The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 2, April 2025
https://doi.org/10.33022/ijcs.v14i2.4759

Enhancing Data Security: A Hybrid Approach of AI-Driven Steganography and Encryption

Ammar Mohammedali Fadhil[1]
ammaral-khafaji@mtu.edu.iq[1]
[1] Information and Communication Technology, Middle Technical University, Iraq

Article Information

Received : 24 Feb 2025
Revised : 2 Apr 2025
Accepted : 15 Apr 2025

Keywords

Data security, AI-driven steganography, encryption, hybrid approach, cybersecurity, deep learning, steganalysis, cryptography

Abstract

In the era of technological development and the Internet, the volume of data transmitted in digital networks is constantly increasing. Ensuring data security has become one of the important challenges in our time. Encryption processes protect data security, but they are often exposed and attract attention. Steganography models are a technique that hides sensitive data but lacks cryptographic protection. The study proposes a hybrid security approach that combines encryption strength and data hiding to be secure against digital attacks. The proposed method takes advantage of one of the artificial intelligence techniques represented by deep learning, which depends on dynamically changing weights during encryption and embedding in the image. This allows us to obtain strong security and high imperceptibility. In the proposed approach, security is enhanced through several layers, the first of which is dynamic changes to generate random numbers and variable encryption as a result of the dynamics of the encryption key and finally hiding the data in a way that cannot be detected. The experimental results showed the merit of the proposed approach through the strength of the results such as the uniformity of the histogram peaks and high entropy = 8 and high imperceptibility represented by BSNR = 91dB. Our research contributes to enhancing data security and countering cyber attacks by exploiting artificial intelligence techniques. Future work has been proposed that opens up horizons for studies using other artificial intelligence techniques such as machine learning and improving real-time data processing in the digital network.

A. Introduction

The era of information technology and the digital age, there is a huge amount of sensitive information that is transmitted daily through different communication networks, so ensuring that information according to strong security mechanisms is a very strong challenge [1]. Traditional encryption techniques in current studies provide different encryption mechanisms such as symmetric encryption and asymmetric encryption that provide confidentiality by converting plain text into unreadable cipher text. However, these methods are vulnerable to cryptographic attacks. Once the encrypted data is displayed and present, it attracts the attention of hackers and intruders. On the other hand, steganography provides an alternative approach by hiding sensitive data in a medium so that it is not perceptible to the observer. While steganography is one of the methods that are worthy of hiding and obscuring data in undetectable environments. However, it does not provide strong encryption, which makes the data vulnerable to manipulation [2].

Researchers have recently discovered hybrid data security models that combine encryption and steganography techniques and overcome their limitations [3]. However, the proposed models are mainly based on traditional encryption and stealth methods. However, they can be detected by modern methods, and traditional encryption methods mainly suffer from computational inefficiency, which is the main reason for their lack of use in various fields. Recent developments in the field of artificial intelligence and machine learning have opened up new possibilities in this field. In order to enhance both encryption and steganography, artificial intelligence can identify the embedding locations in the media that transmit information, which in turn reduces the distortions caused by embedding information to the media. Statistical and visual distortions are what question the quality of the image or data in general, and encryption based on artificial intelligence can generate a variable smart encryption key to improve data security and increase its efficiency [4].

In this manuscript, we propose a new approach based on the integration of encryption and steganography guided by artificial intelligence, to obtain the highest levels of data security. This proposed approach basically consists of three stages: encrypting the data to be hidden using one of the encryption methods, then embedding the encrypted data in the image or in a part of the image. Finally, generating the encryption key and random data using deep learning. The hybrid approach provides multi-layered security methods to ensure the confidentiality and security of the data in the transmitted image and the inability to be discovered by intruders. This is enough to make the proposed model highly resistant to cyber attacks. The manuscript includes several sections: a section on encryption and steganography methods and an overview of them, the following section provides an overview of deep learning and its working mechanism, and then a section detailing the proposed approach, which explains the basis of the contribution to this manuscript, followed by an analysis of the results we have reached. By leveraging the power of artificial intelligence to optimize both encryption and steganography, this study aims to present a robust, efficient, and imperceptible data security framework that can be applied to various fields, including secure communications, digital forensics, and confidential data transmission.

a. **Image security**

Nowadays, dealing with images on the Internet and elsewhere has increased [5], and dealing with digital images has increased. Therefore, unauthorized access and security threats have also increased, including cyber attacks and browsing. These concerns can be dispelled by integrating several methods to maintain data security and using artificial intelligence, which plays a major role in this. Each method has a specific advantage and limitations that we can enhance. Encryption and Steganography play a major role in data security in images [6]. Encryption changes the data format from readable to incomprehensible. Steganography hides the encrypted data inside the image in a way that makes it impossible to detect or track. Text can be encrypted by dividing it into a square matrix with specific names, and for each section we deal with the distribution of places between rows and columns. Then the content of a single location consisting of one byte is changed by changing the places of the bits inside it. This results in a very complex mixture of location and content. Images are made up of tiny cells called pixels, which are made up of a numerical value equivalent to one byte of data. A color image consists of three channels, each color channel, like a circle divided into three images. Data is mostly stored in pixels, and each pixel consists of 8 bits (one byte).

