International Journal of Applied Mathematics and Computing
E-ISSN: 3047-146X
P-ISSN: 3048-1988
IJAMC

Research Article

Implementation of Personal Data Security Using Advanced Encryption Standard (AES) Encrypted QR Codes on Digital Images Processed by the Discrete Cosine Transform (DCT) Method

Dadang Iskandar Mulyana[1*], Sopan Adrianto[2], Sugiyono[3], Muflikhan Dimas Dwiprayogi[4]

[1]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: dadang@stikomcki.ac.id
[2]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: sopan@stikomcki.ac.id
[3]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: sugiyono@stikomcki.ac.id
[4]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: muflikhanofficial@gmail.com
*Corresponding Author: dadang@stikomcki.ac.id

Abstract: The dissemination of personal data through digital media has increased significantly alongside the growing use of Quick Response (QR) Codes for various purposes, such as electronic tickets, certificates, and digital identities. Conventional QR Codes are open and can be easily scanned, copied, or manipulated by unauthorized parties. The personal data referred to in this study includes sensitive information such as full name, identity number (NIK/National ID), date of birth, address, phone number, and email address. This research proposes a layered security system that combines the Advanced Encryption Standard (AES) cryptographic algorithm with steganography using the Discrete Cosine Transform (DCT) method. The process begins with encrypting personal data using AES, converting the encrypted result into a QR Code, and embedding the QR Code into a digital image using DCT, hiding it in the image's frequency domain. The digital images used are of fixed size and formats that preserve visual quality. System evaluation is carried out by testing the visual quality of the stego image, the success rate of QR Code extraction, and the integrity of the encrypted data. The results are expected to conceal sensitive information visually while maintaining its confidentiality, with potential applications in electronic ID cards, digital certificates, e-tickets, and other confidential documents.

Keywords: AES Cryptography; Discrete Cosine Transform; Personal Data Security; QR Code; Steganography.

Received: 22 February 2025
Revised: 12 March 2025
Accepted: 14 April 2025
Published: 30 April 2025
Curr. Ver.: 30 April 2025

1. Introduction

The development of information technology in the digital era has facilitated the online exchange of personal data for administrative purposes, healthcare services, and financial transactions. Such personal data include sensitive information such as full names, identification numbers (NIK/ID card numbers), dates of birth, addresses, medical histories, and financial information. However, this convenience is accompanied by increasing security risks, as many data storage and exchange systems are not yet equipped with adequate protection mechanisms. As a result, data become vulnerable to theft, forgery, and misuse by unauthorized parties. One of the most popular media for storing and distributing data is the Quick Response (QR) Code due to its ability to contain information in a compact and easily

accessible format. Nevertheless, conventional QR Codes have a fundamental weakness: the stored data can be accessed by anyone once the code is scanned. Several previous studies have proposed the use of cryptographic algorithms such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC) to secure the contents of QR Codes. However, these approaches have not fully addressed the issue that QR Codes can still be easily recognized and visually analyzed. Therefore, a layered security approach is required that not only encrypts the data within the QR Code but also conceals it using steganographic techniques. One effective method is embedding QR Codes into digital images using the Discrete Cosine Transform (DCT). This method utilizes the image frequency domain, allowing the QR Code to remain visually imperceptible while still being extracted with high accuracy. This approach is expected to enhance the security and confidentiality of personal data in various digital applications, such as electronic identity cards, digital certificates, e-tickets, and other confidential documents.

In the increasingly advanced digital era, Quick Response (QR) Codes have become a popular medium for data storage and exchange due to their compactness, practicality, and ease of access. QR Codes are frequently used to store personal data such as full names, identification numbers (NIK), dates of birth, addresses, phone numbers, email addresses, and even sensitive information such as medical records and financial details. Despite their benefits, several security issues need to be addressed, including: 1) Data stored in QR Codes can be directly accessed by anyone simply by scanning them with common devices such as smartphones, without requiring additional authorization or authentication. 2) The distinctive and easily recognizable appearance of QR Codes makes them vulnerable to copying, duplication, or modification by irresponsible parties. 3) If only encryption is applied, although the data are protected, the QR Code remains visually apparent and may become a target for analysis and attacks. If only steganography is applied, although the data are hidden, once successfully extracted, the information can be read directly without any additional layer of protection.

