electronics

MDPI

Article

CWAN: Covert Watermarking Attack Network

Chunpeng Wang, Yushuo Liu, Zhiqiu Xia *, Qi Li, Jian Li, Xiaoyu Wang and Bin Ma *

School of Computer Science and Technology (School of Cyber Security), Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China
* Correspondence: mpeng1122@qlu.edu.cn (Z.X.); mab@qlu.edu.cn (B.M.)

Abstract: Digital watermarking technology is widely used in today's copyright protection, data monitoring, and data tracking. Digital watermarking attack techniques are designed to corrupt the watermark information contained in the watermarked image (WMI) so that the watermark information cannot be extracted effectively or correctly. While traditional digital watermarking attack technology is more mature, it is capable of attacking the watermark information embedded in the WMI. However, it is also more damaging to its own visual quality, which is detrimental to the protection of the original carrier and defeats the purpose of the covert attack on WMI. To advance watermarking attack technology, we propose a new covert watermarking attack network (CWAN) based on a convolutional neural network (CNN) for removing low-frequency watermark information from WMI and minimizing the damage caused by WMI through the use of deep learning. We import the preprocessed WMI into the CWAN, obtain the residual feature images (RFI), and subtract the RFI from the WMI to attack image watermarks. At this point, the WMI's watermark information is effectively removed, allowing for an attack on the watermark information while retaining the highest degree of image detail and other features. The experimental results indicate that the attack method is capable of effectively removing the watermark information while retaining the original image's texture and details and that its ability to attack the watermark information is superior to that of most traditional watermarking attack methods. Compared with the neural network watermarking attack methods, it has better performance, and the attack performance metrics are improved by tens to hundreds of percent in varying degrees, indicating that it is a new covert watermarking attack method.

Keywords: digital watermarking; convolutional neural network; watermarking attack; deep learning; covert attack

Citation: Wang, C.; Liu, Y.; Xia, Z.; Li, Q.; Li, J.; Wang, X.; Ma, B. CWAN: Covert Watermarking Attack Network. *Electronics* **2023**, *12*, 303. https://doi.org/10.3390/electronics12020303

Academic Editor: Janos Botzheim

Received: 4 November 2022
Revised: 21 December 2022
Accepted: 24 December 2022
Published: 6 January 2023

1. Introduction

Due to the popularity of modern Internet technology, people's access to information is becoming increasingly convenient. However, as a result of the random proliferation and transmission of massive amounts of information, the copyright of related data cannot be authenticated. The protection of digital image copyright is an urgent issue that requires resolution, as it is one of the most important topics in scientific research [1]. Robust watermarking technology is an efficient key technology for data copyright authentication, confirmation, and tracking. By embedding identifying information (namely digital watermarking) into the protected information, it can realize the authentication and tracking of the carrier copyright. During the propagation of watermarked images (WMI), they may be subjected to various attacks that corrupt the watermark information embedded in the image, making it impossible to extract the watermark information correctly or completely [2], referred to as watermarking attack techniques [3]. On the other hand, the introduction of watermarking attack technology can be used to verify, test, and optimize the robust watermarking algorithm by adding attacks. As can be seen, watermarking attack techniques are an effective method of promoting continuous optimization of digital watermarking technology and enhancing its resistance to attacks.

While digital watermarking algorithms have advanced rapidly, research has made little progress into new watermarking attack techniques. Because most watermarking algorithms are already highly resistant to the traditional watermarking attack methods mentioned above, the existing evaluation system is unable to fully and effectively evaluate the performance of watermarking algorithms. Additionally, the existing available watermarking attack methods interfere with the accurate watermark information extraction. The degree of damage to the embedded watermarked image is greater, resulting in a significant loss of image quality, detrimental to the original carrier's protection, and defeats the purpose of conducting a covert attack on images with watermarks. The watermarking algorithms and watermarking attack methods have been out of balance in terms of development and are unable to establish a virtuous cycle. As a result, it is critical to conduct research into new highly covert watermarking attack methods.

The specific contributions of this paper are as follows:

(1) Applying deep learning techniques to the field of digital watermarking attacks, combining digital watermarking attack techniques with convolutional neural network denoising methods, extracting the features of low-frequency watermark information in WMI using deep CNN, attacking watermark information while removing noise from noise-containing WMI using CNN, and achieving the purpose of removing noise and watermark information at the same time.
(2) The method proposed in this paper is a novel and effective method for digital watermarking attacks due to neural networks' powerful learning and reconstruction capabilities. Attacks on watermarked information are significantly more effective than traditional image processing and geometric attacks.
(3) Improving the shortcomings of the traditional digital watermarking attack methods, namely, that the traditional attack causes varying degrees of distortion and damage to the image while removing the watermark information. The proposed attack method produces a highly imperceptible attack on the image and maximizes the preservation of image details, textures, etc.
(4) Compared with the traditional watermarking attack method and neural network watermarking attack method DnCNN and FCNNDA, we not only improve the attack performance metrics but also significantly improve the remaining performance evaluation metrics.

2. Related Works

Watermarking attack techniques have improved along with the advancement of digital watermarking attack technology. The purpose of traditional image processing is to obstruct the correct extraction of the watermark by altering the energy of the embedded watermark information [4]. This includes noise attacks, filtering attacks, sharpening processes, compression attacks, brightness and contrast changes, and blurring processes, among others. To counteract these traditional attack methods, researchers have proposed a variety of watermarking algorithms, most notably those based on the image spatial-domain [5,6] and transform-domain [7,8] and watermarking strategies such as geometric invariants [9], simultaneous correction, and local feature regions [10]. Watermarking attacks and digital watermarking algorithms operate similarly to a game, where they promote and complement one another.

