A Review of Image Watermarking on Different Methods with its Applications

Suniti Bhadouria[1], Prof. Nirupma Tiwari[2]
[1, 2] Department of CSE
[1, 2] ShriRam College of Engineering & Management, Banmore, India

Abstract- *Watermarking is process to hide some secret data in a cover file. Watermarking is a notion intently related to steganography. In these, both hide information in an image. The information hide in this is in different forms like an image, song, video within the signal itself. We have study comparative analysis of various approaches that may positive and negative of these techniques. This comparison can further be used to improvise and propose of few new techniques for the same.*

Keywords- Applications, Techniques, Watermarking.

I. INTRODUCTION

Present day generation is witness of digital media improvements. Using phone camera capture a photo is a simple example. The use of Digital media is common in present era. Text, audio, video are other digital media example.

We know an internet is the fastest medium of transferring data to any place in a world. This method can be using to every digital media types such as image, audio, video and documents. From many years researchers and developers worked in this area to gain best results [1].

The paper is organized as follows sections:

- Overview of Image watermarking including history of watermarking
- Types of Image watermarking techniques in detail
- Classification & Applications of watermarking
- Threats for Image watermarking

Fig.1. A watermark image

II. BASIC OF WATERMARKING

Digital Image Watermarking contain of two parts:
1. Watermark embedding
2. Watermark extraction

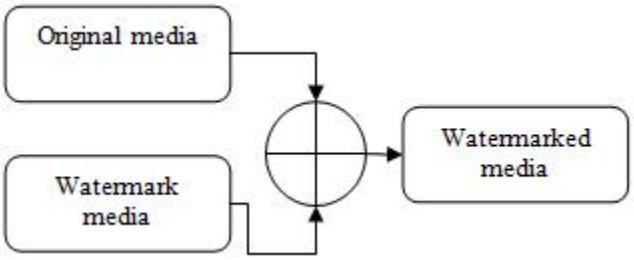

Fig. 2 Watermarking embedding process

The first process is Watermark Embedding that is shown in Figure 2 and the second process is the Watermark Extraction that is shown in Figure 3.

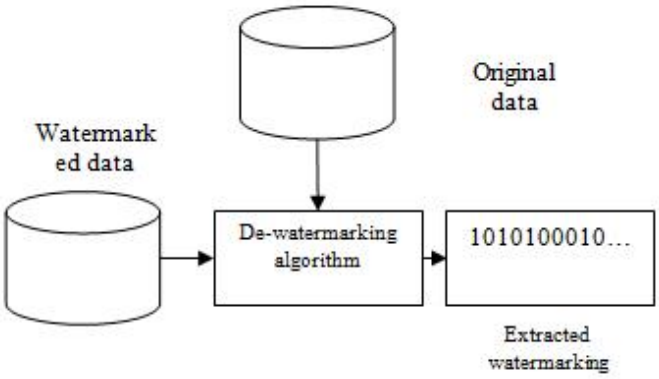

Fig. 3. Watermarking extraction process

Watermark Embedding is the embedding watermark process into the original image which is the final output of watermark image [2].

