Using Steganography and Artificial Neural Network for Data Forensic Validation and Counter Image Deepfakes

Matimu Nkuna *, Ebenezer Esenogho *, Ahmed Ali

Posted Date: 18 December 2025

doi: 10.20944/preprints202512.1619.v1

Keywords: AI; DCT; data authenticity; LSB; ANN; SSIM; peak signal-to-noise ratio; steganalysis

 doi:10.20944/preprints202512.1619.v1

Article

Using Steganography and Artificial Neural Network for Data Forensic Validation and Counter Image Deepfakes†

Matimu Nkuna [1,*], Ebenezer Esenogho [2] and Ahmed Ali [3]

[1] Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg, South Africa

[2] Center for Artificial Intelligence and Multidisciplinary Innovations, College of Accounting Science, Department of Auditing, University of South Africa, Pretoria, South Africa

[3] Department of Electrical and Electronic Engineering Technology, University of Johannesburg, Johannesburg, South Africa

* Correspondence: 201598913@student.uj.ac.za

† This article is a revised and expanded version of our paper entitled Integrating Image Steganography Techniques into an Existing Efficient Image Recognition Artificial Neural Network for Optimal Performance, which was presented in the 2024 IEEE PES/IAS Power Africa Conference, Johannesburg, South Africa, 7-11 October 2024.

Abstract

The merging of the Internet of Things (IoT) and Artificial Intelligence (AI) advances has intensified challenges related to data authenticity and security. These advancements necessitate a multi-layered security approach in ensuring security, reliability and integrity of critical infrastructure and intelligent surveillance systems. This paper proposes a two-layered security approach combining a discrete cosine transform least significant bit 2 (DCT-LSB-2) – with artificial neural networks (ANN) for data forensic validation and mitigating deepfakes. The proposed model encodes validation codes within the LSBs of cover images captured by an IoT camera on the sender side, leveraging the DCT approach to enhance the resilience against steganalysis. On the receiver side, a reverse DCT-LSB-2 process decodes the embedded validation code, which is subjected to authenticity verification by a pre-trained ANN model. The ANN validates the integrity of the decoded code, and ensures that only device-originated, untampered images are accepted. The proposed framework achieved an average SSIM of 0.9927 across the entirely investigated embedding capacity of between 0 to 1.988 bpp. DCT-LSB-2 showed a stable Peak Signal-to-Noise Ratio (average 42.44 dB) under different evaluated payloads of between 0 to 100 kB. The proposed model achieved a resilient and robust multi-layered data forensic validation system.

Keywords: AI; DCT; data authenticity; LSB; ANN; SSIM; peak signal-to-noise ratio; steganalysis

1. Introduction

In recent times, researchers have been extensively investigating steganography techniques and their applications in various contexts. With the growing concept of smart cities worldwide, researchers are combining steganography techniques with artificial intelligence to enhance the security of these frameworks [1,2]. Steganography is the practice of hiding information in a cover medium and is sometimes referred to as hiding in plain sight. Instead of watermarking the cover media, steganography embeds and hides data in the actual cover media by modifying the media data bit structure [2,3].

Data security becomes paramount when introducing aspects of IoT, because it involves numerous systems that communicate over a network and share a significant amount of data. IoT

 doi:10.20944/preprints202512.1619.v1

devices primarily exchange data over the Internet using various network protocols. Unauthorized interceptors can manipulate these network communication protocols and access the data that's being shared between the IoT systems. Some of this data may contain sensitive and private details, such as health records and customer information. As a result, data should be protected as far as possible, equally as IoT adoption gradually increases over time [3].

The increased expansion of IoT devices has led to a significant increase in data generation across various fields, including smart cities, industrial automation, and healthcare. While this growth is positive, it also presents a substantial challenge in terms of cyber/data security, as well as authenticity [3,4]. Cybercriminals are using artificial intelligence to mimic the operation of IoT systems, which raises a challenge to trust in the digital sphere. Furthermore, advances such as Generative AI (GenAI) can be used to create deepfakes which carry similar data as generated by smart IoT devices (i.e., image files, videos, audio, etc.). As a result, there is a need for more research on how digital trust can be maintained in today's era, where IoT and AI models are being rapidly adopted [4–6].

In IoT systems, integrating techniques such as image steganography and artificial neural networks can be implemented to enhance digital authenticity and trust [5,6]. These integrations will enable proactive IoT data forensic validation, ensuring that the data shared between IoT devices is authentic and not generated by AI (i.e., deepfakes, etc.) [2]. Furthermore, these measures will ensure that unauthorized interception of IoT data is rapidly detected and mitigated. Use cases can be in the form of secure real-time intelligent surveillance systems that use image steganography and ANNs for data forensic validation [2–5].

