RACSen: Residue Arithmetic and Chaotic Processing in Sensors to Enhance CMOS Imager Security

Sepehr Tabrizchi
School of Computing, University of Nebraska–Lincoln
Lincoln, NE, USA

Nedasadat Taheri
School of Computing, University of Nebraska–Lincoln
Lincoln, NE, USA

Shaahin Angizi
Department of Electrical and Computer Engineering, New Jersey Institute of Technology
Newark, NJ, USA
shaahin.angizi@njit.edu

Arman Roohi
School of Computing, University of Nebraska–Lincoln
Lincoln, NE, USA
aroohi@unl.edu

ABSTRACT

The widespread adoption of vision sensors raises significant security and privacy concerns. In this paper, we present RACSen as a novel architecture that can increase the security and efficiency of conventional image sensors. RACSen leverages the intricate mathematical properties of the residue number system (RNS) with analog scrambling techniques to create a sophisticated dual-layered encryption mechanism. Incorporating RNS within analog-to-digital converters further strengthens security by mitigating replay attacks and preserving data transmission integrity and confidentiality. Our results demonstrate exceptional encryption, with a perfect pixel change rate of 99.90 and high intensity change of 45.77. This offers robust image data protection with minimal overhead of 11.11%.

ACM Reference Format:
Sepehr Tabrizchi, Nedasadat Taheri, Shaahin Angizi, and Arman Roohi. 2024. RACSen: Residue Arithmetic and Chaotic Processing in Sensors to Enhance CMOS Imager Security. In *Great Lakes Symposium on VLSI 2024 (GLSVLSI '24), June 12–14, 2024, Clearwater, FL, USA.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3649476.3658791

1 INTRODUCTION

Nowadays, several serious challenges are associated with cloud-based communication and computation, including high latency, questionable scalability, quality of service (QoS), privacy, and security. As the Internet of Things (IoT) advances, these issues might be addressed by shifting computing architecture from a cloud-centric to a thing-centric perspective. This transition has significant implications for the deployment and effectiveness of vision sensors within IoT ecosystems. Vision sensors, integral components of modern automation and surveillance systems, play a crucial role in the interpretation and analysis of visual information from the environment. These sensors, which range from simple cameras to complex imaging systems equipped with machine learning capabilities, have transformed numerous industries by enabling machines to perform tasks that require visual identification and assessment. However, the widespread adoption of vision sensors raises significant security and privacy concerns. These devices often capture sensitive information, making them targets for unauthorized access and data breaches. Furthermore, the inherent interconnection of IoT devices, including vision sensors, exacerbates vulnerabilities, potentially allowing attackers to exploit one device to gain access to a broader network. To mitigate these risks, various security measures have been implemented. Traditional encryption methods such as the advanced encryption standard (AES) and data encryption standard (DES) are used to meet security demands, but face challenges in image encryption due to file size and spatial redundancy issues. Further examination reveals limitations such as computational overhead, complex key management, and vulnerability to certain attacks, highlighting the need for advanced encryption techniques [9]. Public Key Infrastructure (PKI) boosts trust and identity verification via a digital certificate management framework, suitable for large-scale deployments. Yet, its complexity and the latency in certificate verification are notable drawbacks. Homomorphic encryption allows computations on encrypted data, preserving privacy and enabling analysis but is hindered by high computational overhead and complexity, limiting its suitability for real-time and low-power IoT applications. Chaotic circuits take advantage of the unpredictable nature of chaotic systems to enhance security by generating difficult-to-predict encryption keys based on system parameters. Their strength lies in the high security and sensitivity to initial conditions, which significantly change output with minimal parameter variations. However, the complexity and need for precise control over system parameters make chaotic circuits technically challenging. This work introduces an innovative encryption methodology that integrates the residue arithmetic and chaotic processing near/in sensors, namely RACSen, to bolster the security of CMOS imagers in a low-power and efficient manner. The RACSen architecture leverages a novel analog scrambling technique with the mathematical properties of the RNS, crucial for encryption, to create a sophisticated dual-layered encryption mechanism. The proposed scrambling mechanism adds a layer of complexity and protection by altering data sequences before digitization, which changes the data's representation for each transmission and is crucial for thwarting unauthorized access to data.