Based on the identified problems described previously, this study focuses on improving the security of personal data stored in the form of Quick Response (QR) Codes. The personal data include sensitive information such as full names, identification numbers (NIK/ID card numbers), dates of birth, addresses, phone numbers, email addresses, medical record data, and financial information. The main problems formulated in this study are as follows: 1) How to design a security mechanism so that personal data within a QR Code cannot be accessed by unauthorized parties, even if the QR Code is obtained or scanned. 2) How to conceal an encrypted QR Code so that it is not explicitly visible, thereby preventing copying, duplication, and misuse by irresponsible parties. 3) How to integrate the Advanced Encryption Standard (AES) cryptographic algorithm with Discrete Cosine Transform (DCT)-based steganographic techniques to effectively embed QR Codes into digital images, thereby producing a layered security system that optimally preserves the confidentiality and integrity of personal data.

This study provides an original contribution to the field of digital data security by proposing a combined approach that integrates cryptographic and steganographic methods specifically focused on protecting personal data. The primary contribution of this research lies in the integration of QR Codes encrypted using the AES algorithm with their embedding into digital images through the Discrete Cosine Transform (DCT) method. Unlike previous studies that generally employed either QR Code encryption or image steganography separately, this research combines both approaches into a unified system to create a dual-layer security mechanism. Personal data originally in text form are encrypted using AES, then converted into a QR Code, and subsequently embedded into a digital image using DCT transformation so that the QR Code is not explicitly visible and becomes difficult to copy or manipulate.

This approach significantly enhances the level of security and confidentiality in digital data distribution because the concealed QR Code cannot be directly scanned by arbitrary individuals and can only be accessed when the embedding location and encryption key are known. Furthermore, the proposed system is efficient, lightweight, and suitable for implementation in various digital media such as electronic identity cards, digital certificates, electronic tickets, and other sensitive documents that are frequently exchanged online.

From an academic perspective, this study contributes to the literature in the field of information security by developing a layered protection system based on visual media. The system utilizes AES as a strong and fast encryption method, QR Codes as a compact data storage medium, and DCT as an effective steganographic technique in the frequency domain of digital images. Therefore, this research opens opportunities for the development of digital

privacy protection systems that are not only cryptographically secure but also visually concealed, thereby reducing the likelihood of data being intercepted, modified, or exploited by unauthorized parties.

2. Literature Review

Personal Data Security and QR Code Technology

The rapid advancement of information technology has significantly increased the volume of personal data exchanged through digital platforms. Personal data includes information that can directly or indirectly identify an individual, such as names, identification numbers, addresses, telephone numbers, biometric records, and other confidential information. The increasing use of digital services has simultaneously increased concerns regarding privacy protection and data security. Unauthorized access, identity theft, phishing attacks, and information leakage have become major threats to personal data management systems (Whitman & Mattord, 2018).

One technology that has experienced widespread adoption in digital information systems is the Quick Response (QR) Code. QR Codes are two-dimensional matrix barcodes capable of storing substantially more information than traditional barcodes while allowing rapid data retrieval through mobile devices and scanners. Due to their flexibility and ease of use, QR Codes have been widely implemented in electronic payments, digital identity systems, healthcare records, attendance management, ticket verification, logistics operations, and e-government services (Feng, 2021).

Despite their advantages, conventional QR Codes present significant security vulnerabilities. Information embedded within a QR Code can generally be accessed by any scanning application without requiring authentication or authorization. This characteristic makes QR Codes susceptible to data theft, unauthorized duplication, phishing attacks, and identity fraud. Subairu et al. (2021) highlighted that malicious QR Codes have increasingly been used as attack vectors to redirect users to fraudulent websites or distribute malware. Similarly, Feng (2021) reported that logistics systems utilizing unprotected QR Codes expose sensitive customer information such as names, addresses, and contact details to unauthorized parties.