Today, deep learning's rapid advancement has resulted in novel solutions and significant success in fields such as speech recognition, image recognition, and natural language processing. Due to its powerful learning capabilities, researchers are increasingly focusing on its application to digital watermarking and attack techniques. Haribabu et al. [11] proposed a self-coding neural network-based digital image watermarking technique in 2015, which uses a convolutional neural network (CNN) in the field of watermarking for the first time. In 2018, Zhu et al. [12] proposed an end-to-end trainable Hidden architecture for steganography and watermarking algorithms. This architecture utilizes neural networks to encode useful information to generate invisible perturbations that complete the

embedding of watermarking information. Ahmadi et al. [13] proposed a deep end-to-end diffusion watermarking framework (ReDMark) in 2018, which is more advantageous in terms of steganography and robustness and can learn new watermarking algorithms in an arbitrary transformation space with adaptivity and flexibility. Lee et al. [14] proposed a neural network-based image blind watermarking algorithm in 2020, claiming that it can embed watermarks without the use of feature layers or components. In 2020, Geng et al. [15] proposed a watermark removal attack utilizing convolutional neural networks (DnCNN). This removal attack not only removes the watermark effectively but also recovers the original image (OI) with minimal image degradation. In 2021, Hatoum et al. [16] proposed a denoising attack based on full convolutional neural networks (FCNNDA) that preserves image quality while impairing the robustness of all evaluated watermarking schemes. As a result, it is certainly a novel and practical idea to apply convolutional neural networks to the field of watermarking attacks by leveraging their inherent learning and reconstruction capabilities.

3. Attacked Robust Watermark Algorithm

The robust image watermarking technique [17] embeds watermark information into the image content to protect an image. It is critical to ensure that the visual quality of the original image is not significantly degraded during the copyright protection process but also that most of the embedded watermark information can be extracted after being subjected to external interference or signal attacks. Robustness is the most important evaluation criterion for robust watermarking algorithms [18], as it indicates the algorithm's ability to resist various attacks.

To design a watermarking attack method with a strong attack capability and ensure that the designed watermarking attack method remains effective when attacking multiple watermarks embedding schemes, a robust watermark embedding scheme [19] should be chosen to maximize the watermarking attack algorithm's universality. Therefore, this paper chooses a robust watermarking algorithm based on polar harmonic Fourier moments (PHFMs) as the watermark embedding algorithm to attack. PHFMs are a kind of image continuous orthogonal moments, with highly concentrated image features [20]. Due to the high stability and geometric invariance of PHFMs, the watermarking algorithm based on them has good robustness against traditional image processing attacks as well as geometric attacks. The performance is significantly superior to that of robust watermarking algorithms [21].

PHFMs are geometrically invariant image features with polar coordinate images $f(r,\theta)$ of order $n(n \geq 0)$ with repetition $m(|m| \geq 0)$ defined as follows [22]:

$$\phi_{nm} = \frac{2}{\pi}\int_0^{2\pi}\int_0^1 f(r,\theta)\overline{H_{nm}(r,\theta)}rdrd\theta \tag{1}$$

where $\overline{[\cdot]}$ denotes the conjugate of the complex numbers, and the basis function $H_{nm}(r,\theta)$ consists of the radial basis function $T_n(r)$ and the angular Fourier factor $\exp(jm\theta)$:

$$H_{nm}(r,\theta) = T_n(r)\exp(jm\theta) \tag{2}$$

where the radial basis function $T_n(r)$ is:

$$T_n(r) = \begin{cases} 1/\sqrt{2} & \text{while } n \text{ is } 0 \\ \sin(n+1)\pi r^2 & \text{while } n \text{ is odd} \\ \cos n\pi r^2 & \text{while } n \text{ is even} \end{cases} \tag{3}$$

$T_n(r)$ is orthogonal in the interval $0 \leq r \leq 1$:

$$\int_0^1 T_n(r)T_{n'}(r)rdr = \frac{1}{4}\delta_{nn'}(1) \tag{4}$$

By the nature of the angular Fourier factor and the above equation, the basis function $H_{nm}(r,\theta)$ is orthogonal in the unit circle:

$$\int_0^{2\pi}\int_0^1 H_{nm}(r,\theta)\overline{H_{kl}(r,\theta)}rdrd\theta = \frac{\pi}{2}\delta_{nk}\delta_{ml} \tag{5}$$

where $0 \le r \le 1$, $0 \le \theta \le 2\,\pi$, δ is the normalization factor.

According to the theory of orthogonal complete function families, the original image function $f(r,\theta)$ can be approximately reconstructed using a finite number of PHFMs. If the PHFMs with the highest order $n_{\max}$ and the maximum repetition $m_{\max}$ are known, the original image is approximately reconstructed as the following equation:

$$f(r,\theta) \approx \sum_{n=0}^{n_{\max}}\sum_{m=-m_{\max}}^{m_{\max}} \phi_{nm}H_{nm}(r,\theta) \tag{6}$$

4. Proposed Watermarking Attack Method

4.1. Details of CWAN

Traditional watermarking attack methods primarily disrupt the watermark's correct extraction by altering the energy of the embedded watermark information or by interfering with the synchronization between the WMI and the watermark information. When attacking WMI, this approach can severely degrade image quality. To remove the watermark information from the WMI while maintaining the image's quality, a covert attack on the WMI is performed. We propose a covert watermarking attack method based on a CNN that takes advantage of deep learning's powerful learning capability.

