SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V12I8P103

Volume 12 Issue 8, 21-26, August 2025

Original Article

Encryption and Decryption Images by Neural Network Algorithms

AliAkbar Ridha Hussein[1], Ismael Hadi Challoob[2], Hayfaa Abdulzahra Atee[3]

[1,2]*Information Technology Department, Technical College of Management, Middle Technical University (MTU), Baghdad, Iraq.*
[3]*Computer Systems Department, Institute of Administration Rusafa, Middle Technical University (MTU), Baghdad, Iraq.*

[1]*Corresponding Author : dac2009@mtu.edu.iq*

Received: 11 June 2025 Revised: 18 July 2025 Accepted: 05 August 2025 Published: 28 August 2025

Abstract *- The field of digital document protection has witnessed increasing interest due to the significant expansion of its use, which has necessitated the proposal of numerous encryption techniques to enhance security, quality, and efficiency. In this study, three different encryption techniques were compared to determine the most appropriate in terms of overall performance. The study included five types of digital documents in various formats: JPEG, PNG, BMP, TIFF, and PDF. The number of documents in each category was 3,000, with a total of 15,000 digital documents. The research focused on three main evaluation criteria: quality, security, and the time required for the encryption and decryption processes. The results showed that the best techniques in terms of quality (i.e., the Lowest Mean Squared Error (MSE)) were: Vector Quantization (VQ), Visual Cryptography (VC), and Mirror-like Image Encryption (MIE). These techniques outperformed each other in preserving image resolution after decryption. In terms of security and speed, Double Random Phase Encoding (DRPE) technology ranked first, recording the highest mean square error of 24365507, indicating the difficulty of recovering the original data if compromised. The shortest execution time was only 0.009612 seconds. Research also revealed that the type of digital document (extension) directly impacted the results, with PDF showing the fastest encryption and decryption time compared to other formats. These results support the importance of choosing the appropriate technology based on the type of document and the purpose of encryption-whether to ensure quality, achieve security, or save time-which enhances organizations' ability to protect their digital data more efficiently and effectively.*

Keywords *- Digital Document Encryption, Neural Networks, Image Security, Encryption Performance Evaluation, File Format Impact, DRPE and VQ Techniques, Mean Squared Error.*

1. Introduction

In light of the rapid global digital transformation, digital documents have become a cornerstone of storage, messaging, and archiving across various government and private sectors. Despite significant advancements in digital image encryption techniques, the majority of current research primarily focuses on offline encryption. In such contexts, data transmission is confined to closed devices or networks, substantially mitigating the risk of unauthorized access. However, this focus does not reflect the practical realities of modern usage, where transmitting images over the internet has become indispensable for daily applications such as telemedicine, e-commerce, and sensitive governmental and military communications. The critical research gap, therefore, lies in the absence of robust and optimized encryption technologies specifically designed to secure images during in-transit phases across public networks. This deficiency exposes individuals and organizations to severe security risks. Consequently, this research aims to address this gap by proposing a novel framework for image encryption that ensures confidentiality, integrity, and reliability during transmission over the internet. This significant expansion in the use of digital documents has been accompanied by growing concerns about protecting them from tampering, hacking, or loss. This has highlighted the importance of adopting effective encryption technologies that ensure high levels of security, quality, and speed in handling this data. The urgent need for these technologies stems from digital documents often containing sensitive or confidential information, making their protection a top priority for organizations.

Accordingly, many different encryption methods have emerged, and numerous studies have been conducted to evaluate their efficiency and suitability for various types of digital documents. This study represents a systematic attempt to compare three of the most prominent encryption technologies against objective criteria, including quality, security, and speed, while considering the document's type and extent. The study seeks to provide accurate indicators that help in selecting the most appropriate encryption technology based on the nature of use and the needs of organizations, thus contributing to improving the efficiency of digital data protection systems in general.

