Original Article

Review On Digital Watermarking Detection Using Image Processing

K. D. S. RAMANI[1], G. R. R. LAKSHMI[2],K. SRAVAN KUMAR[3],A. TEJASWI[4], N. RAVINDHARA VARMA[5],M. V. S. ROJA RAMANI[6]

(6) Asst. Professor, Department of ECE, NS RAJU INSTITUTE OF TECHNOLOGY, SONTYAM, VISAKHAPATNAM
(1,2,3,4,5) U.G. Scholars, Department of ECE, NS RAJU INSTITUTE OF TECHNOLOGY,SONTYAM VISAKHAPATNAM, A.P, INDIA
DOI: 10.47750/pnr.2022.13.S09.1069

Abstract

Watermarking on a picture or an image framework for protecting the image processing models and Digital image watermarking has compelled its suitability for copyright protection and copy control of digital images. Earlier, so many watermarking techniques were introduced to build up the fidelity and robustness of watermarked images against different types of attacks such as additive noise, filtering and some graphical effects. It is very important to guarantee a sufficient level of robustness of watermarked images from such types of effects. We are discussing a technique based on back propagation Neural Network to train a given cover image to produce a desired watermarking image. Especially, given a black box model, affiliated and invisible watermarks are hidden into its outputs which can be regarded as a special task-agnostic barrier. Input-Output pairs of the target model, the hidden watermark will be learned and extracted afterwards to enable marks from binary bits to high resolution images, both traditional and deep spatial invisible watermarking mechanisms are considered.

Keywords: Watermarking, techniques, security, copy infringement, technology.

I. INTRODUCTION

“Watermarking" is the process of screening digital data information in a carrier signal. The digital information in the watermarking does not contain relation to the carrier signal.[1] Mainly digital watermarks are used for identification of owner's identity by authenticating the carrier signal. It is mainly used for finding copyrights violation and for banknote identification. Watermarking is a branch of information hiding which is used to hide information in digital format (or) digital media like photographs, digital music (or) digital video. The digital content is mainly exchanged over the internet and has created copyright infringement.[2] The term "Digital Watermark" was studied by Andrew Tirkel and Charles Osborne in December 1992. The first efficient embedding and extraction of a steganographic spread spectrum watermark was introduced in 1993 by Andrew Tirkel, Charles Osborne and Gerard Rankin. Watermarks are recognizing marks produced during the paper making process. The first watermarks cropped up in Italy during the 13th century, but their use fastly extended across Europe.[3] The marks were frequently created by wire sewn onto the papermold. Nowadays Watermarks are widely used as manufactured marks and to avoid faking techniques.

II. LITERATURE REVIEW

Moreover, the art of papermaking originated in China over one thousand years ago, paper watermarks were not recognized until around 1282, in Italy. These are the marks done by adding thin wire patterns to the paper molds. The paper would be slightly thinner than where the wire was and hence more transparent. The meaning and intention of the earliest watermarks are uncertain. [4]They may have been worn for practical functions such as finding the molds on which sheets of paper were made, or as trademarks to find the paper maker. On the other hand, they may have described magical signs,

or might simply have been provided as decoration.[5] By the eighteenth century, watermarks on paper made in Europe and America had become more apparently effective. They were used as trademarks, to record the date the paper was fabricated, and to express the sizes of original sheets.[6]It was also about this time that watermarks began to be used as anti-forgery measures on money and other documents. The term watermark seems to have been studied near the end of the eighteenth century and may have been derived from the German term Wasser Marke.[7] The term is actually a misnomer, in that water is not especially important in the creation of the mark. It was apparently given because the marks coincide with the effects of water on paper. After Four hundred years, we find the first example of a technology that is equal to the digital methods discussed. In 1954, Emil Hembrooke of the Muzak Corporation registered a patent for "watermarking" musical Works. An identification code was inserted in music by intermittently applying a narrow notch filter centered at 1 kHz. Whenever the energy is absent the notch filter has been pointed out and applied, at the time when the energy is absent the code is either a dot or a dash. The identification signal used Morse code. The 1961 U.S. Patent describing this invention states. In the late 1990s several companies were established to market watermarking products. Nowadays, a huge number of companies have used watermarking technologies for a variety of applications.

