EIU
Emirates International University Journal
مجلة الجامعة الإماراتية الدولية

Volume 1 Issue 1
23-8-2025

Image encryption using RSA & IWT Techniques

Dr. Gamil R. S. Qaid [1,2]
Ph.D. in Computer Sciences and Engineering
dr.gamil@eiu.edu.ye
dr.g_qaid@hoduniv.net.ye

Maha Abdulaziz Al-Aswad[2]
alaswad028@gmail.com

Jumana Abbas Al-Wajih[3]
jumanaabbasjaa@gmail.com

Dr. Malek Algabri [4]
Ph.D. in Computer Science and Technology
dr.malekye@eiu.edu.ye

[1]Department of Cybersecurity, Faculty of Engineering and Information Technology, Emirates International University, Sana'a, Yemen
[2,3] Department of Information security, Faculty of Information Technology, Emirates International University, Sana'a, Yemen.
[4]Department of Cybersecurity, Faculty of Engineering and Information Technology, Emirates International University, Sana'a, Yemen

ABSTRACT

Image encryption is a crucial technique in ensuring the confidentiality and security of digital images, especially when transmitted over untrusted networks. Combining the RSA cryptosystem and Integer Wavelet Transform (IWT) offers a robust method for encrypting images. RSA provides strong asymmetric encryption, while IWT compresses the image efficiently, reducing data size and maintaining image quality.

Keywords: Asymmetric image encryption: IOM,PTM,RSA,IWT

Introduction:

in today's digital age, images play a vital role in various fields, including social media, medical imaging, defense, and telecommunication. With the increase in digital image transmission over the internet, the security and privacy of images have become a major concern [1]. Encryption is a critical method for protecting sensitive images from unauthorized access. In this paper, we explore an integrated approach to image encryption that combines the widely used RSA (Rivest-Shamir-Adleman) algorithm and the Integer Wavelet Transform (IWT). This combination offers [2]

Related Work

Image encryption has been a significant research area for ensuring the confidentiality of images transmitted over the internet [5]. Various techniques have been developed to protect image data, ranging from symmetric key encryption methods like AES (Advanced Encryption Standard) to asymmetric methods such as RSA[4]. The RSA algorithm, due to its reliance on public and private key pairs, is often preferred for its security robustness. However, the RSA algorithm alone can be computationally intensive when dealing with large datasets like images, leading to performance bottlenecks Wavelet-based techniques, such as Discrete Wavelet

Transform enhanced security while maintaining efficient image processing. The RSA algorithm is one of the most robust and well-known public-key cryptosystems, primarily used for securing data through encryption and decryption[1]. Meanwhile, wavelet transform, such as IWT, are widely used for image compression and signal processing. By integrating RSA with IWT we aim to provide an advanced method for securing image data, offering both encryption strength and efficiency [5].

Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT), have gained popularity in image compression and processing. IWT, in particular, preserves the integrity of the data during transformation, making it a preferred choice for lossless encryption processes. The integration of cryptographic techniques with wavelet transforms has been explored in several studies, offering a promising approach to both Encrypt and compress image data. However, combining RSA with IWT for image encryption remains underexplored in the literature, and this paper addresses this gap by proposing an efficient encryption system based on these techniques [4]

Image encryption has become an essential research area for ensuring the confidentiality of images transmitted over the internet. Various encryption techniques have been developed to protect image data. Symmetric key encryption methods such as the Advanced Encryption Standard (AES) are widely adopted due to their speed and efficiency when handling large datasets[3]. However, asymmetric key encryption methods, like the RSA algorithm, rely on public and private key pairs, offering stronger security guarantees. RSA is preferred for its robustness against attacks but can be computationally expensive, especially when processing large datasets like images, leading to performance bottlenecks. Wavelet-based techniques, such as the Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT), have gained popularity in image compression and processing due to their ability to preserve data integrity during transformation. IWT, in particular, is favored in lossless encryption processes because it maintains the exact original data after the inverse transformation. Several previous studies have explored the combination of cryptographic techniques with wavelet transforms. For instance, **Chandra and Pandey (2017)** proposed a hybrid model combining DWT with AES, achieving a good balance between encryption speed and data security. However, one downside of this approach was the potential for data loss during the transformation process, which made it