This study focuses on the integration of image steganography and ANN to enable IoT data forensic validation and hence counter deepfakes. This method creates a two-layer security framework; the image steganography component embeds and hides data within an image, while the ANN will be used to validate the decrypted embedded data and detect any data inconsistencies. The interaction of these components enables data security and authenticity; hence, attackers will find it difficult to successfully intercept, manipulate, or use deepfakes to forge data in an undetectable manner [2,4–6].

Contribution of this study: Image steganography embeds and hides data using techniques such as the least significant bit (LSB) insertion, which alters the least significant bit of pixel values to hide data [1,2]. The discrete cosine transform (DCT) enables embedding data in the frequency domain of the cover media, thereby making it more robust against compression [2]. Further to the DCT, the discrete wavelet transforms (DWT) technique embeds data into different frequency bands, enabling multi-resolution analysis [3]. These embedding techniques will be used to conceal validation codes/metadata within the pixels of the smart camera images, enabling forensic validation of the pictures and secure data transmission. An ANN model will be trained to recognize patterns and detect anomalies in the IoT device images. The incoming data from the smart camera device is compared against the learned patterns for anomaly detection and alteration. Through the use of the ANN model, only validated data is accepted; therefore, the method enhances the security of IoT camera systems.

This paper is organized into six sections. Section 2 outlines previous similar state-of-the-art works and summarizes the contribution of this study in line with the identified study gaps. Section 3 presents the proposed methodology, which includes the proposed embedding scheme. In section 4, the system model and assumptions are discussed. Section 5 presents the experimental evaluation results and discussion of findings. Finally, section 6 concludes the work and outlines the ideas of future related work.

2. Related Works

The researchers in [2] introduced the components of privacy and authenticity in IoT networks by using a weighted pixel classification image steganography. The work focused on improving performance variables, including embedding capacity, imperceptibility, and the security of the transmitted information. Although this state-of-the-art study yielded better PSNR values, ensuring

 doi:10.20944/preprints202512.1619.v1

imperceptibility, compared to other methods, there remains a risk of data tampering due to the lack of data forensic validation for authenticity. The proposed framework presented in this paper aims to close the identified gap and ensure integration with ANN for data forensic validation, in addition to other performance parameters, as per the findings in [2].

The work presented in [3] focused on addressing the challenges arising from the significant advancement of IoT, specifically in the healthcare sector. Some of the difficulties identified in the study are the security and integrity of medical data in healthcare service applications. [3] proposed a dual security model for securing diagnostic text data in medical images. The proposed model integrated steganographic algorithms, such as the 2-D discrete wavelet transform at one level (2D-DWT-1L) and the 2-D discrete wavelet transform at two levels (2D-DWT-2L), with encryption schemes. The schemes included the Advanced Encryption Standard and the Rivest, Shamir & Adleman algorithms. While this study demonstrated improved results compared to other state-of-the-art methods, it didn't include aspects of integration with ANNs for data forensic validation. Hence, our study proposes a framework that integrates ANNs to enable automated data forensic validation.

Another related previous study is presented in [7]. This study presents a novel steganography method that utilizes the singular value decomposition (SVD) and the tunable Q-factor wavelet transformation (TQWT). It applies the TQWT to distinguish the cover signal into discrete frequency sub-bands. They use the SVD to decompose the high-frequency sub-band coefficients into individual values. This novel technique demonstrated improved patient information security and confidentiality, representing a substantial development in steganography studies. Although the state-of-the-art research in [7] presents valuable findings, the gap identified is that it focuses more on the healthcare application and does not include aspects of ANNs to counter deepfakes and forensic data validation. Hence, the study presented in this paper aims to address the identified gap and enhance its contributions.

[8] presents work examining several steganographic techniques for safe data concealing. Some of the methods included are image steganography masking schemes, as well as the LSB-1, 2, and 3 methods. In study [9], researchers employed encrypted secret messages to determine an advanced steganography algorithm. At the encoding side, the encryption process includes a stego-key before embedding the data. This stego key ensures that, in the event of unauthorized interception, the attacker will not be able to decrypt the secret messages, thereby providing the confidentiality of the information. The study in [9] also focused more on imperceptibility aspects and did not include any elements of authenticity or data forensic validation on the receiver side. From the gap analysis, both novel studies in [8] and [9] did not integrate aspects of ANNs into the steganography methods they proposed, nor did they investigate the data forensic validation aspects. Hence, there is a need to explore the identified gap and develop more robust steganography systems.

3. Proposed Scheme and Methodology

This section discusses the methodology of the study and the proposed scheme background.