III. TYPES OF WATERMARKING

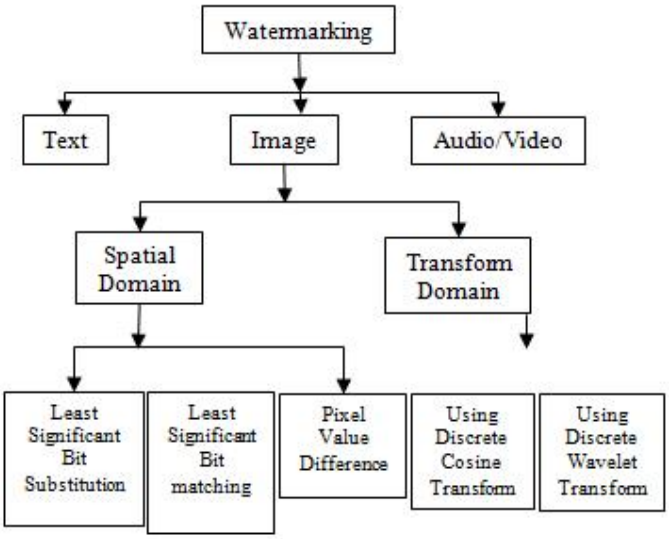

Fig. 4. Watermarking types

Watermarks and watermarking process can be divided into a categories variety in various ways [10].
1) Text Watermarking
2) Image Watermarking
3) Audio Watermarking
4) Video Watermarking [3]

In other way, the digital watermarks can be divided into four different types as follows:
I. Visible watermark
II. Invisible watermark
III. Fragile watermark
IV. Robust watermark

IV. WATERMARKING TECHNIQUE

There are some watermarking technique is:

A. Spatial Domain Techniques

Some pixels modifies in spatial domain technique which is selected by image subsets. Modifications might conclude flipping the all pixel low-order bit. However, this procedure will not be reliable for example filtering or lossy compression. Numerous spatial domain techniques are as follows:-

- **Least Significant Bit Coding (LSB)**

LSB coding is one of the earliest techniques. It is substituted with watermark. At the time of encryption first select that pixel which is embedded. It is simple method but it's robustness is too low.

- **Predictive Coding Schemes**

In this technique correlation between the various adjacent pixels are exploited. A cipher key is generated which enables embedded watermark retrieval at the receiver. This is much additional robust as compared to LSB coding.

- **Correlation-Based Techniques**

In this technique a Pseudo random noise (PN) with a sample W(x, y) is delivered to an image. At the decoder the correlation between random noise and image is discovered and if the value exceeds an exact threshold worth the watermark is detected else it isn't.

- **Patchwork Techniques**

One subset is increased by a factor k, the other subset will be decreased by the same amount. If a[i] is the value of the sample at I in subset 'A' which is increased and b[i] is the value of the sample in the subset 'B' whose value is decreased, then the difference between the two subsets would intuitively result in
$\Sigma(a[i]-b[i]) = 2N$ for watermarked images
$1<=N<=\infty$
$= 0$ otherwise

B. Frequency Domain techniques

In protected image hide some information in lower and middle frequency domain, because the advanced frequency portion is additional likely to be suppressed through compression. But how to select the best image frequency portions for watermark is another important and challenging topic. Numerous frequency domain methods are as follows:-

- **Discrete cosine transform (DCT) based technique**

It is a procedure which converts data points sequence in the spatial domain to sine and cosine waveforms combination with various amplitudes in the frequency domain.

- **Discrete Fourier Transformation (DFT) based technique**

It is translation invariant and rotation resistant, which translates to robust robustness to geometric assaults. DFT makes use of elaborate numbers, even as DCT uses simply real numbers.

- **Discrete wavelet transform (DWT) based technique**

DWT-based approaches enable better spatial localization and have multi resolution characteristics, which are similar to human visual system. Also this method presents robustness to median filtering and low-pass. However, it is not robust to geometric transformations.

C. Wavelet Transform based Watermarking

The wavelet transform based watermarking method divides image into four different sidebands – a low resolution approximation of the tile component and component's horizontal, vertical and diagonal frequency characteristics. The procedure can then be repeated iteratively to produce N scale transform [4].

V. REQUIREMENT OF DIGITAL WATERMARK

The common requirements in digital watermarking are closely related to its purpose of applications, different application has different demands. In general, digital watermarking requirements are as following:

A. Robustness:

Robustness refers to that watermark embedded in information has the surviving ability after processing operations variety and attacks. The watermark for copyright protection does need strongest robustness.

B. Non-perceptibility:

Generally invisible watermark cannot be seen through eye but it can be detect by de-watermarking process.

