A Brief Survey on Image Watermarking Using Frequency Domain Techniques and Attacks

Mrs. Sonali Sharma[1], Dr Nirupma Tiwari[2], Asst.Prof. Madhavi Agrawal[3]
[1]Dept of Computer science & Engineering
[2]Associate Professor, Dept of Computer science & Engineering
[3]Assistant Professor, Dept of Computer science & Engineering
[1, 2, 3] SRCEM, Banmore, Morena, MP

Abstract- *Image watermarking are gaining more popularity as Web and multimedia applications are commonly used. Photo watermarking adds logo / audio / video or text information about the host photo. Water marking's main objective is to provide protection of copyright, authentication of information, identification of ownership, integrity of data. It starts with description, implementations, watermarking properties, classifications, general model, methods, specific attacks, and watermarking quality performance metrics.*

Keywords- Image Watermarking, Techniques, Types of Watermarking, Feature, Attacks, Applications.

I. INTRODUCTION

Privacy and security are currently the world's biggest problem. A primary requirement is data authentication [1].The data including pictures, video, audio, etc. can be multimedia in digital watermarking. Watermarking technology protects data from unauthorized misuse; in short, it is a means of providing protection of information through the handling of the original data. The optical signal is called the host signal. To order to provide secure information to avoid data modification or reuse (video, audio, photography, etc.), the digital information or message placed on the digital signal includes the owner's data itself. We should have found some important fact for the improvement of copyright protection: the use of watermarking should not affect quality of original data, watermarking should be accurate ,reliable, and a non-authorized distributor must not omit and use watermarking. This means that only approved persons can detect watermarking.

Particular emphasis is placed on general watermark problems embedding the issue of stego image stability into transformations, which can lead to embedded data distortion. Digital watermarks can be obtained in different ways and depicted in different graphics. There are many renowned ways to mark the water, such as the LSB form, blocking and additive embedding where bit display and embedding in gray planes and others are used.

An example of a gray plane-based steganographic system based on the Grey codes is described in the Digital Image[2].

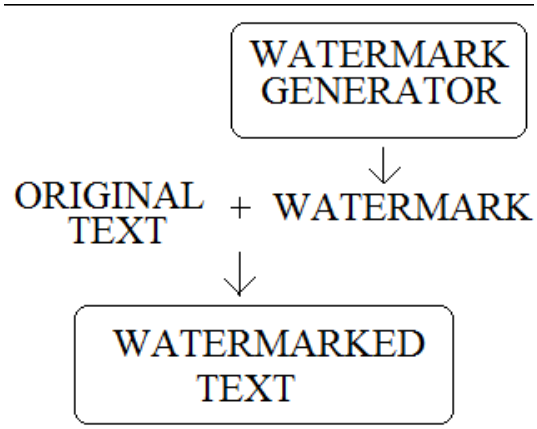

Figure 1. Process of watermarking [3]

Watermarking requires main features [4]:

A. Capacity and data payload: The watermark system capacity is specified as the maximum number of data to be integrated in the cover file. Data payload of number of watermarked bits is called a message, and a record for maximum data payload events is called the watermark capacity.
B. Robustness: The survival potential of watermarks after different operations or aggressions.
C. Imperceptibility: It is not possible to see watermark by the human eye or to listen to the human ear, special processing or special circuits should only be known.
D. Verifiability: Watermark must be able to prove proprietary ownership of information with valid evidence.
E. Computational Cost: Watermark should be in a capacity to provide credible copyrighted evidence of ownership of content.
F. Security: Watermark should be provided by less complicated algorithms and low computational costs.

II. TECHNIQUES OF IN IMAGE WATERMARKING

Digital watermarking techniques are categorized by form of document as:

- Image Watermarking
- Audio Watermarking
- Text Watermarking
- Video Watermarking

Based on human perception they are classified as:

- Invisible Watermarking[5]
- Visible Watermarking[5]

A. Fragile Watermark Image can be detected but region where image was modified cannot be determined. Where completeness is essential, fragile watermarks are used. Unless some modification is made, Cannot detect this kind of watermark.