1) Main Principles in Image Security

- **Biplane**

The image is basically made up of pixels and each pixel consists of 8 bits. That is, the total image consists of eight binary levels. In the encrypted image, according to the proposed method, it consists of data bits and the eighth bit is used as a key to encrypt the original image [7]. The image that the algorithm works on has a resolution of (256.256). As shown in Fig. 1.

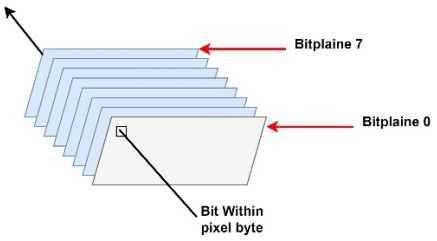

Figure 1: biplane in image encryption

- **Histogram**

The histogram of an image is a graph of the pixel values in the image. It represents the number of pixels with a certain intensity and their number in the image. In a grayscale image, which is basically made up of 8 bits, where a single pixel does not exceed 2^8, or 256, so the histogram displays 256 numbers that show the distribution of pixels at that frequency. One of the characteristics of good encryption is that the distribution of color intensity in the encrypted image is uniform, as we will see in the results section [8].

In the encrypted image, no description is provided in the histogram, especially if the encryption is strong and uniform in the vertices. Often, when detecting attacks, the image with equal borders in the histogram is very immune and cannot be decrypted in any way. In grayscale, the values are distributed according to the color gradient in the image, but in the encrypted one, they are not.

- **Correlation**

One of the most important measures that can be relied upon in encryption is correlation, which symbolizes the strength of the relationship between a pixel and its surrounding pixels. The correlation between neighboring pixels is stronger than its distant counterparts, and they are said to be less correlated as there is a correlation coefficient that can be calculated for that. In the case of encryption, we manipulate the pixel correlations so that neighboring pixels are less correlated, and this is the process of hiding details in the image [9].

$$cor = \frac{cov(x,y)}{\sigma x \times \sigma y} \quad (1)$$

Such as : $\sigma x = \sqrt{var(x)}$ and $\sigma y = \sqrt{var(y)}$ and *var* can be find as :

$$var(x) = \frac{1}{N}\sum_{i=1}^{N}(xi - E(x))^2 \quad (2)$$

$$cov(x,y) = \frac{i}{N}\sum_{i=1}^{N}(xi - E(x))(yi - E(y)) \quad (3)$$

Where *x,y* are the grey value of adjacent values, and *N* is the number of pixels in image.

- ***Encryption Quality***

Encryption quality refers to the total changes in pixel values or grayscale intensity between the original and encoded images [29]. Can be calculated as:

$$Q = \frac{\sum_{i=0}^{255}|HL(F) - HL(\acute{F})|}{256} \quad (4)$$

Where *L* consider as grey level, *HL(F)* number of pixels with grey level in original image and $HL(\acute{F})$ number of pixels with grey level in encrypted image

- **Key sensitivity**

The sensitivity key is used to measure the amount of change that has occurred in the encrypted image. With this key, we can sense any small change, even 1 bit. The image *I* is entered into the program with the encryption key and the key *K*1 is used for encryption to get the image *C*1. The same image *I* is entered into the program but with a second key *K*2 that differs by one bit from the previous one to get the image *C*2. The difference is obtained from the difference between the two images [10].

b. **Deep Learning**

Deep learning is a type of machine learning, which in turn is derived from artificial intelligence. Where the features are learning through experience and the number of times of training to solve a lot of problems. Also, deep learning can extract many complex features from an image that contains simple features. In traditional simple algorithms, features are extracted by manual methods, which makes it difficult for automatic extraction of complex features through the algorithm, and thus the solution to problems is only limited to simple problems. On the basis of this basic structure, many scientists have conducted in-depth research in deep learning, as well as improved the proposed algorithms that are concerned with pixels and their locations in the image. Some deep learning algorithms took care of dividing the image into small sections in order to process each section separately. A core part of the deep learning algorithms emphasized recognition of people and objects, natural language processing, human face recognition, and vision improvement [11]. Deep learning algorithms train low-resolution images in order to improve the quality of the images in pixel alignment on the image

resolution to be more quality [12]. Some algorithms focused on improving the edges of the image and the parts inside the image and extracting features on this basis. The deep neural network algorithm also takes it upon itself to improve the image quality by adapting the neural network to the features extracted from complex images, changing the hidden layer, and sometimes increasing or decreasing nodes in the same layer. As shown in Fig. 2.