GLSVLSI '24, June 12–14, 2024, Clearwater, FL, USA

ACM ISBN 979-8-4007-0605-9/24/06
https://doi.org/10.1145/3649476.3658791

2 BACKGROUND

2.1 Potential Attacks on Imager

Brute Force attacks are a common cybersecurity threat where attackers attempt every possible key to breach encryption. Enhanced encryption standards significantly increase security, while machine learning algorithms offer proactive defense mechanisms [1]. *Man-in-the-Middle* (MiM) attacks involve intercepting communications between two parties, compromising data integrity and confidentiality. Secure communication protocols, such as anomaly-based intrusion detection systems, are vital for mitigating these risks by ensuring encrypted connections and monitoring unusual network traffic patterns [6]. *Replay* attacks allow attackers to fraudulently retransmit or delay valid data transmissions, potentially leading to unauthorized access or communication disruptions. The use of sequence numbers in packets is an effective countermeasure. [2].

2.2 Chaotic Circuit

The chaotic theory explains how systems behave in unpredictable ways, resulting in seemingly random results. This principle has been applied to cybersecurity, resulting in the development of chaotic circuits. These circuits produce signals difficult to foresee or duplicate, making them ideal for secure communications [10]. Built on chaos theory, their sensitivity to initial conditions enhances encryption effectiveness. Shannon's work paved the way for utilizing chaos in cryptographic systems, inspiring advancements in secure data encryption. Despite various encryption methods, challenges like handling images of unequal dimensions highlight the need for more adaptable solutions. Chaotic circuits' unique properties continue to play a crucial role in advancing encryption technologies, particularly against sophisticated attacks.

2.3 Residue Number System (RNS)

A Residue Number System (RNS) representation is defined by L pairwise prime moduli $\{m_i\}$ for $i = 1, \ldots, L$ with $L \geq 2$. The dynamic range M is the product of all moduli, allowing any unsigned integer $X \in [0, M)$ to be represented by an L-tuple $(x_1, \ldots, x_L)$, where x_i is X modulus m_i. Signed integers $\hat{X} \in [-M/2, M/2)$ use the representation $\hat{X} = \langle X + \lfloor M/2 \rfloor \rangle_M - \lfloor M/2 \rfloor$ to relate X and its signed version within the same moduli-set. Let A, B, and R be integers represented by residue sequences $(a_1, a_2, \ldots, a_L)$, $(b_1, b_2, \ldots, b_L)$, and $(r_1, r_2, \ldots, r_L)$, respectively. R results from applying an arithmetic operation $\otimes \in \{+, -, \times\}$ to A and B. In the RNS domain, R is computed as $(r_1, r_2, \ldots, r_L) = \big(\langle a_1 \otimes b_1 \rangle_{m_1}, \langle a_2 \otimes b_2 \rangle_{m_2}, \ldots, \langle a_L \otimes b_L \rangle_{m_L}\big)$, with $\langle a_i \otimes b_i \rangle_{m_i}$ indicating modulo operation $\otimes$ on residues a_i and b_i. RNS arithmetic operations occur in parallel across independent channels, offering efficiency over two's-complement arithmetic. RNS enhances cryptographic security by enabling parallel data processing and incorporating randomness through shuffled moduli and randomized bases, complicating side-channel and power analysis attacks. In addition to encryption, it strengthens elliptic curve and lattice-based cryptography by integrating exponents and message blinding [11].

