

Digital coloured Image watermarking using FCNN and Hopfield Models

¹Amarjeet Kaur, ²Anjana Sharma, ³Nitasha Singla
¹Asst. Professor, CEC, Landran, ²Asst. Prof. CEC Landran, ³Asst. Prof. CEC Landran

Abstract: This research paper deals with the study of digital Image watermarking using FCNN and Hopfield models. The frequent use of computer and internet networks for transfer and sharing of audio, video and images arise the question of security in this vulnerable communication environment. The security issue is resolved by proposing different watermarking techniques. So one of the techniques is using FCNN and Hopfield model.

I. Introduction

A **digital watermark** is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. The need arises for watermarking because (i) internet is the best medium for sharing of any data including videos but internet is used by no of users who are prone to piracy of digital data as copying of data from internet is very easy.

- (ii) To save digital data from malicious attacks which will ultimately make the digital data prone to copying.
- (iii) To protect the intellectual property rights of the owner of the digital data.
- (iv) For authentication of original digital data.

- (v) To save original data from manipulation.

The need of more secure and protective communication environment arises with the development of multimedia systems. There are number of techniques which have been developed for watermarking of digital data for copyright protection. A digital watermark is a visible or invisible identification code that is permanently embedded in the data and remains with the data even after decryption. The data can be audio, video, image or text. If anyone tries to copy the data the watermark will be copied along with the data which will help in keep a check on piracy and illegal copy of data. A signal can contain number of watermarks. Watermarking can be visible or invisible. A watermarked image in which the watermark is imperceptible, or the watermarked image is visually identical to its original constitutes a **invisible digital watermarking**. Examples include images distributed over internet with watermarks embedded in them for copyright protection. Those which fail can be classified as **visible digital watermarks**. Examples include logos used in papers in currencies.

The concept of digital watermarking is developed from steganography and cryptography. **Steganography** is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word *steganography* combines the Greek words *steganos*, meaning "covered, concealed, or protected", and *graphein* meaning "writing". Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol.

Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it. **Cryptography** or **cryptology** is the practice and study of techniques for secure communication in the presence of third parties called adversaries. cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce

Watermark is embedded in the host signal and based upon that watermarking may be classified as:

- i) Digital image watermark: both visible and invisible watermarking is applicable
- ii) Digital video watermarking: watermarking in image can be extended to videos also.
- iii) Digital audio watermarking: only invisible watermarking is possible
- iv) 3D Multimedia based watermark.

A. **Neural networks:** The simplest definition of a neural network, more properly referred to as an 'artificial' neural network (ANN), is provided by the inventor of one of the first neuro computers, Dr. Robert Hecht-Nielsen. He defines a neural network as:

"...a computing system made up of a number of simple, highly interconnected processing elements, which

process information by their dynamic state response to external input".

Neural networks are typically organized in layers. Layers are made up of a number of interconnected 'nodes' which contain an 'activation function'. Patterns are presented to the network via the 'input layer', which communicates to one or more 'hidden layers' where the actual processing is done via a system of weighted 'connections'. The hidden layers then link to an 'output layer' where the answer is output as shown in the graphic below.

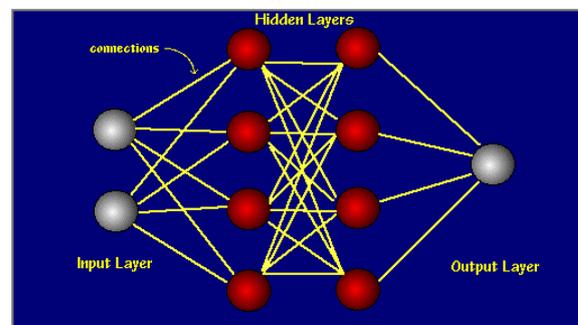


Fig 1: Architecture of a simple neural network

B. Full Counter Propagation Neural Network

Full Counter Propagation Network is the extension of forward only Counter Propagation network with bidirectional mapping which was developed by Hecht-Nielsen and it works as a self-adapting optimal look up table, which provides mapping between input and output layer. The architecture consists of three layers: 1. Input layer. 2. Hidden layer also called Kohonen layer as the weights between input and this layer are trained by self organizing kohonen rule. 3. Output layer is called Grossberg layer. FCNN algorithm has the ability to embed watermark into multiple cover images at a time, where the images and the watermark are presented into the network simultaneously. The

same FCNN is used for watermark extraction too.

