Survey on Digital Video Watermarking

Poonam Uttam Shelke¹, Parul S. Arora Bhalotra²
¹,²E&TC Department, Savitribai Phule Pune University

Abstract: In today’s Digital era, everything is at fingertips with the help of fast internet search engines and plenty of available information in all domain. The data can easily be copied, transferred, downloaded, edited and many more things can be done. Watermarking is recommended to ensure that the rights of the owner remain intact with the original work. Watermarking may be visible or invisible depending upon its application. Here we have presented a review on various Video Watermarking techniques.

Keywords: Digital Video Watermarking, copyright protection, Neural networks, Hopfield Neural Network, Full counter propagation neural network (full CPN), BPN, RBF

I. INTRODUCTION

“Watermark”, n. means “a distinguish mark impressed on a paper during manufacture which is visible when the paper is held up to the light”. Origin: German word “wassermarke”. According to the definition provided by Cox et al. [1], a watermark is an “identification code that is permanently embedded in the data and remains present within the data after any decryption process”. Tirkel et al. [2] were the first to introduce the term “digital watermarking” (and “electronic watermarking”) in 1993, referring to their algorithms designed to hide data in digital images. Since then, watermarks have been widely used for various purposes of security which include data hiding, copyright protection, data authentication, copy prevention and rightful ownership protection of digital media. Nowadays, the information in the form of text, image, audio, video or multimedia format is readily available online. To ensure that the rights of the owner are intact, watermarking the content is essential. The watermark can be visible (example logo or name easily detectable by human eyes) or invisible (not detectable by human eyes, embedding/ extraction algorithms used). Earlier Cryptography was used as a security measure but it has a limitation that once it is decrypted it doesn’t provide further security. Watermark, on the other hand, is embedded such that it cannot be separated without damaging the content. Major characteristics of watermarking are robustness, security, transparency and data payload size. The concept of image watermarking can be extended to video watermarking by viewing each frame as an isolated image. These video frames are used for hiding the watermarked data.

II. LITERATURE REVIEW

An overview of existing technologies is discussed in this section. A good watermarking algorithm should be robust against geometrical and removal transformations. Video watermarking is different as compared to image because video watermarking has a large amount of data and redundancies between video frames. A good video watermarking algorithm must be robust against video compression, frame dropping, frame swapping, geometric attacks, frame rate conversion, frame cropping, collusion attacks, noise, filtering, lighting change, histogram equalization, etc. [4]. Existing approach include spatial domain, frequency domain, MPEG coding structure and neural network based techniques.

Mostafa [5] has proposed novel technique for embedding a digital watermark into video frames based on motion vectors and discrete wavelet transform (DWT). The binary image watermark is divided into blocks and each watermark block is embedded several times in each selected video frame at different locations. The block-based motion estimation algorithm is used to select the video frame blocks having the greatest motion vectors magnitude. The DWT is applied to the selected frame blocks and then, the watermark block is hidden into these blocks by modifying the coefficients of the Horizontal sub-bands (HL). Adding the watermark at different locations in the same video frame makes the scheme more robust against different types of attacks.

Mishra et al. [6] used Back-Propagation Neural network (BPN) to embed the watermark in selected video frames that have a maximum motion in X and Y directions. After that, the watermark is embedded into the DWT coefficients of the blue channel of the selected frames.

Nakano-Miyatake et al. [7] have proposed an algorithm that embeds and detects the watermark in the compressed domain (MPEG-2). The watermark is embedded into the coefficient of the DCT blocks of I-frame and P-frame using the adequate embedding energy. However, the adequate embedding energy is computed for each block using Human Visual System (HVS) criteria.
Wen [8] has proposed a novel scheme of digital image watermarking based on the combination of dual-tree wavelet transform (DTCWT) and probabilistic neural network. The original image is decomposed by DTCWT and then the watermark bits are added to the selected coefficients blocks. Because of the learning and adaptive capabilities of neural networks, the trained neural networks can recover the watermark from the watermarked images.

