# ResSen: Imager Privacy Enhancement through Residue Arithmetic Processing in Sensors

Nedasadat Taheri†, Sepehr Tabrizchi†, Deniz Najafi‡, Shaahin Angizi‡ and Arman Roohi†

†School of Computing, University of Nebraska–Lincoln, Lincoln, NE, USA

‡Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ, USA

aroohi@unl.edu, shaahin.angizi@njit.edu

***Abstract*—The increasing use of image sensors across various domains poses notable privacy challenges. In response, this paper introduces a novel architecture, namely `ResSen`, to enhance the privacy and efficiency of traditional image sensors. Our approach integrates the Residue Number System (RNS) with in-sensor digital encryption techniques to forge a robust, dual-layer encryption mechanism. By embedding RNS within analog-to-digital converters (ADCs), we significantly strengthen privacy measures, effectively countering different violations and ensuring the integrity and confidentiality of data transmissions. A key feature of our system is its programmable key, which complicates unauthorized output prediction or replication, providing a superior encryption methodology. Notably, ResSen demonstrates that deactivating one of the moduli results in 25% bandwidth savings at the cost of minor accuracy degradation. This underscores the practicality and effectiveness of our sensor architecture in addressing the dual objectives of privacy enhancement and operational efficiency.**

***Index Terms*—processing-in-sensor, residue number system, image sensor, privacy**

## I. Introduction

A global network of 75+ billion IoT devices, including smart homes, smart cities, smart industries, wearables, and implantable systems for healthcare, is expected to reach $1100 billion by 2025. Intelligent IoT (IIoT) has recently gained significant attention due to its ability to sense, decide, and act by leveraging artificial neural networks (ANN). Through various sensors, such as CMOS image sensors (imagers), IIoT nodes collect and process data. Image sensor technology has revolutionized the way we capture and process visual information, offering wide applications from surveillance to medical imaging. Nevertheless, ANNs are significantly storage-/computation-intensive in achieving high accuracy and acceptable performance in visual systems, making them difficult to implement on edge devices with limited resources. Additionally, many vision applications require continuous monitoring or detection of anomalies by sensory systems, while low information density wastes bandwidth, storage, and computing resources. Because of that, these IIoTs still lack inherent intelligence and depend heavily on cloud-based decision-making, leading to emerging concerns regarding privacy and performance efficiency. The desire for privacy in the digital transmission of data has led to various solutions aimed at securing sensitive data against unauthorized access. Previous studies have explored a range of techniques, from advanced encryption protocols to secure transmission methods, in an effort to safeguard privacy. However, these solutions often face limitations, particularly in their ability to balance stringent privacy requirements with operational efficiency. For instance, heavy encryption methods, while effective in protecting data, can impose significant computational burdens on sensor systems, compromising their performance and responsiveness. Moreover, many existing strategies lack the flexibility to adapt to the dynamic nature of digital threats, leaving gaps that can be exploited by evolving hacking techniques. These challenges underscore the need for a more holistic and integrated approach to privacy that not only enhances privacy, but also maintains the efficiency and adaptability of image sensor systems. Incorporating the RNS and a light encryption technique significantly enhances privacy in image sensor technology. The RNS, by its design, offers a unique way to represent numbers, which inherently complicates the direct interpretation of data by unauthorized parties. When combined with a light encryption mechanism, the privacy of captured images is further bolstered. This dual approach ensures that even if the data were intercepted, reconstructing the original image would be extremely difficult without access to the specific RNS configuration and encryption algorithm used, thereby maintaining the integrity and confidentiality of sensitive data. The primary contributions of this research are outlined as follows:

- We proposed ResSen, an adaptive, high-performance image sensor for power-limited devices, enhancing privacy and performance through RNS.
- We developed an encryptor that enhances privacy by employing three efficient linear feedback shift registers to secure data processed with RNS.
- We designed a novel adaptive readout circuit that selectively toggles a specific modulus on or off to save bandwidth and power.
- We crafted a bottom-up evaluation framework to showcase the effectiveness of our design, applying it to a wide range of datasets, network types, and various scenarios, highlighting the performance advantages.

