

Improved Visual Cryptography Scheme using Hopfield for Halftone Images

Ramandeep Kaur¹, Ravneet Kaur²

¹Research Fellow, Department of Computer Science & Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India

²Assistant Professor, Department of Computer Science & Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India

Abstract: Visual cryptography is an emerging cryptography technology that uses the characteristics of human vision to decrypt the encrypted images. Watermarking is a method in which an image or pattern is put on paper in the form of various shades of lightness/darkness especially when viewed by transmitted light. Digital watermarking where computer-aided information is used in the hiding information is one of the most popular forms of watermarking. From security point of view it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. In this paper proposed a digital watermarking scheme for halftone images in Visual Cryptography. By using this technique watermark is embedded in the synapse of cover image. The quality of watermarked image is same as that of cover image. In this research two images are taken and results for various parameters are compared. The experimental results show that the scheme is robust and transparent against various watermarking attack.

Keyword: Cryptography, Image Processing, Visual Cryptography, Secret Sharing, Digital Watermarking, Halftone.

1. Introduction

1.1 Visual Cryptography (2, 2)

Visual cryptography is a (2, 2) secret sharing scheme. It was introduced by Naor and Shamir which is used to encrypt written material such as printed text, handwritten notes, pictures, etc., in a perfectly secure way which can be decoded directly by the human visual system. In visual secret sharing scheme an image is broken up into n parts called shares so that only someone with all n shares could decrypt the image, while any $n-1$ shares revealed no information about the original image. Each share was printed on a separate transparency and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. Anyone who holds only one share will not be able to reconstruct the secret information as single share does not contain complete secret information.

Visual cryptography scheme where 2 shares are generated from the original secret image and by stacking together, the secret is revealed. This is the basics of the technique, however if we more than 2 shares are created and some or all of them stacked for getting the real secret is called visual secret sharing. Following Figure shows the basic behind this scheme [7].













Pixel	White		Black	
				
Prob.	50%	50%	50%	50%
Share 1				
Share 2				
Stack share 1 & 2				

Figure 1: Basic concept of 2-out-of-2 VC

In this concept one white or black pixel will divide into two sub pixel. One way combination of the pixel division is shown in above Figure 1. It is mention that the shares 1 and 2 are stacked together and get the result in the form of complete black or gray (it's partially white and black but visualizes as gray). Because of this, when one stacked the shares the white in original secret image become gray in the stacked result. Stacking can be viewed as mathematically ORing, where white is equivalent to "0" and black is equivalent to "1".

(k, n) secret sharing scheme

Naor-Shamir, 1994 shows (k, n) secret sharing in his paper. They explained as "an N -bits secret shared among n participants, using m sub pixels per secret bit (n strings of mN), so that any k can decrypt the secret": Contrast: There are $d < m$ and $0 < \alpha < 1$: If pixel=1 at least d of the corresponding m sub pixels are dark ("1"). If pixel =0 no more than $(d-\alpha m)$ of the m sub pixels is dark Security: Any subset of less than k shares does not provide any information about the secret x . All shares code "0" and "1" with the same number of dark sub pixels in average may have to improvise [5].

1.2 Halftone Images

A halftone image is made up of a series of dots rather than a continuous tone. These dots can be different sizes, different colors, and sometimes even different shapes. Larger dots are used to represent darker, more dense areas of the image, while smaller dots are used for lighter areas. Halftone images are used in newspapers and magazines because it is a much more efficient way to print images. Since a halftone image is made up of discrete dots, it requires significantly less ink to print than a continuous tone image. As long as the resolution of the image is high enough, the dots appear as a continuous image to the human eye. However, if you closely examine the images printed in a newspaper, you should be able to see the dots that make up the halftone image. Photography is referred to as continuous tone medium [7]. To be able to print photographic images the use of halftone photography was developed to achieve the effect of tonality in printing.