Several studies have attempted to address these vulnerabilities. Pariddudin and Syauqi (2020) implemented AES encryption within QR Code-based ticket verification systems and demonstrated that encrypted QR Codes significantly reduce the risk of ticket duplication and identity manipulation. Dallal and Al Mukhtar (2023) proposed a multilayer encryption mechanism for personal information protection, where QR Code data undergoes multiple encryption stages before being distributed. Their findings indicated substantial improvements in confidentiality and resistance against unauthorized access.

Likewise, Nugraha and Barmawi (2024) introduced a QR Code security framework that combines Elliptic Curve Cryptography (ECC) and digital signatures to protect Indonesian identity card information. The study showed that integrating encryption with digital signature verification effectively enhances data authenticity and integrity. These findings suggest that QR Code technology alone is insufficient for protecting sensitive information and must be supplemented with additional security mechanisms.

Advanced Encryption Standard (AES)

Cryptography remains one of the most effective approaches for protecting digital information against unauthorized access. Among various cryptographic algorithms, the Advanced Encryption Standard (AES) has become the most widely adopted symmetric encryption standard worldwide. AES was selected by the National Institute of Standards and Technology (NIST) as the successor to the Data Encryption Standard (DES) due to its superior security, efficiency, and resistance to cryptanalytic attacks (Daemen & Rijmen, 2020).

AES operates by transforming plaintext into ciphertext using a secret encryption key. The algorithm supports key lengths of 128, 192, and 256 bits, providing different levels of security according to application requirements. The encryption process consists of multiple rounds involving substitution, permutation, mixing, and key addition operations. This structure creates a highly complex ciphertext that is computationally infeasible to reverse without the correct decryption key (Katz & Lindell, 2015).

The effectiveness of AES has been validated in numerous studies. Azhari et al. (2022) implemented AES to secure sensitive government documents and reported significant improvements in data confidentiality and protection against unauthorized modifications. Similarly, Iskandar et al. (2024) integrated AES encryption into a document protection

framework and demonstrated its capability to prevent unauthorized disclosure of confidential information.

In the context of QR Code security, Pariddudin and Syauqi (2020) showed that encrypting QR Code contents using AES effectively prevents unauthorized users from interpreting the encoded information. Harits et al. (2021) further compared AES with alternative cryptographic algorithms and concluded that AES provides a favorable balance between security strength and computational efficiency.

Although AES provides robust confidentiality protection, encrypted data remains visible and identifiable. Attackers may not be able to read the content but can still recognize the existence of protected information and potentially target it for future attacks. Therefore, additional mechanisms are required to conceal the presence of encrypted data itself.

Steganography as a Complementary Security Mechanism

While cryptography focuses on protecting the content of information, steganography aims to conceal the existence of the information. The term steganography originates from the Greek words steganos (hidden) and graphia (writing), referring to the practice of hiding messages within innocuous carrier media such as images, audio files, videos, or text documents (Taha et al., 2019).

The primary objective of steganography is to prevent observers from suspecting that secret communication is taking place. Unlike cryptography, which produces visibly encrypted data, steganography embeds information within digital media in such a way that the modifications are imperceptible to human observers. Consequently, steganography provides an additional layer of security by reducing the likelihood of detection.

Several studies have demonstrated the effectiveness of steganographic techniques. Al-Sanjary et al. (2020) developed a secure image communication system by combining AES encryption with Least Significant Bit (LSB) steganography. Their results indicated that the proposed method effectively concealed encrypted information while preserving image quality. Similarly, Abdulmaged and Abdulmaged (2023) introduced a genetic algorithm-based steganographic approach that optimizes data embedding locations, resulting in higher Peak Signal-to-Noise Ratio (PSNR) values and improved imperceptibility.

