Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.5126

Application Optimazion Of Fidelity Watermarking Digital Imegery Discrete Fourier Transform Method And Rivest Shamir Adleman Algorithm

Nur Wulan[1], Herlina Harahap[2], Yunita Sari Siregar[3*]
[1,2,3]Universitas Harapan Medan , Indonesia
[1]nurwulanstth@gmail.com, [2]Herlina_Hrp@yahoo.com, [3]yunitasarisiregar1990@gmail.com

open access

***Corresponding Author**

Article History:
Submitted: 27-11-2024
Accepted: 05-12-2024
Published: 16-12-2024

Keywords:
Watermarking; Crytography; Fidelity; Digital Image, Discrete Fourier Transform (DFT); Rivest Shamir Adleman (RSA).

Brilliance: Research of Artificial Intelligence is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

ABSTRACT

As the field of information and communication technology continues to evolve, the potential for digital crimes increases significantly. Information technology plays a key role in facilitating various human activities in the fields of communication and data exchange. The use of digital data, such as documents, photos, videos, and audio, still creates many challenges in proving ownership.. The proliferation of social media platforms like Facebook, Instagram, and TikTok has made it easier for individuals to duplicate, damage, or even steal content, often for malicious purposes related to copyright infringement.To secure digital image data, the technique of fidelity watermarking using Discrete Fourier Transform (DFT) and cryptographic authentication with the Rivest-Shamir-Adleman (RSA) algorithm can be utilized. Watermarking is a technique that embeds information into an image, serving to provide identification marks and secure copyright information. This process does not damage the original image quality. DFT is a watermarking technique that has the capability to convert the image back to the spatial domain after embedding the watermark. On the other hand, RSA is a cryptographic technique that enables data encryption using a public key and decryption with a private key. In the context of image watermarking, RSA is used to secure the watermark information embedded within the image. Watermark information that is encrypted using the public key can only be accessed or decrypted by the party possessing the private key. This enhances the security of the watermark and ensures that the information embedded within the image remains safe, even if the image is shared.

INTRODUCTION

Watermarking is a technique used to embed a mark or proof of ownership into digital media in a way that is not visible or detectable by others. The embedding of a watermark into a digital image is done without damaging the quality of the image itself. The Discrete Fourier Transform (DFT) method works by identifying the harmonics or frequencies within a discrete signal sequence, which is obtained by periodically sampling a continuous signal in the time domain. Once the results of the digital image that has been watermarked are obtained, the next step involves encryption and decryption authentication using the Rivest-Shamir-Adleman (RSA) algorithm, where the public key (e) is used for encryption and the private key (d) is used for decryption, with e, d, and n being positive integersThe objective of this resea. rch is to design a watermarking and cryptographic authentication application by implementing the Discrete Fourier Transform (DFT) method and the Rivest-Shamir-Adleman (RSA) algorithm to enhance the optimization of digital image fidelity and protect it from misuse and criminal activities.

Images have characteristics that are not found in text data, such as being rich in information (Ramadhani, Siregar, & Siregar, 2018). An image is a distribution of variations in light-dark, dim-bright, and/or color across a flat surface. Its formal representation is done with numbers that represent variations in brightness intensity and/or color along the horizontal direction (Setyansyah, Siregar, & Khairani, 2019). Digital image watermarking is a technique used to embed ownership marks or copyright information into digital media in a way that is not visible. Fidelity refers to the quality of the host image remaining largely unchanged (Wahyuningsih, Pandex, & Stefanny, 2017). The observer is unaware that there is hidden data within the image. Watermarking (M Khairani & Nurwulan, 2018) is an application of steganography, but there are differences between the two. In steganography, secret information is hidden within digital media where the host media itself holds no significance. In watermarking, however, the digital media is protected by embedding a copyright label or watermark, ensuring ownership protection. There are two main processes in digital image watermarking: embedding and extraction (Umar & Darwis, 2019). The watermarking method used in this context is Discrete Fourier Transform (DFT), a mathematical procedure used to determine the harmonics or frequencies within a discrete signal sequence. The discrete signal sequence is obtained by periodically sampling a continuous signal in the time domain (Ariyanto, Ardiansyah, & Paris, 2018).

