Volume 4, Issue IV, April 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

An Analytical Review on Various Watermarking Techniques

Mansi[1], Navneet Verma[2]

[1]M.Tech Scholar, 2Asst. Prof. CSE Dept
Geeta Engineering College, Naultha, Panipat

Abstract *– Now-a-days use of internet is increasing day by day. With the rapid advancement in technology, speed of data over networks has crossed the bars. There is urgent need to preserve the copyright of individual's creation, which is done by using digital watermarking. Digital watermarking is a technology in which embedding of information is done in digital content to protect it from illegal copying. This embedded information to protect the data is embedded as watermark. In digital watermarking, a watermark is embedded into a cover image in such a way that the resulting watermarked signal is robust to certain distortion caused by either standard data processing in a friendly environment or malicious attacks in an unfriendly environment. Beyond the copyright protection, Digital watermarking is having some other applications as fingerprinting, owner identification etc. Digital watermarks are of different types as robust, fragile, visible and invisible. In this paper, we have surveyed various watermarking techniques, its types, applications and various attacks*

Keywords:-*Watermarking, DWT (Discrete Wavelet Transform), SVD (Singular Value Decomposition), PSNR (Peak Signal to Noise Ratio).*

1. Introduction

The purpose of data hiding is to embed data such as imperceptible information in various forms of digital media such as image, audio, video and so on. Especially in the aspects such as military, intelligence and national security, the requirement of data hiding technology is high [1]. It is require that the hiding confidential information is not easy to be detected by detection tools and image cannot be distorted. Data hiding, while similar to compression, is distinct from encryption. Its goal is not to restrict or regulate access to the host signal, but rather to ensure that embedded data remain inviolate and recoverable. For the secure transmission of various types of information over networks, several techniques like steganography, cryptography and digital watermarking techniques are used which are well known. In this paper, we have explained digital watermarking, with its techniques, types, applications and various attacks on digital watermarking.

2. Digital Watermarking

Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including security, data authentication, identification of owner and copyright protection [1]. Digital multimedia content includes image, audio, video etc. Sometimes the scaling factor is also used for embedding the watermark in the cover image. Digital watermarking is used for the security of the digital content and to protect the data from illegal users and provides the ownership right for the digital data. An important characteristic of digital watermarking is robustness and imperceptibility against various types of attacks or common image manipulation like rotation, filtering, scaling, cropping and compression. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications such as E-commerce, E-voting, copyright protection, content authentication, medical safety, broadcasting monitoring, military and indexing [2].

2.1 Digital watermarking life-cycle phases: Digital image watermarking use digital image for embedding the hidden information, after embedding the watermarked image is generated and the watermarked image is more robust against attacks. Figure 1 shows the life-cycle phases of digital watermarking [3]:

