# Pixel-based Homomorphic Residue Number System Scheme for Privacy-Preserving Neuroimaging Datasets Encryption and Decryption

[*1]Usman, M.A., [2]Usman, O.L. and [3]MuniyandI, R.C.
[1,2]Department of Computer Science, Tai Solarin University of Education, Ogun State, Nigeria, P.M.B. 2118 Ijagun, Ijebu-Ode.
[2,3]Research Centre for Cyber Security, Faculty of Information Science and Technology, University Kebangsaan Malaysia,43600 UKM Bangi, Selangor, Malaysia.
*Corresponding Author: morenikejiadebola@gmail.com

## ABSTRACT

Recently, there has been some interest in the development of a homomorphic privacy-preserving classification method for neuroimages based on the residue number system (RNS) and deep CNN. This paper describes the RNS homomorphic encryption system for neuroimages and analyses its security efficiency in relation to the moduli set $\{2^n - 1, 2^n, 2^{n+1} - 1\}$. The proposed system's security efficiency is evaluated using the histogram, key space, key sensitivity, and correlation analysis. The analysis results show that the proposed RNS homomorphic scheme is a fully homomorphic encryption (FHE) scheme capable of encrypting and decrypting neuroimages without sacrificing any inherent neural-biomarker features. The results also show that the scheme is resistant to statistical attacks like histogram, brute-force, correlation coefficient, and key sensitivity. Therefore, the proposed RNS-FHE scheme can be applied to any type of neuroimaging dataset and is suitable for the design of homomorphic privacy-preserving methods compared to the best-known state-of-the-art.

**Keywords:** Neuroimages; Residue number system; Homomorphic encryption; Neural-biomarkers; Cipher-images; Privacy-preservation.

## INTRODUCTION

Due to inherent neural-biomarker features that can be visualized and analyzed to reveal anatomical variations of the brain components, neuroimaging datasets (e.g., MRI scans) can serve as a source of diagnostic information for some critical brain-related neurological conditions and learning disabilities such as dyslexia, autism, and attention deficit hyperactivity (ADHD) (Lundervold & Lundervold, 2019; Płoński et al., 2017). In other words, the underlying neural-biomarkers features of these images could be used to differentiate between normal and abnormal cases in terms of structure, function, and activation patterns of brain tissue components (Shen et al., 2017; Usman & Muniyandi, 2020b), which have been shown to be sensitive as a result of recent increases in neuroimage data generation and cloud deployment of advanced machine learning (ML)/deep learning (DL) models as a service, and thus their privacy and confidentiality must be protected (Usman et al., 2021). This concept, known as privacy preserving classification, paved the way for remote image classification and aided in the faster dissemination of medical decisions (Alex et al., 2022; Boulemtafes et al., 2020; Kwabena et al., 2019; Usman et al., 2022).

Existing algorithms for securing medical images along transmission channels, such as chaotic map, Arnold's cat map, hybrid chaotic magic transform (HCMT), linear congruential generator (LCG), and Lanczo's algorithms (Gatta & Al-Latief, 2018; Koppu & Viswanatham, 2017), do not consider cloudbased classifications because most of them have distorted the pixels' locations of important features in the key region of interest (ROI), necessitating accurate and reliable results. To address the challenges posed by these algorithms, two types of privacy-preserving methods have been used alongside ML and DL, namely perceptual encryption (Chuman et al., 2019; Maekawa et al., 2018) and homomorphic encryption (Al Badawi et al., 2021; Dowlin et al., 2016). The former employs a block-based encryptthen-compress scheme to conceal image visual information and is compatible with certain traditional ML models such as ANN, SVM, decision trees, and so on, whereas the latter allows bitwise arbitrary homomorphic computations on cipher-images and is compatible with recent deep CNN architectures (Sirichotedumrong et al., 2019; Song et al., 2019). The residue number system (RNS) is an unweighted modular arithmetic 'carry-free' number system. Its parallelism, fault-tolerance, and fully

homomorphic properties have been used in a variety of digital signal processing (DSP) and cryptographic applications (Alhassan & Gbolagade, 2013; Muhammed et al., 2021; Navin et al., 2011; Usman et al., 2018). This paper focuses on the security model and analysis of cipher-neuroimages produced by (Usman et al., 2022)'s RNS-FHE scheme. The neuroimage encryption and decryption algorithms are proposed specifically with respect to the moduli set $\{2^n - 1, 2^n, 2^{n+1} - 1\}$ proposed by (Usman et al., 2022). This paper also shows that the proposed scheme can conceal and recover plain neuroimages without sacrificing any inherent neural-biomarker features.