In cryptography terminology, it is the science and art of securing messages when they are sent from one place to

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.5126

another. When exchanging messages (such as letters) with someone, you would want the message to reach the intended recipient securely (Mufida Khairani, Harahap, Siregar, & Lubis, 2022). Cryptography is a method of scrambling information into various forms that cannot be read until translated. One weakness of scrambled messages is that it may raise suspicion, as it allows malicious actors to manipulate or alter the scrambled message, leading to the potential corruption of the secret message.(Mido & Ujianto, 2022). The RSA algorithm is a public-key algorithm that involves several mathematical concepts, such as Greatest Common Divisor (GCD), Euclid's algorithm, prime numbers, modular arithmetic, and congruences. The security of the RSA algorithm is based on the difficulty of factoring large prime numbers that are generated during the key pair creation process. The output of this algorithm is a public key (e), used for encryption, and a private key (d), used for decryption, with e, d, and n being positive integers. The keys used for encryption and decryption in regular messaging are different from those used in digital signatures. In digital signatures, the private key (d) is used to encrypt the message, and the public key (e) is used to decrypt it (HR, Khudzaifah, & Jauhari, 2021)

LITERATURE REVIEW

The previous research used as literature references in the study of fidelity watermarking for digital images with the Discrete Fourier Transform (DFT) method and the Rivest-Shamir-Adleman (RSA) algorithm includes: *Comparison of Discrete Cosine Transforms (DCT), Discrete Fourier Transforms (DFT), and Discrete Wavelet Transforms (DWT) in Digital Image Watermarking*. The conclusion of this study is that the experiments involve a comparative analysis of image watermark quality using Peak Signal to Noise Ratio (PSNR), color conversion, image resizing, optical image scanning, and the noise tolerance of the watermarked image by applying Gaussian noise (Asmara, Agustina, & Hidayatulloh, 2017). The analysis comparing the Discrete Fourier Transform (DFT) method and the Discrete Cosine Transform (DCT) method in the technique of hiding audio signals demonstrates that the technique of hiding audio signals works by increasing the frequency so that the information signal being transmitted cannot be heard by unwanted listeners. Therefore, the DCT method is more effective or suitable compared to the DFT method for hiding audio signals, as it allows the audio signal to be hidden, whereas the DFT method does not (Elawati, Hayati, & Hanafi, 2022).

The analysis of watermarking using the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) methods concludes that, in terms of color, RGB is better for DCT, while binary is better for DFT. Additionally, in terms of the type of watermark inserted, both DCT and DFT show that a good watermark is one that is invisible (Solikhin, Pratama, Pasaribu, Rumahorbo, & Simanullang, 2022). The implementation of watermarking on digital images using the Discrete Fourier Transform (DFT) and Singular Value Decomposition (SVD) techniques concludes that the tests show these techniques are useful for copyright labeling on digital images (Kasihno & Murinto, 2017). The application of cryptography using the RSA algorithm for data security in a desktop-based system at PT Trias Mitra Jaya Manunggal concludes that the speed of the application highly depends on the size of the file being encrypted or decrypted (Rizki & Ariyani, 2021). The implementation of the RSA (Rivest-Shamir-Adleman) cryptographic algorithm for the security of patient medical records data shows that the web-based medical record system can assist Klinik Citra Bunda in enhancing the security of patient medical record data (Sutejo, 2021).

