Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 6, 1560-1568 (2020)

www.astesj.com

Special Issue on Multidisciplinary Sciences and Engineering

ASTESJ

ISSN: 2415-6698

A Computational Modelling and Algorithmic Design Approach of Digital Watermarking in Deep Neural Networks

Revanna Sidamma Kavitha[1 *], Uppara Eranna[2], Mahendra Nanjappa Giriprasad[1]

[1]*Department of Electronics and Communication Engineering, Jawaharlal Nehru Technological University Anantapur, Ananthapuramu, 515002, India*

[2]*Department of Electronics and Communication Engineering, Ballari Institute of Technology and Management, Ballari-583104, India*

ARTICLE INFO

Article history:
Received: 21 October, 2020
Accepted: 12 December, 2020
Online: 25 December, 2020

Keywords:
Digital Water Marking
Neural Networks
Algorithms
Convolution Neural Network

ABSTRACT

In this paper we propose an algorithmic approach for Convolutional Neural Network (CNN) for digital watermarking which outperforms the existing frequency domain techniques in all aspects including security along with the criteria in the neural networks such as conditions embedded, and types of watermarking attack. This research addresses digital watermarking in deep neural networks and with comprehensive experiments through computational modeling and algorithm design, we examine the performance of the built system to demonstrate the potential of watermarking neural networks. The inability of intruder towards the retrieval of data without the knowledge of architecture and keys is also discussed and results of the proposed method are compared with the state of the art methods at different noises and attacks.

1. Introduction

The research presented here is the extension of the work originally presented at International Conference on Artificial Intelligence and Signal Processing (AISP),2020 [1]. The digital revolution and the internet have paved a way to the creation of massive digital information containing images, videos, transactions, intellectual properties. The ease with which this digital data can be copied and reproduced has created avenues for copyright infringements. The massive explosion of digital multimedia devices has resulted in the creation of a large chunk of data and increased demand (and role) of data hiding techniques. Digital watermarking is employed for various applications such as copyright protection (ownership assertion), broadcast monitoring (really broadcasted or not), tamper detection (persistent item identification, forgery detection), data authentication and verification (integrity verification), fingerprinting (transaction tracking and privacy control), content description (labelling and captioning), publication monitoring and copy control (unauthorized distribution) covert communication (data hiding), Medical applications (Annotation and privacy control), and Legacy system enhancement (backward compatibility) [2]. All information hiding techniques revolve around 3 parameters: Imperceptibility, robustness and payload capacity [3]. While payload capacity is important in steganography, in digital watermarking the trade-off between imperceptibility and robustness is needed for the excellent quality of data hiding [4]. The ability of a data hiding technique to remain unchanged to human perception is called imperceptibility i.e. an unintended user should not be able to make out whether the image has undergone watermarking [5]. Robustness is the ability of watermarked data to be immune to attacks and threats. Other goals of digital watermarking are Security (watermark should be secret and undetectable by an unauthorized parties), effectiveness (ease of detection immediately after embedding), uniqueness (multiple watermarks to coexist), cost effectiveness (in terms of hardware and computational speed), and scalability [6]. Several Artificial Intelligent techniques such as neural network, evolutionary computation, fuzzy logic, swarm intelligence, Probabilistic reasoning and multi-agent systems were proposed to secure watermark in digital media [7]. These techniques will be employed at either the transmitter side during embedding the watermark or during the extraction stage at receiver. Recent approaches have also attempted to incorporate AI methods in the pre-processing stage [8].

With such diverse approaches and their unparalleled capabilities, the hiding of data in the digital image will be far more superior in terms of imperceptibility and robustness as compared to the existing ones [9].

*Corresponding Author: R.S Kavitha, drkavithakavana@gmail.com

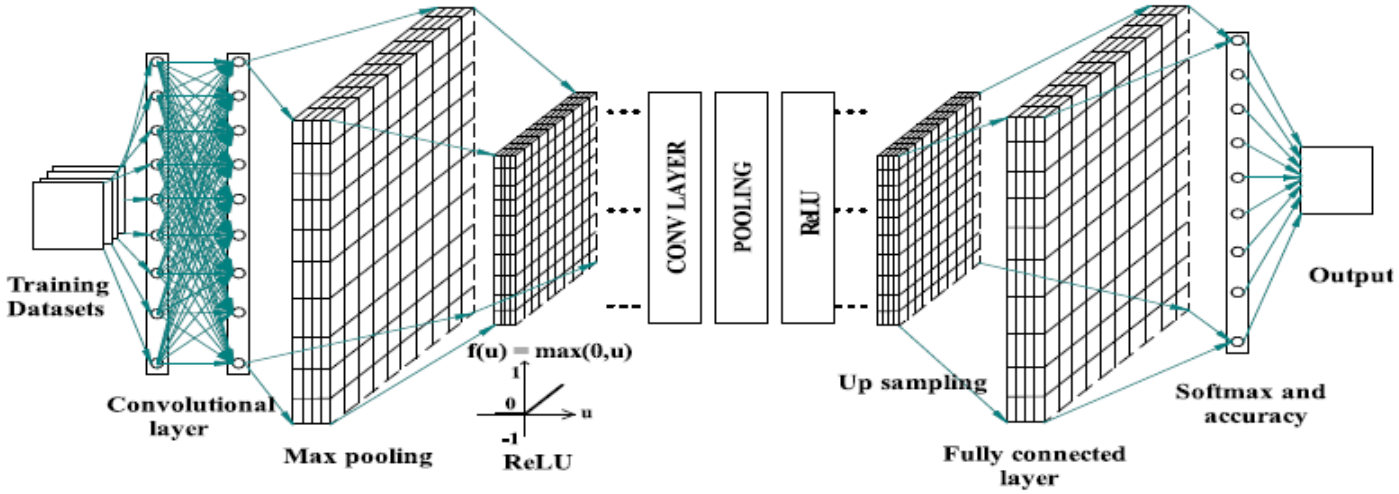

Figure 1: A typical digital watermarking process with Deep learning and its associated architectures