C. Verifiability:

Watermark should be able to provide complete and reliable evidence of copyright and data products ownership. It is used for data protection purposed and also provide user authentication.

D. Security:

Watermark data process provide user secure authentication by sign in, only authorized users can legally detect, extract and even watermark modify, and thus be able to attain copyright protection purpose.

E. Capacity:

Capacity of image watermarking is estimation that of how much secret data can be hidden in a digital image. Watermarking capacity is define through the statistical model used for the host image, by the distortion constraints on the information hider and the attacker, and by the data available to the data hider, to the attacker, and to the decoder [5].

VI. APPLICATION OF DIGITAL WATERMARKING

There are many digital image watermarking applications. In this part, some areas of application for digital watermarking are discussed:

A. Copy Control:-

Watermark may include knowledge required through the content owner that decided the digital content copying policy. The data contained through watermark may specify "content may not be copied‟ or „only one copy‟ etc.

B. Digital Signatures:-

Watermarks may be used to the content owner identify. By having this knowledge user may contact the owner for acquiring the legal rights to copy or applying the content.

C. Authentication:-

A secure authentication provide by watermarking process. Providing an incorrect watermarked picture can either break the watermark or results in wrong watermark after extraction.

D. Broadcast Monitoring:-

Automatic data owners identification may be need to be complete and utilized in systems accountable for monitoring the proclaims.

E. Fingerprinting:-

When a digital media is distributed, it can be include hidden and imperceptible knowledge about user, which can be detected using watermark detector. Thus a licensed copy belonging to a particular user can be ascertained. This also resolves possible conflicts as regards to digital or intellectual property ownership. This thing is referred to as "Fingerprinting".

F. Secret communication:-

Several public domain and shareware programs are available which use watermarking for secret communication. Looking at the important watermarking applications, it becomes very important to enhance the watermarking techniques for providing better "robustness", "fidelity", "payload" while preserving the "authenticity" aspect of watermarking [6].

VII. DIFFERENT CRITERIA OF DIGITAL WATERMARKING

Table I. Types of Watermarking Basis of Different Criteria [7]

S.no	Criteria	Classification
1	Watermark Type	1. Noise: pseudo noise, Gaussian random and chaotic sequences 2. Image: Any logo, Stamp Image etc.
2	Robustness	1. Fragile: Easily Manipulated 2. Semi-Fragile: Resist from some type of Attacks 3. Robust: not affected from attack
3	Domain	1. Spatial: LSB, Spread Spectrum 2. Frequency: DWT, DCT, DFT, SVD
4	Perceptivity	1. Visible Watermarking: Channel logo 2. Invisible Watermarking: like Steganography
5	Host Data	1. Image Watermarking 2. Text Watermarking 3. Audio Watermarking 4. Video Watermarking
6	Data Extraction	1. Blind 2. Semi-Blind 3. Non- Blind

VIII. LITERATURE SURVEY

MANISHA PENDYALA (2016) et al present that Spatial domain technique is utilized taking advantage of it low computational complexity. The initial stage of approach is accomplished by building the algorithm on MATLAB R2014a© platform and then shifting the base to ISE Design Suite 14.7© platform. The VLSI implementation of the spatial domain Watermarking algorithm is targeted on device xc5vlx50t-1ff1136 of Virtex-5 family. The robustness of the Watermarking algorithm is verified by attacking the Watermarked image with various types of noise, compression, transformation and geometrical attacks [8].

R. Surya Prakasa Rao (2016) et al present that Proposed GA based scheme of Digital Image watermarking is enhanced through embedding the watermark in original image Third Level DWT, after using SVD to watermark image. The GA is used for best SF to alter watermark image SVD coefficients. The NCC and PSNR used as fitness function in GA and it estimate watermarking method Imperceptibility and Robustness. Experimental outcomes are provided to illustrate that the proposed method is able to withstand image processing attacks variety very well and comparison is made with previous work [9].

