ChaoSen: Security Enhancement of Image Sensor through in-Sensor Chaotic Computing

Nedasadat Taheri*, Sepehr Tabrizchi†, Shaahin Angizi‡, and Arman Roohi†*
*School of Computing, University of Nebraska-Lincoln, Lincoln, NE, USA
†Department of Electrical and Computer Engineering, University of Illinois Chicago, IL, USA
‡Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ, USA
shaahin.angizi@njit.edu, aroohi@uic.edu

2024 IEEE 42nd International Conference on Computer Design (ICCD) | 979-8-3503-8040-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCD63220.2024.00012

***Abstract*—Wireless Sensor Networks (WSN) are integral to diverse applications, ranging from environmental monitoring to urban smart infrastructure. In the realm of WSNs, security remains a critical challenge owing to the complex nature of the sensor environment. As a result, WSN security has become a research focus in recent years. In this paper, we introduce ChaoSen, a novel image sensor system incorporating analog chaotic circuits within the sensor, thereby enhancing the overall system security. The system utilizes a scrambler module, which intricately intertwines with the chaotic encryption process, to reduce the predictability of pixel values and enhance the security of the system. Comparative evaluations demonstrate that the system achieves an NPCR value of 99.5562% and a UACI of 35.81900%, indicating high sensitivity to input changes and significant alteration in pixel intensity. Our approach also demonstrates its resilience against common cyber attacks, balancing enhanced security with resource efficiency.**

***Index Terms*—Chaotic circuit, sensor attacks, processing-in-sensor, vision sensor**

I. Introduction

Wireless Sensor Networks (WSNs) have increasingly become a focal point in various advanced applications, ranging from environmental monitoring to smart city infrastructure. The fundamental appeal of WSNs lies in their ability to gather and transmit crucial data across diverse and often remote environments. However, this capability also brings to the fore significant challenges, primarily in securing the communication channels within these networks. In an era where cyber threats are becoming more sophisticated, the need for robust security measures in WSNs is more pronounced than ever. Security concerns predominantly revolve around the protection of data integrity and confidentiality. With sensors often deployed in unattended or publicly accessible areas, the data they collect and transmit is vulnerable to interception and manipulation [1]. Moreover, the open nature of wireless communication in WSNs makes them susceptible to Man-in-the-Middle (MiM) attacks, where an adversary intercepts and potentially alters the data in transit, posing a significant threat to both the integrity and confidentiality of the information.

On the other hand, Chaos-based applications have increasingly gained popularity due to the extreme sensitivity of chaotic systems to initial parameters. Utilizing chaos for image encryption has emerged as a prominent area of research over the past twenty years. While this concept has its roots in Shannon's seminal work [2], it has seen significant evolution recently. In the past decade, many chaos-based cryptosystems specifically for image encryption have been developed [3]–[6]. Chaotic

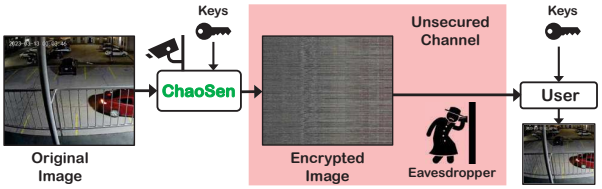


Fig. 1: The main workflow of the proposed ChaoSen approach.

systems are characterized by their unpredictability and apparent randomness despite being deterministic in nature. This paradoxical behavior stems from the system's intrinsic nonlinearity, making it an ideal candidate for secure data encryption. The core principle of a chaotic oscillator is its ability to generate a signal that, although governed by underlying deterministic rules, exhibits random-like properties. This makes it extremely challenging for an unauthorized entity to predict or replicate the system's output without precise knowledge of its initial state and parameters. Furthermore, the integration of chaotic encryption can effectively mitigate the risks associated with MiM attacks by ensuring that any intercepted data remains indecipherable without the correct decryption keys. Furthermore, chaotic systems in the realm of signal processing and communication offer a unique advantage – the blend of randomness and structure. While traditional encryption methods often rely on algorithmic complexity, chaotic encryption leverages the inherent dynamical complexity of these systems. This results in an encryption mechanism that is not only robust against conventional cryptographic attacks but also adaptable to a wide range of applications in image encryption [7] or WSN [8].

In our research, we introduce an innovative solution that further fortifies the security of WSNs by integrating analog chaotic circuits within the sensor, entitled **ChaoSen**. This integration exploits the inherent unpredictability of chaotic systems, making the encrypted data resilient against a range of cyber threats, including sophisticated Man in the Middle and brute-force attacks. Additionally, ChaoSen's design inherently protects against MiM attacks, as the chaotic encryption process significantly complicates any unauthorized interception and modification of the data during transmission. ChaoSen, with its sensitivity to initial conditions, continuous range for the key, and high dependency on system parameters, provides a powerful means to obfuscate data, thereby securing it from unauthorized access and tampering. Utilizing chaotic oscillators in our work is not merely a theoretical exercise but a practical implementation that harnesses the depth of chaos theory to

