IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 13 Issue 02, February 2026
ISSN (Online) 2348 – 7968 | Impact Factor – 6.72
www.ijiset.com

Image Security on Cloud using Enhanced RSA Cryptosystem and Residue Number System

Peter Awonnatemi Agbedemnab[1], Abdul-Ganiwu Yahaya[2*], Edem Kwadzo Bankas[3] & Kassim Korah Nantomah[4]

[1,2,3]School of Computing and Information Sciences, University of Technology and Applied Sciences Navrongo, Ghana.
[2]Gambaga College of Education, Gambaga, Ghana.

Abstract
Digital image is among the most widely used data type transmitted over the cloud, making the development of efficient and secure methods high priority. To address this need, numerous techniques have been proposed to enhance the security of image transmission. In most applications, cryptography, widely regarded as secure and reliable route has been used to enhance the security of digital data which includes images. Popular among the techniques is the Rivest Shamir Adleman (RSA) cryptosystem; however, the primary limitation is the computational complexity involved in the power of factorisation. As a result, there is a need for creative approachs that can improve both computational efficiency thereby making it lightweight for adaptability in the cloud environment without compromising on security. In this paper, we propose a modified version of the RSA by using residues from the Residue Number System (RNS) instead of prime numbers to generated a lightweight cryptosystem. By leveraging on the inherent features of the RNS, we are able to enhance the existing RSA to securely safeguard the confidentiality and integrity of data, particularly images, making it suitable for securing information on cloud systems. The generation of public and private keys is determined by the selected moduli, which also contain the secret information. These moduli are highly sensitive, and any slight modification can lead to corrupt information upon decryption. The results demonstrate significant improvements over the best-known state-of-the-art methods in terms of computation, power consumption, and runtime. Additionally, the proposed approach is capable of identifying and correcting errors that may occur in the encrypted data.

Keywords: *Cryptography, Cloud, RSA Cryptosystem, Data Security, and Residue Number System.*

1. Introduction

In every digital system, encryption and access control are fundamental techniques for ensuring data confidentiality. Managing cryptographic keys becomes a crucial and challenging task in security management, particularly in large organizations where encryption is used to safeguard data confidentiality. Data is considered meaningful when its quality aligns with its intended purpose. Cryptography originates from the Greek words "cryptos," meaning "secret," and "graphein," meaning "writing" [1]. Cryptography is crucial when there is a need to safeguard critical and confidential information [1]. Over the past few decades, cryptography has become one of the most widely used methods for concealing data from unauthorized parties. Cryptographic algorithms provide a secure medium for data transmission, ensuring that even if a malicious user attempts to intercept the data, they cannot extract any useful information due to its encrypted form. Modern cryptography is significantly more complex than its historical origins. While it was initially used to protect diplomatic and military secrets, today, cryptography has evolved to secure vast amounts of electronic data stored and transmitted across global corporate networks. It plays a vital role in maintaining the privacy of sensitive personal, financial, medical, and e-commerce data, preventing it from falling into the wrong hands. Since the 1970s, the field of modern cryptography has seen numerous advancements, with the development of robust encryption-based protocols and new cryptographic applications.

While the cloud model undoubtedly offers long-term viability and significant benefits for organizations and governments, its widespread adoption depends on several key factors aligning to deliver the reliability, desired outcomes, and trust necessary to truly spark a "cloud revolution [2]." Cloud computing has emerged as one of the fastest-growing technologies today, offering numerous benefits, including greater cost efficiency and reliability in the business industry. Its significance cannot be overlooked, as IT organizations increasingly recognize cloud computing as a key concept for providing internet-based services that share resources at minimal cost [3]. Consumers can utilize cloud services without the need for physical hardware investments, with storage capacity that can be scaled according to computing needs. Additionally, the latest applications are accessible at any time, eliminating the need to spend time and money on installations, making it a more economical option [4].

In 1978, Rivest, Shamir, and Adleman introduced a cryptosystem known as RSA, which has since become one of the most widely adopted cryptographic algorithms. It is based on the mathematical properties of large prime numbers and the computational difficulty associated with factoring the product of two large prime. RSA employs asymmetric encryption framework, utilizing a pair of keys: a public key for encryption and a private key for decryption. The security of the system relies on the infeasibility of deriving the private key from the public key within a practical time frame, given sufficiently large key sizes. Due to its robustness and reliability, RSA has been widely adopted in numerous cryptographic applications, including secure data transmission, digital signatures, electronic commence, and secure communication protocols on the internet. [5]

The primary role of a computer is computation, which fundamentally relies on numbers. However, the efficiency of the arithmetic unit and processor is limited by the inherent constraints of binary and decimal numeral systems. These limitations have spurred ongoing research aimed at enhancing the speed, reducing the area cost, and minimizing the power consumption of digital systems. A key challenge in improving digital system performance from a computational perspective is the carry propagation problem, which is a characteristic issue of conventional number systems like binary and decimal numbering system. Carry propagation hampers the efficiency of arithmetic operations and is a major factor contributing to the internal delay in processors built with these traditional number systems [6] [7] [8]. Consequently, there is a growing recognition of the need to adopt unconventional number systems to achieve faster computation.

The Residue Number System (RNS) is a carry-free number system that does not assign weights and is defined by a set of relatively prime integers, $m_1, m_2, \dots, m_n$ known as moduli sets. The condition for these moduli sets is that the greatest common divisor (gcd) of any two distinct moduli, m_i and m_j is 1 for $i \neq j$. The system's Dynamic Range (DR) is represented as $[0, M]$, where $M = \prod_{i=1}^{n} m_i$, ensuring that any integer $X \in [0, M]$ has a unique RNS representation, denoted by the ordered set of residues $x = (x_1, x_2, \dots x_n)$, where $x_i = [X]m_i$ for $i = 1,2, \dots$ RNS has been applied in various fields, including cryptography. Recently, extensive research has focused on improving the security of messages using the RSA cryptosystem. This has been accomplished by either combining it with other methods or modifying the existing cryptosystem. However, these methods alone may not be sufficient to conclusively prove the superiority of an algorithm. In the context of cloud security, the growing demand for large volumes of data and applications across personal, healthcare, commercial, and governmental sectors has become increasingly prevalent. Protecting the vast amounts of data stored in cloud storage from unauthorized tampering is crucial.