3 RACSen ARCHITECTURE

Predominantly, two types of image sensors are recognized: global shutter and rolling shutter. In a global shutter system, each pixel is individually linked to a dedicated ADC to measure the electrical voltage and translate it into a digital representation. On the other hand, the rolling shutter method connects pixels to the ADC sequentially, row by row, offering advantages for low-power devices. In this paper, we introduce a novel architecture to augment the security and efficiency of conventional image sensors, exploiting the rolling shutter approach. RACSen comprises four pivotal components: a command decoder, a row scrambler, a focal plane, aka a pixel array, and a Residue Number System Analog-to-Digital Converter (RNSed-ADC) readout. The pixel array, including $H \times W$ pixels, maintains its standard functionality without modification. A pixel is tasked with the crucial role of transforming the light intensity into electrical voltage, Step ❶. These components and their connectivities are shown in Fig. 1. The command decoder acts as a liaison between the image sensor and the processor. Unlike standard image sensors that utilize a row selector unit to connect pixels to the ADC array, our proposed scrambler selects rows in a random manner in Step ❷. Traditionally, the ADC array component is responsible for converting analog voltage into digital signals, with the resolution of these converters significantly impacting image quality. In our proposed architecture, we presuppose the use of an 8-bit image format that is capable of producing 256 distinct values. However, in Step ❸, we replace traditional ADCs with the novel proposed RNSed-ADC to improve area and power consumption. This arrangement utilizes moduli of $\{m_1 = 5,\ m_2 = 7,\ m_3 = 8\}$ to create a specific window of 280 ($M = 5 \times 7 \times 8$), closely approximating the 256-value range. The implementation details of these components, aimed at enhancing security and performance, are discussed further in the following sections.

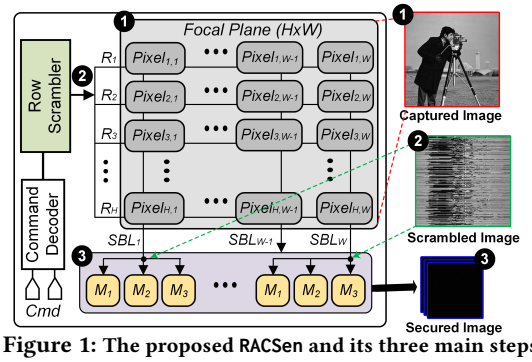

Figure 1: The proposed RACSen and its three main steps.

3.1 Row Scrambler

The proposed row scrambler, depicted in Fig. 2, includes a chaotic circuit, a small ADC, and a secured memory. This component represents a cutting-edge advancement in securing image data against unauthorized access and manipulation. Utilizing a sophisticated noisy-readout module, it embeds controlled noise into images, significantly enhancing their security. Unlike traditional encryption methods, which often focus on digital encoding alone, our scrambler operates by altering the visual data in a way that is subtle yet effective in deterring unauthorized access. This strategy ensures a fortified defense without detracting from the image's authenticity for valid use cases. The chaotic circuit, with an independent control voltage V_C and a starting value X_0, is employed to produce a random value for each frame. The ADC captures this value, which is then utilized as a row address to select a specific sequence

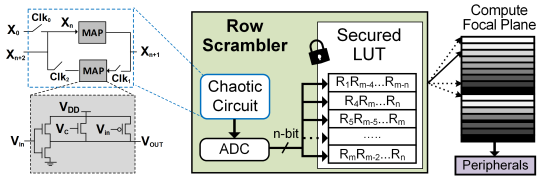

Figure 2: The row scrambler structure.

from the secured lookup table (LUT). Enhancing the resolution of n increases the security level at the cost of more precise and, therefore, costlier ADCs. Considering the image consists of H rows, permuting these rows results in $H!$ potential arrangements. This introduces a dilemma between the complexity of combinations and the memory demands. To address this, the proposed chaotic circuit operates on the LUT [18]. The size of this LUT is established as $2^n \times H \times \lceil \log_2^H \rceil$ bits, where n signifies the length of the key, H denotes the row count within the pixel array, and $\lceil \log_2^H \rceil$ calculates the bit count needed for encoding a row number. The LUT is designed to take an n-bit signal as its input and generate a sequence that triggers the activation of a designated randomized row.