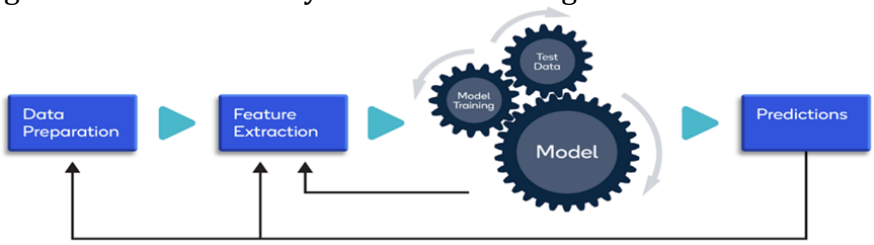

Figure 2. Deep learning System

In this manuscript a modified method of deep learning is proposed in order to increase the image quality. It is considered one of the most important goals of the deep learning network, which is to improve the image [13]. The process here is mainly aimed at restoring a clean image specification free of noise that is the cause of image deterioration. Noise is mostly of the Gaussian type and is added initially to the image. A Deep Neural Network (DNN) is used, which is optimized in this study. The DNN is used to extract a lot of useful information from a noisy image that is of insufficient quality, and this is a common problem with many images. An example of the remaining deep neural network, which was mentioned in the literature, and which was concerned with the formulation of image quality, and these algorithms were used in image processing in patterns recognition and early detection, but on the condition that there is an image with high resolution or high quality .

Features can be processed at the same level, so the features of the original image can be dependent on the resulting image. This reason leads to the size of the data will become smaller and thus the deep network design is more difficult. In the same way, the deep learning algorithm can repeat data during and after work for processing accuracy. Many studies focused on the use of deep learning to enhance images by circumventing the vertical and horizontal vectors represented by the rows and columns in the image. From this method, features are extracted better, which is the basis for building a deep neural network. The non-linear active layer influenced the construction of the deep learning method to increase the image quality. The processing of pixels in the image is done carefully and accurately after processing the regenerative active layer. Many deep learning algorithms do not consider to take time, because the image information is more important than the required time. In this direction, the algorithm can calculate the input and output of the high-quality image and indicate the benefit of the conversion. As shown in the Fig. 3.

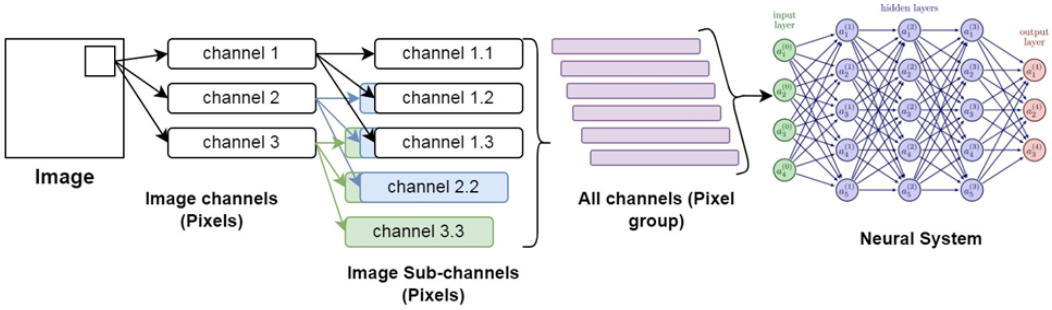

Figure 3. Deep Neural Network within image security.

B. Related Work

The integration of AI, steganography, and encryption has received wide attention to enhance data security, especially in recent years. The need to protect data from various threats has led to the proposal of more than one hybrid model [14]. All the techniques proposed in previous studies offer different advantages, but the integration of these models can provide a more secure data environment and more adaptable to specific circumstances. In this section, we introduce AI-based steganography methods and some encryption methods that rely on hybrid models to enhance data security.

Steganography is an old method in its early days and has evolved through technological imagination. It is a method that relies on hiding data inside other data formats to be familiar and harmless [15]. As in the case of stealth in audio, image and video files, this ensures that sensitive data is hidden from prying eyes and avoids detection attempts. Traditional stealth methods use the replacement of the least significant bits in the image pixels with the least significant bit (LSB) and are widely used because they are simple and uncomplicated, but they remain vulnerable to detection due to their ubiquity [16]. In order to be more robust and robust, alternative methods have been proposed, including the discrete cosine transform (DCT) and the discrete wavelet transform (DWT), which encapsulate sensitive data in the frequency domain, which helps keep mobile data in a form that is resistant to attacks and has less distortion. Recently, some researchers have turned to integrating deep learning techniques into stealth, and the data in the database is trained on convolutional neural networks (CNNs) in order to have better embedding. In this case, the anonymity is better and the robustness against cyber attacks is stronger. A method to improve or increase the data load and avoid detection by hackers by learning patterns in advance [17]. Another method used to maintain data security is encryption, which is one of the most widely used methods to ensure data confidentiality. Symmetric encryption, such as AES (Advanced Encryption Standard), is considered more secure, less complex, and more secure in data encryption. On the other hand, asymmetric encryption methods, such as RSA secure key exchange, are more computationally complex and relatively efficient. In terms of quantum computing, discovered by [18], it was the most advanced step in data security. Despite the great secrecy in maintaining data, it represents a source of attention for intruders. This makes it vulnerable to adversaries and statistical

