Hardware Implementation of Robust Digital Image Watermarking using Neural Network– A Survey

Sneha Nyamagoud[1], Suresh Kuri[2], Praveen Kalkundri[3]

M.Tech. Student, Dept. of E & C, KLS, GIT, Belagavi, India[1]

Professor, Dept of E & C, KLS, GIT, Belagavi, India[2]

Professor, Dept. of E & C, KLS, GIT, Belagavi, India[3]

Abstract: Watermarking is the process of hiding the digital information, such as image, audio and video. It is typically used for authentication and copyright. Communication is a major part in our day-to-day life, now a day's exchanging of information in the form of image, audio and video takes place through internet. There are some issues or threads associated with internet transformation with respect to intellectual property rights (IP rights) like forgery, authentication and copyrights. In this paper we limit the survey to images only and we present a detailed survey of existing and newly existing watermarking techniques.

Keywords: Classification of Watermarking, Properties, Neural network, Performance matrices, Applications and Watermarking techniques.

I. INTRODUCTION

In general information hiding techniques are stenography, cryptography and watermarking. Watermark is a target image, impressed onto a paper which provides evidence of authenticity. Digital image watermarking is the process of superimposing a watermark into a original image or host image, for the copyright [1, 2]. According to working domain, watermarking can be divided as spatial and frequency domain. Least significant bit (LSB) and patch work are comes under spatial domain and discreet wavelet transform and discreet cosine transform comes under frequency domain [3].

A. Classification of Digital Watermarking

Watermark technique can be classified as visible invisible, robust & fragile, asymmetric& symmetric, public& private and stenography & non-Stenography watermarking techniques. Digital watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The hiding process has to be such that the modifications of the media are imperceptible [5]. For images, this means that the modifications of pixel values have to be invisible. The watermark must be either robust or fragile, depending on the applications. Robust means the capability of the watermark to resist manipulations of the media, such as lossy compression, scaling and cropping among others. And for fragile the watermark should not resist tampering, or would resist only up to a certain, predetermined extent [15].

B. Properties of Digital Watermarking

Some properties of digital watermarking are, effectiveness- this determines the probability that message in a watermarked image will be correctly detected. Image fidelity- it checks for the transparency of the image. Payload size- determines the size of watermark and original image [4]. False positive rate- this property determines the number of a digital works that are identified to have a watermark embedded when in a fact they have no watermark embedded. Robustness- determines that watermark can easily embeddable and can easily retrievable. In this paper we provide latest digital image watermarking techniques [16].

C. Requirement of Digital Watermarking

- Robustness: This is important requirement of digital watermarking. It is used to measure a correlation between extracted watermark and original watermark. It can be measured by using normalized correlation (NC). Value of NC must be as high as possible.

- Security : Security in watermarking determines that Watermark should be difficult to remove or alter without damaging the original image as all watermarking system seek to protect watermark information without loss of generality.

- Imperceptibility: This is most commonly used in watermarking. The watermark should not be visible to viewer nor should the watermark degrade the quality of the content.
- Invertibility: It determines the possibility to produce the original data during extraction of watermark.
- Capacity : It describes the information about number of bits those are embedded.

II. NEURAL NETWORK

A neural network involves a large number of processors operating in parallel and arranged in rows. The first row receives the raw input information -- analogous to optic nerves in human visual processing. Each successive row receives the output from the row preceding it, rather than from the raw input -- in the same way neurons further from the optic nerve receive signals from those closer to it. The last row produces the output of the system. In the mid eighties, the PDP group [4] together with others, introduced the back-propagation learning algorithm for neural networks. This algorithm for the 1rst time made it feasible to train a non-linear neural network equipped with layers of the so-called hidden nodes. Since then, neural networks with one or more hidden layers can, in theory, be trained to perform virtually any regression or discrimination task.

A. Neural network in image processing
Neural network is the major part in image processing, it is used to perform many functions which are discussed below [17,18].

- **Preprocessing**
The first step in image processing is the preprocessing, which includes image reconstruction, image restoring and image enhancement. To reconstruct images from electron holograms, Wang and Wahl trained a Hopfield ANN for reconstruction of 2D images from pixel data obtained from projections [17]. This Hopfield ANN is a serve as content-addressable memory systems with binary threshold nodes. They are guaranteed to converge to a local minimum, but will sometimes converge to a false pattern (wrong local minimum) rather than the stored pattern (expected local minimum).
The majority of applications of ANNs in preprocessing can be found in image restoration [21,22, 23]. In the most basic image restoration approach, noise is removed from an image by simple filtering, a regression feed-forward network in a convolution-like way to suppress noise. This can handle mean square error of the image. The goal of image enhancement is to amplify specific features. The most well-known enhancement problem is edge detection [24, 25]. A straightforward application of regression feed-forward ANNs, trained to behave like edge detectors.

