International Conference on Recent Development in Engineering Science, Humanities and Management
National Institute of Technical Teachers Training & Research, Chandigarh, India (ESHM-17)
29th January 2017, www.conferenceworld.in ISBN: 978-93-86171-25-2

A REVIEW ON DIGITAL IMAGE WATERMARKING TECHNIQUES

Chandan Preet[1], Rajesh Kumar Aggarwal[2]

[1]M.Tech Student, [2] Associate Professor Computer Engg. Department,
National Institute of Technology, Kurukshetra,(India)

ABSTRACT

With the increased use of internet in all areas has made our life easier and comfortable. This has lead to rise in opportunities as well as problems that come along with it. The ease of duplication and copying of data has lead to violations of copyrights and content duplication. The solution to these problems is Digital Watermarking. Digital watermarking is embedding of information into the digital data. Digital watermarking can be done in many ways and using various techniques. In this paper, we discuss various watermarking techniques in spatial and frequency domain. Each watermarking technique has some advantages as well as disadvantages .This paper provide a exclusive analysis of all watermarking techniques on the basis of various factors like robustness, performance etc.

Keywords: Watermarking, embedding/detection, wavelet, cosine, transformation, SVD, attacks, PSNR and MSE.

I. INTRODUCTION

The internet provides the ease of distribution and sharing of information. One can access information anywhere and anytime using internet. But this leads the problems of illegal copying, distribution of information without the prior consent. Digital watermarking [1, 2] provides a solution to this problem. Digital watermarking is embedding of information into digital data i.e. text, image, audio or video. Digital watermarking is performed in two steps. In first step, watermark is embedded and in next step extraction of watermark is performed. There is need to embed the watermark to such an extent that the attacker cannot retrieve the same watermark.

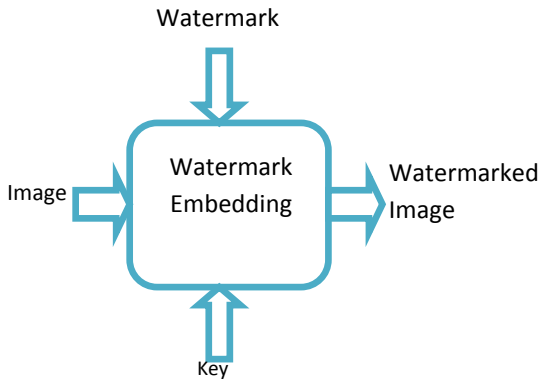


Fig 1: Watermark Embedding Method

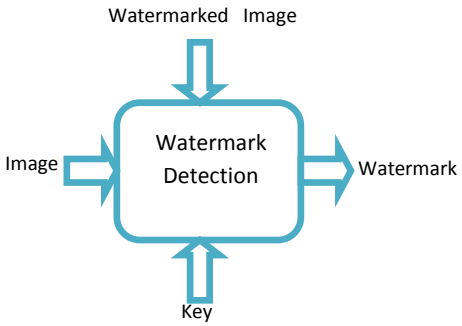


Fig 2: Watermarking tection Method

ISBN: 978-93-86171-25-2

Watermark embedding [3] illustrated in Fig (1) is the first step in digital watermarking. The image on which information is embedded is called cover image. The information that is embedded is known as watermark. In embedding part, watermark is inserted into the cover image using a key. After embedding, the watermarked image is transmitted through the communication channel.

During transmission the watermarked image may be subjected to noise or various kinds of attacks. At receiving end watermark is extracted as shown in Fig (2) from the watermarked image using the key. The extracted and embedded watermark should be same. Any distortion in retrieved watermark means attack is made during transmission. The whole digital watermarking process is shown in Fig (3).

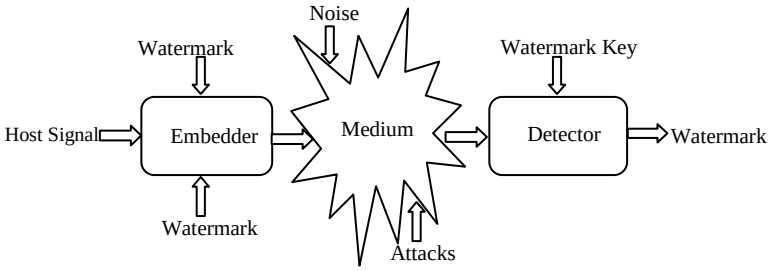


Fig 3: Digital Watermarking Process

II. CLASSIFICATION OF WATERMARKING

Watermarking is categorized in various categories [1, 2,4]:

2.1. Document to be watermarked: watermarking is categorized on the basis of host signal on which watermarking is to be applied. It can be classified as text, audio, video, and image watermarking. The images are highly distributed over internet hence watermarking is preferably/mostly applied on images.