In this study, we propose a discrete cosine transform-least significant bit (DCT-LSB) method with a 2-bit resolution (DCT-LSB-2) for steganography systems. The technique is applied forwardly on the sender side of the system for encryption and embedding the secret data bits within the cover image. And a reverse DCT-LSB-2 is used at the receiver side for decryption and recovery of the hidden information. The hidden information can be a validation code embedded within the pixels of the image captured by the smart camera device (i.e., an IP camera). It can be used as a forensic validation criterion on the receiver side. The successful data forensic validation of the code within the pixels of the image will mean acceptance. The ANN will be located on the receiver side and will perform the reverse DCT-LSB-2 operation, then validate whether the decrypted data matches the criteria of the initial embedded validation code.

The discrete cosine transform-least significant bit 2 method (proposed) utilizes the ASCII method to analyze the image consecutively captured by the IoT device, converting it into decimal

 doi:10.20944/preprints202512.1619.v1

and binary forms [1,2]. Before encryption is initiated, the algorithm verifies the image dimensions and the size of the secret data. The IoT camera captured image is partitioned into RGB (Red, Green, Blue), and the two least significant bits of each image pixel are replaced with pairs of the hidden information bits (bit substitution). This method alters coefficients in the transform domain and randomly embeds the private information in the image pixels, thereby reducing the chances of steganalysis, distortion, and cross-detection. The algorithm runs till all the bits of the hidden information are inserted into the image pixels. As a result, before the captured image is transmitted from the IoT device (i.e., IP camera), the secret data is embedded (as previously stated, this data can be a validation code that will be used at the receiver side by the ANN for authenticity acceptance) [7–12].

The formulae for calculating the DCT coefficients for a single 8x8 block of image pixels is:

$$DCT_{xy} = \frac{1}{4} H_x H_y \sum_{p=0}^{7} \sum_{q=0}^{7} F_{pq} * \cos\left[\frac{(2p+1)x\pi}{16}\right] * \cos\left[\frac{(2q+1)y\pi}{16}\right] \quad (1)$$

Where:

$$H_x, H_y = {}^{1}/_{\sqrt{2}} \text{ when } x, y = 0 \quad (2)$$

$$H_x, H_y = 1 \text{ otherwise} \quad (3)$$

x and y are the horizontal and vertical special frequencies for the integers $0 \leq x, y < 8$.

$$F^{Q}_{pq} = \text{round}\left(\frac{F_{pq}}{Q_{pq}}\right) \quad (4)$$

F_{pq} is the pixel value of the cover image at location coordinates (p, q).

Q_{pq} is a quantization table with 8x8 (64) elements.

To evaluate the performance of the proposed method, key parameters such as the peak signal-to-noise ratio (PSNR), mean square error (MSE), and structural similarity index (SSIM) will be utilized. The secret information for experimental purposes will be a static validation code consisting of numerical values, text characters, and special characters. The ANN model will be pre-trained to verify the decoded validation code and confirm that the received image is authentic, has not been tampered with, and is not AI-generated (deepfake).

The structural similarity index is used to quantify the similarity between two images. It considers multiple aspects of the human visual system and quantifies the apparent quality of images. Three key features of the image are compared: structure, luminance, and contrast. The result produces a value between -1 and 1, where a negative value means dissimilarity, 0 means no similarity, and a value of 1 indicates perfect similarity. Hence, higher SSIM values denote greater similarity between images [2–5].

The formulae for calculating the SSIM, MSE, Embedding Rate, and PSNR are given below [1–10]:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu^2{}_x + \mu^2{}_y + C_1)(\sigma^2{}_x + \sigma^2{}_y + C_2)} \quad (5)$$

Where μ_x *and* μ_y are the average luminance of the cover image (without any hidden data) and the stego image (with data embedded in the image pixels). σ_{xy} is the covariance of the pixel intensities between the cover image and the stego image. C_1 and C_2 are added constants to prevent instability when the denominators are close to zero. $\sigma^2{}_x$ and $\sigma^2{}_y$ are the variances of the pixel intensities of the cover image and the stego image.

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - y_{ij})^2 \quad (6)$$

Where M is the number of rows of the cover image, N is the number of columns of the cover image, x_{ij} is the pixel value from the cover image, and y_{ij} is the pixel value from the stego image.

$$\text{Embedding Rate} = \frac{N}{H * W} \quad (7)$$

Where N is the number of secret hidden data bits, H is the cover image height, and W is the cover image width.

$$PSNR = 10 \log_{10}({}^{R^2}/_{MSE}) \quad (8)$$

Where R is the maximum possible pixel value of an 8-bit image (255) and MSE is the value of mean square error.

$$Byte\ length = \frac{Total\ number\ of\ bits}{8} \quad (9)$$

 doi:10.20944/preprints202512.1619.v1

Byte length represents the calculation of bytes for a total number of bits in a piece of data.

4. System Model and Assumptions

In this section, the system model is presented and assumptions are discussed. Figure 1 below illustrates the proposed system model.