3.2 Proposed RNSed-ADC

The literature discusses a variety of ADCs, including Flash-ADCs, Successive-Approximation Register ADCs (SAR-ADCs), and Folding-ADCs. In flash ADCs, the number of comparators is equal to 2^n, where n denotes the number of bits. Consequently, the comparator count in Flash-ADCs increases exponentially with n, rendering them generally unsuitable for applications requiring resolutions higher than eight bits or those that prioritize low power consumption due to scalability issues. On the other hand, SAR-ADCs significantly reduce the number of comparators at the cost of increased conversion time, as the conversion process is sequential, taking multiple cycles to complete a single conversion. An alternative solution to this problem is to adopt another type of ADC, such as Folding-ADCs. Folding-ADCs divide the n-bit input into two parts: coarse and fine. The coarse part addresses the Most Significant Bits (MSB) of the input, while the fine circuit is responsible for generating the Least Significant Bits (LSB)[4]. The entire architecture of a traditional Folding-ADC is depicted in Fig. 3(a). As illustrated, the fine section operates independently, allowing for the removal of the coarse part, since RNS requires only the folding circuit and fine ADC. This not only simplifies the circuit but also enhances its security, which is elaborated in Section 4. For example, with a modulus of 5, the output sequence would be $\{0, 1, \ldots, 4, 0, 1, \ldots\}$, as the input increases. This feature is advantageous as it allows the folding circuit to mimic this behavior. By linearly increasing the input, the circuit generates a sine-wave-like output within a

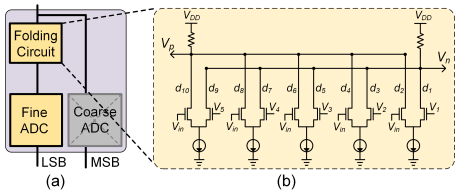

Figure 3: (a) The Folding ADC consists of a folding circuit and a fine ADC. (b) Circuit level of the folding building block.

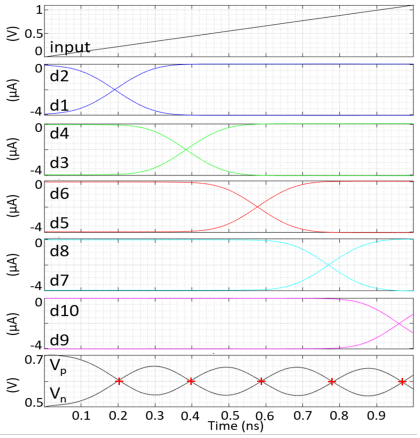

Figure 4: Transient vector for a folding circuit ($m_1 = 5$).

specific range, emulating the desired behavior in RNS applications. RNS is characterized by its property that, upon reaching a certain modulus, the output cycles through a predefined sequence before repeating. The architecture of an RNS-based Folding ADC for a modulus of 5 is partially depicted in Fig. 3(b). To realize its operation, the design incorporates five arms, each consisting of two transistors and a current source. The current source in each arm ensures that the current remains constant, which is critical to maintaining stable operation throughout the system. Additionally, each arm is associated with a distinct reference voltage, allowing for precise control over the modulation process. The dynamics of the linear input signal, the current through each arm, and the output signals are further illustrated in Fig. 4. This configuration underscores the intricate relationship between the input signal, current distribution among the arms, and the final RNS-modulated output, facilitating a comprehensive understanding of the folding ADC's operational principles. At the crossing points where the positive (V_p) and negative (V_n) outputs cross, the modulus is reset to zero. To accurately determine the precise modulus region, the next step involves dividing these regions into five segments, as illustrated in this example. This division requires the addition of four additional folding circuits, each designed with a uniquely shifted output. Adjusting the reference voltages facilitates the requisite shift in outputs. To optimize the power efficiency of the RNSed-ADC, a consolidation strategy is employed for resistor ladders across all folding circuits. The structural design, interconnections, and resultant outputs of this configuration are detailed in Fig. 5 and Fig. 6, respectively, offering a visual exposition of the system's operational framework. As shown in Fig. 5, each pair of positive and negative outputs undergoes a comparison process using a comparator. The results of these comparisons are collectively presented in Fig. 6 under the label Out_{0-4}. Subsequently, an XOR operation is performed on these outputs, as depicted in Fig. 5(b). Here, the outputs Out_{1-4} are XORed with Out_0, culminating in the final RNSed-ADC output, denoted as Xor_{1-4} in Fig. 6. The appearance of V_{DD} across these signals signifies the residue number; for instance, if Xor_{1-4} yield the sequence "1110", the interpreted residue number is 3.