This paper presents a promising approach to enhance the security of hidden messages through a cryptographic scheme by incorporating a carry-free arithmetic platform, which is designed to resist adversarial attacks, increase processing speed, reduce area usage, minimize power consumption, and ensure the integrity and confidentiality of data. The proposed scheme can be seamlessly implemented in various hardware security modules, meeting the needs of cloud providers who manage vast amounts of data and applications. The rest of the paper is organised as follows: in section 2, we present a review of some existing literature on the subject matter, section 3 is where the detailed algorithms and mathematical procedure for the proposed scheme is presented. This also includes the simulated implementation of the proposed scheme. In section 4, we present the results obtained from the implementations as well as an analysis of the results by comparing it to existing similar schemes. The paper is then concluded in section 5.

2. Literature Review

Digital image encryption methods based on asymmetric cryptosystems have attracted considerable interests from researchers and experts. Consequently, a wide range of such algorithm have been proposed and developed. Data concealment techniques differ depending on the nature of the information being hidden and the level of stability required during the data manipulation. An effective data hiding scheme should be capable of embedding information under specific constrains such that the presence of the hidden data remains imperceptible to external observers, while ensuring that the data is seamlessly integrated into the media and remain intact across various file formats [9]. An encryption algorithm that combines the RSA algorithm with the Shimizu Morioka chaotic system to enhance image security. The method employs a confusion-diffusion technique for image encryption. The process is carried out in two stages: fist, a permutation process is applied, while the Shimizu-Morioka system's chaotic properties are used to shuffle the pixel values of the plaintext image. This shuffling is governed by specific initial conditions and control parameters, which act as the encryption key, disrupting pixel correlations. In the second stage, the RSA

algorithm is applied to the shuffled image, resulting in the cipher image. To decrypt, the operations are reversed using the same initial conditions and control parameters from the encryption phase. This approach provides robust encryption and offers resistance against both statistical and brute-force attack [10]

The inventor of edge detection proposed a technique for embedding large amount of textual data within the edges of colour image. Edges were chosen as the embedded regions because they offer high storage capacity while maintaining low detectability. The method employs a 3 × 3 window-based edge detection approach and uses first-component modification techniques to embed the text. As a result, the proposed method achieves both high embedding capacity and excellent image quality [11]. A study that employs a modified RSA encryption techniques for image encryption. This approach applies the RSA cryptosystem a widely recognized public key encryption method to both grayscale and colour image using MATLAB. The RSA algorithm, known for its robust security, is implemented to perform image encryption and decryption. The process involves converting the image into a matrix and dividing it into sub-blocks of size n × m. A modified RSA encryption and decryption algorithm is then applied individually to each sub-block, ensuring secure image processing. This method enhances image encryption security through the effective implementation of the RSA algorithm [12].

A study that integrated the generalized Arnold map with the RSA algorithm for image encryption was proposed. In this approach, RSA is used to generate the parameters of the generalized Arnold map. Subsequently, the generalized Arnold map, together with permutation and diffusion processes is applied to the original image to produce the cipher image. To minimized transmission overhead, the scheme incorporates compressive sensing in conjunction with the RSA algorithm [13]. A novel method was proposed for securing multi-colour image. During the encryption process, the colour image is first decomposed into its red, green, and blue (RGB) components. Each component is then encrypted using the RSA cryptosystem. Subsequently, the fractional discrete cosine transform is applied to the partially encrypted image. Finally, the Arnold transform is employed to further scramble the processed image, producing the final cipher image. [14]. An algorithm was proposed to enhance both the transmission speed and security of images transmitted over the internet or computer networks. The proposed cryptosystem utilizes a modified K-shuffling techniques to scramble image pixels, followed by decomposition using the Residue Number System (RNS). Simulations were conducted using two different moduli sets in combination with the modified k-shuffle method. The results demonstrate that both configurations effectively secure image without information loss. Moreover, the overall encryption and decryption time depends on the selected moduli set, with set requiring fewer bits and less memory for representation exhibiting strong resistance to statistical attacks, including brute-force attacks, correlation analysis, information entropy evaluation, and histogram analysis [15]

3. Proposed Method

The goal of this proposed approach is to create a robust and highly secure method for exchanging information, safeguarding confidential and private data from attacks and unauthorized access. To achieve the desired level of security and resilience, this method integrates the strengths of both cryptography and Residue Number System.

In the proposed method, we utilize the Residue Number System (RNS) alongside the Traditional Chinese Remainder Theorem (CRT) on an image file. The message is first encrypted using a Enhance-RSA encryption technique, the image are initially converted into their RNS equivalents using the forward conversion. The enhance RSA public key encryption is applied on the converted image pixel values, matrix permutation is performed on the image pixel to scramble the image pixel values. The enhance RSA key decryption is then applied on the scramble image pixels and reverse conversion is carry-out using CRT to obtain the plain image.

In this approach, all the three shared secret keys are required to reconstruct the original image. By doing so, it enhances message security while allowing the use of relatively small size-image. While the RSA public key cryptosystem is well-regarded for its security, it is often slower than symmetric key alternatives due to its reliance on modular arithmetic. Consequently, our primary focus has been on enhancing the speed of the RSA algorithm to strengthen computer security. The encryption process, represented by the equation $c = m^e \, mod n$ is computationally intensive, prompting us to develop optimizations to streamline the RSA cryptosystem. Our approach introduces a faster RSA-RNS algorithm for both data encryption and decryption. Unlike other methods that may require computationally intensive processes, our technique emphasizes comprehensives protection that operates in real-time on any image data.