- **Data reduction and feature extraction**
There are mainly two applications in data reduction and feature extraction namely, image compression application and feature extraction applications [26]. In general, an image compression algorithm, used for storing and transmitting images, contains two steps: encoding and decoding. For both these steps, ANNs have been used [27]. Feature extraction is used for subsequent segmentation or object recognition. The kind of features one wants to extract often corresponds to particular geometric or perceptual characteristics in an image, or application dependent ones, e.g., facial features.

- **Image Segmentation**
Image segmentation is the major part in processing of image. The pulse-coupled neural network (PCNN) model of the cat visual cortex has proven to have interesting properties for image processing. Normally PCNN is applied to image denoising and image segmentation [28, 29].

III. PERFORMANCE MATRICES

1. Mean square error (MSE): This performance parameter is used to identify an error present in watermark and original image.

$$\frac{1}{Nt}\sum_{i,j}[X(i,j) - X^{'}(i,j)]\wedge2$$

2. Peak signal-to-noise ratio(PSNR): this performance parameter is defined as ratio of maximum signal power to corrupting signal power. If the value of PSNR is high then watermark image is almost similar to original image else it is dissimilar. This can be calculated by using below formula,

$$10\log_{10}(\frac{Nt}{MSE})$$

3.   Image fidelity (IF): this parameter is used to find the transparency of a image. Can be calculated by using below formula

$$1 - \sum_{i,j} \frac{[\![X(i,j)]\!] - X'(i,j)]^2}{\sum_{i,j} X(i,j)^2}$$

4.   Correlation co-efficient (CC): this parameter is used to find the compatibility between original and watermarked image. Can be calculated by using formula,

$$\frac{\sum_{i,j}[X(i,j)\ X'(i,j)]}{\sqrt{\left(\sum_{i,j}[X(i,j)]^2[X'(i,j)]\right)^2}}$$

5.   Similarity measure(SM): this parameter is used to find the similarity between original and watermarked image. Calculated by using below formula,

$$\sum_{i,j}[X(i,j)X'(i,j)]/[\sum_{i,j} X'(i,j)]\char`\^2$$

IV. APPICATIONS OF DIGITAL IMAGE WATERMARKING

There are many applications of digital image watermarking technique few are listed below,

1. Broadcast monitoring: It means watermarking technique is used for broadcast monitoring to track a specific video by a TV stations. Ex- advertising agencies uses this technique**.**
2. Owner identification: main purpose is to identify the owner of a specific digital work such as video, audio or image, this is a important task especially in case related to copyright infringement.
3. Transaction tracking: digital image watermarking is used for transaction tracking applications. For example, watermarking could be used to record the recipient of every legal copy of a document by embedding a different watermark in each copy. If the document is then leaked to the internet, the document produced could identify which recipient of the document was the source of the leak.
4. Copy control: In these applications, the watermarking technique is used to prevent the illegal copying of any image, video audio or movie by embedding a watermark in above information sources, that instructs a watermarking compatibility.

V. DIGITAL IMAGE WATERMARKING TECHNIQUES

The process of embedding a watermark in a multimedia object is named as watermarking. Watermark can be considered as a signature that reveals the owner of the multimedia object, this technique is implemented for several reasons like copyright protection, content authentication tamper detection etc. Once the watermark is superimposed or embedded it can experience several attacks because the multimedia object can be digitally processed. The attacks may be unintentionally or intentionally so, to avoid these attacks the robust digital image watermark technique can be implemented.

In this paper [1] a digital image watermarking technique is implemented for the copyright protection. The main aim is, the watermarked image should not be recognized by third person only identified by legal owner of the image. Here a new technique called one way- hash function is used for image watermarking process. In this technique, rabin's scheme is used for generating one –way hash functions.

Experimental result determines that the PSNR value of embedded watermark image was 55.56, so the difference between original image and watermarked image is perceptually invisible. And superimposition of secret image pixels are performed at any position of cover image pixels. This method helps to solve the resolution problem and collision problem, by creating transient table during embedding the process.

