A Review of Applications of Neural Network In Watermarking

Neha Bansal
Assistant Professor
Dept. of Electronics & Comm.
GLNAIT Mathura

Pooja Pathak
Assistant Professor
GLA University, Mathura

ABSTRACT
This paper presents a review of the literature on the use of artificial neutral networks in digital watermarking. Digital watermarking is a recent technology evolved to prevent illegal copy or reproduction of digital content. Different neural network based approaches have been categorized based on their applications for embedding and extracting components of watermarking.

Keywords
Watermarking, Steganography, Artificial Neural Networks.

1. INTRODUCTION
The emergence of the Internet with rapid progress of information technologies, digital contents are commonly seen in our daily life distributed through the network. The digital contents are easy to make an exact copy, illegal distribution and copying of digital contents has become main concerns for authors, publishers and legitimate owners of the contents [1]. There are several ways to protect digital content. One can protect the content by encrypting it, but this avoids free distribution and circulation of the content through the network, which is most of the time not desirable to the author of the content. Therefore, for the purpose of protecting the content we use digital watermarking by which content should not be encrypted or scrambled.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity [2]. Steganography conceals a hidden messages to a content but the existence of a message is kept secret [3]. In another word, steganography is a technique to conceal information into digital content files for purposes such as secret communication and covert channel.

Digital watermarking is a recent technology evolved to prevent illegal copy or reproduction of digital content. Many techniques based on spatial and frequency domain have been developed in the recent past and are being used for effective watermarking. However, there is always a tradeoff between robustness and imperceptibility features of watermarking offered by these techniques [10]. Digital watermarking is the process of embedding information into a digital signal in a way that it is difficult to remove [2]. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time. In visible watermarking, the information is visible in the picture or video. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such [10]. There are many digital watermarking and steganographic algorithms been proposed, but there are difficulties to use one algorithm together with another because each other obstruct the embedded information and causing one to destroy another. But there is another method that does not damage the target content; it has an ability to collaborate with another algorithm to strengthen the security of information hiding method. This characteristic is useful where one already manage digital rights using one watermarking algorithm or controls the file integrity using hash functions. If one wishes to strengthen the robustness of watermark using another algorithm, one must examine and assure that applying the algorithm will not affect embedded watermarking signals in advance. Furthermore, applying another watermarking algorithm will alter the fingerprint of the content managed by hash functions and forces administrator to recalculate a new hash values after applying new watermarking algorithm, which most of the time, result in higher calculation cost and time. Because proposed methods do not affect the target content at all, one can apply new watermark seamlessly without altering the fingerprint using proposed method. [4]

The term neural network was traditionally used to refer to a network or circuit of biological neurons. The modern usage of the term often refers to artificial neural networks, which are composed of artificial neurons or nodes. Artificial neural networks may either be used to gain an understanding of biological neural networks, or for solving artificial intelligence problems without necessarily creating a model of a real biological system. Artificial neural networks have been applied successfully to speech recognition, image analysis and adaptive control, in order to construct software agents or autonomous robots [10].

From fig.1 the interval activity of the neuron can be shown to be:

$$v_k = \sum_{j=1}^{p} w_{kj} x_j$$

The output of the neuron, y_k, would therefore be the outcome of some activation function on the value of v_k.

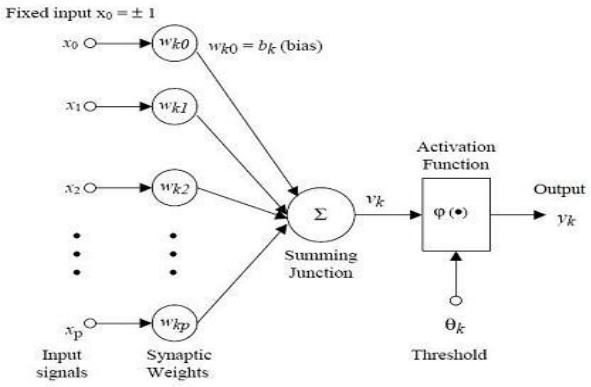

Fig 1

2. USE OF NEURAL NETWORK IN DIGITAL WATERMARKING

Water marking is an approach to hide information into target content and retrieve information from the target content without damaging it. With this method, the use of neural network is the key technique. The embedder adjusts a neural network weights with desired hidden bit code to target content by supervised learning of the neural network. This conditioned neural network works as a classifier to recognize a hidden bit pattern from the content which embedder associates to the target content. Therefore, extractor uses this neural network weights for extracting the hidden bit codes. For the applications for digital watermarking and steganography, this extraction keys must be shared among embedder and extractor in order to extract a proper hidden bit codes from the target content. Considering the difficulties for secret key transportation, this method should be applied in situations where the embedder and the extractor are same person or use certification authorities to assure the integrity of the key[4]. This method can be more secured by applying message digest technique to the watermarked image.