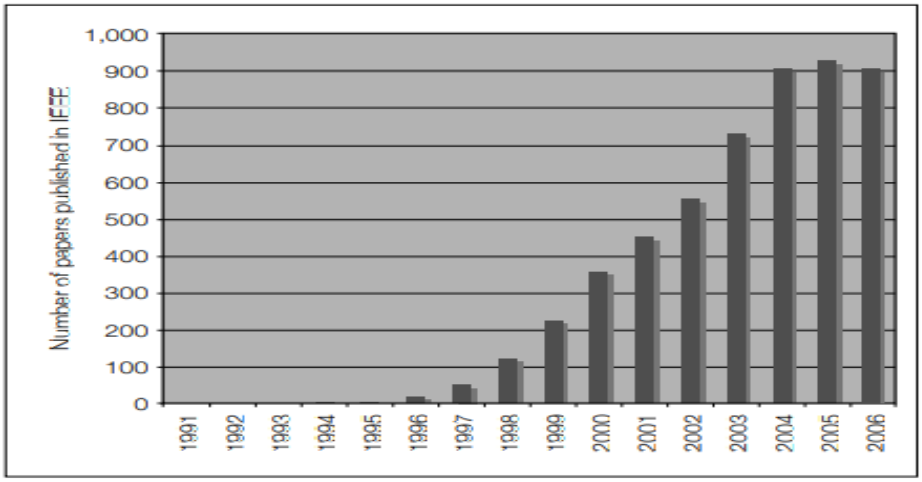


Fig:1 Digital watermarking published percentage[8]

III. THEORY

WATERMARKING

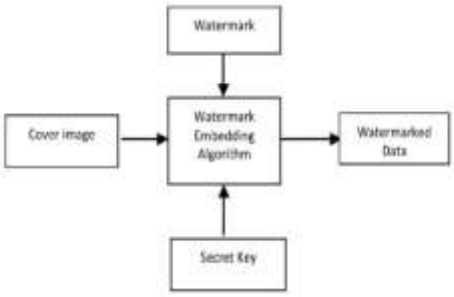
A watermark is a recognizable image or pattern in paper that appears as various shades of lightness (or) darkness when viewed by transmitted light caused by thickness or density variations in the paper. Encoding an identifying code into audio, video, image in a digitized manner is called a digital watermark. Digital watermarking is identifying and thus implementing the concept of watermarking in digital media[9].

DIGITAL WATERMARKING

A digital watermark is called robust with respect to conversions if the embedded information may be identified relatively from the marked signal, even if degraded by any number of conversions. Typical image corruptions are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal changes and MPEG compression again and again are added to this list. A digital watermark is called imperceptible if the watermarked content is absolutely equivalent to the original, unwatermarked content. There are two methods of watermarking: Embedding and detection[10].

EMBEDDING METHOD & DETECTION METHOD

Embedding is adding a watermark object into the original image and detection is finding the image and removing it. Watermarking embedding can be divided into two types of spatial domain and frequency domain. There are some watermark attacks on both spatial domain and frequency domain.



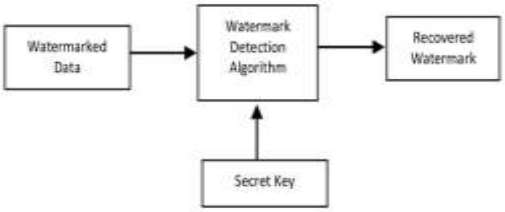


Fig:2 Watermark Embedding process[11]

Fig:3 Watermark Detection Process[11]

SPATIAL DOMAIN & FREQUENCY DOMAIN

Spatial domain embedding is done by modulating the intensity of certain pixels of the original image. watermark is embedded to the least significant bit of the original image.

Frequency domain method uses only one of the following methods such as Discrete cosine transform, Discrete fouriertransform, or Discrete Wavelet transform[12].

These are more robust to attacks because the image is inverse wavelet transform.

Coming to the literature point of view in watermarking, there are three parts to it, watermarking the image, detecting the watermark in an image & removing the watermark.