The primary contribution of this paper is the development of novel encryption and decryption algorithms that are suitable for neuroimaging datasets. Additionally, this study demonstrates the security benefits of a methodical RNS-FHE scheme for designing an effective and efficient privacy preserving framework for these types of datasets.

## Background

### *A. Homomorphic Encryption*

Homomorphic encryption (HE) aims to allow certain arbitrary computations to be performed on ciphertext to produce an encrypted result that is also in cipher form. This result should be the same as the result of performing the same arbitrary computation on the plaintext (Gomathisankaran et al., 2013; Prasanthi & Smitha, 2017). To protect confidential data, HE schemes have a wide range of applications in medicine, education, and finance. A very simple illustration of the HE concept is a user requesting the server to add two integers, such as 5 and 12, as shown in Fig. 1. Assume that the two integers are encrypted as polynomial functions $P_1(x)$ and $P_2(x)$, respectively. The sum was computed by the cloud server as the third polynomial function $P_3(x) = P_1(x) + P_2(x)$, which the user decrypted to integer 17.

Due to its multiplicative property, RSA is regarded as the first HE used in the domain of cloud computing security since 1978. To ensure security, RSA employs a message padding process with random bits; however, the process results in the loss of homomorphic property. To counteract this process, several HE schemes based on public key cryptosystems were proposed (Bos et al., 2013; Gentry, 2010; Gentry & Halevi, 2011). Gentry (Gentry, 2009) presented the first FHE scheme design. Gentry's original scheme was inefficient, but subsequent studies produced significantly more practical schemes, leading to the classification of FHE schemes into three generations (Muhammed et al., 2021): The first generation of FHE is based on ideal lattices; the second and third generations are based on learning with error (LWE) and ring learning with error (RLWE) e.g., Gentry, Sahai, and Waters (GSW) scheme. However, in order to be useful in real-world applications, each of these FHE scheme generation needs to be improved further. The ability of a scheme to perform an infinite depth of arbitrary computations on encrypted data is referred to as FHE. To build FHE, however, a function of Boolean circuit must be designed with the capacity of performing infinite depths of arbitrary additions and multiplications, such that an untrusted cloud server can compute function $Enc(x+y)$ and $Enc(x \times y)$ from $Enc(x)$ and $Enc(y)$ with zero knowledge of $x$, $y$ and key $k$, satisfying the additive and multiplicative properties given in Equations (1) and (2):

Additive property:

$$Enc_k(x) + Enc_k(y) Mod\ N = Enc_k(x + y, Mod\ N) \quad (1)$$

Multiplicative property:

$$Enc_k(x) \times Enc_k(y) = Enc_k(x \times y, Mod\ N) \quad (2)$$

where $x, y \in \mathbb{Z}_N$ are plaintexts, $Enc$ is the encryption function and $k$ is the key generation function.

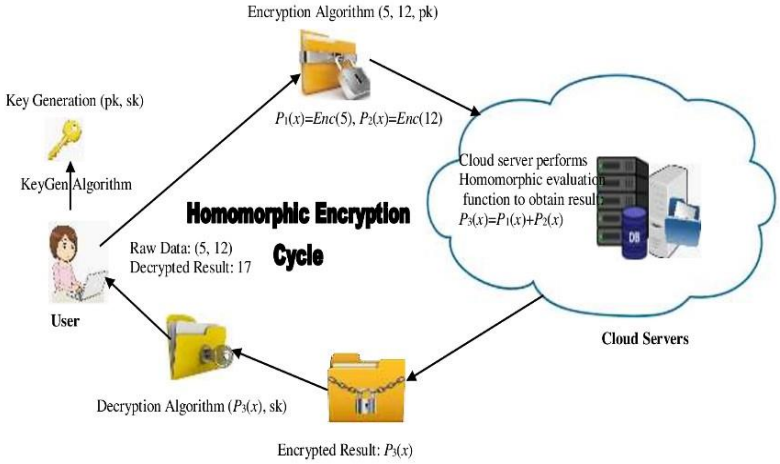



Fig. 1. Traditional homomorphic encryption cycle, *pk*-public key, *sk*-secret key.

### *B. Residue Number System and RNS-FHE Scheme*

The RNS is an unweighted number system that performs arithmetic computations in a secure, fast, parallel, fault-tolerant, and carry-free manner by replacing an integer number with its residues with respect to the given moduli set, thereby simplifying, speeding up, and allowing computations to run concurrently. RNS, in general, provides incredibly fast computer arithmetic due to inherent properties such as parallelism, modularity, non-critical failure adaptation, and carry-free operations (Abdulmumin & Gbolagade, 2017; Navin et al., 2011; Usman & Muniyandi, 2020a).