2576-6996/24/$31.00 ©2024 IEEE
DOI 10.1109/ICCD63220.2024.00012

address real-world challenges in network security. Our method provides a novel way to encrypt sensor data, thereby ensuring its confidentiality and integrity during transmission. This contribution is crucial in a landscape where data security is paramount, and it paves the way for more secure and reliable WSNs, suitable for a wide array of applications where data security is of utmost concern. Figure 1 depicts the high-level ChaoSen workflow, where it captures an image, applies scrambling and noise injections, and then transmits it via an unsecured channel. The proposed technique utilizes an efficient scrambling mechanism, which intricately intertwines with the chaotic encryption process, This scrambling, facilitated by the analog nature of our chaotic circuits, disrupts the order of data elements before digitization, thereby compounding the difficulty for adversaries attempting to breach the encrypted data. Furthermore, adding a chaotic circuit right before the analog-to-digital converter (ADC), adds another layer of complexity to the security framework. It takes advantage of analog signals' rich, continuous nature, which contrasts starkly with the discrete digital signals that attackers are more accustomed to targeting. The remainder of this paper is organized as follows: Section II provides a detailed review of various attacks targeting sensor networks, laying the groundwork for the significance of our work. In Section III, we delve into the intricate architecture of ChaoSen, presenting its design and operational principles. Section IV is dedicated to presenting and analyzing the experimental results, showcasing the efficacy of our approach. Finally, the paper culminates in Section V.

II. Review of Sensor Attacks

A. Brute Force

Brute force attacks represent a fundamental challenge in the realm of cryptographic security, where attackers systematically attempt every possible combination in a key space to decrypt an encrypted message. These attacks exploit the vulnerability of encryption schemes with limited key spaces, where the finite number of possible keys makes it theoretically possible, albeit time-consuming, to eventually find the correct key [9]. On the other hand, chaotic systems are known for their sensitivity to initial conditions, where minute differences in the key lead to drastically different encrypted outputs. This property, coupled with the continuous nature of the key space, means that even approximate guesses of the key are insufficient for decryption. The integration of a chaotic function further strengthens the encryption against brute-force attempts.

B. Nonrepudiation

Nonrepudiation is a critical security principle, ensuring that a communicating entity cannot deny the authenticity of its message [9]. In the context of chaotic signal generation, this principle acquires a unique and potent implementation. The core attribute of a chaotic system is its sensitivity to initial conditions and system parameters, which can be tailored to be distinct for each node in a network. When a message is transmitted with a chaotic signal pattern, this pattern can act as an incontrovertible digital signature, inherently linked to its originating source. The uniqueness of the chaotic signal, governed by its initial conditions and parameters, ensures that it is highly improbable for any other node to replicate the same signal inadvertently. Therefore, the source node cannot feasibly deny its authorship of the transmitted message. This attribute of nonrepudiation is crucial in scenarios where the integrity and origin of the data must be verifiable. Implementing chaotic circuits for this purpose requires meticulous management of the initial conditions and parameters, potentially supported by secure hardware or cryptographic measures, to maintain the integrity of the nonrepudiation property.

C. MiM Attack

MiM attacks pose a significant threat in digital communication systems, particularly in WSNs. In these attacks, an adversary intercepts communications between two parties, potentially altering the information being exchanged without the knowledge of either party [9]. This type of attack is especially dangerous because it can compromise the integrity and confidentiality of the data being transmitted. There is a specific MiM attack that is in sensor-to-microprocessor communication presents a major security threat by allowing attackers to intercept and potentially alter data in transit. This attack occurs between the sensor and the microprocessor, which captures raw data and processes it. The vulnerability lies in the data transmission phase, where attackers gain access to the microprocessor's input, enabling them to manipulate the data undetected. Securing this communication link is critical to protect the data's integrity and confidentiality from such unauthorized access and tampering. A potent defense against MiM attacks, particularly in sensor-to-microprocessor communication, is provided by integrating chaotic behavior within the sensor itself. This approach leverages the high sensitivity of chaotic systems to initial conditions and system parameters, meaning that any interference or alteration of data, as might occur in a MiM attack, would result in a drastically different output. Such an integration ensures that the data captured by the sensor is immediately encrypted in a complex, unpredictable manner before it even reaches the microprocessor. This not only renders interception and modification of the data highly ineffective but also secures the transmission phase from the sensor to the microprocessor. By incorporating chaotic encryption right at the data capture stage, our method effectively shields the data against MiM attacks, ensuring the integrity and confidentiality of the information transmitted within the network.

III. Proposed ChaoSen

ChaoSen is an advanced sensor image system designed for secure image capturing, integrating analog domain processing within the sensor for low-cost but efficient security. The architecture comprises three primary components: a Pixel Array, which converts environmental light into analog voltages; the Scrambling-Row Selector, facilitating the transfer of voltages from the Pixel Array to the next component, Noisy-Readout

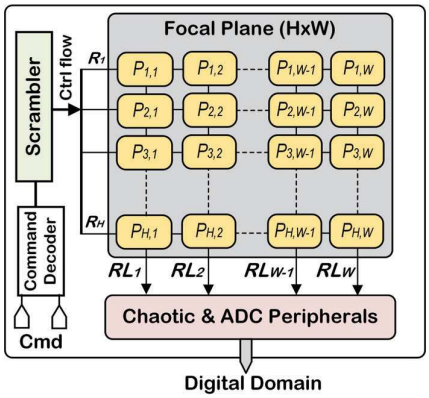


Fig. 2: The ChaoSen architecture.