Research conducted by ALRikabi and Hazim (2021) further demonstrated that combining encryption and steganography significantly enhances communication security. Even if an attacker successfully identifies the existence of hidden data, the encrypted content remains inaccessible without the appropriate decryption key.

These findings indicate that steganography complements cryptography by providing covert communication capabilities, thereby reducing the risk of interception and detection.

Discrete Cosine Transform (DCT) for Secure Data Embedding

Steganographic techniques can generally be classified into spatial-domain and frequency-domain approaches. Spatial-domain methods directly modify pixel values and are relatively simple to implement; however, they are often vulnerable to image processing operations and steganalysis attacks. Frequency-domain methods, on the other hand, transform image data into frequency components before embedding hidden information, resulting in greater robustness and security (Shih, 2017).

One of the most widely used frequency-domain techniques is the Discrete Cosine Transform (DCT). DCT converts image information from the spatial domain into frequency coefficients that represent different levels of visual detail. By embedding secret information within selected frequency coefficients, DCT-based steganography can achieve high levels of imperceptibility while maintaining resistance against image compression and manipulation (Yahya, 2019).

The effectiveness of transform-domain approaches has been confirmed by several studies. Waqas et al. (2019) developed a QR Code watermarking framework based on wavelet transforms and chaotic maps, demonstrating strong robustness against image attacks and modifications. Similarly, Panna et al. (2018) employed frequency-domain transformations to enhance image encryption performance and achieved high entropy and resistance against differential attacks.

Compared with traditional LSB techniques, DCT-based methods provide superior protection against visual detection and statistical analysis. Therefore, DCT is considered an appropriate technique for embedding encrypted QR Codes within digital images while maintaining image quality and security.

Integration of AES, QR Code, and DCT-Based Steganography

Recent developments in information security increasingly emphasize multilayer protection mechanisms that combine several complementary techniques. Cryptography protects information content, QR Codes facilitate efficient data storage and distribution, while steganography conceals the existence of sensitive information within digital media.

Several researchers have explored hybrid approaches involving encryption and data hiding. Taha et al. (2019) concluded that combining cryptography and steganography offers substantially greater protection than either method alone. Rashmi and Jyothi (2018) similarly reported that integrating cryptographic algorithms with reversible data hiding techniques improves confidentiality, integrity, and resistance against unauthorized access.

However, most previous studies have focused either on encrypting QR Code contents or on hiding textual information within images. Limited research has investigated the integration of AES-encrypted QR Codes with DCT-based image steganography as a unified framework for protecting personal information. This limitation highlights an important research opportunity.

Accordingly, this study proposes a multilayer security architecture in which personal information is first encrypted using AES, converted into a QR Code representation, and subsequently embedded into a digital image using the Discrete Cosine Transform (DCT) method. The proposed approach is expected to provide stronger confidentiality, enhanced privacy protection, and greater resistance against unauthorized access and information disclosure.

3. Materials and Method

Research Design

This study employed an experimental approach to develop and evaluate a personal data security system by integrating Advanced Encryption Standard (AES), QR Code technology, and Discrete Cosine Transform (DCT)-based steganography. The proposed method applies multilayer protection in which personal information is first encrypted using AES, encoded into a QR Code, and subsequently embedded into a digital image using the DCT technique. The objective of this approach is to enhance confidentiality, prevent unauthorized access, and conceal the existence of sensitive information within digital media.

Research Data

The data used in this study consisted of simulated personal information represented as plaintext, including full name, national identification number (NIK), date of birth, address, and other sensitive attributes. The dataset was generated specifically for research purposes and did not contain real personal information. The use of simulated data ensured compliance with privacy and ethical considerations while maintaining realistic testing scenarios.

In addition to textual data, digital images were used as cover media for steganographic embedding. PNG image formats with fixed resolutions of 512 × 512 pixels and 1024 × 1024 pixels were selected to preserve image quality during the embedding and extraction processes. These images served as host media for storing encrypted QR Codes.

Proposed Security Framework

The proposed framework consists of three main stages: AES encryption, QR Code generation, and DCT-based embedding. The workflow is designed to provide layered protection for personal information.