## II. Background

### A. RNS and cryptography

The RNS represents a powerful paradigm for enhancing the performance and efficiency of cryptographic systems. By its very nature, RNS enables parallel and carry-free computations, which are particularly advantageous for the implementation of cryptographic algorithms. This unique capability stems from its non-weighted number system, allowing for operations within each modulus to be executed independently, thereby significantly improving computational speed [1]. RNS

2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) | 979-8-3503-5411-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISVLSI61997.2024.00070

2159-3477/24/$31.00 ©2024 IEEE
DOI 10.1109/ISVLSI61997.2024.00070

is characterized by a set of $L$ mutually prime moduli $m_i$, for $i = \{1, \ldots, L\}$, where $L$ is at least 2. The total dynamic range, denoted as $M$, is obtained by multiplying all the moduli together. This allows any unsigned integer $X$ within the range $[0, M)$ to be uniquely represented by a tuple of residues $(x_1, \ldots, x_L)$, where each $x_i$ is the remainder of $X$ divided by $m_i$. The adoption of RNS can lead to hardware implementations of these algorithms that are not only faster but also more energy-efficient, addressing a critical need in devices where power consumption is a concern [2]. Furthermore, the application of RNS extends beyond performance improvements. It offers a pathway to resilience against certain types of hardware attacks, such as side-channel attacks, which exploit information leakage from physical implementations of cryptographic algorithms [3], [4]. The inherent parallelism and the carry-free nature of RNS-based[1] computations can obscure the correlation between cryptographic operations and physical side-channel signatures, like power consumption patterns or electromagnetic emissions, thus improving the privacy protection of cryptographic devices. However, the integration of RNS into cryptographic systems raises some challenges. Among these are selecting appropriate moduli sets, developing efficient converters between the conventional binary system and RNS, and managing operations traditionally complex in RNS, like division. Besides, the implementation of RNSed cryptographic systems must navigate the trade-offs between hardware complexity, power consumption, and the additional overhead introduced by conversions between number systems [5], [6].

### B. Privacy and Encryption

In the digital age, the transmission of images from sensors to cloud services poses significant privacy challenges, requiring robust measures to safeguard sensitive information against unauthorized access, use, or exposure. This issue is not only technical, but encompasses ethical and legal dimensions, underscoring the importance of maintaining the confidentiality and integrity of data through potentially vulnerable networks and systems. In this context, ensuring privacy goes beyond just preventing unauthorized access to data; it also includes safeguarding personal and sensitive information and respecting the consent and rights of data subjects throughout the entire lifecycle of the data. Despite advances in encryption techniques, secure transmission protocols, and data anonymization, there remains a considerable gap in addressing privacy comprehensively. These solutions, while crucial, often fall short in considering user-centric controls, transparency, and legal safeguards, highlighting the need for an integrated approach that combines technical robustness with ethical and legal considerations to enhance privacy protection in the transmission of sensitive data from sensors to cloud platforms [7].

Encryption plays a pivotal role in this landscape, serving as a fundamental mechanism for privacy by rendering data inaccessible and unintelligible to unauthorized parties without the appropriate decryption key. By rearranging the original sequence of data, encryption ensures the confidentiality of sensitive information throughout its lifecycle, from acquisition through transmission to storage. This is particularly essential in applications requiring stringent privacy measures, such as healthcare monitoring systems, secure communications, and scientific research. Moreover, the evolution of encryption methodologies aligns with the increasing complexity of cyber threats, reinforcing the need for advanced protective measures in our increasingly digital world. As data becomes an ever more valuable asset, the application of encryption extends beyond traditional realms into emerging technologies and platforms, such as cloud computing and sensors. In these environments, encryption not only ensures data privacy but also plays a critical role in establishing secure, trust-based interactions among devices, systems, and users. This expanded application highlights encryption's versatility and adaptability, making it indispensable in ensuring the confidentiality and integrity of data across a myriad of digital landscapes. The proactive integration of encryption into the fabric of digital communication and storage systems thus represents a forward-thinking approach to privacy [8].

[1]Hereafter, referred to as RNSed.