METHOD

The method in this study employs a security system with watermarking techniques and cryptographic authentication. Watermarking is a method used to hide secret information or a watermark within a digital image without damaging the visual quality of the image (Utomo, Sari, & Hari, 2024). In watermarking, the Discrete Fourier Transform (DFT) is a mathematical procedure used to determine the harmonics or frequencies that make up the sequence of discrete signals. The discrete signal sequence is obtained from the periodic sampling of a continuous signal in the time domain (Ariyanto et al., 2018). In cryptography, the Rivest-Shamir-Adleman (RSA) method is used. RSA is an asymmetric cryptographic algorithm, first discovered in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The name RSA is derived from the initials of the first names of its inventors. As an asymmetric algorithm, RSA uses two keys: a public key and a private key. The public key can be known by anyone and is used for the encryption of data, while the private key is kept secret and is used for the decryption of data (Christian, Sitorus, & Nirmala, 2023).

Watermarking Method using Discrete Fourier Transform (DFT)

Discrete Fourier Transform is derived from the Fourier Transform function X(f), which is defined in equation 1:

$$X(f) = \int_{\infty}^{\infty} x\,[t].\,e^{-f2\pi ft}\,dt \quad (1)$$

Where:
N = Number of input samples
X(m) = The m-th sequence component of the output DFT (X(0), X(1),…,X(N-1))
m = The index of the DFT output in the frequency domain (0, 1, ..., N-1)
x(n) = The n-th input sample sequence (x(0), x(1), ..., x(N-1))
n = The index of the input sample in the time domain (0, 1, ..., N-1)

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.5126

j = The imaginary number (√−1)
π = Pi (180°)
e = Natural logarithm (2.718281828459)

In the field of continuous signal processing, Equation 1 is used to transform the continuous time-domain function x(t) into a continuous frequency-domain function X(f). The function X(f) allows for determining the frequency content of various signals and enables a wide range of signal analysis and processing techniques used in engineering and physics. With the advent of digital computers, scientists in the field of digital processing successfully defined the Discrete Fourier Transform (DFT) as a sequence of discrete time-domain signals transformed into the frequency domain X(m), as shown in Equation 2.

$$F(x) = \sum_{n=0}^{N-1} x\,(n).\, e^{-f 2\pi nm/N} \quad (2)$$

Where:
N = Number of input samples
X(m) = m-th component of the DFT output sequence (X(0), X(1), ..., X(N-1))
m = Index of the DFT output in the frequency domain (0, 1, ..., N-1)
x(n) = n-th sample of the input sequence (x(0), x(1), ..., x(N-1))
n = Index of the input sample in the time domain (0, 1, ..., N-1)
j = Imaginary number (√-1)
π = Degree (180°)

Then, connect it with Euler's formula e^{-jo} = cos (o) – j sin (0), which can be expressed as the following equation 3:

$$X\,(m) = \sum_{n=0}^{N-1} x\,(n).\,[cos\left(\frac{2\pi nm}{N}\right) - j\,\sin\left(\frac{2\pi nm}{N}\right)] \quad (3)$$

Where:
N = Number of input samples
X(m) = m-th component of the DFT output sequence (X(0), X(1), ..., X(N-1))
m = Index of the DFT output in the frequency domain (0, 1, ..., N-1)
x(n) = n-th sample of the input sequence (x(0), x(1), ..., x(N-1))
n = Index of the input sample in the time domain (0, 1, ..., N-1)
j = Imaginary number (√-1)
π = Degree (180°)

Although more complex than Equation 2, Equation 3 is easier to understand. The constant j = √−1 helps in comparing the phase relationships within the various sinusoidal components of the signal. The value of NN is an important parameter because it determines how many input samples are required, the resulting frequency domain, and the amount of processing time needed to compute the N-point DFT. It requires N complex multiplications and N−1 additions. Then, to calculate all N values X(0),X(1),...,X(N−1)X(0), X(1), ..., X(N-1), N2 multiplications are needed. This results in the DFT computation taking a significant amount of time when the number of samples to be processed is large.