unsuitable for sensitive applications requiring lossless encryption. Another notable study by **Gupta et al. (2019)** examined the use of RSA in combination with DWT. While the encryption system provided strong security, the computational load imposed by RSA, especially when encrypting large datasets like high-resolution images, led to delays and reduced efficiency[1]. Despite the contributions of these studies, the integration of RSA with IWT remains underexplored in the literature. IWT offers the advantage of being a lossless transform, which ensures that the image can be perfectly reconstructed after decryption, a critical feature for high-fidelity image encryption[2]. This paper aims to address the gap by proposing an efficient encryption system based on combining RSA and IWT[7]. The proposed approach seeks to enhance both the security and performance of image encryption, providing a robust solution for securely transmitting image data over the internet without compromising the quality of the encrypted data. Symmetric key encryption methods, such as the **Advanced Encryption Standard (AES)**, have been widely adopted due to their computational efficiency and speed when handling large datasets like images. **Sharma et al. (2016)** proposed a fast and secure image encryption scheme using AES that offered high encryption speed and low computational overhead. However, the symmetric nature of AES requires secure key distribution, which can pose challenges in highly distributed environments like the internet. While AES is suitable for applications where speed is critical, its security is heavily reliant on the secrecy of the shared key. On the other hand, asymmetric key encryption methods, like the **Rivest-Shamir-Adleman (RSA)** algorithm, offer a more secure approach by utilizing two separate keys – a public key for encryption and a private key for decryption. RSA is favored in scenarios requiring strong security, as the use of large key sizes makes it resistant to brute-force attacks[2]. **Singh and Supriya (2013)** conducted a comprehensive analysis of RSA's performance in image encryption, emphasizing its high level of security. However, the authors noted that RSA's computational complexity, especially when dealing with high-resolution images or large datasets, results in significant performance overhead. RSA’s security comes at the cost of speed, making it less suitable for real-time image encryption applications. To address the challenges of computational complexity, researchers have explored the use of **wavelet transforms** in combination with cryptographic algorithms. **Wavelet-based techniques**, such as the **Discrete Wavelet Transform (DWT)** and **Integer Wavelet Transform (IWT)**, are widely used in image compression and processing due to their multi-resolution analysis capabilities[8] . DWT, for instance, decomposes an

image into multiple frequency bands, allowing for efficient compression and manipulation. However, DWT is a lossy transform, meaning that some information is discarded during transformation, which may not be ideal for sensitive applications, on the other hand, is a lossless wavelet transform, making it an attractive choice for image encryption. The main advantage of IWT is that it preserves the original image data after transformation, ensuring that no information is lost during encryption and decryption. Wang et al. (2015) demonstrated the effectiveness of IWT in image encryption, achieving high compression rates while maintaining data integrity. Their work showed that combining IWT with encryption algorithms could result in a more efficient and secure system for image transmission [6]. Several recent studies have explored the combination of cryptographic techniques with wavelet transforms. Chandra and Pandey (2017) proposed a hybrid model that integrated DWT with AES, providing a good balance between encryption speed and data security. However, they acknowledged that the lossy nature of DWT could lead to issues in applications requiring high fidelity and exact data recovery [2]. Similarly, Gupta et al. (2019) investigated the combination of RSA with DWT for secure image encryption. Their system offered strong encryption security, but the computational cost of RSA, particularly when handling large datasets, led to performance bottlenecks. This issue becomes even more significant when encrypting

Methodology

The proposed encryption scheme utilizes the RSA algorithm in conjunction with the Integer Wavelet Transform (IWT) to secure digital images. The process involves several stages, including image preprocessing, IWT-based transformation, RSA encryption, and reverse decryption for recovering the original image[6].