In this field, many research studies have been done. Zhenlong proposed a dual image encryption algorithm based on Convolutional Neural Networks (CNNs) and dynamic adaptive scattering to achieve secure image transmission. The proposed method features a dual-channel (digital/optical) image encryption design, which enhances encryption efficiency and reduces the possibility of attack. The values of the two-dimensional chaotic system are controlled using a chaotic map to improve key security. Chaotic sequences are also used as convolution templates to link the plaintext and encryption steps. The methodology involves image embedding, segmentation, and two-channel encryption to achieve a balance between efficiency and security, and the results have proven effective [1].

The robustness of image encryption remains a major challenge in the field of image security, given the sensitivity and density of information represented by pixels. So many methods suffer from only partial data encryption. Key challenges include computational complexity, information loss during encryption, limited applicability, and scalability. Therefore, Panigrahy proposed an advanced dynamic technique to enhance cryptographic security using Artificial Neural Networks (ANNs).

The methodology consists of two levels: the first involves confusion and pixel swapping, and the second involves propagation using the XOR operation. An ANN model is trained using the encrypted image, and the resulting values are used to perform final neural network-based encryption, making it difficult for an attacker to access the data without knowing the adaptive weights and iterations. The results demonstrate that the proposed system offers high performance against various attacks, outperforming traditional methods in terms of processing time and Structural Similarity Index (SSIM) [2].

Multi-image optical encryption technology is very important in the field of information security, making multi-image optical encryption systems a major research focus. However, increasing information density leads to problems such as image interference and channel noise, which negatively impact system stability, reliability, and capacity. Xi, Sixing proposed three multi-image optical encryption systems to address these challenges based on random phase and amplitude mixing as keys, with wavelength, position, and angle as multi-image encryption mechanisms.

The study presents an innovative neural network-based framework to improve noise removal and increase capacity. This framework includes three key features: a cooperative architecture between optical encryption and deep learning, an adaptive threshold adjustment module, and a multi-mode network capable of adapting to different multi-image systems. The results demonstrate that the proposed approach maintains image fidelity and supports significant capacity increases compared to traditional methods [3].

This study included encrypting a large number of images divided into groups according to image type. Encryption included (JPEG, PNG, BMP, TIFF, and PDF) and neural networks were used to identify the original image, the encrypted image, and the image that was re-obtained after encryption. A comparative analysis of the results of this study with previous research demonstrates a clear superiority on multiple levels. The proposed algorithm achieved shorter encryption time while maintaining higher quality of the reconstructed images and ensuring a higher level of security for the encrypted images. Moreover, the results recorded a lower Mean Squared Error (MSE) after decryption compared to prior studies, whereas a higher MSE value was observed during the encryption phase. This highlights the efficiency of the current methodology in minimizing distortions and ensuring the reliability of the restored images.

2. Research Problem

Organizations increasingly rely on digital documents, and securing these documents has become necessary in light of increasing security threats. Despite the availability of numerous encryption technologies, determining the most appropriate technology in terms of quality, security, and speed remains a challenge, especially when file types or extensions vary. Thus, the problem is keeping digital documents safe and unhackable.

3. Research Significance

The importance of this research stems from its contribution to bridging the knowledge gap related to evaluating and comparing the effectiveness of digital image and document encryption technologies using real data from an official institution. The results also help government and private entities make scientifically based decisions to select the most efficient and appropriate encryption technologies for their digital environment.

4. Research Objective

This research aims to evaluate and compare three different digital document encryption technologies in terms of quality, security, and time required, while studying the impact of document extension type (JPEG, PNG, BMP, TIFF, PDF) on performance results. The goal is to determine the best encryption technology that meets security, accuracy, and speed requirements.

5. Encryption/Decryption Methods

5.1. Vector Quantization (VQ)

It is a technique used for data compression and image encryption. It divides data (such as images) into small blocks (vectors) and then represents each block with its closest representation from a set of templates known as a codebook. The same principle can be used in encryption: each part of the original image is represented by an indirect code that is difficult to interpret without access to the dictionary, making it

suitable for encryption. The VQ Algorithm can be done by the following steps [4].