2.2. Blind and Non Blind: In blind watermarking, the original host image is not required during the extraction process. Whereas in non-blind watermarking, the original host image is required to extract the watermark.

2.3. Robust and fragile: Watermarking is said to be robust if watermark remains intact even being attacked during transmission. Whereas a fragile watermark gets altered during attack and the extracted watermark varies from the original being embedded.

2.4. Visible and invisible watermarks: If watermark is easily perceived by human visual system then it is called visible or perceptible watermark otherwise it is known as invisible or imperceptible watermark. Mostly, imperceptible watermarks are preferred.

2.5. Asymmetric and symmetric watermarking: Two keys are used one for embedding and other for extraction purpose. If both the keys are identical then watermarking is symmetric in nature otherwise asymmetric.

2.6. Spatial and Frequency Domain: Spatial domain techniques are either least significant bit (LSB) or correlation based that simply embed the watermark by modifying the pixel values. On the other hand, in frequency domain first the transformation is applied on the image then the watermarking is performed. Famous frequency domain techniques are DCT, DWT and DFT.

ISBN: 978-93-86171-25-2

II. ATTACKS ON DIGITAL WATERMARKING

An Attack means any modification or tampering of watermarked content during the transmission of data from source to destination via communication channel. Attacks or embedding of unwanted signal or noise to watermarked data during transit can affect the quality as well authenticity.

Attacks are broadly classified as [2, 5]:

3.1. Removal Attack: The main aim of the removal attack is to detect the watermark and remove it. The watermark is degraded such that it is undetectable and unreadable.

3.2. Geometric Attack: Geometric attack as the name specifies distortion to be done in geometry of the digital data. Cropping, flipping the image watermark can cause geometric attack.

3.3. Cryptographic Attack: In cryptography attack the attacker aims to get the secret key to extract the watermark. The attacker may use methods such as brute force to obtain key.

3.4. Protocol Attack: In protocol based watermarking attack, the main aim is to embed another watermark on a previously watermarked data. In protocol based attack, neither the watermark is removed nor it is made undetectable [6].

IV. PROPERTIES OF DIGITAL WATERMARKING

Some properties of watermarked data hold are described below [1, 8]:

4.1. Robustness: Robustness defined up to how much extent the watermarked data can tolerate attacks or noise. The ability of attack tolerance provides robustness to the watermarking.

4.2. Security: The watermark should be secure enough to avoid being detected. The secret key should be arbitrary unique that can prevent the unauthorized access to make watermark intact.

4.3. Irremovable: The embedding algorithm should be strong enough to prevent removal of watermark.

4.4. Transparency: The quality of actual data is important hence the embedding process should not lead to any distortions.

4.5. Invisibility: Invisibility implies that the watermark should not be detected by any attacker.

4.6. Capacity: Capacity means the maximum amount of data that can be embedded. The amount of data entered should not affect the robustness and imperceptibility. It is also known as pay-load [7].

V. DIGITAL WATERMARKING TECHNIQUES

Watermarking techniques are broadly categorized into two categories as in Fig (4) (i) spatial domain (ii) frequency domain.

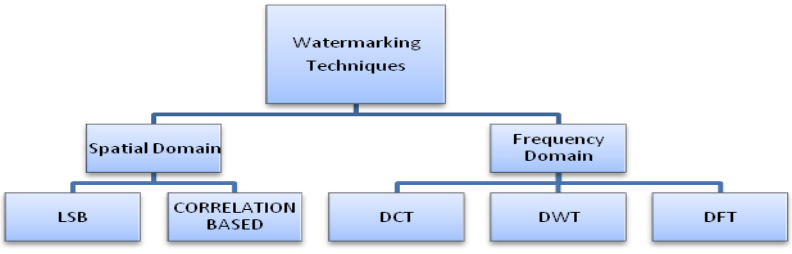


Fig4: Image Watermarking Techniques.

ISBN: 978-93-86171-25-2

5.1 Spatial Domain

In Spatial domain, the watermark bits are embedded by modifying the pixel values of host image. Techniques that uses spatial domain are least significant bit (LSB) and Correlation based.

5.1.1 Least Significant Bit: In this technique [1], the watermark should be embedded to those areas of image that are less prone to attack. Most significant bits are more vulnerable to attacks like cropping, tempering thus to avoid these, the watermarked information bits should be embedded to least significant bits.

51.2 Correlation Based: In correlation based[2] watermarking, The equation to embed watermark into original content is given below:

$$W(x, y) = O(x, y) + w(x, y)*K \quad (1)$$

Where W(x,y) represents the watermarked data. O(x, y) represents the original content that is to be watermarked. w(x, y) is the watermark to be embedded in original content. K implies the gain factor. The more value of K implies that the watermarked content W(x, y) is more robust towards attack[9,13].

