Available online at https://journal.rescollacomm.com/index.php/ijqrm/index

International Journal of Quantitative Research and Modeling

e-ISSN 2721-477X
p-ISSN 2722-5046

Vol. 6, No. 3, pp. 334-344, 2025

Cryptographic Security for Double Encryption on Images Using AES and IDEA Algorithms

Nizar Septi Maulana[1*], Asep Id Hadiana[2], Melina[3]

[1,2,3] *Department of Informatics, Faculty of Science and Informatics, Universitas Jenderal Achmad Yani, Jl. Terusan Jend. Sudirman, Cimahi, West Java, 40525, Indonesia*
**Corresponding author email: nizarsepti21@if.unjani.ac.id*

Abstract

In the digital era, the security of electronic medical record images has become a primary concern due to the high risk of sensitive information leakage. This study investigates and develops the implementation of double encryption on medical image data by combining the Advanced Encryption Standard (AES) and International Data Encryption Algorithm (IDEA) to enhance image security, particularly for electronic medical record images that are vulnerable to information breaches. AES is utilized for its efficiency in encrypting large-sized data, while IDEA offers a complex key structure that provides stronger protection against unauthorized access. A dataset of Magnetic Resonance Imaging (MRI) images obtained from the public Kaggle platform was used as the test object for encryption and decryption processes. The evaluation was conducted using two main approaches: the avalanche effect test to measure the sensitivity of input changes to the ciphertext output, and the processing time test to assess encryption and decryption performance efficiency. The results show that the average avalanche effect value reached 49.97%, which is very close to the ideal 50%, indicating a high level of data diffusion and strong cryptographic strength. Meanwhile, the encryption time test on five image files revealed that the average time required to perform double encryption using AES and IDEA was 52.06 seconds, with a range between 42.0 seconds and 63.5 seconds, depending on the image size and complexity. Therefore, the combination of AES and IDEA has proven to enhance cryptographic strength without significantly compromising operational efficiency. This double encryption approach is considered feasible and effective for implementation in healthcare information systems, particularly to maintain the confidentiality, integrity, and authenticity of electronic medical record images.

Keywords: Dual encryption, AES, IDEA, avalanche effect, medical image security, processing time efficiency

1. Introduction

In the digital era, data security and privacy have become critical issues, particularly for sensitive information such as medical records in the form of digital images (Ayu Nur Oktaviani 2024). Healthcare organizations face approximately 43,000 attempted cyberattacks annually, with about 18% successfully breaching at least one layer of security (ShareFile 2024). Medical records often contain vital information such as radiology scans, MRI, CT scans, and other medical imaging results that must be protected from unauthorized access (Mahmoud Magdy & Neveen I. Ghali 2022). Since these records are stored and transmitted electronically, they are vulnerable to cybersecurity threats including data theft, unauthorized manipulation, and system breaches (Jihad Ramadhan 2025). The compromise of such sensitive data not only violates patient privacy but can also lead to fatal consequences such as misdiagnosis or malicious exploitation of patient information (Denghui Zhang 2023).

In recent years, the frequency and severity of cyberattacks targeting electronic medical record (EMR) systems have continued to increase. Notable incidents include the 2021 SingHealth data breach, where hackers accessed the EMR system of Singapore's largest healthcare provider and stole sensitive data from 1.5 million patients, including that of the Prime Minister (BBC News Indonesia 2021). Similarly, in the United States, a ransomware attack on Universal Health Services (UHS) disrupted operations across more than 250 hospitals, cutting off access to patient records and significantly hampering healthcare delivery (Jonathan Patrick | CNN Indonesia 2020). The second incident shows that the RME system is very vulnerable to cyber attacks that can disrupt the continuity of medical services and endanger patient safety, requiring the implementation of stronger protection methods, one of which is through cryptography (Dipti Kapoor Sarmah 2025). The word cryptography comes from Greek, where kryptos means hidden and graphia means writing. In other words, it refers to writing that is kept secret (Melina et al. 2024).

Various cryptographic algorithms have been developed to enhance data security, among which the Advanced Encryption Standard (AES) and the International Data Encryption Algorithm (IDEA) are widely recognized, previous studies implementing double encryption using AES and Rivest Code 5 (RC5) in military communication demonstrated the effectiveness of this approach in protecting digital images from unauthorized access (Galih 2022). Other research also highlighted the use of AES for securing image data in web-based services, showing that AES is highly effective in maintaining the confidentiality of visual data with efficient encryption time (Aulia 2023). On the other hand, IDEA offers distinct advantages, particularly its robustness against cryptanalysis. The application of IDEA in encrypting hidden messages within images using the End of File (EOF) steganography method has been proven to preserve image quality without altering the readability or structure of the original file, while effectively concealing the embedded message from external parties(Irawati et al. 2018). Furthermore, related studies have shown that IDEA outperforms DES and Triple DES in terms of processing speed and achieves decryption accuracy of up to 100% across various bitmap image sizes (Yosanny 2020).