RSA algorithm overview:

RSA is a public-key encryption algorithm that uses two keys: a public key for encryption and a private key for decryption. The algorithm is based on the difficulty of factoring large prime numbers, providing a high level of security. The mathematical foundation of RSA can be summarized as follows high-resolution images, where RSA's slow encryption time can hinder its practical usability[1]. Despite the promising results from these studies, the integration of **RSA with IWT** remains underexplored in the literature. Given that IWT is a lossless transform, it has the potential to overcome the limitations posed by DWT-based systems, particularly in scenarios where

preserving the exact original image is critical[7]. Moreover, by combining the security advantages of RSA with the data-preserving capabilities of IWT, a more efficient and robust image encryption system can be developed. In this paper, we aim to address this gap by proposing a novel image encryption system based on **RSA and IWT[4]**. Our system leverages RSA for its robust security features and IWT for its lossless data transformation, ensuring that the original image can be perfectly reconstructed after decryption. By integrating these two techniques, we strive to enhance both the security and performance of image encryption, offering a solution that is suitable for the secure transmission of high-fidelity images over the internet. The proposed system not only provides strong encryption but also minimizes computational overhead, making it more practical for real-time applications.

1. *Select two prime numbers, p & q.*
2. *Compute $p \times q=n$.*
3. *Compute the Euler's totient function $(p-1) \times (q-1) = \phi(n)$*
4. *Choose d, such that $d \times e \equiv 1 \bmod \phi(n)$ the public key is (e, n) and the private key is (d, n).*
5. *Encryption: a message m is encrypted as*

$em \bmod n = c$.

6. *The ciphertext c is decrypted as*

$dc \bmod n = m$.

Integer wavelet Transform (IWT):

Wavelet transform are widely used for signal and image processing due to their ability to decompose signals into different frequency components. The integer wavelet transform (IWT) is a specific type of wavelet transforms that ensures lossless data recovery by working with integer values. This makes it ideal for applications that require exact reconstruction of the original data, such as image encryption. In the proposed method, IWT is applied to the image to decompose it into frequency subbands. The transformed coefficients are then passed through the RSA encryption algorithm to protect the image data[1].

Proposed encryption scheme:

The encryption scheme can be summarized as follows:

1. Image preprocessing: The input image is first converted into its grayscale form if it is a color image. This simplifies the encryption process by reducing the data dimensions[2].
2. IWT decomposition: the grayscale image is then decomposed using the integer wavelet

transform (IWT), producing several subbands representing different frequency components of the images.

3. RSA encryption: the coefficients from IWT decomposition are treated as message data and encrypted using the RSA algorithm. The public key is used for encrypting the coefficients.
4. Ciphertext image generation: The encrypted coefficients are recombined into a transformed image. This image is the encrypted version, ready for transmission.

Decryption process:

The decryption process follows the reverse of the encryption process:

1. RSA decryption: The encrypted image coefficients are decrypted using the private key of the RSA algorithm.
2. Inverse IW: the decrypted coefficients are then passed through the inverse IWT to reconstruct the original image.
3. Image reconstruction: The original grayscale image is restored, and if needed, converted back to its original color form.

Simulation and implementation

In this experiment, we aim to implement and test a secure image encryption and decryption process using RSA (Rivest-Shamir-Adleman) and Inverse Wavelet Transform (IWT). The method ensures that image data can be protected during transmission and later reconstructed without any significant loss of quality. Below are the steps and results obtained during the encryption and decryption phases.

Tools: python, Python Imaging Library (PIL) or Pillow, PyCryptodome.

1. **Image Preparation**

To begin, the image used in this experiment is a colored image of Lena (Figure 1), which is widely used for image processing tasks. We first read the image in its original RGB format. The image is then divided into its red (R), green (G), and blue (B) channels for further processing.