In the preprocessing stage, we add random Gaussian noise to the WMI I to obtain an image containing both noise and watermark information, I_w, as the input of the convolutional neural network. Then, the noise-containing watermarked image, I_w, is fed into this watermarking attack network. The deeper the neural network layers, the richer the image features it learns. After experiments, we finally set the number of neural network layers to 18. Each layer uses 64 convolution kernels of size 3×3 for the convolution operation, ensuring that the image size at the input and output of each neural network layer remains the same size. At the same time, the step size of the complementary zero filling is set to 1, and Leaky-ReLU is used as the activation function.

The final RFI I_r of the same size as the noise-containing watermarked image I_w is obtained at the output of the CNN. The noise-containing watermarked image I_w is then subtracted the RFI I_r to obtain the noise and AWMI I_o after the attack. At this point, a complete digital watermarking attack process is completed. Finally, the WMI I is compared with the de-noised and de-watermarked residual image I_o. The PSNR and SSIM values are used to judge the effect of image reconstruction after an attack [23], while the BER value is used to judge the effect of watermark information removal. The attacking network removes noise from the image while corrupting the watermark data throughout this process.

In the network structure of the watermark attack module, there are eighteen attack module blocks. Each block consists of a convolutional layer, an activation layer, and a residual structure, and the residual structure contains two convolutional layers and a ReLU activation function. The watermark information exists in the low-frequency region of the image, and the introduction of the residual module can better enable the network to learn the low-frequency information of the image, thus improving the network's ability to attack the watermark information. The details are shown in Figures 1 and 2.

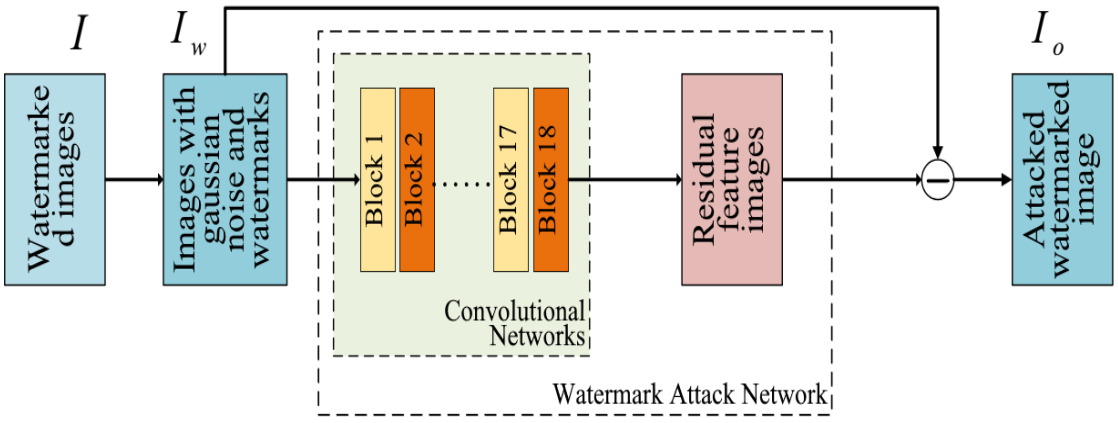


Figure 1. The flow chart of watermark attack algorithm.

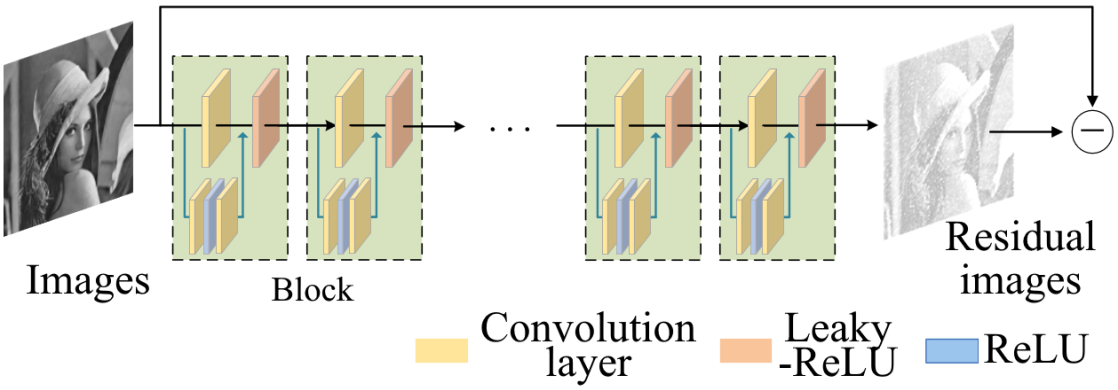


Figure 2. The details of the watermark attack network.

4.2. Loss Function and Performance Evaluation Indicators

We use the mean square error (MSE) as the loss function in the model training stage [24]. The MSE loss function is primarily used to forecast the mean value of the sum of squares of AWMI and WMI's corresponding point errors. The following is the calculation formula:

$$MSE = \sum_{i=1}^{n} (y_i - y_i^p)^2 \tag{7}$$

where y_i is the true value of the training data, y_i^p represents the predicted output of the neural network, and i represents the dimensionality of the data.