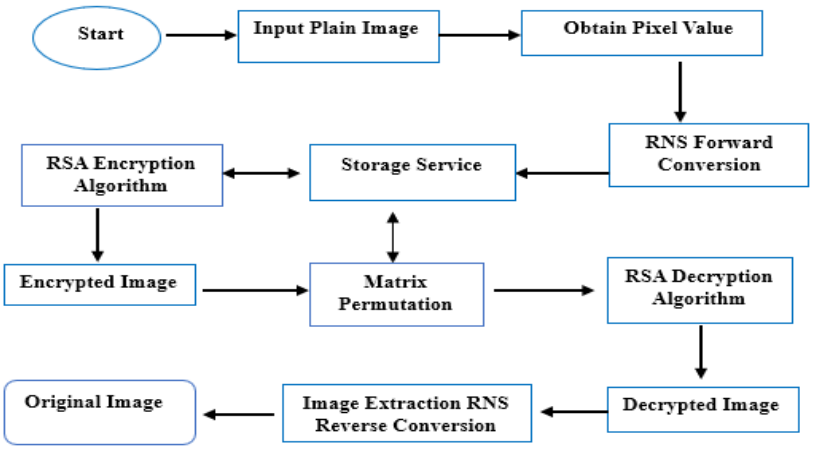

Fig. 1 Flow diagram for the proposed scheme

Figure 1 represent the architecture of the proposed cryptosystem, the start utilized image imported from a text file. This image is converted into pixel values through a three-layer process (namely RNS data conversion). Subsequent, the Enhance RSA encryption is applied to the pixel values ensuring the convert transmission of the message. The sender sent the message in an encrypted form to the receiver. The receiver retrieves the message using the private keys, the cipher text is deciphered to get the message and transform the message using RNS reverse conversion to get the original image.

3.1. Implementation on the cloud

In this system, the user who sends the data is referred to as the sender, while the user who receives the data is the receiver. Although the sender and the receiver can something be the same individual, in this case, they are distinct users. Both the sender and the receiver can access the system through either a single cloud service provider or a multiple provider. Regardless of the setup, the cloud service providers communicate via a shared interface. This interface interacts with a storage service that maintains a bidirectional connection with the user interface used by the sender. The user interface retrieves the required data from the storage service, which uses the Enhanced RSA algorithm to secure the data. The Enhance RSA algorithm generates both the public and the private keys based on a selected set of moduli. Before data is stored, it is encrypted using the public key, while the private key remains confidential. The encrypted data is later retrieved from the storage service and sent to the receiver, who decrypts it before gaining access to the original information.

3.2. Algorithm for the Proposed Scheme

Let $\mathcal{P} \rightarrow \mathcal{E} \in Z_h$ and $p = 2^n - 3$, $q = 2^n - 1$ and $r = 2^2 + 1$ where $p \neq q \neq r$ are relatively prime numbers from the moduli set $\{2^n - 3\ ,\ 2^n - 1,\ 2^2 + 1\}$ for $h = pqr$ and $\varphi(h) = \frac{(p-1)(q-1)(r-1)}{2}$ for $n = 4$ chose e such that $\left(1 < e < \varphi(h)\right)$ so that the $\gcd\left(e,\ \varphi(h)\right) = 1$ and $d \leftarrow e^{-1} mod \varphi(h)$ for $ed \equiv 1\left(mod\varphi(h)\right)$, compute $e_1 = emod(p-1)$, $e_2 = emod(q-1)$ and $e_3 = emod(r-1)$ and for $d_1 = dmod(p-1)$, $d_2 = dmod(q-1)$ and $d_3 = dmod(r-1)$ where the public keys are (h, e_1, e_2, e_3) and the private keys are $(p, q, r, d_1, d_2, d_3,)$. Now compute the residue pixels $b_1 = Pmodm_1$, $b_2 = Pmodm_2$ and $b_3 = Pmodm_3$ where b_1, b_2 and b_3 are the residue of the pixels (P) from the individual modulus m_1, m_2, m_3 which are selected . the value of $b_3 = Pmodm_3$ where b_1, b_2 and b_3 represents the pixels of the share m_1, m_2, m_3, encryption is performed on this pixel values and matrix permutation is applied on these pixel values before the decryption process.

3.2.1 Forward Conversion Process

The moduli set $\{2^n - 3\ ,\ 2^n - 1,\ 2^2 + 1\}$ is employed in the implementation. These moduli are relatively co-prime and possess a notable characteristic. For the given data M, where $C_i = M^e < h$, it passes through the encryption stage, during which the encryption system will transform M^e into a different form, represented as $(r_i < h)$. As a result, the proposed scheme is well- suited and inherently designed to enhance the throughput.

Consider the calculation of a residue of an arbitrarily integer X with respect to a modulus m. Given that X can be represented as an n-bit binary number $(x_{n-1}, x_{n-2}, \dots x_0)$, its residue with respect to m can be represented as:

$$|X|_m = |x_{n-1}x_{n-2}x_{n-3}, \dots x_0|_m \quad (1)$$

Which can also be computed as;

$$|X|_m = |2^{n-1}x_{n-1} + 2^{n-2}x_{n-2} + 2^{n-3}x_{n-3}+, \dots 2^0x_0|_m \quad (2)$$

such that;

$$|X|_m = ||2^{n-1}x_{n-1}|_m + |2^{n-2}x_{n-2}|_m + |2^{n-3}x_{n-3}|_m, \dots + |2^0x_0|_m|_m \quad (3)$$

Since x_1 can only be either 0 or 1, computing the residue of X involves evaluating the values $|2^i|_m$ which are then added up with a reduction relation to the modulus. To find the remainder of the integer X, we can treat the binary representation of the input as 3n-bit value and calculate the partial reduction for each subset of n bits using the moduli set $\{2^n - 3, 2^n - 1, 2^n + 1\}$. This involves computing three residues, each corresponding to one of the moduli [16].

The schematic diagram for the forward converter is shown in the figure below.