Zhang [9] proposed a blind watermarking algorithm using Hopfield neural network and then observed the watermarking capacity based on the neural network. Hopfield neural network is a non-linear dynamical system that uses computational energy function to evaluate the stability property. The energy function always decreases toward a state of lowest energy. The neuron states in a Hopfield network are usually binary. The gray scale test image was decomposed and for each pixel, a decision had to be made whether the pixel should be modified or not. This was stored in a matrix. The watermark amplitude was decided based on this matrix. Basin of attraction is the set of points in the space of the system. The radius of attraction basin is designed as the largest Hamming distance within which almost all states are similar to the pattern. The attraction basin of Hopfield neural network decides the watermarking capacity.

Chang [10] presented a specific designed full counter-propagation neural network for digital image watermarking. Different from the traditional methods, the watermark was embedded in the synapses of the Full Counter-Propagation Neural Network (FCNN) instead of the cover image. The quality of the watermarked image was almost same as the original cover image. Most of the attacks could not degrade the quality of the extracted watermark image as the watermark was stored in the synapses.

C. R. Piao et al. [11] proposed a new blind watermarking scheme in which a watermark was embedded into the DWT (Discrete Wavelet Transform) domain. Radial Basis Function (RBF) Neural network was used to learn the characteristic of the image, using which the watermark would be embedded and extracted.

Wang [12] 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 [13] proposed a video watermarking algorithm which combined neural networks with motion estimation in the wavelet domain. A novel digital video watermarking scheme based on 3D-DWT and an artificial neural network was also proposed later [14]. Here, a 3D wavelet transform was performed on each of the selected video shots and then the watermark was embedded in the LL sub-band wavelet coefficients of the low-pass frames. In order to ensure perceptual invisibility, the coefficient was selected adaptively to embed the watermark and the embedding intensity was adaptively controlled using statistical characteristics such as mean and standard deviation.

Jin [15] proposed a digital watermarking scheme using neural networks. The original image was divided into some 8*8 blocks. Then neural networks were used according to different textural features and luminance of each block to decide adaptively different embedding strengths. By exploiting neural networks, it provides the maximum watermark embed strength which is robust to common attacks. By different embedding strengths decided by neural networks according to different textural features and the mean luminance of each block, the resulting watermarked image is extremely robust to a wide range of image JPEG compression. It does not require the original image for watermark detection.

In [16], a novel blind digital watermarking scheme based on BP neural network in the wavelet domain is presented. HVS characteristics were taken into consideration to make the watermark invisible during the process of watermark embedding. An artificial neural network was applied to watermarking to enhance the performance of conventional watermarking techniques.

Paper [17] proposed a color image watermarking algorithm based on fractal and neural networks in Discrete Cosine Transform (DCT) domain. The algorithm utilized the fractal image coding technique to obtain the characteristic data of a gray-level image watermark signal and encrypted it by a symmetric encryption algorithm before it was embedded. By exploiting the abilities of neural networks and considering the characteristics of HVS, a Just Noticeable Difference (JND) threshold controller was designed to ensure the strength of the embedded data adapting to the host image itself entirely. Thus the watermark scheme possessed dual security characteristics.

Yi [18] 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 learned 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 [19] 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...
represents the copyright symbol and also reflects the feature of the image. Arnold transform was used to increase the security of watermark. The backpropagation neural network was applied to improve its imperceptibility and robustness.

C.-Y. Chang et al. [20] used a full counter-propagation neural network (FCNN) for copyright protection where the ownership information was embedded and detected by a specific FCNN. The watermark is stored in the synapses of the FCNN. Since the FCNN has storage and fault tolerance, most attacks did not degrade the quality of the detected watermark image. The watermark embedding and retrieval procedures were integrated into the FCNN.