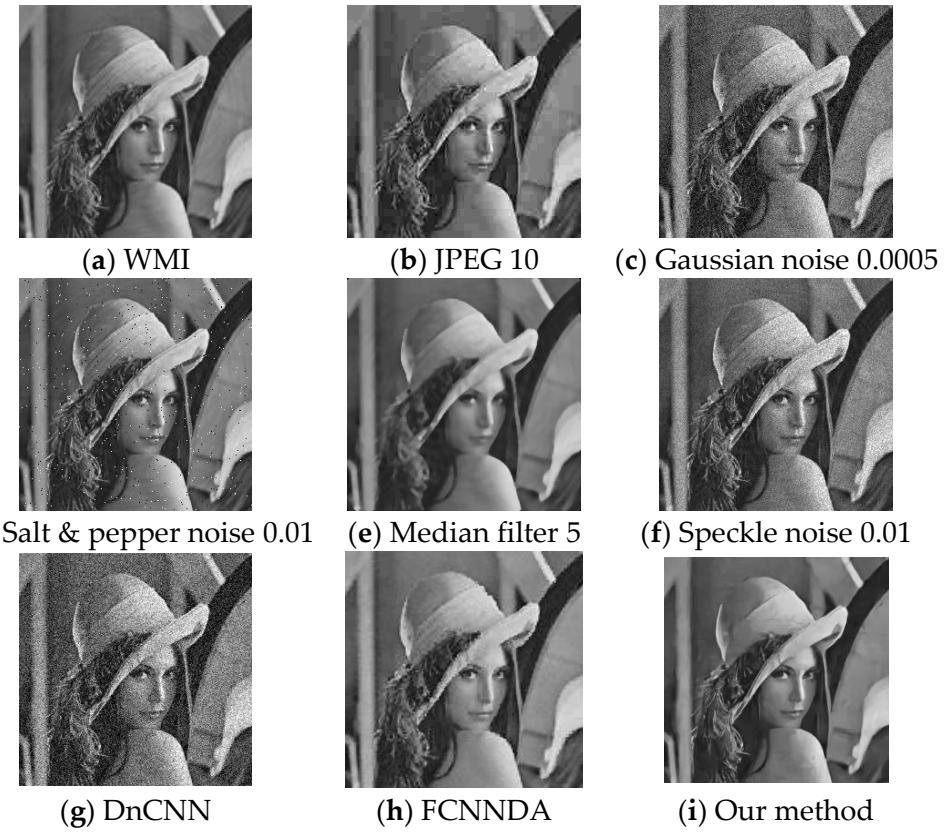
5. Experiment

In this chapter, experiments will be conducted to verify the effectiveness of this method. The experiments are as follows. To measure the attack effectiveness of the proposed attack method, we conducted experiments on the original images embedded with three different sizes of image watermarks, 8×8, 16×16, and 32×32. Then, we compared the proposed method with five kinds of common attack methods [4], i.e., JPEG compression, Gaussian noise, Salt & pepper noise, Median filter, Speckle noise, and two CNN-based watermarking attack methods, i.e., DncNN [15] and FCNNDA [16].

5.1. Comparison with Other Methods

In this subsection, we use the Lena image embedded with a 16×16 size image watermark for the experiments and then apply different attack methods to measure the effectiveness of the attacks on the attack network.

The obtained AWMIs are shown in Figure 3. At this point, the image watermark is extracted from the AWMI; the resulting image watermarks are depicted in Figure 4. The specific results are as follows:

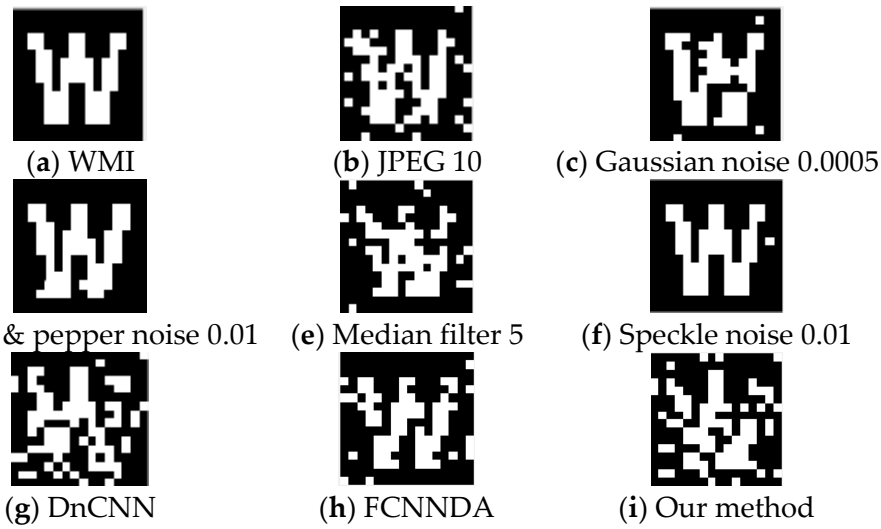


(**a**) WMI (**b**) JPEG 10 (**c**) Gaussian noise 0.0005

(**d**) Salt & pepper noise 0.01 (**e**) Median filter 5 (**f**) Speckle noise 0.01

(**g**) DnCNN (**h**) FCNNDA (**i**) Our method

Figure 3. Comparison of AWMIs after applying different attacks to WMIs; the watermark size is 16×16.



(**a**) WMI (**b**) JPEG 10 (**c**) Gaussian noise 0.0005

(**d**) Salt & pepper noise 0.01 (**e**) Median filter 5 (**f**) Speckle noise 0.01

(**g**) DnCNN (**h**) FCNNDA (**i**) Our method

Figure 4. The image watermark extracted from the AWMI; the watermark size is 16×16.