The 2D Discrete Fourier Transform (DFT) is a discrete Fourier transform applied to a 2D function (a function with two independent variables), which is defined in Equation 4 as follows:

$$F\,(u, v) = \frac{1}{MN} \sum_{y=0}^{M-1} \sum_{Y=0}^{N-1} f\,(y, x) \begin{pmatrix} \cos\left(2\pi\left(\frac{ux}{N}+\frac{vy}{M}\right)\right) \\ -j\,\sin\left(2\pi\left(\frac{ux}{N}+\frac{vy}{M}\right)\right) \end{pmatrix} \quad (4)$$

The 2D DFT is widely used in digital image processing because image data is represented as a 2D function.

Rivest Shamir Adleman (RSA) Algorithm

1. Key Generation Process

The RSA algorithm involves both a public key and a private key. The public key is known to everyone and is used to encrypt messages. Messages encrypted with the public key can only be decrypted using the corresponding private key. The process of generating the public and private keys using RSA is as follows:

a) Select two large random prime numbers, denoted as (p) and (q). These prime numbers should be sufficiently large, typically at least three digits.
b) Calculate the value of (n), which is referred to as the security parameter in equation 4:

$$n = p \times q \quad (4)$$

c) Select a random number for the public key (e) such that e does not share any common divisors with Φ(n) or

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.5126

(p-1) (q-1) other than 1, meaning it is relatively prime.

d) Compute the private key (d) using the Euclidean algorithm to find the value of d in equations 5 and 6:

$$e \times d = 1 \ (mod\ \Phi(n)) \quad (5)$$

or

$$e \times d = (1 + k\ \Phi\ (n))\ (3) \quad (6)$$

Since both equations are equivalent, d can be calculated using this formula, provided that k is an integer, which will also result in a valid decryption key as shown in equation 7.

$$d = \frac{(1+k\ \Phi\ (n))}{e} \quad (7)$$

e) The values of n and e are publicly known, while the values of p and q are kept secret to prevent public knowledge. The public key consists of the values (n,e), while the private key consists of the values (d,n)

2. Encryption Process

In the data encryption process, encoding is performed using the public key (n, e). Initially, the data in the form of plaintext is inputted and then converted into ASCII format for each character. Next, the plaintext (P) will be encrypted with the public key using the calculation in equation 8.

$$C = P^{e}\ (mod\ n) \quad (8)$$

3. Data Decryption Process

In the data decryption process, the data that was previously encrypted (ciphertext) using the public key (e, n) will be converted back into the original message (plaintext) using the private key (d, n). The first step is to input the ciphertext (C), and then the data is decrypted into its ASCII form for each character using the calculation in equation 9.

$$P = C^{d}\ (mod\ n) \quad (9)$$

RESULT

Analysis is the breakdown of a perfect information system into its component parts with the aim of identifying and evaluating problems, opportunities, obstacles, and expected needs, so that improvements can be proposed. In the increasingly advanced digital era, protecting copyright and the authenticity of digital images has become crucial, especially with the rising risks of counterfeiting and misuse of digital works. One solution used is watermarking, which embeds a watermark into the image to protect copyright and maintain data integrity. However, the main challenge in watermarking is maintaining the image quality or fidelity after the watermark is inserted. Fidelity measures how well a watermark can be embedded without disturbing the visual quality of the original image.

To address this issue, a combination of Discrete Fourier Transform (DFT) and the Rivest Shamir Adleman (RSA) Cryptographic Algorithm is often considered as a method to improve watermarking optimization. DFT allows the watermark to be inserted into the frequency domain, making it more resistant to attacks or image modifications such as compression and rotation. On the other hand, RSA provides a strong cryptographic mechanism to secure the watermark, ensuring that only authorized parties can access or verify the watermark. However, while this method offers a more secure and robust solution, challenges remain in balancing security, speed, and fidelity. The combination of these two methods must be optimized to ensure watermarking remains effective without significantly reducing image quality.

The application of the Discrete Fourier Transform (DFT) method and the Rivest Shamir Adleman (RSA) Cryptographic Algorithm in digital image watermarking is a combination of techniques aimed at improving the security and quality of the embedded watermark. DFT is a mathematical method that transforms data from the spatial domain to the frequency domain, enabling the watermark to be embedded in the image's frequency components. By embedding the watermark in the frequency domain, the image becomes more resistant to attacks such as compression, rotation, or noise, which frequently occur in digital images. A watermark hidden in a specific frequency is harder to detect or remove without affecting the overall image quality.