Homomorphic technique [2] is a type of encryption technique that allows editing of encrypted image without decrypting it, this preserves the privacy of original data. This technique results in data expansion and gives more computing time. Author also compares the parameters like noise reduction, PSNR, security, MSE and it's merits and de-merits with respect to different techniques. Homomorphic encryption allows the complex mathematical operations and to be performed on encrypted data without compromising the encryption. This homomorphic encryption method gives best result for image robustness and noise reduction.

In this paper [3] the main challenge for image watermarking is to get an efficient method of removing noise from the image. Noise can be removed before transmission and applying for different processes. There are many algorithm for removing noise from the image which depends on the type of noise present in the image.

Experimental result determines the PSNR and MSE value for various noise with respect to desired filters, where BM3D filter gives higher PSNR value i.e 31.15dB for salt and pepper noise, when compared to other noise with other filters, and MSE value is minimum i.e 49.79 for same filter compared to other filters.

This paper reviews [4] the performance analysis of watermarking method based on the concept of combined entropy of blocked image and LSB substitution for different attacks to note the robustness of above methods.

Author uses three data sets for determining PSNR value with respect to above methods, the value is determined for with and without noise. For without noise and with respect to LSB substitution the PSNR value is higher i.e 69.2377 for first bit LSB substitution for data set three and lower value i.e 31.2072 for seventh bit LSB substitution for data set first.

With Gaussian noise PSNR value is higher i.e 21.4098 for third bit LSB substitution for data set 2 and minimum i.e 19.9143 for seventh bit LSB substitution for data set three.

With salt and pepper noise PSNR value is higher i.e 25.615 for fiveth bit LSB substitution for datset 3 and lower i.e 23.8972 with fourth bit substitution for data set two. Result concludes that cropping attack gives best PSNR value compared to above noises.

A digital image watermarking technique is performed by using an edge detection method. The main function of this paper [5] is to get transparent watermark i.e the watermark should not affect the quality of the original image after it is watermarked and watermark should be resistant to various attacks.

The watermark embedding process depends on the coefficients of sub bands that lie on edges, where distortions are less. The watermark is embedded around the edges of selected coefficients.

Author proposes a digital image watermarking technique [6] based on the DWT+DFT+SVD transforms for data transmission. Discrete Fourier transform (DFT) is used to perform the Fourier analysis in practical applications. Singular value decomposition (SVD) is used to embed the watermark image in to the cover image. Author conclude that, PSNR value for different combination of images and for various sub bands, is more when HH sub band is used for transmission and also concludes that PSNR value of the extracted watermark is increases after addition of Gaussian filter watermarking [6].

In this paper [7], a new robust digital image watermarking algorithm is implemented based on the joint DWT-DCT transformation technique. Watermark is embedded in the host image by using 3-level discrete wavelet transform (DWT) method. Experimental result achieved the significantly higher robustness against enhancement and noise addition attacks.

By referring [8], more efficient, more robust, noise free and less attackable watermarking technique can be implemented by using pseudo random number (PRN). In this paper a digital image watermarking technique was implemented by using DWT and this can uses PRN sequence and these sequence can be generated by using Elman neural network, to get more and more robust image.

Author gives the more importance to the security as well as authentication of image. The algorithm were tested for robustness and quality of recovery with respect to different attacks like speckle noise and poissons noise. This algorithm gives more robust and highly secured watermarking technique because of Dubache's wavelet and PRN sequence by neural network, with comparing the above discussed various techniques and this method also reduces the noise addition, during image transmission and also results good PSNR value.

In this paper [9], a new robust and secure digital image watermarking scheme that can be used for copyright protection is proposed. The scheme uses the integer wavelet transform (IWT) and singular value decomposition (SVD). The grey image watermark pixels values are embedded directly into the singular values of the 1-level IWT decomposed sub-bands.

Experimental results demonstrate the effectiveness of the proposed scheme in terms of robustness, imperceptibility and capacity due to the IWT and SVD properties. A challenge due to the false positive problem which may be faced by most of SVD-based watermarking schemes has been solved in this work by adopting a digital signature into the watermarked image. The proposed digital signature mechanism is applied to generate and embed a digital signature after embedding the watermarks; the ownership is then authenticated before extracting watermarks.

In this paper[10], the author predicts that during extraction, watermarks can be successfully extracted without the need for the original image. The author have developed discrete wavelet transform with a Haar filter to embed a binary watermark image in selected coefficient blocks. A probabilistic neural network is used to extract the watermark image.