attacks. In this context, researchers were urged to find ways to hide encrypted data, which is considered one of the best features in data security. This is the idea behind combining encryption with steganography.

In the proposed hybrid models that combine steganography and encryption, the common advantages offered by both methods can be taken advantage of. In this context, data is encrypted and then hidden in a medium such as an image, to ensure confidentiality first and intangibility second. Here, the data is included in two layers of security, encryption and steganography. In early studies, such as [19], it was shown that steganography and encryption can be combined in order to preserve data during digital communication. Sometimes, these methods face problems in terms of computational operations, inefficiency, and inability to withstand attacks. In order to enhance security and meet the challenges, artificial intelligence has been used to activate the role of both encryption and steganography. In this field, [20] presented a new approach to embed encrypted data in a secure medium such as an image and operate in a mobile and adaptive manner. This can produce a more efficient and reliable system in data security. In addition to all of the above, AI has shown promising solutions in this field to secure data in encryption, stenography, and embedding, through adaptive models that improve methods. [21] Were interested in developing a model based on adjusting encryption keys and adapting to new embedding patterns that are created during training. Hybrid models enhanced by AI are very effective in applications that require real-time, faster, imperceptible, and secure data transfer.

In this context, we know that the problem statement we intend to solve is to overcome the weaknesses in the two methods of encryption and stenography to reach the best efficiency, and to address the challenges based on the use of artificial intelligence in data security applications to prevent computational complexity.

From the above we can state the objective of this study as:

- To design hybrid model of securing data on encryption and steganography.
- To develop the model of generating random key based on deep learning of dynamic weight.
- To increase the robustness and imperceptibility of securing data in image.

C. Research Method

The The process of securing data in images is done through encryption and there are three main processes to achieve this goal other than pre-processing and evaluation processes, which are: The first stage called diffusion involves the process of changing the data locations in the image, i.e. mixing the block data components, in order to destroy the relationship between adjacent data. This process includes two secondary processes: key generation and mixing. The encryption key is generated using a Gaussian map with the help of the CNN model. The second process is diffusion, which aims to change the data values themselves and change randomly. The histogram in this case must be approximately uniform after encryption in order to resist interference with the data and erase any evidence of it. Fig. 4 illustrate the general framework of proposed model.

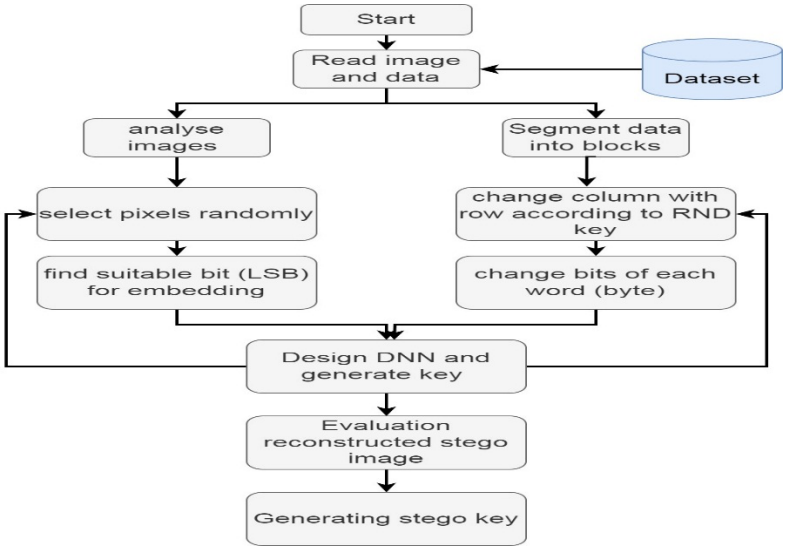

Figure 4. General framework

In the proposed model, the image and data to be encrypted are obtained from a standard database, and then two parallel methods are used. The first works on dividing the explicit data into several square blocks, provided that the data in the columns is the same number as the rows. In the initial method, the columns are replaced by rows according to the random number generated by the DNN, and then the data is scrambled inside the block in an incomprehensible way. The next stage is to scramble the bits in the word of the data. The second method that works in parallel is the image that comes from a database and randomly selects the pixels, and then we take the encrypted data and embed it to the LSB pixel bits. As shown in Fig. 5.