Circuit, which receives generated voltages. The ChaoSen structure is shown in Fig. 2. The following sections provide detailed explanations of each component.

A. Pixel Array

The pixel array consists of $H \times W$ pixels, where H is the height, and W is the width of the array (image). Generally, pixel arrays are categorized into global and rolling shutters. Generally, pixel arrays are categorized into two types: global and rolling shutters. In a global shutter [10], all pixels are read simultaneously in parallel, offering the advantage of capturing the entire image instantaneously, which is ideal for fast-moving objects as it avoids motion artifacts. However, this method typically requires more complex and power-intensive circuitry. On the other hand, a rolling shutter [11] reads pixels sequentially, row by row, which is simpler and less power-consuming, making it suitable for low-power devices. The downside of rolling shutters is the potential for distortion in fast-moving scenes, as different parts of the image are captured at slightly different times. Despite this, for applications where power efficiency is paramount and motion artifacts are less of a concern, such as in many low-power, portable devices, a rolling shutter is the better fit, which is why ChaoSen leverages this approach. Each pixel comprises four photodiodes (subpixels), each designed to absorb red, green, and blue colors. The arrangement of these is depicted in Fig. 3(a). Two common pixel implementations are illustrated in Figs. 3(b) and (c), namely 4T and 3T, respectively. Herein, T_1 is responsible for charging the pixel capacitor (CPD), T_2 generates a current at the pixel output based on the CPD voltage, and T_3 connects the pixel to the read line (RL_n). The gates of all T_3 transistors in a row are connected and activated via the row selector. In Fig. 3(b), the capacitor is connected to the ground both through a photodiode (PD) and transistor T_4. This configuration allows greater control over the capacitor's discharge process. Conversely, in Fig. 3(c), the CPD is grounded solely through PD, necessitating a more complex readout circuit. Consequently, in this work, we employ the 4T pixel.

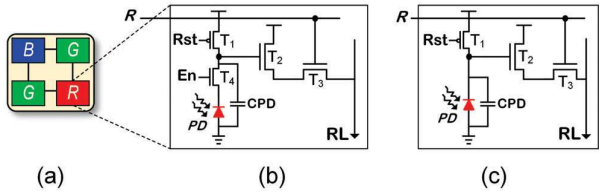
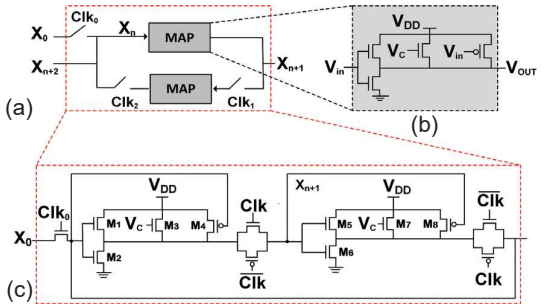


Fig. 3: (a) A pixel structure, including four photodiodes. The widely-used (b) 4T pixel, and (c) 3T pixel.

B. Chaotic Oscillator

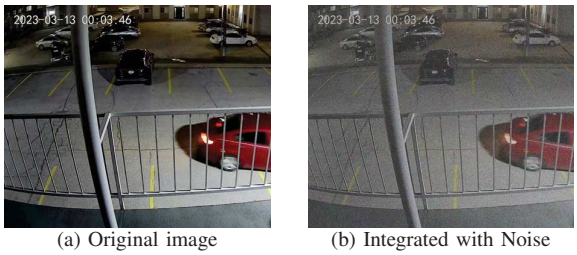
In the proposed design, we deployed a cascade circuit, as illustrated in Fig. 4(a), to effectively implement a random number generator using the specified chaos map. We have incorporated the 45nm chaotic map circuit as the seed map [12] due to its wide chaotic space and low overhead with only four MOS transistors (Fig. 4(b)), which enhances the security and robustness of the ADC's input signals.

Our chaotic oscillator is engineered by interlinking two instances of these chaotic maps, as depicted in Fig. 4(c). The initial condition, signified by X_0, is set through a switch controlled by Clk_0. Each iteration commences with an input voltage X_n propagating through the first map, culminating in the output X_{n+1}. The sequence of operations within the circuit is precisely orchestrated by a single clock signal, Clk, and its inverse, ensuring synchronization and control of the timing sequence, which direct the functioning of the associated switches. A gate capacitance embedded within the second map instance acts as a sample-and-hold mechanism, ensuring the feedback loop's output, X_{n+2}, is consistently fed into the next cycle's input. Moreover, in chaotic oscillators, width-to-length ratios (W/L) for the primary pMOS and nMOS transistors are essential for



Trans.	W/L
M_1 , M_6	1200/45
M_2 , M_7	90/45
M_3 , M_8	90/90
M_4 , M_9	90/45
M_{Clk}	45/150

Fig. 4: (a) The chaotic oscillator Schematic, (b) map Circuit, (c) circuit-level of the chaotic oscillator, and (d) the transistor sizing table. (e) and (f) V_{OUT} signals for different initial key values, (V_C= 0.2 , X_0= 0.3), and (V_C= 0.7 , X_0= 0.4), respectively.