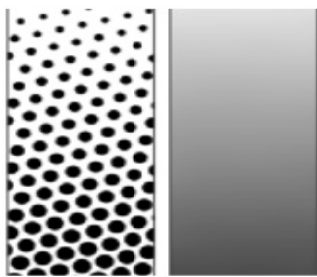


Figure 2: Half Tone Image type

1.3 Digital Watermarking

Digital Watermarking is a technology that hides information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible.

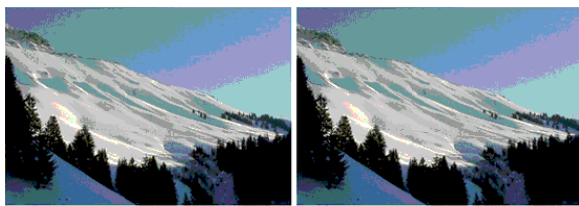


Figure 3: Image without watermark and with watermark

Digital watermarking can be of two types: (a) Visible watermarking and (b) Invisible watermarking [16]. In visible watermarking, the information is visible in the image or video. The information may be a text or a logo which identifies the owner of the media. In invisible watermarking, information is added as digital data to audio, picture or video, but cannot be perceived. The hidden information can be detected to some extent.

2. Related Work

Askari et al. in the paper [1] propose a method for processing halftone images that improves the quality of the share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share images and the recovered image is the same as for the original halftone secret image. The share images are constructed to contain meaningful cover images.

Pratiksha et al. in the paper [6] proposed a technique named halftone visual cryptography is implemented to achieve visual cryptography via halftoning. This method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information.

Ching-Sheng and Shu-Fen et al. in the paper [14] propose a novel digital watermarking scheme using visual cryptography. Based on the security property of visual cryptography, our scheme can make sure that the two shares cannot leak any information about the watermark. Unlike other researchers' method, our scheme needs not a trust third party to avoid the multiple claiming problem.

Bansal et al. in the paper [15] 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 and also helps to sustain authenticity.

3. Proposed Work

In this work secured data can be proposed. Hopfield algorithm is applied to the secret data and out generate in the form of secured data. Users use the original image that will be sending to the next user in the secured form. And image will be divided into different shares so that no one can decrypt the image. Hopfield algorithm applied makes the image secure desired data. And finally generate secured image. Hopfield algorithm is used to secure the image from various attacks using watermarking in visual cryptography.

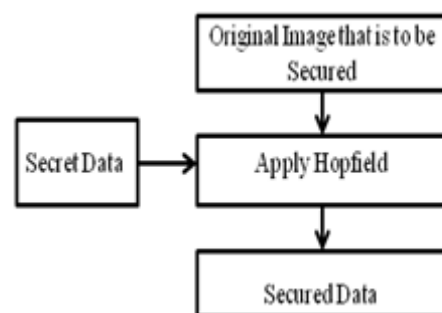


Figure 4: Flowchart of Proposed Work

4. Proposed Algorithm

A Hopfield network is a form of recurrent artificial neural network invented by John Hopfield. Neural networks are used in our proposed algorithm with hybrid cryptography technique to get well encrypted image.

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.

Steps:

Step1-Input the gray levels of $n, G=\{g_1, g_2, \dots, g_n\}$ and the number of classes of an image.

Step2-Compute the distance measure $DIS=\{d_{x,y}\}$ and the histogram $\{h_y\}$, where $X=1, 2, \dots, n$, and $y=1, 2, \dots, n$.

Step3-Set the initial number of the neurons to be x every class contains of least one gray level.

Step4-Calculate the total input of each neuron (x, i) in a row x as

$$\text{Net}_{x,i} = -1 / \sum_{y=1}^n h_y V_{y,i} \sum_{y=1}^n d_{x,y} h_y V_{y,i}$$

Step5-Apply the WTA learning scheme to compute the new output value for each neuron on the row.

Step6-Repeat step 4 and 5 for all rows and count the number of neuron for the new state. If there are no changing neurons, then go to step 7, otherwise go to step 4.