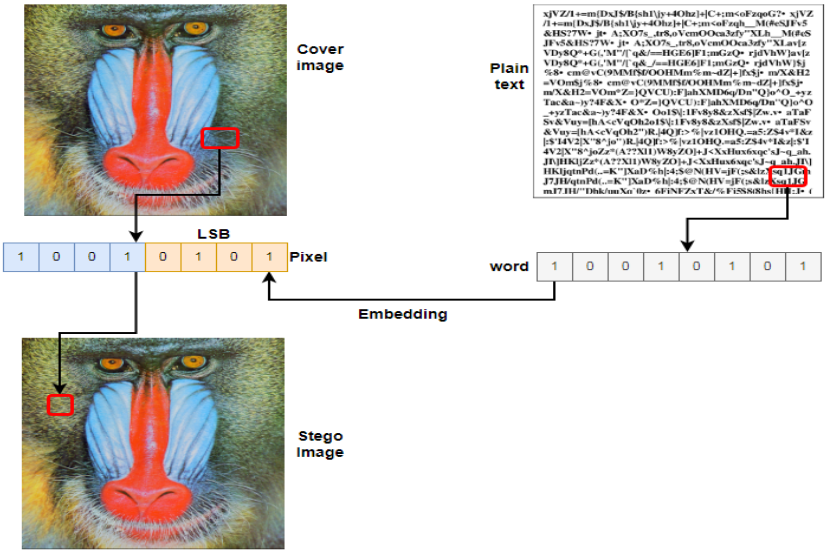

Figure 5. Embed encrypted text into cover image

In the diffusion process, a chaotic map is used with Gaussian noise added to it to create the diffusion key. In the first step, a random matrix is generated for

diffusion with the size of the normal image, and then an XOR is performed between the diffusion matrix and the encrypted image.

Proposed method contribute the dynamic weight that effect the DL system at this stage, by making the difference in construction layer less as possible to take effect the pixel contrast and number of pixels in certain image. Every layer in neural network system have different weight then different action accordingly, we aim to find the highest effected weight and try to use or modify it. There are many variables affecting the deep neural network, sometimes some variables are controlled to have a greater impact on the result. And some variables cannot change along the course of the deep learning process, these variables can change in the case of changing the structural structure of the neural network. Changing the shape of the deep neural network is the basis for increasing the quality of the image, and this is necessary in medical images to increase the accuracy of diagnosis, but sometimes it takes a long implementation time. As shown in the Fig. 6.

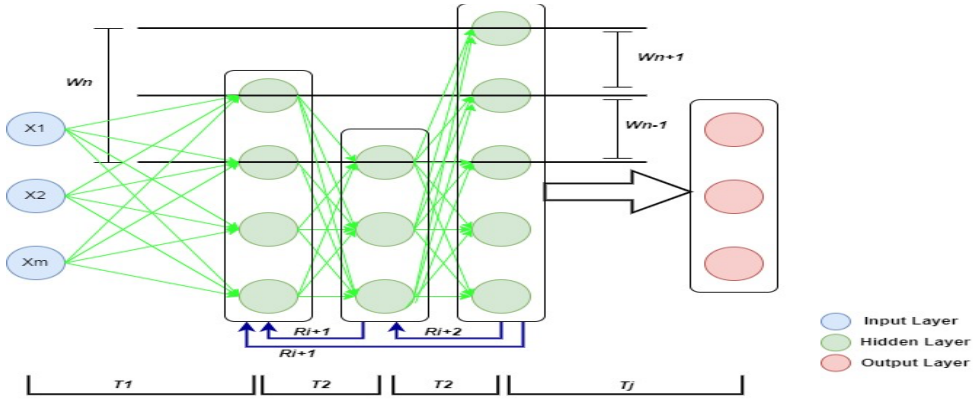

Figure 6. Restructure of deep neural network within its layers.

During the training period, there are multiple variables that control the neural network, and to get a good result, the neural network can predict the result better. Variables such as weight, transaction, recursive number, iteration rate with feedback and acknowledgment are all considered in our study. The creation and updating of hidden layers in the deep neural network depends on the acknowledgment of each layer by feedback to the layer before it, and so on.

After the embedding process, the stego image is produced, after evaluation with the two types of encryption and steganography as will be discussed in detail in the next section. The image containing the secret data is sent to the other party. The encryption key and stego can also be sent with the image or separately. After receiving, the process is carried out in reverse of the embedding procedure in order to extract the secret data with the help of the encryption key.