5.1.1. Dividing the Image

The image is divided into fixed-sized blocks (vectors). Each block is treated as a vector in a multidimensional space. Let the original image be :

$$I \in \mathbb{R}^{M \times N} \quad (1)$$

Divide it into fixed-size blocks of $n \times n$

The total number of blocks is:

$$T = \frac{M \cdot N}{n^2} \quad (2)$$

Each block x_i is represented as a vector of dimension

$$d = n^2 \quad (3)$$

$$x_i \in \mathbb{R}^d, \quad i = 1,2,\ldots,T$$

5.1.2. Creating a Codebook

An algorithm (such as the LBG algorithm) is trained to generate a set of templates representing the most frequently occurring blocks in the image. These templates are numbered with unique indexes. A codebook C with K codewords (templates) is generated:

$$C = \{c_1, c_2, \ldots, c_K\}, \quad c_j \in \mathbb{R}^d \quad (4)$$

The codebook is trained using the LBG or K-means algorithm to minimize the total quantization error:

$$\min_C \sum_{i=1}^{T} \min_j \| x_i - c_j \|^2 \quad (5)$$

5.1.3. Encoding

The closest template from the dictionary is searched for each block in the image. The block is replaced with the template index, resulting in an encrypted image consisting of only symbols. The codebook is considered the encryption key. For each input vector x_i, the closest codeword is c_j :

$$\text{index}(x_i) = \arg \min_{j \in \{1,\ldots,K\}} \| x_i - c_j \|^2 \quad (6)$$

Then, only the index of the code word is stored. The encrypted (compressed) image is represented as:

$$I_{enc} = \{\text{index}(x_1), \text{index}(x_2), \ldots, \text{index}(x_T)\} \quad (7)$$

5.1.4. Decoding

Using the dictionary, each symbol (index) is replaced with the original block it represents from the dictionary. The image is reassembled from these blocks. Each vector is reconstructed from its index using the codebook:

$$\hat{x}_i = c_{\text{index}(x_i)} \quad (8)$$

The decoded image is reconstructed by merging all the recovered blocks:

$$\hat{I} = \text{Reconstruct}(\{\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_T\}) \quad (9)$$

5.1.5. Performance Evaluation

Mean Squared Error (MSE) is used to evaluate the model performance by following this equation :

$$\text{MSE} = \frac{1}{M \cdot N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(I(i,j) - \hat{I}(i,j)\right)^2 \quad \ldots \quad (10)$$

5.2. Optical Cryptography (VC)

It is an encryption technique that divides the original image into multiple parts, known as "shares", so no single share can reveal any information from the original image. However, when a sufficient number of shares (usually two or more) are overlaid, the original image is visually revealed without the need for any mathematical operations or digital keys. This technique was invented by Naor and Shamir in 1994 and is commonly used to encrypt images, signatures, and sensitive forms. This algorithm can be done by the following steps [5].

5.2.1. Input

A binary (black and white) or grayscale image. Each pixel is converted to a set of pixels in each slice (usually 2x2 or 1x2), as:

$$I = \{p_1, p_2, \ldots, p_n\}, \quad p_i \in \{0,1\} \quad \ldots \quad (11)$$

$p_i = 0$: white pixel

$p_i = 1$: black pixel

5.2.2. Create Shares

Each pixel in the original image is converted to a pattern defined in each slice based on its value (black or white). If the pixel is white, a symmetrical pattern is chosen across the slices (appearing transparent when overlaid). If the pixel is black, a complementary (asymmetrical) pattern that appears black when overlaid is chosen. Two shares were generated. S_1 and S_2 using different patterns depending on the pixel value p_i:

$$(S_1^i, S_2^i) = \begin{cases} \text{RandomPair}(P_0), & \text{if } p_i = 0 \text{ (white pixel)} \\ \text{RandomPair}(P_1), & \text{if } p_i = 1 \text{ (black pixel)} \end{cases} \quad (12)$$

Where:

P_0: the set of identical patterns for white pixels (resulting in a transparent overlay)

P_1: the set of complementary patterns for black pixels (resulting in a dark overlay)

5.2.3. Overlaying the Shares

The mathematical model for overlaying (combining) the two shares per pixel is:

$$O^i = S_1^i \vee S_2^i \tag{13}$$

∨: bitwise logical OR operation per pixel

The resulting overlay O^i Gives:

$$O^i = \begin{cases} [1,0] \vee [1,0] = [1,0], & \text{(white pixel appears light)} \\ [1,0] \vee [0,1] = [1,1], & \text{(black pixel appears dark)} \end{cases} \tag{14}$$

5.2.4. Reconstructing the Image

The visually decoded image is obtained by overlaying all corresponding pixel pairs:

$$\hat{I} = \bigcup_{i=1}^{n} O^i \tag{15}$$

Note: The overlay is visual and requires no computation; it just requires stacking transparencies or digital image blending.

5.2.5. Security Analysis

Perfect secrecy is achieved because no single share reveals any information:

$$\Pr(S_1^i | p_i = 0) = \Pr\left(S_1^i \middle| p_i = 1\right) \tag{16}$$

That is, the distribution of patterns in each share is statistically independent of the original pixel value, ensuring information-theoretic security.

5.3. Mirror-Like Image Encryption (MIE)

It is a method that relies on geometric transformations (symmetry, reflection, and rotation) to encrypt images. The idea is to rearrange the pixel positions in the original image in such a way that the resulting image is visually incomprehensible unless the opposite operations (reversing the transformations) are applied to restore the original shape. This method is similar to looking at an image through a mirror, but with a more complex and encrypted approach, making it both more secure and easier to implement [6]. The algorithm can be done using the following steps:

5.3.1. Input the Original Image

Assume the original grayscale or color image is:

$$I \in \mathbb{R}^{M \times N} \tag{17}$$

5.3.2. Apply Mirror Reflection Operations

Choose one or more of the following reflection types:

Horizontal Flip:

$$I_{\text{flipH}}(i,j) = I(i, N - j + 1) \tag{18}$$

Vertical Flip:

$$I_{\text{flipV}}(i,j) = I(M - i + 1, j) \tag{19}$$

Diagonal Flip:

$$I_{\text{flipD}}(i,j) = I(j,i) \tag{20}$$

5.3.3. Optional Rotation

For example, 90-degree clockwise rotation:

$$I_{\text{rot}}(i,j) = I(N - j + 1, i) \tag{21}$$

5.3.4. Divide Image into Blocks and Shuffle

Divide the image into non-overlapping blocks of size $B \times B$, then rearrange the blocks using a secret key-based permutation:

$$I_{\text{enc}} = \text{PermuteBlocks}(I_{\text{transformed}}, \text{Key}) \tag{22}$$

5.3.5. Output the Encrypted Image

The final encrypted image after applying all transformations is:

$$I_{\text{encrypted}} = \text{Shuffle}(\text{Rotate}(\text{Flip}(I))) \tag{23}$$

5.3.6. Decryption Process

To recover the original image, apply the inverse of each transformation in reverse order:

$$I = \text{InverseFlip}(\text{InverseRotate}(\text{InversePermute}(I_{\text{encrypted}}(24)$$

Or generally:

$$I = T_1^{-1}(T_2^{-1}(\cdots T_k^{-1}(I_{\text{enc}} \cdots)) \tag{25}$$

Where $T_1, T_2, \ldots, T_k$ Are the applied transformations.

5.3.7. Mathematical Representation

Let the sequence of transformations be T = {T_1, T_2, ….T_k} , then:

$$I_{\text{enc}} = T_k(\cdots T_2(T_1(I)) \cdots) \tag{26}$$

$$I = T_1^{-1}(T_2^{-1}(\cdots T_k^{-1}(I_{\text{enc}}) \cdots)) \tag{27}$$

6. Data Set

The data set included five types of digital documents in various formats: JPEG, PNG, BMP, TIFF, and PDF. The number of documents in each category was 3,000, with a total of 15,000 digital documents. The following figure represents a sample of a data set.

