Enhancing Security Of Digital Communication Using Image Watermarking

Daksh Goel[1], Nancy Jaiswal[2], Shourya Sharma[3], Ananya Thakur[4], Mukesh Singh[5]
Student[1], Student[2], Student[3], Student[4], Assistant Professor[5]
Department of Computer Science[1, 2, 3, 4, 5],
Graphic Era University, Dehradun, India[1, 2, 3, 4, 5]

***Abstract* —** It is very important to ensure the security and integrity of multimedia content in the near future. This paper analyzes deep learning paradigms and provides an approach to safely and securely transfer data over the Internet. Current digital watermarking techniques often cause significant distortion in the original image, which can lead to a poor user experience and the effectiveness of watermarks in protecting against unauthorized use or alteration reduction. This will need the use of advanced deep learning techniques to accurately find the position where to embed the watermark in original image. The main objective was to design a watermark system with powerful learning depth of field will be used to add and remove watermarks from digital images with ease, all while preserving image quality.

***Keywords*—** Convolutional Neural Network (CNN) Model, Non-Subsampled Contourlet Transform (NSCT) Algorithm, Linear Feedback Shift Algorithm (LFSA), Normalized Correlation (NC), Peak Signal-to-Noise Ratio (PSNR), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT)

I. INTRODUCTION

In the age of technology and the Internet, the protection of authenticity and ownership of digital content has become a serious issue. Digital watermarking A method of encapsulating data in digital products such as images, audio files and videos to prevent illegal use of information A watermark is a purposeful addition of visible information to products is to identify ownership, control usage, and discourage copyright infringement. This paper provides insights of digital watermarking, including development stages, watermarking studies, and the overall structure of the watermarking system. The aim of the paper is to build a framework that uses watermarking based on deep learning to ensure smooth transmission of information over the Internet. Watermarking is a method of encapsulating information in digital content such as images, audio, video etc. to prevent unauthorized copying and distribution. The proposed method will incorporate a unique watermark into digital content by on a deep learning system. The system will also use encryption techniques to make content illicit. The system will be designed to handle a variety of digital content such as images, audio and video files. The watermark algorithm will be adjusted so that the embedded watermarks do not degrade the quality of the original text.

A. Problem Statement

The watermarking techniques which are currently being used cause significant distortion in original image, which can lead to less effectiveness of watermarks in protecting against unauthorized access and also cause poor user experience. Considering this problem statement we will develop an efficient and robust digital watermarking method.

B. Background Literature

Digital watermarking is important tool to maintain integrity and provide security to multimedia content. This includes photos, audio files, videos and other digital content that you provide information to protect against unauthorized use and copyright infringement. As the Internet has become an increasing medium for data transmission, the need for robust watermarking techniques that do not compromise the quality of the original content is paramount This literature review explores the development of digital watermarking , combination of deep learning methods, and robustness methods as well as the efficiency of watermark systems.[1]

Digital watermarking techniques have evolved significantly since their inception. Early methods mainly focused on spatial region methods, which involved the direct use of pixel values to encode watermarks. Because these paths were straight they were much more susceptible to attack from different angles, and the original image was often very distorted. To overcome these limitations, researchers have turned to frequency domain methods such as discrete cosine transform (DCT) and discrete wavelet transform (DWT) methods to improve the attack efficiency and reduce optical distortion but still face balancing the trade-off between stability and inconsistency.[2, 3]

The advent of deep learning has transformed digital

watermarking by providing advanced tools for modeling complex relationships in data. Convolutional neural networks (CNNs) have shown great promise in optimizing embedding and extraction processes. CNNs can recognize complex images, enabling efficient and complex watermarking.[4, 5]

To improve the results of digital watermarking, many methods have been developed by combining deep learning and traditional methods. Non-sampled contour transform (NSCT) is a machine that provides multi-resolution, versatile image parsing and is

suitable for adding watermarks. Additional encryption provides an additional layer of security; The Linear Feedback Shift Algorithm (LFSA), combined with mathematics, provides a strong encryption process to ensure the transmission of watermarked images when infected. This method avoids watermarking while preserving the integrity of the original image.[6]

Peak Signal-to-Noise Ratio (PSNR) and Normalized Correlation (NC) are the measures to evaluate the performance of watermarking algorithm. PSNR measures the quality of watermarked images. The higher the value, the better the original image is preserved. NC checks the similarity between the original watermark and the selected watermark and evaluates the accuracy and robustness of the watermark.[6, 7]

C. Objective

1) To develop an effective and robust watermarking algorithm using deep learning techniques that can embed and extract a watermark in a digital image without significantly degrading its quality.

