_and(R, R, mask=A) watermark = cv2.merge([B, G, R, A])
#       loop over the input images
for imagePath in paths.list_images(args["input"]):
#       load the input image, then add an extra dimension to the
#       image (i.e., the alpha transparency) image = cv2.imread(imagePath)
(h, w) = image.shape[:2]
image = np.dstack([image, np.ones((h, w), dtype="uint8")   *
255])
#       construct an overlay that is the same size as the input
#       image, (using an extra dimension for the alpha transparency),
#       then add the watermark to the overlay in the bottom-right
# corner
overlay = np.zeros((h, w, 4), dtype="uint8")
overlay[h - wH - 10:h - 10, w - wW - 10:w - 10] = watermark
#       blend the two images together using transparent overlays output =
image.copy()
cv2.addWeighted(overlay, alpha, output, beta, 0, output)
#       write the output image to disk
```

filename = imagePath[imagePath.rfind(os.path.sep) + 1:] p = os.path.sep.join((args["output"], filename)) cv2.imwrite(p, output)

EXECUTION AND RESULT

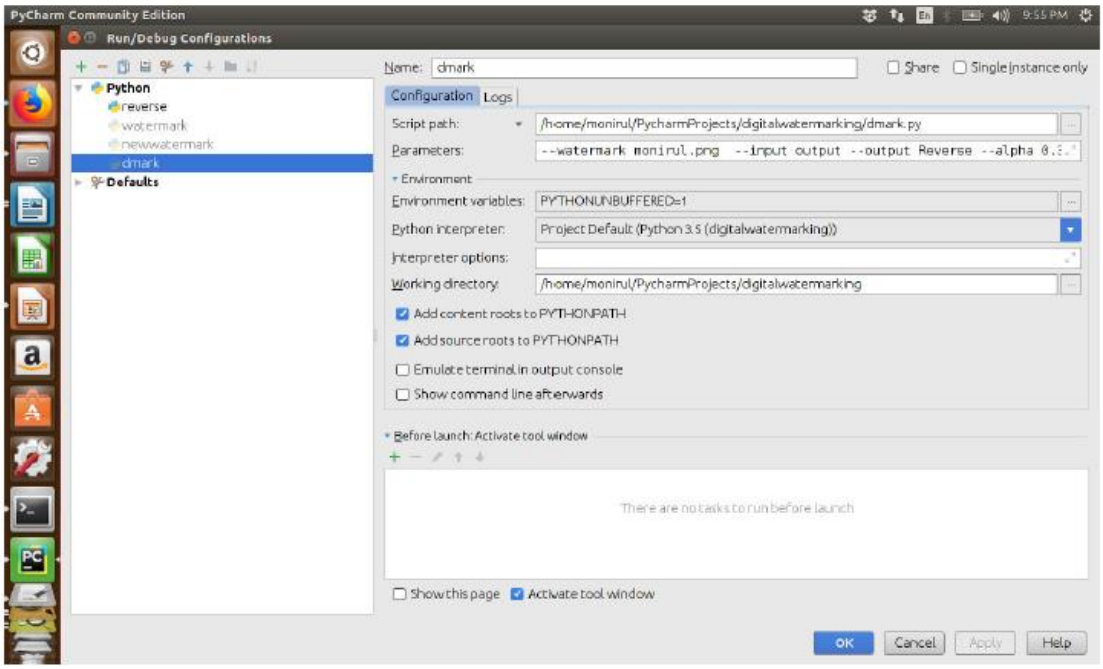


Fig. Run/Debug Configuration

Figure 3.2(a) Watermarked Image

Figure 3.2(b) Original Image

Chapter VI

A TECHNIQUE FOR REMOVAL OF A WATERMARK

6.1 Proposed Technique For Removal

- Import required Python packages. We'll be making use of the packages like imutils,numpy/argparse/cv2/os.
- Parsing our required command line arguments. We require three command line arguments and can supply two additional (optional) ones.
- --watermark : Here we supply the path to the image we wish to use as the watermark. We presume that (1) this image is a PNG image with alpha transparency and (2) our watermark is smaller (in terms of both width and height) then all images in the dataset we are going to apply the watermark to.
- --input : This is the path to our input directory of watermarked images we are going to de watermark.
- --output : We then need to supply an output directory to store our de watermarked images.
- --alpha : The optional --alpha value controls the level of transparency of the watermark. A value of 1.0 indicates that the watermark should be 100% opaque (i.e., not transparent).
- --correct : Finally, this is used to control whether or not we should preserve a "bug" in how OpenCV handles alpha transparency.
- The cv2.imread function loads our watermark image from disk using cv2.IMREAD_UNCHANGED.This value is supplied so we can read the alpha transparency channel of the PNG image (along with the standard Red, Green, and Blue channels).