AES Encryption

The first stage involves encrypting personal data using the Advanced Encryption Standard (AES). Plaintext data are transformed into ciphertext using a secret encryption key. AES was selected due to its strong security, computational efficiency, and widespread adoption in information security applications. The encryption process ensures that sensitive information cannot be interpreted without the corresponding decryption key.

QR Code Generation

The ciphertext generated by AES encryption is converted into a QR Code. Error correction levels are applied during QR Code generation to improve resilience against minor distortions that may occur during the embedding process. The resulting QR Code serves as a compact representation of the encrypted information and facilitates efficient storage within digital images.

DCT-Based QR Code Embedding

The generated QR Code is embedded into a digital image using the Discrete Cosine Transform (DCT) method. Initially, the cover image is transformed from the spatial domain into the frequency domain. Selected DCT coefficients are then modified to store QR Code information. After embedding, the inverse transformation is applied to reconstruct the stego-image. This approach minimizes visual distortion while maintaining the recoverability of the hidden QR Code.

The embedding process can be represented as follows:

1) Personal data → AES encryption → Ciphertext.
2) Ciphertext → QR Code generation.
3) Cover image → DCT transformation.
4) QR Code embedding into selected DCT coefficients.
5) Inverse DCT → Stego-image.

Extraction and Recovery Process

To recover the hidden information, the stego-image undergoes the reverse procedure. The image is transformed into the frequency domain using DCT, and the modified coefficients are analyzed to reconstruct the embedded QR Code. The extracted QR Code is then decoded to obtain the ciphertext. Finally, AES decryption is performed using the correct secret key to recover the original plaintext data. Successful recovery indicates that both confidentiality and data integrity have been preserved throughout the process.

Experimental Evaluation

The performance of the proposed system was evaluated through two testing scenarios.

Confidentiality Testing

This test evaluates whether encrypted personal data can be accessed without the correct AES key. Unauthorized decryption attempts are performed on the extracted ciphertext. The system is considered successful if the output remains unreadable and does not reveal meaningful information. This evaluation measures the effectiveness of AES encryption in protecting sensitive data.

Data Integrity Testing

The integrity test evaluates whether the recovered information is identical to the original plaintext before encryption. After extraction and decryption, the resulting data are compared with the original input. A successful test indicates that the QR Code embedding and extraction processes do not alter the encrypted content and that the complete security framework preserves information accuracy throughout transmission and storage.

4. Results and Discussion

Implementation and Testing

This section describes the implementation and testing stages of the embedding and extraction system for QR Codes that have been encrypted using the Advanced Encryption Standard (AES) algorithm into digital images using the Discrete Cosine Transform (DCT) method. The testing process was conducted to verify the success of the embedding procedure and the system's ability to recover encrypted data without altering its content, thereby ensuring compliance with the principle of data integrity.

Testing Environment

The experiments were conducted using the hardware and software environment described in Section 4.1. Specifically, the testing platform consisted of a Lenovo ThinkPad T430 laptop equipped with an Intel® Core™ i5-3320M processor running at 2.60 GHz, 12 GB DDR3 RAM, and a 240 GB SSD storage device. The operating system used was Linux Mint 21.3 (64-bit). Software development was carried out using Python version 3.10, supported by several libraries, including numpy, opencv-python, pycryptodome, qrcode, pyzbar, and scikit-image.

Test Data and Pre-processing

The test dataset consisted of three JPEG cover images with a resolution of 512 × 512 pixels, namely a horse image, a beach image, and a road image. Each image was used to embed personal information represented as plain text strings without additional metadata, simulating practical scenarios such as personal data protection in electronic documents. The personal information included sensitive attributes such as names, identification numbers, addresses, and contact information. Prior to embedding, the data were encrypted using the AES-128

algorithm operating in Cipher Block Chaining (CBC) mode with a randomly generated Initialization Vector (IV).