RNS is formalized as an *n*-tuple of pairwise relatively-prime moduli. If $m_i$ denotes the moduli set, then $m_i = \{m_1, m_2, \dots, m_n\}, GCD(m_i, m_j) = 1 \; for \; i \neq j$, where GCD stands for greatest common divisor. Equation (3) defines this system's dynamic range *M* as:

$$M = \prod_{i=1}^{n} m_i \tag{3}$$

Any integer number $X \in \mathbb{Z}_M$ can be replaced by its residue in the RNS as $X \xrightarrow{RNS} (x_1, x_2, \dots, x_n)$ using Equation (4) below:

$$x_i = X \; mod \; m_i = |X|_{m_i} \tag{4}$$

where $x_{i,i=1,2,\dots,n}$ are residues, $m_i$ is a module, and *M* represents system dynamic range which must be sufficiently large enough. The ring $\mathbb{Z}_M$ ranges from [0, M) called the legitimate range of *X*. If *X* and *Y* are two integer numbers bounded by the ring $\mathbb{Z}_M$ in RNS, then, Equation (5) can be used to compute the arbitrary homomorphic operation that maps their respective residues, implying that the RNS scheme is FHE.

$$X \oplus Y \xrightarrow{RNS} (x_1 \oplus y_1, x_2 \oplus y_2, \dots, x_n \oplus y_n), where \; \oplus \in \{+, -, \times\} \tag{5}$$

In the RNS cryptosystem, a binary-to-residue (BR) converter circuit is required to encode 8-bit grayscale values of pixels to their residues, while a residue-to-binary (RB) converter circuit is required as a reverse converter to obtain the original pixel values. Chinese remainder theorem (CRT) and mixedradix conversion (MRC) algorithms are the two reverse converter methods in RNS. Because of the computational overhead that characterized large modulo-M of CRT, this study adopted MRC, which is defined as follows (Abdul-mumin & Gbolagade, 2017): The integer equivalent of X can be computed from its residues $(x_1, x_2, \dots, x_n)$ using MRC with respect to a set of pairwise relatively-prime moduli $\{m_1, m_2, \dots, m_n\}$ as:

$$X = a_1 + a_2 m_1 + a_3 m_1 m_2 + \cdots + a_n m_1 m_2 m_3 \dots m_{n-1}, \tag{6}$$

where $a_{i=1,\dots,n}$, are the MRDs, which can be computed as follows:

$$a_1 = x_1,$$

$$a_2 = |(x_2 - a_1)|m_{1-1}|_{m_2}|_{m_2},$$

$$a_3 = |((x_3 - a_1)|m_{1-1}|_{m_3} - a_2)|_{m_3},$$

$$\vdots$$

$$a_n = |(\ldots((x_n - a_1)|m_{1-1}|_{m_n} - a_2)\ |m_{n--11}|_{m_n} - \cdots - a_{n-1})|m_{n--11}|_{m_n}| \quad ,(7)$$

$m_n$

## Proposed Method

According to (Usman et al., 2022)'s conceptual model of RNS-FHE privacy-preserving scheme, the RNS-FHE scheme encrypts neuroimages ($I_i$) by combining a secret key $k$ chosen from a set of keys ($K_i$) with random noise ($rm_i$) and a large $N$-prime number ($N_i$) with respect to moduli set $m_i = \{2^n - 1, 2^n, 2^{n+1} - 1\}$ to generate cipher-images ($C_i$), where $i$ = 1,2,...,$n$. The encryption process begins with the decomposition of the neuroimage into its pixels ($X_i$), each of which has an 8-bit grayscale value in the range [0, 255]. Each $X_i$ is then converted to cipher-pixel ($x_i$) based on RNS-FHE parameters with respect to $m_i$, which are then concatenated to form $C_i$, where $n \geq 3$ is the *pk* used by the RNS bitstream encoder during the encryption process. The decryption block employs the MRC as a reverse algorithm to generate a $N_i$-form of $C_i$ from the encrypted results using residues $x_i$ and $m_i$. Finally, the user will retrieve $I_i$ from $C_i$ using the generated $k$. Fig.2 depicts the flow of neuroimage encryption and decryption process summarized in Table 1 below:

*i. Pixel decomposition:*

$$I_i \leftarrow X_1 X_2 \ldots X_n \; where \; X_i \; is \; the \; pixel \; of \; neuroimage \; I_i \tag{8}$$

$$X_i \leftarrow x_{3n} x_{3n-1} x_{3n-2} \ldots x_1 x_0 \; for \; \forall x_i \in \{0,1\} \; where \; x_i \; is \; a \; bit$$

*Encryption Process:*

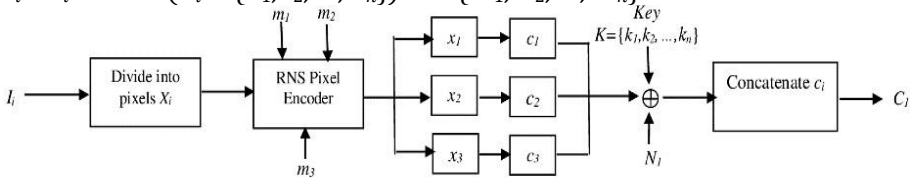
$$c_i \leftarrow Enc_K(X_i) = |\{X_1, X_2, \ldots, X_n\} \oplus \{k_1, k_2, \ldots, k_n\} * \{N_1, N_2, \ldots, N_n\}|_{\{m1, m2, \ldots, mn\}} \tag{9}$$

$$C_i \leftarrow concatenate(c_i) = x_1 x_2 \ldots x_n \tag{10}$$

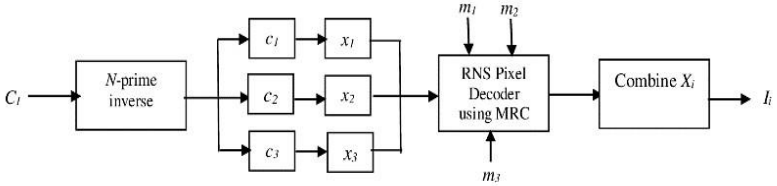
*ii. Decryption process:*

$$I_i \leftarrow Dec_K(C_i, m_i) = MRC(C_i) \oplus \{k_1, k_2, \ldots, k_n\} Mod\, m_i \tag{11}$$

$$N_i * C_i \leftarrow MRC(C_i = \{x_1, x_2, \ldots, x_n\}) Mod \{m_1, m_2, \ldots, m_n\} \tag{12}$$




(a). Pixel encoding




(b). Pixel decoding

Fig. 2. The flow of RNS-FHE cryptosystem.

Table 1. The homomorphic encryption and decryption algorithms for neuroimages.

| **Algorithm 1:** The Encryption Algorithm | **Algorithm 2:** The Decryption Algorithm |
|---|---|
| The algorithm for the encryption process is as follows:<br>1) Input $n$, $k$, $p$, $rm$ $N$ and plain neuroimage $I$<br>2) Obtain the values of $m_1$, $m_2$, $m_3$ using $\{2^n-1, 2^n, 2^{n+1}-1\}$<br>3) Decompose $I$ into $X_i$ using Equation (8)<br>4) For $i$ = 1 to $p$<br>Encode $X_i$ into the cipher-pixel $c_i$ using Equations (9)<br>Concatenate $c_i$ to obtain cipherimage $C$ using Equation (10) 5) Save $C$ | The algorithm for the decryption process is as follows:<br>1) Input $n$, $k$, $p$, $rm$, $N$ and cipher-image $C$<br>2) Obtain the values of $m_1$, $m_2$, $m_3$ using $\{2^n-1, 2^n, 2^{n+1}-1\}$<br>3) Obtain $N$-prime inverse $C$ and decompose into $c_i$<br>4) For $i = p$ down to 1<br>Extract $x_i$ from $c_i$ Mod $m_i$<br>Obtain $X_i$ from $x_i$ using Equations (6) and (7)<br>5) Recover the neuroimage $I$ by using Equations (11) and (12) 6) Save $I$ |

## Experimental Results and Discussion

The results of the RNS-FHE scheme performance analysis are summarized in this section. The simulations were run on a GPU system equipped with a 2.70GHz processor, 8.0GB RAM, and a 4 Core(s) Intel (R) processor. Grayscale neuroimages (Test1, Test2, Test3, Test4) of varying sizes were used to evaluate the efficiency of the proposed scheme. The proposed scheme was evaluated using visual inspection, encoding analysis, and security analysis.

### *A. Visual Inspection Analysis*

Fig. 3 depicts a visual comparison of a few selected neuroimages and their corresponding cipher forms. The results indicate that there is no similarity between the image pairs. The visual inspection analysis also reveals similarities in the histograms of plain and cipher neuroimages, indicating that the RNSFHE scheme recovers the neuroimages completely during the decryption process.