Fig. 1 A sample of data set images

7. Results

The following tables and figures represent the experimental results.

Table 1. Time for encryption and decryption by VQ technology

Image-kind	Encryption time/sec	Decryption time/sec	Total time/sec
BMP	0.037433	0.000077	0.368492
JPEG	0.092907	0.000214	0.111889
PNG	0.040576	0.001330	0.198142
PDF	0.000900	0.000404	0.051684
TIFF	0.036329	0.000080	0.557583

These results noted that the shortest encryption time was 0.000900 seconds for a PDF document, and the shortest decryption time was 0.000077 seconds for a BMP document. The shortest total time required to perform this process was 0.051684 seconds for a PDF document.

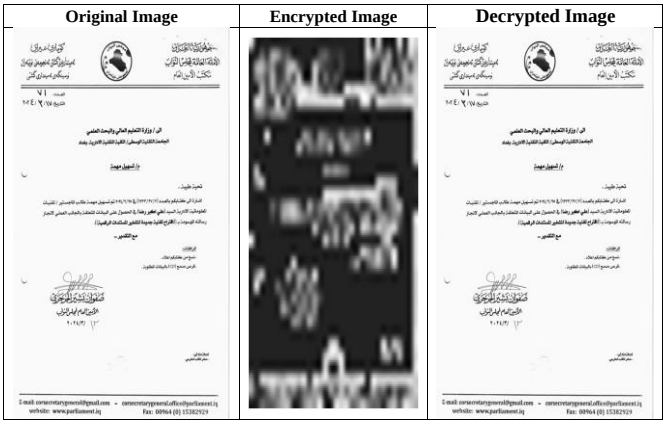

Fig. 2 Original vs Encrypted and decrypted image for VQ

Results of the VQ technique on the selected set of documents for encryption showed that the lowest Mean Square Error (MSE) was (10304.306210164) for TIFF images, the highest Mean Square Error (MSE) was (243492992.11419) for BMP images, and the average Mean Square Error (MSE) was (48707022.71). Regarding the digital documents recovered after decryption, the lowest Mean Square Error (MSE) was (7.30E-32) for BMP images, the highest Mean Square Error (MSE) was (0.000245071282106744) for TIFF images, and the average Mean Square Error (MSE) was (0.000187105).

Table 2. Time for encryption and decryption by VC technology

Image-kind	Encryption time/sec	Decryption time/sec	Total time/sec
BMP	0.000496	0.000496	0.303570
JPEG	0.000545	0.000545	0.087667
PNG	0.000565	0.000565	0.124239
PDF	0.001385	0.001385	0.010752
TIFF	0.000516	0.000516	0.384302

The results of the VC technique noted that the shortest encryption time was 0.000496 seconds for a BMP document, and the shortest decryption time was 0.000496 seconds for a BMP document. The shortest total time required to perform this process was (0.010752) seconds for a PDF document.

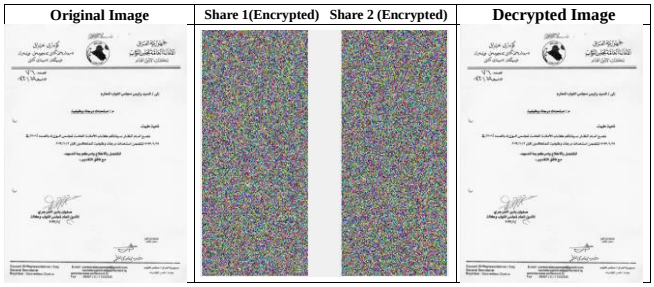

Fig. 3 Original vs Encrypted and decrypted image for VC

Results of the VC technique on the selected set of documents for encryption showed that the lowest Mean Squared Error (MSE) was (19542.2795944417) for JPEG images, the highest Mean Squared Error (MSE) was (19566.8140892605) for PNG images, and the average Mean Squared Error (MSE) was (19553.7984). As for the digital documents recovered after decryption, the lowest Mean Squared Error (MSE) was (0) for all image kinds.