- The spatial dimensions (i.e., height and width) of the watermark image is taken.
- To ensure that each of the Red, Green, and Blue channels respected the alpha channel, the bitwise AND is taken.
- Start looping over each of the images in our --input directory. For each of these images, we load it from disk and its width and height is taken.
- It's important to understand that each image is represented as a NumPy array with shape (h, w, 3), where the 3 is the number of channels in our image — one for each of the Red, Green, and Blue channels, respectively.

- However, since we are working with alpha transparency, we need to add a 4th dimension to the image to store the alpha values. This alpha channel has the same spatial dimensions as our original image and all values in the alpha channel are set to 255, indicating that the pixels are fully opaque and not transparent.
- The overlay for our watermark is constructed. Again, the overlay has the exact same width and height of our input image.
- Finally, our image is constructed by applying the cv2.addWeighted function.
- then take our output image and write it to the --output directory.

6.2 Implementation For Removing Watermark:

```
# USAGE
#python watermark_dataset.py —watermark
pyimagesearch_watermark.png --input input --output output
#	import the necessary packages from imutils import paths import numpy as np
import argparse import cv2 import os
#	construct the argument parse and parse the arguments

ap = argparse.ArgumentParser()
ap.add_argument("-w", "--watermark”, required=True,
help=”path to watermark image (assumed to be transparent PNG)")
ap.add_argument("-i", "--input", required=True, help="path to the input directory of images")
ap.add_argument("-o", "--output", required=True, help="path to the output directory")
ap.add_argument("-a", "--alpha", type=float, default=0.25,
help="alpha transparency of the overlay (smaller is more transparent)")
ap.add_argument("-c", "--correct", type=int, default=1, help="flag used to handle if bug is displayed or not")
args = vars(ap.parse_args()) alpha= 1/(1-args["alpha"]) beta = (1 -1/(1- args["alpha"]))
print("alpha" + str(alpha)) print("beta" + str(beta))
#	load the watermark image, making sure we retain the 4th channel
#	which contains the alpha transparency
watermark = cv2.imread(args["watermark"], cv2.IMREAD_UNCHANGED) (wH, wW) = watermark.shape[:2]
#	split the watermark into its respective Blue, Green, Red, and
```

```
#       Alpha channels; then take the bitwise AND between all channels
#       and the Alpha channels to construct the actual watermark

#       NOTE: I'm not sure why we have to do this, but if we don't,
#       pixels are marked as opaque when they shouldn't be if args["correct”] > 0:
(B, G, R, A) = cv2.split(watermark)
B =     cv2.bitwise     and(B, B,       mask=A)
G =     cv2.bitwise     and(G, G,       mask=A)
R =     cv2.bitwise     and(R, R,       mask=A)
watermark = cv2.merge([B, G, R, A])
# loop over the input images
for imagePath in paths.list_images(args["input"]):
#       load the input image, then add an extra dimension to the
#       image (i.e., the alpha transparency) image = cv2.imread(imagePath)
(h, w) = image.shape[:2]
image = np.dstack([image, np.ones((h, w), dtype="uint8")   *
255])
#       construct an overlay that is the same size as the input
#       image, (using an extra dimension for the alpha transparency),
#       then add the watermark to the overlay in the bottom-right
#       corner
overlay = np.zeros((h, w, 4), dtype="uint8")
overlay[h - wH - 10:h - 10, w - wW - 10:w - 10] = watermark
#       blend the two images together using transparent overlays
output = image.copy()
cv2.addWeighted(output, alpha, overlay, beta, 0, output)
# write the output image to disk
filename      =      imagePath[imagePath.rfind(os.path.sep)      +      1:]      p      =
os.path.sep.join((args["output"], filename)) cv2.imwrite(p, output)
```

Chapter VII

DIGITAL WATERMARKING APPLICATIONS

Digital watermarking is rapid evolving field, this section identifies digital watermarking applications and provides an overview of digital watermarking capabilities and useful benefits to customers. The various applications are:

1. Authentication
2. Broadcast Monitoring
3. Copy Prevention
4. Forensic Tracking
5. E-Commerce/Linking

1. AUTHENTICATION

Authentication identifies if content has been altered or falsified. For example digital watermarking can verify authenticity and identify counterfeiting as a second layer of security for encrypted content. The presence of digital watermark and/or continuity of watermark can help ensure that the content has not been altered.

2. BROADCAST MONITORING

Broadcast content is embedded wit a unique identifier, and optionally, distributor information. Detectors are placed at popular markets, where broadcasts are received and processed, resulting in reports to be sent to the owner.