Testing Procedure

The testing procedure was carried out in two main stages, namely embedding and extraction:

a) Personal data were encrypted using AES-128-CBC with a random IV.
b) The encrypted output (ciphertext) was converted into a QR Code with a predefined size and error correction level.
c) The QR Code was embedded into the cover image through DCT transformation on the luminance (Y) component of the image.
d) The resulting embedded image (stego-image) was saved in PNG format.
e) During the extraction stage, the stego-image was processed to recover the embedded QR Code through inverse DCT transformation.
f) The extracted QR Code was scanned to retrieve the ciphertext.
g) The ciphertext was decrypted using the same parameters applied during the embedding stage, resulting in plaintext identical to the original input data.

Figure 1. Horse Image Encoding Process.

Figure 2. Horse Image Encoding Result.

Figure 3. Horse Stego Image.

Figure 4. QR Code Message.

Figure 5. Beach Image Encoding Process

Figure 6. Beach Image Encoding Result.

Figure 7. Beach Stego Image.

Figure 8. QR Code Message.

Figure 9. Road Image Encoding Process.

Figure 10. Road Image Encoding Result.

Figure 11. Road Stego Image.

Figure 12. QR Code Message.

Figure 13. Message Decoding Process.

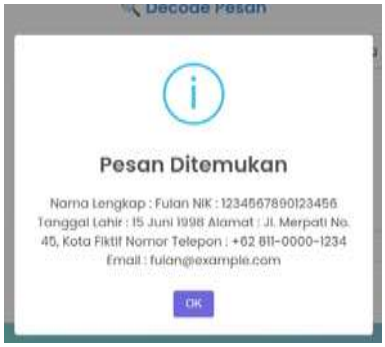

Figure 14. Extracted Message from Horse Image.

Figure 15. Beach Image Decoding Process.

Figure 16. Extracted Message from Beach Image.

Figure 17. Road Image Decoding Process.

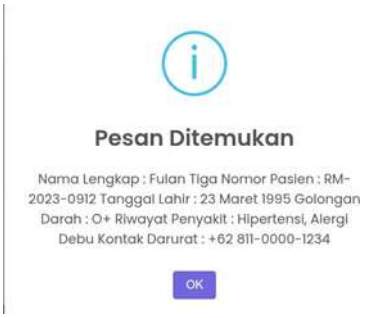

Figure 18. Extracted Message from Road Image.

Final Testing Results

The final testing results of the AES-encrypted QR Code embedding and extraction system implemented in digital images using the Discrete Cosine Transform (DCT) method indicate that the proposed approach successfully achieved the research objectives. All test scenarios employed QR Codes with dimensions of 770 × 770 pixels and a High (H) error correction level. Embedding was performed within the middle-frequency coefficients of the image while maintaining consistent AES-128-CBC encryption parameters throughout the experiments.

Embedding and Extraction Performance

All embedding processes successfully generated stego-images that were visually indistinguishable from the original cover images. No noticeable visual differences could be observed by the human eye without specialized analytical tools, indicating that modifications within the frequency domain did not affect image perception.

During the extraction phase, all embedded QR Codes were successfully recovered and scanned without any decoding errors. The ciphertext obtained from the extraction process was identical to the original encrypted ciphertext, with byte-by-byte comparisons showing a 100% match. Furthermore, the decrypted plaintext was identical to the original source data used before encryption.

Table 1. Testing Results.

No.	Cover Image	Resolution	QR Code Size	Error Correction	Scanning Status	Ciphertext Match
1	Horse.jpg	512 × 512	770 × 770	H	100% Readable	100% Identical
2	Beach.jpg	512 × 512	300 × 300	H	100% Readable	100% Identical
3	Road.jpg	512 × 512	770 × 770	H	100% Readable	100% Identical