Table 3. Time for encryption and decryption by MIE technology

Image-kind	Encryption time/sec	Decryption time/sec	Total time/sec
BMP	0.000094	0.0000680	0.389684
JPEG	0.000075	0.0000600	0.099407
PNG	0.000119	0.0000883	0.355758
PDF	0.000060	0.0000527	0.009874
TIFF	0.000054	0.0000467	0.373201

The results of the MIE technique noted that the shortest encryption time was (0.000054) seconds for a TIFF document, and the shortest decryption time was (0.0000467 seconds for a TIFF document. The shortest total time required to perform this process was (0.009874) seconds for a PDF document.

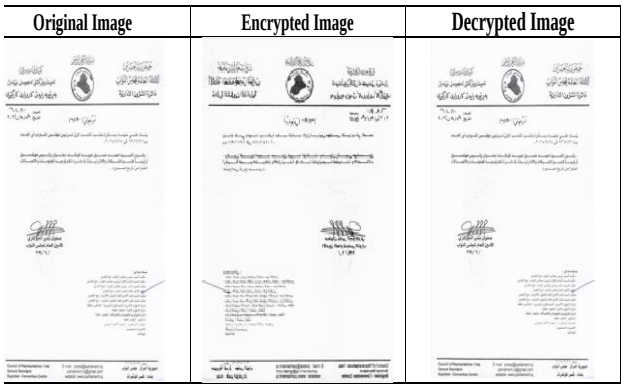

Fig. 4 Original vs Encrypted and decrypted image for MIE

Results also showed that the lowest Mean Squared Error (MSE) was (0.0442154818194862) for PDF images, the highest Mean Squared Error (MSE) was (0.0486514125709676) for TIFF images, and the average Mean Squared Error (MSE) was (0.047262188). As for the digital documents recovered after decryption, the lowest Mean Squared Error (MSE) was (0) for all image kinds.

8. Conclusion and Suggestions

The results demonstrated the methods' ability to encrypt and re-encrypt images at high speed, with high security and accuracy. The results also showed that the method is affected by the type of image and that the best type used for encryption is PDF.

The effect of the encryption method on both the image size and the content of the image can be investigated. The effect of the encryption process on image denoising and image zooming can also be investigated.

Acknowledgement

Thanks to the esteemed Iraqi Council of Representatives administration for providing various images for scientific research purposes.

Conflict of Interest

The authors affirm that there is no conflict of interest related to the content of this article.

Funding

The study was carried out independently and without financial assistance from any funding agency.

References

[1] Abrar Haider, and Andy Koronios, "Promises of Open Source Software for Australian Government Agencies-An Exploratory Study," *PACIS 2009 Proceedings*, 2009. [Google Scholar] [Publisher Link]

[2] Asisa Kumar Panigrahy et al., "A Faster and Robust Artificial Neural Network based Image Encryption Technique with Improved SSIM," *IEEE Access*, vol. 12, pp. 10818-10833, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Sixing Xi et al., "Neural Network-based Denoising and Capacity Enhancement Techniques for Optical Multi-image Encryption Systems," *Engineering Research Express*, vol. 7, no. 2, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Juncan Deng et al., "ViM-VQ: Efficient Post-Training Vector Quantization for Visual Mamba," *arXiv Preprint*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Xuan Yu, Julang Chen, and Xiaogang Wang, "Optical Cryptography based on Computational Ghost Imaging and Computer-Generated Holography," *Optics and Lasers in Engineering*, vol. 186, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] Michael D. Singh et al., "Reflection Mode Polarimetry Guides Laser Mass Spectrometry to Diagnostically Important Regions of Human Breast Cancer Tissue," *Scientific Reports*, vol. 14, 2024. [CrossRef] [Google Scholar] [Publisher Link]