Compared to the images following the previous attacks, the distortion degree caused by the rotation attack is the greatest. However, the effect on the image watermark is minimal. This is due to the PHFMs' rotational invariance.

According to the extracted image watermarks from AWMI and the calculated BER values, both JPEG compression with a quality factor of 10 and the median filter with a window size of 5 × 5 cause effective WMI degradation. However, their AWMIs exhibit excessive noise and visual blurring, which fall short of meeting effective protection requirements.

Our method can improve the attack capability by up to 450.76% compared with the traditional watermarking attack method, and the highest improvement in PSNR and SSIM indexes is 170.47% and 290.11%. Compared with the traditional watermarking attack method, it can improve the attack capability by 232.77% on average, and the PSNR and SSIM are improved by 27.25% and 33.79% on average.

Compared with the DnCNN and FCNNDA, with a small lead in attack effect, both PSNR and SSIM achieved a significant improvement, 49.71% and 71.21%, respectively. Our method achieves the best results by balancing the degree of AWMI detail preservation and the degree of WMI damage. It demonstrates that our method is capable of generating effective attacks against image watermark and that the attack performance is superior to that of the majority of traditional attack methods. Table 1 summarizes the various evaluation indicators.

Table 1. Comparison of evaluation indicators; watermark size of 16 × 16.

Attack	PSNR (dB)	SSIM	BER
WMI	-	-	-
JPEG 10 [4]	28.2991	0.7908	0.1094
Gaussian noise 0.0005 [4]	23.0334	0.4733	0.0508
Salt & pepper noise 0.01 [4]	25.1640	0.7988	0.0234
Median filter 5 [4]	28.6722	0.8415	0.1211
Speckle noise 0.01 [4]	26.9181	0.6833	0.0039
DnCNN [15]	20.3051	0.4956	0.1736
FCNNDA [16]	29.0245	0.7637	0.1609
Our method	30.3979	0.8485	0.1797

5.2. Attack Effect on Image Watermarks of Different Sizes

The previous section's experimental results demonstrate that the attack network can continue to generate effective attacks on WMI of any size with little loss of image detail such as texture. This section continues to verify the effectiveness of this network for attacking larger size (32 × 32), and smaller (8 × 8) size image watermarks, again comparing the traditional attack methods.

5.2.1. Effectiveness of Attack Network on Image Watermark of Size 32 × 32

This subsection will continue to explore the effect of this attack model on watermarked images containing large size (32 × 32) watermarks, and the specific experimental results are shown below:

The larger the image watermark, the more watermark information the CWAN can learn during the training stage, and the more effective the attack on the image watermark will be. Similarly, the larger the ratio of the image watermark size to the image size, the more details are lost in the CWAN-recovered image, and the PSNR and SSIM values of AWMI will decrease. Nevertheless, most of the details and textures in the AWMIs following the CWAN attack have been preserved. The experimental results are shown in Figures 5 and 6.

The values of the indicators of the median filter attack in Table 2 are consistent with our method. Although its attack on the watermark is equally effective, it is still obvious that it causes a blurring effect on the WMI image.

Meanwhile, the speckle noise attack alters the image's visual quality less significantly, but its effect occurs because the attack method does not effectively damage the watermark information.

Compared with other methods, our method can improve the attack capability by 117.78% and 17.26% on average and improve the PSNR and SSIM metrics by about 20% to

60% on average. For FCNNDA, another neural network attack method, the attack effect increased by 39.1332%, and the other two indicators also improved to varying degrees. On balance, our attack method still outperforms the competition.

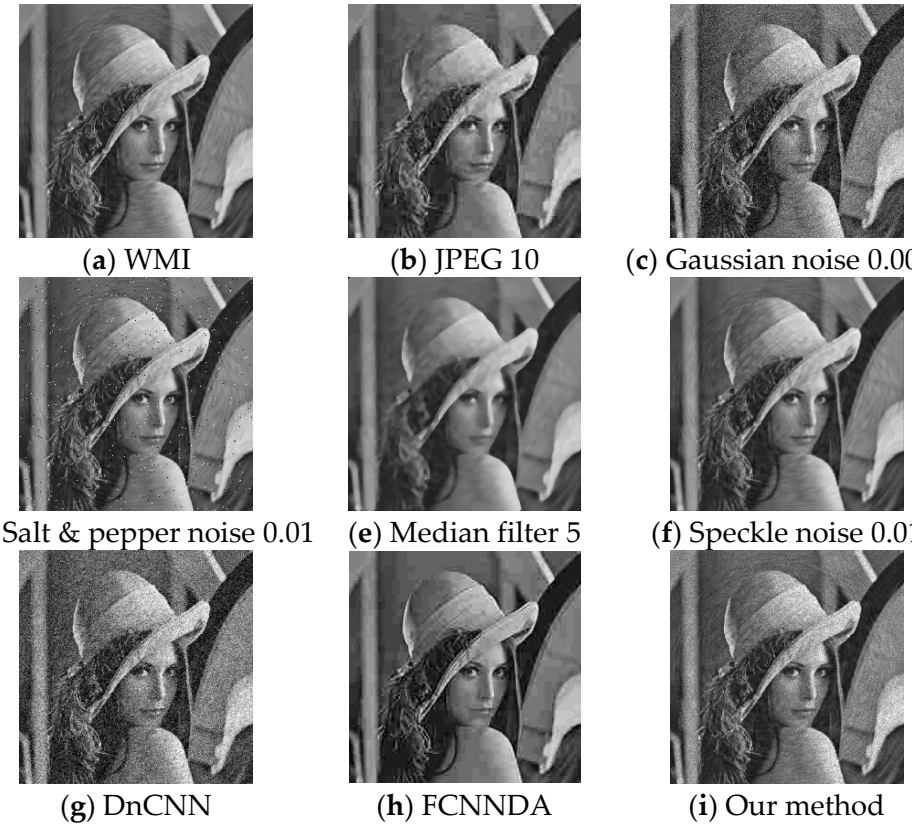


Figure 5. Comparison of AWMIs after applying different attacks to WMIs; the watermark size is 32×32.