Arbi [21] proposed a video watermarking algorithm that embedded different parts of a single watermark into different shots of a video under the wavelet domain. Based on motion activity analysis and region complexity different regions of the original video are separated into perceptually distinct categories. This algorithm prevents the occurrence of motion artifacts as watermark moves along with the moving objects. Zhang and Li [22] proposed a novel watermarking algorithm for non-compressed video where the original video frame is divided into 8x8 blocks. DCT (Discrete Cosine Transform) was applied on these 8x8 blocks to calculate the energy from the DCT coefficients. According to the energy calculated, the embedding areas in the blocks were classified based on information contained and motion. In the watermark extraction process, a BPN (Back Propagation Network) was trained in order to detect the areas where the watermark is embedded based on the DCT coefficient energy values.

We can summaries properties of Digital Video Watermark [23] as:
1) **Invisibility**: The digital watermark should be not be seen by our eyes.
2) **Robustness**: It's watermark resistance to various attacks. High robustness preserves the nature of the video.
3) **Perceptible**: It means the presence of our mark is noticeable. Getting Imperceptibility is a great task for a researcher.
4) **Capacity**: It designates the period of the embedded message into digital video.
5) **Fidelity**: This factor decides if video handed to the public is degraded or not. It should be high for good watermark.
6) **Computational Cost**: it refers to the cost or time necessary for embedding and extracting the watermark from the digital video. For better working, digital video watermarking scheme computational cost should be minimized.
7) **Interoperability**: the watermark should carry on video including the compression and decompression operations performed regarding that video.
8) **Blind/informed detection**: In informed watermarking schemes, the detector requires access to the original video without watermark for the extraction process. In blind watermarking, Detectors do not require any original information.
9) **False positive rate**: An inaccurate positive refers detection of watermark information given by a digital media which can include video or an image that really does not actually contain that watermark.

A. **Neural Networks**

A neural network is a processing device, either an algorithm or an actual hardware, whose design was inspired by the design and functioning of animal brains and components thereof. The neural networks have the ability to learn by example, which makes them very flexible and powerful. For neural networks, there is no need to devise an algorithm to perform a specific task, that is, there is no need to understand the internal mechanisms of that task. These networks are also well suited for real-time systems because of their fast response and computational times which are because of their parallel architecture [24]
3) **Signal function:** A function that generates the output signal of the neuron based on its activation is called a signal function. Functions may differ from neuron to neuron within the network; although most networks are field-homogeneous i.e. all neurons within a field or layer have the same signal function.

4) **The pattern of connectivity:** This determines the inter-neuron connection architecture or the graph of the network.

5) **Activity aggregation rule:** This aggregated the activity at a particular neuron.

6) **Activation rule:** This function determines the new activation level of a neuron based on its current activation and its external inputs.

7) **Learning rule** [26]: The learning rule provides a means of modifying correction strengths based on both the external stimuli and the network performance with the aim of improving the network performance.

8) **Environment:** The environments in which neural networks can operate could be deterministic (noiseless) or stochastic (noisy). A neural network can be viewed as a weighted directed graph in which artificial neurons are nodes and directed weighted edges represent connections between neurons. Local groups of neurons may be connected in either Feed-forward architecture (i.e. no loops) or Feedback architecture.

Different types of artificial neural networks are

![Diagram of different types of neural networks](image)

**Fig. 2 Types of Neural networks**

**B. Back Propagation Neural Network**

The aim of the neural network is to train the net to achieve a balance between the net’s ability to respond (memorization) and its ability to give reasonable responses to the input that is similar but not identical to the one that is used in training (generalization).

![Diagram of back propagation network](image)

**Fig. 3 Architecture of Back propagation network** [27]

A back-propagation neural network is a multilayer, feed-forward neural network consisting of an input layer, a hidden layer and an output layer. The neurons present in the hidden and output layers have biases, which are the connections from the unit whose activation is always 1. The bias terms also act as weights.
C. **Radial Basis Function Network (RBF):**
It is a classification and functional approximation neural network developed by M.J.D.Powell. The network uses the most common nonlinearities such as sigmoidal and Gaussian kernel functions. The Gaussian functions are also used in regularization networks.