B. Semi-fragile watermark The robustness and features of this watermark are robust and delicate. It can detect data that changes transformations.

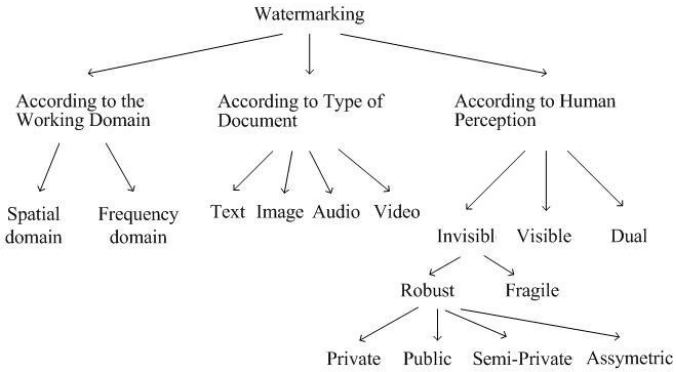

Figure 2. Types of watermarking [6]

There are many frequency domain methods:

Discrete Wavelet Transform (DWT) domain The image is divided into four parts the portion is a low frequency image, and the one below left is vertical picture information, the one above right horizontal image data, and the one at the bottom right high frequency. High frequency A multidimensional image transforms into one DWT.

The transform move grade by grade and model DWT decomposing is shown in Fig. 3.

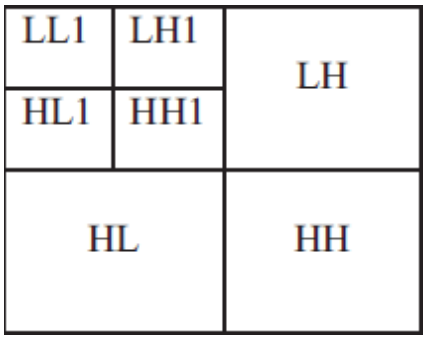

Figure 3. DWT watermarking [7]

Discrete Cosine Transform (DCT) domain Technique of DCT is use if image data signal is not changed but only the signal display is changed to a different form. The DCT technique is usually broken up into two phases: the Global DCT technique; and the DCT technical technique, which is based on blocks. The method of Global DCT is conducted throughout the picture while the image in the DCT block is segregated. Three types of frequency bands are formed in the form of low frequency, medium frequency and high frequency bands after each block test. Nevertheless, the watermark is typically used for the mid-frequency band. Because in addition to several watermarking attacks, it offers robustness, since the low frequency band contains all important information on picture so that the watermark cannot be added. When this happens, the image brightness and image quality is affected. [8].

Table I. Comparison of Techniques [5]

Method	Advantages	Disadvantages
Hamming codes & Color image watermarking using repetition codes	Resistant to Salt & Pepper noise	Less perceptual quality
DCT based watermarking	High robustness to JPEG Compression attack	Large overhead, Not resistant to geometric attacks
DWT based Watermarking	Strong Robustness	Frequency changes decrease robustness
DCT-DWT based hybrid method	Strong Robustness, Good Imperceptibility	Increased complexity of Method, Extraction is Not good Enough

III. LITERATURE SURVEY

Ponni et al. [9] Proposed a new video watermarking, secure and stable, with DWT and SVD, based on the chaotic diagram. proposed use method achieve the imperceptibility and robustness of video watermark and extracted watermark. Confidentiality of embedding location is assured which chaotic key technique. The SVD method is used to provide stability and achieve robustness, DWT for localization. The time complexity of embedding and extraction is reduced by watermark embedded in key frame. The result of proposed method gives perceptual quality of the video as well as watermark also proves well in security and capacity.