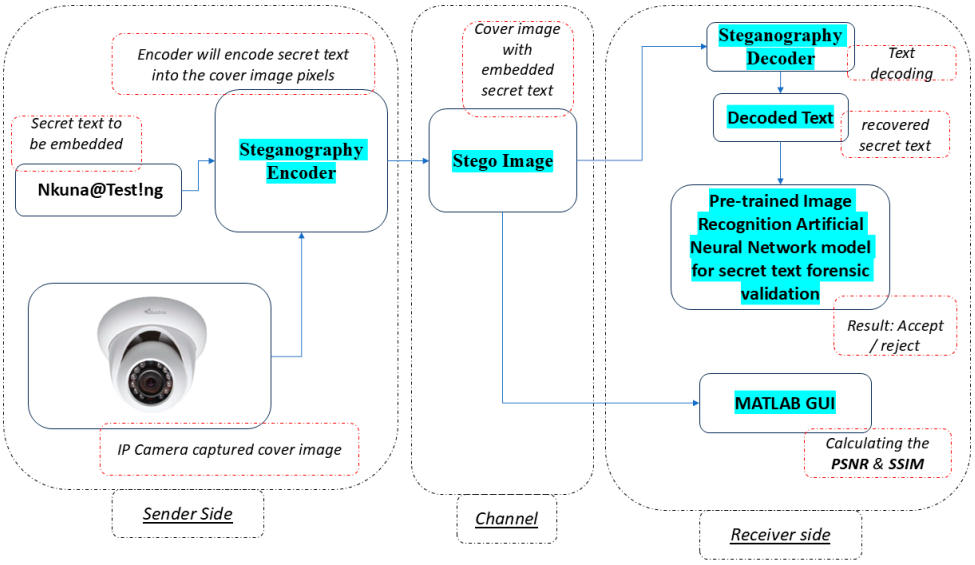

Figure 1. Proposed System Model.

The IP camera will capture the cover image and parse it to the steganography encoder system (where the embedding of the secret text will occur). The encoding algorithm that will be tested is the proposed DCT-LSB-2 scheme. Once the hidden text is successfully encoded into the cover image pixels, the encoder produces a stego image as output. The stego image will be transmitted through a communication channel to the receiver's side, where the embedded secret text will be decoded and fed into the pre-trained ANN for validation. The stego decoder system will use a reverse DCT-LSB-2 algorithm to decode/decrypt the secret text. The recovered text will serve as an input to the pre-trained ANN model for data forensic validation. If the text matches the original secret text, the ANN model will return an 'accept' message, indicating successful authentication. This means that the image captured by the IP camera has not been tampered with and is therefore valid.

However, suppose the ANN model detects that the decoded secret text does not match the pre-trained text. In that case, it will return a 'reject' message, indicating that the received image file is not from an authorized device, has been intercepted, and may be a deepfake image file, which means that the IP camera has been compromised. An unsuccessful verification indicates that an unauthorized interception of the images sent from the IP camera has occurred. The ANN can be configured to send notification alerts for any unsuccessful authentication attempt, allowing responsible individuals to remediate the breach.

To ensure the robustness of the stego system, MATLAB tool is used to calculate the PSNR and SSIM between the original cover image and the stego image, thereby maximizing imperceptibility. Using these parameters, the risk of steganalysis and unauthorized detection of image alterations will be minimized. Hence, increasing the robustness of the whole system. The PSNR and SSIM results obtained through the proposed method will be compared to those achieved in related previous state-of-the-art schemes from the literature.

 doi:10.20944/preprints202512.1619.v1

5. Results and Discussion

This section presents the results obtained during the experimentation of the system model indicated in Figure 1. The results are divided into four sub-sections: the data forensic validation portion, which looks at the authenticity of the decoded secret text (also referred to as the validation code), and the second, third, and fourth sub-sections focuses on the robustness of the proposed encoding scheme by comparison of the obtained PSNR, MSE & SSIM results between the proposed framework and previous results obtained from the related novel studies.

5.1. Determining the Authenticity of the Encoded & Decoded Secret Text for Data Forensic Validation on the Sender and Receiver Side

5.1.1. Encoding

The encoding algorithm was executed, and the following Java console shows the output obtained.

The validation code "Nkuna@Test!ng" contains a total of 112 data bits as indicated in Figure 2. Using formula (9), the byte length of the validation code is calculated to be 14 bytes. The output in Figure 2 also shows that a total of 4 least significant bits were altered in the corresponding pixel locations of the cover (original) image during the encoding process on the sender's side, and the validation code was successfully embedded within the cover image.