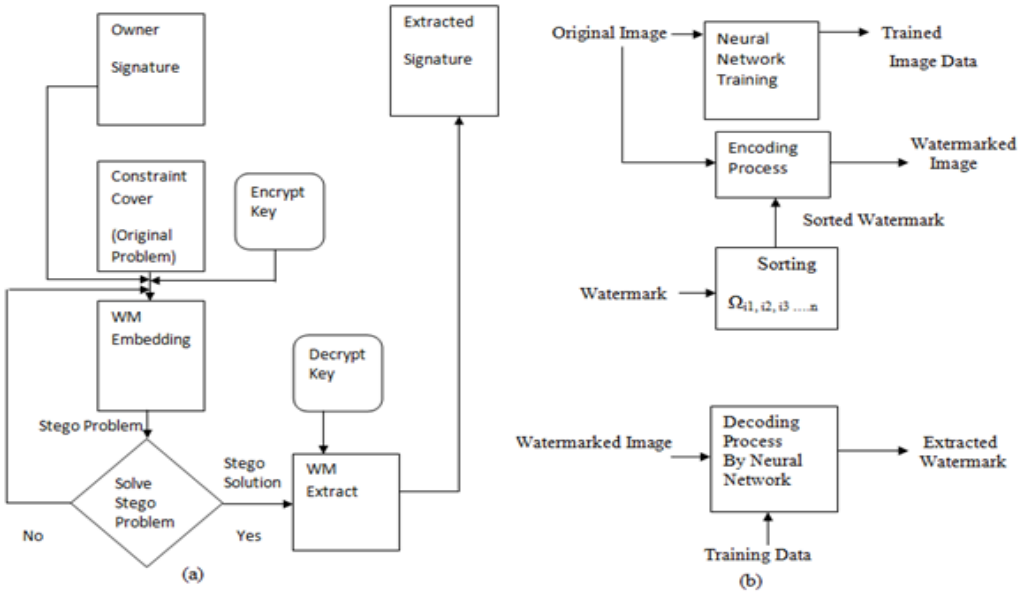

Figure 2: Experimental setup block diagram for digital watermarking process

A typical digital watermarking mechanism with embedding and extracting stages is depicted in Figure 1. It enables owners of the digital documents to embedded their copyright information for information security.

Digital watermarking can be done on text, image, audio, video and graphics in spatial or frequency domain. The watermark can be of noise type (pseudo noise, Gaussian random and chaotic sequences) or image type (binary image, stamp, logo and label) [10]. Based on the deployment conditions various watermarking techniques can be used. For public use, visible watermarks are preferred while for private applications and to arrest unauthorized copying invisible watermarking can be used [11]. Fragile watermarks are used in tamper-proof applications whereas robust watermarking is used in applications where the watermark should remain intact even after modification or tampered with [12]. According to the detection stage, visual watermarking is more robust which needs the original media and the embedded watermark for detection while blind watermarking does not require any of these. This is the most demanding type of watermarking as the watermarking is generated and embedded at the transmitter, while detection and extraction will happen at receiver as illustrated in Figure 2. Watermarking is also done even in prepossessing stage and the approach presented here does not impact the efficiency of the network in which a watermark is inserted as the embedded watermark while it is training the host network [13, 14].

The robustness of hard and soft decision detectors can be measured using Receiver Operating Characteristic graphs while Bit Error Rate is used for the detector response with bit sequence.

2. Literature Review

Many standard quantitative measures and metrics have been proposed to evaluate digital watermarking while comparing with their counterparts. Here we report all the standard methods found in the literature as illustrated in Table 1 and those used in this work to measure imperceptibility and robustness (along with capacity and computational cost) [34]. We use the methods for performance evaluation by ensuring

Table 1: Summary of literature review on Algorithm Transforms and Classifications

Reference		Survey/Tutorial	Parameter(s)
Frequency Domain + Back Propagation NN			
[15]		Discrete Wavelet Transform	Robustness
[16]		Multiwavelet Transform	Imperceptibility
[17]		Discrete Wavelet Transform	Robustness
[18]		Fourier Transform	Fidelity
[19]		Discrete wavelet Transform	Imperceptibility
[20]		Discrete wavelet Transform	Imperceptibility
Frequency Domain + Radial Basis NN			
[21]		Discrete Cosine Transform	Robustness
[22]		Discrete wavelet Transform	Imperceptible
[23]		Discrete wavelet Transform	Invisible and Robust
[24]		Discrete wavelet Transform	Robustness
Frequency Domain + Hopfield NN			
[25]			Capacity
[26]			Imperceptibility
[27]			Image Quality
[28]		Discrete Cosine Transform	Invisible and Robust
Frequency Domain + Full Counter Propagation NN			
[29]			Robustness, Imperceptibility
[30]		Discrete Cosine Transform	Robustness
[31]		Discrete Cosine Transform	Complexity, Capacity, PSNR
[32]		Discrete Cosine Transform	Imperceptibility, and robustness
Frequency Domain + Synergetic NN			
[33]		Discrete Wavelet Transform	Robustness and Imperceptibility

i) model and sources of distortion remain uniform
ii) All test images are 8-bit grey-scale images and are defined in same color space.

Quality assessment can also be done by comparing the original watermark and extracted watermark. This alternate metric is called a Normalized Correlation which exploits the correlation between the original watermark and the extracted one. The value lies between [0 1], any value nearer to 1 assures better quality. Another way of defining the similarity between the original watermark and the extracted one is accuracy ratio. It is the ratio of correct bits to the total bits. The architecture of CNN is different, unlike neural network where all layers are fully connected, here the layers are recognized in 3D: height, width, and depth. Further neurons in one layer are connected to only a small region of the next layer. Finally, the output is a single vector of probability scores, organized along the depth dimension [35]. The CNN consists of series of convolutional, pooling/sub-sampling layers followed by a fully connected layer. To implement the act of recognition in machines we need to show an algorithm of millions of images before it makes a pattern by generalizing the input and start making predictions for images it has never seen before [36]. The aim is to evolve a more robust and imperceptible watermarking scheme that can cater to the needs of content protection [37].