[Table content writing format: cambria 10, space single]

D. Result and Discussion

In this section, we will list the results and the effect of the proposed method on the result in encryption. In the confusion part, the goal is to reduce the correlation to the minimum possible between the data items in the block text, and

breaking the correlation is done by redistributing the data and distributing them in the image in a chaotic way.

One of the most successful methods in attacks is the statistical method, and in order to resist this attack, the encryption method must be good. To ensure a good encryption method, the horizontal, vertical, and diagonal pixel correlation must be calculated in the plain and encrypted image, and the correlations are calculated according to the following equations.

$$Cor = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (5)$$

Such as : $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - x')^2$ (6)

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - y')^2 \quad (7)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - x')(y_i - y') \quad (8)$$

Where *(x,y)* is the data position and (x', y') is the next position. The confusion step reduces the correlation between adjacent data in the image as shown in the Table 1 while the entropy will not be affected due to the change in the data item locations.

Table 1. Evaluation correlation

Item	block Size	*Horizontal*	*Vertical*	*Diagonal*
Item 1	512 x 512	-0.000569	0.00232	0.000910
Item 2	256 x 256	0.001282	0.00182	0.003093
Item 3	256 x 176	-0.000971	0.00034	-0.00584
Item 4	200 x 289	-0.000775	-0.00956	0.000796
Item 5	512 x 420	0.000788	0.00568	0.00374
Item 6	256 x 300	0.000982	-0.00457	0.00323
Item 7	512 x 400	0.000342	0.000239	-0.00765
Item 8	512 x 256	-0.00026	-0.00098	-0.00261

The histogram shows the distribution of data intensity in the blocks. One of the specifications of a good encryption method is that the histogram should be uniform to reflect the impossibility of obtaining the encrypted information. After implementing the histogram method, the data will be as shown in the Fig. 7, and the image will be of size 256×256 pixels.

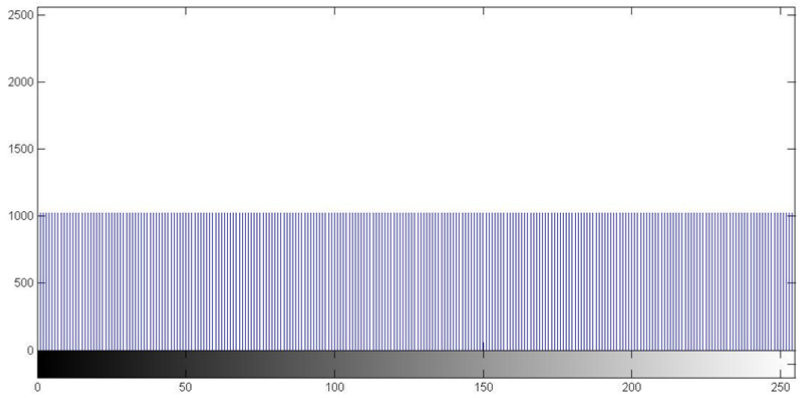

Figure 7. Histogram uniformed through proposed method of 256×256 pixels

Chaotic

Chaos is known to be a widespread phenomenon in most nonlinear systems and is highly sensitive and random in behavior. The logistic map is a quadratic boundary that has been used in cryptography due to its simple application and complex result and can be described in the equation.

$$X_{n+1} = rX_n(1 - X_n) \quad (9)$$

Consider *r* the control parameter such as $r \in (0,4)$ and *n=1,2,3,… . X1* represent initial condition (seed value) occur ($0< X_1 <1$). And the chaotic will be in value of (between 3.5699 and 4) as shown in Fig. 8.

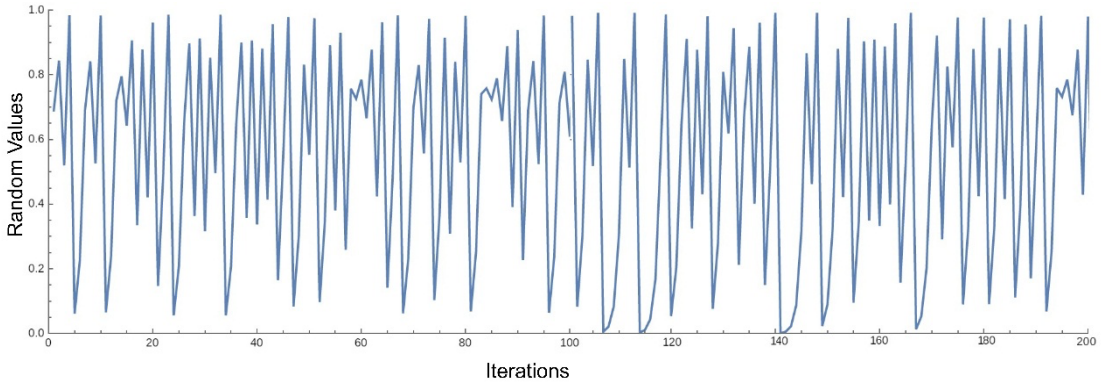

Figure 8. Logistic map behavior

In term of cobweb diagram easy can draw the chaotic logistic map as in Fig. 9. The behavior in the form is based on the chaos in the encrypted text, which depends on the method used. The more chaos there is, the more impossible it is to decrypt without the encryption key. Text encryption is considered complex due to the limited dimensions of the image to be encrypted and thus the limited data. But when repeating the training process in DNN, we reach a stage where the chaos is almost impossible in order to transfer the text to the other party safely.

