ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

Digital Watermarking: Review

Shraddha S. Katariya (Patni)
nileshpatni@indiatimes.com, nileshpatni1977@gmail.com

Abstract*— Digital watermarking technology is a frontier research field and it serves an important role in information security. According to the analysis of the definition and basic characteristics of digital watermarking technology, the system model of digital watermarking is given. The system consists of two modules which are watermark embedding module and watermark detection and extraction module. In view of the importance of digital images copyright protection, based on the analysis of the main digital watermarking algorithms, the digital watermarking technology can be applied to the image copyright protection. The two dimension discrete cosine transform is encoded on the Windows platform by using Visual C++ program language. The experiment result shows that the digital watermark is non-perceptible; the watermark information can be extracted even if it has been attacked, and the expected effect can be achieved.

***Index Terms*—Digital watermarking, encryption, algorithm.**

I. INTRODUCTION

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.

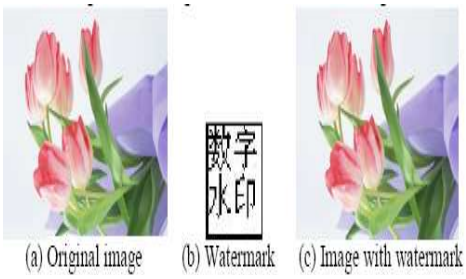

Fig 1.1. Watermark and image

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 documents i.e. documents created in digital media are having certain Advantages like-

- Efficient data storage, duplication, manipulation and transmission.
- Copying without loss.

Such digital documents consist of images, audio clips and videos. But due to some delimits of digital documents, they become inefficient to use. These delimits are as follows

- Illegal copying
- Falsification(duplication)
- No copyright protection
- No ownership identification

The large use of networked multimedia system has created the need of "Copyright Protection" for different digital medium as images, audio clips, videos etc. The term "Copyright Protection" involves the authentication of ownership and identification of illegal copies of digital media. Though digital media provides various efficient facilities like distribution, reproduction and manipulation of images, audio clips and videos, they increase illegal copying of digital media. The solution for this problem is to add the visible or invisible structure to digital media which is to be protected from copyright. These structures are known as "Digital Watermarks" and the process of adding digital watermarks to digital media is known as "Digital Watermarking". Digital watermarking is created by inserting a digital signal or pattern into digital content. Digital watermarking is nothing but process of conveying information by imperceptibly embedding it into digital media. The purpose of embedding the information depends upon application and need of user of digital media. Digital watermarking provides the solution for difficult problem of providing guarantee to organizer and consumer of digital content about their legal rights. Copyright protection for multimedia information is nothing but a golden key for multimedia industry. Digital watermarking is a technology that opens a new door for authors, producers, publishers and service providers for protection of their rights and interest in multimedia documents.

There are various techniques for prevention of illegal copying. They are described as follows

- Encryption methods which include use of public and private keys to encode the data, so that image can decoded only with required key.
- Site security methods which includes use of firewalls to access the data.
- Using Thumbnail images. and the most popular and important
- Digital watermarking which includes robust labeling of an image with Information which is to be prevent from illegal copying and also use of image checksum or other techniques to detect manipulation of image data.

In general sense, Digital Watermarking means "Author Signature". Digital watermarking is the process of encoding hidden copyright information in an image by making small modifications in its pixel content. In this case watermarking

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

doesn't restrict the accessing image information. The important function of watermarking is to remain present in data for proof of ownership. The use of digital watermarking is not restricted up to copyright protection. Digital watermarking can also be used for owner identification to identify content of owner, fingerprinting to identify buyer of content, broadcast monitoring and authentication to determine whether the data is changed from its original form or not Finally, the actual meaning of Digital watermarking technique is come to know from following three point of views

- Work = A specific song, video, picture or specific copy of such.
- Content = Set of all possible works.
- Watermarking =The practice of imperceptibly altering a work to embed a message about that work.

The watermarking solution promise to protect your images by inserting text information and then tracking the images. Digital watermarking distinguishes digital copies and mark documents with owner's ID. There are many reasons to embed information in digital content using digital watermarking. The internet boom is one of the reasons. It has become very easy to connect to internet from home computers to obtain or provide various information using World Wide Web (WWW). All information handled on internet is in digital form. Such digital content can be copy such that new file is indistinguishable from original one. Then content can be re produce in large quantities. .Digital watermarking protecting such illegal copying. A watermark discourages piracy and determines criminals of making illegal copies of digital media. Information hiding has emerged as an exciting and important research field which encompasses steganography, steganalysis and digital watermarking [1]. 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. At any given moment, the hidden information can be extracted to prove ownership, to ensure integrity, or simply to get some copyright-related information. Watermarking is analogous to the task of communication. It can normally be described as three stage process: watermark generation and embedding (akin to information transmission), distribution and possible attacks (transmission through the channel), and watermark retrieval or detection (information decoding at the receiver side) [2].In some applications, the original, un-watermarked work is needed during detection. In other applications, detection must be performed without access to the original work

A. ***Need of Digital Watermarking:*** The purpose of digital watermarks is to provide copyright protection for intellectual property that is in digital format .First important application come into mind is copyright protection of digital media. It is easy to duplicate digital data exactly without quality loss. Similar to process in which artist signed their painting with a brush to claim their copyrights, artist of today can watermark their work and hide some information say their name in the image. Hence, embedded watermark will allow identifying the owner of work. This concept is applicable to digital video and audio also .Especially, distribution of digital audio over internet in MP3 format is currently a big problem. Digital watermarking may be useful to setup controlled audio distribution and provide efficient means for copyright protection, usually in collaboration with international registration bodies such as IDDN (Inter Deposite Digital Number).