Jianfei Li et al. [10] discuss a new design idea of embedding watermark which is to embed the watermarking information into the last DC coefficient of the last macro block in every slice in the luminance component. The result of method shows that it reduced complexity of the video watermarking system, the video's quality and bit rate of the video stream remain stable, and it can extract watermarking information without distortion. The watermark is used in the DC coefficients, because just a bit of watermarking information is embedded in a slice of a frame, so it can solve the blocking effect which may be caused by embedding watermark in the DC coefficients.

Sudhanshu et al. [11] the two-component combined i.e. A watermarking DWT-DCT is planned. The combination of two watermarks for the frequency domain provides authenticity and copyright. The aim of the analysis is to ensure that the watermark is secure and checks are safely transferred from the branch home bank with Check system to branch clearing house. The advanced encryption standard is employed in this experiment to provide protection for watermarked images using a 256 bit key. PSNR against different attacks is the same, with the exception of the harvesting attack for watermarked images. Discrete transform wavelet is a Jpeg 2000 kernel technique. Discrete transform cosine is useful for the method of compression. It prevents compression attacks from Jpeg due to this property. This helps to keep the original image imperceptible and the watermark stable. The watermark ruggedness is obtained 99 percent against any attack, for cropping, using two different techniques in this combination. But robustness of the watermark against rotational attacks is 87 percent.

Mahmoud et al. [12] Proposed a scanned colored pdf files watermarking technique. A watermark has been introduced into scanned PDF files in this technique. The main objective is to secure the security and ownership of PDF documents. A logo was used and inserted into the green channel of the file as a clear watermark for copyright. Successfully eliminating the watermark. The machine survived multiple assaults. Some manipulations in the PDF file have changed the second fragile watermark and suggested falsification. The algorithm has been tested successfully in various colored PDF files.

Mohammad Moosazadeh [13] YCoCg-R presented space for the watermarking algorithm for optical image. YCoCg-R color space thryplet components have a good relationship and changing one component affects the other two color components least. It allows the watermarking to be more reliable against specific assaults.

Sudhanshu Suhas Gonge[14] Digital still image has been suggested to be used for experimental purposes. Protection and copyright protection services are provided by the techniques and algorithms are diverse DCT and DWT digital watermarking technology has been use in order protection of copyright and the AES technology can provide copyright and security service using a 256-bit key. Electronic watermarking and AES safety are a mixture that provides durability, copyright and electronic protection against attacks, including cropping, The noise of Gaussian, salt and pepper, JPEG, filtration medium and rotation.

IV. PERFORMANCE MEASURE

There are two phases of the general watermarking diagram of integration and extraction phases as shown below in figure 4 and 5.

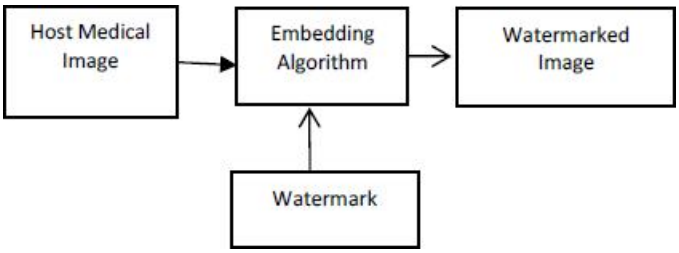

Figure 4: Image watermarking Embedding Process [15]

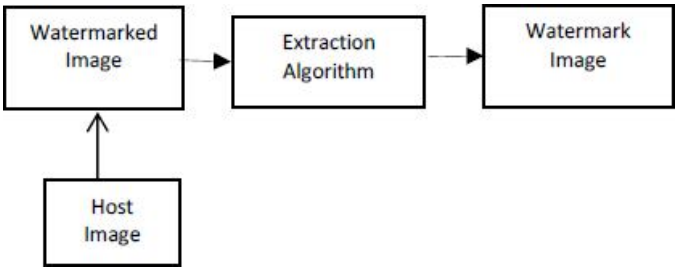

Image quality measurement using Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) Instruments for measuring. MSE and PSNR are able to calculate the

comparison of the picture cover with a watermark image. This is the equation for calculating the MSE value.

$$MSE\ x = 1\ ||x - x\hat{}|| 2 = 1\ n\ (x - x\hat{})^2$$

Calculate PSNR and MSE value of watermarked image and cover image.