## III. ResSen Architecture

Image sensors are categorized into two main types: global shutter and rolling shutter. In systems employing a global shutter, each pixel is directly connected to its own ADC to convert the electrical voltage into a digital format. On the contrary, the rolling shutter technique involves connecting pixels to the ADC in a sequential manner, processing them row by row, which benefits low-power applications [9]. In our study, we present a new architecture designed to enhance the privacy and performance of traditional image sensors by leveraging **Res**idue arithmetic processing in the rolling shutter **Sen**sor, namely **`ResSen`**. The ResSen architecture comprises five components: a Command Decoder, a Focal Plane, aka a pixel array, a row selector, an adaptive residual readout, and an encryptor (Fig. 1). The command decoder acts as an intermediary, interpreting incoming control signals and translating them into specific actions for the sensor hardware, enabling dynamic control over the sensor's operations, such as pixel row activation, exposure adjustment, and readout initiation. In ❶, the pixel array of image sensors converts light into electrical voltage with respect to a captured image, each pixel including a photodiode and a capacitor. The Row Selector ❷, managed by the command decoder, enables the selection of specific pixel rows for processing by connecting them to source bias lines (SBLs) and facilitating their values' readout by the ADCs. Adaptive Residue Readout in ❸ optimizes the captured image by converting analog signals to digital ones using RNSed ADCs. It enables efficient resolution adjustment and privacy enhancement through selective channel deactivation, which is performed by the Channel Selector in ❹. It can disable/enable one (or more) specified modules. One of the most important components of our design is Encrypter (❺), which secures image data by applying XOR operations with

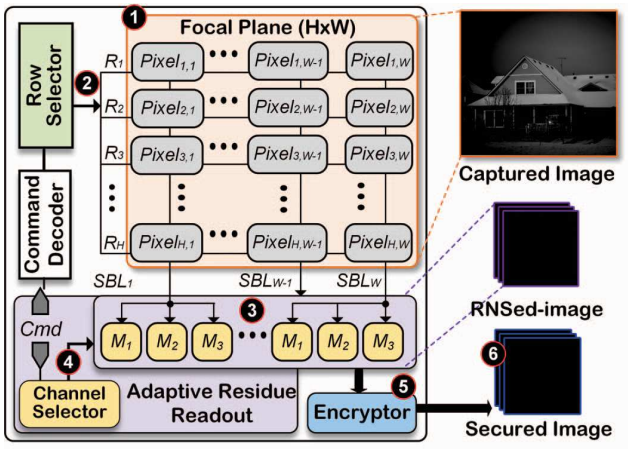


Fig. 1: The proposed ResSen Architecture.

pseudo-random sequences generated by shift registers, each tailored to a modulus, ensuring that each image row is uniquely encrypted before transmission. Consequently, the captured image is encrypted before sending it to the cloud/server ❻. All ResSen components and their functionalities are outlined in the following sections.

### A. Pixel Array

The pixel array, consisting of $H \times W$ pixels, retains its original functionality without any modifications to convert light intensity into an electrical voltage. As depicted in Fig. 1, the pixels' values are connected from $SBL_1$ to $SBL_W$ and read in a row-by-row manner. Figure. 2 depicts the structure and connection of six pixels. Each pixel comprises four transistors, denoted as $T_1$, $T_2$, $T_3$, and $T_4$, a photodiode ($PD$), and a capacitor ($CPD$). During the capture phase, by setting the $Rst$ signal to $V_{DD}$, all capacitors are charged. Subsequently, by activating $T_2$, the voltage stored in these capacitors is discharged through the photodiode's resistance, which is sensitive to light. Finally, $T_3$ generates a current based on the CPD's voltage upon activating $T_4$.

### B. Command Decoder

The command decoder functions as an intermediary to interpret incoming control signals and translate them into specific actions/sequences that the image sensor hardware must execute. This component is crucial for enabling dynamic configuration and control of the sensor's behavior, including the activation of pixel rows, the adjustment of exposure settings, and the initiation of readout processes. The decoder achieves this by mapping each command signal to a corresponding set of control lines or switches within the sensor architecture. As a result, the command decoder facilitates precise control over the sensor's functionality, allowing for the efficient capture of images under varying conditions. This capability is essential for optimizing image quality and performance across a wide range of applications, from consumer electronics to advanced scientific imaging.

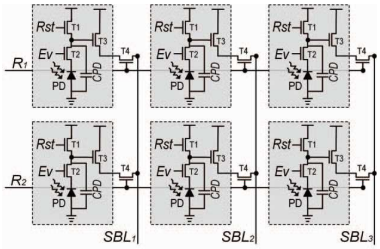

Fig. 2: The arraignment of $2 \times 3$ pixels.