(a) Original image (b) Integrated with Noise

Fig. 5: Visualization of noise augmentation applied to an image using the chaotic oscillator.

the initiation of chaotic behavior. The illustrated table in Fig. 4(d) lists the W/L for our transistors. Also, as can be seen in Fig. 4(e,f), the initial values for V_C and X_0 are critical for the onset of chaos. This design not only preserves the chaotic dynamics within a broader operational range but also adapts the output for the ADC, reinforcing the system's security protocols. The robustness of this implementation before the ADC is essential, offering improved immunity against environmental variations and potential security threats, as derived from the cited works.

C. Scrambling-Row Selector

Incorporating noise into the output of the image enhances offers a strategic defense against adversarial attacks targeting AI-based image recognition. Adversarial attacks exploit subtle, often imperceptible perturbations in images to deceive neural networks, leading to incorrect image classification or detection. By introducing controlled noise through our Noisy-Readout module, we intentionally create a level of distortion that AI systems, particularly neural networks, find challenging to interpret. This noise acts as an adversarial input that can effectively degrade the performance of AI classifiers without hindering human recognition capabilities. Even with adding that noise, we still maintain clarity that allows human eyes to easily recognize the image (Fig. 5). As a result, we employ a scrambler module within the ChaoSen system, as depicted in Fig. 6, to safeguard against the dual threats of human and AI-driven image analysis, providing robust defense without compromising image integrity for legitimate applications.

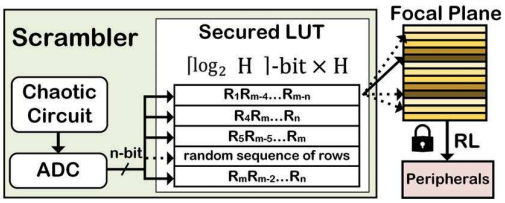


Fig. 6: Scrambling-Row Selector structure.

Since there are H rows, read ordering the rows provide H! combinations. Thus, there is a trade-off between the combinations (higher complexity) and the required memory. Herein, we developed a scrambler using a secure lookup table (LUT). The dimensions of the LUT are determined by $2^n \times H \times \lceil \log \frac{H}{2} \rceil$ bit, where n represents the key length, H is the number of rows in the pixel array, and $\lceil \log \frac{H}{2} \rceil$, represents required bits for one-row number. This table receives n-bit signal as an input address and produces a sequence to activate specific randomized rows. The system generates a random value in each frame through a chaotic circuit. The chaotic circuit has two inputs, an independent control (V_C) and X_0. The generated value is captured by an ADC, and the output of the ADC is used as the key to select a sequence from the secure LUT. The security level is enhanced with a higher n resolution, which requires a more precise and costly ADC.

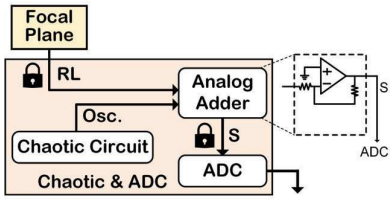


Fig. 7: Noisy-Readout schematic.

D. Noisy-Readout Circuit

As mentioned in the previous section, ChaoSen uses a rolling shutter mechanism, leading to the W (width of the pixel array) ADCs. Consequently, pixels within a column are connected to RL_n, where n represents the column number. In conventional architectures, an ADC is situated at the end of each column. To augment the security of the sensor, our design introduces a chaotic oscillator and an analog adder to each RL. The architecture and connectivity of the proposed Noisy-Readout circuit are illustrated in Fig. 7, which is crucial for adding controlled noise to each pixel's value. For the purpose of injecting noise, a chaotic oscillator is incorporated prior to each ADC. With varying control voltages and initial conditions, each oscillator generates a unique analog voltage sequence, as depicted in Fig. 4(e)-(f). This random voltage is then added to the value of each pixel. However, this addition can lead to an overflow in the pixel's value. For instance, if a pixel's value is $0.4V_{\text{ref}}$ and the oscillator's output is $0.7V_{\text{ref}}$, the sum exceeds V_{ref}. To address this, during data restoration in the cloud, subtracting $0.7V_{\text{ref}}$ from the overflowed value results in an inaccurate $0.3V_{\text{ref}}$. To mitigate this issue, we scale the voltage of both the pixels and oscillators by half, ensuring that their cumulative voltage never surpasses V_{ref}. This approach inevitably leads to the loss of the least significant bit of the image. In the evaluation section, we demonstrate that this bit loss has a minimal impact on the quality of regular images, particularly for edge devices.