Digital watermarking allows effective content identification by providing a novel digital into all or any varieties of media content in an exceedingly means that persists with the content where it should travel.Digital watermarks are simply embedded into content without intrusive with the consumer‟s enjoyment of it.
It is invisible humans, however simply detected and understood by computers; networks and a large vary of common digital devices. The watermark will carry such data, equivalent to the owner identity, however it should be used or anything the owner desires to convey. It can also predefine actions, together with linking to websites or alternative consumer experiences. Content identification helps:

- Consumers to search out the content they are trying to find, learn a lot of regarding it, try it out, and find wherever and the way several to get it.
- Copyright owners, brands and distributors to locate and find out about however, once and wherever content is being unknowingly or purposely makes its approach onto the

Where x is cover image, x^ is watermarked image, N is the size of the cover image

$$PSNR\ x = \frac{10\ X\log\ ((255))}{MSE(x)}$$

Where m is the maximum value of the cover image

Maximum value for an image of 8-bit pixels is 255. High PSNR values can create the cover picture can well store good eye imperceptibility or messages.

V. APPLICATIONS

In the following, several existing areas of technology and reference technologies are clarified and case studies are provided to illustrate some of the most common situations in the real world. most of the shown examples apply to the watermarking of digital images, but often are used in other media, such as audio or video streams. [16]

A. Copyright Protection The first area of use for this watermarking is the protection of digital media through copyright. Almost everyone can replicate or exploit digital information in the digital world without losing quality. This has allowed copyright violation issues previously unseen. Digital watermarking adds an additional safety layer to the Content Chain to prevent unauthorized use or replication of content through the embedding of watermarks which provide the original media and the permissible content usage. In this case, devices scan the watermark during the replication or copying of the text. If the watermark says the application is unauthorized, the replication or copying is prevented as well as the informative message. Good content protection protects content, copyrights and uses consumer rights in tandem with the TV network to protect it from that piracy threats.

B. Content filtering The data contained in the digital watermark is easily connected to different materials or actions. On the one hand, when the watermark is detected, a specific action or perhaps some content is activated to allow customer interactivity. For instance, when experiencing a scene in a picture can cause a specific decision. A targeted ad can also be activated. Likewise, rather than a commercial showing at regular times.

VI. ATTACKS IN WATERMARKING

A watermark object is likely to experience many potential intentional or unintentional attacks. The wide range of image processing applications has allowed robust watermarking systems for attack. The purpose is to prevent the watermark from achieving its desired goal[4].

A basic introduction to different types of watermark attacks is as follows,

A. Forgery attack Deletion are similar to the replacement of scene context transformations and the forgery attacks that result in object input.

B. Low pass filtering attack The low pass filtering results in a noise-based variation diagram variation diagram.

C. Geometric attack All manipulations that concern geometry of image such as, , cropping, flipping, rotation etc. An example of this attack should be cropping assault on right and bottom of image.

D. Removal Attack Removal attacks propose the removal from a watermark object of the watermark data. These attacks use the knowledge that an additive noise sign in the host signal is the watermark typically.

E. Interference attack Attacks add additional water-marked noise to the target. Lossy compression, averaging , consent, continuation, remodulation, denoising , and noise storm is some examples of attacks of this kind.

F. Security Attack In particular, an attacker can further attempt to make changes in order to invalidate watermark or to estimate , alter watermark if a watermarking algorithm is found. In this situation, we are talking about a security threat. If embedded information is not impaired, detected or fabricated, the watermarking algorithm will be secure.