5. Conclusion and Suggestion

Conclusion

Based on the results of the research and testing conducted on the personal data security system using the method of embedding AES-encrypted QR Codes into digital images using the Discrete Cosine Transform (DCT), several conclusions can be drawn as follows: 1) The developed system is capable of performing personal data encryption using the AES-128-CBC algorithm and converting the encrypted output into a QR Code, which is subsequently embedded into a digital image using the DCT method. 2) Embedding within the middle-frequency coefficients of the image in the DCT domain was proven to produce a stego-image that is visually identical to the original cover image, thereby satisfying the imperceptibility aspect. 3) The process of extracting the QR Code from the stego-image was successfully performed without any decoding errors. The extracted ciphertext was proven to be identical to the ciphertext generated during the initial encryption process, and after decryption, it produced the same plaintext as the original data, thus fully preserving data integrity. 4) Variations in the carrier image did not affect the success of either the embedding or extraction processes, demonstrating the flexibility of the method with respect to differences in image content.

Suggestions

For further development and future research, the following recommendations are proposed: 1) The use of stronger cryptographic algorithms. 2) Although AES-128 has met the security requirements of this study, the use of longer key lengths such as AES-192 or AES-256 may further enhance resistance against cryptographic attacks. Improving robustness against image modifications, the DCT method can be combined with error correction coding or spread spectrum techniques to increase resistance to compression, noise, and other forms of image manipulation. Testing on various image resolutions and formats, future studies may include experiments using images with higher resolutions or different formats such as PNG and BMP to evaluate their effects on visual quality and extraction performance.

References

Abdulmaged, S. M., & Abdulmaged, N. M. (2023). A new steganography technique based on genetic algorithm. *Global Journal of Engineering and Technology Advances, 16*(2), 123–131. https://doi.org/10.30574/gjeta.2023.16.2.0146

Aljazaery, I. A., Alrikabi, H. T. S., & Aziz, M. R. (2020). Combination of hiding and encryption for data security. *International Journal of Interactive Mobile Technologies, 14*(9). https://doi.org/10.3991/ijim.v14i09.14173

AlRikabi, H. T. S., & Hazim, H. T. (2021). Enhanced data security of communication system using combined encryption and steganography. *International Journal of Interactive Mobile Technologies, 15*(16). https://doi.org/10.3991/ijim.v15i16.24557

Al-Sanjary, O. I., Ibrahim, O. A., & Sathasivem, K. (2020). A new approach to optimum steganographic algorithm for secure image. In *Proceedings of the International Conference on Computing and Communication Systems*. https://doi.org/10.1109/I2CACIS49202.2020.9140186

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi pengamanan data pada dokumen menggunakan algoritma kriptografi Advanced Encryption Standard (AES). *Jurnal Pengabdian Sistem Komputer, 2*(1). https://doi.org/10.47709/jpsk.v2i1.1390

Cisneros, B., Ye, J., Park, C. H., & Kim, A. Y. (2021). CoviReader: Using IOTA and QR code technology to control epidemic diseases across the US. In *Proceedings of the IEEE Consumer Communications & Networking Conference*. https://doi.org/10.1109/CCWC51732.2021.9376093

Daemen, J., & Rijmen, V. (2020). *The design of Rijndael: The Advanced Encryption Standard (AES)* (2nd ed.). Springer. https://doi.org/10.1007/978-3-662-60769-5

Dallal, H. R. H. A., & Mukhtar, W. N. M. A. (2023). A QR code used for personal information based on multi-layer encryption system. *International Journal of Interactive Mobile Technologies, 17*(9). https://doi.org/10.3991/ijim.v17i09.38777

Feng, H. (2021). Application of QR code technology in the design of user information privacy protection logistics system. *International Journal of Frontiers in Engineering Technology, 3*(3). https://doi.org/10.25236/IJFET.2021.030302

Han, Q., Zhang, Y., & Li, H. (2018). Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things. *Future Generation Computer Systems, 92*, 1110–1119. https://doi.org/10.1016/j.future.2018.01.019

Irawan, A. I., Santoso, I. H., Istikmal, & Rahayu, M. (2022). Implementation of QR code attendance security system using RSA and hash algorithms. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*. https://doi.org/10.22146/jnteti.v13i1.4395