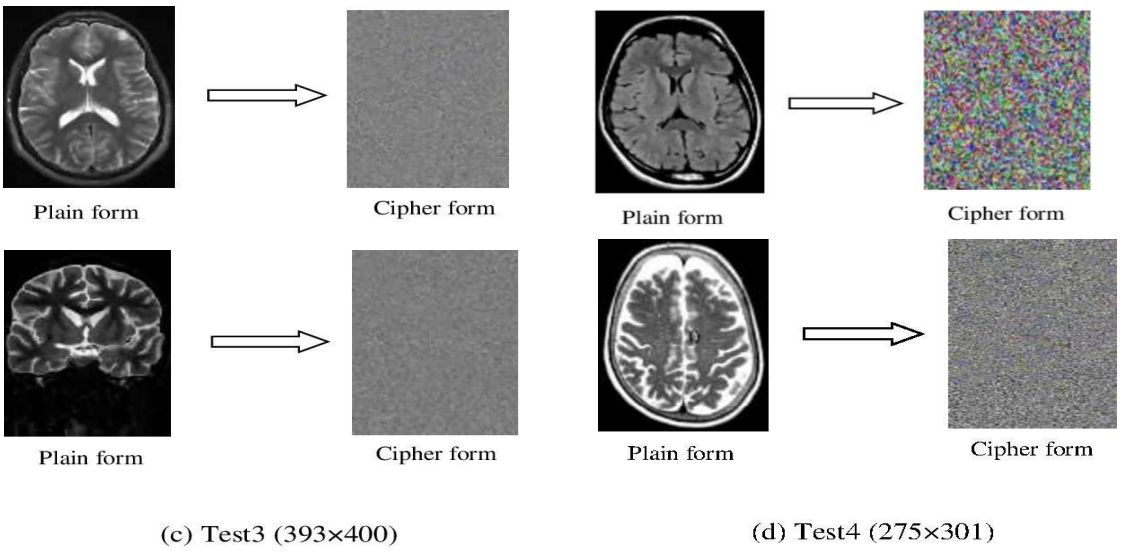



Fig. 3. Visual comparison of plain neuroimage and their cipher form ($n$=3, $k$=2, $p$=15)

### *B. Encoding Analysis*

Table 2 compares the size of plain neuroimages and their cipher forms. When $n = 3$, $m_i = \{7, 8, 15\}$, the pixel encoding component of the encryption process reduces the size of the cipher-images. Therefore, the computational time required for homomorphic operations is reduced, as is the disc space usage. On average, the proposed scheme reduced the size of cipher-images by 62%.

Table 2. Comparison of disc sizes between plain and cipher neuroimages

| Label (dimension) | Size (disk space usage) | | |
|---|---|---|---|
| | Plain form (kb) | Cipher form (kb) | Reduction ratio (%) |
| Test1 (256×256) | 407 | 146 | 62.13 |
| Test2 (512×512) | 380 | 107 | 71.84 |
| Test3 (393×400) | 216 | 89.7 | 58.47 |
| Test4 (275×301) | 163 | 72.6 | 55.46 |

### *C. Security Analysis*

A security analysis was performed to evaluate the proposed RNS-FHE scheme's effectiveness against some common image attacks such as histogram, key space, key sensitivity, and correlation coefficient. The experimental results demonstrated that the scheme is extremely secure against such attacks. As illustrated in Fig. 4, the histograms of test neuroimages differ completely from those of their corresponding cipher forms. This figure shows that the histogram of the cipher-image provides no information about the plain neuroimage. This implies that the scheme is resistant to statistical attacks.