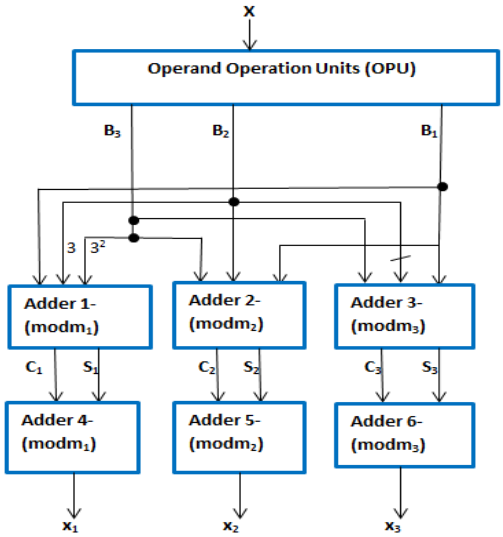

Figure 2: Block diagram of Forward Converter for the Proposed Scheme

Conversion Process

The reverse conversion is implemented in order to minimize the delay generated. The moduli set used can invade the imbalance issue due to its utilization of either n or (n + 1) −bit width to represent the large residue within the moduli set. Employing this approach, greater parallelism is achieved without introducing significant hardware redundancy. To invert an RNS number using the given moduli set, we utilize a simplified Chinese Remainder Theorem (CRT) via mathematical

manipulation. For the given moduli set, if $(x_n, x_{n-1}, \dots x_1)$ are the residue representation then, any integer X can be uniquely express in the form as

$$X = \sum_{i=1}^{n} a_i x_i u_i mod M \quad (4)$$

Were

$$M = \prod_{i=1}^{n} m_i \,, a_i = \frac{M}{m_i}, u_i = a_i^{-1} mod m_i$$

And

$$x_i = (x_1, x_2, x_3, \dots x_n)$$

Therefore

$$X = \left| a_1 \left\lceil |u_1 \times x_1|_{m_1} \right\rceil + a_2 \left\lceil |u_2 \times x_2|_{m_2} \right\rceil + \cdots a_n \left\lceil |u_n \times x_n|_{m_n} \right\rceil \right|_M \quad (5)$$

$$= |A + B + C|_M \quad (6)$$

Were

$$A = |(2^n - 1)(2^n + 1)(2^{n-1})|_{m_1} = (x_{1,0}, x_{1,n-1}, \dots x_1 x_0)$$

$$B = |(2^n - 3)(2^n + 1)(2^n - 3)|_{m_2} = (x_{2,0}, x_{2,n-1}, \dots x_2 x_{2,n-1} \dots x_2 x_0)$$

$$C = |(2^n - 3)(2^n - 1)(2^n)|_{m_3} = (x_{3,0}, x_{3,n-1}, \dots x_3 x_{3,n-1}, \dots x_3 x_0$$

Since the representation of x_1, x_2 and x_3 have a bit length of n. Then the above can be computed as the sum of 3n-bit formed by concatenation and rotation. The two-level architecture realized by the Chines Remainder Theory (CRT) method can lead to an efficient implementation of RNS to binary converter of the moduli set $M = \{2^n - 3, 2^n - 1, 2^n + 1\}$.

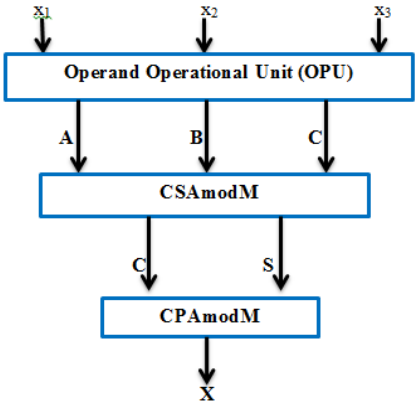

Figure 3: Flow diagram of the Reverse Conversion for the Proposed Scheme.

The proposed moduli set deploys carry save adder (CSA) and carry propagated adder (CPA). An optimized structure has been proposed by several authors [17] [18] [19] [20] on modulo $(2^n - 1)$ and $(2^n + 1)$. The circuit area required by this structure is given as $A_{CSA} = n \times A_{FA}$ for modulo $(2^n - 1)$ and $A_{CSA} = n \times A_{FA} + A_{not}$ for $(2^n + 1)$ where n represents the number of bits and A_{FA} and A_{not} are a Full Adder and a Not gate respectively. The critical path is given by the delay of a FA for modulo $(2^n - 1)$ and for modulo $(2^n + 1)$ a further delay of Not gate is registered resulting in theoretical critical path of $\Delta_{CSA} = \Delta_{FA} + \Delta_{Not}$. For modulo $(2^n - 3)$ no delay overhead is experience and overall latency [16].

4. Results and Discussion

Given that the proposed algorithm is tailored for cloud applications, it is imperative to minimize both the data insertion time and the time required for secret data retrieval. Fortunately, our solution has effectively achieved this goal.

4.1 Performance Evaluation

The experimental setup was developed and refined using MATLAB programming. Multiple datasets were generated and integrated into a graphical user interface to improve user interaction and responsiveness. The systems were designed to leverage various components within the MATLAB environment to produce results. This innovative system particularly focused on the influence of the Residue Number System on data hiding and RSA encryption as the foundational stage of data security.

The proposed method was tested multiple time using various RGB colour images of different size. In every case, the correlation coefficient between the original and the decrypted image was consistently one (1), indicating that the method reliably produces accurate results without any loss or distortion of information. Additionally, it is evident that the difference in appearance between the encrypted images and the original images is minimal. From a security perspective, the proposed approach is highly robust. An attacker would need in-depth knowledge of the moduli set, including the sequence of individual moduli and the value of 'n'. Additionally, access to both the private and public keys would be required to decrypt the encrypted image. This multi-layered security framework significantly enhances the scheme's resistance to unauthorized access. Figure 4, shows an illustration of encryption and the decryption of the proposed scheme.

Figure 4: shows the encryption and decryption of an Eagle.