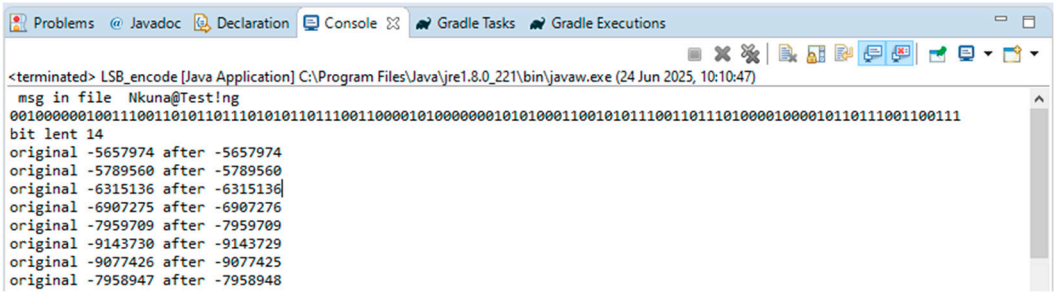

Figure 2. Encoding output -- Java console.

5.1.2. Decoding

The decoding algorithm was also executed on the receiver side, and the following results were obtained from the Java console.

The results presented in Figure 3 above indicate that, according to the system model in Figure 1, the original validation code encoded into the image was successfully decoded on the receiver side. This demonstrates that the proposed framework achieves a successful data recovery, and this output (validation code) will then be fed into a pre-trained ANN for automated data forensic validation.

 doi:10.20944/preprints202512.1619.v1

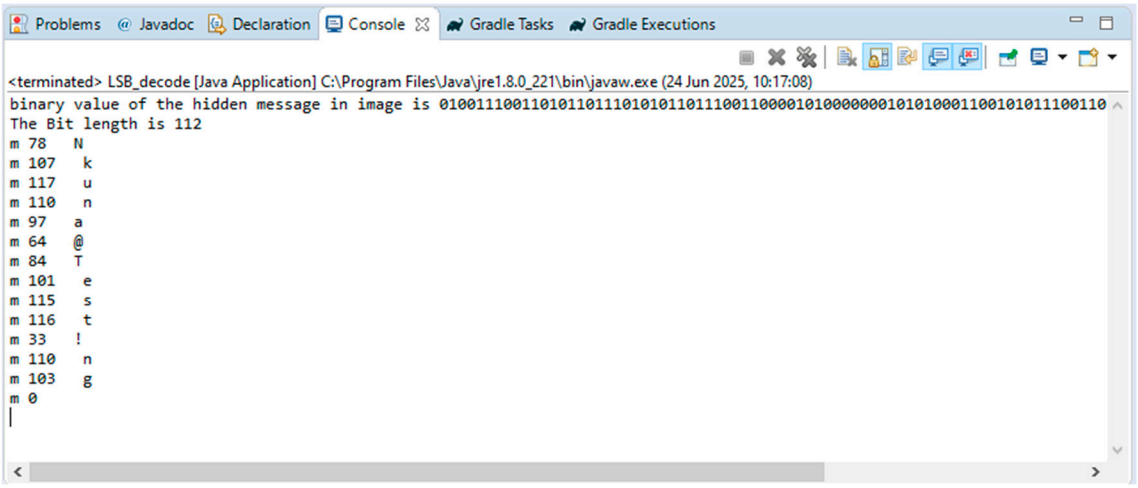

Figure 3. Validation code decoding output -- Java console.

5.2. Experimental Evaluation Results Obtained in Determining PSNR, SSIM, and MSE for the Proposed Framework, with a Cover Image Size of 259 x 194 Pixels

This subsection presents the experimental results obtained from the execution of the proposed model.

From the experimental evaluation and analysis results presented in Table 1, the average PSNR for the proposed framework with a payload of up to 100,000 bits is 42.44 dB. This aligns with theoretical knowledge to limit steganalysis and maximize stego image quality [2–5]. The average SSIM for the system, as per the parameters in Table 1, is 0.9927, which aligns with theoretical expectations to maximize system robustness and resilience.

Table 1. Experimental evaluation results -- PSNR, MSE, SSIM, and PBC.

Payload (kB)	Embedding Rate (bpp)	Percentage Bytes Changed (%)	Peak Signal-to-Noise Ratio (dB)	Structural Similarity Index (SSIM)	Mean Square Error (square pixels)
0.0	0.000	0.00	Inf	1.0000	0.0000
0.03	0.001	0.03	54.29	0.9997	0.2419
0.1	0.003	0.11	52.07	0.9993	0.4039
0.2	0.005	0.19	43.54	0.9948	2.8793
0.8	0.016	0.63	42.18	0.9924	3.9380
2.7	0.053	2.06	42.07	0.9925	4.0372
4.5	0.090	3.49	41.96	0.9922	4.1446
7.0	0.140	5.43	42.08	0.9922	4.0279
11.2	0.223	8.66	42.15	0.9924	3.9681
17.0	0.338	13.14	41.78	0.9917	4.3190
22.6	0.450	17.47	41.91	0.9923	4.1926
26.6	0.529	20.56	41.81	0.9923	4.2833
30.5	0.607	23.57	41.70	0.9923	4.3932
38.4	0.764	29.68	41.61	0.9919	4.4924
46.4	0.923	35.86	41.62	0.9919	4.4821
54.3	1.081	41.96	42.04	0.9920	4.0652
62.2	1.238	48.07	42.05	0.9920	4.0558
63.8	1.270	49.30	41.90	0.9921	4.1955
64.8	1.290	50.08	41.98	0.9922	4.1189