Step7- Output the final state of neuron that indicates the gray level being assigned to the given classes.

$$\text{Net}_{x,i} = \sum_{y=1}^n \sum_{j=1}^n W_{x,i,y} V_{y,j} + I_{x,i}$$

5. Proposed Digital Watermarking using Hopfield Model

5.1 Embedding the Watermark

- 1) In this approach we use an encoded image rather than the original cover image at the input layer of Hopfield Model.
- 2) For embedding the cover image, first it is encoded using encoding bits and then the image is given Hopfield Model along with the desired watermark at the input layer.
- 3) Cover image of any size is first converted into 512 by 512 pixel value and then it is further converted into Discrete Cosine Transform (DCT) block by block and encoding bits are embedded in the mid band coefficients of the blocks.
- 4) Inverse Discrete Cosine Transform (IDCT) of this embedded cover image is given to the input layer.
- 5) Hopfield Model with the desired watermark to obtain watermarked cover image and the watermark images at the output layer of Hopfield Model.

5.2 Extraction of Watermark

- 1) First the watermarked image is DCT converted block wise.
- 2) Then encoding bits are obtained from this image using

the extraction algorithm and compared with the original encoding bits.

- 3) If the match is found, then IDCT of this image is taken and given to the input layer of the Hopfield Model to extract the watermark, otherwise error message is displayed.
- 4) The suspected image is given to the Hopfield Model for extraction only when the encoded bits are successfully derived from the suspected image.
- 5) This encoded image is supplied as input to the Hopfield Model. The algorithm to obtain output watermark works only when the image is authentic.

6. Experimental Results

The following images are the experimental results:

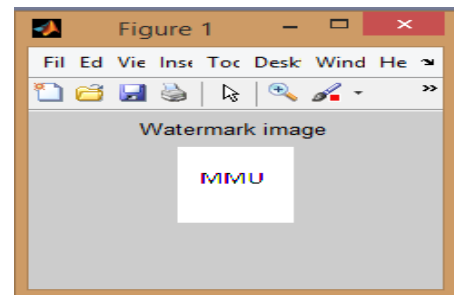


Figure 5: Secret Image

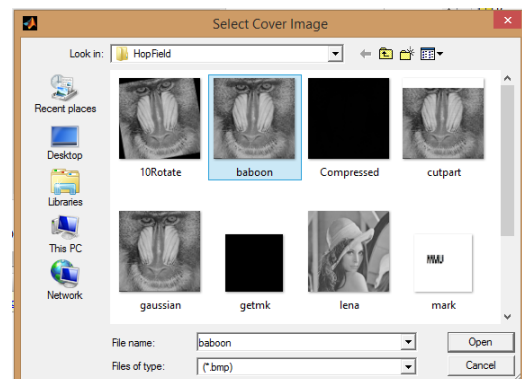


Figure 6: To Select Cover Image



Figure 7: Cover Image



Figure 8: Original Image

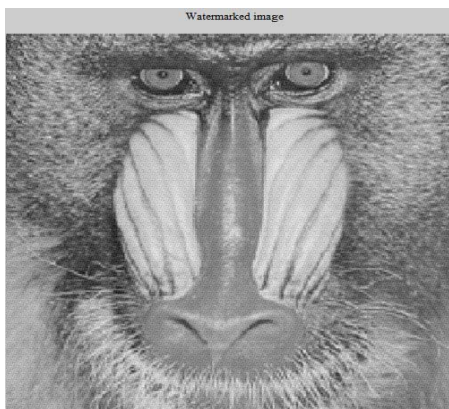


Figure 9: Embedded Image

In Fig 10, test the robustness of the proposed scheme several watermarking attacks have been applied such as Add white noise, Gaussian Low Pass Filter, Compression, Crop etc