The RSA Algorithm is an implementation of asymmetric cryptography, a type of cryptography that uses two different keys: a public key and a private key. The security levels in the RSA algorithm are determined by several key factors, including the size of the keys used in the algorithm:

a. p and q are prime numbers (secret)
b. N = p . q (not secret)
c. Φ(n) = (p–1) (q–1) (secret)
d. e = (encryption key) (not secret)
e. d = (descryption key) (secret))
f. X (plainteks) (secret)
g. Y (cipherteks)(not secret)

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.5126

Encryption will be performed using the RSA algorithm on the plaintext M = FISIKA. First, the plaintext is converted into ASCII format, as shown in Table 1 below:

Table 1. Encryption ASCII Table

TEXT	F	I	S	I	K	A
ASCII HEKS	46	49	53	49	4B	41
ASCII DES	70	73	83	73	75	65

The plaintext in decimal ASCII format is then divided into blocks of three digits as follows:
M_1 =707
M_2 = 383
M_3 = 737
M_4 = 565

In creating an RSA key, it is necessary to design it such that the value mm remains within the range of 0 to n−1n - 1. Therefore, it is determined that the minimum value of nn is 909. This value is chosen based on the consideration that the largest uppercase letter is 'Z', with an ASCII value of 5Ah or 90. The combination of 'ZZ' would then result in values of 909 or 090.

Assume p=23p = 23 and q=43q = 43 (both prime), the calculations are as follows:
n = p x q = 989
m = (p – 1) x (q – 1) = 924

The public key e=25e = 25 is chosen, which is relatively prime to 924 because their greatest common divisor (GCD) is 1. The fact that 25 is relatively prime to 924 can be proven by finding the GCD of 25 and 924 using the following algorithm.
25 = 0 (924) + 25
924 = 36 (25) + 24
25 = 1 (24) + 1
4 = 24 (1) + 0

The result of the GCD in this algorithm is the last remainder before reaching zero. As shown in the calculation above, the remainder before zero is 1. Therefore, gcd(25, 924) = 1. Next, to calculate the private key d, the Extended Euclidean algorithm is used as follows.
$Step_0$: 924 = 36 (25) + 24
$Step_1$: 25 = 1 (24) + 1
$Step_2$: 4 = 24 (1) + 0
P_0 = 0
P_1 = 1
P_2 = 888
P_3 = 37

P2 and P3 are calculated using the following equations.
P2 = (pi-2 – pi-1q-i-2-) mod n
= (0 – 1(36)) mod 924 = 888
P3 = (1 – 888(1)) mod 924 = 37

Thus, the public key obtained is 25 and 989, while the private key is 37 and 989. The encryption of each block is performed using the public key 25 and 989 as follows:
c1 = 70725 mod 989

To calculate 70725 mod 989, we can use the "divide and conquer" technique to break down the exponentiation into smaller parts. The illustration is as follows:
707^{25} = $707^{16}.707^{8}.707^{1}$
707^{2}mod 989 = 4998 49 mod 989 = 404
707^{4}mod 989 = $(707^{2}.707^{2})$mod 989
= [(707^{2}mod 989) (707^{2}mod 989)]mod 989
= (404.404) mod 989
= 163216 mod 989 = 31
702^{8}mod 989 = $(707^{4}.707^{4})$mod 989
= [(707^{4}mod 989) (707^{4}mod 989)]mod 989
= (31.31)mod 989
= 961 mod 989 = 961
707^{16}mod 989 = $(707^{8}.707^{8})$mod 989
= [(707^{8}mod 989) (707^{8}mod 989)]mod 98= (961.961) mod 989
= 923521 mod 989 =784
707^{25}mod 989 = $707^{16}.707^{8}.707^{1}$ mod 989

