DOI: https://doi.org/10.24113/ijoscience.v4i3.130

A Study on Digital Watermarking Techniques

Garima Bhargava
M.Tech Scholar
Department of Computer Science and Engineering
Sagar Institute of Research & Technology
Bhopal, M.P, India
garima.bhargava@gmail.com

Arun Jhapate[2]
Professor [2]
Department of Computer Science and Engineering
Sagar Institute of Research & Technology
Bhopal, M.p, iNDIA

***Abstract*: Digital watermarking was introduced as a result of rapid advancement of networked multimedia systems. It had been developed to enforce copyright technologies for cover of copyright possession. This technology is first used for still images however recently they need been developed for different multimedia objects like audio, video etc. Watermarking, that belong to the information hiding field, has seen plenty of research interest. There's a lot of work begin conducted in numerous branches in this field. The image watermarking techniques might divide on the idea of domain like spatial domain or transform domain or on the basis of wavelets. The copyright protection, capacity, security, strength etc are a number of the necessary factors that are taken in account whereas the watermarking system is intended. This paper aims to produce a detailed survey of all watermarking techniques specially focuses on image watermarking types and its applications in today's world.**

Keywords: Digital watermarking, SpatialDomain, Image Transforms, LSB, DWT, DCT, SVD.

1. INTRODUCTION

Nowadays, as the Internet becomes ubiquitous and digitizing devices such as scanners and digital cameras become more available, individuals easily share their own resources on the web. While we enjoy its numerous conveniences, some crucial issues for digital media such as illegal copying, distribution, editing and authentication also arose. This phenomenon has led to an increasing need for developing some standard solutions to prevent these issues. As a powerful method to protect digital copyright, digital watermarking has been developing for many years [1].

Digital watermarking [2] is a technique of inserting a signal (i.e., a watermark) into a digital media to create a variant of the original media containing the watermark information. The inserted watermark is unbearable however it ought to be detectable for proof of possession, authentication, tampering detection, and different applications. The presence of watermark in an exceedingly digital media does not prevent the observer from either viewing, examining or dynamical the media content. However, the watermark is non-removable while not considerably affecting the standard of watermarked media. Currently, watermarking for copyright protection has considerably reduced unauthorized or illegal distribution of digital media over the web.

Watermarking method can be categorized into two groups, namely spatial domain and transform domain. In the spatial domain, the host image pixels are manipulated and the watermark information is directly inserted into them. Although the spatial domain methods have lower computational complexity and higher capacity, they are vulnerable to various attacks and have worse robustness. On the other hand, transform domain methods not only tolerate various attacks but have good performances. Although transform domain methods need predefined transformation and inverse transformation, and the watermark information is distributed over the whole range of pixels of the host image instead of local parts, transform domain methods are more robust to various attacks [2].

At present, the watermarks used in colour image watermarking techniques are most pseudo-random sequence, binary or grayscale image and only few watermarking schemes used the colour image as watermark [5-7].

FindIk et al. [3] proposed to embed the binary image of size 32 × 32 to the blue component of colour image with size 510 × 510 by artificial immune recognition system, and this method has good performances of the watermark. Vahedi et al. [4] proposed a new wavelet-based watermarking approach for colour images using bio-inspired optimisation principles, and the binary logo of size 64 × 64 was embedded into the colour image of size 512 × 512.

Chou and Wu [5] proposed to embed the colour image watermarks into the colour host image, in which the computational complexity was very low but its robustness needs to be improved. Moreover, some watermarking methods based on matrix decomposition have been proposed [6-8]. Among them, Lai [6] designed a novel watermarking method based on HVS and singular value decomposition

(SVD), in which the binary watermark was embedded into greyscale image of size 512 × 512 by modifying the certain elements of the unitary matrix U. This method has better performance of resisting adding noise, cropping and median filtering, but is worse in the aspect of resisting the rotation and scaling.

Golea et al. [7] proposed an SVD-based colour image watermarking scheme to embed colour watermark image into colour host image, but its invisibility is bad because one or more singular values of embedding block must be modified to keep the order of singular values. Bhatnagar and Raman [8] embedded the greyscale watermark of size 256 × 256 into the greyscale image of size 512 × 512. This method is non-blind watermarking method and has the false-positive detection problem.

Charles Way Hun Fung et al. [9] proposed a method to embedded the watermark in videos that insert information in the side view. After this process the DWT-SVD watermarking is used to insert a grayscale image on the luminance(Y) of YUV converted video. High performance when the PSNR metric is measured. Due to the use of a non-blind watermark the requirements for the extraction process are the original watermark and video. This work was only suitable for tamper detection and authentication.