2) The effectiveness of the developed watermarking algorithm is evaluated by examining the amount of distortion added to the original image, the resilience of the watermark to various attacks, and its ability to be reliable and remove the watermark.

3) To explore the utilize of profound learning-based watermarking in regions such as copyright security, confirmation, and alter location.

4) Overall, the main objective of this work is to design an optimal watermarking system that can provide high levels of security and robustness against attacks, while not affecting the quality of original.

II. METHODOLOGY

We used MATLAB to design and execute the entire image watermarking process. MATLAB also have extensive collection of mathematical functions and image processing libraries, both of them proved to be an important tool to implement and refine our watermarking algorithms. This type of versatile environment allowed us to easily code modules for image processing, encryption, embedding, recovery, and evaluation. We got empowered by the graphical capabilities of MATLAB and its suite of mathematical functions, providing an efficient platform for building and optimizing our watermark systems from scratch.

A. ER Diagram

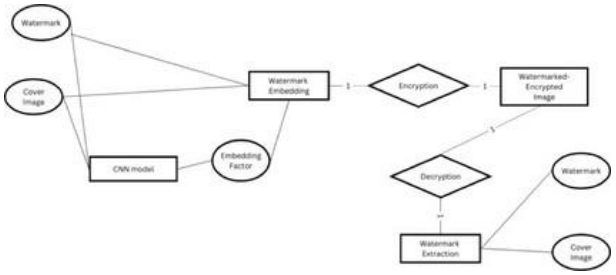

Fig. 1. ER Diagram

Fig. 1 shows the ER (Entity Relationship) model of a watermarking system that uses deep learning. The diagram shows the components and the relationships of the system. The relationships show how the components are connected with each other with arrows. The diagram shows how the system can embed and extract watermarks, encrypt and decrypt images.

B. Working of the Project

1) Watermark Embedding: Using Non-Subsampled Contourlet Transform (NSCT) algorithm to embed a watermark effectively within the digital image. This algorithm ensures a robust integration of the watermark. An embedding factor will be generated using Convolutional Neural Network (CNN) model which will enhance the robustness of the watermarking process, adapting to varying image characteristics.

2) Image Encryption: The watermarked image will be encrypted using the combination of chaotic mathematics and Linear Feedback Shift Algorithm (LFSA) and this dual-layered encryption approach will add an extra level of security, enhancing the protection of the embedded watermark. Ensure secure transmission by employing the encrypted watermarked image, mitigating the risk of unauthorized access.

3) Image Decryption: Apply the same chaotic mathematics and Linear Feedback Shift Algorithm (LFSA) for decrypting the received image. This ensures a seamless and secure decryption process. Preserve the integrity of the embedded watermark throughout the decryption process, maintaining the authenticity of the communicated content.

4) Watermark Extraction: Employ specialized techniques to extract the embedded watermark from the decrypted image. This step is crucial for verifying the authenticity and integrity of the communicated content. Implement thorough verification processes to ensure the extracted watermark aligns with the originally embedded one, validating the legitimacy of the transmitted data.

C. Performance Parameters

In our image watermarking project, we analyzed performance by using two key metrics, Normalized Correlation (NC) and Peak Signal-to-Noise Ratio.

(PSNR). These metrics are very useful in detecting and analyzing the accuracy and quality of our watermarking technique.

1) The Normalized correlation (NC): shows the relationship between the original and retrieved watermarks, and provides valuable insight into the accuracy of our watermark system. With a NC value of 0.8, we observe an exceptionally high degree of correlation, indicating the robustness of our watermark retrieval process. This high NC value suggests minimal distortion between the original and retrieved watermarks, affirming the fidelity of the embedded information.