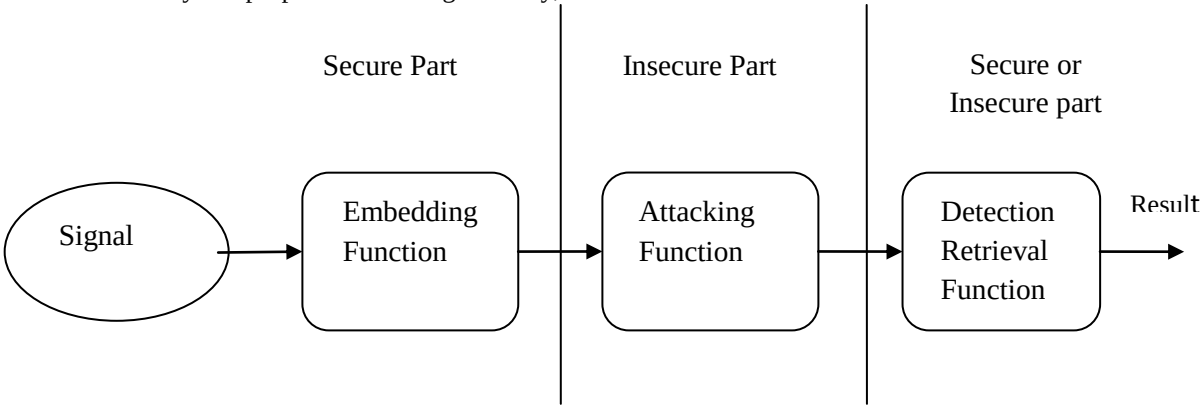

Figure 1: General Digital watermarking life-cycle phases

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

i) Embedding: An algorithm accepts the host and the data to be embedded, and produces a watermarked signal. Then, the watermarked digital signal is transmitted to another person or stored.
ii) Attack: Unauthorized person try to make modifications. In this stage, when the data is transmitted over the network. Either some noise is added with the watermarked image or some attacks are performed on the watermarked image. So, our watermarked data is either modified or destroyed.
iii) Extraction: An algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted.

2.2 Types of Digital Watermark: Watermarks and watermarking techniques can be divided into various categories in various ways. According to the type of document to be watermarked, watermarking techniques can be divided into four categories as follows [5]:
i) Text Watermarking: This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.
ii) Image Watermarking: This is used to hide the special information into the image and to later detect and extract that special information for the author‘s ownership.
iii) Audio Watermarking: This application area is one of the most popular and hot issue due to internet music, MP3.
iv) Video Watermarking: This adds watermark in the video stream to control video applications. It is the extension of image watermarking. This method requires real time extraction and robustness for compression.

***2.3 Types of Digital watermarking techniques*:** Digital watermarking techniques may be classified as [6]:
i) Spatial domain watermarking: Spatial domain methods are based on direct modification of the values of the image pixels, so the watermark has to be embedded in this way. Such methods are simple and computationally efficient, because they modify the color, luminance or brightness values of a digital image pixels, therefore their application is done very easily, and requires minimal computational power. Some of its algorithms are LSB; SSM Modulation based technique [6]. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression. Least Significant Bit Coding (LSB) [5] is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component.
ii) Frequency domain watermarking: In Frequency domain the secret data are hidden in the lower or middle frequency portions of the protected image, because the higher frequency portion is more likely to be suppressed by compression. Embedding of a watermark is made by modifications of the transform coefficients, accordingly to the watermark or its spectrum. Finally, the inverse transform is applied to obtain the marked image. This approach distributes irregularly the watermark over the image pixels after the inverse transform, thus making detection or manipulation of the watermark more difficult [6]. Frequency (transform) domain methods are based on the using of some invertible transformations like discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT) etc. to the host image. Discrete cosine transform (DCT) [7] is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to a set of n coefficients. Discrete Fourier Transformation (DFT) is translation invariant and rotation resistant, which translates to strong robustness to geometric attacks.DFT uses complex numbers, while DCT uses just real numbers. Discrete wavelet transforms (DWT) [6] based methods enable good spatial localization and have multi resolution characteristics, which are similar to the human visual system. Also this approach shows robustness to low-pass and median filtering. However, it is not robust to geometric transformations.

2.4 Applications of Digital watermarking: Various applications of digital watermarking are as follows [8]:
i) Broadcasting Monitoring: This type of monitoring is used to confirm the content that is supposed to be transmitted. As an example, commercial advertisements could be monitored through their watermarks to confirm timing and count.
ii) Fingerprinting: This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner. A watermarked object contains information about the owner permissions. Several fingerprints can be hosted in the same image since the object could belong to several users.
iii) Image and Content Authentication: In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are inserted and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method [4]. Digital signature essentially represents some kind of summery of the content. If any part of the content is modified, its summery, the signature, will change making it possible to detect that some kind of tampering has taken place. One example of digital signature technology being used for image authentication is the trustworthy digital camera.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

iv) Temper Detection: Fragile watermarks are used for tamper detection. If the watermark is destroyed or degraded, it indicates presence of tampering and hence digital content cannot be trusted.

v) Medical Application: Name of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster.