Iskandar, D. M., Nadip, M. Z., Dinilhaq, N., & Purnama, A. (2024). Penerapan kriptografi AES pada Fres-Caesas: Perlindungan pesan teks dan fail dokumen. *INTECOMS: Journal of Information Technology and Computer Science, 7*(3). https://doi.org/10.31539/intecoms.v7i3.9426

Katz, J., & Lindell, Y. (2015). *Introduction to modern cryptography* (2nd ed.). CRC Press. https://doi.org/10.1201/b17668

M, A. R. H., Ridwan, Hafidzin, A. P., & Taufik, M. (2021). Proteksi keamanan data pada Quick Response (QR) code. *Jurnal Teknik Rekayasa Multimedia, 3*(2). https://doi.org/10.48182/jtrm.v3i2.58

Mawla, N. A., & Khafaji, H. K. (2023). Enhancing data security: A cutting-edge approach utilizing protein chains in cryptography and steganography. *Computers, 12*(8), Article 166. https://doi.org/10.3390/computers12080166

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2019). *Handbook of applied cryptography* (Reprint ed.). CRC Press. https://doi.org/10.1201/9780429466335

N, M. R., & K, D. J. (2018). An improved method for reversible data hiding steganography combined with cryptography. In *Proceedings of the International Conference on Information Systems and Computing*. https://doi.org/10.1109/ICISC.2018.8398946

Naman, H. A., Hussien, N. A., Al-Dabag, M. L., & AlRikabi, H. T. S. (2021). Encryption system for hiding information based on Internet of Things. *International Journal of Interactive Mobile Technologies, 15*(2). https://doi.org/10.3991/ijim.v15i02.19869

Nugraha, R. A., & Barmawi, A. M. (2024). Securing KTP data using QR code modification and elliptic curve cryptography. *Indonesian Journal of Computing, 9*(1). https://doi.org/10.34818/INDOJC.2024.9.1.909

Panna, B., Kumar, S., & Jha, R. K. (2018). Image encryption based on block-wise fractional Fourier transform with wavelet transform. *Journal of Information and Optimization Sciences, 40*(2), 527–537. https://doi.org/10.1080/02564602.2018.1533892

Pariddudin, A., & Syauqi, F. (2020). Penerapan algoritma AES pada QR code untuk keamanan verifikasi tiket. *Jurnal Bisnis dan Sains*, *10*(2). https://doi.org/10.36350/jbs.v10i2.87

Shih, F. Y. (2017). *Digital watermarking and steganography: Fundamentals and techniques* (2nd ed.). CRC Press. https://doi.org/10.1201/9781315121109

Subairu, S., Alhassan, J., Abdulhamid, S., & Ojeniyi, J. (2021). A review of detection methodologies for Quick Response code phishing attacks. In *Proceedings of the International Conference on Computational Intelligence and Security*. https://doi.org/10.1109/ICCIS49240.2020.9257687

Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of steganography and cryptography: A short survey. *IOP Conference Series: Materials Science and Engineering, 518*(5), Article 052003. https://doi.org/10.1088/1757-899X/518/5/052003

Waqas, U. A., Khan, M., & Batool, S. I. (2019). A new watermarking scheme based on Daubechies wavelet and chaotic map for Quick Response code images. *Multimedia Tools and Applications, 79*, 1–23. https://doi.org/10.1007/s11042-019-08570-5

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6th ed.). Cengage Learning.

Xu, J., Wei, L., Wu, W., Wang, A., Zhang, Y., & Zhou, F. (2018). Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber-physical systems. *Future Generation Computer Systems, 89*, 327–338. https://doi.org/10.1016/j.future.2018.04.018

Xu, M., Lv, L., Zhang, J., Xu, M., Zhang, C., & Zhang, J. (2019). A new QR code multi-layer encryption system based on image geometric processing. In *Proceedings of the IEEE International Conference on Mechatronics and Automation*. https://doi.org/10.1109/ICMA.2019.8816462

Yahya, A. (2019). *Steganography techniques for digital images*. Springer. https://doi.org/10.1007/978-3-319-78597-4