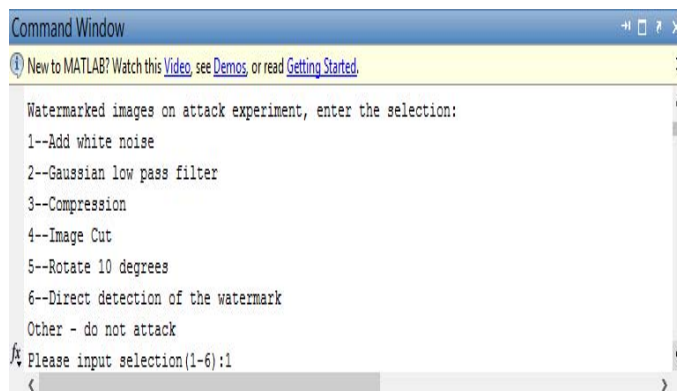


Figure 10: Enter the Image Selection

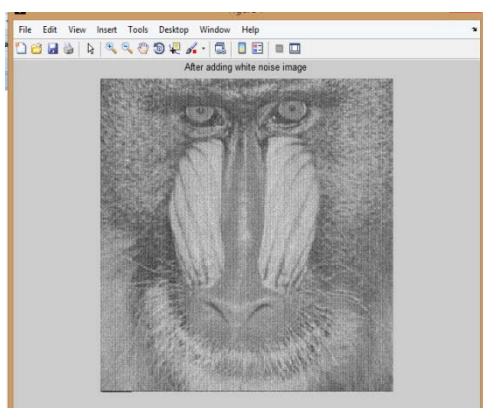


Figure 11: After adding white noise image

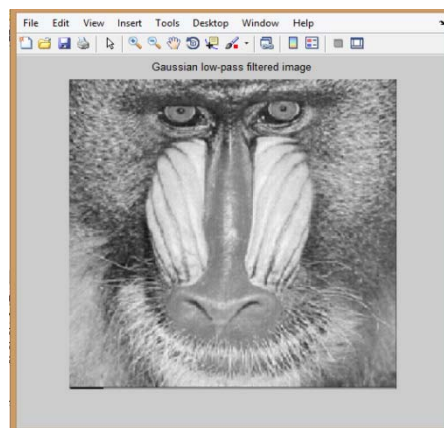


Figure 12: Gaussian Lowpass Filter

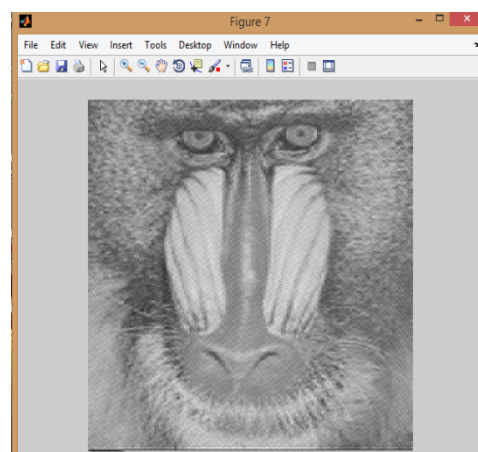


Figure 13: Compression

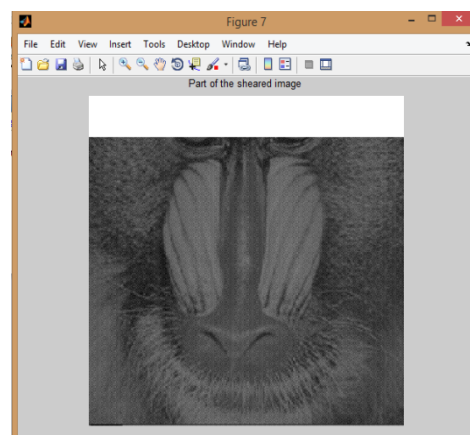


Figure 14: Crop Image

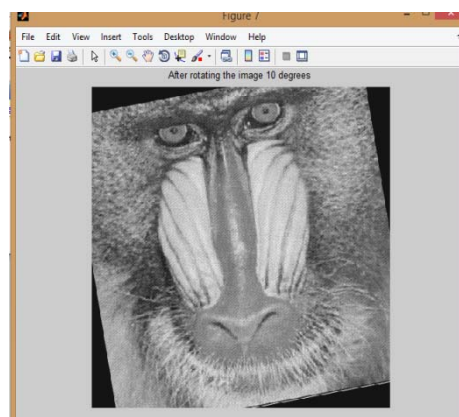


Figure 15: Rotate 10°

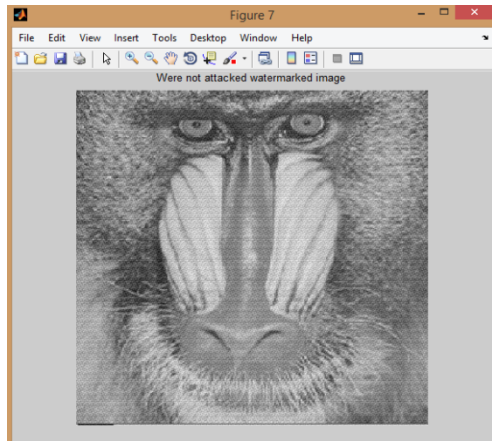


Figure 16: Without Noise

7. Analysis of the Proposed Scheme

This section shows results regarding the Peak Signal to Noise Ratio (PSNR) and Normalized Cross Correlation (NC) to evaluate the proposed watermarking scheme.

• **PSNR**- To calculate the Peak Signal to Noise ratio (PSNR), the following formula is used.

$$\text{PSNR}(\text{db}) = 10 \log_{10}$$

Where $\sigma^2 = 2$

Where $M \times N$ is the size of cover image, X_{ij} is the gray level of (i,j) pixel of the cover image. Z_{ij} denotes the gray level of (i,j) pixel of the watermarked image. X^2 Peak shows the squared peak values of the cover image. The higher PSNR means more similar encoded image and the cover image.

• **NCor**- NCor means Normalized Correlation. It means that there is visibly no difference between cover image and watermarked image i.e. two images are correlate with each other.

In the tables and diagrams we compared our proposed work with the previous implemented technique by using PSNR and NCor parameters on two images, Baboon and Lena. The Comparison shows that our technique is much better than the previous implemented technique.

Table 1: Baboon (PSNR) for FCNN and Hopfield Model

S. No	Parameters	Baboon	
		PSNR	
		FCNN	HOPFIELD MODEL
1	Add. White Gaussian Noise	33.5555	51.668
2	Gaussian Low pass filter	25.4505	48.7944
3	Compression	43.4607	43.457
4	Image cut	43.4693	43.4731
5	Rotate 10°	43.4623	43.463
6	Direct Detection of watermark	32.3705	46.0236