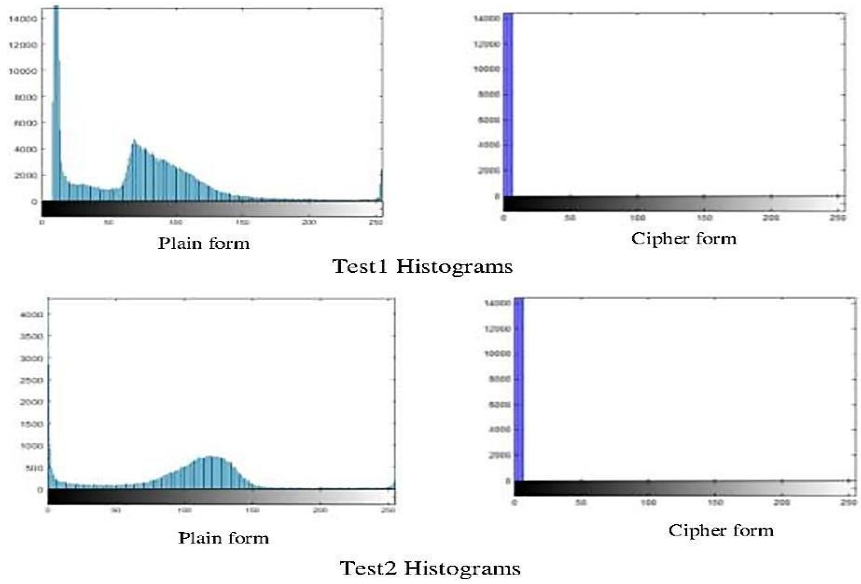



Fig. 4. Comparison of histograms: left column is plain form, right column is cipher form

For cryptosystems with a sufficiently large key space, a brute-force attack is computationally impossible. The proposed scheme makes use of three encryption keys ($n$,$k$,$p$). When $n = \{3,4,5,8,11\}$, the FPGA simulation of the scheme achieved an efficient pixel encoding with a time complexity of $O(n^3)$ (Usman et al., 2022; Usman & Muniyandi, 2020b). But, since $k \in \mathbb{Z}$ and $p = 1,2,3,...$, there is a wide range of options. Assume we use a 128-bit key for $k$ and $p$, as in DES. This gives us a total of $2^4 \times 2^{128} \times 2^{128} \cong 1.8527e + 78$ combination of options. If an adversary uses a 1000 MIPS computer to guess the combination, he or she will need $\frac{24 \times {}_6 2^{128} \times 2^{128}}{1000 \times 10 \times 3600 \times 24 \times 356} > 1000$ years. This time is long enough to resist brute-force attack.

The sensitivity to cipher key is another important feature of a good cryptosystem. A small change in the key value should result in a significant change in either the plain or cipher-image. When the value of one of the parameters is changed, the decrypted version of Test1 neuroimage (Fig. 3) is shown in Fig. 5. Therefore, the proposed scheme is extremely sensitive to the secrete keys.

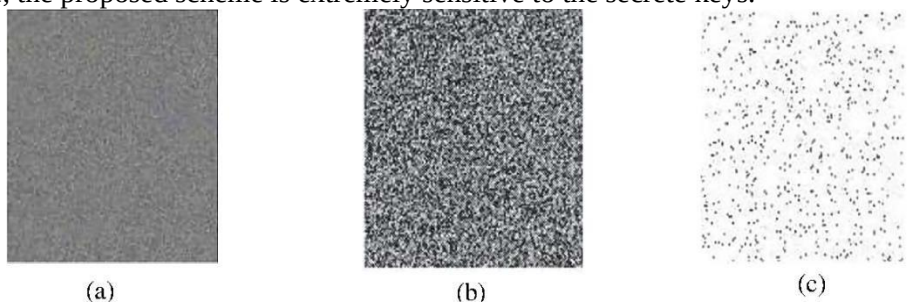



Fig. 5. Key sensitivity analysis (a) Decrypted Test1 with *k*=-3 (b) Decrypted Test1 with *p*=12 (c) Decrypted Test1 with *n*=5.

Finally, a good image-based cryptosystem should be able to generate cipher-images with significantly low correlation coefficient values. This enables the system to properly conceal the image's visual identity. For the correlation analysis, 500 adjacent pixels (vertical, horizontal, and diagonal) of the Test2 neuroimage and its corresponding cipher-image were chosen at random. Equation (13) was used to perform the computation:

$$r = \frac{Cov(x,y)}{\sqrt{I_p(x) * I_c(y)}} \tag{13}$$

where *x* is a plain image pixel and *y* is an adjacent cipher-image pixel, and $I_p$ and $I_c$ are functions with the condition that $r = -1 \leq r \leq 1$ and $r^2 \leq 1$. Table 3 demonstrates that the cipher-images have low correlation coefficient values between pairs adjacent pixels.