Building upon these findings, this study implements a double encryption approach using AES and IDEA to enhance the security of electronic medical image records such as MRI and CT scans. AES is applied to ensure fast and efficient processing of large medical data, while IDEA strengthens the system with its complex key structure and cryptographic resilience. This layered encryption scheme is designed to improve confidentiality and prevent unauthorized access to sensitive medical data. Furthermore, the study evaluates the effectiveness of the proposed system by analyzing encryption and decryption processes, measuring performance based on processing time, and examining the Avalanche Effect as an indicator of encryption reliability.

2. Literature Review

2.1. Cryptography

Cryptography is a scientific discipline that studies mathematical methods used to ensure key aspects of information security, such as confidentiality, integrity, and authentication of both identity and data sources (Dzikri, 2024)Rather than serving as a single solution, cryptography comprises a collection of techniques that support the broader security system, cryptographic algorithms are commonly classified into two categories based on key usage symmetric and asymmetric algorithms, symmetric algorithms employ the same key for both encryption and decryption, while asymmetric algorithms use a pair of different keys—one public key for encryption and one private key for decryption (Febri Dwinata Yonathan 2021). In cryptography, there are several important terms such as plaintext, ciphertext, encryption and decryption processes, and cryptographic keys, where encryption is the technique or process of converting original text or data (plaintext) into an unreadable or incomprehensible form (ciphertext) using an encryption algorithm and an encryption key (cipherkey) with the aim of preventing unauthorized access or interpretation of transmitted or stored information, while decryption is the process of converting ciphertext back into plaintext so that the encrypted message or data is restored to its original form (Taris Monica, 2024).

2.2. Advanced Encryption Standard (AES)

The AES algorithm is a cryptographic method used to ensure data security, AES belongs to the class of symmetric block ciphers, functioning to perform encryption (transforming data into an unreadable form known as ciphertext) and decryption (restoring ciphertext back to its original form, or plaintext) (Meko 2018). The AES algorithm supports variable key lengths for the encryption and decryption processes, with key sizes of 128 bits, 192 bits, and 256 bits (Siswanto and Herwanto 2024).

1) Encryption Process

a. AddRoundKey
   The first stage is called the AddRoundKey round, which performs an XOR operation between the working state and the round key in each round (Prameshwari and Sastra 2018). This XOR process uses the RCON table to generate the first column in each round.
b. SubBytes
   The next stage is the SubBytes transformation, which performs a non-linear byte substitution (Prameshwari and Sastra 2018). This process replaces each byte in the state with the corresponding byte from the S-Box table, where S′[r, c] = xy represents the element in the S-Box.
c. ShiftRows
   After that, the ShiftRows operation rearranges the state matrix by performing a circular left shift for each row (Prameshwari and Sastra 2018). The shift is carried out by a certain number of positions.
d. MixColumns
   The MixColumns process transforms each column in the state into a new column using Galois Field Multiplication (Prameshwari and Sastra 2018). Then, the initial stage, AddRoundKey, starts again.

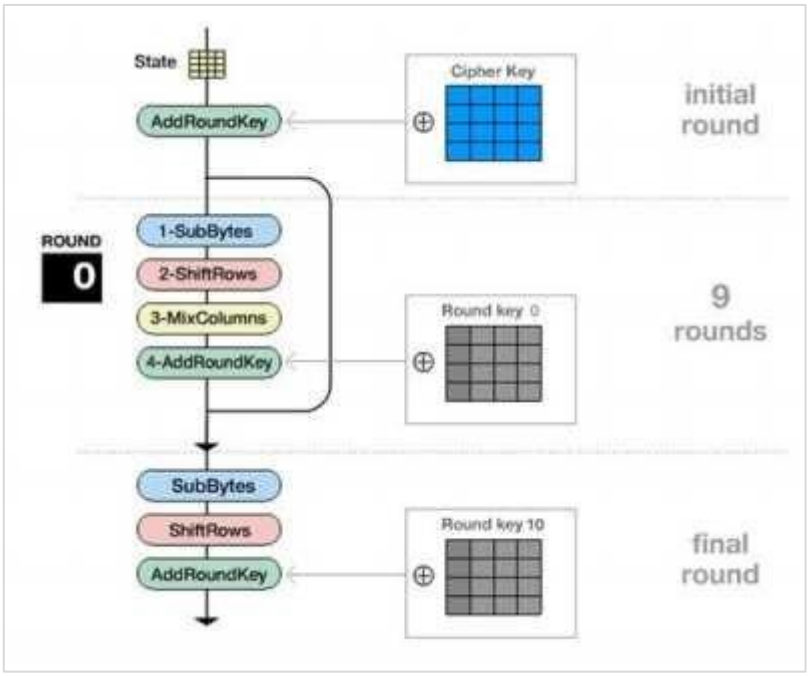

Figure 1: AES encryption process

2) Decryption Process

a. InvAddRoundKey
In this process, an XOR operation is performed between the bytes of the state matrix, consisting of the ciphertext, and the bytes of the previously generated round key.

b. nvShiftRows
This process is the inverse of the ShiftRows stage in encryption, where the rows of the state are shifted to the right by a certain number of positions.

c. InvSubBytes
This process is the reverse of SubBytes, where each byte in the state is transformed back using the Inverse S-Box.

d. InvMixColumns
The InvMixColumns process is the inverse of the MixColumns stage, where the columns of the state are restored using Inverse Galois Field Multiplication.

