Abstract — Vision is the primeval sensing action which imparts immense pleasure to even the beleaguered soul. It conveys huge amount of information in this fast developing and moving timeless world. Information is the basis for lots of human activities and images. It is vision that propels a large amount of this important information in a very short span of time. The recent advancements in the field of digital media and communication have proposed large facilities for data transport, transmission and manipulation. Chemical images have lead the way to the digital images long back, which have a variety of formats for storing the information and they come with large number of advantages. Along with these facilities however, there are larger number of threats in authentication of data, its licensed use and protection of data against illegal use. The images suffer from large amount of distractions and attacks. It becomes very necessary to protect the image originality and authenticity. Thus to stop the illegal use of the digital multimedia images a variety of digital image watermarking techniques have been designed and implemented. Also, watermarking does not disturb the composition of the image visibly.

This paper covers the following areas— definition of digital watermarking, purpose, techniques, and types of watermarking attacks. Also, we shall discuss the issues and the future of digital watermarking technology.

Keywords — Steganography, Digital image watermarking, DWT, robustness, attacks.

I. INTRODUCTION

Images being the major source of information, it developed almost randomly with the ages. Earlier chemical images on the photographic film were used but due to large amount of discomforts, it gave way to digital images which can be an integral part of digital communication and media. These images have numerous advantages especially in their storage and manipulation. Hence, they ensure effective communication using digital media.

Each day huge amount of information is embedded on digital media or it is distributed over the internet. This has created threats to copyright protection and content integrity, as digital entities can be easily duplicated, manipulated and even tampered. The information which is distributed can also be replicated without any errors, thus putting the rights of their owners at risk. Even when encrypted for distribution, data can easily be decrypted and copied. Engineers have accepted this challenge in a gallant way. Many techniques have been devised to protect the copyrights of digital entities.

Encryption and authentication are some of the traditional methods for providing security for digital media. However, they fail in providing the required copyright protection for digital images which is very important. Digital watermarking is potentially a good tool in enabling content protection.

II. DIGITAL IMAGE WATERMARKING

There is an increasing need for software that allows for protection of ownership rights and it is in this context where watermarking techniques come to our help. The concept of watermarking can be dated back to the late Middle Ages. Watermarks were used as anti-counterfeiting measures. Later the study of watermarking and its usage began to mushroom. The Government uses it for currencies, postage stamps, revenue stamps etc. The term is used from a process that was used since 1282 in the production of paper bearing a watermark for visible identification.

Digital Watermarking means embedding information into digital material in such a way that it is imperceptible to a human observer but easily detected by computer algorithm. A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of data source by using a specific computer algorithm. Digital watermarks are signal added to digital data that can be detected or extracted later to make an assertion about the data. The signal may be picture, audio or video. It can hold several watermarks at the same time. The information is usually a text or logo, which identifies the owner of the media. This digital watermark is a secret code or image that is hidden inside the original image. Steganography is “secret writing”. The steganographic message is integrated invisibly and covered inside other harmless source, it is very difficult to detect the message without knowing its existence and its appropriate encoding scheme. Watermarking is closely related to steganography, but in watermarking the hidden information is usually related to the cover object. Figure 1 explains how watermarking is derived from steganography [13].

![Fig. 1 Types of Steganography](image_url)

III.DIGITAL WATERMARKING – THE PURPOSE

Watermarks serve a wide range of purposes as follows:
a) Ownership Assertion – Protects the ownership rights.
b) Fingerprinting–To avoid unauthorized duplication of copies and its distribution.
c) Authentication and integrity verification – A unique key is used to embed and extract, this verifies the integrity of the system.
d) Content labelling – Extra information like date, place etc can be added.
e) Usage control – Only a limited number of copies can be created.
f) Content protection – Visible watermark makes it very difficult to modify the contents.

However, there is no one technique that can accomplish all the purposes. Depending on the requirement of the application we need to choose the right technique.