Thottempudi Pardhu (2016) et al present that performs imperceptible watermarking of images in frequency domain. In the decoding phase, once watermark is extracted from the watermarked image, certain performance measures for example PSNR and correlation are calculated [10].

Tamirat Tagesse Takore (2016) et al present that an improved blind image watermarking algorithm applying DWT, DCT and SVD is proposed in this paper. One level DWT operation is achieved on original host image applying Haar wavelet and approximation (LL) sub-band is selected to split it into two sub images. SVD and DCT operations are achieved in both sub images applying 8x8 block size [11].

N. SenthilKumaran (2016) et al present that algorithm is verified on different watermarking images. And it's providing robust and secure results. To measure the effectiveness of this algorithm is provide embedding and extracting images. PSNR and MSE also calculated the embedding watermarking images. In this DWT watermarking embedding result images provide the good, secure and robust. In this paper proposed to how to process LSB technique [12].

C. N. Sujatha (2016) et al present that objectives of digital watermarking techniques are capacity, robustness and imperceptibility. In all the proposed watermarking schemes, imperceptibility and robustness are estimated by measuring Peak Signal to Noise Ratio (PSNR) and Correlation Factor (CF). And this paper conveys the potency of the existing algorithms against various attacks [13].

VIII. CONCLUSION

Digital media is the need of a people now a day as the alternate of paper media. Watermarking approaches have been developed to fulfill this requirement. In this paper, we present the survey on digital image watermarking. In this paper, we also explain the watermarking types and various watermarking techniques and also we explained the digital watermarking requirements.

REFERENCES

[1] Lalit Kumar Saini and Vishal Shrivastava," A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and

Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014, pp:70-73.

[2] Ruchika Patel and Parth Bhatt," A Review Paper on Digital Watermarking and its Techniques", International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 1, January 2015, pp: 10- 13.

[3] Jaishri Guru and Hemant Damecha," Digital Watermarking Classification : A Survey", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, Sep-Oct 2014, pp:8-13.

[4] Sasmita Mishra, Amitav Mahapatra and Pranati Mishra," A Survey on Digital Watermarking Techniques", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 451-456

[5] Manjinder Kaur and Varinder Kaur Attri," Survey on Digital Image Watermarking and Its Techniques", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 8, No. 5 (2015), pp. 145-150.

[6] Chauhan Usha and Singh Rajeev Kumar," Digital Image Watermarking Techniques and Applications: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016 pp. 533-540.

[7] Sunanda Datta and Dr. Asoke Nath," Data Authentication using Digital Watermarking", International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 12, December 2014 pg. 30-45.

[8] MANISHA PENDYALA and ANIKET GOKHALE," Design of a Spatial domain Watermarking technique with VLSI Implementation", 2016 Conference on Advances in Signal Processing (CASP) Cummins College of Engineering for Women, Pune. Jun 9-11, 2016

[9] R. Surya Prakasa Rao and Dr. P. Rajesh Kumar," An Efficient Genetic Algorithm Based Gray scale Digital Image watermarking for Improving the Robustness and Imperceptibility", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016, pp: 4568- 4571.

[10] Thottempudi Pardhu and Bhaskara Rao Perli," Digital Image Watermarking in Frequency Domain", International Conference on Communication and Signal Processing, April 6-8, 2016, India

[11] Tamirat Tagesse Takore, Dr. P. Rajesh Kumar and Dr.G.Lavanya Devi," A Modified Blind Image Watermarking Scheme Based on DWT, DCT and SVD domain Using GA to Optimize Robustness", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016, pp: 2725- 2729.

[12] N. SenthilKumaran, and S. Abinaya," Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique", International Conference on Communication and Signal Processing, April 6-8, 2016, India, pp: 0448- 0451.

[13] C. N. Sujatha and P. Satyanarayana," Analysis of Robust Watermarking Techniques: A Retrospective", International Conference on Communication and Signal Processing, April 6-8, 2016, India, pp: 0336- 0341.