IV. Experimental Results

A. ChaoSen Validation

1) Circuit-to-architecture Level Results: The functionality of ChaoSen architecture is verified by leveraging HSPICE with a 45nm PTM library. It is worth noting that ChaoSen, featuring a 128×128 pixel array, consumes 4.43 mW, of which chaotic oscillators and analog adders account only for 5%. The transient

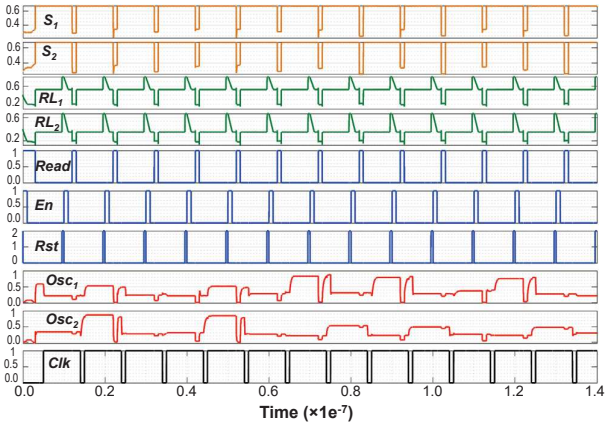


Fig. 8: Circuit level simulation for two selected pixels in columns 1 and 2.

vector is illustrated in Fig. 8, where the black signal represents the components' clock, Clk. The signals Osc_1 and Osc_2 are the outputs of the chaotic oscillators. The values of two pixels are selected and connected to the read lines denoted as RL_1 and RL_2, while S_1 and S_2 represent the final outputs before the ADC in Fig. 7. In the proposed circuit, the Clk is connected to all chaotic oscillators. Whenever it becomes zero, the oscillators generate a new random value. This value remains constant until the next clock cycle. Additionally, the Rst and En signals are associated with the pixels. The pixel's capacitors charge to V_{DD} whenever Rst is equal to V_{DD}. Subsequently, the capacitor starts discharging based on the light intensity when En equals V_{DD}. For this simulation, the light is kept constant, resulting in the output of the pixels remaining unchanged over time. The output values are approximately 0.2V and 0.4V for S_1 and S_2, respectively. The $Read$ clock is the signal for adding the value of pixels RL_n with chaotic oscillators Osc_n. At this moment, the two values are connected, leading to a temporary change in the output level. To ensure that all transistors remain in the active mode after connecting, a negative voltage is applied, and, with the op-amp configuration presented in Fig. 7, it is converted to a positive voltage. As depicted by RL_1 and RL_2, the output values differ whenever the $Read$ signal is V_{DD}.

2) Application Level Results: Figure 9 showcases the efficacy of the proposed image encryption method through various stages of transformation. In (a), the original image retains all visual information, while (b) reveals the fully scrambled image, where the original content is no longer discernible, thus affirming the robustness of the encryption technique in safeguarding against unauthorized data retrieval. In (c), additional noise is introduced, signifying a further level of encryption that starts obscuring the image content, indicating increased security measures. Finally, (d) demonstrates the decryption process by the authenticated user or in the cloud. During the restoration phase, the least significant bit is distorted. However, as the results show, the image quality remains acceptable. The Peak Signal-to-Noise Ratio (PSNR) of this image, compared to the original one, is 40.25, which is considered high.

TABLE I: Performance comparison of various approaches.

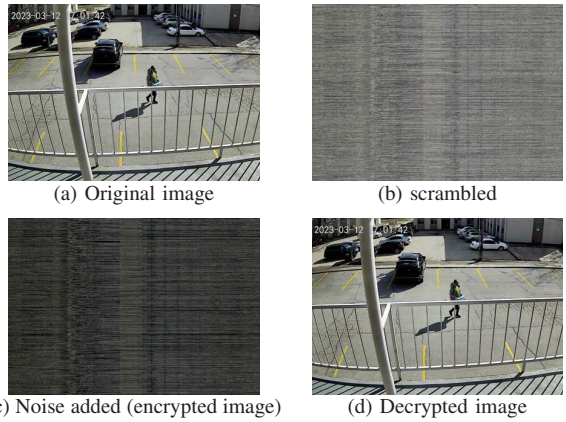
Method	NPCR (%)	UACI (%)	Correlation Analysis		
			Horizontal	Vertical	Diagonal
[13]	98.1734	33.1985	0.0116	0.016	0.0173
[1]	99.609	33.463	0.898492	0.932197	0.856771
[4]	–	–	0.962333	0.979071	0.979133
[14]	99.6094	33.4635	0.0008	0.0038	0.0028
[15]	97.7814	17.543	0.0456	0.0568	0.0202
[7]	99.63	33.54	0.011	0.0667	0.0186
[16]	99.8122	33.4611	0.9861	0.924	0.9538
[17]	99.6076	33.4481	0.028	0.023	0.023
[18]	99.61318	33.4474	0.0021	0.0043	0.00607
[19]	99.6117	33.4833	0.00059	0.002257	0.00146
[20]	99.6245	33.471	0.001132	0.0095388	0.008409
[21]	99.6134	33.46	0.004786	0.005835	0.007702
[22]	99.6123	33.4512	0.00106	0.0835	0.017
[23]	99.6124	33.549	0.0013	0.0021	0.0037
[24]	99.6278	33.5052	0.00063	0.0058	0.0051
[25]	99.6105	33.4656	0.0014	0.0016	0.00882
[26]	99.6261	33.467	0.000027	0.00045	0.00081
[27]	99.6094	33.4635	0.0015	0.00056	0.002
[28]	99.6314	33.5513	0.0031	0.0005	0.0041
[29]	99.61	33.4766	0.0034	0.0019	0.0134
[29]	99.6233	33.4766	0.0034	0.0019	0.0134
[30]	99.6944	33.4162	0.00094	0.00084	0.0027
[31]	99.6059	33.4173	0.003644	0.00262	0.001239
[32]	99.1841	33.5284	0.0017	0.0029	0.0009
[31]	99.6059	33.4173	0.003644	0.00262	0.001239
[33]	99.6105	33.4539	0.001787	0.001203	0.001497
[34]	99.6073	33.4254	0.0041	0.0016	0.00206
ChaoSen	**99.5562**	**35.81900**	**0.029839**	**0.0070**	**0.012700**

B. ChaoSen Evaluation

In assessing the efficacy of image encryption schemes, especially regarding their sensitivity to minor alterations in the original image, three predominant metrics are customarily employed: the Number of Pixel Change Rate (NPCR), the Unified Average Changing Intensity (UACI), and the Correlation Coefficient (Corr. Coeff.).