To evaluate the efficiency of the algorithm and the quality of the extracted watermark images, author used widely known image quality function measurements, such as peak signal-to- noise ratio (PSNR) and normalized cross

correlation (NCC). Results indicate the excellent invisibility of the extracted watermark image (PSNR = 68.27 dB), as well as exceptional watermark extraction (NCC = 0.9779).

In this paper[11], a new robust blind image watermarking scheme based on Region of Interest (ROI) using Arnold scrambling is proposed. The proposed scheme satisfies the requirements via using a watermark generated from the host image, the used embedding strategy and Arnold scrambling. In this paper, the ROI of the host image is used as the watermark image.

First-level DWT is applied to the watermark and approximation coefficients are chosen as information to be embedded. Each approximation coefficient is embedded into the low frequency sub band of a selected block of the host image in the wavelet domain. Before embedding, Arnold scrambling is performed on the approximation coefficients of the watermark as well as the blocks of the host image. This makes the scheme more robust and secure.

In this paper [12], we discuss the development and implementation of the hardware architecture of Digital Image Watermarking in transform domain using a newly developed simple yet secured algorithm. Walsh Transform is used to convert the cover image from spatial domain to transform domain as it is a secured Transform function and it is also feasible to synthesize the developed architecture using HDL (Hardware Description Language) synthesizer.

The proposed architecture is not very resource rich. The proposed watermarking architecture will be very useful particularly for image authentication process and secured transmission of message inside an image. It is difficult to design the hardware architecture of Digital Image Watermarking with very high precision when the algorithm involves more theoretical computational complexity.

In this paper [13], Digital watermarking is the process that embeds data called a watermark into a multimedia object such that the watermark can be detected or extracted later to make an assertion about the object. Several software implementations of the proposed algorithms are available, but very few attempts have been made for hardware implementation. Watermarking is also a type of information hiding where secret codes are embedded in the hidden form inside an image file, audio file or video file. This Paper proposes to implement the invisible LSB-watermarking technique in Lifting compression technique by using the microblaze Processor.

In this paper [14], the digital information can be easily obtained by the unauthorized users in the present era. To avoid this security must be provided to such digital information in the form of image. Image watermarking is the best solution to maintain the security of image. In this paper the MATLAB Simulink based model for invisible image watermarking is implemented on FPGA platform and hardware simulation results are carried out.

The watermarking technique can be implemented by various methods. To determine the proper watermarked image some parameters has to be considered such as, PSNR, MSE, noise attacks and correlation coefficient (CRC). By comparing above discussed methods it can be concluded that, a discrete wavelet transform with pseudo random number with Elman neural network can be implemented to get highly robust and better PSNR value compared to other algorithms for watermarking. So this can be implemented on FPGA for real time applications, and also determine power utilized by device and some hardware parameters.

VI. CONCLUSION

Embedding and extraction algorithm of a digital image watermarking are necessary for providing copyright protection and ownership identification. This paper gives a broad survey on assorted or different digital image watermarking techniques in various domains. In this paper we have gone through the survey and categorized the different techniques based on their requirements. It has been concluded that to minimize the distortion and to increase capacity, methods by using frequency domain techniques along with other required techniques, will increase the robustness against the various attacks.

REFERENCES

[1] Min-Shiang Hwang'f', Chin-Chen Chang, Felled, and Kuo-Feng Hwang' "**A WATERMARKING TECHNIQUE BASED ON ONE-WAY HASH FUNCTIONS**" IEEE Transactions on Consumer Electronics, Vol. **45**, No. 2, MAY 1999.
[2] Jaskaran Singh, Prabhpreet Kaur "Digital Image Watermarking of Homomorphic Encrypted Images: A Review" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.
[3] Mr. Rohit Verma and Dr. Jahid Ali " A Comparative Study of Various Types of Image Noise and Efficient Noise Removal Techniques"International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 10, October 2013.
[4] Sanjay Kumar, Ambar Dutta "A Study on Robustness of Block Entropy Based Digital Image Watermarking Techniques with respect to Various Attacks", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India.
[5] John N. Ellinas "A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection" World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:1, No:10, 2007.

[6]   Saravanan P, Sreekara M and Manikantan K"Digital Image Watermarking Using Daubechies Wavelets" 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN).