3. COPY PREVENTION

Copy prevention helps the digital watermarks to identify whether the content can be copied. It guards against unauthorized duplication.

4.FORENSIC TRACKING

Forensic tracking locates the source of the content. The key advantage of digital watermarking is that it enables tracking of the content to where it leaves an authorized path.

5.E-COMMERCE/LINKING

The digital watermarking enables the user to purchase or access information about the content, related content, or items with in the content.

Chapter VIII

ADVANTAGES AND DISADVANTAGES

8.1 Advantages

- Digital Watermarking allows embedding of arbitrary information (the watermark) into digital media (such as video or images) by applying imperceptible, systematic alterations to the media data.
- Higher level of security: Security and confidentiality of the embedded information is provided by a secret key. Without this key the
- watermark cannot be accessed or modified. Watermarks can be designed in such a way that the embedded information is still retrievable even after the carrier medium changed.
- The advantage of digital watermarking is that the product of the embedding process is still a digital medium. Customers can do everything with a marked medium that they can do with an unmarked one. Watermarked media can be played or copied without any restrictions
- Digital Watermarking is non-restrictive - only misuse is detectable and traceable.
- Easy to implement and understand.
- Low degradation of image quality.
- High perceptual transparency.
- Gain factor can be increased resulting in increased robustness.
- High level of robustness against most type of attacks.
- This method hides data within the continuous random texture patterns of a picture.
- The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.
- Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception.
- DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions

8.2 Disadvantages

Digital watermarking is a recent research field; therefore its intrinsic limits are not well understood yet. On the other hand, more insight into the technical possibility of satisfying the requirements imposed by practical applications is needed, if the practical possibility of using watermarking for copyright protection is to be evaluated. In the following, some of the most common limits shared by digital watermarking schemes are described.

- Visible watermark can be easily removed.
- A watermarking algorithm which is really robust does not exist yet. In the image case, robustness is still an open issue. More specifically, resistance to geometric manipulations such as cropping is recognized as a very difficult goal to achieve in a computationally efficient way.
- Owners can erase the mark: virtually all the watermarking schemes
- proposed so far are reversible according to the definition previously given.
- In other words, by knowing the exact content of the watermark, and the algorithms used to embed and retrieve it, it is always possible to make it unreadable without any significant degradation of the data.

Chapter IX

CONCLUSION

To embed a hidden robust watermark to digital multimedia is the ultimate goal of watermarking system. Digital watermarking technology is an emerging field in computer science, cryptology, signal processing and communications. We have discussed the algorithms for watermarking and dewater marking of image as part of the project. The watermarking research is more exciting as it needs collective concepts from all the fields along with Human Psychovisual analysis, Multimedia and Computer Graphics. The watermark may be of visible or invisible type and each has got its own applications.

To maintain the security of the watermark, it should be embedded into randomly selected regions in some domain of the watermark signal. By doing this, it is difficult to remove the watermark.

- As Described Recent Development In The Digital Water Marking Of Images In Which The Water Marking Technique Is Invisible.
- Digital Water Marking Is Rapidly Evolving Area Of Research And Development.
- Digital Watermarking Technology Can Provide New Way To Protect The Copyright Of Multimedia Information And To Ensure The Safe Use Of Multimedia Information.
- The study of the watermark technology has become active since mid-1990s, and some technologies are already adopted in practical applications as a product or as proprietary services for enterprises.
- Although this is a relatively new technology area, it quickly becomes a practical and effective solution in some application areas, and has great potential for some other areas as well.
- The key to the successful implementation is to understand the advantages and the limitations of the watermark technology, and to use the watermark technology as a complimentary element to the existing security elements.

REFERENCES

- K.Sridhar, Dr. Syed Abdul Sattar , Dr. M Chandra Mohan," Comparison of Digital Watermarking with Other Techniques of Data Hiding", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (1) , 2014, 350-353
- Namita Chandrakar, Jaspal Bagga,"Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of Computer Applications Technology and Research Volume 2- Issue 2, 126 - 130, 2013
- Prabhishek Singh, R S Chadha,"A Survey of Digital Watermarking Techniques, Applications and Attacks",International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013
- Methodologies in Digital Watermarking: Robust and Reversible Watermarking Techniques for Authentication, Security and Privacy Protection by Xin Cindy Guo
- Digital Watermarking: A Tutorial, Dr. Vipula Singh
- Selective Region Based Invisible Watermarking Using Asymmetric Key Encryption, Somenath Nag Choudhury CSE Department
- Security and Robustness Enhancement of Digital Image Watermarking by Chittaranjan Pradhan
- Watermarking of Digital Images by Saraju Prasad Mohanty