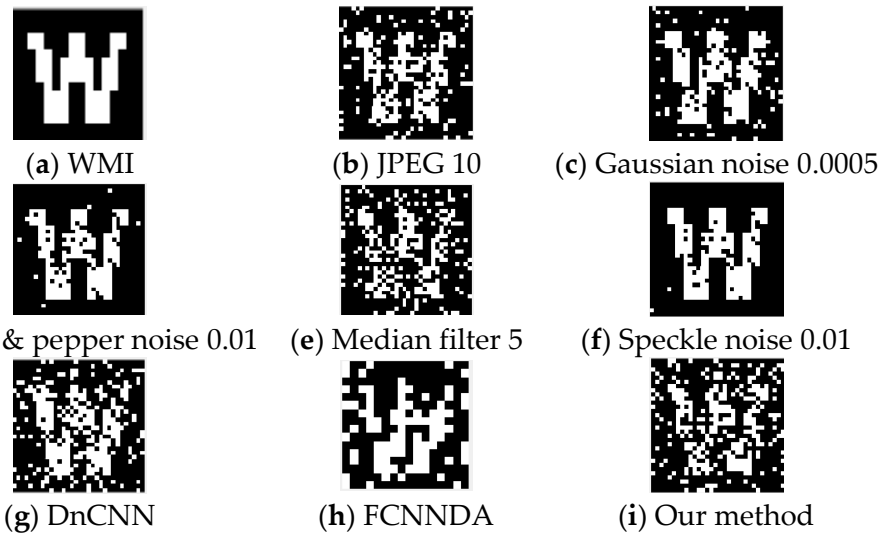


Figure 6. The image watermark extracted from the AWMI; the watermark size is 32×32.

Table 2. Comparison of evaluation indicators; watermark size of 32 × 32.

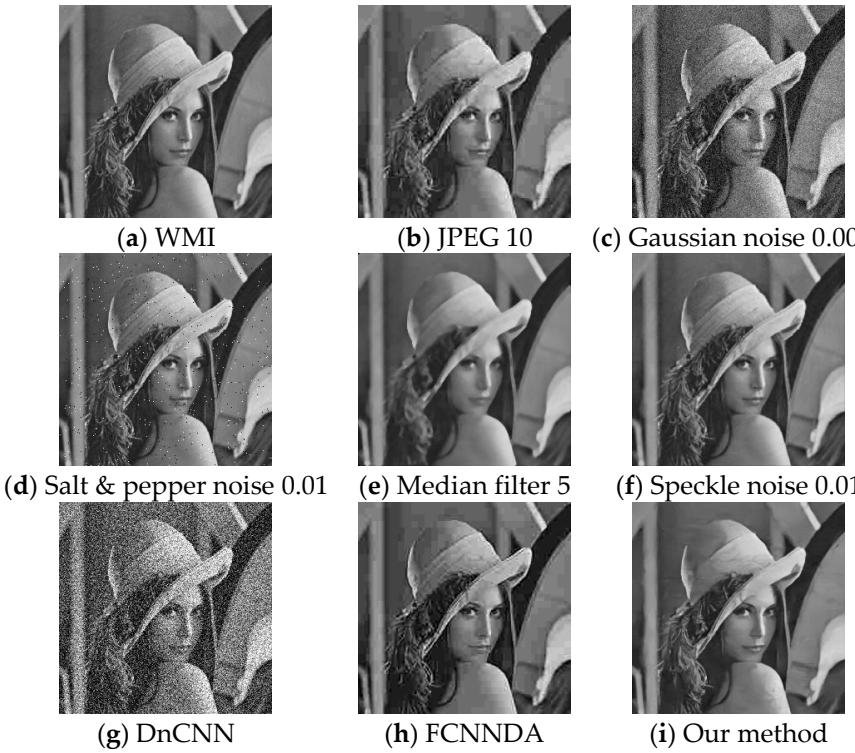
Attack	PSNR (dB)	SSIM	BER
WMI	-	-	-
JPEG 10 [4]	28.0461	0.7696	0.1504
Gaussian noise 0.0005 [4]	23.0342	0.4957	0.0889
Salt & pepper noise 0.01 [4]	25.3781	0.8128	0.0508
Median filter 5 [4]	28.3594	0.8102	0.1992
Speckle noise 0.01 [4]	26.9106	0.7057	0.0342
DnCNN [15]	20.3096	0.5076	0.1807
FCNNDA [16]	27.2243	0.7453	0.1523
Our method	29.8257	0.8178	0.2119

5.2.2. Effectiveness of Attack Network on Image Watermark of Size 8 × 8

The previous experiments verified that our attack method can effectively attack images containing watermarks of 16 × 16 and 32 × 32 sizes, and in this section, we will continue to verify the effectiveness of the attack method for small size (8 × 8) watermarks.

When the original image is embedded with a small-size image watermark, the neural network is able to better learn the image's features during the convolution process and recover the image with more details. As a result, the image's SSIM value increases to varying degrees.