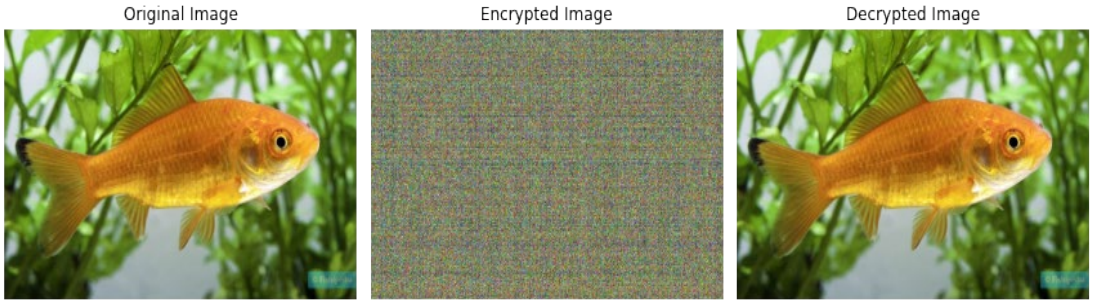

Figure 5: shows the encryption and decryption of the Goldfish.

4.2 Histogram Analysis

The histogram of an image shows the distribution of pixel intensity values, indicating how many pixels fall within each intensity level. For a cipher image, security against statistical attacks is strengthened when its histogram conceals any trace of the plain image and differ substantially from it. As illustrated, the histograms of the plain image and its cipher image are completely distinct. This clear divergence ensures that the cipher image's histogram provides no information about the original image, demonstrating the robustness of the proposed system against statistical attacks. This is shown in figure 6.

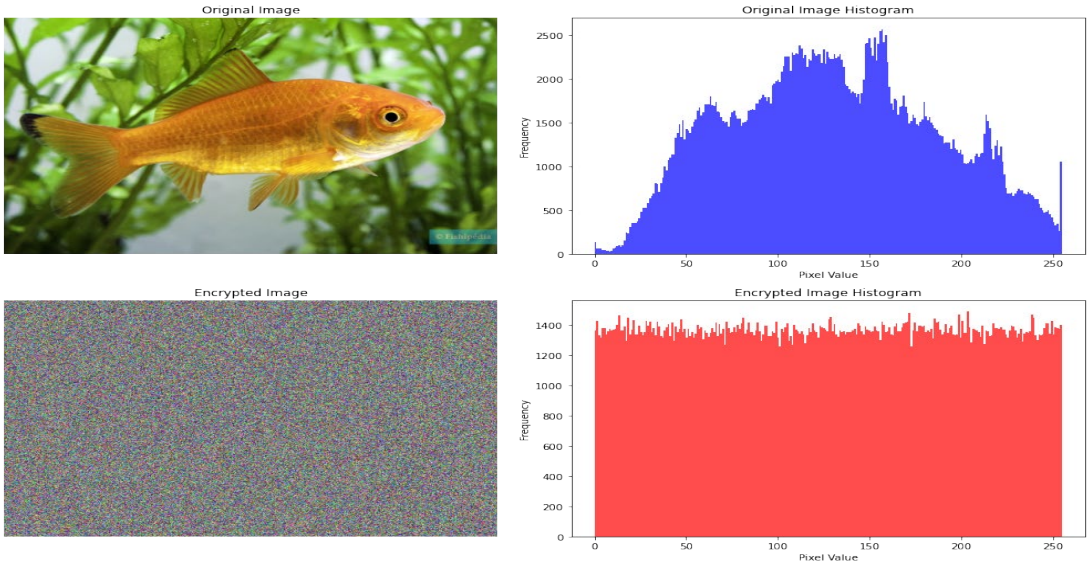

Figure 6: shows the histogram of plain image and the cipher image.

4.3 Visual Degradation

Visual distortion in image can be quantify using

i. **Number of Pixel Changing Rate (NPCR) and Unified Average Intensity (UAI):** The NPCR quantifies the percentage of differing pixels between two images, whiles UACI evaluate the average intensity of pixels between the two images [21]. The scrambled cipher-image is utilised to perform the difference measurement since, at this stage, both the plain and the cipher image share the same dimensions. The high percentage value of the NPCR metrics indicate significant randomisation of pixel positions. Additionally, the UACI values demonstrate that nearly all pixel gray-scale values in the cipher-image have been altered compared to those in the plain image, thereby making it significantly harder to decipher the plain image from the cipher-image.

The Peak Signal-to-Noise Ratio (PSNR) and the Means Square Error (MSE): The Mean Square Error represents the cumulative square differences be tween the original and the compressed images, whereas Peak

Signal-to-Noise Ratio measures the peak error, lower MSE value indicates smaller error, whiles lower PSNR value suggest greater visual degradation.

To carry out this analysis, a MATLAB function was written to compute the NPCR, UAI, MSE and PSNR values, which is represented in the *figure 7*.

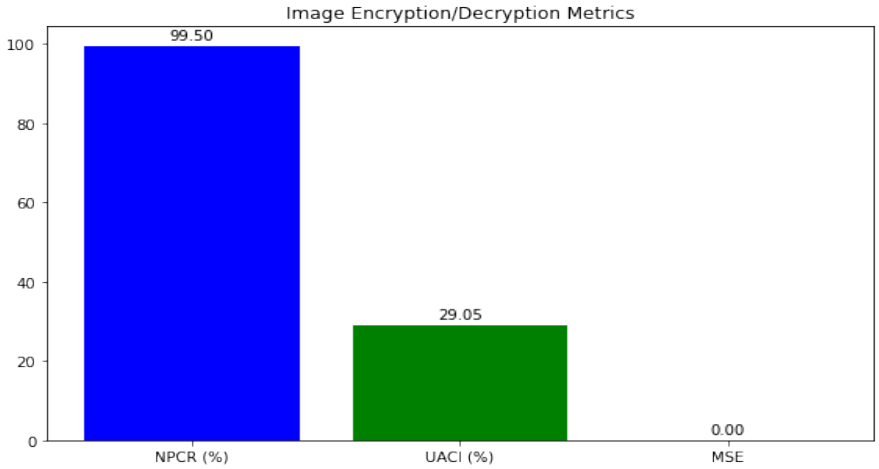

Figure 6: shows the histogram of image quality of a Goldfish.