IV. APPLICATIONS OF DIGITAL WATERMARKING

Now we identify some of the digital watermarking applications. It’s expected that digital watermarking will have a wide-span of practical applications in digital camera, digital libraries, medical imaging, image databases, surveillance imaging and video-on-demand systems. Some of them are:

1. Copyright Protection : For any new piece of work, we can insert a copyright information as the watermark. This will also help us solve any dispute if in case it arises, as this watermark can provide evidence.
2. Broadcast Monitoring : This will help to check whether any unauthorised data is transmitted or not.
3. Covert Communication: Here exchange of secret information takes place.
4. Tamper Detection :If the watermark of the image is destroyed or degraded, we conclude that the image is tampered.
5. Content Description: Labelling and content information of the host image can be used as a watermark.
6. Authentication and Integrity Verification:Here any small changes in the content can be tested and its integrity can be verified.
7. Owner’s signatures :This helps to eliminate Multimedia piracy
8. Alert Line on TV broadcasts : This application is used during emergency public address
9. Time stamping of digital images 
10. Geo tagging of digital images
11. Saving patient’s data on biomedical images

V.WATERMARK EMBEDDING AND EXTRACTION

Here a binary data sequence is used as a watermark, which is inserted into the host signal with the use of a key as shown in Fig.2. The key and the watermark together generate a watermarked signal, which is embedded into the host signal. This embedding procedure is the most important design challenge which imperceptibly modifies the host signal. It reflects the information content in the watermark so that we can observe if there are any changes later with the use of the key to ascertain the embedded bit sequence. This process is called watermark extraction. For copy protection applications, it should be possible to recover the watermark even when the signal has undergone huge amount of distortion. Also, for tamper detection applications, the watermark should be able to effectively characterize all the signal distortions. A Random key is the most important device to completely secure the system. Without the knowledge of the key it is impossible to extract or forge or remove the watermark effectively.

V. IMAGE WATERMARKING SURVEY

Within watermarking, image watermarking has gained lot of attention within the research community. The reason for this popularity is its ready availability and it carries large amount of redundant information that can be used to embed watermarks. Images can be represented either in spatial domain or transform domain. In spatial domain we make use of pixels to represent the digital image while in transform domain we represent it in terms of frequencies, ie, the image is segmented into many frequency bands. Several reversible transform techniques are available which transfer an image into its frequency domain representation like: Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT).

VI. CLASSIFICATION OF WATERMARKING TECHNIQUES

Today digital watermarking is the most extensively exploited and is regarded as the best solution against illegal duplication or theft of multimedia information. Thus many watermarking schemes have come up and are classified based on the characteristics of the watermarking scheme. Here are some of the watermarking techniques [8]:

A. Based on the robustness of the watermark:

1) Robust watermarks: These can resist non-malicious distortions. Robust watermarks[1] are generally used for copyright protection and ownership verification. They are robust to all types of signal processing operations

2) Fragile watermarks: These can be very easily destroyed by all image distortions. They are used to
detect tampering and authenticate an image as it is sensitive to changes.

3) Semi-fragile watermarks: Minor changes do not destroy such type of watermarks but certain specific distortions destroys the watermark. These are applied for some special cases of authentication and tamper detection.

B. Visible and invisible watermarks:

1) Visible Watermarks: These contain a clear visible message or a company logo. This visible watermarks indicates the ownership details. These [3] are used to protect digital images and videos that have to be released for certain purposes, such as contents used in distant learning web sites or digital library, while illegal copying or reproduction is prohibited. It is impossible to directly use a visible watermarked image unless the watermark is completely removed without destroying visual quality of contents they protect.

2) Invisible Watermarks: These are more widely used compared to visible watermarks. They are imperceptible and do not change the visual quality of the images. The images watermarked with this technique visually look the same like the original image. Invisible watermarks maintains the aesthetic value and privacy of the image. IPR can be protected using this scheme. Here, copyrights of content owners is protected in a passive way. This is done by checking if watermarks are found in questionable contents. Based on the way the watermark is applied, invisible watermarking can be categorized as follows:
   a. Blind detection watermarking: If the watermarking used is known then only it is possible to recover the watermark data.
   b. Non-Blind detection watermarking: Only if the original image is known then it is possible to recover the watermark data.

C. Types of domains:

1) Spatial Domain: Here the pixel valued are changed to encode the watermark signal. Slightly the scheme modifies the pixels of one or two randomly selected subsets of an image. For example the low-order bit of each pixel can be flipped as a part of modification. Some of the techniques are as follows:
   a) Using-Mintzer scheme: Here a logo smaller than the image is considered as the watermark and stretched later to form as big as the image. A lookup table is generated by scanning the pixel and extracted from it with the help of the key. If the extracted watermark bit and the authentic watermark bit are same, then pixel is left as it is else we adjust the pixel till it becomes equal to the authentic one.
   b) Wong’s public scheme: Here, all LSB are set to zero, then image is divided into blocks, Hash function is applied to these blocks followed by XOR operation.

