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

A Review on Digital Watermarking -Its features, types, Applications and Security Threats-

Deepak Sharma[1], Munna Singh Kushwaha[2]

[1]M.Tech student, ECE Deptt., [2]Assistant Professor
S(PG)ITM, Rewari
sharma.deepak1406@gmail.com, munnasinghkushwaha.92@gmail.com

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

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. Digital multimedia content includes image, audio, video etc. 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.

1.1 Digital watermarking life-cycle phases:

The life cycle of digital watermarking is shown in Figure 1. The watermarking technique consists of three steps:

(i) Embedding: Algorithm accepts host and the data to be embedded, and produces watermarked signal. Then, watermarked signal is transmitted to another person or stored.

(ii) Attack: Unauthorized person try to make modifications.

(iii) Extraction: is 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.

1.2 Features of Digital watermarking:

(i) Robustness: The watermarked image should not be removed or eliminated by unauthorized person, thus it should resist modifications by attacks.

(ii) Imperceptibility: The watermarked image should be not affect the quality of the original image, thus it should be invisible for human eye.

(iii) Security: A watermark should only be accessible by authorized parties. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys. Watermark information owns the unique correct sign to identify, only the authorized users can legally detect, extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection.

(iv) Capacity and data payload: Capacity of the watermarking system is defined as the maximum amount of information that can be embedded in the cover work. The number of watermark bits in a message in data payload and the maximum repetition of data payload within an image is the watermark capacity. Depending on the application some watermarking methods require a data payload exceeding 10,000 bits. A watermark may have high data capacity but low data payload.

1.3 Types of Digital watermarking techniques:

(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 imbedded 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.

(ii) Frequency domain watermarking:

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. 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.

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

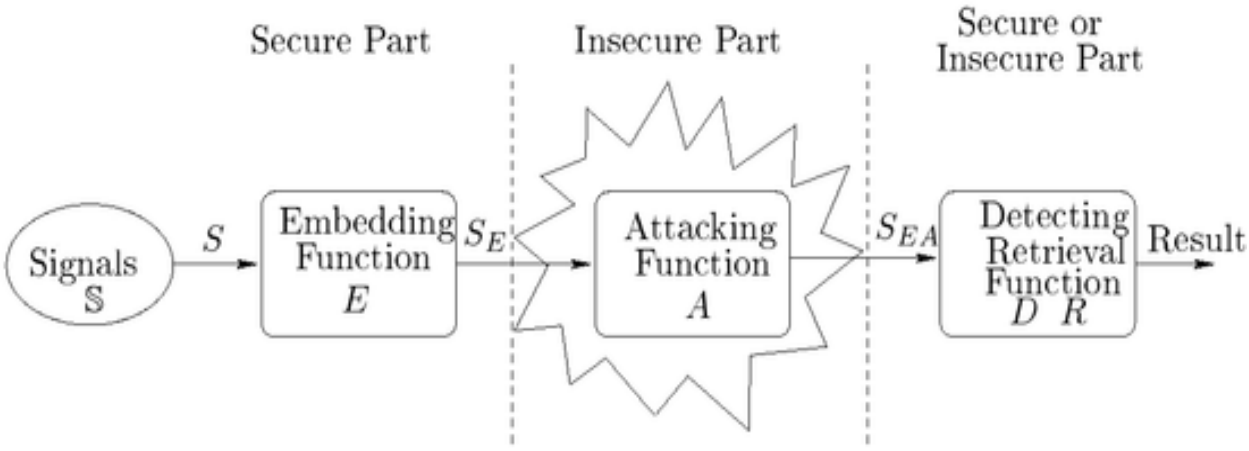

Figure 1: General digital watermark life-cycle phases

1.4 Applications of Digital watermarking:

There are diverse applications of image watermarking. These are listed as follows:

(i) Copyright Protection: 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.

(ii) Broadcast Monitoring: This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not.

(iii) Tamper 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.

(iv) Authentication and Integrity Verification: Content authentication is able to detect any change in digital content. This can be achieved through the use of fragile or semi-fragile watermark which has low robustness to modification in an image.

(v) Fingerprinting: Fingerprints are unique to the owner of digital content and used to tell when an illegal copy appeared.

(vi) Content Description: This watermark can contain some detailed information of the host image such as labeling and captioning. For this kind of application, capacity of watermark should be relatively large and there is no strict requirement of robustness.

(vii) Covert Communication: It includes exchange of messages secretly embedded within images. In this case, the main requirement is that hidden data should not raise any suspicion that a secret message is being communicated.

1.5 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.

(ii) Geometric attack: All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.

(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. 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.

(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.

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. LITERATURE REVIEW

In [1], proposed algorithms unmarked original image required for watermark extraction. They are also more sophisticated algorithms in digital image watermarking that does not need original unmarked image for watermark extraction. In [2], 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

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

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 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. The authors in [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. 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. 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] have 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 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.

3. DIGITAL WATERMARKING TECHNIQUES

Following are the techniques used for watermarking.

3.1 Discrete Wavelet Transform (DWT):

Wavelet domain is a promising domain for watermark embedding. Wavelet refers to small waves. Discrete Wavelet Transform is based on small waves of limited duration and varying frequency. This is a frequency domain technique in which firstly cover image is transformed into frequency domain and then its frequency coefficients are modified in accordance with the transformed coefficients of the watermark and watermarked image is obtained which is very much robust. DWT decomposes image hierarchically, providing both spatial and frequency description of the image. It decompose an image in basically three spatial directions i.e., horizontal, vertical and diagonal in result separating the image into four different components namely LL, LH, HL and HH. Here first letter refers to applying either low pass frequency operation or high pass frequency operations to the rows and the second letter refers to the filter applied to the columns of the cover image. LL level is the lowest resolution level which consists of the approximation part of the cover image. Rest three levels i.e., LH, HL, HH give the detailed information of the cover image.

For second level of decomposition any one sub-band is selected and is further decomposed into four levels. Maximum the level of decomposition, maximum will be the robustness of the watermarked image. At every level of decomposition, the magnitude of DWT coefficients is larger in lower bands (LL), and is smaller in other three bands (LH, HL, and HH).

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Larger magnitude of wavelet coefficients shows their higher significance in comparison with the wavelet coefficients of smaller magnitude.

3.2 Singular Value Decomposition (SVD):

Singular Value Decomposition transform is a linear algebra transform which is used for factorization of a real or complex matrix with numerous applications in various fields of image processing. As a digital image can be represented in a matrix form with its entries giving the intensity value of each pixel in the image, SVD of an image M with dimensions m x m is given by:

M = USVT

Where, U and V are orthogonal matrices and S known as singular matrix is a diagonal matrix carrying non-negative singular values of matrix M. The columns of U and V are called left and right singular vectors of M, respectively. They basically specify the geometry details of the original image. Left singular matrix i.e., U represents the horizontal details and right singular matrix i.e., V represents the vertical details of the original image. The diagonal values of matrix S are arranged in decreasing order which signifies that importance of the entries is decreasing from first singular value for the last one, this feature is employed in SVD based compression techniques.

There are two main properties of SVD to employ in digital watermarking schemes:

1. Small variations in singular values does not affect the quality of image.
2. Singular values of an image have high stability.

3.3 Hybrid DWT-SVD:

Hybrid technique is a fusion of two techniques. Here, DWT and SVD are used together to improve the quality of the watermarking. Advantages of both these techniques are employed in this. DWT and SVD are novel techniques used for watermarking so their fusion makes a very attractive watermarking technique.

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.Ramakrishnan, T.Gopalakrishnan 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.