The visualization of the encryption and decryption transformation process is shown in Figure 2.2

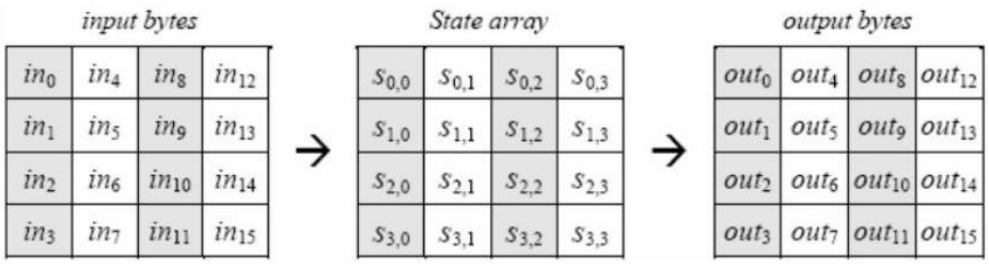

Figure 2: Process of Input Bytes, State Array, and Output Bytes

Based on Figure 2, the AES algorithm operates using a two-dimensional byte array structure known as the state. The size of the state is determined by the formula NROWS × NCOLS. Both encryption and decryption processes take place within this state array. At the initial stage, the input data is first inserted as input bytes and then copied into the state array. The transformations are performed within this array, and the final result is stored as output bytes.

After the initial AddRoundKey step, the state array undergoes a series of transformations repeatedly according to the number of rounds (Nr) defined in the AES algorithm. These transformations consist of SubBytes, ShiftRows, MixColumns, and AddRoundKey, collectively known as the round function in the AES encryption process. However, in the final round, the MixColumns transformation is omitted (Munir 2019).

2.3. International Data Encryption Algorithm (IDEA)

IDEA is a symmetric block-based cryptographic method designed to secure information by transforming it into an unreadable form during transmission over networks such as the Internet. This algorithm operates on 64-bit block sizes and utilizes a 128-bit key (Yosanny 2020). The encryption process involves eight full rounds and an additional half round, using six subkeys in each round and four additional subkeys in the final stage for output transformation (Yosanny 2020). The process in the IDEA algorithm consists of two main activities, namely encryption and decryption.

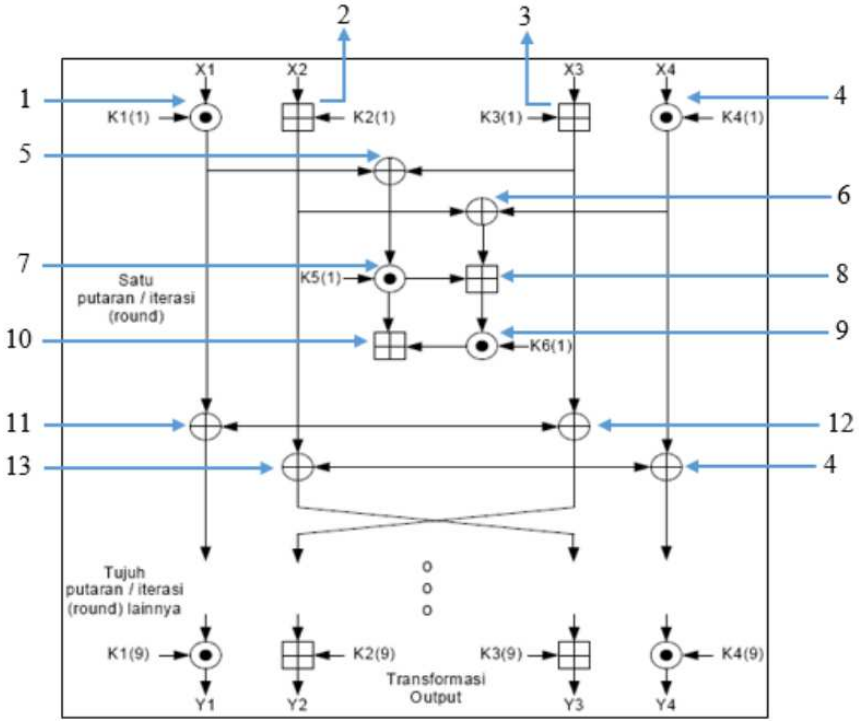

Figure 3: IDEA encryption proces

The encryption process can be seen in Figure 2.The IDEA encryption process begins with a 64-bit plaintext block by dividing it into four 16-bit subblocks: X1, X2, X3, and X4. These subblocks enter the first major iteration of eight rounds (rounds). In each round, the subblocks undergo modular addition, modular multiplication, and XOR operations with six 16-bit subkeys. Between certain steps, subblocks are exchanged to improve diffusion. After completing all rounds, a final transformation step is performed using four additional subkeys, resulting in the final 64-bit ciphertext block. The detailed steps of each iteration are as follows (Irawati et al. 2018):