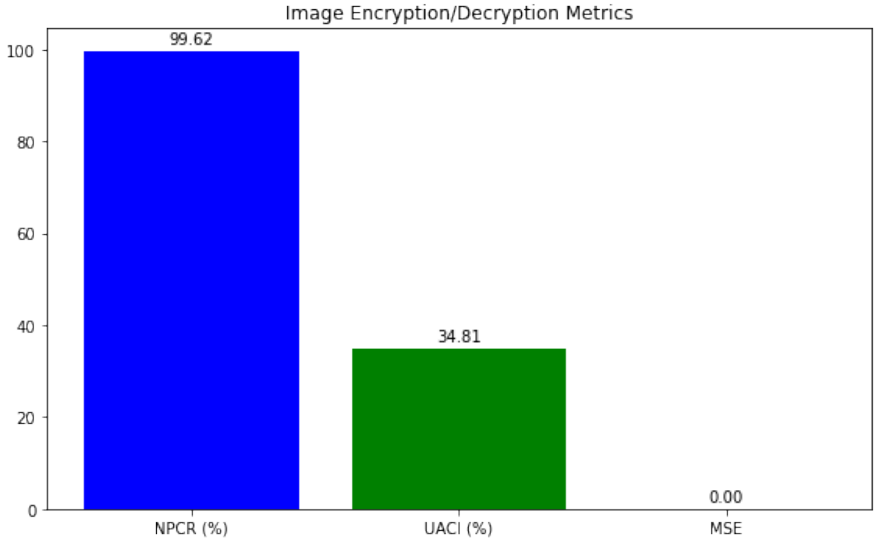

Figure 6: shows the histogram of image quality of an Eagle.

Theoretical Evaluation

The experimental setup involved processing sample image sourced from image file. These images were initially converted into their Unicode equivalents. Following this, the forward conversion process was applied to encrypt the image, dividing it into three residues, that represents the pixel values. Subsequently, the Enhance RSA encryption was employed with matrix permutation before transmitting the cipher image to the intended recipient. The recipient used the corresponding private keys to decrypt the data. To retrieve the original image, a reverse conversion process was conducted, utilizing the same moduli set that was employed during the initial forward conversion. This reverse conversion process enabled the retrieval of the image.

4.5 Comparative Analysis

The Enhance RSA (EH-RSA) encryption was implemented using the Residue Number System to convert text into an image file, allowing for discreet data transmission. The tables presented the average time required for encryption, decryption and

data extraction. Experimental results show that the EH-RSA approach significantly outperforms the conventional RSA cryptosystem in terms of computational speed, as well as the method proposed by [22] [23]. Attempting to breach the system requires knowledge of the message's initial position, the encryption method employed, and the insertion technique. This complexity makes it significantly challenging for potential infiltrators, thereby enhancing the security of the system.

Table 1: Comparing average Encryption time of the Proposed Scheme with Other Schemes

Cover Image	RSA Encryption (Time)	3-D-RSA Encryption (Time)	MD-RSA Encryption (Time)	EH-RSA Encryption (Time)
Eagle	9.81865	0.89554	0.97831	0.68764
Monkey	9.63074	0.88564	0.981225	0.33677
Gold Fish	9.60733	0.89654	0.98218	0.33781
Pepper	9.54888	1.87584	2.43215	0.69164
Lena	9.50828	0.89087	0.98765	0.33441
Baboon	9.75871	0.87965	0.99876	0.35147
Red-roses	9.61927	0.89665	0.99805	0.31145
Dog	9.56801	0.89765	1.43812	0.31332

Table1 provides a comparative analysis of the Average encryption times for Conventional RSA Cryptosystem (RSA), RSA algorithm with 3-D chaotic system (3-D RSA) Techniques, Modified RSA Encryption (MD-RSA) Technique and Enhance RSA (EH-RSA) Proposed Technique. The results from this table enable us to evaluate the efficiency of encryption in these scenarios. Notably, when we apply the Residue Number System alongside the traditional Chinese Remainder Theorem to RSA encryption with the chosen moduli set, a substantial reduction in encryption time is observed. This improvement is visually represented in Figure 7.

Table 2: Comparing of the average Decryption time of the Proposed Scheme with Other Schemes

Cover Image	RSA Decryption (Time)	3-D-RSA Decryption (Time)	MD-RSA Decryption (Time)	EH-RSA Decryption (Time)
Eagle	9.30895	0.44987	0.57213	0.28856
Monkey	9.44301	0.44327	0.56439	0.34545
Gold Fish	9.37791	0.45336	0.57094	0.34002
Pepper	13.32207	0.58769	0.68907	0.34272
Lena	9.30294	0.43421	0.58743	0.34644
Baboon	9.44602	0.49786	0.58790	0.35119

In Table 2 provides a comparative analysis of the Average decryption times for RSA with RNS, RSA algorithm with 3-D chaotic system (3-D RSA) Techniques, the Modified RSA Encryption (MD-RSA) Technique, and the time recorded for RSA without the RNS technique. The results clearly highlight a significant reduction in decryption time when applying the Residue Number System in combination with the traditional Chinese Remainder Theorem to RSA with the chosen moduli set. This substantial improvement is visually depicted in Figure 8.

Extraction time refers to the duration required to recover the original image. The cumulative time needed for this process is considerably more significant when using RSA with RNS, RSA algorithm with 3-D chaotic system (3-D RSA) Techniques, and the Modified RSA Encryption (MD-RSA) Technique, than the time recorded for RSA without the RNS technique. This data is detailed in Table 3 and visually depicted in Figure 9.