Er. Ashish Bansal et al. proposed, Backpropagation Neural Network is being used for training cover image fragments into corresponding target watermark image fragments. Encoding the watermark using the weights of Backpropagation network has reduced the chances of watermark destruction with image processing operations. The watermark image needs to be supplied with the trained network weights to produce the watermark output. As the target watermark image is normalized with the help of random state key Rs which is stored in the image itself, this is used for the authenticity purpose. Results have revealed that a Backpropagation Neural Network may be successfully employed to provide a successful watermarking scheme by training the cover image fragments for the corresponding target watermark image fragments.[5]

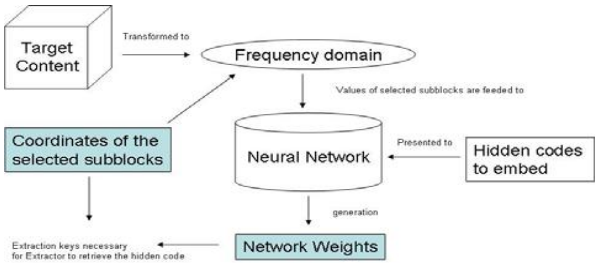

Fig 2: Embedding procedure

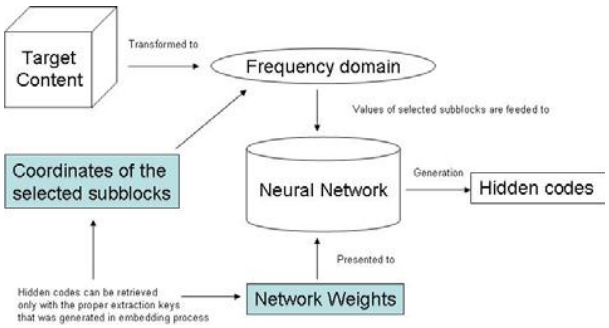

Fig 3: Extracting procedure

Yu et al. [6] introduced a process to introduce the training process for a neural network memorizing the characteristics of the relations between watermark and original image. The signature S is retrieved by using the adaptive capability of the trained neural network. This step is performed in the watermark extraction phase. The original signature is compared with this signature and identifies the copyright of owner's intellectual property. Full counterpropagation neural network (FCNN) was used by Chuan-Yu Chang et al for image watermarking [8].Neural networks have been suggested as alternative approaches owning to high fault tolerance and potential for adaptive training. The full counterpropatation neural network is a supervised-learning network with capacity of bidirectional mapping. This watermarking method integrated the embedding and extraction procedure into a full counterpropagation based neural network. The FCNN could resist various attacks. In addition, the watermark embedding procedure and extracting procedure is integrated into the FCNN. By doing so, this approach simplifies traditional procedures. The experimental results show that the application achieved robustness, imperceptibility and authenticity in digital watermarking. Maher EI Arbi et al. suggested video watermarking based on neural network [7]. They propose a novel digital video watermarking scheme based on multi

resolution motion estimation and artificial neural network. A multi resolution motion estimation algorithm was adopted to preferentially allocate the watermark to coefficients containing motion. In addition, embedding and extraction of the watermark were based on the relationship between a wavelet coefficient and its neighbor's. A neural network was given to memorize the relationships between coefficients in a 3x3 block of the image. Experimental results showed that embedding watermark where picture content is moving is less perceptible. Further, it showed that the scheme was robust against common video processing attacks. Guohua Wu el al. [9], suggested Counter propagation Neural Network (CNN) based method for fast audio digital watermark. By making use of the capabilities of memorization and fault tolerance in CPN, watermark is memorized in the nerve cells of CPN. In addition, they adopt a kind of architecture with an adaptive number of parallel CPN to treat with each audio frame and the corresponding watermark bit. Comparing with other traditional methods by using CPN, it was largely improve the efficiency for watermark embedding and correctness for extracting, namely the speed of whole algorithm. The extensive experimental results showed that, we can detect the watermark exactly under most of attacks. This method efficaciously trade off both the robustness and inaudibility of the audio digital watermark.

3. CONCLUSION

In this paper, we have reviewed several methods which adopt neural network approach for watermarking. Actually with steganalysis, we can find the loop holes in our algorithm and we can improve them. In digital watermarking, we can make our algorithm more robust and fast with the help of the neural approach. Imperceptibility and authenticity can be achieved with neural network support in digital watermarking.

Proposed methods use different neural network models for classifying the input patterns to corresponding hidden signals.