2) Peak Signal-to-Noise Ratio (PSNR) : shows tquality of watermark retrieved, stands at an impressive 35. This value indicates an exceptionally high signal to noise ratio in the received watermark which indicates good quality. Our watermarking technique demonstrates an adeptness in preserving the original information during both the embedding and retrieval processes.

TABLE 1. TEST RESULTS

Attack	**NC**	**PSNR**
JPEG Compression	0.829	35.096
Salt and Pepper	0.754	30.852
Gaussian Noise	0.594	15.727
Histogram Equaliser	0.757	16.482

III. RESULT ANALYSIS AND DISCUSSION

The system is successfully able to embed a watermark in the cover image using deep learning used alongside the NSCT algorithm by calculating the coefficients where the watermark could be embedded and it is not visible to the naked eye. The system successfully encrypts the watermarked image using the Chaotic Maps algorithm used in hybrid with linear feedback shift register to generate the encryption key which is then used to decrypt the image. The model extracts the watermark from the cover image after the decryption and then it is compared with the original watermark to check its robustness. After performing the various attacks the NC value does not fall 0.7 which indicates our watermark will remain as intact as the original even after attacks. These test results help us conclude that the system is functioning as expected and there are no errors as of now in the deep learning model as well as in the encryption and decryption. The system is able to perform well.

ACKNOWLEDGMET

We would like to express my sincere gratitude to all those whose support and guidance has been invaluableto the completion of this study. First of all, we would like to express my heartfelt thanks to my mentor, Mr. Mukesh Singh for his valuable guidance and encouragement throughout the research process. The work in this paper is enhanced by his expertise and commitment. We would also like to thank our friends who supported us and provided stimulating learning environment. Their encouragement and friendship were important to overcome the challenges during thisresearch. Lastly, We are so grateful for the support, understanding and encouragement of our family. Their love and belief in my abilities helped us through the highs and lows of this research journey.

REFERENCES

[1] A. Singh and M. K. Dutta, “A robust zero-watermarking scheme for tele-ophthalmological applications,” J. King Saud Univ. - Comput. Inf. Sci., vol. 32, no. 8, pp. 895–908, 2020.

[2] A. Roy, A. K. Maiti, and K. Ghosh, “An HVS inspired robust non-blind watermarking scheme in YCbCr color space,” Int. J. Image Graph., vol. 18, no. 03, p. 1850015, 2018.

[3] M. Sadeghi, R. Toosi, and M. A. Akhaee, “Blind gain invariant image watermarking using random projection approach,” Signal Processing, vol. 163, pp. 213–224, 2019.

[4] X. Zhong, P.-C. Huang, S. Mastorakis, and F. Y. Shih, “An automated and robust image watermarking scheme based on deep neural networks,” IEEE Trans. Multimedia, vol. 23, pp. 1951–1961, 2021.

[5] Li D., Deng L., Bhooshan Gupta B., Wang H., and Choi C.. 2019. A novel CNN based security guaranteed image watermarking generation scenario for smart city applications. Inf. Sci. (N.Y.) 479 (2019), 432–447, 2019.

[6] Bagheri M., Mohrekesh M., Karimi N., and Samavi S.. 2020. Adaptive control of embedding strength for image watermarking using neural networks. arXiv (2020).

[7] Sinhal R., Kumar D., and Ahmad I.. 2021. Machine learning based blind color image watermarking scheme for copyright protection ☆. Pattern Recogn. Lett. 145 (2021), 171–177.

[8] Jagadeesh B., Kumar P. R., and Reddy P. C.. 2016. Robust digital image watermarking based on fuzzy inference system and back propagation neural networks using DCT. Soft Comput 20, 9 (2016), 3679–3686.

[9] Hou J., Ou B., Tian H., and Qin Z.. 2020. Reversible data hidingbased on multiple histograms modification and deep neural networks. Signal Process. Image Commun. 92 (2020).

[10] A. Anand and A. K. Singh, “An improved DWT-SVD domain watermarking for medical information security,” Comput. Commun., vol. 152, pp. 72–80, 2020.

[11] Islam M., Roy A., and Laskar R. H.. 2018. Neural network based robust image watermarking technique in LWT domain. J. Intell. Fuzzy Syst. 34, 3 (2018), 1691–1700.