1) NPCR: This metric assesses how a single pixel change in the original image impacts the encrypted image. A high NPCR indicates that the encryption algorithm is highly sensitive to changes in the input image, which is desirable for robust encryption.

2) UACI: UACI measures the average difference in intensity between the original and encrypted images. A higher UACI suggests a greater average change in pixel values, signifying a more effective encryption process.



(a) Original image (b) scrambled

(c) Noise added (encrypted image) (d) Decrypted image

Fig. 9: A sample captured image by ChaoSen.

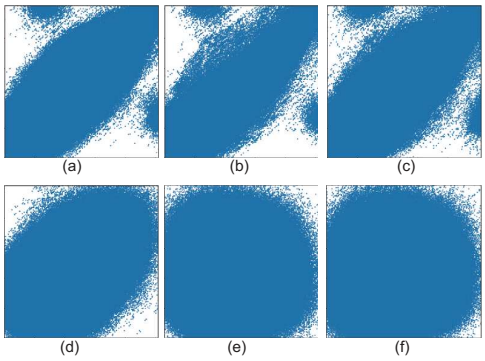


Fig. 10: (a)-(c) Horizontal, vertical, and diagonal correlation plain images, respectively. (d)-(f) Horizontal, vertical, and diagonal correlation cipher images, respectively.

3) Corr. Coeff.: This measures the similarity between the original and encrypted images. A lower Correlation Coefficient implies less similarity and, thus, indicates a more secure encryption method.

As evidenced in Table I, all aforementioned metrics strongly corroborate the robustness of our proposed encryption scheme compared to previous methods. Unlike these compared approaches that implemented chaotic processes digitally, our method innovatively applies chaos in the analog domain. This analog implementation allows for more nuanced and intricate encryption patterns better suited to the continuous nature of real-world sensor data. The NPCR and UACI values, being significantly high, demonstrate the scheme's sensitivity to input variations and its effectiveness in comprehensively altering pixel intensities. Concurrently, the absolute values of the Correlation Coefficient values further affirm the scheme's capability to drastically reduce the resemblance between the original and encrypted images, thereby fortifying the encryption's security integrity. The correlation analysis of the encrypted image revealed a marked decrease in pixel value correlation across all dimensions when compared to the plain image, shown in Fig. 10. Specifically, the horizontal correlation coefficient was measured at 0.2984, indicating a moderate level of correlation between horizontally adjacent pixels in the encrypted image, which is significantly lower than typically observed in unencrypted images. The vertical and diagonal correlations were substantially lower, with coefficients of 0.0070 and 0.0270, respectively, demonstrating the encryption algorithm's effectiveness in obfuscating the vertical and diagonal relationships within the pixel structure. These results underscore the robustness of the encryption scheme, confirming its capability to significantly reduce the predictability of pixel values and enhance image security.

C. Discussion

1) From Attack Perspective: Our proposed method uniquely employs a chaotic function combined with W^1+1 keys in continuous space, significantly enhancing its resistance to brute-force attacks. In contrast to traditional discrete key spaces, the continuous key space allows the key to take any value within a range, resulting in an uncountably infinite set of possible keys. This vastness makes it impractical for attackers to systematically try every possible key, as the concept of 'every key' becomes indefinable in a continuous space. Additionally, the precision required to correctly identify the key is beyond current computational capabilities, given the infinite granularity of potential key values. Comparative simulations show that our method's complexity and required precision for key identification extend the time and computational resources needed for a successful brute-force attack far beyond practical limits. Consequently, our approach enhances computational demands and moves into the realm of theoretical infeasibility for brute force decryption.

Moreover, our proposed encryption method, grounded in the principles of chaotic circuits, inherently enforces nonrepudiation by embedding unique signatures within each transmitted message. These signatures are generated through a sensitive dependency on initial conditions and system parameters that are unique to each communication instance, making it theoretically impossible for senders to repudiate their transmissions. In the event of a dispute, the chaotic nature of the encryption allows for clear differentiation between messages, ensuring that each message can be unequivocally traced back to its origin. Thus, our method not only ensures the integrity and authentication of the data but also solidifies the attribution, effectively shielding against nonrepudiation attacks and bolstering the overall trustworthiness of the communication within the network.