Watermark can be done using various methods. Some of them are:

- Using DCT based **pyramid Transform**
- Watermarking using **Two-Step Sudoku** method
- Digital watermarking by Discrete **Wavelet Transform**
- Watermarking using **LSB method**

Second part of watermarking detection, this can be achieved using multiple ways.

- **Deep learning embedding and detection method**-In this deep learning model is trained with embedding and detection simultaneously.

By using the Fourier Melin Transform watermark detection can be identified.

- Detection of watermark using **just noticeable distortion method**-minimum difference perceived by human visual system and can be used in various domains such as image or video coding and compression, image quality assessment or data hiding[13].

Watermark removal is the last part of the process where we try to remove the watermark from the target image to get the original image or a replica of the original.

- Watermark removal using **Cross-Channel Correlation-**in this correlation of nearby objects are minimized and color space of image is transformed using Kullback-Liebler distance.

Implementation for watermark removal was done on the basis of building a U-Net based generator discriminator neutral networks. Bounding box from the output of the detection model is used for getting the watermark after being expanded two times to nullify the error in detection of edges. Evaluation of watermarks.

Removal algorithm is done using PSNR (Peak Signal Vs Noise Ratio) and DSSIM (Structural Dis-similarity index). Algorithms can remove watermarks from the superimposed image with good effect along with keeping the details for the original image.

DIFFERENT WATERMARKING TECHNIQUES USED IN SPATIAL DOMAIN AND FREQUENCY DOMAIN

- **Least Significant Bit:** It is the simplest watermarking technique used in spatial domain to embed a watermark in the least significant bits of irregularly selected pixels of the cover image. It is easy to implement and understand low degradation of image quality[14]. It lacks basic robustness.
- **Additive Watermarking:**The most common method in a spatial domain for embedding watermark is to add a pseudo random noise pattern to the intensity of image pixels.
- **Texture mapping coding Technique:** It is a method useful when the images have some texture part. In this method the texture part covers the watermark. This method is only suitable for containing large numbersof arbitrary texture images. It cannot be done automatically.
- **SSM modulation based technique:** Combine host image using pseudo noise signal embedded with watermark bases on spread spectrum modulation distributed in time.
- **Discrete cosinetransform:** This method used in frequency domain in the watermark is embedded into the coefficients of middle frequency. so that the image visibility will not be affected.
- **Discrete Fourier transform:** It transforms continuous function into frequency function. It tells geometric attacks like rotation, scaling, cropping, translation etc.

IV. BACK PROPAGATION ALGORITHM

Back propagation in Neural Networks: The principle of back propagation algorithm is to minimize the error values in randomly allocated weights and bias values such that it produces the correct output.

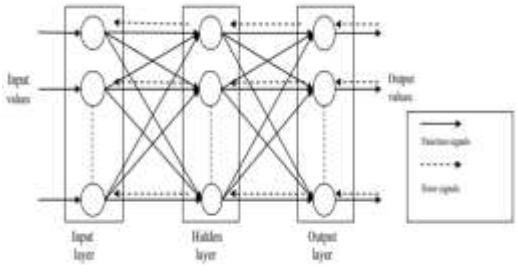


figure:4 Back propagation neural network[15]

In an artificial neural network, the weighted values and biasing values are randomly initialized. Due to random initialization, the neural network probably has errors in giving the correct output. We have to reduce error values as much as possible. So, for reducing these error values, we need a mechanism that can compare the desired output of the neural

network with the network's output that consists of errors and adjusts its weights and biases such that it gets closer to the desired output after every iteration.[16] For this, we train the network such that it back propagates and renews the weights and biases. This is the concept of the back propagation algorithm.

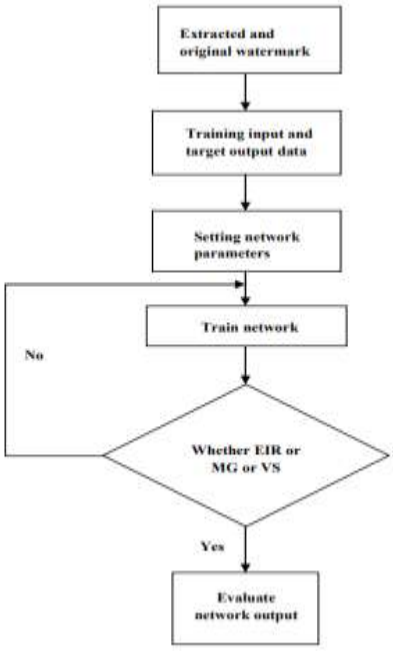


figure:5 BPNN training process.