At the same time, due to the small size of the image watermark, the attack effect of this attack network is weakened compared to when attacking a large image watermark, but it still has a significant effect. According to Figures 7 and 8, while the Gaussian noise 0.0005 attack method is the most effective in the traditional attack, the image distortion is too high, and the PSNR and BER values are too far apart compared to our method.

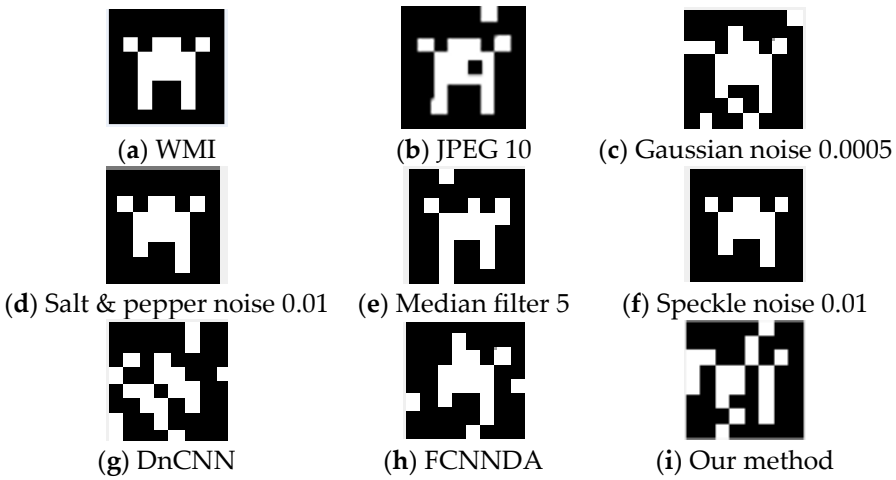


(**a**) WMI (**b**) JPEG 10 (**c**) Gaussian noise 0.0005

(**d**) Salt & pepper noise 0.01 (**e**) Median filter 5 (**f**) Speckle noise 0.01

(**g**) DnCNN (**h**) FCNNDA (**i**) Our method

Figure 7. Comparison of AWMIs after applying different attacks to WMIs; the watermark size is 8 × 8.



(**a**) WMI (**b**) JPEG 10 (**c**) Gaussian noise 0.0005
(**d**) Salt & pepper noise 0.01 (**e**) Median filter 5 (**f**) Speckle noise 0.01
(**g**) DnCNN (**h**) FCNNDA (**i**) Our method

Figure 8. The image watermark extracted from the AWMI; the watermark size is 8 × 8.

Additionally, when used in conjunction with the comprehensive comparison in Table 3. Although our method is slightly inferior in attack effect compared to DnCNN, its improved attack effect makes the image distortion severe, which is evident from the remaining two metrics, which defeats the original purpose of steganography and is not conducive to image protection. In summary, our method can still have a significant attack effect on small-size image watermarks.

Table 3. Comparison of evaluation indicators; watermark size of 8 × 8.

Attack	PSNR (dB)	SSIM	BER
WMI	-	-	-
JPEG 10 [4]	28.3582	0.7934	0.0938
Gaussian noise 0.0005 [4]	23.0057	0.4677	0.1094
Salt & pepper noise 0.01 [4]	25.2494	0.7930	0.0156
Median filter 5 [4]	28.7087	0.8420	0.0625
Speckle noise 0.01 [4]	26.9325	0.6780	0.0156
DnCNN [15]	15.1509	0.2740	0.1956
FCNNDA [16]	28.4396	0.7989	0.1126
Our method	29.5310	0.8297	0.1719

6. Conclusions and Future Work

This paper proposes a novel covert digital watermarking attack method based on deep learning that removes watermark information by extracting low-frequency RFI from WMI. Experiments demonstrate that the network can produce an effective attack effect on the robust watermark embedding algorithm based on the PHFMs, which can attack different sizes of image watermarks while retaining most of the image texture details and achieving a high degree of covert attack, while the attack effect on the watermark is superior to that of traditional watermarking attack methods and DnCNN and FCNNDA, and the attack effect has been significantly improved by tens to hundreds of percent. While the PHFMs-based watermarking algorithm is resistant to various attacks, our proposed method can still achieve the desired attack expectation on its embedded image watermark. In the next step, we will continue to improve this attack method's attack capability and image reconstruction capability to achieve a combined attack effect while maintaining a high level of image covertness.

Author Contributions: Conceptualization, C.W. and Y.L.; methodology, Z.X.; software, Q.L.; validation, J.L. and X.W.; formal analysis, B.M.; investigation, Z.X.; resources, C.W.; data curation, Y.L.; writing—original draft preparation, C.W.; writing—review and editing, B.M.; visualization, Z.X.;

supervision, X.W.; project administration, Q.L.; funding acquisition, J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data are not publicly available due to privacy.