### C. Row Selector

Another main component, even in conventional imagers, is the Row Selector, shown in Fig. 1. Command Decoder manages this unit and enables row selection ($R_n$). As illustrated in Fig. 2, two row-lines, $R_1$ and $R_2$, are connected to the $T_4$ transistors. For example, activating $R_1$ connects all pixels in the first row to the Source Bias lines ($SBLs$) and allows the ADCs to read their values.

### D. Adaptive Residue Readout

Since we target a low-power vision sensor, an 8-to-14-bit image format capable of generating 256—to 16384 unique values is sufficient. The resolution of the ADC has a significant impact on both image quality and energy consumption. To exploit the strength of RNS encoding and mitigate the overhead of RNS converters, our previous RNSed ADC is utilized to improve area and power efficiency. By integrating the RNS into the design of folding ADCs, our novel approach allows for high-speed and high-resolution conversions efficiently by employing multiple folding circuits, each corresponding to distinct prime moduli within the RNS. This methodology not only simplifies the hardware architecture but also minimizes power consumption, enhancing the overall efficiency of digital signal processing systems. In this paper, we consider the moduli set of $\{2^n+1,\ 2^{n+1}-1,\ 2^{n+1}\}$, where $n \in \{2,\ 3,\ 4\}$. The higher value of $n$ offers a larger dynamic range, allowing the system to obtain more accurate images up to 14-bit. To do so, we utilized our previously proposed RNSed ADC to enhance speed and resolution without an exponential increase in complexity and power usage. In this situation, putting $n = 2$ employs moduli of $\{5,\ 7,\ 8\}$, establishing a specific range of 280, which closely approximates the 256-value range for 8-bit conventional images. The RNSed ADCs within the adaptive residue readout are connected to a channel selector so that one or more moduli can be turned off as needed. This capability not only enhances power efficiency and data transfer within the chip and cloud but also increases the desired privacy levels. In the ResSen architecture, the way we send data plays a key role in improving privacy without losing much quality. The ability to selectively deactivate one of the ADC channels, which is made feasible through the parallel processing capabilities of RNS and the folding technique of ADCs, is a significant advancement toward ensuring privacy. This feature is crucial for scenarios where the system does not have enough power or sensitive information might be captured by the sensor and must be protected from unauthorized access. When a channel

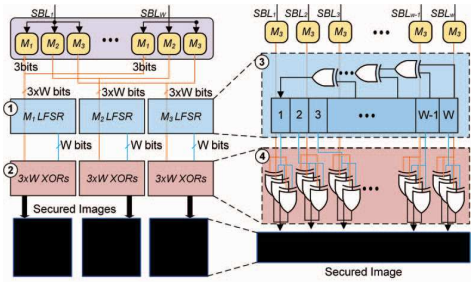


Fig. 3: The proposed encryptor, including the LFSR (①, ③) and the XOR arrays (②, ④).

is turned off, the data corresponding to that particular modulus is not recorded or transmitted, making it exceedingly difficult for an unintended recipient to reconstruct the full gray-scale image accurately.

### *E. Light Weight Encryption Block*

The proposed encryptor, as a key feature of the ResSen architecture, is designed to enhance both privacy and image processing performance. The encryptor operates in harmony with the rolling shutter technique, enhancing the privacy of the image data by obfuscating it before storing and/or transmitting. It consists primarily of three (number of moduli set) linear feedback shift registers (LFSRs) combined as depicted on ① in Fig. 3. The size of these LFSRs is equal to the width of the pixel array, $W$. The proposed design uses a separate LFSR for each modulus, making the reverse process more challenging. The shift registers are initialized with a predefined key, known only to authorized entities, ensuring that the encryption process is secure. It generates a pseudo-random sequence of bits by performing an XOR operation. It should be mentioned that the number of XORs and the desired input positions can be varied in the current state shift register. The shift and XOR operation occurs after reading each row. The detail of an LFSR unit is depicted in Fig. 3③. As mentioned above, for 8-bit images, each RNSed ADC should have three 3-bit outputs to show the numbers between 0 and $\{4, 6, 7\}$ (the largest remainder of each moduli). Each output of the RNSed ADC is XORed with the corresponding register in the shift register, as shown by ② in Fig. 3. Details of the connections for $M_3$ can be seen in Fig. 3④. This process effectively encrypts the image data, rendering it unintelligible to unauthorized viewers. The mentioned mechanism ensures that each image row is encrypted with a different key, further enhancing privacy. The output of the XOR operation, which is the encrypted image data, is then ready for transmission.