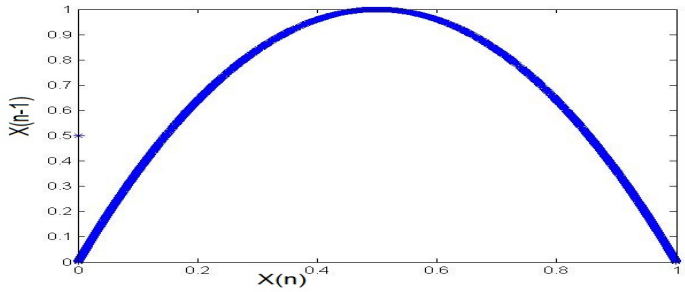

Figure 9. Cobweb behavior of complex chaotic

Entropy

The change from the degree of certainty can be measured by entropy. Entropy is often defined as the degree of randomness or disorder of the system. Hence, entropy came as a standard to measure the degree of randomness in the encrypted image. In the case of the closeness of the red, green or blue color intensity, the entropy is close or most likely = 8, and even in the case of the gray image, when the intensity of the pixels is equal, the entropy = 8, so the entropy of the encrypted image is 8, and this is what the proposed method did, which relied on the number of training times to get the best result. Entropy can find by this equation:

$$H(m) = \sum_{i=0}^{M-1} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (10)$$

Considering M is the total number of pixels, $P(m_i)$ is the possibility of occurrence symbol m_i in binary mode. Then the perfect of entropy in image encryption is 8. In Table 2 shows some encrypted images with their entropy.

Table 2. Entropy with different iterations and complex data

Data item	*Data Size*	*Entropy*
Data 1	2^{512}	8
Data 2	2^{128}	7.9
Data 3	2^{256}	7.9
Data 4	2^{128}	8
Data 5	2^{128}	8
Data 6	2^{512}	7.9

From here we know that the encryption system is important in securing data and also depends on the method used. The image from the dataset is encrypted and also produces a cipher image and is sent to the other party and at the other party it starts reversing the encryption method to form and return the original image.

The processing of an image may affect its quality or lose some image information. There are two methods for evaluating the stego image including objective and subjective. The former one depends on finding the differences by applying some criteria such as ground truth or prior knowledge of statistical issue. Conversely, the subjective methods depend on the observation of humans and judgment without requiring any reference criteria. This section presents the results on PSNR obtained using objective methods. The results obtained using the

subjective methods. The quality of image after embedment is measured using PSNR, which is defined as:

$$PSNR = 10.log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad (11)$$

The expression Mean Square Error (MSE) yields:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (12)$$

Where MAX is the maximum possible pixel value of the image with m, n are the dimensions of the image and I, and K are the original and noisy pixel, respectively.

The value of PSNR is adversely affected by MSE. The parameters of PSNR allowed to normalizing the equation for all methods and image types. Three types of embedment are used to evaluate the system such as the simple LSB and the BIM as displayed in Table 3.

Table 3. Imperceptibility with different payload capacity

Payload (Bytes)	Embedding (%)	*PSNR (dB)*		
		Simple LSB	***Hybrid***	***With DNN***
16384	6.25	62	82	91
32768	12.5	60	80	96
49144	18.75	58	78	87
65576	25	47	61	81

E. Conclusion

In this study, a novel approach is proposed that uses a hybrid of stenography and encryption for data based on a deep learning algorithm and dynamic weight change. When these two techniques are combined, the result is enhanced. Encryption secures sensitive data and stenography ensures that it cannot be explicitly discovered. The AI represented by the updated deep learning algorithm increases data security and efficiency. The proposed approach addresses the common challenges of vulnerability to attacks and computational inefficiency. The system based on deep learning algorithm adjusts encryption through patterns during the training process and thus the dynamic encryption strength that adapts to the characteristics and conditions of the network. In addition, the encryption when embedded in the image cannot be viewed or detected at best. The experimental results show that the hybrid model is better than independent encryption or stealth methods in terms of security and imperceptibility. The Histogram showed an indication of encryption strength through the unification of peaks, and the entropy was better = 8, while in terms of imperceptibility, the result of the BSNR was of high merit = 91 dB. The hybrid system enhanced by artificial intelligence provided a more robust and secure solution. Future work can focus on increasing the storage capacity of the transmitted image and improving performance in terms of using models based on artificial intelligence such as

machine learning. Cyber threats still pose a risk to data transmitted through the network, so challenges still exist to overcome them and maintain data security.