Acknowledgments: This work was funded by the National Natural Science Foundation of China (61802212 and 61872203), the National Key Research and Development Program of China (2021YFC3340600), the Shandong Provincial Natural Science Foundation (ZR2020MF054), Jinan City "20 universities" Funding Projects (2020GXRC056 and 2019GXRC031), Jinan City-School Integration Development Strategy Project (JNSX2021030), Key Research and Development Program of Shandong Academy of Science. ChinaMFS 2022.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kadian, P.; Arora, S.; Arora, N. Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey. *Wirel. Pers. Commun.* **2021**, *118*, 3225–3249. [CrossRef]
2. Vassaux, B.; Nguyen, P.; Baudry, S.; Bas, P.; Chassery, J.-M. Survey on attacks in image and video watermarking. In *International Society for Optics and Photonics*; SPIE: Philadelphia, PA, USA, 2002; pp. 169–179.
3. Licks, V.; Jordan, R. Geometric attacks on image watermarking systems. *IEEE Multimed.* **2005**, *12*, 68–78. [CrossRef]
4. Song, C.; Sudirman, S.; Merabti, M.; Llewellyn-Jones, D. Analysis of Digital Image Watermark Attacks. In Proceedings of the 2010 7th IEEE Con-sumer Communications and Networking Conference, Las Vegas, NV, USA, 9–12 January 2010; pp. 1–5.
5. Hua, G.; Xiang, Y.; Zhang, L. Informed histogram-based watermarking. *IEEE Signal Process. Lett.* **2020**, *27*, 236–240. [CrossRef]
6. Zong, T.; Xiang, Y.; Natgunanathan, I.; Guo, S.; Zhou, W.; Beliakov, G. Robust histogram shape-based method for image water marking. *IEEE Trans. Circuits Syst. Video Technol.* **2014**, *25*, 717–729. [CrossRef]
7. Shen, Y.; Tang, C.; Xu, M.; Chen, M.; Lei, Z. A DWT-SVD based adaptive color multi-watermarking scheme for copyright protec-tion using AMEF and PSO-GWO. *Expert Syst. Appl.* **2021**, *168*, 114414. [CrossRef]
8. Liu, X.; Han, G.; Wu, J.; Shao, Z.; Coatrieux, G.; Shu, H. Fractional Krawtchouk transform with an application to image watermarking. *IEEE Trans. Signal Process.* **2017**, *65*, 1894–1908. [CrossRef]
9. Hu, R.; Xiang, S. Cover-Lossless Robust Image Watermarking Against Geometric Deformations. *IEEE Trans. Image Process.* **2020**, *30*, 318–331. [CrossRef] [PubMed]
10. Wang, C.; Ma, B.; Xia, Z.; Li, J.; Li, Q.; Shi, Y.-Q. Stereoscopic Image Description with Trinion Fractional-Order Continuous Or-thogonal Moments. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 1998–2012. [CrossRef]
11. Haribabu, K.; Subrahmanyam, G.; Mishra, D. A robust digital image watermarking technique using auto encoder based convolutional neural networks. In Proceedings of the 2015 IEEE Workshop on Computational Intelligence: Theories, Applications and Future Di-rections (WCI), Kanpur, India, 14–17 December 2015; pp. 1–6.
12. Zhu, J.; Kaplan, R.; Johnson, J.; Fei-Fei, L. Hidden: Hiding data with deep networks. In Proceedings of the European Conference on Computer Vision (ECCV), Munich, Germany, 8–14 September 2018; pp. 657–672.
13. Ahmadi, M.; Norouzi, A.; Karimi, N.; Samavi, S.; Emami, A. ReDMark: Framework for residual diffusion watermarking based on deep networks. *Expert Syst. Appl.* **2020**, *146*, 113157. [CrossRef]
14. Lee, J.-E.; Seo, Y.-H.; Kim, D.-W. Convolutional Neural Network-Based Digital Image Watermarking Adaptive to the Resolution of Image and Watermark. *Appl. Sci.* **2020**, *10*, 6854. [CrossRef]
15. Geng, L.; Zhang, W.; Chen, H.; Fang, H.; Yu, N. Real-time attacks on robust watermarking tools in the wild by CNN. *J. Real-Time Image Process.* **2020**, *17*, 631–641. [CrossRef]
16. Hatoum, M.; Couchot, J.-F.; Couturier, R.; Darazi, R. Using Deep learning for image watermarking attack. *Signal Process. Image Commun.* **2021**, *90*, 116019. [CrossRef]
17. Chen, Y.; Bai, Y.; Zhang, W.; Mei, T. Destruction and Construction Learning for Fine-Grained Image Recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, 16–17 June 2019.
18. Wang, C.; Wang, X.; Xia, Z.; Ma, B.; Shi, Y.-Q. Image description with polar harmonic Fourier moments. *IEEE Trans. Circuits Syst. Video Technol.* **2020**, *30*, 4440–4452. [CrossRef]
19. Mun, S.-M.; Nam, S.-H.; Jang, H.; Kim, D.; Lee, H.-K. Finding robust domain from attacks: A learning framework for blind water-marking. *Neurocomputing* **2019**, *337*, 191–202. [CrossRef]
20. Wang, C.; Wang, X.; Xia, Z.; Zhang, C. Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm. *Inf. Sci.* **2019**, *470*, 109–120. [CrossRef]
21. Xia, Z.; Wang, X.; Zhou, W.; Li, R.; Wang, C.; Zhang, C. Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms. *Signal Process.* **2019**, *157*, 108–118. [CrossRef]
22. He, B.; Cui, J.; Xiao, B.; Peng, Y. Image analysis using modified exponent-Fourier moments. *EURASIP J. Image Video Process.* **2019**, *2019*, 72. [CrossRef]

23. Wang, C.; Hao, Q.; Xu, S.; Ma, B.; Xia, Z.; Li, Q.; Li, J.; Shi, Y.-Q. RD-IWAN: Residual Dense based Imperceptible Watermark Attack Network. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 7460–7472. [CrossRef]
24. Li, Q.; Wang, X.; Ma, B.; Wang, X.; Wang, C.; Gao, S.; Shi, Y.-Q. Concealed attack for robust watermarking based on generative model and perceptual loss. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 5695–5706. [CrossRef]