4 EVALUATION AND DISCUSSION

The architecture and hardware components of the envisioned system were delineated and scrutinized in the preceding section. Each

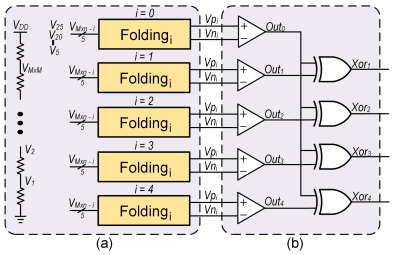

Figure 5: RNSed-ADC, including (a) folding and (b) XOR circuits.

component was simulated via HSPICE, leveraging a 45nm MOSFET PTM library. The behavior and reasons for using this method are simulated in Python and illustrated in Fig. 7. As illustrated, merely scrambling the image alters its preview without impacting the histogram, a phenomenon that presents a potential vector for AI-based detection algorithms. Conversely, employing an RNS-only strategy modifies the image's histogram, albeit without obfuscating all image details. For a more vivid exposition, Fig. 7 also showcases these residual details by normalizing the RNS-processed images. Importantly, the proposed hardware solution effectively addresses both identified issues, as demonstrated in Fig. 7. It is imperative to note that all processing operations are confined to the sensor, preventing performance degradation.

The quantitative metrics used to evaluate the encryption scheme include the Mean Squared Error (MSE), which reflects the average squared differences between original and encrypted images' pixels, indicating effective encryption at higher values. Peak Signal-to-Noise Ratio (PSNR) assesses reconstruction quality, with lower values suggesting better encryption by indicating less resemblance to the original. The Number of Pixels Change Rate (NPCR) measures the sensitivity of the encryption to changes in the image, with higher rates demonstrating a more robust encryption response. The Unified Average Changing Intensity (UACI) quantifies the average intensity difference between original and encrypted images, with higher values indicating a stronger encryption capability. Finally, the correlation coefficients measure the linear dependency between

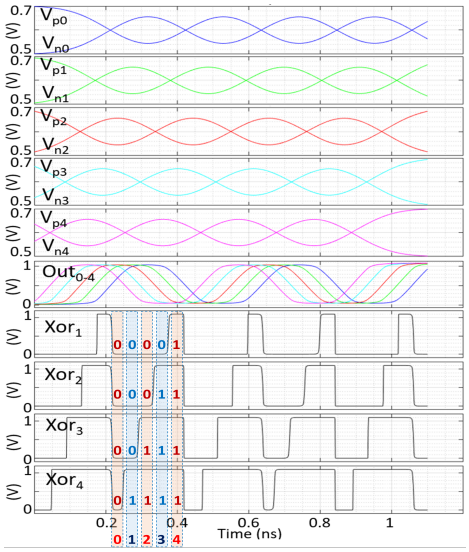

Figure 6: Results for five folding circuits and the XOR array.

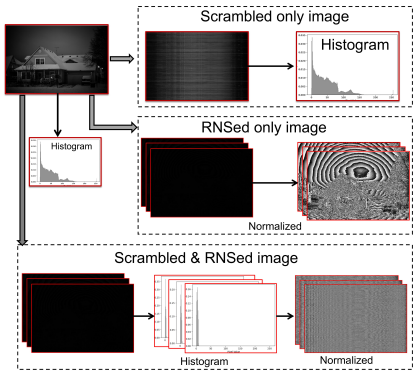

Figure 7: RACSen efficiency versus scrambled-only and RNSed-only.

the corresponding pixels in different orientations, vertical, horizontal, and diagonal, with lower values indicating a more secure encryption that significantly reduces the predictability of the pixel values. The quantitative metrics presented in Table 1 decisively confirm the efficacy of our encryption scheme. Notably, the Lena image achieved a perfect NPCR score of 100, which signifies that every pixel was altered during the encryption process. This result is exemplary, indicating that the encryption is exceptionally sensitive to changes in the input image, thus providing an impressive level of security against differential attacks. Moreover, the MSE values for all images are significantly high, but they are particularly noteworthy for the Lena and Cameraman images, registering at 16362.88 and 17504.29, respectively. These values are indicative of the substantial alterations made by the encryption process, ensuring that the encrypted images bear no discernible resemblance to the original ones. The UACI values for the Lena image are also striking, exceeding 45% in all cases. This reflects the considerable change in intensity between the original and encrypted images, further cementing the encryption's strength. The correlation coefficients for the Lena image in all orientations (vertical, horizontal, and diagonal) show a marked decrease compared to the original image, which disrupts potential patterns that could be exploited for decryption. Specifically, the vertical correlation coefficient is reduced to 0.684349, which, while being the highest correlation observed for the encrypted Lena image, still represents a substantial reduction in predictability from a typical unencrypted image's correlation that would be close to 1. These metrics not only underscore the reliability of our encryption method, but also highlight its suitability for scenarios where the integrity and confidentiality of image data are paramount. Our results for the Lena image, with a perfect NPCR score, high MSE, and significant UACI values, demonstrate an exceptional level of encryption that provides a strong defense against various attack vectors, solidifying our method's position as a highly secure solution for image data protection.