VII. CONCLUSION

A complete description of digital watermarking images techniques is provided here. Many new techniques for digital watermarking to help the security of Internet users against copying are given. These techniques are categorized according to area, document and interpretation in which the secret data are incorporated and extracted in a series of categories. This survey shows altered robustness rates for isolated attacks in various digital watermarking techniques. We attempted to provide complete knowledge on digital watermarking in this paper, to enhance awareness among new investigators in this area.

REFERENCES

[1] Neha Agarwal, Subodh Gupta, Sandeep Gupta," A Comparative Study on Discrete Wavelet Transform with Different Methods", 2016 IEEE, CDAN, pp 1-6.
[2] Valery Gorbachev, Elena Kaynarova, Anton Makarov, Elena Yakovleva," Digital Image Watermarking Using DWT Basis Matrices",IEEE 2017, ISSN 2305-7254, pp 128-133.
[3] Sameeka Saini," A survey on watermarking web contents for protecting copyright", ICIIECS'15, pp 1-4.
[4] Prabhishek singh, R.S Chadha (2013) A survey of digital watermarking technique, application and attacks. IJEIT volume 2, Issue 9, 165-175.
[5] Urvi H. Panchal, Rohit Srivastava," A Comprehensive Survey on Digital Image Watermarking Techniques", 2015 Fifth International Conference on Communication Systems and Network Technologies, pp 592-595.
[6] Uma Rajput, Nirupma Tiwari," A novel technique for RGB Invisible Watermarking Based on 2-DWT-DCT Algorithm", GCCT 2015 IEEE, pp 386-390.
[7] Nirupma Tiwari, Manoj Kumar Ramaiya, Monika Sharma," Digital Watermarking using DWT and DES", 2012 IEEE (IACC), pp 1100-1102.
[8] Dimple Bansal, Manish Mathuria," Color Image Dual Watermarking using DCT and DWT Combine Approach", ICEI 2017, pp 630-634.
[9] Mingwei Zhao and Yanzhong Dang, "Color Image Copyright Protection Digital Watermarking Algorithm Based on DWT & DCT," IEEE, 2008, 978-1-4244-2108-4/08
[10] Mohammad Nuruzzaman, "Digital Image Fundamentals in MATlAB,"AuthorHouse 08/23/05, ISBN 1-4208-6965-5 (sc), 2005.
[11] Munesh Chandra, Shika Pandey, Rama Chaudhary, "Digital Technique for Protecting Digital Images", 978-1-424- 5540-9/10, IEEE, 2010.
[12] Dr. Neeraj Bhargava, Dr. M. M. Sharma, Abhimanyu Singh Garhwal and Manish Mathuria, "Digital Image Authentication System based on Digital Watermarking," IEEE Conference Publications of ICRCC, pp.185-189, 2012.
[13] Mohammad Moosazadeh, Gholamhossein Ekbatanifard, An Improved Robust ImageWatermarking Method UsingDCTand YCoCg-R Color Space,(2017), http://dx.doi.org/10.1016/j.ijleo.2017.05.011.
[14] Sudhanshu Suhas Gonge, Ashok A.Ghatol," An Enhancement in Security and Copyright Protection Technique Used for Digital Still Image", ICNTE-2017, IEEE, pp 1-9.
[15] Priyanka Verma, Ritulika Ghosh Dastidar, Sheetal Jain, Sneha Potghan," Comparative Analysis of Conventional 2-Level DWT and Color Plane Watermarking for Telemedicine Applications", TEL-NET 2017, pp 1-8.
[16] M.Hariharalakshmi1, Dr.M.Sivajothi2, Dr.M.Mohamed Sathik3, "Survey of Digital Watermarking techniques for Data security", Vol. 5, Issue 3, March 2017, IJIRCCE, pp 4369-4377.