 doi:10.20944/preprints202512.1619.v1

66.2	1.317	51.13	41.94	0.9921	4.1608
67.5	1.343	52.15	41.72	0.9921	4.3780
68.8	1.369	53.17	41.94	0.9923	4.1637
69.5	1.383	53.71	41.94	0.9923	4.1637
70.1	1.395	54.17	41.84	0.9922	4.2558
78.0	1.552	60.28	41.84	0.9921	4.2558
78.6	1.565	60.76	42.05	0.9921	4.0549
79.2	1.577	61.24	42.08	0.9921	4.0270
79.9	1.589	61.72	42.25	0.9921	3.8697
80.5	1.602	62.19	42.25	0.9920	3.8697
81.1	1.614	62.67	42.25	0.9920	3.8697
81.7	1.626	63.15	42.06	0.9919	4.0465
82.3	1.639	63.63	42.06	0.9919	4.0465
83.0	1.651	64.11	41.93	0.9920	4.1685
83.6	1.663	64.59	42.01	0.9920	4.0915
84.2	1.676	65.07	41.87	0.9919	4.2284
84.8	1.688	65.55	41.98	0.9918	4.1265
85.4	1.700	66.03	41.98	0.9929	4.1265
85.8	1.708	66.31	41.84	0.9924	4.2558
88.6	1.763	68.47	41.89	0.9924	4.2090
91.2	1.815	70.48	41.97	0.9924	4.1360
86.0	1.712	66.46	41.97	0.9923	4.1360
93.9	1.869	72.57	42.17	0.9926	3.9462
95.1	1.893	73.49	41.97	0.9922	4.1360
96.3	1.917	74.42	41.97	0.9923	4.1360
97.5	1.940	75.35	41.99	0.9923	4.1123
98.7	1.964	76.28	41.99	0.9924	4.1104
99.9	1.988	77.20	41.99	0.9926	4.1142

5.3. Determining the Level of Robustness of the Proposed DCT-LSB-2 Framework and the Previous State-of-the-Art Models, Considering Similar Cover Image Sizes

The proposed framework yields competitive PSNR results compared to the novel work presented in [13–15] (see Table 2 bellow). This allows the system to exhibit no physical modification properties on the stego image, thereby increasing the robustness of the stegosystem. The novel work presented in [13,15] did not indicate the corresponding payload associated with the PSNR values presented.

Table 2. Average PSNR comparison of the proposed framework with other state-of-the-art schemes.

Without Schur Decomposition [13]	With Schur Decomposition [13]	Hybrid Cryptography and Steganography-Based System [14]	Crypto-steganography scheme [15]	Proposed Framework
16.51	72.50	34.83	70.42	42.44

The results in Table 3 indicate that the proposed framework achieves competitive and, at times, improved PSNR performance compared to the state-of-the-art results presented in [2]. The work in [2] is limited to embedding rates between 0.05 and 0.9 bpp, whereas the proposed framework is evaluated for an embedding rate of up to 1.869 bpp (as shown in Table 1). The proposed framework exhibits stable PSNR values across varying embedding rates, demonstrating system stability and resilience compared to [2].

Table 3. PSNR performance comparison of the proposed scheme with state-of-the-art work presented in [2].

 doi:10.20944/preprints202512.1619.v1

Embedding Rate (BPP)	Scheme PSNR (dB)			
	Difference Histogram Shifting (DHS) [2]	Statistical Features Maintained (SFM_A) [2]	IoTSteg [2]	Proposed Framework
0.05	47	60	65	42.07
0.1	45	57	63	41.956
0.2	43	54	57	42.145
0.3	41.7	52.8	54	41.777
0.4	40	51	51	41.906
0.5	37	50.7	48.7	41.813
0.6	-	-	-	41.703
0.75	-	-	-	41.606
0.9	-	-	-	41.616

According to the results in Table 4, the proposed framework demonstrates highly competitive SSIM performance compared to the state-of-the-art work presented in [2]. The results in [2] were obtained using image sizes of 512 x 512 pixels. In contrast, the proposed framework was evaluated using a smaller image size of 259 x 194 pixels (hence the slight difference in the SSIM values). The proposed model can be further assessed using the same image size as in [2] to increase the SSIM values even higher, thereby enhancing imperceptibility, resilience and robustness.