F. Acknowledgment

I would like to express our sincere gratitude to all those who contributed to the completion of this research. My sincere appreciation goes to the Middle Technical University that supported this research, providing the resources and opportunities to conduct this work. Lastly, we would like to thank our families and loved ones for their unwavering support and understanding during this project. Their patience and encouragement have been a constant source of motivation.

G. References

[1] A. A. Abdulla, "Digital image steganography: challenges, investigation, and recommendation for the future direction," *Soft Comput.*, vol. 28, no. 15, pp. 8963-8976, 2024.

[2] A. M. Fadhil, H. N. Jalo, and O. F. Mohammad, "Improved security of a deep learning-based steganography system with imperceptibility preservation," *Int. J. Electr. Comput. Eng. Syst.*, vol. 14, no. 1, pp. 73-81, 2023.

[3] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image steganography using LSB and hybrid encryption algorithms," *Appl. Sci.*, vol. 13, no. 21, p. 11771, 2023.

[4] D. Xu, G. Li, W. Xu, and C. Wei, "Design of artificial intelligence image encryption algorithm based on hyperchaos," *Ain Shams Eng. J.*, vol. 14, no. 3, p. 101891, 2023.

[5] S. Rahman *et al.*, "A novel and efficient digital image steganography technique using least significant bit substitution," *Sci. Rep.*, vol. 15, no. 1, p. 107, 2025.

[6] A. F. H. Al-Bayati, M. Çevik, and A. M. Fadhil, "An improved steganography system based on contrast variation with Fibonacci decomposition to increase imperceptibility," M.S. thesis, Altınbaş Univ., Lisansüstü Eğitim Enstitüsü, 2023.

[7] A. M. Fadhil, "Bit inverting map method for improved steganography scheme," Ph.D. dissertation, Univ. Teknologi Malaysia, 2016.

[8] A. Atadoga *et al.*, "A comparative review of data encryption methods in the USA and Europe," *Comput. Sci. IT Res. J.*, vol. 5, no. 2, pp. 447-460, 2024.

[9] C. D. Liu and S. Santini, "Hiding from Facebook: An encryption protocol resistant to correlation attacks," *arXiv preprint arXiv:2404.18817*, 2024.

[10] L. L. Zheng *et al.*, "Enthalpy and entropy synergistic regulation–based programmable DNA motifs for biosensing and information encryption," *Sci. Adv.*, vol. 9, no. 20, p. eadf5868, 2023.

[11] M. Falih, A. Fadhil, M. Shakir, and B. T. Atiyah, "Exploring the potential of deep learning in smart grid: Addressing power load prediction and system fault diagnosis challenges," in *AIP Conf. Proc.*, vol. 3092, no. 1, AIP Publishing, 2024.

[12] Y. Liu *et al.*, "Deep learning for pixel-level image fusion: Recent advances and future prospects," *Inf. Fusion*, vol. 42, pp. 158-173, 2018.

[13] C. Tian *et al.*, "Deep learning on image denoising: An overview," *Neural Netw.*, vol. 131, pp. 251-275, 2020.

[14] T. Javid, M. K. Gupta, and A. Gupta, "A hybrid-security model for privacy-enhanced distributed data mining," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 6, pp. 3602-3614, 2022.

[15] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727-752, 2010.

[16] N. Khalil, A. Sarhan, and M. A. Alshewimy, "A secure image steganography based on LSB technique and 2D chaotic maps," *Comput. Electr. Eng.*, vol. 119, p. 109566, 2024.

[17] G. Shidaganti, V. L. Manoj, M. Vinay, and P. Patil, "Enhancing data protection using cryptography and image steganography in cloud environment," in *Proc. 5th Int. Conf. Circuits, Control, Commun. Comput. (I4C)*, 2024, pp. 93-99.

[18] A. K. Bharatwaj and A. R. Hasabnis, "Steganography in the quantum era," in *Proc. Int. Conf. Emerg. Smart Comput. Informatics (ESCI)*, 2024, pp. 1-5.

[19] K. Challita and H. Farhat, "Combining steganography and cryptography: new directions," *Int. J. New Comput. Archit. Appl. (IJNCAA)*, vol. 1, no. 1, pp. 199-208, 2011.

[20] K. N. Jassim *et al.*, "Hybrid cryptography and steganography method to embed encrypted text message within image," in *J. Phys.: Conf. Ser.*, vol. 1339, no. 1, p. 012061, IOP Publishing, 2019.

[21] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, "CNN-based adversarial embedding for image steganography," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2074-2087, 2019.