Full counter propagation neural network reduced the distortion to a negligible level. A network can be trained in various ways to extract a watermark to prove ownership which is a threat to authentication.

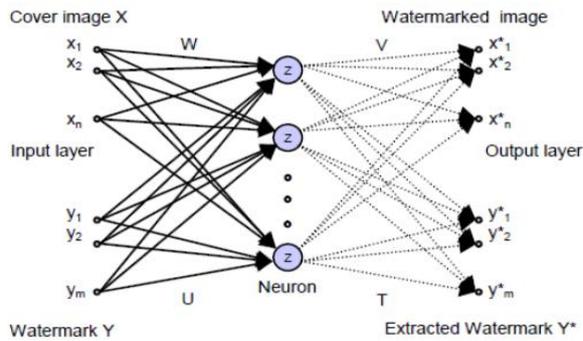


Fig 2. Architecture of full counter propagation neural network

C. Hopfield Model:

Hopfield networks are constructed from artificial neurons. These artificial neurons have N inputs. With each input i there is a weight w_i associated. They also have an output. The state of the output is maintained, until the neuron is updated. Updating the neuron entails the following operations:

- The value of each input, x_i is determined and the weighted sum of all inputs, $\sum_i w_i x_i$ is calculated.
- The output state of the neuron is set to $+1$ if the weighted input sum is larger or equal to 0 . It is set to -1 if the weighted input sum is smaller than 0 .
- A neuron retains its output state until it is updated again.

Written as a formula:

$$o = 1 : \sum_i w_i x_i \geq 0$$

$$-1 : \sum_i w_i x_i < 0$$

A Hopfield network is a network of N such artificial neurons, which are fully connected. The connection weight from neuron j to neuron i is given by

a number w_{ij} . The collection of all such numbers is represented by the weight matrix W , whose components are w_{ij} . Now given the weight matrix and the updating rule for neurons the dynamics of the network is defined if we tell in which order we update the neurons.

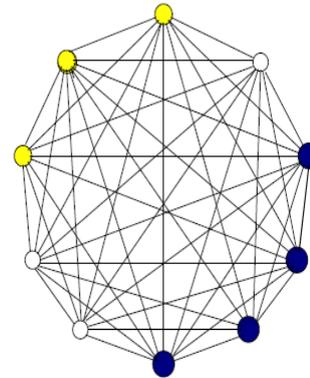


Fig.3. Hopfield network as an auto associate

A pattern is entered in the network by setting all nodes to a specific value, or by setting only part of the nodes. The network is then subject to a number of iterations using asynchronous or synchronous updating. This is stopped after a while. The network neurons are then read out to see which pattern is in the network. The idea behind the Hopfield network is that patterns are stored in the weight matrix. The input must contain part of these patterns. The dynamics of the network then retrieve the patterns stored in the weight matrix. This is called Content Addressable Memory (CAM). The network can also be used for auto-association. The patterns that are stored in the network are divided in two parts: cue and association (Fig.). By entering the cue into the network, the entire pattern, which is stored in the weight matrix, is retrieved. In this way the network restores the association that belongs to a given cue.

II. Literature survey

Bansal[1] et al. proposed the technique to hide the watermark into digital content to protect it from illegal copy or reproduction. The earlier techniques

based on full counter propagation neural network (FCNN) used the concept of embedding the watermark into synapses of neural net to improve PSNR of watermark and FCNN can be practically employed to obtain a successful watermarking scheme with better time complexity and higher capacity. In proposed technique an encoded image is used instead of actual cover image which solve the problem like 'proprietary neural network' and 'sure win' and also helps to sustain authenticity.

Chang[2] proposed a neural network based robust watermarking scheme based on the full counter propagation neural network for digital watermarking in which the watermark is embed and extract through specific FCNN. In this scheme multiple cover image and watermark embedded in the synapses of FCNN simultaneously instead of cover image. Watermarked image is almost same as original cover image. In addition quality of the extracted watermark image does not degrade after most attacks. This technique achieved robustness, imperceptibility and authenticity in digital watermarking.