5.1. Frequency Domain

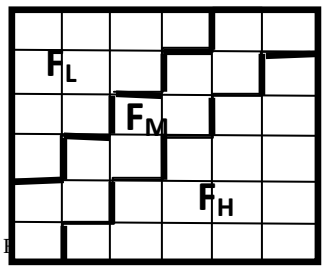
In Frequency Domain, the watermark is embedded to image after transformation. Firstly the image is subjected to transformation like Cosine, Wavelet or Fourier and then the coefficients so received are updated as per watermark bits. Finally, Watermarked image is obtained after performing inverse transformation [14].

5.2.1. Discrete Cosine Transformation: DCT is widely used in the field of signal processing [10]. DCT turns the signal from spatial domain to frequency domain. The embedding of watermark is more robust in frequency domain than spatial domain. In this, the image is divided into small parts or bands as shown in Fig (5). Each image is subdivided into three frequency bands i.e. lower frequency bands, middle frequency bands and higher frequency bands. Middle frequency bands are generally preferred for embedding due to less vulnerability. As lower frequency bands are more sensitive toward attacks and high frequency bands are easily detectable by human visual system [11, 17].

Steps involved in the Cosine [20] transformation are:

- Divide the image into 8*8 non-overlapping parts or blocks.
- DCT is applied to each of the 8*8 block.
- A coefficient selection criterion is then applied.
- Watermark bits are then embedded in coefficients selected above.
- Inverse Cosine transformation is applied.

On comparing, DCT gives better result and is robust towards various attacks like cropping, sharpening etc over spatial domain techniques. It has better efficiency.



ISBN: 978-93-86171-25-2

5.2.2. Discrete Wavelet Transformation: Wavelet transformation [16, 18,19] analyzes the image at multiple resolutions. Image to be transformed is divided in four bands as shown in Fig (6). At subsequent level, the process mentioned above is applied on each band to divide it further. Low frequency coefficients have maximum information about host image whereas higher frequency bands are prone to geometric or cropping attack so these frequency bands are neglected. Hence mixed frequency band (LH, HL) are used to embed information. Wavelet transformed image deliver frequency and spatial description for image. Wavelet transformation perceives the functioning of HVS with more clarity and better visual quality than DCT.

5.2.3. **Discrete Fourier Transformation**: Fourier transform converts the host into frequency based components by using a continuous function. DCT, DWT are not robust towards geometric distortions. DFT [7] is invariant to geometric distortions. DFT also provides robustness against attacks like rotation, cropping, scaling and translation. DFT converts a non periodic function into sine and cosine form.

The disadvantage of DFT is low computational efficiency and the process of applying DFT is complex. So, DFT is not commonly used.

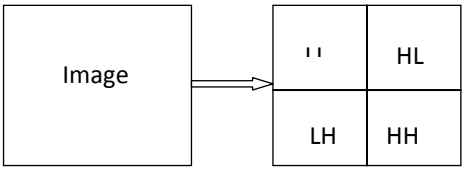


Fig 6: 1-Level DWT

LL: Low frequency coefficient

HL: coefficient of High frequency horizontally.

LH: coefficient of High frequency vertically.

HH: coefficient of High frequency diagonally.

5.2.4 Singular Value Decomposition

SVD is essential tool to examine matrices. Singular values of image are stable and are not prone to attacks. Hence SVD [11, 12] provide robustness and good image quality. In this technique, singular values of host image or blocks are adjusted to embed watermark. SVD of image X of size n*n can be written as

$$X = USV'$$

Where U, V are orthogonal matrices. S is diagonal matrix comprising of singular values of matrix X. The singular values are unique and arranged in descending order. U represents left orthogonal and V represents right orthogonal matrix. Watermarking applied using SVD gives more secure and robust results. The computational cost of SVD is high when compared with other techniques [15,17].

VI. APPLICATIONS OF DIGITAL WATERMARKING

6.1. Copyright protection: The most common use of digital watermarking technique is to protect the owner's right by embedding owner's information so as to avoid illegal copying [7].

ISBN: 978-93-86171-25-2

6.2. Distribution monitoring: In watermarking, the information embedded is related to the owner of data, thus detection of watermark can prevent copying of watermarked data, by unauthorized means thus avoiding illegal distribution of copies [2].

6.3. In medical field: watermarking is widely used in medical fields [17]. For example, in case of X-ray the name and other important details of patients are embedded on x-ray sheet.

6.4. Fingerprinting: In this, information of owner is watermarked so as to detect the source from where illegal copying of digital content starts [3, 7, 8].

6.5. Broadcast monitoring: Broadcast monitoring helps to keep a control over how the digital content is broadcasted and to verify that IPR (Intellectual Property Right) is not violated [7, 9].