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.5126

$= ((707^{16} \bmod 989.707^{8} \bmod 989) \quad \bmod 989.707^{1} \bmod 989) \bmod 989$
$= ((784.961) \bmod 989.707) \bmod \quad 989$
$= ((753424) \bmod 989.707) \bmod \quad 989$
$= (795.707) \bmod 989 = 313$

So, $C_1 = 707^{25} \bmod 989 = 313$
Using the same method, we can obtain the following results:
$C_2 = 383^{25} \bmod 989 = 776$
$C_3 = 737^{25} \bmod 989 = 737$
$C_4 = 565^{25} \bmod 989 = 909$
Thus, the ciphertext is C = 313,776,737,909

It should be noted that this ciphertext is in decimal ASCII format. When converted back to character format, the result is shown in Table 2:

ASCII DES	**31**	**37**	**76**	**73**	**79**	**09**
ASCII HEKS	1F	24	4C	49	4F	09
TEXT		%	L	I	O	

Hexadecimal 1F and 09 are non-printing characters. This refers to specific control characters in the ASCII or Unicode character sets.

a. 1F (in hexadecimal) corresponds to the "Unit Separator" in ASCII, which is a control character used in data formatting, and it's non-printing, meaning it doesn't have a visual representation when printed.
b. 09 (in hexadecimal) corresponds to the **"Tab"** character in ASCII, which is also a non-printing character used for text alignment (a horizontal tabulation space).

DISCUSSION

In this research, the Discrete Fourier Transform (DFT) watermarking technique has been combined with the RSA encryption algorithm to achieve both data security and integrity for digital images. This combination is highly relevant in the context of securing digital assets, such as images, from unauthorized access and modification.

a. DFT Watermarking Technique

Watermarking is a process of embedding a hidden mark (or watermark) into a digital image to protect its authenticity, copyright, and integrity. The method used in this research employs Discrete Fourier Transform (DFT), which allows the watermark to be embedded in the frequency domain of the image, instead of the spatial domain.

b. DFT Watermarking Advantages:
   1. Increased Resilience to Attacks: By embedding the watermark in the frequency domain, DFT watermarking makes the watermark more resistant to common image manipulations like compression, cropping, or rotating. These types of modifications usually affect the spatial domain (pixels) more directly. Since the watermark is hidden in the frequency domain, it is much harder to detect and remove without degrading the quality of the image significantly.
   2. Minimal Impact on Image Quality: The watermark embedded using DFT does not significantly affect the visual quality of the image. The human eye is less sensitive to changes in the frequency domain, especially in areas that are less important visually, such as the high-frequency components. As a result, the image maintains its fidelity (visual quality) even after the watermark is inserted.

c. RSA Encryption and Watermarking Together

The RSA encryption algorithm ensures the confidentiality and security of the image data, while DFT watermarking protects the image's integrity. When used together, RSA and DFT complement each other in several ways:

   1. Encryption Using RSA: RSA provides a robust method for encrypting the image or its associated metadata. By using the public key, the image data is transformed into ciphertext, ensuring that only the holder of the private key can decrypt it. This ensures data confidentiality by making the image content unreadable to unauthorized users.
   2. Watermarking for Integrity: While RSA secures the image content, watermarking with DFT ensures that any unauthorized modifications made to the image can be detected. Even if an attacker has access to the encrypted image, they would not be able to alter the image without disturbing the watermark embedded through DFT. This watermarking acts as a safeguard against tampering and serves as a proof of authenticity.

d. Challenges in Combining RSA and DFT Watermarking

While combining RSA encryption with DFT watermarking strengthens both confidentiality and integrity, there are still challenges to consider:

   1. Processing Complexity and Speed: The use of DFT watermarking requires the transformation of the image from the spatial domain to the frequency domain, which can be computationally intensive, especially for large images. When combined with the RSA encryption, which also involves heavy computations for key

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.5126

generation, encryption, and decryption, the system's performance might slow down, particularly for high-resolution images. This trade-off between security and processing time is a key consideration in real-world applications.