1) Multiply **X1** by subkey **K1** modulo $(2^{16} + 1)$.
2) Add **X2** with subkey **K2** modulo 2^{16}.
3) Add **X3** with subkey **K3** modulo 2^{16}.
4) Multiply **X4** by subkey **K4** modulo $(2^{16} + 1)$.
5) XOR the results of steps 1 and 3.
6) XOR the results of steps 2 and 4.
7) Multiply the result of step 5 by subkey **K5** modulo $(2^{16} + 1)$.
8) Add the results of steps 6 and 7 modulo 2^{16}.
9) Multiply the result of step 8 by subkey **K6** modulo $(2^{16} + 1)$.
10) Add the results of steps 7 and 9 modulo 2^{16}.
11) XOR the result of step 1 with step 9.
12) XOR the result of step 3 with step 9.
13) XOR the result of step 2 with step 10.
14) XOR the result of step 4 with step 10.

After these transformations, the four sub-blocks are rearranged, and the process continues into the next round. Once all eight rounds are completed, the final output transformation is performed, where the four 16-bit sub-blocks are combined with four subkeys. This produces the final 64-bit encrypted ciphertext. Meanwhile, the decryption process consists of the following steps :

1) Matrix and Permutation Inversion: All encryption operations are reversed during decryption, including matrix and permutation inversions.
2) Inverse Byte Substitution: The byte substitution process is reversed using the inverse substitution tables.
3) Addition and XOR Reversal: Modular addition and XOR are reversed to restore the data.

4) Decryption Rounds: Similar to encryption, decryption also consists of multiple rounds but carried out in reverse order.
5) Final Output: The resulting decrypted block represents the original information before encryption.

2.4. Digital Image

A digital image is a visual representation obtained through digital devices, formed via the processes of sampling and quantization (Imam Zaki 2020). Sampling refers to dividing an image into a grid of pixels that represent brightness or grayscale levels, while quantization defines the number of colors or grayscale values each pixel can take. Based on representation, digital images can be classified into two types: bitmap (raster) images and vector images (Imam Zaki 2020). Bitmap images are composed of pixels, where image quality decreases when scaled up, making formats like BMP, GIF, and JPG common in photography and digital captures. Vector images, on the other hand, are generated through mathematical formulas, allowing them to be scaled without quality loss, and are widely used in graphic design applications. Examples include PDF and SVG formats (Yuni et al. 2017).

2.5. Magnetic Resonance Imaging (MRI)

Magnetic Resonance Imaging (MRI) is a non-invasive medical imaging technique that produces detailed internal images of the human body using strong magnetic fields and radio waves (dr. Caisar Dewi Maulina 2025). Unlike X-rays or CT scans, MRI excels in visualizing soft tissues, making it particularly useful for diagnosing brain, spinal cord, joint, and internal organ abnormalities such as those in the liver and kidneys. Its capability to deliver high-resolution images without harmful radiation makes MRI a preferred diagnostic tool in modern medicine (dr. Caisar Dewi Maulina 2025).

2.6. Avalanche Effect

The Avalanche Effect is a test used to evaluate how modifications in the encryption process influence the resulting encrypted data (Paramita C 2021). This evaluation provides insight into how changes in the encryption key structure impact the arrangement of bits in the ciphertext (Paramita C 2021). In other words, even a minor alteration in the input text can produce a significant transformation in the output. The principle of this method is that the higher the avalanche effect value, the stronger and more secure the cryptographic algorithm. In this study, encryption results and avalanche effect testing are carried out sequentially, meaning the analysis is performed after both the encryption and decryption processes. The Avalanche Effect can be calculated using the following formula:

$$Avalanche\ Effect = \frac{Jumlah\ bit\ yang\ berbeda}{Total\ Bit} \times 100\%$$

3. Materials and Methods

3.1. Research Approach

This study adopts a qualitative research approach, aiming to gain an in-depth understanding of the process and effectiveness of implementing double encryption algorithms to secure electronic medical imaging data. The analysis focuses on the conceptual and exploratory application of the Advanced Encryption Standard (AES) and the International Data Encryption Algorithm (IDEA) in protecting medical images from potential unauthorized access. Qualitative approaches are widely used in information system research to explore technical solutions to complex and dynamic problem (John W.Creswell & J.David Creswell 2020). The research relies on publicly available medical imaging datasets obtained from the Kaggle platform. These datasets serve as case studies for testing the encryption and decryption processes using AES and IDEA. The evaluation process involves two primary tests:
1) avalanche effect testing, to assess the sensitivity of encrypted outputs to minor input changes
2) efficiency analysis, to measure encryption and decryption times.