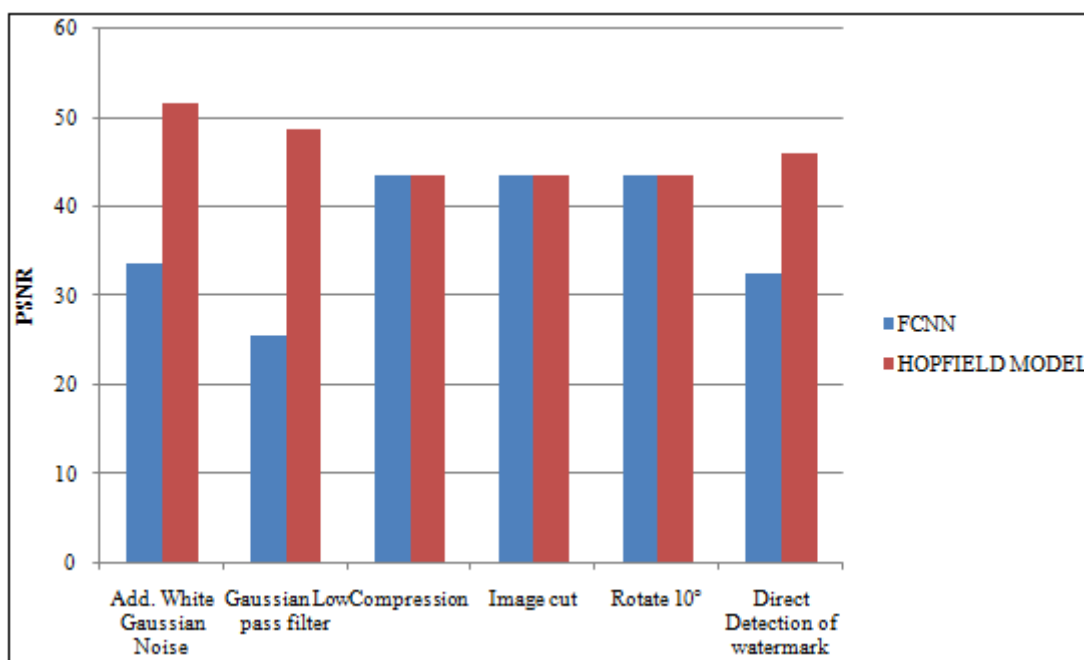


Figure 17: Baboon (PSNR) for FCNN and Hopfield Model

Table 1 and fig 17 shows the image Baboon's PSNR value by using FCNN and Hopfield model for six different parameters. In this table we can see that for three parameters compression, image cut, rotate 10° the results are almost same and by adding white Gaussian noise, Gaussian low pass filter, Direct detection of watermark the results are better for Hopfield model.

Table 2: Baboon (NCor) for FCNN and Hopfield Model

S. No	Parameters	Baboon NCor	
		FCNN	
		FCNN	Hopfield Model
1	Add. White Gaussian Noise	0.9997	0.9998
2	Gaussian Low pass filter	0.99320	0.9933
3	CompCompression	0.0041	0.0045
4	Image cut	0.0031	0.0027
5	Rotate 10°	0.0039	0.0039
6	Direct Detection of watermark	1	1

Table 2 shows the image Baboon's NCor value by using FCNN and Hopfield model for six different parameters. In this table we can see that for all parameters compression, image cut, rotate 10°, by adding white Gaussian noise, Gaussian low pass filter, Direct detection of watermark the

results are same for FCNN and Hopfield model. It means that there is visibly no difference between cover image and watermarked image i.e. two images are correlate with each other.

Table 3: Lena (PSNR) for FCNN and Hopfield Model

S. No	Parameters	Lena PSNR	
		FCNN	
		FCNN	Hopfield Model
1	Add. White Gaussian Noise	32.7601	50.2369
2	Gaussian Low pass filter	23.9393	43.7169
3	Compression	43.4587	43.4589
4	Image cut	43.4645	43.4675
5	Rotate 10°	43.4604	43.4610
6	Direct Detection of watermark	31.5751	44.4329