[7]   Mr.D.V.N.Koteswara Rao#1,Y.Madhuri#2, S.V.Rajendra Kumar#3 ,Y.V.Suresh Babu, " Robust Image Watermarking using DCT & Wavelet Packet Denoising", International Journal of Scientific & Engineering Research Volume 3, Issue 5, May-2012 1 ISSN 2229-5518.

[8]   Suresh Kuri1*, V.B.Deshmukh, Dr. G.H.Kulkarni "Robust Digital Image Watermarking Using Pseudo Random Numbers", Proceedings of International Conference on Circuits, Communication, Control and Computing (I4C 2014).

[9]   Nasrin M.Makbol, Bee EeKhoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition", Journal- Elsevier, Year 2014.

[10]   Yahya AL-Nabhani, Hamid A. Jalab, Ainuddin Wahid, Rafidah Md Noor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network", Journal of King Saud University – Computer and Information Sciences ,Year-10 September 2015.

[11]   Razieh Keshavarzian, Ali Aghagolzadeh, "ROI based robust and secure image watermarking using DWT and Arnold map", International Journal of Electronics and Communications (AEÜ), Year- 3 December 2015.

[12]   Dibya Das, Mriganka Gogoi, "Design and implementation of an MSI number based image watermarking architecture in transform domain", Journal-IEEE, Year- 16 February 2016.

[13]   Somisetti Asha Latha, Maddireddy Sowjanya, "FPGA Implementation of a Digital Watermarking using Discrete Wavelet Transformation", International Journal of Scientific Engineering & Technology Research, Vol.03,Issue.27 September-2014.

[14]   Shamali Vijay Chavan, S. S. Patil, "FPGA Implementation Of invisible Watermarking Using Matlab Simulink", International Journal of Advanced Technology in Engineering & Science, Vol-4, Issue-08, Year Aug 2016.

[15]   Urvi H. Panchal and Rohit Srivastava "**A** Comprehensive Survey on Digital Image Watermarking Techniques**"** 2015 Fifth International Conference on Communication Systems and Network Technologies.

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

[17]   V. Srinivasan, Y.K. Han, S.H. Ong, Image reconstruction by a Hop1eld neural network, Image Vision Comput. 11 (5) (1993) 278–282.

[18]   R.R. Meyer, E. Heindl, Reconstruction of oI-axis electron holograms using a neural net, J. Microsc. 191 (1) (1998) 52–59.

[19]   Y.M. Wang, F.M. Wahl, Vector-entropy optimization based neural-network approach to image reconstruction from projections, IEEE Trans. Neural Networks 8 (5) (1997) 1008–1014.

[20]   N. Ansari, Z.Z. Zhang, Generalised adaptive neural 1lters, IEE Electron. Lett. 29 (4) (1993) 342–343.

[21]   C.C. Lee, J.P. Degyvez, Color image processing in a cellular neural-network environment, IEEE Trans. Neural Networks 7 (5) (1996) 1086–1098.

[22]   Z.Z. Zhang, N. Ansari, Structure and properties of generalized adaptive neural 1lters for signal enhancement, IEEE Trans. Neural Networks 7 (4) (1996) 857–868.

[23]   M.A.T. Figueiredo, J.M.N. Leitao, Sequential and parallel image restoration: neural network implementations, IEEE Trans. Image Process. 3 (6) (1994) 789–801.

[24]   V. Chandrasekaran, M. Palaniswami, T.M. Caelli, Range image segmentation by dynamic neural network architecture, Pattern Recognition 29 (2) (1996) 315–329.

[25]   F.Y. Shih, J. Moh, F.-C. Chang, A new ART-based neural architecture for pattern classi1cation and image enhancement without prior knowledge, Pattern Recognition 25 (5) (1992) 533–542.

[26]   C. Amerijckx, M. Verleysen, P. Thissen et al., Image compression by self-organized Kohonen map, IEEE Trans. Neural Networks 9 (3) (1998) 503–507.

[27]   W. Skarbek, A. Cichocki, Robust image association by recurrent neural subnetworks, Neural Process. Lett. 3 (1996) 131–138.

[28]   B.S. Manjunath, T. Simchony, R. Chellappa, Stochastic and deterministic networks for texture segmentation, IEEE Trans. Acoustics, Speech Signal Process. 38 (6) (1990) 1039–1049.

[29]   W.-C. Lin, E.C.-K. Tsao, C.-T. Chen, Constraint satisfaction neural networks for image segmentation, Pattern Recognition 25 (7) (1992) 679–693.