vi) Copyright Protection: Watermarking is essentially applied for copyright protection. The aim is to evade other parties from claiming the copyright by embedding the information that identifies the copyright owner of the digital media. The application must make certain that embedded watermark cannot be eliminated without causing a noteworthy deformation in digital media though maintaining a high level of robustness [6]. It is important to consider further necessities in addition to robustness. For instance, the watermark must ably determine rightful ownership if other parties embed additional watermarks and also explicit by nature. When a new work is produced, copyright information can be inserted as a watermark. In case of dispute of ownership, this watermark can provide evidence.

vii) Content Protection: Modern digital formats employed for sale or rental of commercial audio and video content to consumers-such as DVD, Blue-Ray Disc, and iTunes-incorporate content protection technologies that control access to and use of the content and limit its unauthorized copying and redistribution. Parties seeking to engage in unauthorized distribution and copying of protected commercial music or video content must circumvent the content protection to obtain a decrypted copy of the content [4].

viii) Convert Communication: The embedded signal is employed in the transmission of secret information from one person (or computer) to another, devoid of anyone along the way becoming aware that this information is being transmitted [4]. It includes exchange of messages secretly inserted within images. In this case, the main requirement is that hidden data should not raise any suspicion that a secret message is being communicated.

2.5 Attacks on Digital watermarking:

i) Removal attack: Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal. Examples of this category attacks are Denoising i.e. Gaussian, uniform, or salt-pepper, Multiple watermarking, Demodulations, lossy compression (JPEG, JPEG2000), quantization, Mean/median/Gaussian filtering, Wiener-Lee filtering, Averaging N instances of the same image, bearing different watermarks, Sharpening, Contrast enhancement (histogram equalization), Gamma correction etc.

ii) Geometric attack: This type of attack is different from removal attack as those attacks will not remove the watermark but distort it using geometric distortions specific to images. Those operations are rotation, scaling, translation, cropping etc. Template based or invariant domain or feature based schemes are used to survive from these attacks [9]. Examples are Global geometric transforms as Translation, rotation, Jittering, mirroring, scaling, shearing, cropping, Local geometric transforms as Random bending, local shifting, rotation, scaling, Stir mark attack as Slight global stretching, shifting, shearing, and rotation, Mosaic attack is Cutting the image into pieces, Template removal attack as Estimate and remove the synchronization template, apply a geometric transform.

iii) Cryptographic attack: Cryptographic attacks deal with the cracking of the security. For example, finding the secret watermarking key using exhaustive brute force method is a cryptographic attack [8]. Another example of this type of attack is the oracle attack. In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography. Statistical averaging and collusion attacks are also types of this category. In this attack many instances of a given data set, each time signed with a different key or different watermark, are averaged to compute the attacked data. Many instances of the same data are available in the collusion attack, but the attacked data set is generating by tacking only a small part of each data set and rebuilding an new attacked data set from these parts.

iv) Protocol attack: The protocol attacks do neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather than that, they take advantage of semantic deficits of the watermark‘s implementation. Consequently, a robust watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one media into another without knowledge of the secret key [9]. It will not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data. IBM attack is creation of a fake original by adding a watermark in watermarked image. The attacker can claim that he has both the original and watermarked image. As above four main classes of attacks are described the attacker may apply single or combination of more attacks. In this paper we are focusing on robustness that is resistant to attack such as filtering, additive noise, compression, RST and other forms of image manipulation, which is very important property of watermark.

3. Literature Review

Candik et.al [1] presented some basic principles and properties of digital watermarking in digital images. Presented methods use discrete orthogonal transforms for watermark embedding and watermark extracting too. Basic properties of digital watermarking based on discrete cosine transform and Karhunen-Loeve transforms are also presented. Practical implementation of watermark requires next analysis of robustness. A robustness analyze is a large group of tests,