VII. METRIC TO MEASURE IMAGE QUALITY

PSNR (Peak signal to noise ratio): Quality of image is measured by calculating PSNR values of images. The higher PSNR[20] value means high quality. It is calculated using:

$$\text{PSNR (db)} = 10 \log 10 \left(\frac{255^2}{MSE}\right) \quad (2)$$

where MSE is Mean Square Error

$$\text{MSE} = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \left(X(i,j) - X_W(i,j)\right)^2 \quad (3)$$

Where N represents two dimensional array. X (i,j) represents pixel of original image and X_w (i,j) represents pixel of watermarked image.

BER (Bit Error Rate): Bit error rate is defined as number of bits error divided by total number of watermark bits. BER = (No. of incorrect/error bits obtained)/ (Total no. of bits).

Normalized Correlation Coefficient:

NC[11] measures the similarity between the original watermark and the retrieved watermark. It can be computed using formula given below:

$$NC(W, W') = \frac{\sum W W'}{\sqrt{\sum W_i^2 \sqrt{\sum W_i'^2}}}$$

Where W is the original bit sequence of watermark and W' is extracted bit sequence of watermark. Its value lies between 0 to 1. The value of NC is 1 tells that the watermark are same but value of 0.7 is also acceptable. The algorithm is robust when the obtained watermark and original watermark are highly correlated [20].

VIII. CONCLUSION

This paper provides a review of Digital Watermarking. Various types of attacks are explored in this paper. The techniques like DCT, DWT, DFT and SVD to prevent from attacks with their merits and demerits are also demonstrated.

ISBN: 978-93-86171-25-2

REFERENCES

[1] Shraddha S. Katariya "Digital Watermarking: Review" in International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 2, February 2012.

[2] Ekta Miglani, Sachin Gupta **"**Digital Watermarking Methodologies - A Survey" in International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 5, May 2014.

[3] Keshav S Rawat, Dheerendra S Tomar **"**Digital Watermarking Schemes for Authorization against Copying or Piracy of Color Images**"** in Indian Journal of Computer Science and Engineering Vol. 1 No. 4 295-300.

[4] Prabhishek Singh, R S Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks" in International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.

[5] S. Voloshynovskiy, S. Pereira; T. Pun; J. J. Eggers; J. K. Su "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks" in IEEE Communications Magazine in 2001, vol. 39, no. 8, p.118-127.

[6] Sunesh, Harish Kumar "Watermark Attacks and Applications in Watermarking" in International Journal of Computer Applications (IJCA), 2011.

[7] Vidyasagar M. Potdar, Song Han, Elizabeth Chang "A Survey of Digital Image Watermarking Techniques" in 3rd IEEE International Conference on Industrial Informatics (INDIN) in 2005.

[8] Manpreet Kaur, Sonika Jindal, Sunny Behal "A Study of Digital Image Watermarking" IJREAS Volume 2, Issue 2 (February 2012) ISSN: 2249-3905, pp. 126-136.

[9] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan , "A Novel Technique for Digital Image Watermarking in Spatial Domain" in 2nd IEEE International Conference on Parallel, Distributed and Grid Computing in 2012.

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

[11] Amit Kumar Singh "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images" in Multimed Tools Appl. of Springer in 2016.DOI 10.1007/s11042-016-3514-z.

[12] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[13] Dipti Prasad Mukherjee, Subhamoy Maitra, Scott T. Acton, "Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication" in IEEE Transactions on Multimedia, Vol. 6, No. 1, February 2004.

[14] Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Shamoon , "Secure Spread Spectrum Watermarking for Multimedia" in IEEE Transactions on Image Processing, Vol. 6, No. 12, December 1997.

[15] Sarthak Nandi and V. Santhi , " DWT–SVD-Based Watermarking Scheme Using Optimization Technique". DOI: 10.1007/978-81-322-2656-7_7

ISBN: 978-93-86171-25-2

[16] Chih-Chin Lai and Cheng-Chih Tsai ,"Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition" in IEEE Transactions on Instrumentation and Measurement, Vol. 59, No. 11, November 2010.

[17] Aditi Zear , Amit Kumar Singh & Pardeep Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine" in Multimed Tools Appl of Springer. DOI: 10.1007/s11042-016-3862-8.

[18] Jung-Chun Liu, Chu-Hsing Lin, and Li-Ching Kuo , "A Robust Full-Band Image Watermarking Scheme" Proc. of IEEE 2006.

[19] Mohammad Reza Soheili, "A Robust Digital Image Watermarking Scheme Based on DWT " in Journal of Computer Engineering , 2009.

[20] Chih-Ta Yen , Yi-Jie Huang "Frequency domain digital watermark recognition using image code sequences with a back-propagation neural network" in Multimed Tools Appl. of Springer.DOI : 10.1007/s11042-015-2718-y.