![Fig.4 Architecture of RBF](image)

In three layers RBF network the input vector is the first layer, hidden layer is RBF neurons and the third layer is the output layer containing linear combination neurons.

D. **Hopfield Neural Network**
John J. Hopfield developed a number of neural networks based on fixed weights and adaptive activations.

![Fig.5 Architecture of Hopfield Neural Network](image)

The architecture consists of a set of neurons forming a multiple loop feedback system. The number of feedback loops is equal to the number of neurons. Hopfield networks normally have units that take on values of +1 or -1.

E. **Full Counter Propagation Neural Network (full cpn):**
Counter propagation networks were proposed by Hecht Nielsen in 1987. They are multilayer networks based on the combinations of the input, output and clustering layers. It is the extension of forwarding only counter propagation network, which is a supervised learning network with the capacity of bi-directional mapping. The counter propagation network is basically constructed from an instar-outstar model. This model is a three-layer neural network that performs input-output data mapping, producing an output vector \( y \) in response to an input vector \( x \), on the basis of competitive learning. The three layers in an instar-outstar model are the input layer, the hidden (competitive) layer and the output layer. The connections between the input layer and the competitive layer and the instar structure, and the connections existing between the competitive layer and the output layer are the outstar structure. The competitive layer is winner-take-all network or a Maxnet with lateral feedback connections. There exists no lateral connection within the input layer and the output layer. The connections between the layers are fully connected.
The Full counter propagation network [24] represents a large number of vector pairs $x: y$ by adaptively constructing a look-up-table. The vectors $x$ and $y$ propagate through the network in a counter flow manner to yield output vectors $x^*$ and $y^*$, which are the approximations of $x$ and $y$, respectively. During the competition, the winner can be determined either by Euclidean distance or by dot product method.


Using full search block matching method multi-resolution motion estimation is performed on input video. In the discrete wavelet decomposition of the image relationship among coefficients is performed using Back Propagation Neural Network (BPNN). Watermark is inserted by altering the coefficient value of the locations decided by secret key in the image.

Formula:

$$I_{w(x,y)} = \begin{cases} \max \{ I_{x,y}, \sigma_1 + \delta \} & \text{if } w_i = 0 \\ \min \{ I_{x,y}, \sigma_0 - \delta \} & \text{if } w_i = 1 \end{cases}$$

Where $w_i$ is $i^{th}$ bit of watermark,

$I_{x,y}$ is original coefficient,

$I_{w(x,y)}$ is the watermarked coefficient.
σ is the embedding strength

Three level DWT is performed to obtain watermarked image. Using motion vectors and selected previous frame coefficients the new location for watermark is calculated. During watermark detection process, the watermark is extracted using watermarked video, secret key, DWT and model of BPNN. Average of watermark obtained from different frames taken to reduce attack effect. Experimental results show that proposed scheme is robust against common attacks.

III. CONCLUSIONS

In this paper, we have presented a review on various digital video watermarking techniques based on neural networks. Many of these techniques have been able to satisfy the basic requirement of watermarking i.e. the extraction process does not require the original signal or in other words, the algorithm is blind. The neural networks used include Back Propagation Network (BPN), Radial Basis Function Neural Network (RBF), Full Counter Propagation Network (full CPN) and Hopfield Neural Network. An ideal watermarking algorithm should be blind in nature, robust against attacks, should guarantee correct and fast watermark detection with low error rate.

Future scope of work would include other neural networks and fuzzy logic.

IV. ACKNOWLEDGMENT

I would first like to thank my guide Dr. Parul Arora of the JSPM’s ICOER at Savitribai Phule Pune University. The doors to her office were always open whenever I had a question about my writing. She steered me in the right the direction whenever she thought I needed it.

I would also like to acknowledge HOD and staff members for providing me valuable resources for completion of this work.

REFERENCES

[16] Song Huang and Wei Zhang, Wei Feng and Huaqian Yang, “Blind Watermarking scheme based on Neural Networks”, In the Proceedings of the 7th World Congress on Intelligent Control and Automation, June 25-27, 2008.