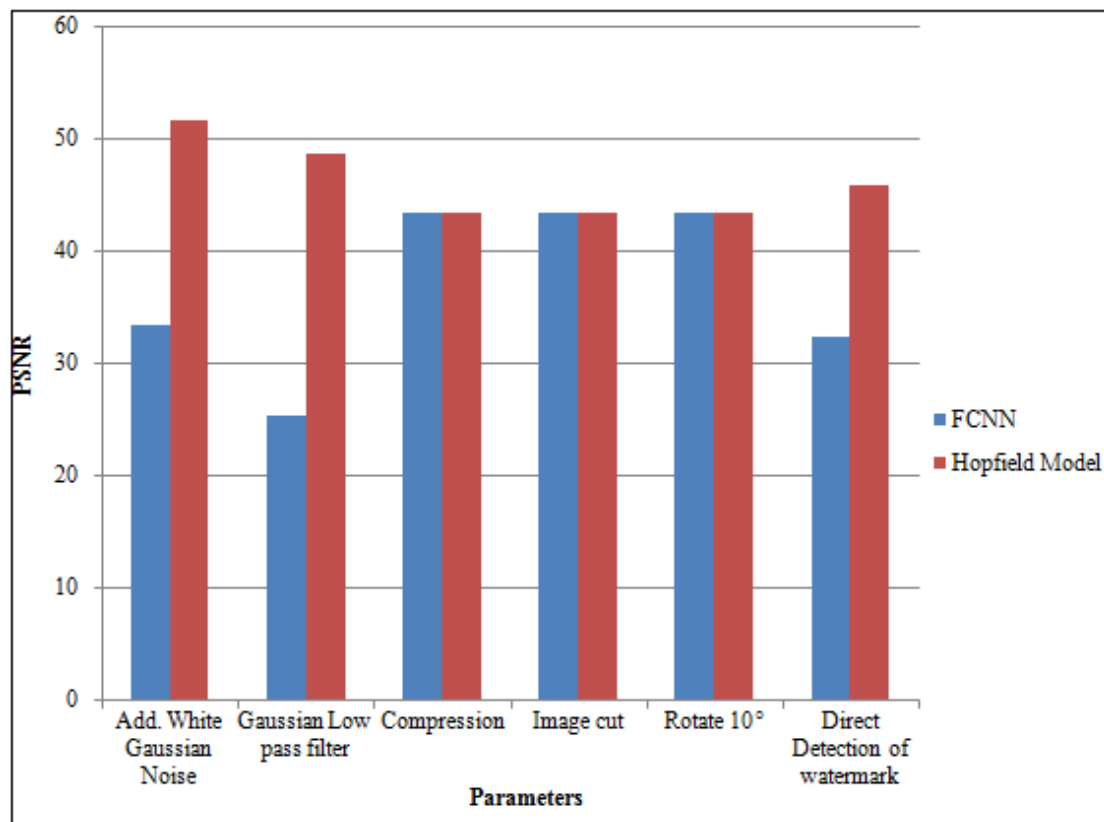
**Figure 18:** Lena (PSNR) for FCNN and Hopfield Model

Table 3 and fig 18 shows the image Lena's PSNR value by using FCNN and Hopfield model for six different parameters. In this table we can see that for three parameters compression, image cut, rotate 10° the results are almost same and by adding white Gaussian noise, Gaussian low pass filter, Direct detection of watermark the results are better for Hopfield model.

Table 4: Lena (NCor) for FCNN and Hopfield Model

S. No	Parameters	Lena NCor	
		FCNN	
		FCNN	HOPFIELD MODEL
1	Add. White Gaussian Noise	1	1
2	Gaussian Low pass filter	0.9963	0.9963
3	Compression	0.0036	0.0036
4	Image cut	0.0030	0.0026
5	Rotate 10°	0.0034	0.0034
6	Direct Detection of watermark	1	1

Table 4 shows the image Lena's Ncor value by using FCNN and Hopfield model for six different parameters. In this table we can see that for all parameters compression, image cut, rotate 10°, by adding white Gaussian noise, Gaussian low pass filter, Direct detection of watermark the results are same for FCNN and Hopfield model. It means that there is visibly no difference between cover image and watermarked image i.e. two images are correlate with each other.

8. Conclusion & Future Scope

In this paper Hopfield model are presented for digital water marking in Visual Cryptography. By using this techniques watermark is embedded in the synapse of cover image. The quality of watermarked image is same as that of cover image. In this research two images are taken and results for various parameters are compared. But Hopfield model

shows better results for Peak Signal to Noise Ratio in three parameters i.e. by adding white Gaussian noise, by using Gaussian low pass filter, direct detection of water mark and for other three parameters compression, image cut and rotate 10° the results are same. This shows that Hopfield model can resist various attack better than FCNN. In the case of normal correlation FCNN and Hopfield model shows almost same result. i.e. there is visibly no difference between the cover image and watermarked image.