In addition with copyright protection, Digital watermarking is playing a important role in many fields of applications such as broadcast monitoring, owner identification, transaction tracking, proof of ownership, fingerprinting, content authentification, copy control, device control. Digital watermarks can also serve as invisible labels and content link. For example, photo development labs may insert a watermark into the picture to link the print to its negative. so, it is becomes easy to find out negative of a print. All one has to do is to scan the print and extract the information from negative. In a completely different scenario, the digital watermarks may be used as a geometrical reference which may be useful for programs such as Optical Character Recognition (OCR) software. The embedded calibration watermark may improve the detection reliability of the OCR software since it allows the determination of translation, rotation and scaling. Digital watermarking also serves as a means of advertising within the digital media. For instance, the user may download and view a digital image, use a watermark reader to extract the digital signature, then access a web based directory to find the company's name and up-to-date address phone number and web and e-mail address. Digital watermarks also serve the purposes of identifying quality and assuring authenticity. A graphic or audio file bearing digital watermark can inform the viewer or listener who owns to the item.

B. Objectives of Digital Watermarking: *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

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

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.

II. DIGITAL WATERMARKING TECHNOLOGY

A. Classification of digital watermarking

1) Digital watermarking can be divided into robust watermarking and fragile watermarking according to its characteristics. Robust watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossy compression, the watermark is not destroyed after some attack and can still be detected to provide certification. Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

2) Digital watermarking can be divided into image watermarking, video watermarking, audio watermarking, and text watermarking and graphic watermarking based on the attached media. Image watermarking refers to adding watermark in still image. Video watermarking adds digital watermark in the video stream to control video applications. Text watermarking means adding watermark to PDF, DOC and other text file to prevent changes of text. Graphic watermarking is embedding watermark to two-dimensional or three-dimensional computer-generated graphics to indicate the copyright.

3) Digital watermarking can be divided into visual watermarking and blind watermarking according to the detection process. Visual watermarking needs the original data in the testing course, it has stronger robustness, but its application is limited. Blind watermarking does not need original data, which has wide application field, but requires a higher watermark technology.

4) Digital watermarking can be divided into copyright protection watermarking, based on its purpose. Copyright protection watermarking means if the owners want others to see the mark of the image watermark then the watermark can be seen after adding the watermark to the image, and the watermark still exists even if it is attacked. Tampering tip watermarking protects the integrity of the image content, labels the modified content and resists the usual lossy compression formats. Note watermarking is added to the building process of the paper notes and can be detected after printing, scanning, and other processes. Anonymous mark watermarking can hide important annotation of confidential data and restrict the illegal users to get confidential data.

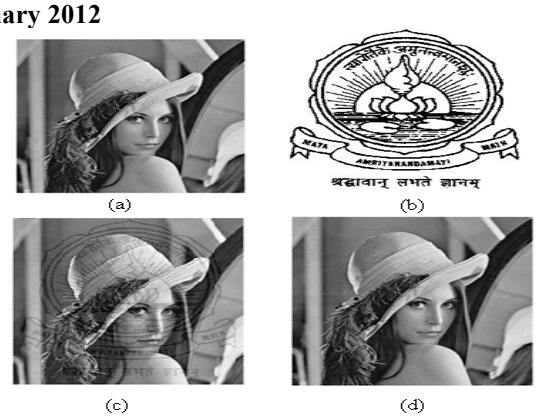

Fig. 2 .1.The figure shows (a) the original Lena image (b) the logo to be watermarked (c) visible watermarked image and (d) invisible watermarked image

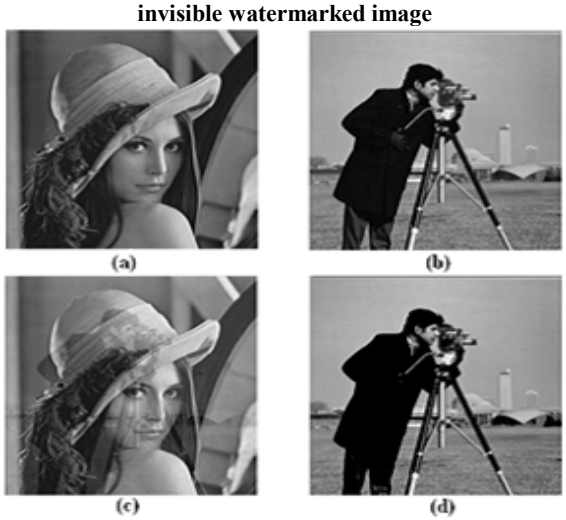

Fig. 2.2. The figure shows (a) the Lena image (b) the original Cameraman image to be watermarked (c) visible watermarked Image and (d) the recovered cameraman image.

B. Basic Characteristics of Digital Watermarking

The basic requirement of digital watermarking is closely related to its purpose of applications, different application has different demand. In general, the characteristics of digital watermarking are as follows.