Table 3: Comparing of the average Extraction time of the Proposed Scheme with Other Schemes

Cover Image	RSA Extraction (Time)	3-D-RSA Extraction (Time)	MD-RSA Extraction (Time)	EH-RSA Extraction (Time)
Eagle	5.16450	0.36754	0.40923	0.18756
Monkey	5.02793	0.41129	0.49254	0.20545
Gold Fish	5.04051	0.47501	0.54301	0.0.21002
Pepper	5.01641	0.52752	0.53094	0.38274
Lena	5.01482	0.41253	0.50651	0.21654
Baboon	5.02233	0.39874	0.48907	0.21889
Red-roses	5.01106	0.38972	0.49084	0.20498
Dog	5.01943	0.37903	0.48129	0.20101

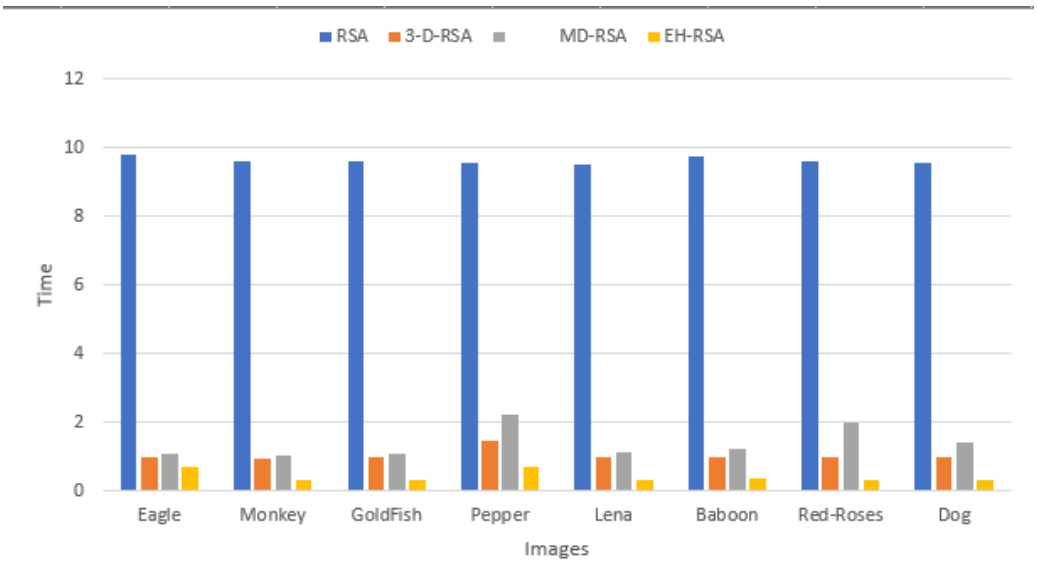

Figure 7. Chart showing the time for Encryption of the Proposed Scheme and with Other Methods

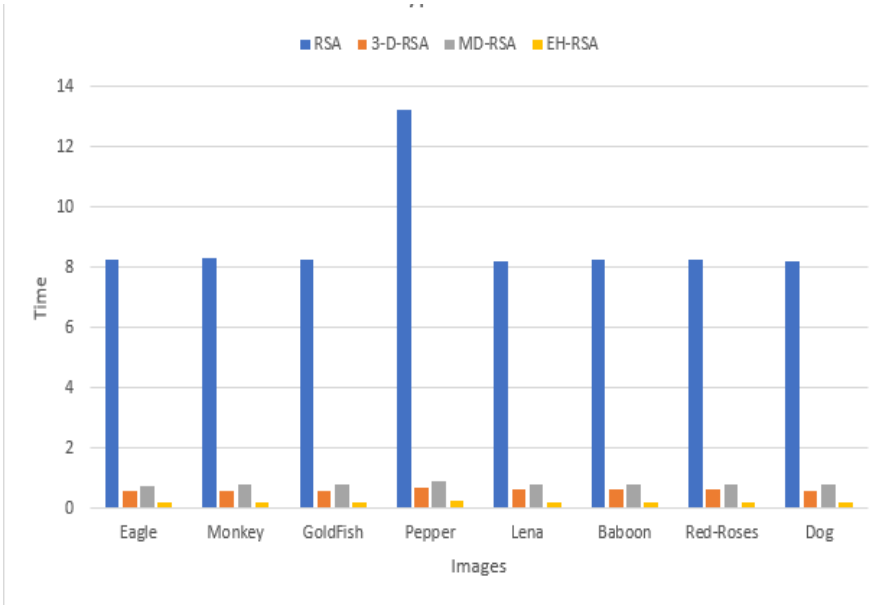

Figure 8. Chart showing the time for Decryption of the Proposed Scheme and with Other Methods

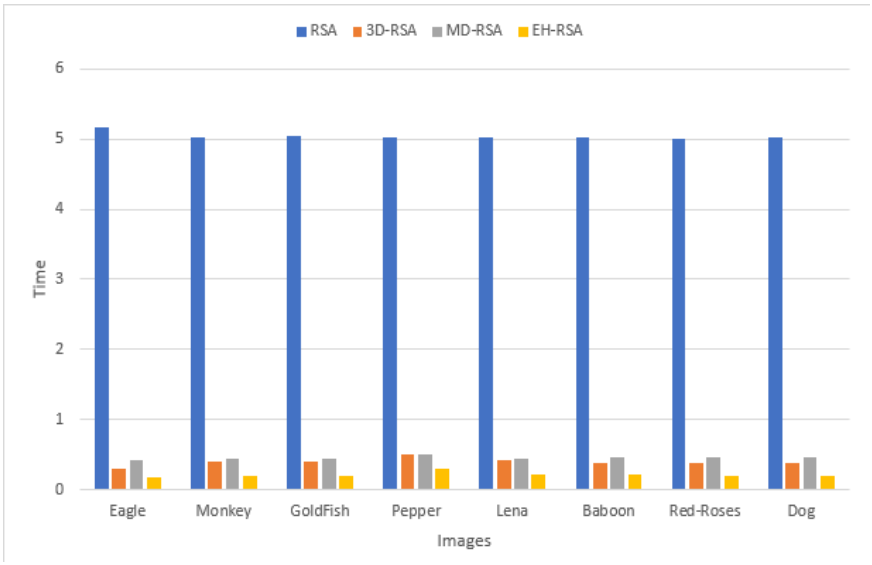

Figure 9. Chart showing the time for Extraction of the Proposed Scheme with and Other Methods

5. Conclusion

Safeguarding data from unauthorized access is a prominent concern in today's swiftly evolving realm of communication. Among the techniques we have explored, one of the most effective involves combining the efficient RNS with the RSA algorithm and leveraging on the Traditional Chinese Remainder Theorem. This combination results is exceptionally robust and secure systems, with the added benefit of distorting data in the image file by employing these efficient EH-RSA techniques, we successfully addressed the issue of slow encryption and decryption. Our approach utilized RSA encryption with a dual-layer security strategy, revealing that the decryption process with EH-RSA is significantly faster compared to other schemes. Additionally, incorporating EH-RSA into the decryption process greatly enhances the speed of data extraction from the image file.