Time measurement is particularly important in healthcare information systems, where rapid cryptographic operations are crucial for practical implementation. Unlike quantitative hypothesis testing, this study emphasizes conceptual analysis, literature review, and technical observation of file encryption and decryption processes, focusing on identifying strengths and weaknesses of the applied system.

3.2. Dataset

In this study, the dataset serves as the primary source of data to be analyzed in order to obtain new insights or conclusions. There are two common types of datasets, namely private datasets and public datasets. Private datasets are usually obtained from specific institutions or organizations and are only accessible for internal purposes, while public

datasets are openly available and can be used by anyone. One of the most popular and widely used public dataset repositories in research and data analysis is the Kaggle platform [35].

This research utilizes Kaggle as the main source of electronic medical record (EMR) image data. The selected dataset is considered relevant and representative of the research focus, which emphasizes privacy protection and the security of medical image data. The dataset contains medical image files in .jpg or .png formats, such as MRI, CT Scan, and X-ray images, which resemble the data structure in Electronic Medical Record (EMR) systems. The availability of openly accessible and legally usable datasets makes them in line with the ethical principles of data usage in research. In addition, this dataset supports technical simulations for testing the implementation of AES and IDEA encryption algorithms, as well as performance evaluations of the algorithms based on the avalanche effect method and the measurement of encryption and decryption processing time. The use of this dataset is consistent with the exploratory case study approach, which aims to investigate the challenges of medical data security in depth and to evaluate the effectiveness and efficiency of the applied technical solutions in a data-driven scenario. Figures 3.2 show some of the datasets used in this study.

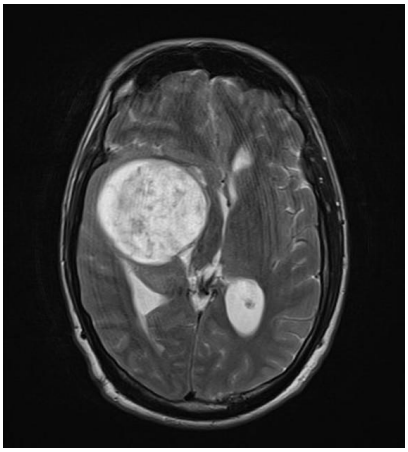

Figure 4 : dataset

3.3. System Design

The design of the image encryption and decryption application in this study is illustrated in Figure 5.

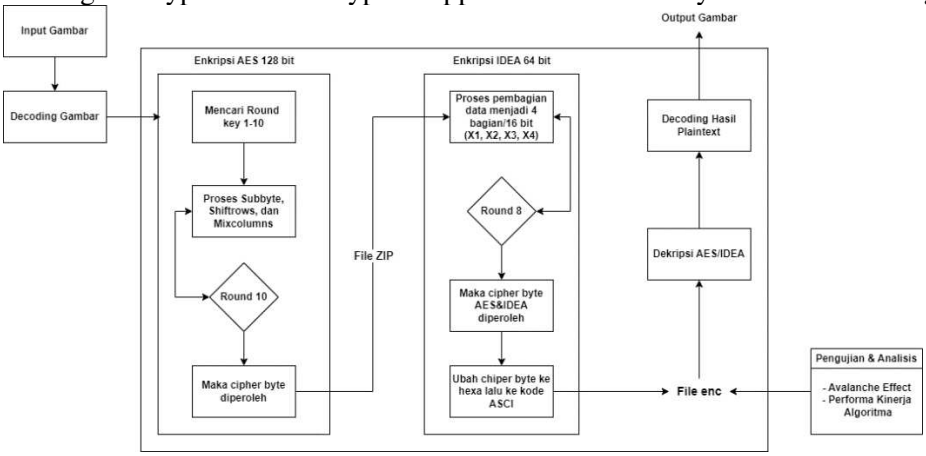

Figure 5 : System Design

Stage One begins with preprocessing, where the input image is decoded into pixels. These pixels are then converted into binary form and subsequently transformed into hexadecimal code, which serves as the raw data for encryption.

Stage Two is the AES 128-bit encryption process. The hexadecimal data is first processed with the AddRoundKey operation, followed by SubBytes, ShiftRows, and MixColumns transformations. These operations are performed iteratively across ten rounds, with each round utilizing its corresponding round key generated through key expansion. At the end of the tenth round, the final AES cipher bytes are obtained and temporarily stored in a ZIP file.

Stage Three applies a second layer of encryption using the IDEA 64-bit algorithm. The AES cipher output is divided into four 16-bit blocks ($X1, X2, X3, X4$) and processed through eight iterative rounds, each involving subkeys derived from IDEA key expansion. After all rounds are completed, the IDEA cipher output is produced, converted into hexadecimal form, transformed into ASCII representation, and saved as an encrypted file with the .enc extension.