3. Algorithm Design

Watermarking can be achieved in any of the following two methods: either by changing the pixel values (least significant) of the image or by changing the coefficient values [38]. The quality of watermark depends on the method used. The first method where bits (representing the pixel values) are manipulated refers to a spatial domain which is very simple but not robust and can be easily perceived. In simple terms, spatial domain techniques refer to replacing pixels of the original image by watermark image [39]. In a given image first, the target pixels are identified and are replaced by pixels of watermark image. The spatial domain techniques are simple, fast and with less computational complexity [40]. They are immune to cropping and noising but are sensitive to signal processing attacks. In pursuit of enhancing robustness, if more pixels are manipulated we may end up with visible watermarks. These algorithms should carefully achieve a trade-off between robustness and imperceptibility [41]. In this section the experimental setup of watermarking a digital image is described with Algorithm 1 and Algorithm 2. At the various stages of digital watermarking from encoding of original image to decoding process and finally up to extracting the watermark and obtaining the high-resolution output decoded image. The aim is to evolve a more robust and imperceptible watermarking scheme that can cater to the needs of content protection and piracy prevention [42]. All the transform (and few hybrid approaches with NN) methods are good for watermarking but lack learning and adaptability [43]. We propose a digital watermarking method using deep learning methods which exploit the expressiveness of deep NN to securely embed invisible, imperceptible, attack-resilient binary signatures into the cover images. Coming to the

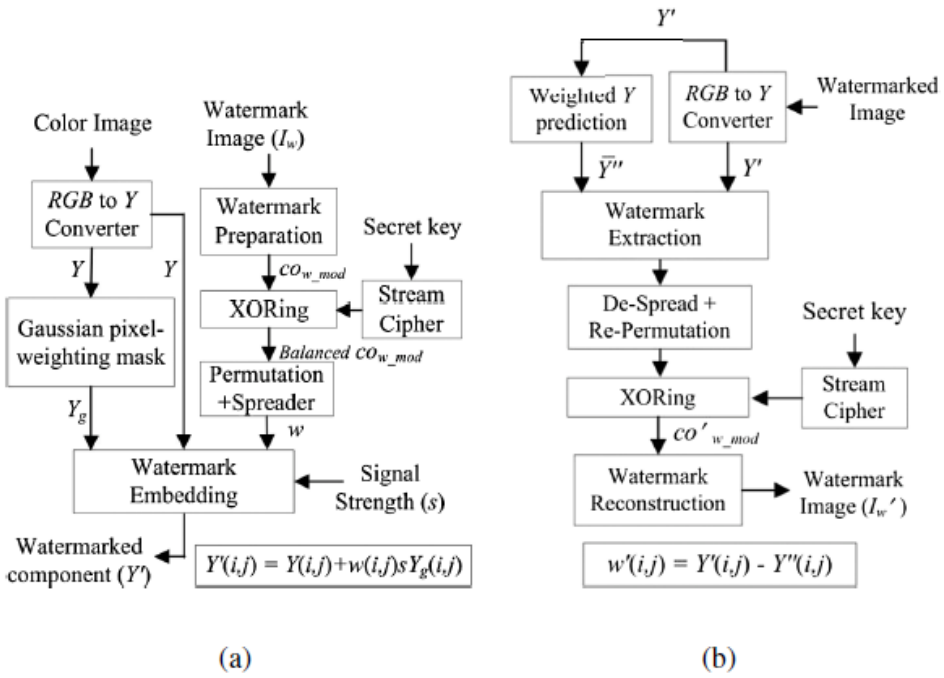

Figure 3: Block diagram representation of a typical digital watermarking process (a)Watermark Embedding and (b)Watermark Extraction.

decoder, we adopt adversarial model techniques to cause disorders to decode the desired signature [44]. We perform extended gradient descent under the Expectation over Transformation framework. In training the decoder network an Expectation-Maximization (EM) framework is employed to learn feature transformations that are more resilient to the attacks [45]. Experimental results indicate that our model achieves robustness across different transformations (all transformations, including scaling, rotation, adding noise, blurring, random cropping, and more) [46]. The aim is to evolve a more robust and imperceptible watermarking scheme that can cater to the needs of content protection and piracy prevention [47]. All the transform (and few hybrid approaches with NN) methods are good for watermarking but lack learning and adaptability [48]. We propose a digital watermarking method using deep learning methods which exploit the expressiveness of deep NN to securely embed an invisible, imperceptible, attack resilient binary signature into the cover images [49]. Coming to the decoder, we adopt adversarial model techniques to cause disorders to decode the desired signature.

Algorithm 1: Watermarking using Deep NN(Part-I)

Result: Encoding
Initialization;
Input_IMG: Image for Watermarking
Compute α transparency;
Construct an overlay;
Add Watermark to the overlay
while *setup* **do**
  Start encoding model;
  Image Encoding Process Starts;
  return encoded images;
  if *Given the model and targets* **then**
    compute the cross entropy loss;
  Else
    Given number of Iterations;
    Encode the set of images with specified binary targets;
    Image Encoding Process Ends;
  End Encoding Model
End

We perform extended gradient descent under the Expectation over Transformation framework. In training the decoder network an Expectation-Maximization (EM) framework is employed to learn feature transformations that are more resilient to the attacks. To implement the act of recognition in machines we need to show an algorithm of millions of images before it makes a pattern by generalizing the input and start making predictions for images it has never seen before [50]. The architecture of CNN is different, unlike NN where all layers are fully connected, here the layers are recognized in 3D: height, width, and depth. Further neurons in one layer are connected to only a small region of the next layer. Finally, the output is a single vector of probability scores, organized along the depth dimension. The CNN consists of series of convolutional, pooling/sub-sampling layers followed by a fully connected layer. The Figure 3 elucidates the block diagram representation of a typical digital watermarking process with Figure 3(a) as Watermark embedding process and Figure 3(b) watermark extraction phase. In this the input of the deep learning algorithm is the colour image and watermark to embed inside the colour image to watermark the deep Neural Network (DNN). The Algorithm 1 and Algorithm 2 are formulated based on the Figure 3(a) and 3(b).

Algorithm 2: Watermarking using Deep NN(Part-II)

Result: Decoding
Initialization;
While *setup* **do**
  Start the Decoding model;
  if *decoding network* **then**
    Initialize Decoding;

Extract Watermark;
Obtain High Resolution
Decoded Image;
Else
End of Decoded Network;
Return predictions;
Return decoding model;
Image Decoding Process Ends;
End Decoding Model
End

The Algorithm 1 illustrates the encoding process of digital watermarking using deep neural network and the Algorithm 2 presents the decoding process of digital watermarking using deep neural network.