1) Robustness: Robustness refers to that the watermark embedded in data has the ability of surviving after a variety of processing operations and attacks. Then, the watermark must be robust for general signal processing operation, geometric transformation and malicious attack. The watermark for copyright protection does need strongest robustness and can resist malicious attacks, while fragile watermarking; annotation watermarking do not need resist malicious attacks.

2) Non-perceptibility: Watermark cannot be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits.

3) Verifiability: Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.

4) Security: Watermark information owns the unique correct sign to identify, only the authorized users can legally detect,

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection

5) Capacity: Image watermarking capacity is an evaluation of how much information can be hidden with in a digital image. Watermarking capacity is determined by the statistical model used for the host image, by the distortion constraints on the data hider and the attacker, and by the information available to the data hider, to the attacker, and to the decoder.

C. Architecture of Digital Watermarking

1. System model of digital watermarking: The process of digital watermarking embeds the special information which stands for the particular identity of the owner of the copyright by some sort of algorithm to multimedia data. We can extract the watermark, verify the ownership of the copyright and ensure the legitimate rights of the copyright owners though the appropriate algorithms. Complete digital watermarking system is composed of two basic modules: watermark embedding module and watermark detection and extraction module. Watermark embedding module is responsible for adding the watermark signal to the original data. The watermark can be any form of data, such as numeric, text, image, and so on. Key can be used to strengthen security to prevent unauthorized parties restore and modify the watermark. The watermark embedding module is as shown in figure 2.3.

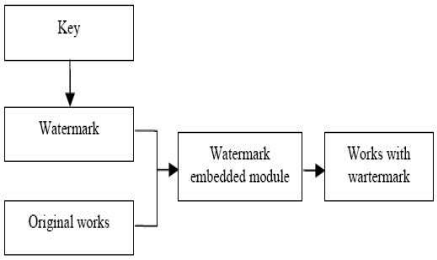

Fig. 2.3.water embedded module

Watermark detection and extraction module is used to determine whether the data contains specified watermark or the watermark can be extracted. The module input may be image, key, watermark or original image, the output is a watermark or some kind of credibility value. It indicates the possibility of the data having a given watermark.

2. Main algorithms of digital watermarking: In recent years, the study of digital watermarking technology makes great progress. There are a lot of good algorithms which can be divided into spatial domain algorithm and transform domain algorithm.

i) Spatial domain algorithms: Spatial domain digital watermarking algorithms directly load the raw data into the original image.

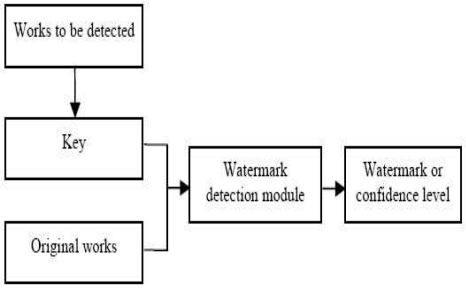

Fig 2.4. Detection and extraction module of watermark

- **Last significant bit algorithm:** The algorithm embeds the information with the form of the least significant bits selected randomly which can ensure the embedded watermark is invisible. But the algorithm has poor robustness, and watermark information can easily be destroyed by filtering, image quantization, and geometric distortion.
- **Patchwork algorithm:** Based on the statistics, the algorithm uses the statistical characteristics of pixels to embed the information into the brightness values of pixel. It can resist lossy compression coding and malicious attacks. However, the amount of embedded information is limited, in order to embed more watermark information; we can segment the image, and then implement the embedding operation each image block.
- **Texture mapping coding method:** It hides the watermark in the texture part of the original image. The algorithm has strong resistance ability to attacks for a variety of deformation, but only suitable for areas with a large number of arbitrary texture images, and can not be done automatically.

ii) Transform domain digital watermarking algorithm: Transform domain algorithm is a method of hiding data similar to spread-spectrum communication technology. Firstly, it does a kind of orthogonal transformation for image, and then embed watermark information in the transform domain of image, finally use the inverse transform to recovery the image in spatial domain, the detection an extraction of the watermark are also realized in transform domain. There are several common used transform domain methods, such as discrete Fourier transform (DFT), discrete cosine transforms (DCT), and discrete wavelet transforms (DWT), and so on. As a classical mathematical transformation method, DCT does a very important role in image compressing; coding and other applications. The watermarking algorithms based on DCT domain are compatible with the existing international compression standards. The main idea of these methods is to select middle or low frequency coefficients to superposition watermark in the DCT transform domain. Image x(m, n) can be seen as a matrix of M×N and be transformed from the spatial domain DCT.