Table 3. Results of correlation analysis

| Iteration | Adjacent pixels | | |
|---|---|---|---|
| p | Vertical | Horizontal | Diagonal |
| 1 | 0.02931271 | 0.00382114 | 0.02571660 |
| 2 | -0.00317026 | 0.03184451 | 0.01788132 |
| 3 | -0.02462755 | 0.00111348 | 0.01973822 |
| 7 | 0.00887553 | -0.02502754 | -0.02490016 |
| 12 | 0.01659221 | 0.00114103 | 0.03442093 |
| 15 | -0.02411439 | -0.01222003 | 0.03510737 |
| 17 | 0.01659177 | 0.03312468 | 0.01222013 |

## Conclusion

This paper presents the security model and analysis of cipher-neuroimages generated by the RNS-FHE scheme, which was used in (Usman et al., 2022) to model homomorphic HoRNS-CNN for privacypreserving classification task. The neuroimage encryption and decryption algorithms are based on the powerful encoding/decoding strengths of RNS pixel bitstream encoder/decoder with respect to the moduli set $\{2^n - 1, 2^n, 2^{n+1} - 1\}$. The proposed scheme can conceal and recover plain neuroimages without sacrificing inherent neural-biomarker features. The experimental results show that fewer bits are required to represent the cipher-pixels. The results also show that the proposed RNS-FHE scheme is resistant to statistical attacks and highly sensitive to slight changes in the cipher keys, outperforming the state-of-the-art equivalent proposed by (Sirichotedumrong et al., 2019).

**References**

Abdul-mumin, S., & Gbolagade, K. A. (2017). An Improved Residue Number System Based RSA Cryptosystem. *International Journal of Emerging Technologies in Computational and Applied Sciences*, *20*(1), 70–74.

Al Badawi, A., Chao, J., Lin, J., Mun, C. F., Sim, J. J., Tan, B. H. M., Nan, X., Mi Aung, K. M., & Chandrasekhar, V. R. (2021). The AlexNet moment for homomorphic encryption: HCNN, the first homomorphic CNN on encrypted data with GPUs. *IEEE Transactions on Emerging Topics in Computing*, *9*, 1–13. https://doi.org/10.1109/TETC.2020.3014636

Alex, S., Dhanaraj, K. J., & Deepthi, P. P. (2022). Private Decision Tree-based Disease Detection with Energy-Efficiency at Resource-constrained Medical User in Mobile Healthcare Network. *IEEE Access*, *PP*, 1–15. https://doi.org/10.1109/access.2022.3149771

Alhassan, S., & Gbolagade, K. A. (2013). Enhancement of the Security of a Digital Image using the Moduli Set. *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, *2*(7), 2223–2229.

Bos, J. W., Lauter, K., Loftus, J., & Naehrig, M. (2013). Improved security for a ring-based fully homomorphic encryption scheme. In M. Stam (Ed.), *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 8308 LNCS* (Cryptograp, pp. 45–64). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-45239-0_4

Boulemtafes, A., Derhab, A., & Challal, Y. (2020). A review of privacy-preserving techniques for deep learning. *Neurocomputing*, *384*, 21–45. https://doi.org/10.1016/j.neucom.2019.11.041.hal02921443 HAL

Chuman, T., Sirichotedumrong, W., & Kiya, H. (2019). Encryption-then-compression systems using grayscale-based image encryption for JPEG images. *IEEE Transactions on Information Forensics and Security*, *14*(6), 1515–1525.

Dowlin, N., Gilad-Bachrach, R., Laine, K., Lauter, K., Naehrig, M., & Wernsing, J. (2016). Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. *33rd International Conference on Machine Learning, ICML 2016*, *1*, 342–351.

Gatta, M. T., & Al-Latief, S. T. A. (2018). Medical image security using modified chaos-based cryptography approach. *Journal of Physics: Conference Series*, *1003*(1), 1–6. https://doi.org/10.1088/1742-6596/1003/1/012036

Gentry, C. (2009). A Fully Homomorphic Encryption Scheme [Standford University]. In *Standford University* (Issue September). http://cs.au.dk/~stm/local-cache/gentry-thesis.pdf

Gentry, C. (2010). Computing Arbitrary Functions of Encrypted Data. *Communication of the ACM*, *53*(3), 97–105. https://doi.org/10.1145/1666420.1666444

Gentry, C., & Halevi, S. (2011). *Implementing Gentry ' s Fully-Homomorphic Encryption Scheme*. 1–29.