4. Performance Evaluation

Fair performance evaluation of any system is fundamental for its acceptance and accreditation. Many standard quantitative measures and metrics have been proposed to evaluate digital watermarking while comparing with their counterparts. Here we report all the standard methods found in the literature and those used in this work to measure imperceptibility and robustness (along with capacity and computational cost). We use the methods for performance evaluation by ensuring i) model and sources of distortion remain uniform ii) all test images are 8-bit gray-scale images and are defined in same color space. For an image size of M x N pixels, with a pixel value of O for original image (without watermark) and W for watermarked image, the performance metrics can be calculated as below:

MSRE:

$$MSRE(O,W) = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{J=0}^{N-1}[\mathrm{O(i,j)} - W(i,j)]e^2$$

PSNR:

$PSNR(O,W) = 10\log 10[\{255\}\,e^2/\mathrm{MSRE\ (O,W)}$

4.1. Robustness Metrics

Robustness Metrics: Robustness of a watermark is a measure of resistance to attacks. The detectors dictate the evaluation method to measure robustness. The three types of detector responses are i) hard decisions (true or false for the presence and absence of watermark respectively), ii) soft decisions (correlation or similarity coefficients in terms of real numbers) iii) bit sequence (if the embedded watermark is in form of a message). The robustness of hard and soft decision detectors can be measured using Receiver Operating Characteristic (ROC) graphs while Bit Error Rate (BER) is used for the detector response with bit sequence.

ROC:

True Positive Fraction (TPF): $\frac{Number\ of\ True\ Positive\ Results}{True\ Positive+False\ Negative\ Results}$

False Positive Fraction (FPF): $\frac{Number\ of\ False\ Positive\ Results}{Fasle\ \ Positive+True\ Negative\ Results}$

Quality assessment can also be done by comparing the original watermark and extracted watermark. This alternate metric is called a Normalized Correlation which exploits the correlation between the original watermark and the extracted one. The value lies between [0 1], any value nearer to 1 assures better quality. Another way of defining the similarity between the original watermark and the extracted one is accuracy ratio. It is the ratio of correct bits to the total bits. When the attack is not going to affect the commercial value then it is better to consider only the watermark-to-noise ratio. This ratio signifies the power of watermark signal against the noise introduced by such attacks. For a watermark of size m x n pixels, the performance metrics can be calculated as below:

$$NC(OW,EW) = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{J=0}^{n-1}[\delta[\mathrm{OW(i,j)} - EW(i,j)]$$

where,

δ (X,Y) = 1 if X=Y and 0 otherwise;

5. Results Obtained

In this section we discuss the watermarking in the presence of various attacks at different noise levels. We present the results in terms of robustness of the watermark (BER and NC). The CNN is trained using standard descent back propagation algorithm. The performance consistency of the proposed method is verified by considering 2 different cover images: Lena and Camera man as presented in Figure 4 shows the watermarking process with different transforms (scaling, rotation, adding noise, blurring, random cropping, and more)and also confirms that that the proposed method is applicable to any cover image and with any watermark. BER is a measure of noise injected when the

signal is received after transmission channel. The BER shows the signal loss and fading in a wireless channel. The BER for various noise levels is shown in Figure 5(a). Normalized (cross) correlation is a template-matching method in digital watermarking. The template will be an image that shows a critical feature; by repeatedly computing a statistic between the watermarked image and corresponding pixels of a subset of an original image presents the noise correlation for various noise levels of 2,5,10 and 15. The important parameter in watermarking is the loss of original information and the accuracy with which the watermark is hidden in the cover image. There is a fine balance between the robustness and imperceptibility. The trade-off is to achieve high robustness without showing any trace of watermark. The accuracy of our model is gradually increasing as the epochs increases, on the contrary loss is gradually decreasing. The models training and testing results are shown in Figure 6 with the over fit, under fit and good fit are shown in Figures 6(a), 6(b) and 6(c) respectively. Our model Adam performs well and is consistent as compared to other models as shown in Figure 7. The Figure 8 shows the noise injected/present and the model performance. In the Figure 8(a) noise in hidden layer is shown while Figure 8(b) depicts the noise in input layer.

Figure 4: Typical digital watermarking process for Lena and Cameraman Images (a)original image (b)watermarked image (c)initial decoded image with watermark (d) extracted watermark (e)high resolution output image

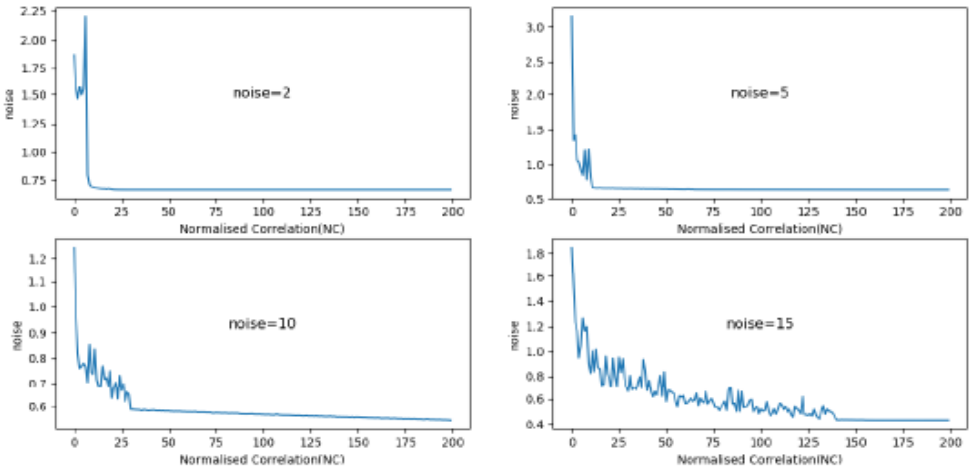

Figure 5: Verification of Robustness of the digital watermark against various type of transformations, shows the BER of watermark for various noise levels 2, 5, 10 and 15