C.-R. Piao et al. [3] proposed a new blind watermarking scheme in which a watermark was embedded into the DWT (Discrete Wavelet Transform) domain. It also utilized RBF Neural network to learn the characteristic of the image, using which the watermark would be embedded and extracted. The embedding scheme resulted in a good quality watermarked image.

Wang [4] presented a novel blind digital watermarking scheme based on neural networks in the multi-wavelet domain. The watermark was embedded into the coefficients selected based on the weight factors calculated by exploiting the HVS characteristics. The neural network was fused properly with watermarking to enhance the performance of conventional watermarking techniques.

El' Arbi [5] proposed a video watermarking algorithm which combined neural networks with motion estimation in the wavelet domain in a way that was less perceptible and robust against common video processing attacks.

Yi [6] proposed a novel digital watermarking scheme based on improved Back-propagation neural network for color images. The watermark was embedded into the discrete wavelet domain of the original image and extracted by training the BPN which learnt the characteristics of the image. To improve the rate of learning and reduce the error, a momentum coefficient is added to the traditional BPN network.

Huang [7] proposed a novel watermarking technique based on image features and neural networks. The watermark used is a fusion of a binary copyright symbol and image feature label that is obtained by analyzing the image fractal dimension. The watermark not only visually represents the copyright symbol, but also reflects the feature of the image. Arnold transform is used to increase the security of watermark. The back propagation neural network is applied to improve its imperceptibility and robustness.

Bibi Isac[8] presented a review on various watermarking techniques in her research paper and concluded that each of the algorithm has their own advantages and disadvantages. Thus, an ideal watermarking algorithm should be blind in nature and must be robust against attacks. Also it should guarantee correct and fast watermark detection with low error rate. A new algorithm can be created to embed and extract the watermark image. The neural network used may be trained to detect the suitable place to embed the watermark based on Region of Interest (ROI). Once the watermark is embedded, the embedded area can be again detected from the watermarked signal using another trained neural network.

Poulmi Ghosh[9] concluded in her research paper that including both visible and invisible watermark which gives an extra edge in the copyright protection. As we are using compound mapping to embed the visible watermark it helps to increase the robustness of the video. The proposed algorithm works well on gray scale and on video of uncompressed .avi format. In future work will be done on the colored video, so that the approached method works well on all types of videos.

III. Proposed Work

A Number of techniques have been proposed for embedding and extracting watermark in digital data using neural network. I am using FCNN and Hopfield model for analysing the PSNR value when the watermark is extracted from coloured leena image and experienced different attacks. The input coloured leena image is converted into 512*512 size and then the cover image is converted into discrete cosine form and the encoded bits are embedded into the mid band coefficient of block.

Inverse discrete cosine transform (IDCT) of this embedded cover is given to the input of FCNN and Hopfield model. The PSNR value of extracted watermark is obtained at the output of FCNN and Hopfield model.

A. Full Counter Propagation Neural Network: Full counter propagation neural network (FCNN) is used for embedding and extracting watermark from image. Full counter propagation neural network is a supervised-learning network with capacity of bidirectional mapping. The proposed watermarking method integrate the embedding and extraction procedure into full counter propagation based neural network. FCNN designed to learn bidirectional mapping through the process of supervised learning.

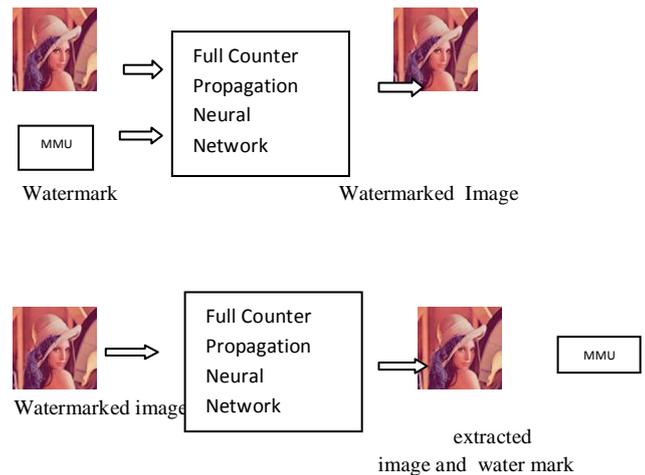


Figure 4.: Schematic Block Diagram of FCNN
(a) Embedding Procedure (b) Extracting Procedure

B. Hopfield Model: Hopfield nets serve as content-addressable memory systems with binary threshold nodes. The Hopfield neural network is a simple feedback neural network which stores the pattern similar to brain and full pattern can be recovered using partial information. Furthermore there is a degree of stability in the system if just a few of the connections between the nodes are served, the recalled pattern is not too badly corrupted and the network can respond with a best guess. Pattern storage is generally accomplished by a feedback network consisting of processing units with non linear bipolar output functions. The stable state of the network represents the stored patterns.