2. Memory Usage: Both RSA encryption and DFT watermarking require substantial memory, especially for larger images. DFT involves calculating the frequency components of the image, and RSA requires large key sizes for secure encryption, further increasing memory consumption.

e. Optimizing the Combination of RSA and DFT Watermarking

For real-world deployment, it is important to balance the effectiveness of both techniques while ensuring efficiency. Several optimizations can be made:

1. Smaller Key Sizes in RSA: While larger key sizes offer stronger security, they also significantly slow down the encryption and decryption process. For practical applications where speed is crucial, smaller RSA key sizes could be used, as long as they still provide a sufficient level of security for the intended use.
2. Compression Techniques for Watermarked Images: To reduce the processing time for DFT watermarking, lossy compression algorithms can be employed for the image, but care must be taken to ensure that the watermark remains intact during compression. The trade-off between compression and watermark strength should be carefully considered.
3. Hybrid Methods: One possible optimization is to combine DFT watermarking with other lightweight encryption algorithms (such as AES) for faster encryption and decryption, while still using RSA for critical applications that demand stronger security.

CONCLUSION

Based on the research results regarding the Optimization of Fidelity Watermarking Application for Digital Images Using Discrete Fourier Transform (DFT) and Rivest Shamir Adleman (RSA) Algorithm, the following conclusions can be drawn:

a. Watermarking using Discrete Fourier Transform (DFT) successfully embeds a watermark into digital images without compromising their visual quality. This technique allows the watermark to be inserted in the frequency domain, making the image more resistant to attacks such as compression, rotation, or noise, while maintaining a high level of fidelity.
b. Security Using RSA. The use of the RSA Algorithm provides strong security for the embedded watermark by applying encryption with a public key and decryption with a private key. This ensures that only authorized parties can access or verify the existence of the watermark on the digital image.
c. Optimization of Watermarking and Encryption. The combination of DFT watermarking and RSA cryptography provides an effective solution to enhance the security and integrity of digital images. This system not only protects the copyright of the images but also preserves the quality of the involved images.
d. Challenges in optimization. Although this combination offers a secure solution, challenges remain in terms of . processing speed, especially for large images. Therefore, further optimization is needed to improve efficiency and processing time.
e. Applications utilizing these two techniques are highly relevant for industries that require digital copyright protection and data integrity, such as in digital arts, management of important documents, and the medical sector.

ACKNOWLEDGMENT

We would like to express our sincere gratitude and pride to the Ministry of Education, Culture, Research, and Technology (Kemdikbudristek) for their invaluable support in providing research funding through the 2024 Junior Lecturer Research Scheme via the Directorate of Research, Technology, and Community Service. We also extend our thanks to the LPPM of Universitas Harapan Medan for their support, monitoring, motivation, and evaluation during the research process.

REFERENCES

Ariyanto, Y., Ardiansyah, R., & Paris, B. (2018). Steganografi Menggunakan Metode Discrete Fourier Transform (DFT). *Jurnal Informatika Polinema*, *4*(2), 87. https://doi.org/10.33795/jip.v4i2.151

Asmara, R. A., Agustina, R., & Hidayatulloh. (2017). Comparison of Discrete Cosine Transforms (DCT), Discrete Fourier Transforms (DFT), and Discrete Wavelet Transforms (DWT) in Digital Image Watermarking. *International Journal of Advanced Computer Science and Applications*, *8*(2). https://doi.org/10.14569/ijacsa.2017.080232

Christian, C., Sitorus, S. H., & Nirmala, I. (2023). Implementasi Algoritma RSA Dan One Time Password (OTP) Untuk Pengamanan Data Pengguna dan Proses Transaksi pada Website E-Commerce. *Coding: Jurnal Komputer Dan Aplikasi*, *11*(1), 62–72.