Stage Four is decryption, which reverses the encryption steps. The encrypted .enc file is first decrypted using the IDEA algorithm to reconstruct the AES cipher data. This AES cipher is then decrypted using inverse AES operations, including InvShiftRows, InvSubBytes, InvMixColumns, and AddRoundKey, across ten rounds. The result is

hexadecimal data that is converted back into binary, decoded into pixels, and finally reconstructed into the original image.

Stage Five is the evaluation phase, which analyzes the encryption and decryption results. The evaluation includes measuring the Avalanche Effect to assess the strength of diffusion and calculating performance based on the time required for both encryption and decryption processes.

3.4. Testing Scenarios

The testing in this study aims to evaluate the effectiveness and robustness of the dual encryption method using the AES and IDEA algorithms on medical image data. To achieve this objective, several testing scenarios were designed based on cryptographic security indicators and resistance against unauthorized access. The tests were conducted technically through the encryption and decryption process of digital image files (.jpg/.png format) as well as security simulations using supporting software.

1) Encryption and Decryption Testing
   This test was carried out to ensure that the encryption process successfully encodes the original image into ciphertext, and the decryption process can restore it to its original form. The testing was performed on several MRI image samples from the Kaggle dataset. The decrypted results were compared visually and through byte-level verification to ensure that no data corruption occurred during the encryption-decryption process.
2) Avalanche Effect Testing
   The avalanche effect test aims to evaluate how sensitive the algorithm is to small changes in the input data. In this scenario, one bit of the plaintext was modified, and the resulting ciphertexts were compared using AES and IDEA separately as well as in combination. The percentage of altered bits in the ciphertext was calculated to determine the magnitude of the avalanche effect produced. A high avalanche effect indicates that the encryption system has a strong level of diffusion.
3) Process Efficiency Evaluation
   This test was conducted to measure the efficiency of the algorithms in terms of processing time. The time required for the encryption and decryption processes was measured in milliseconds using the Python time library. The evaluation was performed on image files of varying sizes to determine the consistency of system performance across small to large datasets.

4. Results and Discussion

In this study, results were obtained from the processes of encryption, decryption, avalanche effect testing, and encryption performance evaluation. The outcomes of the encryption process can be seen in Figure 4 and Figure 5.

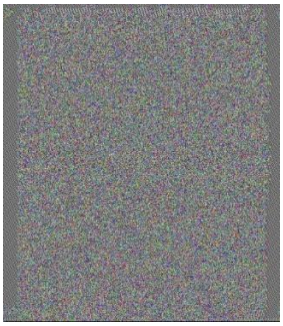

Figure 6 : AES Algorithm Encryption Results

Figure 7: IDEA Algorithm Encryption Results

4.1. Encryption Results

At this stage, the results of the medical image encryption process using the implemented algorithm are presented. Figure 4 shows the image after undergoing encryption, where the original visual pattern has been transformed into a random distribution of colors, making the information within the image completely unrecognizable without decryption. This indicates that the visual data has been successfully concealed.

Furthermore, Figure 5 illustrates the encrypted files stored in the .enc format. These files represent the final output of the encryption process, which cannot be directly accessed or interpreted by users unless decrypted with the correct key. The different file names also demonstrate that the system supports the encryption of various types of medical images, producing uniformly secure encrypted outputs.

4.2. Decryption Results

The decryption results demonstrate that the previously encrypted file has been successfully restored to its original form. This is evident from the file named decrypted_encrypted_outros_6_2.zip, which indicates that the decryption process was executed correctly and was able to recover data that was previously unreadable into an accessible format. Furthermore, the decrypted medical image is displayed clearly as a brain scan, where the anatomical structures and abnormal areas of interest remain visible. This outcome confirms that the applied encryption and decryption methods effectively preserve both the integrity and readability of the data without causing any damage or distortion to the medical image, ensuring that the information remains secure while still usable for medical analysis. The results of this decryption process can be observed in Figure 6 and Figure 7.

Figure 8: IDEA Decryption Results

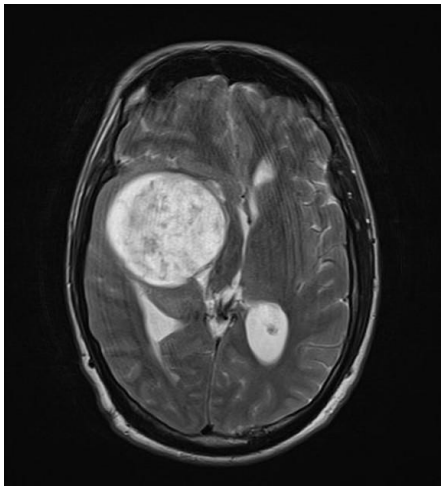

Figure 9 : IDEA Decryption Results

4.3. Algorithm Performance Testing

The performance testing of the algorithm was carried out to ensure the security and reliability of the AES and IDEA cryptographic algorithms used in the image data encryption and decryption process. The evaluation indicators included the avalanche effect, which measures the extent of change in the output (ciphertext) caused by a minor alteration in the input, such as a single-bit modification in the plaintext or key. The greater the change produced, the higher the level of diffusion achieved by the algorithm, which reflects its cryptographic strength against attacks. In

addition, execution time efficiency testing was performed, covering the measurement of the duration required for both encryption and decryption processes by each algorithm individually as well as in combination. This testing aimed to evaluate the performance of the algorithms in terms of speed and efficiency, which is crucial for implementation in information systems that handle large-scale data.