Divjot Kaur Thind [10] proposed a digital video watermarking scheme which combines Discrete wavelet transform (DWT) and Singular Value Decomposition (SVD). The simulation result provide robustness against attacks such as frame dropping, frame averaging and lossy compression. The main drawback of this scheme was that its complexity translates in this case into more resources required to perform the computation - more memory and/or processor cycles and/or time.

Aparna J R et al. [11] proposed a block based image watermarking algorithm which uses cryptographic algorithm to find out the positions of the cover image in which the watermark is to be embedded. The result shows that this scheme is robust enough to withstand scaling, blurring and sharpening attacks. The drawback is that PSNR values are not much improved.

Adamu Muhammad et al. [12] proposed a human visual system based watermarking algorithm for spatial scalable coding based on the H.264/SVC standard. The minimal watermark detection rates after re-encoding, recompression and Gaussian filtering attacks are 0.96, 0.94 and 0.66, respectively. Drawbacks are that visual quality degradation and bit rate overhead.

Lamia Rzouga et al. [13] proposed an approach that ensures security level of a person's biometric data. Computational complexity is reduced in this scheme but not performed well on degraded data.

Rohit Thanki et al. [14] proposed a scheme that utilizes various image processing transforms and Compressive Sensing (CS) to achieved Security for multimedia data which are embedded with embedding factor into the hybrid coefficients. High payload capacity, faster execution time and used for multimedia data authentication. PSNR value is quite low in this scheme.

Venugopala P S, et al. [15] discusses about the bit stream watermarking techniques in spatial and temporal domain. Watermark embedding is performed by embedding binary bits in the random positions of the video as per the random numbers generated. Insertion time approx 150 sec and extraction time is approx 100 sec. Power consumed by videos is between 400-700 mW. The drawback is that the watermarking bits are embedded into the random position as well as Bit error rate is high.

2. WATERMARKING TECHNIQUE

Watermarking technique provides more information about host image. Watermarking is basically four step process as shown in Fig. 1 that includes: Generation, embedding, distribution and attacks and extraction [10-16]. Watermark generation steps generate a logo in form of audio/video/text that is unique to the content and must be such that extraction or distortion from different attacks is difficult. Embedding is a process that embeds logo or mark image into host image. Distribution is a process that can be seen as the transmission of watermarked data. And if someone tries to modify the content then it is called attacks. Extraction is the process that allows owner to be identified and provides information to the intended recipients. Extraction is same process as embedding but occurs in reverse manner. Different techniques are used for watermark embedding and extraction.

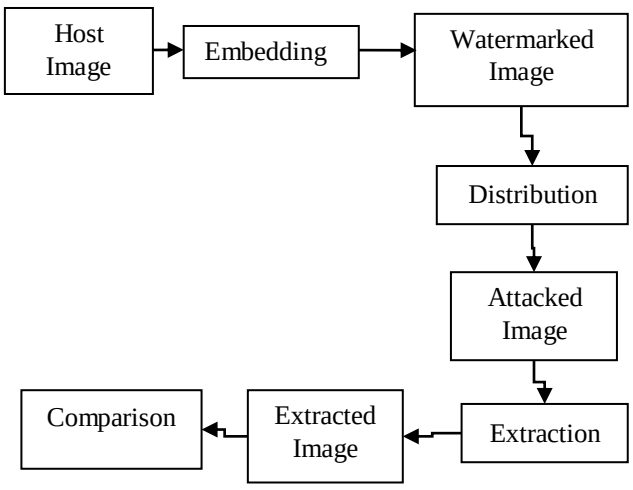

Fig.3. General Image watermarking procedure

Properties of any watermarking techniques are imperceptibility, robustness, capacity and security [17]. Each application has its own requirements. Watermarking technologies are developed according to the requirements of application and each application does not require each of the properties.

Digital watermarking techniques are classified according to documents types are as:

a. Text Watermarking
b. Image Watermarking
c. Video Watermarking
d. Audio Watermarking

Based on human perception they are classified as:

a. Visible Watermarking
b. Invisible Watermarking
   i. Robust Watermark- It embeds the information in such a way that cannot be easily destroyed. All the application where security is main concern robust watermark is used. It can tolerate both malicious and content preserving operations.
   ii. Fragile Watermark- It can detect image tamparing but it cannot locate the region where the image has been modified. Where integrity is main requirement, fragile watermark is used. Such type of watermark cannot be detected if some modification is done.
   iii. Semi-fragile watermark-It provides robustness and characteristics between robust and fragile watermark. It can detect information altering transformations.

3. DIFFERENT WATERMARKING TECHNIQUES

3.1 Least Significant Bits Method

This is the most widely used method for embedding and extraction in spatial domain. In this method image is first divided into subset of images. Encoder first selects the subset of images and then selects the number of bits to be replaced. It replaces LSB of host image with MSB of watermark image. In this method size of host and watermark image must be same. Embedding is done in LSB of pixels because change in LSB of pixels cannot be easily detected by human eyes. Visibility of watermark in host image depends on the number of bits that is replaced [16].