Furthermore, integrating analog scrambling with chaotic encryption fortifies the system against a wider array of attack vectors. The scrambling process, akin to a pre-encryption layer, disorients potential attackers by presenting them with a pre-processed image that lacks coherent structure or discernible patterns. When coupled with the subsequent encryption phase, the overall security is elevated, creating a two-tiered defense mechanism that is robust against intrusion and illicit decryption attempts. In essence, the scrambling process serves as an enhancement to the encryption, making the decryption without the correct keys not just computationally demanding but also algorithmically challenging. This dual-layer protection, rooted in the analog domain and extended through chaos theory, renders our encryption method a formidable adversary to the common and advanced threats alike, significantly raising the bar for security within WSNs.

In addition to these robust defenses, our proposed method crucially integrates the chaotic oscillator directly within the sensor hardware, providing an effective countermeasure against MiM attacks. This strategic placement is vital as it secures the data right at the capture point, long before it reaches the microprocessor for processing. In typical MiM scenarios, attackers aim to intercept and manipulate data during its transmission. However, by encrypting the data using chaotic principles at the source, our approach ensures that any data intercepted mid-transmission is already in a securely encrypted form. The intrinsic complexity and unpredictability of the chaotic

[1]W represents the width of the pixel array.

encryption, applied at this early stage, make it exceedingly difficult for an attacker to extract any meaningful information from the intercepted data, thereby rendering MiM attacks ineffective. This proactive security measure, embedded within the sensor, significantly enhances the overall security of the data transmission process, ensuring the integrity and confidentiality of information in WSNs and effectively neutralizing one of the most critical vulnerabilities in sensor networks.

2) Encryption Metrics: The results obtained from our proposed method demonstrate its robustness and effectiveness in encryption. The NPCR value is an impressive 99.5562%, indicating a high sensitivity to even minute changes in the input data. Such a high NPCR is indicative of the fact that a single pixel change in the original image results in a significant alteration in the encrypted image, highlighting the strength of the encryption against differential attacks. Alongside this, the UACI is recorded at 35.81900%, suggesting a substantial level of pixel intensity change, further reinforcing the security of the encryption method against potential threats. In terms of correlation analysis, the method shows exceptional performance. The horizontal correlation coefficient is only 0.29839, while the vertical and diagonal correlation coefficients are remarkably low at 0.00702 and 0.02700, respectively. These low correlation values indicate an effective diffusion and confusion process in the encryption algorithm, leading to a significant reduction in the predictability and pattern recognition within the encrypted data. Such low correlation in all three dimensions (horizontal, vertical, and diagonal) is crucial for thwarting attempts at statistical attacks, as it demonstrates the algorithm's capability to produce an output that bears minimal resemblance to the original data in terms of pixel arrangement.

3) In-Sensor Encryption Advantages: The decision to implement our encryption process directly within the sensor apparatus itself represents a paradigm shift in secure data handling within WSNs. This in-sensor encryption strategy ensures that data is secured at the point of capture, which is critical in mitigating the risk of interception before any transmission occurs. By integrating the encryption mechanism at the source, we effectively close a common security gap where raw data, if intercepted prior to encryption, could be exploited. Moreover, this method capitalizes on the analog characteristics of the sensor signals, which are naturally rich in entropy and conducive to the chaotic encryption process. This symbiotic relationship between the sensor's analog output and the chaotic encryption enhances the transmitted data's security and optimizes the encryption process to align with the sensor's inherent signal properties. Additionally, in-sensor encryption presents a formidable obstacle to attackers who now must breach the physical sensor hardware itself, which can be fortified with tamper-resistant designs and situated in inaccessible locations. Additionally, in our method, we only miss the least significant bits (LSBs). This approach preserves the overall image quality (SNR ≈ 40), ensuring that adding security does not perceptibly impact the visual fidelity. Targeting LSBs allows us to enhance encryption strength without demanding additional transmission overhead, a crucial consideration in resource-limited WSNs. Consequently, our approach achieves a significant elevation in data security while only adding a negligible ($\sim 5\%$) increase in the sensor's power consumption, achieving an ideal balance between robust encryption and operational efficiency.

V. Conclusion

The paper presented ChaoSen, a novel image sensor system incorporating chaotic computing for enhanced security. ChaoSen uses the unpredictability of chaotic circuits to effectively encrypt sensor-captured images in the analog domain. It has been rigorously tested, showing precise functionality and effective image encryption and recovery. Quantitative analyses confirm ChaoSen's high performance in security metrics like sensitivity and unpredictability. The system achieves an NPCR value of 99.5562% and a UACI of 35.81900%, indicating high sensitivity to input changes and significant alteration in pixel intensity. Additionally, with low correlation coefficients (horizontal: 0.029839, vertical: 0.0070, diagonal: 0.012700), ChaoSen demonstrates effective diffusion and confusion, enhancing its defense against statistical attacks. Comparative evaluations also demonstrate its resilience against common cyber attacks, balancing enhanced security with resource efficiency. These results highlight ChaoSen's capabilities in providing robust security solutions for WSNs.

Acknowledgment

This work is supported in part by the National Science Foundation under Grant No. 2216772, 2216773, and 2447566.

References

[1] M. Farajallah *et al.*, "Dynamic adjustment of the chaos-based security in real-time energy harvesting sensors," in *iThings and GreenCom*. IEEE, 2013, pp. 282–289.

[2] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] C. Yang *et al.*, "Image encryption based on fractional chaotic pseudo-random number generator and dna encryption method," *Nonlinear Dynamics*, vol. 109, no. 3, pp. 2103–2127, 2022.