References

[1] R. Verma & A.K. Sharma, (2020). "Simulation-Based Comparative Analysis of Symmetric Algorithms," *International Journal of Advanced Research in Computer Science,* vol. 11, no. 0976-5697, pp. 64-69.

[2] H. Li, L. Zhu, M. Shen, F. Gao, X. Toa & S. Liu, (2018). "Blockchain-based data preservation system for medical data," *Journal of medical systems,* vol. 42, no. 141.

[3] I. Ahmed, (2019). "A brief review: security issues in cloud computing and their solutions," *Telkomnika (Telecommunication Computing Electronics and Control),* vol. 17, no. 1693-6930, p. 2812~2817.

[4] A. Almtrf, Y. Alagrash & M. Zohdy. (2019). "Framework modeling for User privacy in cloud computing," in *Annual Computing and Communication Workshop and Conferenc*, USA.

[5] U. H. Mir, D. Singh & P. N. Lone (2022). "Color image encryption using RSA cryptosystem with a chaotic map in Hartley domain," *Information Security Journal: A Global Perspective,* no. 31(1), pp. 49-63.

[6] ME. Xie & L. Qiao, (2022). "Exploring the Application of Computer Intelligence Algorithms in Logistics and Supply Chain Management," in *Proceedings of the 7th International Conference on Intelligent Information Processing* , Shenyang,

Liaoning, China.

[7] BK. Patel & J. Kanungo, (2022). "Area Efficient Diminished 2n-1 Modulo Adder using Parallel Prefix Adder," *Journal of Engineering Research - ICAPIE ,* no. ICAPIE Special Issue,, pp. 8-18,

[8] MV Valueva, NN Nagornov, PA Lyakhov GV Valuev & NI Chervykor (2020). "Application of the residue number system to reduce hardware costs of the convolutional neural network implementation," *Mathematics and Computers in Simulation,* vol. 177, pp. 232-243.

[9] Antonio, H., Prasad P., & Alsadoom A. (2019). " " Implementation of cryptography in steganography for enhanced security"," *Multimedia Tools and Applications,* no. 78(23), p. 32721–32734.

[10] Yakubu H, Joseph S., & Yahi N (2023). "RGB Image Encryption Algorithm Using RSA Algorithm and 3D Chaotic System," *Arid Zone Journal of Basic and Applied Research,* Vols. 2(2),, no. 811-2881, pp. 151-167.

[11] WS. Farhani & A. Dwiharzoandis (2022) "Steganografi Metode Least Significant BIT (LSB) Pada Mpeg Spatial Audio Object Coding," *Rang Teknik Journal,* vol. 5, no. 2.

[12] KDM Alsabti & HR. Hashim (2016). "A new approach for image encryption in the modified RSA cryptosystem using MATLAB," *Global Journal of Pure and Applied Mathematics,* vol. 12, no. 973-1768, pp. 3631-3640.

[13] K Jiao, G Ye, Y Dong , X Huang & J He (2020). "Image Encryption Scheme Based on a Generalized Arnold Map and RSA Algorithm," *Security and Communication Networks,* vol. 2020(1), no. 9721675, p. 14.

[14] V Guleria, S Sabir & DC Mishra (2020). "Security of multiple images RGB image by RSA cryptosystem combined with FrDCT and Arnold transform," *Journal of Information Security and Applications,* vol. 54, no. 102524.

[15] IZ Alhassan, ED Ansong, G Abdul-Salaam & S Alhassan (2020). "Enhancing Image Security during Transmission using Residue Number System and k-shuffle," *Earthline Journal of Mathematical Sciences,* vol. 4, no. 2, pp. 399-424.

[16] AG Yahaya, PA Agbedennab & EK Bankas (2024). "A Modified RSA Cryptosystem for Cloud Security Using Residue Numbers," *International Journal of Computer and Organization Trends,* vol. 14, no. 1, pp. 12-18.

[17] A Almtrf, Y Alagrash & M Zohdy (2019). "Framework modeling for User privacy in cloud computing," in *Annual Computing and Communication Workshop and Conferenc* , USA.

[18] BK. Patel & J. Kanungo, (2022). "Area Efficient Diminished 2n-1 Modulo Adder using Parallel Prefix Adder," *Journal of Engineering Research,* no. ICAPIE Special Issue,, pp. 8-18.

[19] F Begum & GR Sulhoju (2021). "Types of Steganography for Secure Data Maintenance," *Annals of the Romanian Society for Cell Biology, ,* vol. 25 (6), p. 2144–2159.

[20] M. K. Chande, (2021). "Modified ElGamal signature with secret key pair and additional random number," *Serdica Mathematical Journal,* no. 47, p. 85–290.

[21] A. Oluwakemi, A. Christaina, T. Abikoye, (2024). "An Improved Machine Learning-Based Framework for Fake News Detection," in *Proceedings of the 3rd International Conference on ICT for National Development and Its Sustainability*, Ilorin, Nigeria.

[22] KDM Alsabti & HR. Hashim (2016). "A new approach for image encryption in the modified RSA cryptosystem using MATLAB," *Global Journal of Pure and Applied Mathematics,* no. 12(4),, p. 3631–3640., 2016.

[23] Yakubu H, Joseph S., & Yahi N. (2023). "RGB Image Encryption Algorithm Using RSA Algorithm and 3D Chaotic System," *Arid Zone Journal of Basic and Applied Research,* Vols. 2(2), , no. 2811-2881, pp. 151-167, 2023.