This method may not resistant to different types of attacks such as cropping, addition of noise or lossy compression etc. A better attack would be simply set the LSB of each pixel to defeat the watermark with negligible impact on host image. Furthermore, once an algorithm is discovered watermark can be easily altered by the third party. An improvement over basic LSB method will use the pseudorandom number generator to determine the pixels that is to be used for embedding based on seed point or key values. This method lacks the basic robustness that any watermarking applications require.

3.2 Discrete Cosine Transformation based Watermarking

It is a kind of transform whose kernel is in cosine function. It works for complex numbers. It converts an image from spatial domain to transform domain and vice versa. When an image is transformed using DCT it divides given image into 8*8 blocks. Then it finds low and high frequency components by zigzag scanning. And then embeds watermark in low frequency components. This method provides high robustness against JPEG compression. DCT methods lack resistance to strong geometric attacks [18].

3.3 Discrete Wavelet Transformation based Watermarking

It is a decomposition technique that decomposes given image into set of basic wavelets. It provides spatial and transform representation of an image. DWT is suitable technique to identify the area in the image that contains secret image. DWT decompose given image into low and high frequency components and finds high frequency components and embeds an image into high frequency components [19]. In DWT based method frequency resolution depends on frequency so when frequency is corrupted it decreases robustness. DWT multiresolution technique decomposes given image into four sub bands – LL (High scale low frequency components), LH (Vertical low scale high frequency components), HL (Horizontal low scale high frequency components), HH (Diagonal low scale high frequency components) [10].It embeds watermark into LH and HL bands. This method does not provide strong robustness against different types of geometric and image processing attacks.

3.4 Discrete Wavelet Transform-Discrete Cosine Transform based Watermarking

In this method hybrid watermarking technique is used that combines DWT and DCT. In this method first DWT is applied on the host image up to different levels followed by DCT and then applies different types of attacks. As the number of level increases size of watermark decreases and PSNR increases [20].In this method mark image is multiplied with deviation of host image so quality degrades very slowly. This method provides high PSNR and can extract high quality and large marks. It does not change the view of host image. This method satisfies the requirements of robustness.

3.5 Discrete Wavelet Transform(DWT)-Discrete Cosine Transform(DCT)-Singular Value Decomposition(SVD) based Watermarking

DWT, DCT and SVD are combined in a zigzag way to satisfy the requirement of robustness. First DWT is applied on host image which decomposes the given image into four bands. And then DCT is applied on HH band and map the DCT coefficient using zigzag scanning and then applies SVD to get singular value coefficients [21]. Same procedure is then applied on watermark image. Extraction is same as embedding but works in reverse manner. This method provides good robustness. But complexity increases as process of application of DWT, DCT, SVD and IDWT, IDCT, and inverse SVD.

3.6 Watermarking in Frequency Domain

Invisible watermarking hides small image behind the large image. During embedding in frequency domain first DCT method is applied and AC coefficient is selected in high frequency domain and watermark is embedded into LSB of AC coefficient. Then the JPEG encoding algorithm is used that is based on pseudorandom number generator that is used to determine in which color component the embedding will takes place.RC4 is used to generate the pseudo random bit sequence. This method provides more security. This method provides good robustness against JPEG compression [22].

4. PERFORMANCE MEASURES

Robustness of watermark means that the after intentional or unintentional attacks the watermark is not destroyed and it can be still used to provide certification and it is measured using correlation coefficient. It is measured "after attack". For the robust capability, mean absolute error (MSE) measures the mean of the square of the original watermark and the extracted watermark from the attacked image. The lower the value of the MSE lower will be the error. It is represented as:

$$MSE = \frac{1}{XY[\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,j) - e(i,j))}$$

X and Y are height and width respectively of the image. The c (i, j) is the pixel value of the cover image and e (i, j) is the pixel value of the embed image.

PSNR represents the degradation of the image or reconstruction of an image. It is expressed as a decibel scale. Higher the value of PSNR higher the quality of image. PSNR is represented as:

$$PSNR = 10log10(\frac{(L * L)}{MSE}$$

Correlation coefficient (CC) measures the robustness of the watermark. It correlates the extracted watermark with the original watermark. More the value of CC, more robust is the scheme.

BER is the ratio that describes how many bits received in error over the number of the total bits received.

$$BER = \frac{P}{(H * W)}$$

5. CONCLUSION

Watermark embedding and extraction algorithms are required for providing copyright protection and ownership identification. This paper provides comprehensive survey on various digital image watermarking techniques in different domains and their requirements. It has been concluded that to minimize distortions and to increase capacity, techniques in frequency domain must be combined with another techniques which has high capacity and strong robustness against different types of attacks.