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

The expression of two-dimensional DCT is as follows.

$$X(k,l)=\frac{2}{\sqrt{MN}}c(k)c(l)\sum_{m=0}^{M-1}\sum_{N=0}^{N-1}x(m,n)\bullet X$$

$$X=\cos\left[\frac{(2m+1)k\pi}{2M}\right]\cos\left[\frac{(2n+1)l\pi}{2N}\right]$$

$$k=0,1,2,\cdots,M-1;l=0,1,2,\cdots,N-1$$

The inverse transform of DCT is:

$$x(m,n)=\frac{2}{\sqrt{MN}}\sum_{k=0}^{M-1}\sum_{l=0}^{N-1}c(k)c(l)X(k,l)\bullet Y$$

$$Y=\cos\left[\frac{(2m+1)k\pi}{2M}\right]\cos\left[\frac{(2n+1)l\pi}{2N}\right]$$

$$m=0,1,2,\cdots M-1;n=0,1,2,\cdots N-1$$

where,

$$c(k)=\begin{cases}1/\sqrt{2},k=0\\1,k=1,2,\cdots,M-1\end{cases}$$

$$c(l)=\begin{cases}1/\sqrt{2},l=0\\1,l=1,2,\cdots,N-1\end{cases}$$

D. Applications of digital Watermarking in Image Copyright Protection

Digital watermarking can indicate the copyright owner, identify the buyer or provide additional information of digital content, and embed the information into digital images, digital audio and video sequence. This paper introduces an application of digital watermark in image copyright protection. The system can use DCT algorithm to embed the chaotic sequence or meaningful watermark into the protected image, and provide effective technical means for the identification of the image copyright. The structure of image copyright protection system is as shown in figure 2.5.

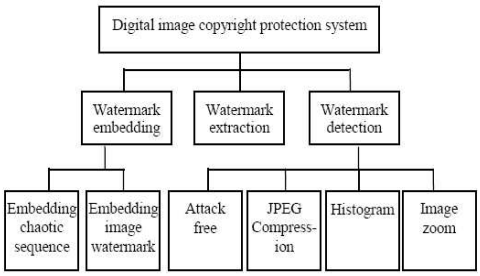

Fig.2.5. Image copyright protection

1. Implementation of DCT algorithm

We use Visual C++ to program and implement the system. The image data is transformed to transform domain data which is also transformed back to the image data by inverse transform. These transformations are complete by DCT.

- **Generation and embedding of watermark**

a) Calculate the DCT transform of the original image.
b) Select N random numbers according to normal Distribution N (0, 1). Generally, the larger N is, the Better watermark effect has X=x1, x2... xN.
c) Do linear transformation for the coefficients vi of DCT transform vi = **vi** (1+xi αi) where, αi is control variable
d) Compute inverse transform coefficients of DCT, and embed the watermark information into digital images.

- **Extraction and detection of watermark**

a) Calculate the DCT transform coefficient X of image After adding watermark.
b) Calculate the DCT transform coefficient X0 of the Original image.
c) Compare X and X0
d) Define S as the inner product of two vectors to detect the watermark information.

2) Digital Signature Standard Algorithm:

i) Watermark generation and embedding algorithm

Input: The original image itself or, as a variation, original image and a watermark. The watermark could be an image or a logo or with slight modifications it could also be text or a Random binary sequence.

Output: A watermarked image, perceptibly having no difference with respect to the original image, yet on processing it contains the signatures or the watermark. adapted to digital watermarking of images

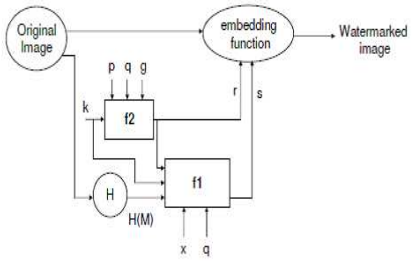

Fig. 2.6. Digital Signature Algorithm (generation)

Algorithm:

Step1. Input the original image or the watermark as a two dimensional array or matrix, M.
Step2. Convert the two dimensional matrix, M to a single dimension row matrix, M1.
Step3. Convert the row matrix M1 into a binary string, S such that each element of the row matrix is represented by 8-bit sequence of 1s and 0s.
Step4. Call a sub-routine for calculating the hash value with input as the binary string, S. The output is, say H. The hash function is the Secure Hash algorithm, SHA-1.
Step5. Obtain the pre-generated values of p and q. With these as input call a sub-routine to calculate other parameters, g, y, x and k.
Step6. With p, q, g, x, k and H as input, calculate the digital signatures 'r' and's' by calling the signature function. This function returns the values of 'r' and's'.
Step7. Concatenate the signatures 'r' and's into a single string.
Step8. Process the original image into 8x8 blocks and calculate their DCT.
Step9. Encode each bit of the signature or watermark by manipulating the DCT Coefficients corresponding to positions (5,2) and (4,3).

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

Step10. Perform an inverse DCT. We have now obtained the watermarked image.

ii) Watermark detection and verification algorithm

Input: The watermarked image along with the global communicating principals (q,g,y). The original image and/or watermark is needed for finding hash value and in detection, as well, this being a private watermarking scheme.

Output: Digital signatures, 'r''s', and output of the verification function 'v'.

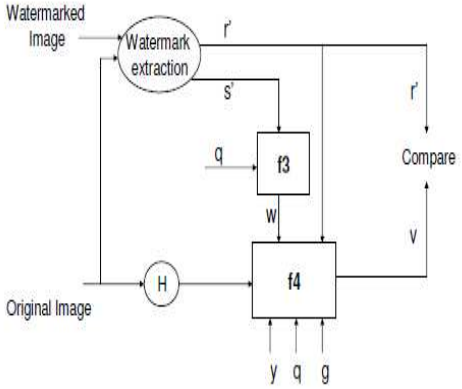

Fig. 2.7. Digital Signature Algorithm (verification) Adapted to extraction of watermarks in images

Algorithm:

Step1. Process the watermarked image into 8x8 blocks and calculate their DCT.