To exemplify the functionality of the proposed encryptor, consider the scenario in which the values of two pixels located in the second column but different rows are 75 and 178, respectively. The binary outputs of the RNSed ADCs are expressed as {0b000, 0b101, 0b011} and {0b011, 0b011, 0b010}, respectively. Assume that during the encryption process, we utilize three simple LFSRs, each featuring a single XOR operation in the two MSBs. The initial values of these LFSRs, corresponding to the moduli sets, are 0b1101, 0b1111, and 0b0110, respectively. The encryption process involves XORing the first number with the second bit (due to the pixel's location in the second column) of the first LFSR. Similarly, the second and third numbers are XORed with the equivalent bits of the second and third LFSRs, respectively. Consequently, encrypted results are obtained as {0b111, 0b010, 0b011}. For the next row, all LFSRs are moved to the right, producing new values of 0b1110, 0b0111, and 0b1011, respectively. Following this shift, the second row's values are XORed with the updated LFSR values. The resulting encrypted values are {0b100, 0b100, 0b010}. It is important to note that the first result is non-reversible, while the reverse operation on the second encrypted value yields 74.

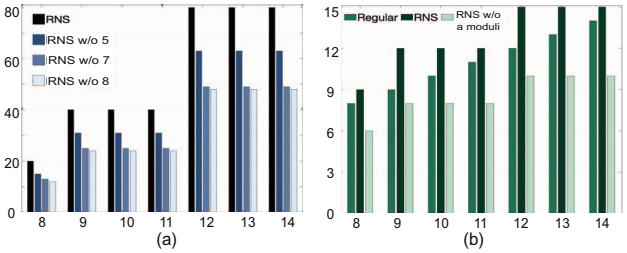


Fig. 4: (a) The number of comparators regarding different RNS implementations, and (b) the required bit. The number of bits is affected similarly by removing a channel 5, 7, or 8.

## IV. Analysis and Evaluation

### *A. Performance*

ResSen is engineered to optimize efficiency in image sensors, with special emphasis on the readout and encryption circuits. A critical innovation in this work is the substantial reduction in the number of comparators in ADCs, which directly influences both the area and power consumption of an imager. For instance, the number of comparators within a flash ADC is $2^n$, where $n$ represents the resolution. As depicted in Fig. 4(a), an 8-bit resolution is achieved by reducing the number of comparators to 20. Moreover, it illustrates that the comparator count remains unchanged for resolutions from 9-to-11 bits and from 12-to-14 bits, attributable to the chosen moduli set that does not allow for a narrower window size among the possible resolutions. Thus, the proposed system is most efficient at resolutions of 8, 11, and 14 bits. Note that while the storage or transmission requirements do not vary between modules, their power consumption does. Higher moduli require a greater number of comparators and additional subcircuits, as evidenced in Fig. 4(a). Further, Fig. 4(b) reveals the bit requirements for storing or transferring a single pixel in ResSen compared to a standard system. For example, a conventional 12-bit system requires 12 bits per pixel, whereas ResSen requires 15 bits, representing a 25% overhead. Altering the resolution to 14 bits reduces this overhead to 7.14%. In addition to comparator reduction, another significant advantage of ResSen is its channel selector mechanism, which can deactivate a modulus to decrease the data stored or transferred to 10 bits, thus offering a 28.57% and 33.33% improvement over the conventional image sensor and original ResSen, respectively.

### B. Privacy

The rationale and operation of the chosen method were modeled using Python, with the results presented in Fig.5. Despite the fact that an RNS approach alters the image histogram, it does not completely obscure every aspect of it. To provide a clearer understanding, Fig.5 further highlights these remaining details through the normalization of images processed by RNS when one channel is off (in this case, modulus 5). To overcome this challenge and increase the complexity of our model, the proposed adaptive residue readout is leveraged. It has been observed that turning off one channel decreases the probability of recovering data because normalizing the modified images does not result in data recovery. In the conducted analysis, the Mean Squared Error (MSE) was found to be 3169.41, indicating the average squared difference between the pixel intensities of the original and the modified images. The Peak Signal-to-Noise Ratio (PSNR) was calculated to be 13.12 dB, which quantifies the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. The Number of Pixels Change Rate (NPCR) was computed at 90.41%, reflecting the percentage of different pixels' values between the two images. The Unified Average Changing Intensity (UACI) was determined to be 16.54%, which measures the average intensity of differences between the original and modified images. The correlation analysis between the corresponding pixels of the two images yielded correlation coefficients of 0.027 for the horizontal, 0.014 for the vertical, and 0.014 for the diagonal directions, suggesting a low degree of linear relationship between the pixel intensities in these directions. All the obtained results using previous approaches and ours are summarized in Table I. Our approach achieves the best UACI. Also, the RNS adds complexity to the algorithm, thereby enhancing its resilience against attacks even if we got lower NPCR.