Table 2 supports the effectiveness of our newly developed encryption scheme over earlier methods. Unlike previous methods that employed their processes in a digital format, our approach uniquely incorporates chaos and RNS in the analog domain. This shift to analog allows for the creation of more complex and refined encryption patterns, which are particularly advantageous for encoding the continuous data produced by real-world sensors. The notably high values of NPCR and UACI highlight our scheme's responsiveness to changes in input and its ability to modify pixel

Table 1: Evaluation of RACSen using MSE, PSNR, NPCR, UACI, and correlation coefficients on different images.

Image		MSE*	PSNR†	NPCR*	UACI*	Correlation†		
						Horizontal	Vertical	Diagonal
House (Fig. 7)	5	3067.22	13.26335	97.94769	16.58685	0.624485772	0.620307578	0.385093403
	7	2944.992	13.43996	97.85004	16.09018	0.5254362	0.698228473	0.357348991
	8	2985.112	13.3812	97.71576	16.24495	0.549819748	0.679732421	0.372845288
Lena	5	16362.88	5.992206	99.99847	46.46121	0.684349852	0.558694359	0.385082215
	7	16018.37	6.084621	100	45.88388	0.578900796	0.632070984	0.358506398
	8	16130.39	6.054354	100	46.07281	0.573888	0.608341491	0.337385508
Cameraman	5	17504.29	5.699357	99.90387	45.77519	0.625369	0.638139	0.385873
	7	17160.83	5.78542	99.88098	45.18902	0.668674	0.53759	0.346995
	8	17277.22	5.756065	99.89166	45.39225	0.64646	0.534997	0.330554

*The higher the value, the more robust the system is. †The lower the value, the better.

brightness levels thoroughly. Our method achieves an NPCR 100%, which is unparalleled in the table and demonstrates the total transformation of the image data at the pixel level, making it extremely resistant to differential attacks. This is a testament to our scheme's ability to introduce a high degree of unpredictability into the encrypted image, which is essential for secure communications. The UACI value of our method is 46.46%, which is among the highest reported, indicating a significant alteration in pixel intensity, thus providing enhanced protection against statistical attacks. As a result, our encryption changes not only the positions of the pixels but also their values, which adds an additional layer of complexity. Furthermore, the correlation coefficients in our method are significantly lower than those of many of the previously reported techniques, suggesting that the encryption effectively disrupts the coherence between adjacent pixels in all directions. This is crucial for defeating pattern-based and statistical analysis attacks, as it eliminates any visible structure. RACSen addresses the significant threats of replay, MiM, and brute force attacks by introducing advanced scrambling techniques and RNS integration in the analog domain. Using RACSen, each communication has a unique data representation, making replay attacks ineffective. Its analog domain scrambling mechanisms disrupt the order of data before it is digitized. Using RNS, RACSen provides dynamic encryption that changes encryption keys and algorithms based on the session. Further, replayed data cannot match new keys and parameters, making decoding intercepted data extremely challenging for MiM attackers.

5 CONCLUSION

This paper introduced RACSen, a novel secure image sensor architecture that leverages RNS and chaotic circuits to create a sophisticated dual-layered encryption mechanism. Key innovations include integrating RNS within the ADC readout circuitry to enhance encryption protocols and combining this with analog scrambling techniques for added complexity. The results demonstrated RACSen's exceptional performance. A great NPCR score of 99.903% signifies the encryption's high sensitivity to input changes, making it resilient to differential attacks. As a result of the high MSE, UACI above 45%, and significantly reduced correlation coefficient, the encryption strength is clearly demonstrated.