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

which are focused to immunity of embedded watermark in next image processing operations, mainly loss operations of watermarked image (loss compression techniques, image quantization), noise, image filtering, non-linear processing, etc.). In the proposed algorithms, the original unmarked image is required for watermark extraction. They are also more sophisticated algorithms in digital image watermarking that not need original unmarked image for watermark extraction. *Lin et.al* [2] presented a novel dual watermarking mechanism for digital media that embeds a recognizable pattern into the spatial domain and an invisible logo into the frequency domain. Undoubtedly, visible watermarking is important for protecting online resources from unauthorized reproduction. Due to the visibility of embedded patterns, however, watermarked digital media are vulnerable to the in painting attack and common signal processing operations. Utilizing hybrid strategies, simulation results show that the novel method can resist these attacks. In particular, the new mechanism allows legal subscribers to restore an unmarked image, whereas other dual watermarking schemes do not. This feature makes it suitable for protecting artistic and valuable media.

Ishikawa et.al [3] described the robustness of optical watermarking against the defocusing of images, which usually occurs in images taken with digital cameras under non-optimal conditions. They evaluated measurements of the defocusing of images against the accuracy of detection of optical watermarking. The value of full width at half maximum (FWHM) of the Gaussian function was used to measure the defocusing of images and measured the FWHM of isolated points and evaluated the accuracy with which watermarked images could be detected when the focal length of the digital camera was changed. They found from the results of evaluation that optical watermarking technology was extremely robust against defocusing of images. As a result, the practicality of optical watermarking in a real-use environment along with the robustness against geometric distortion was demonstrated. They evaluated degradation in the accuracy of detection that arises from defocusing of images when taking the photographic conditions into consideration that are not optimal assuming a practical-use environment of optical watermarking. They concluded that optical watermarking has strong tolerance against image defocusing. The practicality of optical watermarking in a real-use environment was demonstrated with the robustness against geometric distortion.

Jun et.al [4] presented a novel, Image Retrieval based Image Watermark (IRIW) framework to identify copyright-violated images in both efficient and accurate manner for large-scale image databases. They first perform SIFT-based image retrieval to identify similar images given a query image and store them as an output list. Then we extract watermark patterns and check watermark similarity only for images stored in the list. As a final step, re-rank images by considering various information available between each image in the list and the query image and by utilizing information even among images in the list.

Ramakrishnan et.al [5] aimed at developing a hybrid image watermarking algorithm which satisfies both imperceptibility and robustness requirements. In order to achieve the objectives they have used singular values of Wavelet Transformation's HL and LH sub bands to embed watermark. Further to increase and control the strength of the watermark, use a scale factor. An optimal watermark embedding method is developed to achieve minimum watermarking distortion. A secret embedding key is designed to securely embed the fragile watermarks so that the new method is robust to counterfeiting, even when the malicious attackers are fully aware of the watermark embedding algorithm.

Ramaiya et.al [6] presented a hybrid Scheme based on DWT and Singular Value Decomposition (SVD). After decomposing the cover image into four bands, applied the SVD to each band, and embedded the same watermark data by modifying the singular values. Modification in all frequencies allows the development of a watermarking scheme that is robust to a wide range of attacks. In this technique a new robust watermarking technique for color images was performed. The RGB image was converted to HSV and watermarked by using discrete wavelet transform. Watermarking embedded stage and extraction stage is designed using low power invisible watermarking algorithm. Here the host signal is an image and after embedding the secret data a watermarked image is obtained and then extracts secret image and original image separately.

Hemdan et.al [7] presented a hybrid image watermarking technique for data hiding over Internet. The idea of the proposed technique was based on fusing multiple watermark images using wavelet fusion algorithm. Then, the resultant fused watermark was embedded in the original image using hybrid DWT-SVD watermarking algorithm to produce the watermarked image. The performance of the proposed algorithm was evaluated and a comparative study is done between the hybrid DWT-SVD and SVD watermarking algorithm for single and multiple watermarks. The experimental results verified and proved that the wavelet fusion is an efficient algorithm for fusing multiple watermarks. The image watermarking technique using the hybrid DWT-SVD is more robust than that using the SVD only.