In future, a new algorithm can be designed to embed and extract a watermark using neural networks in Visual Cryptography, where the neural network will be used in both the embedding process as well as the extraction process. 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.

References

- [1] N. Askari, H.M. Heys, and C.R. Moloney, "An Extended Visual Cryptography Scheme without Pixel Expansion for Halftone Images" 26th IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 2013.
- [2] Naveen Jarold K, P Karthigaikumar, N M Sivamangai, Sandhya R, Sruthi B Asok, "Hardware Implementation of DNA Based Cryptography", Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013).
- [3] Kyungroul Lee, Youngjun Lee, Junyoung Park, Kangbin Yim, Ilsun You, "Security Issues on the CNG Cryptography Library (Cryptography API: Next Generation)" Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2013
- [4] Savita Patil, Jyoti Rao, "Extended Visual Cryptography for Color Shares using Random Number Generators" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 6, August 2012.
- [5] Talal Mousa Alkharobi, Aleem Khalid Alvi, "New Algorithm for Halftone Image Visual Cryptography" <http://www.ccse.kfupm.edu.sa/~akalvi/myweb/9.pdf>.
- [6] Pratiksha P.Patil, 2Y.M. Patil, "Visual Cryptography Based on Halftoning" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) PP: 65-69.
- [7] Zhi Zhou, Gonzalo R. Arce Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions On Image Processing, Vol. 15, No. 8, August 2006.
- [8] Young-Chang Hou "Visual cryptography for color images" Pattern Recognition 36 1619 –1629, 2013.
- [9] Sozan Abdulla, "New Visual Cryptography Algorithm For Colored Image" Journal Of Computing, Volume 2, Issue 4, April 2010.
- [10] Cryptography Algorithms, http://en.wikipedia.org/wiki/Cryptography#Symmetric_key_cryptography
- [11] Er.Supriya Kinger, "Efficient Visual Cryptography" Journal of Emerging Technologies In Web Intelligence, Vol. 2, No. 2, May 2010.
- [12] Nicolae Popoviciu, Mioara Boncut, "On the Hop field algorithm Foundations and Examples" General Mathematics, Vol. 13, No. 2, 35-50, 2005.
- [13] Kai-Hui Lee and Pei-Ling Chiu, "An Extended Visual Cryptography Algorithm for General Access Structure" IEEE Transaction on Information Forensics and Security, Vol. 7, No. 1, February 2012.
- [14] Ching-Sheng Hsu and Shu-Fen Tu, "Digital Watermarking Scheme with Visual Cryptography", Proceedings of the International Multi Conference of Engineers and Computer Scientists, Vol I IMECS 2008, 19-21 March, 2008.
- [15] Bansal A. and Bhaduria S.S., "A Novel approach using full counter propagation neural network for watermarking", IJCSE, vol.02, pp 289-296, 2010.
- [16] Chang C and Sheng-Jyun S, "A Neural network based Robust watermarking scheme", National science council Taiwan, NSC 92-2213E-224-041.
- [17] Zhou Y. Wang J. and Yin J., "Design and Analysis of Positively Self-Feedback Hopfield Neural Network for Crossbar Switching", IJCSNS, Vol.7 No.5, May 2007.
- [18] Ishwarjot Singh, J. P. Singh Raina "Advance Scheme for Secret Data Hiding System using Hop-field & LSB", International Journal of Computer Trends and Technology (IJCTT), vol. 4 Issue 7, July 2013.
- [19] <http://www.en.wikipedia.org>
- [20] <http://www.google.com>.

Author Profile



Ramandeep Kaur is Student of M.Tech in the department of Computer Science and Engineering at Sri Guru Granth Sahib World University (SGGSWU), Fatehgarh Sahib, Punjab. She has done B.Tech from Continental Group of Institutes, Jalvehra, Fatehgarh Sahib under Punjab Technical University, Jalandhar.