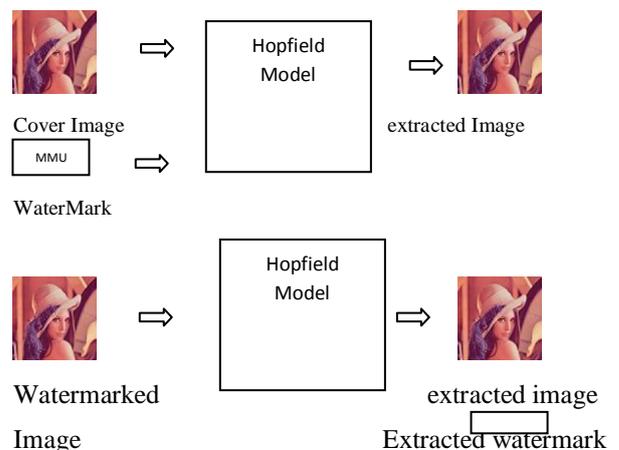


Figure 5: Schematic Block Diagram of Hopfield (a) Embedding Procedure (b) Extracting Procedure

IV. Results

In order to show the proposed research work two models are used FCNN and Hopfield and the results are tabulated as under.

Attacks	PSNR value	
	Hopfield	FCNN
Salt and pepper noise	37.19	49.56
contrast adjustment	36.28	48.29

Table.1 :Values received after image processing

In the above table it is clear that the PSNR value is less when Hopfield model is used. It means the image and watermark are of good quality after extraction using hopfield model.

V. Conclusion

In this paper two techniques Full Counter Propagation Neural Network and Hopfield model are used for digital water marking. In these techniques watermark is embedded in the cover image and extracted. But Hopfield model shows better results for Peak Signal to Noise Ratio in two parameters i.e. adding salt and pepper noise and contrast adjustment. This shows that Hopfield model can resist various attack better than FCNN. The research can be extended using more parameters and new algorithms can be created to extract better image.

VI. References

1. Bansal A. and Bhaduria S.S. ,” A Novel approach using full counter propagation neural network for watermarking”,2010,IJCSE,vol.02,pp 289-296
2. Chuan-Yu Chang and Sheng-Jyun Su, “The Application of a Full Counterpropagation Neural Network to Image Watermarking”, 2005.
3. Cheng-Ri Piao, Suenghwa Beack, Dong-Min Woo and Seung-Soo Han, “A Blind Watermarking Algorithm based on HVS and RBF Neural Network for Digital Image”, ICNC 2006, Part 1, LNCS 4221, pp. 493-496, 2006.
4. Zhenfei Wang, Nenchango Wang and Baochang Shi, “A Novel Blind Watermarking Scheme based on Neural Networks in the Multiwavelet Domain”, In the Proceedings of the 6th World Congress on Intelligent Control and Automation, June 21-23, 2006.
5. Maher El’Arbi, Chorki Ben Amar and Henri Nicolas, “Video Watermarking based on Neural Networks”, 2006.
6. Qianhui Yi and Ke Wang, “An Improved Watermarkingmethod based on Neural Network for Color Image”, In theProceedings of the 2009 IEEE International Conference on Mechatronics and Automation, August 9-12, 2009.
7. Song Huang, Wei Zhang, “Digital Watermarking based on Neural Network and Image Features”, 2nd International Conference on Information and Computing Science, 2009.
8. Bibi Isac,”A study on digital image and video watermarking schemes using neural network” International Journal of computer applications, Vol-12, NO. 9, January 2011.
9. Poulami ghosh,” A Novel Digital Watermarking Technique for Video Copyright Protection” csit 2360, pg no. 601-609.