REFERENCES

[1] Ali, M., Ahn, C.W., Pant, M., *et al.*: 'An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony', *Inf. Sci.*, 2015, **301**, (4), pp. 44–60.

[2] Makbol, N.M., Khoo, B.E., Rassem, T.H.: 'Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics', *IET Image Process.*, 2016, **10**, (1), pp. 34–52.

[3] FindIk, O., Babaoglu, I., Ülker, E.: 'A color image watermarking scheme based on artificial immune recognition system', Expert Syst. Appl., 2011, 38, (3), pp. 1942–1946.

[4] Vahedi, E., Zoroofi, R.A., Shiva, M.: 'Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles', Digit. Signal Process., 2012, 22, (1), pp. 153–162.

[5] Chou, C.H., Wu, T.L.: 'Embedding color watermarks in color images', *EURASIP J. Adv. Signal Process.*, 2003, **2003**, (1), pp. 32–40.

[6] Lai, C.C.: 'An improved SVD-based watermarking scheme using human visual characteristics', *Opt. Commun.*, 2011, **284**, (4), pp. 938–944.

[7] Golea, N.E.H., Seghir, R., Benzid, R.: 'A blind RGB color image watermarking based on singular value decomposition'. 2010 IEEE/ACS Int. Conf. on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, May 2010, pp. 1–5.

[8] Bhatnagar, G., Raman, B.: 'A new robust reference logo watermarking scheme', *Multimedia Tools Appl.*, 2011, **52**, (2–3), pp. 621–640.

[9] Charles Way Hun Fung, Walter Godoy Jr., "A New Approach of DWT-SVD Video Watermarking", International Conference on Computational Intelligence, Modelling & Simulation, IEEE, 2011.

[10] Divjot Kaur Thind, Sonika Jindal, "A Semi Blind DWT-SVD Video Watermarking", International Conference on Information and Communication Technologies, 2-14.

[11] Aparna J R, Sonal Ayyappan, "Image Watermarking using Diffie Hellman Key Exchange Algorithm", International Conference on Information and Communication Technologies, 2014.

[12] Adamu Muhammad Buhari, Huo-Chong Ling, Vishnu Monn Baskaran, KokSheik Wong, "Fast Watermarking Scheme for Real-time Spatial Scalable Video Coding", Signal Processing : Image Communication, 2016.

[13] Lamia Rzouga Haddada, Bernadette Dorizzi, Najoua Essoukri Ben Amara, "A combined watermarking approach for securing biometric data", Signal Processing : Image Communication, 2017.

[14] Rohit Thanki, Vedvyas Dwivedi, Komal Borisagar, "A hybrid watermarking scheme with CS theory for security of multimedia

data", Journal of King Saud University – Computer and Information Sciences, 2017.

[15] Venugopala P S, Dr. Sarojadevi H, Dr.Niranjan.N.Chiplunkar, "An Approach to Embed Image in Video as Watermark Using a Mobile Device", Elsevier, 2017.

[16] D. Chopra, P. Gupta, Gaur Sanjay B.C and A. Gupta, "Lsb Based Digital Image Watermarking For Gray Scale Image," IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Vol. 6, No. 1, pp. 36-41, Sep-Oct. 2012.

[17] [8] B. Surekha, Dr G.N. Swamy, "A Spatial Domain Public Image Watermarking," International Journal of Security and Its Applications Vol. 5, No. 1, Jan. 2011.

[18] S. D. Lin and C. F. Chen, "A Robust DCT-Based Watermarking for Copyright Protection", IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, pp. 415-421, August 2000.

[19] [10] S.M. Mohidul Islam, Rameswar Debnath, S.K Alamgir Hossain, "DWT Based Digital Watermarking Technique and its Robustness on Image Rotation, Scaling, JPEG compression, Cropping and Multiple Watermarking," IEEE Conference on ICICT, ISBN: 984-32-3394-8, pp. 7-9, March 2007.

[20] [11] A.Akter, Nur-E-Tajnina, and M.A.Ullah, "Digital Image Watermarking Based on DWT-DCT: Evaluate for a New Embedding Algorithm", IEEE, 3rd INTERNATIONAL CONFERENCE ON INFORMATICS, ELECTRONICS & VISION, pp. 1-6, 2014.

[21] [12] S. K. Prajapati, A. Naik and A. Yadav, "Robust Digital Watermarking using DWT-DCT-SVD", International Journal of Engineering Research and Applications Vol. 2, No. 3, pp.991-997, May-Jun 2012.

[22] [16] Sami E. I. Baba, Lala Z. Krikor, Thawar Arif and Zyad Shaaban, "Watermarking of Digital Images in Frequency Domain," Proc. Springerlink International Journal of Automation and Computing 7(1), pp. 17-22, February 2010, DOI: 10.1007/s11633-010-0017-7.