A Survey on Digital Image watermarking

Er. Sonia, Er. Naresh Kumar Garg, Er. Gurvinder Singh

Abstract-Digital Watermarking is a technique which is used for concealing the information in any document for its copyright protection. The purpose of digital watermarking is to embed information imperceptibly and robustly in the host media. Confidential information of owner that is inserted into host media is known as watermark. The digital watermark may be used to verify the authenticity or integrity of the signal or to show the identity of its owners. In this paper, its objectives, characteristics, types and various techniques that are implemented for copy control are introduced. Various types of attacks and different fields where digital watermarking is applied are also discussed in this paper.

***Index Terms*—DCT, DFT, DWT, Host Image, Watermark Image, Watermarked Image.**

I. INTRODUCTION

A digital watermark is a digital signal in form of pattern of bits that is inserted into the host media such as an image or audio or video file. The bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated [6]. The name “watermark” is derived from the faintly visible marks imprinted on organizational stationery. It contains important information for the owner like that producer's name, company logo etc. The watermark is extracted later to get information about the host media. There are two essential characteristics for watermarking, the first is inserting watermark should not change the quality and visually of the host image. The second is robustness. It means that the attacker can’t remove watermark form host media [1]. In general, any watermarking scheme consists of three parts [1] [8]:

i. Watermark: It is pattern of bits that are inserted into host media.

ii. Encoder (marking insertion algorithm): It insert watermark into host media. Each owner has a unique Watermark or an owner can also put different watermarks in different objects. The marking algorithm incorporates the watermark into the object.

iii. Decoder and comparator (verification or extraction or detection algorithm): It authenticates the object determining both the owner and the integrity of the object. It extracts the watermark from the host media using extraction algorithms.
A simple example of a digital watermarking would be a visible “seal” placed over an image to identify the copyright. However the watermark may also contain additional information including the identity of the purchaser of a particular copy of the material [6].

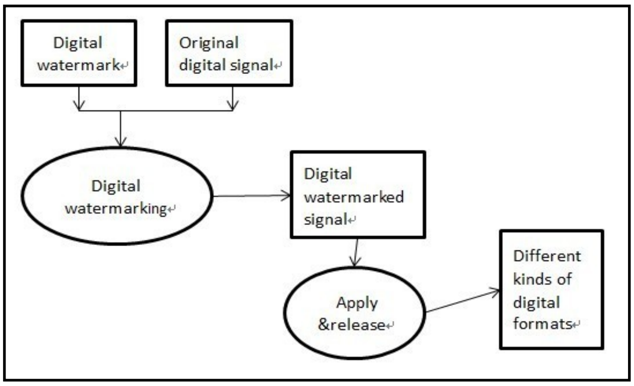

Fig. 1: Watermarking Process

II. PURPOSES

- Purpose of digital watermarks is to provide copyright protection for intellectual property that is in digital format [1].
- Digital Watermarking is used to avoid illegal copying of images [1].
- The digital watermarking embeds the information in host image for hiding the data [8].
- The quality of the host image after watermarking should not be degraded [8].
- The purpose of inserting digital watermark into host image is identifying the source, author, creator, owner, distributor or authorized consumer of a document or image [10].
- The watermark should be robust. It means it can’t be removed by the attacker [2].

III. CHARACTERISTICS

A watermark should have following characteristics [2]:

A. Robustness: Watermark should be cumbersome to remove, to detect or to damage. Robustness measures immunity of watermark against any type of attacks like compression, filtering, rotation, scaling, and collision, resizing, cropping etc.

B. Imperceptibility: It measures the quality of host image should not be degraded when watermark is inserted in host image.

C. Capacity: It measures the capacity of embedded information in large amount.

Er. Sonia, *M.Tech Student, Computer Science & Engg.*
G. Z. S. P. T. U. Campus, Punjab, India..
Er. Naresh Kumar Garg, *Assistant Prof., Computer Science & Engg.*
G. Z. S. P. T. U. Campus, Punjab, India.
Er. Gurvinder Singh, *Assistant Prof., Electronics & Comm. Engg.*
G. T. B. K. I. E. T. Punjab, India.

D. Blind Watermarking: Watermark can be extracted from watermarked image in the absent of original image. Because original image cannot be easily available.

E. Unobtrusive: It is required that watermark should be perceptually invisible.

F. Universal: The same digital watermarking algorithm should be applicable for all three media. This is potentially helpful in the watermarking of multimedia products. This feature is desirable.