[4] W. Wu *et al.*, "A chaotic compressive sensing based data transmission method for sensors within bbns," *Sensors*, vol. 22, no. 15, p. 5909, 2022.

[5] J. Mo *et al.*, "A provably secure three-factor authentication protocol based on chebyshev chaotic mapping for wireless sensor network," *IEEE Access*, vol. 10, pp. 12 137–12 152, 2022.

[6] S. Tabrizchi *et al.*, "Racsen: Residue arithmetic and chaotic processing in sensors to enhance cmos imager security," in *Proceedings of the Great Lakes Symposium on VLSI 2024*, 2024, pp. 551–555.

[7] P. R. Krishna *et al.*, "A chaos based image encryption using tinkerbell map functions," in *ICECA*. IEEE, 2018, pp. 578–582.

[8] C. Duran-Faundez and V. Lecuire, "Error resilient image communication with chaotic pixel interleaving for wireless camera sensors," in *Proceedings of the workshop on real-world wireless sensor networks*, 2008, pp. 21–25.

[9] P. C. Gupta, *Cryptography and Network Security*. PHI Learning Pvt. Ltd., 2014.

[10] S. Angizi *et al.*, "A near-sensor processing accelerator for approximate local binary pattern networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 1, pp. 73–83, 2023.

[11] A. Roohi *et al.*, "Pipsim: A behavior-level modeling tool for cnn processing-in-pixel accelerators," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2023.

[12] M. Sadia *et al.*, "Robust chaos with novel 4-transistor maps," *IEEE TCASII*, vol. 70, no. 3, pp. 914–918, 2022.

[13] M. A. Khan *et al.*, "An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box," *Journal of Modern Optics*, vol. 64, no. 5, pp. 531–540, 2017.
[14] W. Feng *et al.*, "A secure and efficient image transmission scheme based on two chaotic maps," *Complexity*, vol. 2021, pp. 1–19, 2021.
[15] S. Somaraj and M. A. Hussain, "Performance and security analysis for image encryption using key image," *Indian journal of science and technology*, vol. 8, no. 35, p. 1, 2015.
[16] S. G. Gollagi *et al.*, "A novel image encryption optimization technique," in *International Conference on FABS*, vol. 1. IEEE, 2021, pp. 1–6.
[17] J. Thiyagarajan *et al.*, "A chaotic image encryption scheme with complex diffusion matrix for plain image sensitivity," *Serbian Journal of Electrical Engineering*, vol. 16, no. 2, pp. 247–265, 2019.
[18] G. Hanchinamani and L. Kulkarni, "An efficient image encryption scheme based on a peter de jong chaotic map and a rc4 stream cipher. 3d res 6 (3): 30-30," 2015.
[19] S. Sam *et al.*, "An intertwining chaotic maps based image encryption scheme," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 1995–2007, 2012.
[20] I. S. Sam *et al.*, "A novel image cipher based on mixed transformed logistic maps," *Multimedia tools and applications*, vol. 56, pp. 315–330, 2012.
[21] M. François *et al.*, "A new image encryption scheme based on a chaotic function," *Signal Processing: Image Communication*, vol. 27, no. 3, pp. 249–259, 2012.
[22] 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.
[23] S. Mortajez *et al.*, "A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of dicom images," *Informatics in Medicine Unlocked*, vol. 20, p. 100396, 2020.
[24] J. Zhou *et al.*, "Fast color image encryption scheme based on 3d orthogonal latin squares and matching matrix," *Optics & Laser Technology*, vol. 131, p. 106437, 2020.
[25] 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.
[26] R. Vidhya and M. Brindha, "A chaos based image encryption algorithm using rubik's cube and prime factorization process (cierpf)," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 5, pp. 2000–2016, 2022.
[27] L. Huang *et al.*, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Optics and Lasers in Engineering*, vol. 115, pp. 7–20, 2019.
[28] K. A. K. Patro and B. Acharya, "An efficient colour image encryption scheme based on 1-d chaotic maps," *Journal of Information Security and Applications*, vol. 46, pp. 23–41, 2019.
[29] W. Xingyuan *et al.*, "An image encryption algorithm based on zigzag transform and ll compound chaotic system," *Optics & Laser Technology*, vol. 119, p. 105581, 2019.
[30] S. Kandar *et al.*, "Image encryption using sequence generated by cyclic group," *Journal of information security and applications*, vol. 44, pp. 117–129, 2019.
[31] M. Zarebnia *et al.*, "A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images," *Optik*, vol. 179, pp. 761–773, 2019.
[32] R. Enayatifar *et al.*, "Index-based permutation-diffusion in multiple-image encryption using dna sequence," *Optics and Lasers in Engineering*, vol. 115, pp. 131–140, 2019.
[33] M. Wang *et al.*, "A novel chaotic encryption scheme based on image segmentation and multiple diffusion models," *Optics & Laser Technology*, vol. 108, pp. 558–573, 2018.
[34] A. ur Rehman *et al.*, "A color image encryption technique using exclusive-or with dna complementary rules based on chaos theory and sha-2," *Optik*, vol. 159, pp. 348–367, 2018.