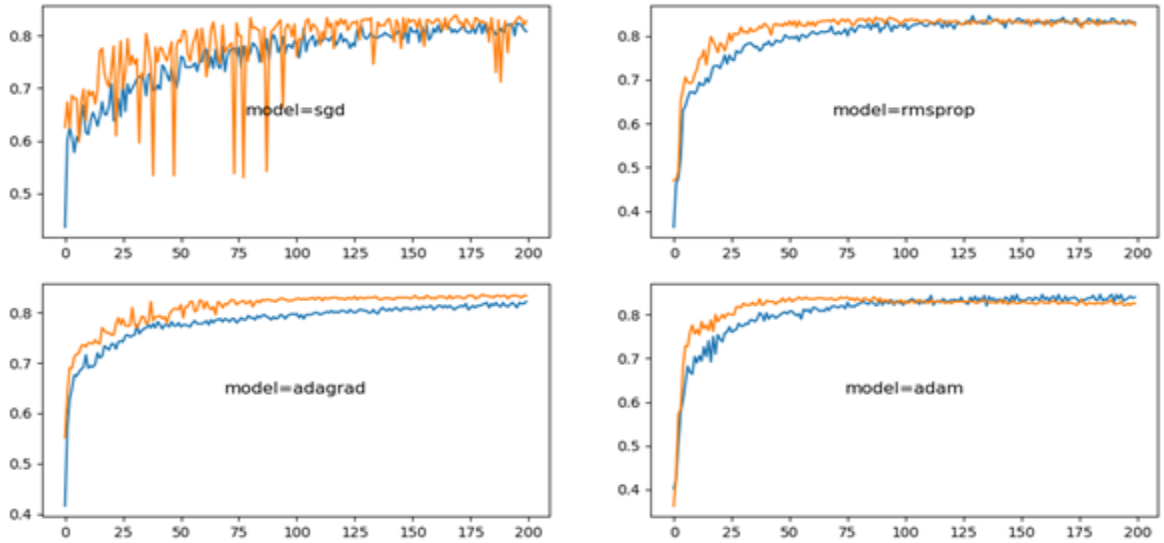

Figure 6: Validation of Neural Network Model

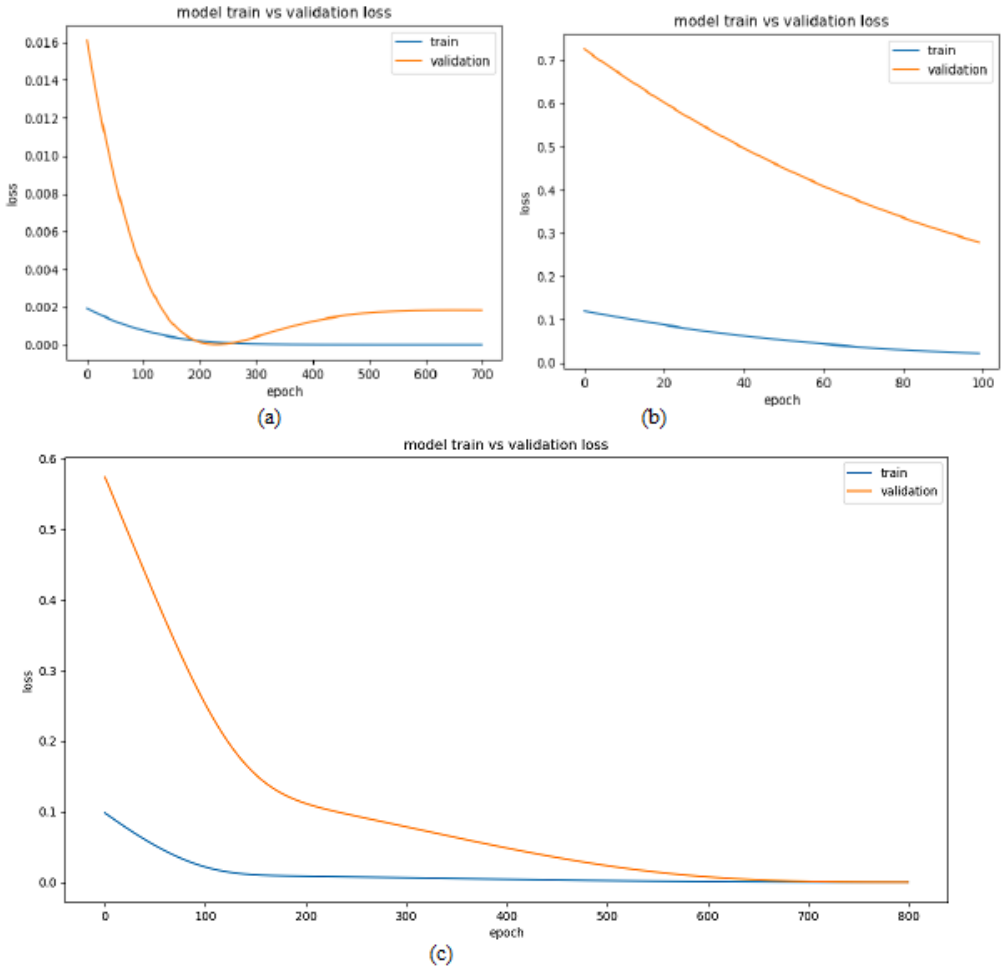

Figure 7: Fitting the model for validation (a)over fit (b) under fit and (c) good fit.