G. Unambiguous: Retrieval of the watermark should recognize the owner without any ambiguity

IV. TYPES OF DIGITAL WATERMARK

A. Visible digital watermark: A visible watermark is a visible semi-transparent text or image that is laid on the host image. It allows the host image to be viewed, but it still provides copyright protection by marking the image as its owner's property. Visible watermarks are more robust against image transformation. Thus they are preferred for strong copyright protection of intellectual property that's in digital format. A visible watermark clearly identifies the cover object as copyright-protected material [8].

B. Invisible watermark: An invisible watermark is an embedded image which cannot be seen with human's eyes. Only electronic devices or specialized software can extract the hidden information to identify the copyright owner. Invisible watermarks are used to mark a specialized digital content (text, images or even audio content) to prove its authenticity [8].

C. Fragile watermark: A fragile watermark is destroyed if anybody tries to tamper with the object in which it is embedded. A digital watermark is called fragile if it becomes fail to be detectable after the slight modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are noticeable and commonly are not referred to as watermarks but as generalized barcodes [7].

D. Robust watermark: A digital watermark is called robust if it resists any kind of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information. It is difficult to remove from the object in which it is embedded.These watermarks cannot be broken easily. Robust watermark should remain intact permanently in the cover image. If we try to remove robust watermark then quality of image will be degraded [3] [8].

V. CLASSIFICATIONS OF DIGITAL WATERMARKING

There are following classifications of digital watermarking according to domain of watermark insertion:

A. Spatial Domain Technique: In spatial domain technique, the watermark is embedded by modifying the pixel values of the host image directly. The images are generally manipulated by changing one or more of the bits of the byte that make up the pixels of the image. Generally, spatial domain watermarking is easy to implement from a computational point of view [1].The most commonly method in the spatial domain technique is the least significant bit (LSB). In this, least significant bit (LSB) of each pixel of host image was modified to embed the secret message [3]. LSB algorithm is very simple, strong, real time, embedded stack information. The embedding of the watermark is performed by choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. It is based on the substitution of LSB plane of the host image with the given watermark of the image. This technique uses the entire host image to store the watermark [7] [11] .Watermark is extracted by performing the extraction of least significant bit of each of the selected image pixels. If the extracted bits match the inserted bits, then the watermark are detected [7].This technique is robust to attacks like cropping, noise, lossy compression, etc. But an attack that is applied on a pixel to pixel basis can fully uncover the watermark, which is the major drawback [7].

B. Transform or Frequency Domain Technique: There are three main methods of data transformation such as Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT). In transform domain technique, the watermark is inserted distributive in overall domain of an original data. Here, the host image is first transformed into frequency domain by transformation techniques. The transformed domain coefficients are then changed to store the watermark information. The inverse transform is finally applied in order to obtain the watermarked image. In subsample based watermarking technique, DCT coefficients of the sub images were utilized to store the watermark. The method was considered complex and having high computations. However, the method was robust against attacks than spatial domain methods. Embedding the watermark image in three times can be at three different frequency bands, namely, low, medium and high. The watermark cannot be totally destroyed by either low pass, medium or high pass filter. The main advantage obtained from these techniques is that they can take benefits of properties of alternate domains. Generally, the main drawback of transform domain methods is that they have higher computational requirement [7] [12].

VI. ATTACKS ON DIGITAL WATERMARKING:

The attacks against the watermark attempt to neutralize the watermark, without damaging the image too much. The watermark is neutralized if the detector cannot detect the watermark (distortion, attenuation etc.), the detector cannot recognize the watermark in the image from another one, and the watermark is no longer in the image [1]. In the field of digital watermark, there are various categorizations of attacks on watermarks [2] [10].

A. Subtractive Attack: In this attack, the malicious user attempts to detect the presence, location of the watermark and tries to extract it from the host.

B. Distortive Attack: In this attack, an adversary user degrades the watermark by applying some distortive transformation uniformly over the object in order to make watermark undetectable.

C. **Additive Attack**: An adversary or malicious user can add his own watermark in the host. An effective additive attack is one in which adversary's mark replaces original mark completely. So that it cannot be extracted original watermark.

D. **Filtering:** This type of attack dramatically affects the performance but does not degrade the watermark images.

E. Cropping: In this type of attack, attacker show his interest in small portion of watermarked object such as parts of a certain picture or frames of a video sequence.