There is a lot of work that still needs to be done. Many other watermarking schemes and algorithm will be included in this research and extensive tests need to be done with larger number of images.

4. REFERENCES

[1] H. Sasaki, editor. Intellectual Property Protection for Multimedia Information Technology. IGI Global, 12 2007.

[2] Ren –Junn Hwand, Chuan-Ho Kao and Rong-Chi Chang, "Watermark in Color Image" in Proc. First International

Symposium on cyber worlds, 2002, pp 225-229

[3] F. Rosenblatt. The perceptron a probabilistic model for information storage and organization. Brain Psych. Revue, 62:386.408, 1958.

[4] K. Naoe et al. Damageless Information Hiding using Neural Network on YCbCr Domain. IJCSNS, 09 2008.

[5] A. Bansal et al. Application of Back propagation Neural Network to generate fragmented watermarks and Full Watermark by Union. IJCSNS, 10 2008.

[6] Yu et al, "Digital Watermarking Based on Neural Networks for Color Images", Elsevier Signal Processing, 81 (2001), p.p. 663-671.

[7] Maher El' Arbi et al, "Video Watermarking Based On Neural Networks", ICME 2006, pp. 1577-1580.

[8] Chuan-Yu Chang et al, "Using a Full Counter propagation Neural Network for Image Watermarking", International Computer Symposium, Dec. 15-17, 2004.

[9] Guohua Wu, Xiaodong Zhou, "A Fast Audio Digital Watermark Method Based on Counter-propagation Neural Networks", International Conference on Computer Science and Software Engineering, 2008, pp. 583-586.

[10] D. T. Meva et al, "Adoption Of Neural Network Approach In Steganography And Digital Watermarking For Covert Communication And Copyright Protection", International Journal of Information Technology and Knowledge Management July- December 2011, Volume 4, No. 2, pp. 527-529

[11] D. Artz. Digital steganography: hiding data within data. IEEE Internet Computing, 5(3):75.80, May/June 2001.

[12] D. Rumelhart and J. McClelland. Parallel distributed processing: explorations in the microstructure of cognition, vol.1: foundations. MIT Press Cambridge, MA, USA, 1986.

[13] S. Katzenbeisser and A. P. Fabien, editors. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House Publishers, 1 2000.

[14] D. Kahn. The history of steganography. In Proceedings of the First International Workshop on Information Hiding, pages 1.5, London, UK, 1996.

[15] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker. Digital Watermarking and Steganography. Morgan Kaufmann, 2nd edition, 11 2007.

[16] David Point cheval, "Neural networks and their cryptographic applications," in Proc. of the IEEE Symposium on Foundations of Computer Science, 586 – 597, 1993.

[17] G. C. Meletiou, D. K. Tasoulis, and M. N. Vrahatis, "A first study of the neural network approach in problems related to cryptography," in Proc. of the FEES conf. on Financial Engineering, E-commerce & Supply Chain, and Strategies of Development, 2002.

[18] W. Kinzel, and Kanter, "Neural Cryptography," in Proc. 9th In1'l Conf. on Neural Information Processing ICONIP'02), vol. 3, pp. 1351-1354, 2002.

[19] Wolfgang Kinzel and Ido Kanter. Interacting neural networks and cryptography. Advances in Solid State Physics. B Kramer (ed.), (Berlin: Springer) (42): 383-91.2002.

[20] J. Lin, H. Tsai, and P. Yu, "Color Image Watermarking Based on Neural Networks," Advances in Neural Networks, pp. 651-656, 2004.

[21] J. Lin, H. Tsai, and P. Yu, "Short communication Digital watermarking based on neural networks for color images," Signal Processing, (81), 663-671, 2001.

[22] K.J.Davis and K.Najarian "Maximizing Strength of Digital Watermarks Using Neural Networks", in Proc. International Joint Conf. Neural Network, 2001, vol 4, pp. 2893-2898.

[23] R.Schyndel, A.Tirkel, and C.Osborne, "A Digital Watermark" in Proc. IEEE Int. Conf. on Image Processing, Nov. 1994 ,vol II, pp.86-90.

[24] D.Kundur and D. Hatzinakos, "A Robust Digital Image Watermarking Method using Wavelet – Based Fusion", in Proc, IEEE Int. Conf. on Image Processing , Oct. 1997, vol. I, pp. 544-547.

[25]I. Pitas, "A Method for Signature Casting on Digital Images", in Proc, IEEE Int. Conf. on Image Processing ,Sept 1996,vol.III,pp.215-218.

[26] Ren –Junn Hwand, Chuan-Ho Kao and Rong-Chi Chang, "Watermark in Color Image" in Proc. First International symposium on cyber worlds, 2002, pp 225-229.