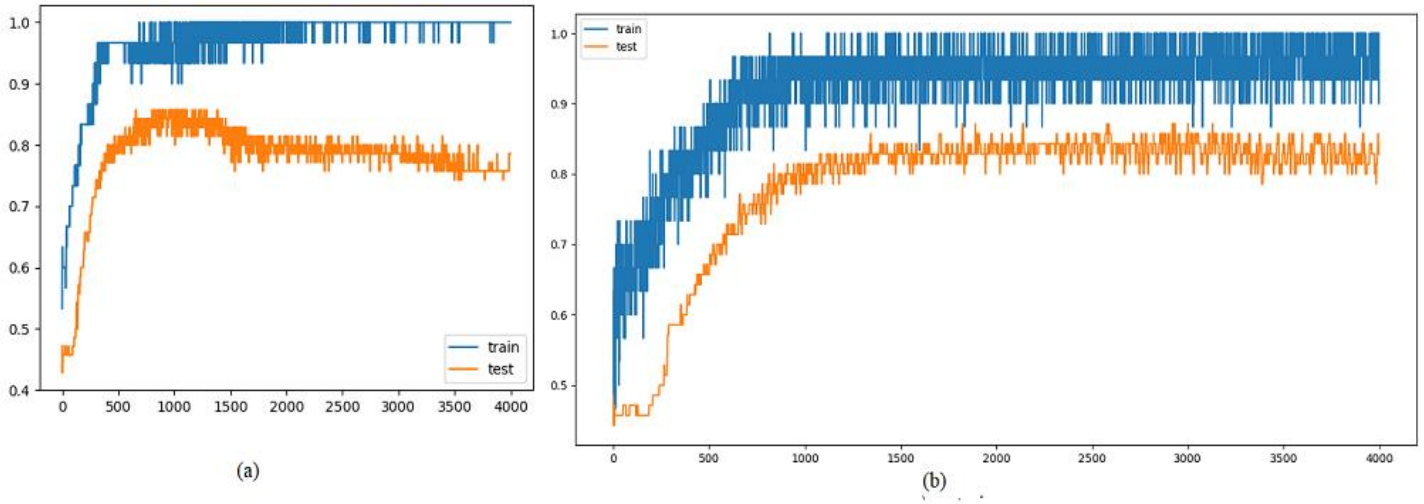

Figure 8: Injected/present noises in(a)hidden layers and (b)input layer of the proposed convolutional neural network.

Table 2: Comparison of Results

S.No	Noise/Attack	Parameter	[51]	[52]	[53]	[54]	[55]	[56]	[57]	[58]	Our Work
1	No Noise	PSNR(db)	58.91	48.29	48.47	51.45	34.33	56.47	35.6	47	**62.3**
		NC	1	1	1	1	1	1	0.99	0.98	**1.00**
2	With Noise	PSNR(db)	55.10	43.04	32.74	31.66	22.43	40.18	29.1	41.72	**58.78**
		NC	1	0.91	0.81	0.92	0.91	0.93	0.95	0.91	**1.00**

The graph shows that training and test results are in good accordance and validate the model used for training and optimization in digital watermarking. The proposed model is suitable for video too as the training is done off-line hence can be used in real-time applications. Hence the use of deep neural networks will enable us to realize complex features like learning weight sharing and update mechanism, noise-resilience and immunity towards attacks, and scaling. The proposed method has low loss and the accuracy goes on increasing as the number of epochs increases. The accuracy is 85% for 15 epochs and will slightly increase for more epochs. The level of high accuracy shows that the original image and watermarked image are indistinguishable.

This high performance of the model can be owed to the learning feature embedded in the watermarking. A digital watermarking task comprises embedding a signal into an image in accordance with robustness and quality constraints, it can be said that it is in essence a multi-objective optimization problem. The faster convergence of the algorithm (more accuracy with less epochs) can be achieved by introducing reinforcement learning or transfer learning method which has got huge attention in recent times. The current digital watermarking can also be validated by applying it to protect the copyrights of trained neural networks where ownership protection and piracy prevention is of utmost priority. The traditional approaches in digital watermarking are not fit for the digital data that can be stored efficiently and with very high quality and manipulated easily using computers [59, 60]. The aim is to evolve a secure digital communication that remarkably pushes forward the limits of legacy digital watermarking schemes across all dimensions of performance metrics. As this research space is ever increasing and innovations have spurred at all levels of communication, considerable progress is required in understanding the deep learning approaches for digital watermarking. The convergence of technological, economic and environmental forces is driving the digital watermarking and deep learning simultaneously, then each drives the other forward. Be it the deep neural networks driving digital watermarking or vice-versa, the continued expansion of each is good for the other. The complete suitability of digital watermarking for securing deep neural networks dataset is yet to be conducted. The trained models can be viewed as intellectual property, and it is a worthy challenge to provide copyright protection for trained models. We emphasis on how the copyrights of trained models can be protected computationally and propose for neural networks a digital watermarking technology. We propose a conceptual framework for integrating a watermark into models of deep neural networks to safeguard copyrights and identify violation of trained models of intellectual property. The Table 2 illustrates the comparison of obtained results with the previous works and it is noteworthy that the proposed work has shown an improvement of 5.75% in PSNR without noise and 6.68% in PSNR with noise = 5.

6. Conclusions

In this paper, we proposed a learning framework for robust digital image watermarking technique based on deep neural network. As observed, previous efforts in this space focused on optimization of embedding parameters with use of evolutionary computing. Demonstration of the watermarking under various noise and attacks is performed. The detailed experiments were carried out and we analyzed the performance of designed system. We have shown that our model could embed a watermark without impairing a deep neural network's efficiency. In future the research would continue in the direction towards digital watermarking based on intelligence.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] R.S. Kavitha, U. Eranna, M.N. Giriprasad, “DCT-DWT Based Digital Watermarking and Extraction using Neural Networks,” in 2020 International Conference on Artificial Intelligence and Signal Processing, AISP 2020, 2020, doi:10.1109/AISP48273.2020.9073104.

[2] N. Memon, P.W. Wong, “A buyer-seller watermarking protocol,” IEEE Transactions on Image Proc., **10**(4), 643-649, 2001, doi:10.1109/83.913598.

[3] I.A.T. Hashem, I. Yaqoob, N.B. Anuar, S. Mokhtar, A. Gani, S. U Khan, "The rise of “big data” on cloud computing: Review open research issues." Information systems, **47**, 98-115, 2015, doi:10.1016/j.is.2014.07.006.

[4] N.F. Johnson, Z. Duric, S. Jajodia, N. Memon, “Information Hiding: Steganography and Watermarking—Attacks and Countermeasures,” Journal of Electronic Imaging, 2001, doi:10.1117/1.1388610.

[5] J.C. Ingemar, M.L. Miller, A.B. Jeffrey, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, 2008, doi:10.1016/B978-0-12-372585-1.X5001-3.

[6] Y.S. Singh, B.P. Devi, K.M. Singh, “Image comp using Multilayer Feed Forward Artificial Neural Network with Conjugate Gradient,” in Proceedings of the 2012 World Congress on Information and CommunicationTechn,976-980,2012, doi:10.1109/WICT.2012.6409216.

[7] A.Z. Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J. Ho, N.R.A. Mee, C.F. Osborne, “Electronic Water Mark,” Digital Image Computing, Technology and Applications (DICTA’93), 1993.