STEPS IN BACK PROPAGATION

1. Extracted and original watermarks are taken as input.
2. Training input data and produces the target.
3. Adjusting network parameters.
4. Train the network in iterative manner
5. If there are any errors in range(EIR) or minimum gradient reached(MG) or validation stop(VS),then it will propagate back for training again.
6. If there are no errors in range(EIR) or minimum gradient reached(MG) or validation stop(VS),then it will evaluate the output[17].

APPLICATIONS

Major applications of watermarks are

- copyright protection
- broadcast monitoring,
- Authentication
- Fraud detection
- content monitoring..etc.

V. CONCLUSION

The discussed method helps to find potential application in prevention of digital document theft/alteration/modification in different social applications. The concern of many techniques were combined to optimize the robustness of the watermarks and the quality of the watermarked image which is the prime objective of the research. However, this may

have increased the computational complexity to some extent which needs to be investigated separately. We also need to enquire about this method with multiple watermarks which is required in various applications. We would like further improve the performance, which will be compatible for future communication.

REFERENCES

[1] Er. Ashish Bansal , Dr. Sarita Singh Bhadauria " WATERMARKING USING NEURAL NETWORK AND HIDING THE TRAINED NETWORK WITHIN THE COVER IMAGE" Department of Information Technology,MIT,Ujjain,India,2005

[2] JieZhang,†Dongdong Chen,† Jing Liao, Han Fang, WeimingZhang,Wenbo Zhou, Hao Cui, NenghaiYu"Model Watermarking for Image Processing Networks" ,University of Science and Technology in China

[3] Makram W. Hatoum , Jean-Francois Couchot , Rapha¨el Couturier , Rony Darazi "Using Deep Learning for Image Watermarking Attack"

[4] Tahera Akhtar Laskar , K. Hemachandran Department of Computer Science,Assam University, Silchar, Assam, India "DIGITAL IMAGE WATERMARKING TECHNIQUES AND ITS APPLICATIONS"International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March - 2013.

[5]AditiZear, Amit kumarsingh,Robust watermarking technique using back propagation neural network: a security protection mechanism for social applications"January 2017 ,International Journal of Information and Computer Security

[6]Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica, Fridrich Ton Kalker "Digital Watermarking and Steganography Second Edition",2008.

[7] Christine I. Polischuk and Edward J. Delp, Digital Watermarking Algorithms and Applications, IEEE SIGNAL PROCESSING MAGAZINE, JULY 2001.

[8] Jian Zhao, A WWW SERVICE TO EMBED AND PROVE DIGITAL COPYRIGHT WATERMARKS, In: Proc. of the European Conference on Multimedia Applications, Services and techniques, Louvain-La-Nevue, Belgium, May 1996.

[9] Jiang Xuanhua, ―Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation.

[10]V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN)

[11]I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital watermarking and steganography, Morgan Kaufmann, 2007.

[12] Manpreet Kaur, Sonika Jindal,SunnyBehal, A STUDY OF DIGITAL IMAGE WATERMARKING, International Journal of Research in Engineering & Applied Sciences,2012.

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

[14] Edin Muharemagic and BorkoFurht, Survey Of Watermarking Techniques And Applications.

[15] Vassilis E. Fotopoulos and Athanassios N. Skodras, Digital ImageWatermarking: An Overview.

[16] R.G.VanSchyndel,A.Z.Tirkel and CF.Osborne, "A Digital Watermark" in Proc. IEEE International Conf. Image processing,1994,vol.2 pp 86-92.

[17] V. M. Potdar, S. Han, E. Chang, A survey of digital image watermarking techniques, in: INDIN '05. 2005 3rd IEEE International Conference onIndustrial Informatics, 2005., 2005, pp. 709–716. doi:10.1109/INDIN