F. Compression: It is an unintentional attack that often appears in multimedia applications. Practically all the audio, video and images that are currently being distributed via Internet have been compressed.

G. Rotation and Scaling: Correlation based detection becomes to fail when rotation or scaling is performed on the watermarked image because the embedded watermark and do not share the same spatial pattern anymore.

H. Statistical Averaging: An attacker may attempt to measure the watermark and then subtract the estimate to unwatermark the object .It is dangerous when the watermark does not depend substantially on the data.

I. Multiple Watermarking: An attacker may watermark an already watermarked object and claims of its ownership. The certification authority timestamps the hidden information for finding solution.

VII. APPLICATIONS OF DIGITAL WATERMARKING

Several applications are listed as below [4] [6] [9]:

A. Owner identification –It is same as copyright protection that establishes ownership of the content. Being able to identify the owner of a specific digital work of art, such as a video or image can be quite difficult.

B. Copy protection – It is also known as copy control that does not allow to people for making illegal copies of copyrighted content.

C. Content authentication – It detects modifications of the content, as a sign of invalid authentication.

D. **Fingerprinting** – Sometimes referred as transaction tracking or traitor tracking. It traces back illegal duplication and distribution of the content.

E. Broadcast monitoring –It is specifically used for advertising and in entertainment industries. It monitors content being broadcasted by the authorized source.

F. Medical applications –It is also known as invertible watermarking that provides both authentication and confidentiality in a reversible manner and does not affect the medical image in any way.

VIII. CONCLUSION

Due to growth of technologies, there is more important issue on security for copyrighted documents. This paper presents the review of Digital Image Watermarking. It is basis on the concept of embedding information into a digital signal and secures it from unauthorized access. This technique provides secure ownership for owner’s document with authentication and protection from various attacks.

IX. REFFERENCS

[1] A. Aggarwal, M. Singla, “Image Watermarking Techniques in Spatial Domain: A Review International Journal of Computer Technology and Applications, vol.2 (5), pp. 1357–1363, ISSN: 2229-6093, Sept-Oct, 2011.

[2] T. Jayamalar, Dr. V. Radha, “Survey on Digital Video Watermarking Techniques and Attacks on Watermarks”, International Journal of Engineering Science and Technology, vol. 2(12), pp. 6963-6967, ISSN: 0975-5462, 2010.

[3] A. Hood, Prof. N. J. Janwe, “Robust Video Watermarking Techniques and Attacks on Watermark – A Review”, International Journal of Computer Trends and Technology, vol.4, Issue 1, pp.30-34, ISSN: 2231-2803, 2013.

[4] Y. Yusof and Othman O. Khalifa, “Digital Watermarking For Digital Images Using Wavelet Transform”, Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 14-17 May 2007, Penang, Malaysia.

[5] C. Huang, C. liao, “A Blind Image Watermarking Based on Dual Detector” journal of information science and engineering, vol. 25, pp.1723-1736, 2009.

[6] http://en.wikipedia.org/wiki/Digital_watermarking.

[7] D. Singh, N. Choudhary, M. Agrawal, “Spatial and Frequency Domain for Grey level Digital Images”, Special Issue of International Journal of Computer Applications (0975–8887) on Communication Security, No.4, pp.16-20, Mar.2012.

[8] S. P. Mohanty, “Digital Watermarking : A Tutorial Review”.

[9] R. T. Paul, “Review of Robust Video Watermarking Techniques”. IJCA Special Issue on Computational Science - New Dimensions & Perspectives NCCSE, pp. 90-95, 2011.

[10] A. R. Madane, K. T. Talele, M. M. Shah, “Watermark Logo in Digital Image using DWT”, Proceedings of SPIT-IEEE Colloquium and International Conference, Mumbai, India, Vol. 1, pp.121-127.

[11] B. L. Gunjal, R. R. Manthalkar, “An overview of transform domain robust digital image watermarking algorithms”, Journal of Emerging Trends in Computing and Information Sciences,

Volume 2, No.1, ISSN 2079-8407,pp. 37-42, 2010-11.

[12] S. P. Singh, S. Agrawal, “A Literature Review on Water Marking Techniques”, International Journal of Scientific Engineering and Technology, Volume No.1, Issue No.4, pp: 21-23, ISSN: 2277-1581, Oct. 2012.