### C. Robustness

We conducted ResSen experiments on several datasets to evaluate the robustness of the proposed approach, including MNIST, Fashion-MNIST, CBCL FACE, Minimalist Histopathology (MHIST), Street View House Numbers (SVHN), and CIFAR-10, illustrated in Figs. 6 (a-f), respectively. RNS-encrypted images are decrypted and classified by the cloud. The received decrypted RNSed samples are depicted in Figs. 6 (g-l). MNIST dataset contains 70,000 images of

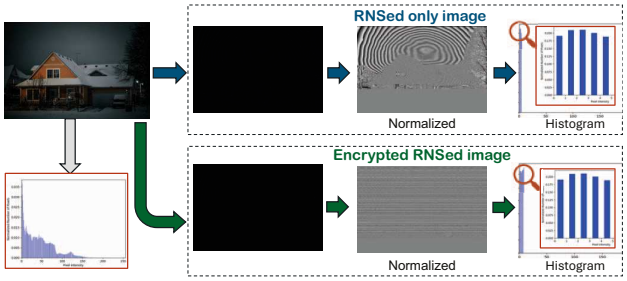


Fig. 5: ResSen efficiency versus RNSed-only approaches.

TABLE I: Performance comparison of various approaches.

| Method | NPCR (%) | UACI (%) | Correlation Analysis | | |
|---|---|---|---|---|---|
| | | | Horizontal | Vertical | Diagonal |
| [10] | 99.6094 | 33.4635 | 0.0008 | 0.0038 | 0.0028 |
| [11] | 99.8122 | 33.4611 | 0.9861 | 0.924 | 0.9538 |
| [12] | 99.6123 | 33.4512 | 0.00106 | 0.0835 | 0.017 |
| [13] | 99.6176 | 33.4502 | 0.000033 | 0.000295 | 0.000085 |
| [14] | 99.60 | 33.552 | 0.0016 | 0.0034 | 0.0032 |
| [15] | 99.6105 | 33.4656 | 0.0014 | 0.0016 | 0.00882 |
| [16] | 99.6261 | 33.467 | 0.000027 | 0.00045 | 0.00081 |
| [17] | 99.60 | 33.433 | 0.00296 | 0.00274 | 0.00436 |
| [18] | 99.5994 | 33.4183 | 0.0042 | 0.0079 | 0.0361 |
| [19] | 99.78342 | - | 0.0080415 | 0.089618 | 0.010518 |
| [20] | 99.85 | 34.25 | 0.0026 | 0.0035 | 0.0027 |
| [21] | 99.6192 | 33.4240 | - | - | - |
| [22] | 99.648 | 30.752 | - | - | - |
| **Ours** | **90.41** | **16.54** | **0.027** | **0.014** | **0.014** |

handwritten digits from 0 to 9. Similarly to MNIST, Fashion-MNIST consists of images of ten fashion categories. MHIST features 3,152 medical images divided into two categories: Hyperplastic Polyp (HP) samples, which are benign, and Sessile Serrated Adenoma (SSA), which are nearly malignant. The CBCL FACE dataset consists of high-resolution images featuring frontal, semi-profile, and full-profile views. The SVHN dataset is a real-world image dataset used for developing machine learning and object recognition algorithms, consisting of digit images obtained from house numbers in Google Street View images. Finally, CIFAR-10 is used for its 60,000 images spread over ten categories. In our experimental setup, we evaluated various models using modified images alongside the original dataset, as shown in Table II to validate the robustness of ResSen. We employed the PyTorch platform to construct well-known neural network architectures, including multilayer perception (MLP), VGG16, ResNet18, and AlexNet. In the preprocessing step, we converted all images to a gray-scale.