Further, the result is encrypted using private key and embedded with original image.

c) Least Significant Bit Coding (LSB): This is one of the most earliest techniques. This technique embeds watermark data by alternation of certain bits of digital image which are selected based on secret key. For extraction the bit values are read. This technique has high watermark channel capacity. Also the algorithm is less complex with its computations. However there is no robustness, search space is huge and is weak against D/A and A/D conversions.

d) Predictive Coding Schemes: Here the correlation between adjacent pixels is found. First the set of pixels which need to be embedded with the watermark is taken and the difference between the adjacent pixels is used to replace alternate pixels. We can also improve it by adding a constant value to them. A cipher key is used at the receiver end for the retrieval of the embedded watermark. This technique is much more robust when compared to LSB coding.

e) Correlation-Based Techniques: Here a pseudo random noise PN is added to an image and at the decoder the correlation between the two is found. If their value exceeds a certain threshold level then watermark is detected else it is not.

f) Patchwork Techniques: The image is partitioned into two subsets. An operation is chosen and it is applied to these two subsets in the opposite direction. For example if one subset is increased by a factor I, the other subset will be decreased by the same amount.

2) Frequency Domain: These are widely used in image watermarking. These techniques are more robust and can be used to embed more bits than those of spatial domain.
   i. Discrete cosine transform (DCT) based technique: Here a sequence of data points in the spatial domain is converted into a sum of sine and cosine waveforms with different amplitudes in the frequency domain. DCT uses only real numbers.
   ii. Discrete fourier transform (DFT) based technique: This is the most popular technique which is very robust. It gives the phase and magnitude representation of an image. DFT applies to complex numbers.


VI. DIGITAL WATERMARKING: REQUIREMENTS

Depending on the application different properties of watermarking are looked at. Also requirements will vary and hence results in many design issues. These requirements need to be taken into consideration while designing watermarking system. Some of the requirements are as follows:
a. Fidelity measures the imperceptibility of watermark. It gives the degree of similarity between un-watermarked and watermarked images. Here the limitation of human vision is exploited.

b. Robustness: It should not be possible for simple image processing operations to remove watermark intentionally or unintentionally. Hence watermarks should be robust.

c. Data Payload: It is the measure of maximum capacity of watermarking to hide the information without degrading the quality of the image.

d. Security: Both embedding and detection processes make use of a secret key.

e. Computational Complexity: It is the measure of the amount of time the algorithm takes to encode and decode the image.

VIII. ATTACKS

Digital watermarking is not as very secure as data encryption is. Hence, digital watermarking is not at all immune to hacker attacks also. The attacks are broadly classified into Signal Processing Attacks and Geometrical Attacks. Some of the intentional attacks are[11]:

1. Active Attacks: An attempt to completely remove or make the watermark undetectable is done here.
2. Passive Attacks: Only is the watermark is present or not is ensured in this case while there is no harm done to the image.
3. Collusion Attacks: A copy with no watermark is formed by using several copies of one piece of media where each is with a different watermark.
4. Forgery Attacks: The hacker will embed his own valid watermark instead of removing the one.
5. Distortive Attacks: The hacker here degrades the watermark so that it becomes undetectable or unreadable by applying some distortive transformation uniformly over the object.

Watermarking system could be judged against these attacks:

1. JPEG compression: All watermarking system should be resilient to some degree of compression.
2. Geometric transformations: Transformations like Horizontal flip, Cropping, Scaling, color quantization, printing-scanning, noise addition etc

IX. ISSUES AND FUTURE SCOPE

Some of the issues observed from our survey are as follows:

1. Lack of protocols, standards and benchmarking.
2. Lack of comprehensive mathematical theory.
3. Watermark survival for all attacks.
4. No watermarking technique is found on compressed images.
5. Relating robustness, capacity, perceptual quality and security.

6. Color image watermarking, and other multimedia signals. Also, watermarking of maps, graphics and cartoons.

7. Applications beyond copyright protection.

Digital watermarking and its technological advancements should continue to be researched and developed further. The future scope for digital watermarking relies on setting appropriate standards and also creating applications so that creators of digital content can easily implement the same. The study considering various performance parameters and numerous other attacks on the response of the watermarking technique on can be carried out.

XII. CONCLUSION

In last few years, Digital watermarks have thus helped us to protect the ownership of digital data. Now, webmasters and legitimate businesses need not fear from copyright law. Webmasters can freely continue to make sites audio visually attractive, by using audio files and images only when they have obtained permission of the appropriate owner. This paper focuses on the study of robustness of the watermarking techniques chosen from all the three domains of watermarking. Some of the issues have been observed and these challenges can further be extended to the enhancement of digital watermarking.

REFERENCES