Table 4. SSIM comparison of the proposed scheme with state-of-the-art work presented in [2]

Scheme	Embedding Rate (bpp)	Average SSIM
IoTSteg [2]	0.1	0.9997
	0.2	0.9994
SFM_A [2]	0.1	0.9997
	0.2	0.9997
SFM_B [2]	0.1	0.9985
	0.2	0.9993
Proposed Framework	0.1	0.9922
	0.2	0.9924

5.4. Comparison of the PSNR and SSIM Parameters Between the Proposed Framework and the Work Presented in [16]

The results in Table 5 indicate an improved PSNR performance of the proposed framework compared to the state-of-the-art PVD_Red method presented in [16]. The proposed DCT-LSB-2 scheme also demonstrates competitive SSIM performance compared to results in [16], indicating a strong imperceptibility property of the stegosystem.

Table 5. PSNR and SSIM comparison of the proposed framework with state-of-the-art work presented in [16].

Embedding Rate (bpp) – as per in [16]	Scheme PSNR (dB)		SSIM	
	PVD_Red [16]	Proposed Framework	PVD_Red [16]	Proposed Framework
1.6737	34.5616	41.87	0.9998	0.9919
1.5364	40.4276	41.84	0.9999	0.9921
1.5586	39.7468	42.05	0.9999	0.9921
1.6721	34.1093	41.87	0.9999	0.9919
1.6727	36.1913	41.87	0.9998	0.9919
1.5505	41.0545	42.05	0.9999	0.9921
1.5920	39.6321	42.25	0.9999	0.9921

 doi:10.20944/preprints202512.1619.v1

6. Conclusions and Recommendations

This paper proposes a two-layered secure steganography-ANN system that combines an image steganography framework with an artificial neural network for robust and resilient IoT systems. The proposed DCT-LSB-2 method demonstrated improved and competitive performance compared to previous state-of-the-art methods, indicating successful evaluation and potential for further investigation to enhance application and performance using higher pixel size cover images. The DCT-LSB-2 method achieved an average SSIM of 0.9927 across the entire range of embedding capacity values, from 0.00 bpp (minimum) to 1.988 bpp (maximum), as specified by the evaluation parameters presented in Table 1. The proposed framework demonstrated stable PSNR performance throughout the evaluation with different payloads (in kB), indicating a resilient system with varying secret/validation code sizes. The proposed system further demonstrates complete and robust encoding and decoding capabilities, enabling the full recovery of validation codes for data forensic validation and thus satisfying the objectives and scope of this work.

Future work will involve evaluating the model using higher pixel size images of various color gradients and color distributions to further enhance the scheme's resilience and robustness. Another aspect is the application of convolutional neural networks (CNNs) rather than the current artificial neural networks (ANNs) in evaluating the proposed framework and examining how it will respond to this approach [17–22].

Author Contributions: Conceptualization, M.N.; methodology, M.N.; software, M.N.; validation, M.N., A.A. and E.E.; formal analysis, M.N., A.A. and E.E.; investigation, M.N.; resources, A.A. and E.E.; data curation, A.A. and E.E.; writing—original draft preparation, M.N.; writing—review and editing, A.A. and E.E.; visualization, M.N.; supervision, A.A. and E.E.; project administration, M.N.; funding acquisition, A.A and E.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Research Fund (NRF) South Africa, grant number PMDS23041994813. The APC was funded by the University of Johannesburg's Department of Electrical and Electronic Engineering Technology and the University of South Africa's Center for Artificial Intelligence and Multidisciplinary Innovations, College of Research and Graduate Studies.

Data Availability Statement: All data has been presented in the article.

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

References

1. Singh, W.G.; Shikhar, M.; Kunwar, S.; Kapil, S. Robust stego-key directed LSB substitution scheme based upon cuckoo search and chaotic map. *Optik* **2018**, *170*, 106-124. https://doi.org/10.1016/j.ijleo.2018.04.135
2. Alarood, A.; Ababneh, N.; Al-Khasawneh, M.; Rawashdeh, M.; Al-Omari, M. IoTSteg: ensuring privacy and authenticity in internet of things networks using weighted pixels classification based image steganography. *Clust.Comput* **2022**, *25*, 1607-1618. https://doi.org/10.1007/s10586-021-03383-4
3. Elhoseny, M.; Ramirez-Gonzalez, G.; Abu-Elnasr, O.M.; Shawkat, S.A.; Arunkumar, N.; Farouk, A. Secure Medical Data Transmission Model for IoT-Based Healthcare Systems. *IEEE Access* **2018**, *6*, 20596-20608. https://doi.org/10.1109/ACCESS.2018.2817615
4. Li, L.; Hossain, M.S.; El-Latif, A.A.; Alhamid, M.F. Distortion less secret image sharing scheme for Internet of Things system. *Clust.Comput* **2019**, *22*, 2293-2307. https://doi.org/10.1007/s10586-017-1345-y
5. Pannu, A. Artificial Intelligence and its Application in Different Areas. *IJEIT* **2015**, *4*, 79-84. https://doi.org/10.1007/s10586-017-1345-y
6. Ebiaredoh-Mienye, S.A.; Esenogho, E.; Swart, T.G. Artificial neural network technique for improving prediction of credit card default: A stacked sparse autoencoder approach. *IJECE* **2021**, *11*, 4392-4402. https://doi.org/10.11591/ijece.v11i5.pp4392-4402
7. Mathivanan, P.; Ganesh, A.B. ECG steganography based on tunable Q-factor wavelet transform and singular value decomposition. *IMA* **2020**, *31*, 270-287. https://doi.org/10.1002/ima.22477