4.3.1. Avalanche Effect Testing

Avalanche effect testing was conducted by analyzing the changes in the bit structure of the test data. The avalanche effect is considered optimal if the percentage of bit changes ranges between 45% and 60%, with the ideal benchmark being 50% as the primary indicator of maximum test results [32]. The avalanche effect testing results are presented in Table 1.

Table 1 : Avalanche Effect Test Table

No	Secret key	Dokumen Terenkripsi	Original Size	Bit Deffence	Nilai Avalanche
1	nizar123	encrypted_schwannoma_10.enc	33839	356774	49.94%
2	123456	encrypted2_outros_6.enc	62586	95788	50.0%
3	aaaaaa	encrypted_neurocitoma_85.enc	21017	219161	50.0%
4	!@#$%^	Encrypted_normal_24.enc	34523	249906	49.98%
5	A!S@D#	encryted_glioma_76.bin	27944	249288	49.99%
		Rata-Rata			49.97%

4.3.2. Analysis of Avalanche Effect Testing Results

Based on the results of five encrypted files using AES and IDEA algorithms, the avalanche effect values obtained were highly consistent and very close to the ideal benchmark of 50%, with an overall average of 49.97%. The individual values ranged from 49.94% to 50.00%, despite variations in file size and secret keys of different lengths and character types (numeric, alphabetic, and symbolic). This consistency demonstrates that the applied encryption algorithms possess excellent diffusion capability. In practice, this means that even a small change in the input, such as flipping a single bit in the plaintext or key, produces a significant and randomized change in the ciphertext. This strongly reflects the avalanche effect principle, which serves as a crucial indicator of cryptographic robustness. The high diffusion values also indicate that the encryption system effectively obscures patterns that might otherwise be exploited in cryptanalysis attacks, thereby enhancing the overall level of data security. Thus, it can be concluded that AES and IDEA algorithms in this encryption system operate stably, effectively, and reliably in safeguarding information confidentiality.

4.3.3. Algorithm Performance Testing

Execution time testing was carried out to measure the efficiency of the encryption and decryption processes performed by AES, IDEA, and their combination on medical image data. This testing recorded the execution time of each encryption and decryption process across several MRI images from the same dataset, under consistent device conditions and file sizes. The purpose of this evaluation was to determine how quickly the algorithms perform and to assess the impact of double encryption on overall processing time. The results provide insight into the feasibility of both algorithms in practical implementation, particularly in health information systems where high security is required without compromising operational performance. The algorithm performance testing results are shown in Table 2.

Table 2 : Performance Testing Results

No	Original File	Waktu Enkrispsi
1	schwannoma_10.jpeg	44.0
2	outros_6.jpeg	58.6
3	neurocitoma_85.jpeg	42.0
4	normal_24.jpeg	63.5
5	glioma_76.jpeg	52.2
	Mean	52.2

4.3.4. Analysis of Algorithm Performance Testing Results

The encryption time testing results on five medical image files using AES and IDEA algorithms showed processing times ranging from 42.0 seconds to 63.5 seconds. The longest encryption time was recorded for *normal_24.jpeg* at

63.5 seconds, while the shortest time was for *neurocitoma_85.jpeg* at 42.0 seconds. The overall average encryption time was approximately 52.06 seconds.The variation in processing time was influenced by several factors, including the original file size, the complexity of image details, and differences in bit structures affecting the cryptographic transformation process. Despite the variations, the encryption times remained relatively stable and acceptable.

From these results, it can be concluded that the application of double encryption using AES and IDEA does indeed increase processing time compared to single-algorithm encryption. However, this increase remains within a reasonable range for applications that demand high levels of security—particularly in medical imaging data, where confidentiality and integrity are paramount. The balance between performance and security achieved in this study demonstrates that the AES–IDEA combination is effective and suitable for implementation in health information systems, such as electronic medical records, without significantly compromising system efficiency.

5. Conclussion

Based on the implementation and testing results, it can be concluded that the AES and IDEA algorithms are capable of performing encryption and decryption processes on electronic medical image records effectively. The medical images were successfully encrypted using a dual-layer combination of both algorithms and later decrypted back to their original form without any loss of integrity. This demonstrates the system's ability to maintain the confidentiality and reliability of sensitive medical data. The effectiveness of the encryption was evaluated through the avalanche effect, which yielded an average value close to the ideal 50%. This indicates that the AES and IDEA combination has a strong diffusion capability, where even small changes in plaintext cause significant variations in the ciphertext. Furthermore, performance testing showed that the encryption and decryption times remain within an efficient range, despite the additional processing time required for dual-layer encryption. Therefore, the use of double encryption with AES and IDEA provides a balanced solution between security and efficiency, making it suitable for implementation in healthcare information systems to protect digital medical image records.