Step2. Decode each bit of the signature or watermark by seeing which of the DCT coefficients corresponding to position (5,2) and (4,3) is greater than the other. This allows us to obtain the signatures 'r' and's'. The steps 3 to 6 are the same as steps 1 to 4 in the embedding algorithm.

Step3. Input the original image or the watermark as a two dimensional array or matrix, M.

Step4. Convert the two dimensional matrix, M to a single dimension row matrix, M1.

Step5. Convert the row matrix M1 into a binary string, S such that each element of the row matrix is represented by 8-bit sequence of 1s and 0s.

Step6. Call a sub-routine for calculating the hash value with input as the binary string, S. The output is, say H.

Step7. With q, g, and y known at the reception end, along with H, r and s, we call the verification function for calculating parameter, v.

Step8. Compare r and v. if they are the same then the signatures or the watermark embedded in the image are verified.

iii) Blind watermarking scheme for protecting rightful ownership

This section presents the proposed innovative invisible and blind watermarking scheme for copyright protection of digital images. As the proposed digital watermarking scheme doesn't require the original image or any of its characteristics for extraction, the proposed watermarking scheme is blind. The watermark data utilized is a binary image and its pixels are invisibly embedded into the host image for copyright protection. The following subsections describe the steps involved in the watermark embedding and extraction processes.

Watermark Embedding -

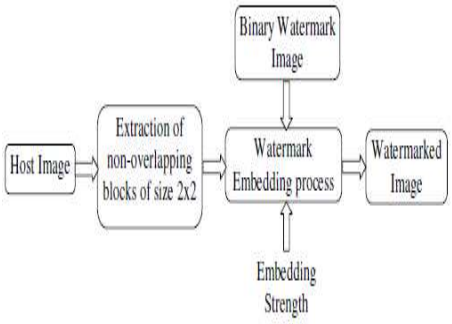

Fig.2.8. Watermark Embedding Process

This sub-section presents the process of binary watermark image embedment into the host image. The size of the host image chosen is dyadic (2nx2n) and the watermark used is a binary image. Firstly, non-overlapping blocks sized 2x2 are extracted from the host image and every pixel of the binary watermark image is embedded into a single block of the host image. The watermark embedding process involves: mean calculation, embedding strength (γ) and signum function. Each non-overlapping block is converted into a vector, and the mean value of the vector is computed and divided with the embedding strength (γ).

III. SYSTEM OVERVIEW

The structure of typical Digital watermarking system consists of mainly three Parts viz watermark insertion unit, watermark extraction unit and watermark detection unit. Thus process of digital watermarking technique includes three Processes i.e. watermark insertion process, watermark extraction process and watermark detection process. The watermark insertion unit provides the generic approach to watermarking any digital media[2].

A generic watermarking system:

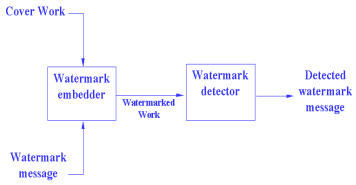

Fig. 3.1. The generic approach of watermarking system

Generic approach consists of watermark embedder and watermark detector. The watermark embedder is having two inputs i.e. cover work and watermark message and its output is watermarked work which is input to watermark detector. Then after performing some operations detector gives detected watermark message. Inputs to insertion unit are original image (i.e any digital content), the watermark and user key to obtain watermarked image. The output of insertion unit is watermarked object. The input to extraction unit consists of watermarked image and key used during insertion

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

unit If, object has not been altered, since it was marked and correct key is used, output of extraction unit is watermark .If, the object has been altered or wrong key is used, the extraction procedure outputs an error message.

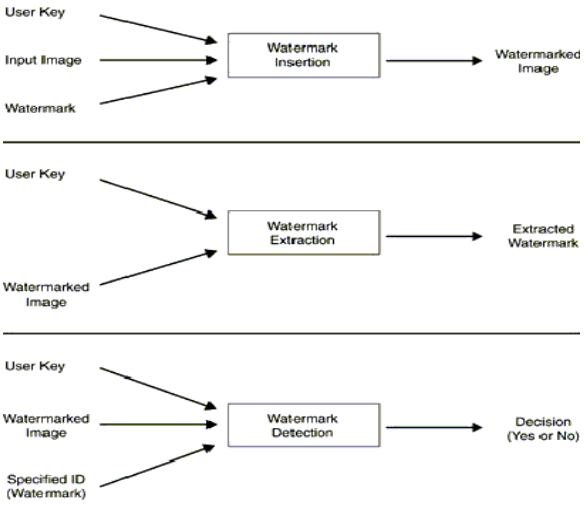

Fig. 3.2 Working Phase of Digital Watermarking

The inputs to detection units are watermarked object (may be alter), the watermark that was inserted into object and the key. The detection process then indicates whether the object contains a mark that is "close to" the original watermark. The meaning of "close" depends on the type of alterations that a marked object might undergo the course of normal use.