Table 2: Performance comparison of various approaches.

Method	NPCR (%)	UACI (%)	Correlation Analysis		
			Horizontal	Vertical	Diagonal
[3]	99.6094	33.4635	0.0008	0.0038	0.0028
[5]	99.8122	33.4611	0.9861	0.924	0.9538
[12]	99.6076	33.4481	0.028	0.023	0.023
[13]	99.6123	33.4512	0.00106	0.0835	0.017
[8]	99.6124	33.549	0.0013	0.0021	0.0037
[15]	99.6105	33.4656	0.0014	0.0016	0.00882
[17]	99.6278	33.5052	0.00063	0.0058	0.0051
[14]	99.6261	33.467	0.000027	0.00045	0.00081
[16]	99.61	33.4766	0.0034	0.0019	0.0134
[16]	99.6233	33.4766	0.0034	0.0019	0.0134
[7]	99.6944	33.4162	0.00094	0.00084	0.0027
Ours	**99.90387**	**45.77519**	**0.62536**	**0.53759**	**0.53499**

ACKNOWLEDGMENTS

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

REFERENCES

[1] Monther Aldwairi et al. 2017. Multi-factor authentication system. In *RICCES Malaysia Technical Scientist Association.*
[2] Fadi Farha et al. 2020. Timestamp scheme to mitigate replay attacks in secure ZigBee networks. *IEEE Transactions on Mobile Computing* 21, 1 (2020), 342–351.
[3] Wei Feng et al. 2021. A secure and efficient image transmission scheme based on two chaotic maps. *Complexity* 2021 (2021), 1–19.
[4] Pedro M Figueiredo et al. 2009. *Offset reduction techniques in high-speed analog-to-digital converters: analysis, design and tradeoffs.* Springer Science & Business Media.
[5] Shantappa G Gollagi et al. 2021. A Novel Image Encryption Optimization Technique. In *FABS*, Vol. 1. IEEE, 1–6.
[6] Kapil M Jain et al. 2016. A survey on Man in the Middle Attack. *IJSTE-International J. Sci. Technol. Eng* 2, 09 (2016), 277–280.
[7] K et al. 2019. Image encryption using sequence generated by cyclic group. *Journal of information security and applications* 44 (2019), 117–129.
[8] Sareh Mortajez et al. 2020. A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images. *Informatics in Medicine Unlocked* 20 (2020), 100396.
[9] National Academies of Sciences Engineering and Medicine. 2022. Cryptography and the Intelligence Community: The Future of Encryption. (2022).
[10] Claude E Shannon. 1949. Communication theory of secrecy systems. *The Bell system technical journal* 28, 4 (1949), 656–715.
[11] Leonel Sousa et al. 2016. Combining residue arithmetic to design efficient cryptographic circuits and systems. *IEEE Circuits and Systems Magazine* 16, 4 (2016), 6–32.
[12] Janani Thiyagarajan et al. 2019. A chaotic image encryption scheme with complex diffusion matrix for plain image sensitivity. *Serbian Journal of Electrical Engineering* 16, 2 (2019), 247–265.
[13] R Vidhya et al. 2019. A secure image encryption algorithm based on a parametric switching chaotic system. *Chinese Journal of Physics* 62 (2019), 26–42.
[14] R Vidhya et al. 2022. A chaos based image encryption algorithm using Rubik's cube and prime factorization process (CIERPF). *Journal of King Saud University-Computer and Information Sciences* 34, 5 (2022), 2000–2016.
[15] Tian Wang et al. 2020. A novel trust mechanism based on fog computing in sensor–cloud system. *Future Generation Computer Systems* 109 (2020), 573–582.
[16] Wang Xingyuan et al. 2019. An image encryption algorithm based on ZigZag transform and LL compound chaotic system. *Optics & Laser Technology* 119 (2019), 105581.
[17] Jie Zhou et al. 2020. Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix. *Optics & Laser Technology* 131 (2020), 106437.
[18] Ranyang Zhou et al. 2022. LT-PIM: An LUT-based processing-in-DRAM architecture with RowHammer self-tracking. *IEEE CAl* 21, 2 (2022), 141–144.