Gomathisankaran, M., Namuduri, K., & Tyagi, A. (2013). HORNS: A semi-perfectly secret homomorphic encryption system. *American Journal of Science and Engineering*, *2*(1), 17–23. https://doi.org/10.1109/icccnt.2012.6479590

Koppu, S., & Viswanatham, V. M. (2017). A Fast Enhanced Secure Image Chaotic Cryptosystem Based on Hybrid Chaotic Magic Transform. *Modelling and Simulation in Engineering*, *2017*, 1–13. https://doi.org/10.1155/2017/7470204

Kwabena, O. A., Qin, Z., Zhuang, T., & Qin, Z. (2019). MSCryptoNet: Multi-Scheme PrivacyPreserving Deep Learning in Cloud Computing. *IEEE Access*, *7*, 29344–29354. https://doi.org/10.1109/ACCESS.2019.2901219

Lundervold, A. S., & Lundervold, A. (2019). An overview of deep learning in medical imaging focusing on MRI. *Zeitschrift Fur Medizinische Physik*, *29*(2), 102–127. https://doi.org/10.1016/j.zemedi.2018.11.002

Maekawa, T., Kawamura, A., Kinoshita, Y., & Kiya, H. (2018). Privacy-Preserving SVM Computing in the Encrypted Domain. *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC 2018 - Proceedings*, *November*, 897–902. https://doi.org/10.23919/APSIPA.2018.8659529

Muhammed, K. J., Isiaka, R. M., Asaju-Gbolagade, A. W., Adewole, K. S., & Gbolagade, K. A. (2021). Improved Cloud-based N-Primes Model for Symmetric-based Fully Homomorphic Encryption using Residue Number System. In H. Chiroma, P. Abdulhamid, S M Fournier-Viger, & N. M. Garcia (Eds.), *Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics* (pp. 197–216). Springer, Cham. https://doi.org/10.1007/978-3-030-66288-2_8

Navin, A. H., Oskuei, A. R., Khashandarag, A. S., & Mirnia, M. (2011). A Novel Approach Cryptography by using Residue Number System. *ICCIT, 6th International Conference on Computer Science and Convergence Information Technology IEEE*, 636–639.

Płoński, P., Gradkowski, W., Altarelli, I., Monzalvo, K., van Ermingen-Marbach, M., Grande, M., Heim, S., Marchewka, A., Bogorodzki, P., Ramus, F., & Jednoróg, K. (2017). Multi-parameter machine learning approach to the neuroanatomical basis of developmental dyslexia. *Human Brain Mapping*, *38*(2), 900–908. https://doi.org/10.1002/hbm.23426

Prasanthi, B. G., & Smitha. (2017). Security Issues and Comparison of Existing Algorithms in Cloud to Support Multi-Cloud. *Adarsh Journal of Information Technology*, *6*(1), 33–36.

Shen, D., Wu, G., & Suk, H. (2017). Deep Learning in Medical Image Analysis. *Annual Review of Biomedical Engineering*, *19*(1), 221–248. https://doi.org/10.1146/annurev-bioeng-071516044442

Sirichotedumrong, W., Maekawa, T., Kinoshita, Y., & Kiya, H. (2019). Privacy-Preserving Deep Neural Networks with Pixel-Based Image Encryption Considering Data Augmentation in the Encrypted Domain. *Proceedings - International Conference on Image Processing, ICIP*, *2019-Septe*(September), 674–678. https://doi.org/10.1109/ICIP.2019.8804201

Song, B. K., Yoo, J. S., Hong, M., & Yoon, J. W. (2019). A Bitwise Design and Implementation for Privacy-Preserving Data Mining: From Atomic Operations to Advanced Algorithms. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/3648671

Usman, O. L., & Muniyandi, R. C. (2020a). A Framework for a Secure Brain Image Classification using Deep Learning and Residue Number System. *TEST Engineering & Management*, *83*(MayJune), 6323–6330.

Usman, O. L., & Muniyandi, R. C. (2020b). CryptoDL : Predicting Dyslexia Biomarkers from Encrypted Neuroimaging Dataset Using Energy-E ffi cient Residue Number System and Deep Convolutional Neural Network. *Symmetry*, *12*(5), 1–24. https://doi.org/10.3390/sym12050836

Usman, O. L., Muniyandi, R. C., Omar, K., & Mohamad, M. (2021). Advance Machine Learning Methods for Dyslexia Biomarker Detection: A Review of Implementation Details and Challenges. *IEEE Access*, *9*, 36879–36897. https://doi.org/10.1109/ACCESS.2021.3062709

Usman, O. L., Muniyandi, R. C., Omar, K., & Mohamad, M. (2022). Privacy-Preserving Classification Method for Neural-Biomarkers using Homomorphic Residue Number System CNN: HoRNS-CNN. *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*. https://doi.org/10.1109/ICBATS54253.2022.9759007

Usman, O. L., Olusanya, O. O., Adedeji, O. B., & Rufai, K. . (2018). Modelling a Secure Digital Image Cryptosystem using the Traditional Moduli Set. *TASUED Journal of Pure and Applied Sciences (IJOPAS)*, *1*(1), 197–207.