8. Umamaheshwari, M.U.; Sivasubramanian, S.; Pandiarajan, S. Analysis of Different Steganographic Algorithm for Secured Data Hiding. *IJCSNS* **2010**, *10*, 154-160. http://paper.ijcsns.org/07_book/201008/20100825.pdf
9. Nath, J.; Nath, A. Advanced Steganography Algorithm Using Encrypted Secret Message. *IJACSA* **2011**, *2*, 19-24. https://doi.org/10.14569/IJACSA.2011.020304
10. Houssein, E.H.; Ali, M.A.; Hassanien, A.E. An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption Algorithm. In Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), Gdansk, Poland, 11-14 September 2016.
11. Zhang, Y.; Jiang, J.; Zha, Y.; Zhang, H.; Zhao, S. Research on Embedding Capacity and Efficiency of Information Hiding Based on Digital Images. *IJIS* **2013**, *3*, 77-85. https://doi.org/10.4236/ijis.2013.32009
12. Driss, M.; Berriche, L.; Atitallah, S.B.; Rekik, S. Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions. *IEEE Access* **2025**, 13, 74844-74875. https://doi.org/10.1109/ACCESS.2025.3564120
13. Susanto, A.; Sinaga, D.; Mulyono, I.U. PSNR and SSIM Performance Analysis of Schur Decomposition for Imperceptible Steganography. *SJI* **2024**, *11*, 803-810. https://doi.org/10.15294/sji.v11i3.9561
14. Suguna, T.; Padma, C.; Rani, M.J.; Priya, G.P. Hybrid Cryptography and Steganography-Based Security System for IoT Networks. *IJRITCC* **2023**, *11*, 415-421. https://doi.org/10.17762/ijritcc.v11i8s.7221
15. Alsamaraee, S.; Ali, A.S. A crypto-steganography scheme for IoT applications based on bit interchange and crypto-system. *BEEI* **2022**, *11*, 3539-3550. https://doi.org/10.11591/eei.v11i6.4194
16. Setiadi, D.I. PSNR vs SSIM: Imperceptibility quality assessment for image steganography. *Multim. Tools Appl.* **2021**, *80*, 8423-8444. https://doi.org/10.1007/s11042-020-10035-z
17. Helmy, M.; Torkey, H. Secured Audio Framework Based on Chaotic-Steganography Algorithm for Internet of Things Systems. *Computers* **2025**, *14*, 207. https://doi.org/10.3390/computers14060207
18. Nkuna, M.C.; Esenogho, E.; Heymann, R.; Matlotse, E. Using Artificial Neural Network to Test Image Covert Communication Effect. *JAIT* **2023**, *14*, 741-748. https://doi.org/10.12720/jait.14.4.741-748
19. Daiyrbayeva, E.; Yerimbetova, A.; Merzlyakova, E.; Sadyk, U.; Sarina, A.; Taichik, Z.; Ismailova, I.; Iztleuov, Y.; Nurmangaliyev, A. An Adaptive Steganographic Method for Reversible Information Embedding in X-Ray Images. *Computers* **2025**, *14*, 386. https://doi.org/10.3390/computers14090386
20. Nkuna, M.C.; Esenogho, E.; Heymann, R. Using Artificial Neural Network to Analyze Stego Images. *RJEES* **2021**, *6*, 476-482. https://doi.org/10.5281/zenodo.5805077
21. Nkuna, M.C.; Esenogho, E.; Heymann, R. Integrating Smartphone Network Architecture and Data Security Techniques to Mitigate Sharp Practises in Non-Profit Organisations. *JCM* **2020**, *15*, 755-767. https://doi.org/10.12720/jcm.15.10.755-767
22. Nkuna, M.C.; Ali, A.; Esenogho, E. Integrating Image Steganography Techniques into an Existing Efficient Image Recognition Artificial Neural Network for Optimal Performance. In Proceedings of the IEEE PES/IAS Power Africa Conference, Johannesburg, South Africa, 7-11 October 2024. https://doi.org/10.1109/PowerAfrica61624.2024.10759430