Watermark insertion unit integrates the input image and watermark to form output watermarked image. Watermark extraction uncovers the watermark in watermarked images, a technique usually applicable in verification watermarks. Watermark detection detects presence of ID .e.g. in robust watermarks presence of specified ID (watermarks) can be detected using predefined threshold; i.e. answering to question either YES or NO indicates whether ID is present or Not. Figure shows what actual process is carried out during embedding and extraction process. Original data and watermark on submitting to embedding algorithm gives watermarked data. During extraction, this watermarked data is then given to extraction algorithm gives extracted watermark. 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.

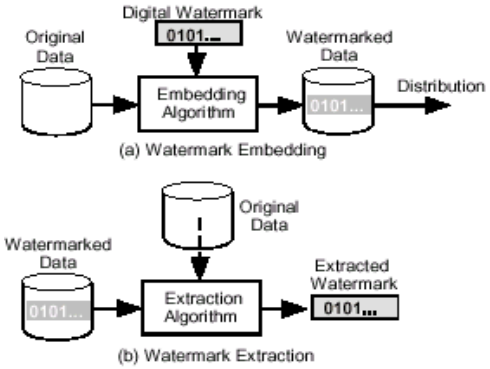

Fig. 3.3. General digital watermarking process.

In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark. In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of stegnography, 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. One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

Annotation of digital photographs with descriptive information is another application of invisible watermarking retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. Annotation of digital photographs with descriptive information is another application of invisible watermarking. While some file formats for digital media may contain additional information called metadata, digital watermarking is distinctive in that the data is carried right in the signal.

IV. SYSTEM ANALYSIS

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

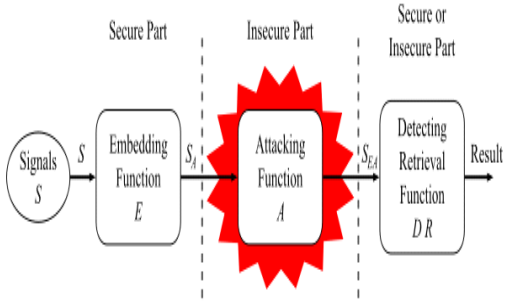

Fig.4.1. Digital watermarking life-cycle phases

General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions. The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal. A digital watermarking method is referred to as spread spectrum if the marked signal is obtained by an additive modification. Spread-spectrum watermarks are known to be modestly robust, but also to have a low information capacity due to host interference. A digital watermarking method is said to be of quantization type if the marked signal is obtained by quantization. Quantization watermarks suffer from low robustness, but have a high information capacity due to rejection of host interference.

A digital watermarking method is referred to as amplitude modulation if the marked signal is embedded by additive modification which is similar to spread spectrum method, but is particularly embedded in the spatial domain. Digital Watermarking works by concealing information within digital data, such that it cannot be detected without special software with the purpose of making sure the concealed data is present in all copies of the data that are made whether legally or otherwise, regardless of attempts to damage/remove it. Digital watermarking technology makes use of the fact that the human eye has only a limited ability to observe differences. Minor modifications in the color values of an image are subconsciously corrected by the eye, so that the observer does not notice any difference. While vendors of digital watermarking schemes do not publicly release the exact methods used to create their watermarks, they do admit to using the following basic procedure (with obvious variations and additions by each vendor). A secret key (string or integer) produces a random number which determines the particular pixels, which will be protected by the watermarking. The watermark is embedded redundantly over the whole image, so that every part of the image is protected.

One way of doing this is by “Patchwork”. This technique uses a random number generator to select n pairs of pixels and slightly increases or decrease their luminosity (brightness level). Thus the contrast of this set is increased without any change in the average luminosity of the image. With suitable parameters, Patchwork even survives compression using JPEG. Although the amount of secret information has no direct impact on the visual fidelity of the image or the robustness of the watermark, it plays an important role in the security of the system. The key space, that is the range of all possible values of the secret information, x must be large enough to make exhaustive search attacks impossible. In the process of extracting the watermark, the secret key is used to identify the manipulated pixels and finally to decode the watermark.

Digital watermarking [3] has become an accepted security technology in the recent years, especially in the area of copyright protection. Its ability to withstand analogue conversion and its independence from media file formats makes it an alternative to digital rights management based on cryptographic mechanisms. Most copyright protection approaches use transaction watermarks which embed individual customer IDs or transaction codes within each distributed copy of a media file. This allows tracing back these copies to the original buyer when a misuse based on this copy is detected. Being able to distinguish between individual copies is obviously a very important advantage when fighting the illegal distribution of content as without watermark embedding all copies are alike and therefore cannot be traced by to the origin of their illegal distribution.

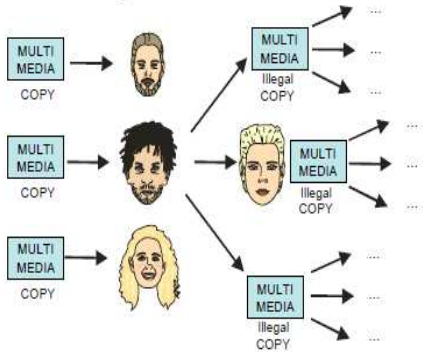

Fig. 4.2 Digital copies.