In one phase of our experiment, we enhanced the original dataset by including gray-scaled images encrypted with RNS sequences 5, 7, and 8, creating a diverse training dataset. This augmented dataset combined the original images with their RNSed counterparts using the specified sequences. The training phase consists of two methods, considering (a) the original dataset and all three channels off separately, and (b) the original dataset with only one of the channels off. For testing purposes, we separately evaluated the model's accuracy on RNSed data with each of the sequences 5, 7, and 8 for both experimental phases, ensuring a thorough assessment of the model's generalization capabilities across different encryption schemes. The performance of these models varied, with the most notable outcomes reflected in the table. The highest test accuracy was achieved by the MLP network on the MNIST dataset, while the lowest was observed with the VGG 16 network on the MHIST dataset. By deactivating the channel with a modulus of 5, we significantly enhanced privacy and decreased the volume of data transmission, as this process eliminates the need to transmit one of the channels. This adjustment, while resulting in a slight decrease in accuracy (1.7% in the best-case scenario and 4.6% in the worst-case scenario), presents a valuable trade-off for scenarios where privacy enhancement and bandwidth conservation are prioritized. These results highlight the efficacy of our method, demonstrating how selective RNS encryption may dramatically balance

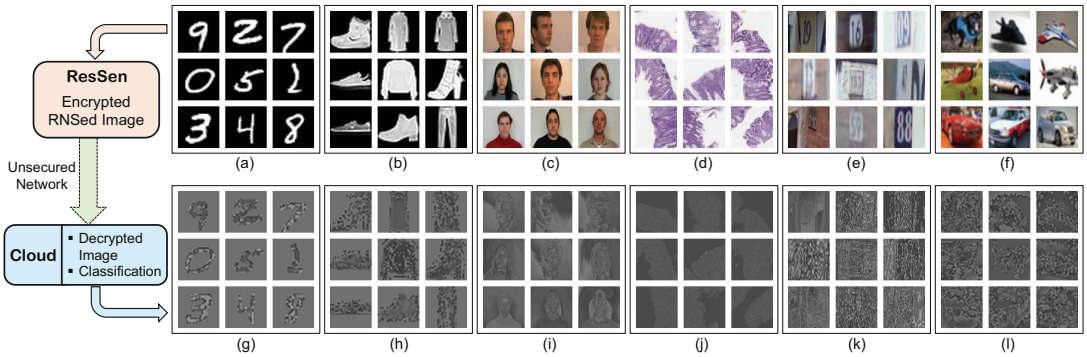


Fig. 6: (a)-(f) Samples from various datasets and (g)-(l) their reconstructed images.

TABLE II: Test accuracy evaluation using different models on various datasets.

| Dataset | Network | Original | RNSed w/o 5 | RNSed w/o 7 | RNSed w/o 8 | Train on RNS w/o 5,7,8 | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | RNSed w/o 5 | RNSed w/o 7 | RNSed w/o 8 |
| MNIST | MLP | 98.83 | 97.13 | 95.64 | 95 | 97.98 | 97.974 | 97.971 |
| Fashion-MNIST | AlexNet | 90.17 | 88.72 | 86.9 | 86.31 | 89.01 | 88.99 | 88.9 |
| SVHN | AlexNet | 93.651 | 89.032 | 87.664 | 87.004 | 89.954 | 89.943 | 89.897 |
| MHIST | VGG 16 | 75.11 | 71.98 | 70.87 | 70.17 | 73.1 | 73.07 | 72.91 |
| CBCL-Face | VGG 16 | 98.28 | 96.31 | 94.82 | 94.21 | 97.11 | 97.05 | 96.99 |
| CIFAR-10 | ResNet 18 | 93.07 | 90.01 | 88.62 | 88.03 | 91.96 | 91.87 | 91.02 |

privacy enhancement and bandwidth conservation while maintaining commendable model accuracy.

## V. Conclusion

By integrating RNS with digital encryption, we developed the ReSen architecture to enhance image sensor privacy, effectively balancing privacy improvement with image fidelity. This methodology maintains a high degree of privacy by significantly altering pixel values, as evidenced by our comprehensive analysis, while ensuring minimal impact on image quality. In the normal case, the bandwidth overhead of using RNS is equal to 12.5%, while thanks to the proposed adaptive readout circuit in low power mode, the required bandwidth is reduced to 25%. These results underscore the effectiveness of our approach in improving privacy without significantly compromising the usability of the images; when a single channel is deactivated, there is an average decrease in accuracy of 3.1%.