***Figure 1**: Original Lena image before encryption.*

2. Encryption Process

After separating the image into its RGB channels, each channel undergoes the following steps:

- IWT Transformation: We apply the Inverse Wavelet Transform (IWT) to each channel to break down the image into multi-resolution subbands.
- Data Flattening: The resulting IWT coefficients from each channel are flattened into a single array to simplify the encryption process.

RSA Encryption: Using the public key generated via RSA, we encrypt the data in 128-byte chunks. RSA ensures the security of the flattened image data during transmission.

3. Decryption Process

The decryption process is the reverse of the encryption:

- Data Decryption: The binary file containing the encrypted data is read and decrypted using the RSA private key. The encrypted chunks are decrypted back into the original flattened IWT coefficients.
- IWT Reconstruction: After decrypting the data for each channel, we reassemble the coefficients into the proper shape and perform the inverse IWT on each channel to reconstruct the R, G, and B channels.
- Image Reassembly: The reconstructed RGB channels are combined to recreate the original image.

The decrypted image is then saved and displayed (Figure 2).

4. Results

***Figure 2**: Lena image after decryption.*

In this implementation, the reconstructed image retains the original quality, and the encryption-decryption process is validated. The steps were confirmed by observing the successful decryption of the image without any visible artifacts or color loss.

Experimental Resulte

To validate the proposed encryption scheme,
experiments were conducted on various standard test images, including Lena, Cameraman, and Peppers. The encryption process was evaluated based on key metrics such as encryption time, decryprtion time, and image quality after decryption (measured using PSNR-Peak Signal-to-Noise Ratio).

1. Encrption and decryption times:

The encryption times for different images size were compared with traditional RSA-based images encryption. The proposed method showed a significant reduction in encryption time due to the use of IWT, which reduces the overall data size before encryption.

2. Image quality analysis:

After decryption, the quality of the reconstructed images was evaluated using PNSR. The results indicated that the decrypted images were nearly indentical to the original images, with minimal loss in quality. This highlights the effectiveness of the IWT in preserving the images integrity during the encryption process.

Conclusión and future Works

This paper presenta aan integrated aproach to image encryption using the RSA alogrithm and the Integer Wavelet Trabsform (IWT). The combination or these techniques offers a robust solution for securing image data while maintaining high-quality imagereconstruction. The experimental results demonstrate that the proposed method significantly reduces encryption and decryption times compared to traditional methods while ensuring the confidentiality and integrity of the image data. In the future work, we aim to explore the integration of other cryptographic alogrithm with wavelet transforms to further enhance the security and efficiency of image encryption. Additionally, the application of this method in real-time systems, such as medical imaging or surveillance, will be investigated.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[2] C. S. Burrus, R. A. Gopinath, and H. Guo, Introduction to Wavelets and Wavelet Transforms: A Primer, Prentice Hall, 1997.

[3] J. Daemen and V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, Springer, 2002.

[4] W. Sweldens, "The lifting scheme: A custom-design construction of biorthogonal wavelets," Applied and Computational Harmonic Analysis, vol. 3, pp. 186-200, 1996.

[5] A. E. Ismail, "A hybrid cryptosystem for image encryption using RSA and wavelet transform," International Journal of Computer Applications, vol. 75, no. 7, pp. 26-32, 2013.

[6] A. Chandra and A. Pandey, "A Hybrid Image Encryption Scheme Based on AES and Discrete Wavelet Transform (DWT)," International Journal of Computer Science and Information Security, vol. 15, no. 10, pp. 231-238, 2017.

[7] A. Gupta, S. Rani, and S. Kumar, "RSA-Based Image Encryption with Discrete Wavelet Transform," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 9, no. 5, pp. 22-30, 2019.

[8] Y. Wang, X. Wu, and Y. Zhang, "Lossless Image Encryption Using Integer Wavelet Transform and RSA," Journal of Visual Communication and Image Representation, vol. 26, pp. 123-131, 2015.