This makes it impossible to trace back illegal copies to their origin. One important fact that needs to be understood about this procedure is that a watermark can only identify the user who has received the content from the distributor or content owner, for example an online shop. If the user provides content marked with this ID to friends and they upload it to e.g. file sharing networks, only the ID of the first user will be found in the copy. Therefore in some cases the detection of the watermark may only be the beginning of further investigations starting from the first user. An alternative would be to prohibit any distribution of digital content by the regulations of the content provider which is already the case in many online shops today. This would render any distribution illegal and therefore any found copy would be an indicator of the first user acting against the regulations. The only exception would be theft of files from his computer, making a computer forensics analysis of the users’ computer

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

necessary. The challenge for digital watermarking in this area is to embed such individual watermarks fast enough to not cause significant delays within the media distribution. At the same time, a high robustness and very good transparency of the watermark is required to be accepted by content owners and customers. Attacks - Due to some reasons, there is need of adding, altering or removing false watermarks. Attacks on watermarks may be accidental or intentional. Accidental attacks may caused due to the standard image processing or due to the compression Procedures. Intentional attacks includes cryptanalysis, steganalysis, image processing techniques or other attempts to overwrite or remove existing watermarks Following are the methods of attacks vary according to robustness and Perceptibility. Mosaic attack- Mosaic attack is the method in which pictures are displayed so as to confuse watermark-searching program, known as "Web Crawler". Mosaic is created by subdividing the original image into randomly sized small images and displaying the resulting image on webpage.

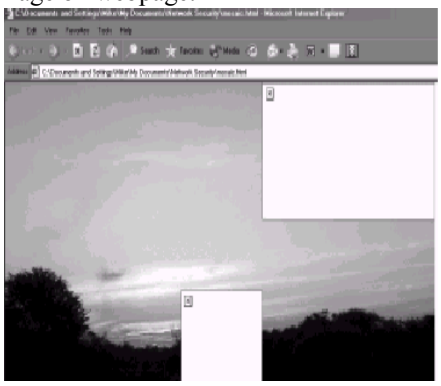

Fig.4.3. image is cut into pieces to confuse web crawler

Figure shows the example of mosaic schemes. The aim is to confuse the web crawler into thinking that there is no watermark within the picture because it has been sub divided into smaller separate pictures. This form of attack becomes to a large degree obsolete due to new improved methods of watermarking and more intelligent web crawlers. Geometric attack- Geometric attack is related to geometric properties of data. It is concerned with images, documents and audio files. This attack is further classified as-

1) **Subtractive attack-**It involves the attacker in the area of located watermark if imperceptible and then removing the mark by cropping or digital editing.

2) Distortive attack -In this attack, attacker attempts to make some uniform distortive changes in the images such that mark becomes unrecognizable. These two watermark attacks are usually performed on robust watermark.

3) Stirmark attack- Stirmark is generic tool developed for simple robustness techniques of image marking algorithms and steganographic techniques. In its simplest version, stirmark simulates resampling process in which it introduces same kind of errors into an image to print it on high quality printer and scanning it again with high quality scanner .It includes minor geometric distortion. This testing tool is an effective program to remove fairly robust watermarks in images and become a form of attack on it's own.

4) Forgery attack- Forgery attack is also known as 'Additive attack' in some cases. Forgery attack includes the attacker who can add his or her own watermark overlaying the original image and marking the content as their own.

5) Inversion attack -Inversion watermark render the watermark information ambiguous. idea behind the inversion attack that attacker who receives watermarked data can claim that data contains his watermark also by declaring part of data as his watermark. The attacker can easily generate the original data by subtracting the claimed watermark.

V. Conclusion and Future Scope

With the popularity of the network, the safety communication issue of digital product becomes an important and urgent research topic. In this paper, the basic principles and algorithms of the digital watermarking technology are discussed, and the DCT algorithm is selected to do the application test of digital image copyright protection. The experiment proves that DCT-based watermark can well withstand a variety of image processing, and the watermark can survive after compression, cropping, and other attacks. Digital watermarking technology can provide a new way to protect the copyright of multimedia information and to ensure the safe use of multimedia information. Comparing to the traditional information security technology, digital watermarking technology has its own advantages in the multimedia information security protection. Then it can meet the application need in many aspects and has a bright development prospect.

The field of digital watermarking is still evolving and is attracting a lot of research interest. The watermarking problem is inherently more difficult that the problem of encryption, since it is easier to execute a successful attack on a watermark. In cryptography, a successful attack often requires deciphering an enciphered message. In the case of digital watermarking, merely destroying the watermark, usually by slightly distorting the medium containing it, is a successful attack, even if one cannot decipher or detect any hidden message contained in the medium. The enormous popularity of the World Wide Web in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights.

Digital watermarking has been proposed as one way to protect such interests. Though much research remains before watermarking systems become robust and widely available, there is much promise that they will contribute significantly to the protection of proprietary interests of electronic media. Collateral technology will also be necessary to automate the process of authentication, non-reputable transmission and validation. An exhaustive list of watermarking applications is

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

of course impossible. However, it is interesting to note the increasing interest in fragile watermarking technologies. Especially applications related to copy protection of bills with digital watermarks. Various companies have projects in this direction solutions will soon be available. In addition to technological developments, marketing and business issues are extremely important and require in-depth analysis and strategic planning. It is very important to prepare the industry to the usage of digital watermarks and it is very likely that fully functioning to convince them of the added value their products can gain if they employ digital watermarking technologies.