Bisla et.al [8] has done a comparative study of two most recent techniques used in digital image watermarking. They are DWT and hybrid DWT-SVD. Both these techniques are very much robust and imperceptible. In case of DWT, decomposition of the original image is done to embed the watermark and in case of hybrid DWT-SVD firstly image is decomposed according to DWT and then watermark is embedded in singular values obtained by applying SVD. Here, the techniques are compared on the basis of PSNR value at different values of scaling factor, high value of PSNR is desired as it shows good imperceptibility of the technique. From the results, on comparing the values of PSNR at different values of scaling factor, it is concluded that the hybrid technique DWT-SVD is much better than DWT

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

technique. As at every value of scaling factor, value of peak signal to noise ratio is more in case of the hybrid technique. Less the value of PSNR more will be the degradation in the quality of the original image. This shows that after watermarking, the quality of original image degrades more when DWT technique is used for embedding the watermark in comparison with DWT-SVD technique embedding.

As per research work done for robustness of watermarking, there are many techniques are suggested as spatial domain and frequency domain based watermarking techniques. Watermarking in frequency domain as DFT, DCT, DWT are more robust than watermarking in spatial domain because information can be spread out to entire image. As features of the image have high invariance to distortions, they can be used as a key to find the insertion location. The goal is to resist both geometric distortion and signal processing attacks, feature based watermarking scheme is suggested in combination with frequency or spatial domain based watermarking [9]. Since no watermarking algorithm resists all the attacks. Still we can find better which will give more robust watermark. Future work Future work can be done for selecting different robust features and selecting proper embedding technique can improve the robustness of watermark and different Optimization techniques can be used for selecting different regions of the watermark embedding.

4. Conclusion

Since the digital data has no difference in quality between an original and its copy, it is impossible to distinguish original from the copy. Digital media causes extensive opportunities for piracy of copyrighted material. The ways and means are required to detect copyright violations and control access to these digital media. Digital image watermarking is modification of the original image data by embedding a watermark containing key information such as authentication or copyright codes. In future, we will propose some hybrid technique to improve the quality of resultant image and hence increases the robustness and imperceptibility of an image by using digital watermarking technique with the concept of image hiding.

References

[1] Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing*, second edition, Pearson Education India, ISBN 9780131687288 2009.

[2] Pei-Yu Lin, Jung-San Lee, and Chin-Chen Chang, "Dual Digital Watermarking for Internet Media Based on Hybrid Strategies", IEEE transactions on circuits and systems for video technology, vol. 19, no. 8, august 2009.

[3] Yasunori Ishikawa, Kazutake Uehira and Kazuhisa Yanaka, "Robustness against Defocusing of Images in Optical Watermarking Technique", March 2012.

[4] Ezz El-Din Hemdan, Nawal El-Fishaw/, Gamal Attiya and Fathi Abd El-Samii, "Hybrid Digital Image Watermarking Technique for Data Hiding", 30th National Radio Science Conference(NRSC 2013), April 2013.

[5] S. Rama krishnan, T. Gopala krishnan and K. Balasamy, "SVD Based Robust Digital Watermarking For Still Images Using Wavelet Transform", CCSEA 2011, CS & IT 02, pp. 155–167, 2011.

[6] Jong Yun Jun, Kunho Kim, Jae-Pil Heo and Sung-eui Yoon, "IRIW:Image Retrieval based Image Watermarking for Large-Scale Image Databases", 2010.

[7] Manoj Ramaiya and Richa Mishra, "Digital Security using Watermarking Techniques via Discrete Wavelet Transform", National Conference on Security Issues in Network Technologies (NCSI-2012) August, 2012.

[8] Nidhi Bisla and Prachi Chaudhary, "Comparative Study of DWT and DWT-SVD Image Watermarking Techniques", Volume 3, Issue 6, June 2013.

[9] Seema Malshe (Gondhalekar) Hitesh Gupta, Saurabh Mandloi "Survey of Digital Image Watermarking Techniques to achieve Robustness" in International Journal of Computer Applications (0975 – 8887) Volume 45– No.13, May 2012.