Elawati, Hayati, R., & Hanafi. (2022). Analisis Perbandingan Metode Descrete Fourier Transform Dan Metode Descrete

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.5126

Cosine Transform Pada Teknik Menyembunyikan Sinyal Suara. *Jurnal Tektro*, *6*(2), 74.

HR, A. H., Khudzaifah, M., & Jauhari, M. N. (2021). Implementasi Fungsi Hash MD5 dan Kriptografi Algoritma RSA pada Pembuatan Tanda Tangan Digital. *Jurnal Riset Mahasiswa Matematika*, *1*(2), 51–63. https://doi.org/10.18860/jrmm.v1i2.13992

Kasihno, T., & Murinto. (2017). Implementasi Watermarking pada Citra Digital Menggunakan Teknik Discrete Fourier Transform (DFT) dan Singular Value Decomposition (SVD) (Implementation of Watermarking in Digital Image Using Discrete Fourier Transform (DFT) Technique and Singular V. *Juita*, *V*(1), 31–37.

Khairani, M, & Nurwulan, N. (2018). Algoritma Blowfish Pada Watermarking Video Digital. *JURIKOM (Jurnal …*, *5*(4), 357–361. Retrieved from http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom/article/view/842

Khairani, Mufida, Harahap, H., Siregar, Y. S., & Lubis, Y. F. A. (2022). Implementation Of Discrete Cosine Transform (DCT) And Blowfish Methods In Digital Video Security. *Sinkron : Jurnal Dan Penelitian Teknik Informatika*, *7*(1), 232–242.

Mido, A. R., & Ujianto, E. I. H. (2022). Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA dan STEGANOGRAFi LSB. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *9*(2), 279. https://doi.org/10.25126/jtiik.2022914852

Ramadhani, R., Siregar, D., & Siregar, Y. S. (2018). Implementasi Steganografi Menggunakan Algoritma Diversity Pada Citra Digital. *Jurnal Teknologi Dan Ilmu Komputer Prima (JUTIKOMP)*, *1*(1), 102–114. https://doi.org/10.34012/jutikomp.v1i1.337

Rizki, M., & Ariyani, P. F. (2021). Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal. *Skanika*, *4*(2), 1–6. https://doi.org/10.36080/skanika.v4i2.1991

Setyansyah, R., Siregar, Y. S., & Khairani, M. (2019). Noise Removal Pada Citra Digital Dengan Menggunakan Metode Active Contour. *ALGORITMA: Jurnal Ilmu Komputer Dan Informatika*, *5*(1), 978–979. Retrieved from http://www.seminar.ilkom.unsri.ac.id/index.php/ars/article/view/2130

Solikhin, M., Pratama, Y., Pasaribu, P., Rumahorbo, J., & Simanullang, B. (2022). Analisis Watermarking Menggunakan Metode Discrete Cosine Transform (DCT) dan Discrete Fourier Transform (DFT). *Jurnal Sistem Cerdas*, *5*(3), 155–170. https://doi.org/10.37396/jsc.v5i3.192

Sutejo. (2021). Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien. *INTECOMS: Journal of Information Technology and Computer Science*, *4*(1), 104–114. https://doi.org/10.31539/intecoms.v4i1.2437

Umar, F., & Darwis, H. (2019). Watermarking Citra Digital Berwarna Menggunakan Stationary Wavelet Transform (Swt). *ILKOM Jurnal Ilmiah*, *11*(1), 1–10. https://doi.org/10.33096/ilkom.v11i1.409.1-10

Utomo, D. W., Sari, C. A., & Hari, R. E. (2024). OPTIMASI INVISIBLE WATERMARKING METODE DCT BERBASIS SVD PADA CITRA BERWARNA. *Seminar Nasional Riset Dan Inovasi Teknologi (SEMNAS RISTEK)*, 96–102.

Wahyuningsih, S., Pandex, T. V. D., & Stefanny, V. (2017). Implementasi Visible Watermarking Dan Steganografi Least Significant Bit Pada File Citra Digital. *Jurnal TELEMATIKA MKOM*, *8*(2), 140–145.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.