VI. APPLICATIONS

The technique "Digital Watermarking" is the recent research in the field of multimedia and internet copyright protection field. There are various applications of DWM as broadcast monitoring, owner identification, proof of ownership, transaction hacking, content authentication, copy control, device control and so on. Out of these, some important applications are described as-

1. Broadcast monitoring: This application identifies that when and where works are broadcast by recognizing watermarks embedded in these works. There are variety of technologies to monitor playback of sound recording on broadcast. The DWM is alternative to these technologies due to its reliable automated detection. A single PC based monitoring station can continuously monitor to 16 channels over 24 hours with no human interaction. Resulted monitoring is assembled at central server and is now available to interested one. The system can distinguish between identical versions of songs, which are watermarked for different distribution channel. Such system requires Monitoring infrastructure and watermarks to be present in content. Watermarking video or music is planned by all major entertainment companies possessing closed networks.

2. Encoding: According to the thinking of major music companies and major video studios, encoding happens at mastering level of sound recording. In such downstream, transactional watermarks are also considered. Each song is assigned with unique ID from the identifier database. After completion of all mastering processes, ID is encoded in sound recording. To enhance encoding of audio or video recordings requiring special processing, the human-assisted watermark key is available.

3. Copy and playback control: The data carried out by watermark may contain information about copy and display permissions. We can add a secure module into copy or playback equipment to automatically extract the permission information and block further processing if required. This approach is being taken in Digital Video Disc (DVD)

.4. Content authentication: The content authentication is nothing but embedding the signal information in Content. This signature then can be checked to verify that it has not been alter. By watermarks, digital signatures can be embedded into the work and any modification to the work can be detected.

REFERENCES

[1] Zhang Jihua, "Research on Copyright Protection Technology of Digital Image Based on Digital Watermarking", Doctor Degree thesis. Changsha, Hunan, China: South-Central University for Nationalities. 2004. (In Chinese).

[2] Ingemar J. Cox, J. P. Linnartz, "Some general methods for tampering with watermarks", IEEE Journal on Selected Areas in Communication, 1998, 16(4):587-593.

[3] Arnold, Michael, Techniques and Application of Digital Watermarking, London: Artech House Publisher. 2003.

[4] L. Qian, K. Nahrstedt. "Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Rights", Journal of Visual Communication and Image Representation, 2005,29(4):194- 210.

[5] G. Voyatzis, I. Pitas. "Protecting Digital Image Copyrights A Framework", IEEE Transactions on Computer Graphics and Applications, 1999,19(1):18□24.

[6] Christine I., Podilchuk, Edward J. Delp. "Digital watermarking: Algorithms and applications", Signal processing Magazine, 2001.

[7] Performance Comparison of Novel, Robust Spatial Domain Digital Image Watermarking with the Conventional Frequency Domain Watermarking Techniques Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian,Vineeth Sarma Venugopala Sarma Department of Electronics and Communication, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam, Kerala, India.

[8] Capacity and Reliability of Digital Watermarking Zhang Fan, Zhang Hongbin Computer institute, Beijing University of Technology Pingleyuan 100#, Chaoyang District, Beijing, China 100022

[9] An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images by Dr.M.A.Dorairangaswamy Professor, Computer Science and Engineering Chennai, India.

[10] Performance Comparison of Novel, Robust Spatial Domain Digital Image Watermarking with the Conventional Frequency Domain Watermarking Techniques Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian, Vineeth Sarma Venugopala Sarma Department of Electronics and Communication, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam,

[11] A robust wavelet-based watermarking scheme for copyright protection of digital images mr.manjunatha prasad.r Assistant Professor and Head Department of Electronics, K.S.Institute of Technology, Bangalore

[12] Capacity and Reliability of Digital Watermarking Zhang Fan, Zhang Hongbin Computer institute, Beijing University of Technology Pingleyuan 100#, Chaoyang District, Beijing, China 100022 .

[13] Efficient Dual Domain Watermarking Scheme for Secure Images Amit M Joshi PG Student, Electronics Engg.

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

Department, Sardar Vallabhbhai National Institute of Technology, Surat, India.

[14] Digital Right Management Model Based on Cryptography and Digital Watermarking Jiaming He, Hong bin Zhang Department of Computer Science Beijing University of Technology Beijing, China Jiaming.He@live.cn, zhb@public.bta.net Digital watermarking techniques: A case study in fingerprints and faces Sonia Jain,

[15] A Digital Watermarking Algorithm Based On DCT and DWT Mei Jiansheng1, Li Sukang1 and Tan Xiaomei2 1 Nanchang Power Supply Company, Nanchang, China.

[16] Jiang Xuehua "Digital Watermarking & its Application in image copyright Protection" published in proceedings of International Conference on Intelligent Comp0utation Technology & Automation ICICTA2010.

AUTHOR BIOGRAPHY

Prof. Shraddha S. Katariya (Patni), has completed her M.E.(Electronics) & B.E. (E& TC), Member of IEEE & ISTE. She is working as a Assistant Professor in Electronics Department, Amrutvahini College Of Engineering, Sangamner, Dist. Ahmednagar, Maharashtra, India. Prof Katariya has teaching experience of 13 years to Undergraduate, Graduate & Post Graduate Students. Prof S S Katariya has Published 03 papers in International Journal, 02 papers in National Journal & presented 02 papers in International Conference & 13 papers in National Conferences.