References

And, Informatics, and Digital Expert. 2022. *Cryptography For Double Encryption On Images Using Algorithms AES (Advanced Encryption Standard) Dan RC5 (Rivest Code 5) Informasi Artikel A B S T R A K*. Vol. 4. no. 1. https://e-journal.unper.ac.id/index.php/informatics.

Ayu Nur Oktaviani. 2024. "Email Client Security Using Hash-Based Message Authentication Code And Pretty Good Privacy." *Seminar Nasional Penelitian (Semnas Corisindo 2024)*, October 23.

BBC News Indonesia. 2021. "Hackers Steal Data on 1.5 Million Patients in Singapore, Including PM Lee Hsien Loong's Prescriptions." Https://Www.Bbc.Com/Indonesia/Dunia-44899248, July 20.

Denghui Zhang, Lijing Ren, Muhammad Shafiq. 2023. "A Privacy Protection Framework for Medical Image Security without Key Dependency Based on Visual Cryptography and Trusted Computing." *Wiley Online Library*, January 31.

Dipti Kapoor Sarmah, Neha Bajpai. 2025. *Proposed System for Data Hiding Using Cryptography and Steganography*.

dr. Caisar Dewi Maulina. 2025. "MRI." Https://Www.Halodoc.Com/Kesehatan/Mri?Srsltid=AfmBOoqyfVLbj2mZhoB6hi2aUGKOvR7up5100nXO819LRDYsYimuwtlv, February 24.

Dzikri. (2024). Data Security Techniques Using Advance Encryption Standard Algorithm With Common Event Format To Improve Network Log Security. *Journal Of Information Technology And Computer Science (Intecoms)*.

Febri Dwinata Yonathan. 2021. *JEPIN (Jurnal Edukasi Dan Penelitian Informatika)*. August 2.

Imam Zaki. 2020. *Sistem Keamanan Citra Digital Menggunakan Algoritma Spritz*.

Irawati, Dyah Ayu, Mungki Astiningrum, and Elistya Rahma Dinda. 2018. *Implementation of Idea Algorithm and End Of File Method In Images To Hide Messages*.

Jihad Ramadhan, S.H. 2025. "The Importance of Protecting Personal Health Data." Siplawfirm.Id, February 26.

Jonathan Patrick | CNN Indonesia. 2020. "Read the full CNN Indonesia article "US Hospital Paralyzed by Hacker Attack" here: Https://Www.Cnnindonesia.Com/Teknologi/20200929134458-185-552240/Rumah-Sakit-as-Lumpuh-Akibat-Serangan-Peretas. Download Apps CNN Indonesia Sekarang Https://App.Cnnindonesia.Com/." Https://Www.Cnnindonesia.Com/Teknologi/20200929134458-185-552240/Rumah-Sakit-as-Lumpuh-Akibat-Serangan-Peretas, September 29.

Mahmoud Magdy & Neveen I. Ghali. 2022. "Security of Medical Images for Telemedicine: A Systematic Review." *Springer Nature*, March 22.

Meko, Donzilio Antonio. 2018. "Comparison of DES, AES, IDEA and Blowfish Algorithms in Data Encryption and Decryption." *Jurnal Teknologi Terpadu* 4 (1).

Melina, Melina, Asep Id Hadiana, Eddie Krishna Putra, et al. 2024. "Digital Signature Authentication Using Rivest-Shamir-Adleman Cryptographic Algorithm." *AIP Conference Proceedings* 2867 (1): 020011. https://doi.org/10.1063/5.0225078.

Munir, Rinaldi. 2019. *Sandi Rijndael. Fondasi Matematika Untuk Bekerja.* In *Studfile.Net*.

Prameshwari, Asri, and Nyoman Putra Sastra. 2018. "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi Dan Dekripsi File Dokumen." *Eksplora Informatika* 8 (1): 52. https://doi.org/10.30864/eksplora.v8i1.139.

ShareFile. 2024. *Healthcare Data Security: Safeguarding Patient Information in the Digital Age*. AS.

Siswanto, Arya Fajar, and Agus Herwanto. 2024. *Penerapan Metode Enkripsi Base64, SHA-512 DAN AES Untuk Menjamin Sebuah Keabsahan Ijazah*.

Taris Monica1*, A. I. (2024). Question Bank Security Using Rivest Shamir Adleman Algorithm and Advanced Encryption Standard. *JIko (Jurnal Informatika dan Komputer)*.

Yosanny, Agustinna. 2020. *Perancangan Enkripsi Pada… (Agustinna Yosanny) PERANCANGAN ENKRIPSI PADA CITRA BITMAP DENGAN ALGORITMA DES, TRIPLE DES, DAN IDEA*.

Yuni, Hertika, Asti Sinaga, and Lamhot Sitorus. 2017. *Pengamanan File Citra Digital Dengan Menggunakan Metode Least Significant Bit Dan End Of File*.