[8] S. Wu, S. Zhong, Y. Liu, “Deep residual learning for image steganalysis,” Multimedia Tools Apps, **77**(9), 10437-10453, 2017, doi:10.1007/s11042-017-4440-4.

[9] S.J. Lee, S.H. Jung, “A survey of watermarking techniques applied to multimedia,” in IEEE International Symposium on Industrial Electronics,1,272-277, 2001, doi:10.1109/isie.2001.931796.

[10] R. Warkar, P. More, D. Waghole, “Digital audio watermarking and image watermarking for information security,” in 2015 International Conference on Pervasive Computing: Advance Comm. Tech. and Application for Society, ICPC2015, doi:10.1109/PERVASIVE.2015.7086980.

[11] A.K. Singh, B. Kumar, M. Dave, A. Mohan, “Robust and Imperceptible Spread-Spectrum Watermarking for Telemedicine Applications,” Proceedings of the National Academy of Sciences India Section A - Physical Sciences, **85**(2),295-301, 2015, doi:10.1007/s40010-014-0197-6.

[12] M. Barni, F. Bartolini, V. Cappellini, A. Piva, “A DCT-domain system for robust image watermarking,” Signal Processing, 1998, doi:10.1016/S0165-1684(98)00015-2.

[13] T. Ashkan et al.,"A modified dual watermarking scheme for digital images with tamper localization/detection and recovery capabilities." 2012 9th International ISC Conference on Information Security and Cryptology. IEEE, 2012.

[14] P.K. Dhar, J.M. Kim, “Digital watermarking scheme based on fast Fourier transformation for audio copyright protection,” International Journal of Security and Its Applications, **5**(2),33-48, 2011. doi: 10.1016/j.future.2018.07.029.

[15] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Transactions on Image Processing, 1997, doi:10.1109/83.650120.

[16] D. Kundur, D. Hatzinakos, “Digital watermarking for telltale tamper proofing and authentication,” Proceedings of the IEEE, 1999, doi:10.1109/5.771070.

[17] A. Tiwari, M. Sharma, R.K. Tamrakar, “Watermarking based image authentication and tamper detection algorithm using vector quantization approach,” AEU - International Journal of Electronics and Communications, **78(5)** ,114-123, 2017, doi: 10.1016/j.aeue.2017.05.027.

[18] Z. Ma, M. Jiang, H. Gao, Z. Wang, “Block chain for digital rights management,” Future Generation Computer Systems, **89**(7), 746-764, 2018, doi: 10.1016/j.future.2018.07.029.

[19] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, A. Akutsu, "The Block Chain-Based Digital Content Distribution System," in Proceedings - 2015 IEEE 5th International Conference on Big Data and Cloud Computing, B D Cloud 2015, 2015, doi:10.1109/BDCloud.2015.60.

[20] Stefik, Mark J., et al. "System for controlling the distribution and use of rendered digital works through watermaking." U.S. Patent No. 6,233,684. 15 May 2001.

[21] T. Jitha Raj, E.T. Sivadasan, "A survey paper on various reversible data hiding techniques in encrypted images," in Souvenir of the 2015 IEEE International Advance Computing Conference, IACC 2015, 2015, doi:10.1109/IADCC.2015.7154881.

[22] A.A. Philip, P.R. Geetharanjin, "Fingerprint Encryption and Dual Watermarking to Verify the Security Issues in Teleradiology," in Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018, 2018, doi:10.1109/CESYS.2018.8724112.

[23] I.J. Cox, M.L. Miller, "The first 50 years of electronic watermarking," EURASIP Journal on Applied Signal Processing, **2**(2)**,** 820-936, 2002, doi:10.1155/s1110865702000525.

[24] J. Bajpai, A. Kaur, "A literature survey - Various audio watermarking techniques and their challenges," in Proceedings of the 2016 6th International Conference - Cloud System and Big Data Engineering, Confluence 2016, 2016, doi:10.1109/CONFLUENCE.2016.7508162.

[25] C. Kumar, A.K. Singh, P. Kumar, "A recent survey on image watermarking techniques and its application in e-governance," Multimedia Tools and Applications, **77(3)**, 3597-3622, 2018, doi:10.1007/s11042-017-5222-8.

[26] M.H. Alkawaz, G. Sulong, T. Saba, A.S. Almazyad, A. Rehman, "Concise analysis of current text automation and watermarking approaches," Security and Communication Networks, **9**(18), 6365-6378, 2016, doi:10.1002/sec.1738.

[27] A. Świerkosz, "Digital watermarking in telemedicine an example from ECG - Review of challenges, methods and applications," Advances in Intelligent Systems and Computing, 248-255, 2017, doi:10.1007/978-3-319-47154-929.

[28] S. Mirghasemi, P. Andreae, M. Zhang, "Domain-independent severely noisy image segmentation via adaptive wavelet shrinkage using particle swarm optimization and fuzzy C-means," Expert Systems with Applications, **133**(4), 126-150, 2019, doi: 10.1016/j.eswa.2019.04.050.

[29] Q.D. La, M. V. Ngo, T.Q. Dinh, T.Q.S. Quek, H. Shin, "Enabling intelligence in fog computing to achieve energy and latency reduction," Digital Communications Networks, 2019, doi: 10.1016/j.dcan.2018.10.008.

[30] H. Kandi, D. Mishra, S.R.K.S. Gorthi, "Exploring the learning capabilities of convolutional neural networks for robust image watermarking," Computers Security ,**65**(3), 247-268, 2017, doi: 10.1016/j.cose.2016.11.016.

[31] M.S. Hsieh, D.C. Tseng, Y.H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," IEEE Transactions on Industrial Electronics, **48**(5) ,875-882, 2001, doi:10.1109/41.954550.

[32] N.M. Makbol, B.E. Khoo, "Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition," AEU - International Journal of Electronics and Communications,**67(2)**,102-112, 2013, doi: 10.1016/j.aeue.2012.06.008.

[33] H.T. Hu, L.Y. Hsu, J. Garcia-Alfaro, "Exploring DWT-SVD-DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression," Computers and Electrical Engineering, **41**(8), 52-63, 2015, doi: 10.1016/j.compeleceng.2014.08.001.