## Acknowledgement

This work is supported in part by the National Science Foundation under Grant No. 2216772, 2216773, 2303114, and 2247156.

## References

[1] L. Sousa *et al.*, "Combining residue arithmetic to design efficient cryptographic circuits and systems," *IEEE Circuits and Systems Magazine*, vol. 16, no. 4, pp. 6–32, 2016.

[2] A. Roohi *et al.*, "Rnsim: Efficient deep neural network accelerator using residue number systems," in *IEEE/ACM ICCAD*. IEEE, 2021, pp. 1–9.

[3] A. Vennos, K. George, and A. Michaels, "Attacks and defenses for single-stage residue number system prngs," *IoT*, vol. 2, no. 3, pp. 375–400, 2021.

[4] J. B. Eseyin, "Enhanced asymmetric data encryption algorithms using residue number system and steganography," Ph.D. dissertation, Kwara State University (Nigeria), 2022.

[5] S. Abdul-Mumin *et al.*, "Residue number system-based approach to minimise energy consumption in wireless sensor networks," *Asian Journal of Research in Computer Science*, vol. 14, no. 4, pp. 46–65, 2022.

[6] A. Roohi and S. Angizi, "Efficient targeted bit-flip attack against the local binary pattern network," in *IEEE HOST*. IEEE, 2022, pp. 89–92.

[7] M. P. Joshi and S. Pandey, "A review paper for transmission of encrypted image over cloud system," *Journal of Data Acquisition and Processing*, vol. 38, no. 3, p. 1920, 2023.

[8] D. Dhinakaran *et al.*, "Privacy-preserving data in iot-based cloud systems: A comprehensive survey with ai integration," *arXiv preprint arXiv:2401.00794*, 2024.

[9] A. Roohi *et al.*, "Pipsim: A behavior-level modeling tool for cnn processing-in-pixel accelerators," *IEEE TCAD*, 2023.

[10] W. Feng *et al.*, "A secure and efficient image transmission scheme based on two chaotic maps," *Complexity*, vol. 2021, pp. 1–19, 2021.

[11] S. G. Gollagi *et al.*, "A novel image encryption optimization technique," in *FABS*, vol. 1. IEEE, 2021, pp. 1–6.

[12] R. Vidhya *et al.*, "A secure image encryption algorithm based on a parametric switching chaotic system," *Chinese Journal of Physics*, vol. 62, pp. 26–42, 2019.

[13] J. Zhao *et al.*, "Block image encryption algorithm based on novel chaos and dna encoding," *Information*, vol. 14, no. 3, p. 150, 2023.

[14] X. Chen and e. a. Wang, "A novel chaotic image encryption scheme armed with global dynamic selection," *Entropy*, vol. 25, no. 3, p. 476, 2023.

[15] T. Wang *et al.*, "A novel trust mechanism based on fog computing in sensor–cloud system," *Future Generation Computer Systems*, vol. 109, pp. 573–582, 2020.

[16] R. Vidhya *et al.*, "A chaos based image encryption algorithm using rubik's cube and prime factorization process," *JKSUCI*, vol. 34, no. 5, pp. 2000–2016, 2022.

[17] T. M. Hoang, "A novel structure of fast and efficient multiple image encryption," *Multimedia Tools and Applications*, vol. 83, no. 5, pp. 12 985–13 028, 2024.

[18] N. Rani *et al.*, "Image encryption model based on novel magic square with differential encoding and chaotic map," *Nonlinear Dynamics*, vol. 111, no. 3, pp. 2869–2893, 2023.

[19] M. Gupta *et al.*, "An efficient image encryption technique based on two-level security for internet of things," *Multimedia Tools and Applications*, vol. 82, no. 4, pp. 5091–5111, 2023.

[20] F. Ahmed *et al.*, "A dna based colour image encryption scheme using a convolutional autoencoder," *ACM TOMM*, vol. 19, no. 3s, pp. 1–21, 2023.

[21] A. Durdu, "Image transfer with secure communications application using a new reversible chaotic image encryption," *Multimedia Tools and Applications*, vol. 83, no. 2, pp. 3397–3424, 2024.

[22] P. Kumari and B. Mondal, "Lightweight image encryption algorithm using nlfsr and cbc mode," *The Journal of Supercomputing*, vol. 79, no. 17, pp. 19 452–19 472, 2023.