[34] T.T. Takore, P.R. Kumar, G.L. Devi, "A modified blind image watermarking scheme based on DWT, DCT and SVD domain using GA to optimize robustness," in International Conference on Electrical, Electronics, and Optimization Techniques, 2016, doi:10.1109/ICEEOT.2016.7755190.

[35] A.K. Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images," Multimedia Tools and Applications, **76(6)**,8881-8900, 2017, doi:10.1007/s11042-016-3514-z.

[36] B.J. Saha, Arun, K.K. Kabi, C. Pradhan, "Non-blind watermarking technique using enhanced one-time pad in DWT domain," in 5th International Conference on Computing Communication and Networking Technologies, ICCCNT 2014, 2014, doi:10.1109/ICCCNT.2014.6963061.

[37] N.M. Kumar, T. Manikandan, V. Sapthagirivasan, "Non-blind image watermarking based on similarity in contourlet domain," in International Conference on Recent Trends in Information Technology, ICRTIT 2011, 2011, doi:10.1109/ICRTIT.2011.5972280.

[38] G.H. Yann LeCun, Yoshua Bengio, "Deep learning,", Nature, **521**(7553)**,** 436–444, 2015.

[39] R. Namba, J. Sakuma, "Robust watermarking of neural network with exponential weighting," in Asia CCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, 2019, doi:10.1145/3321705.3329808.

[40] E. Le Merrer, P. Pérez, G. Trédan, "Adversarial frontier stitching for remote neural network watermarking," Neural Computing and Applications, **32**(13), 9233-9244, 2020, doi:10.1007/s00521-019-04434-z.

[41] B. Prashanth, "Design and Implementation of Radar Cross-Section Models on a Virtex-6 FPGA," Journal of Engineering (United Kingdom), 2014, doi:10.1155/2014/489765.

[42] L. Pang, S. Zhu, C.W. Ngo, "Deep Multimodal Learning for Affective Analysis and Retrieval," IEEE Transactions on Multimedia, **17**(11), 2008-2020, 2015, doi:10.1109/TMM.2015.2482228.

[43] B. Prashanth, P.A. Kumar, G. Sreenivasulu, " Design and Implementation of floating point ALU on a FPGA processor," in 2012 International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012, 2012, doi:10.1109/ICCEET.2012.6203790.

[44] B. Vijay Krishna, B. Venkata Prashanth, P. Sujatha, "Design and implementation of DPFC for multi-bus power system," International Journal of Engineering and Technology (UAE), **7**(2), 2018, doi:10.14419/ijet.v7i2.8.10318.

[45] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, A. Rabinovich, "Going deeper with convolutions," in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2015, doi:10.1109/CVPR.2015.7298594.

[46] S.R. Qasim, H. Mahmood, F. Shafait, " Rethinking table recognition using graph neural networks," in Proceedings of the International Conference on Document Analysis and Recognition, ICDAR, 2019, doi:10.1109/ICDAR.2019.00031.

[47] J. Li, P. He, J. Zhu, M.R. Lyu, "Software defect prediction via convolutional neural network," in Proceedings-IEEE International Conference on Software Quality, Reliability and Security, 2017, doi:10.1109/QRS.2017.42.

[48] Y. Uchida, Y. Nagai, S. Sakazawa, S. Satoh, "Embedding watermarks into deep neural networks," in ICMR 2017 - Proceedings of the 2017 ACM International Conference on Multimedia Retrieval, 2017, doi:10.1145/3078971.3078974.

[49] A. Van Den Oord, S. Dieleman, B. Schrauwen, "Deep content-based music recommendation," in Advances in Neural Information Processing Systems, **26(1)**, 2643-2651, 2013, doi:10.1145/2500098.2500109.

[50] A. Karatzoglou, B. Hidasi, "Deep learning for recommender systems," in RecSys 2017 - Proceedings of the 11th ACM Conference on Recommender Systems, 2017, doi:10.1145/3109859.3109933.

[51] A. Karpathy, L. Fei-Fei, "Deep Visual-Semantic Alignments for Generating Image Descriptions," IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017, doi:10.1109/TPAMI.2016.2598339.

[52] H.O. Song, Y. Xiang, S. Jegelka, S. Savarese, "Deep Metric Learning via Lifted Structured Feature Embedding," in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2016, doi:10.1109/CVPR.2016.434.

[53] B. Kim, H. Kim, K. Kim, S. Kim, J. Kim, "Learning not to learn: Training deep neural networks with biased data," in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2019, doi:10.1109/CVPR.2019.00922.

[54] L. Shao, D. Wu, X. Li, "Learning deep and wide: A spectral method for learning deep networks," IEEE Transactions on Neural Networks and Learning , **25**(12), 2303-2308, 2014, doi:10.1109/TNNLS.2014.2308519.

[55] A.B. Duque, L.L.J. Santos, D. Macêdo, C. Zanchettin, "Squeezed Very Deep Convolutional Neural Networks for Text Classification," in Lecture Notes in Computer Science, 2019, doi:10.1007/978-3-030-30487-4_16.

[56] K. He, X. Zhang, S. Ren, J. Sun, "Deep residual learning for image recognition," in Proceedings of the IEEE Computer Society Conference on Computer Vision Pattern Recognition, 2016, doi:10.1109/CVPR.2016.90.

[57] K. Zhang, W. Zuo, Y. Chen, D. Meng, L. Zhang, "Beyond a Gaussian denoiser: Residual learning of deep CNN for image denoising," IEEE Transactions on Image Processing, **26**(7), 3142-3155, 2017, doi:10.1109/TIP.2017.2662206.

[58] B.D. Rouhani, H. Chen, F. Koushanfar, "Deep Signs: An End-to-End Watermarking Framework for Ownership Protection of Deep Neural Networks," in International Conference on Architectural Support for Programming Languages and Operating Systems - ASPLOS, 2019, doi:10.1145/3297858.3304051.

[59] A.I. Orhean, F. Pop, I. Raicu, "New scheduling approach using reinforcement learning for heterogeneous distributed systems," Journal of Parallel and Distributed Computing, **117**(1)**,** 292-302, 2018, doi:10.1016/j.jpdc.2017.05.001.

[60] Q. Guo, X. Wang, Y. Wu, Z. Yu, D. Liang, X. Hu, P. Luo, "Online knowledge distillation via collaborative learning," in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2020, doi:10.1109/CVPR42600.2020.01103.