IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 2 February 2024, accepted 5 March 2024, date of publication 18 March 2024, date of current version 8 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3377665

RESEARCH ARTICLE

A Lightweight Multi-Chaos-Based Image Encryption Scheme for IoT Networks

KURUNANDAN JAIN[1], BETRANT TITUS[1], PRABHAKAR KRISHNAN[1], (Senior Member, IEEE), SUJITHA SUDEVAN[1], P. PRABU[2], AND ALA SALEH ALLUHAIDAN[3]

[1]Center for Cybersecurity Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri Campus, Kollam 690525, India
[2]Department of Computer Science, CHRIST (Deemed to be University), Bengaluru 560029, India
[3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 11564, Saudi Arabia

Corresponding author: Ala Saleh Alluhaidan (asalluhaidan@pnu.edu.sa)

This work was supported by Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia, through the Princess Nourah Bint Abdulrahman University Researchers Supporting Project under Grant PNURSP2024R234.

ABSTRACT The swift development of the Internet of Things (IoT) has accelerated digitalization across several industries, offering networked applications in fields such as security, home automation, logistics, and quality control. The growth of connected devices, on the other hand, raises worries about data breaches and security hazards. Because of IoT devices' computational and energy limits, traditional cryptographic methods face issues. In this context, we emphasize the importance of our contribution to image encryption in IoT environments through the proposal of Multiple Map Chaos Based Image Encryption (MMCBIE), a novel method that leverages the power of multiple chaotic maps. MMCBIE uses multiple chaotic maps to construct a strong encryption framework that considers the inherent features of digital images. Our proposed method, MMCBIE, distinguishes itself by integrating multiple chaotic maps like Henon Chaotic Transform and 2D-Logistic Chaotic Transform in a novel combination, a unique approach that sets it apart from existing schemes. Compared to other chaotic-based encryption systems, this feature renders them practically indistinguishable from pure visual noise. Security evaluations and cryptanalysis confirm MMCBIE's high-level security properties, indicating its superiority over existing image encryption techniques. MMCBIE demonstrated superior performance with NPCR (Number of Pixel Changing Rate) score of 99.603, UACI (Unified Average Changing Intensity) score of 32.8828, MSE (Mean Square Error) score of 6625.4198, RMSE (Root Mean Square Error) score of 80.0063, PSNR (Peak Signal to Noise Ratio) score of 10.2114, and other security analyses.

INDEX TERMS Chaotic systems, data encryption, image encryption, Internet of Things (IoT), key mixing, network security.

I. INTRODUCTION

IoT (Internet of Things) is a system of interconnected devices that collect and share data for various purposes, including but not limited to smart-home applications, healthcare systems, automation, and logistics in industries. Due to the diverse applications of IoT, both in households and industries, and the recent drive to convert every household device to 'smart devices' by connecting them to the internet, IoT has shown unprecedented growth over the last few years [1]. The data collected by an IoT device, ranging from sensor data to multimedia elements like digital images, audio, or video, are usually transferred to cloud storage for further processing and analysis [2]. This is due to the limited storage and computational power in IoT devices, which are usually powered by a small battery. Although developments in the IoT infrastructure enable potential applications and benefits to interconnect and digitalize various aspects of human life, the amount of sensitive data sent among these devices raises security concerns that should be addressed

The associate editor coordinating the review of this manuscript and approving it for publication was Shu Xiao.

thoroughly. Traditional cryptographic algorithms use larger keys, complex algorithms, and many rounds to ensure unabridged security for the encrypted data. And reducing the complexity and the number of rounds may compromise the scheme's security and make it vulnerable to various attacks [3]. Hence, the conventional cryptographic algorithms are inefficient in guaranteeing bonafide security to the data transmitted in IoT due to the resource constraints of the same. This prevents the need for a dedicated image encryption algorithm that considers these constraints and provides security to the sensitive data stored and transmitted among the IoT devices. Furthermore, the properties or features of each kind of information collected and transmitted by the IoT devices bring a need to hide perceptive features of the information medium. For example, encrypted images using substitution ciphers visually represent same information as substitutions in raw data may be only shifts in color spaces and not pixel orders, which effectively implies information concealed in original images can be still seen in encrypted images. Digital pictures may convey more information in a smaller space than text data, hence a sizable portion of IoT devices analyze and communicate data in this format. There is a specific need encryption technique that considers IoT's resource constraints along with special characteristics of digital images like pixel correlations and redundancies. Multipart secret sharing mechanisms were suggested. Since then, multiple specialized algorithms have been proposed to efficiently encrypt the visualized manner of data, transforming the visually identifiable features into seemingly random pixels, thus making the image appear like noise. To hide data efficiently, image encryption algorithms apply the concepts of confusion and diffusion into the visual domain. In these algorithms, confusion is achieved by separating or shuffling adjacent pixels. In contrast, diffusion is achieved by applying a calculated magnitude of change to a pixel to a subset of other pixels in the image [4].

The Internet of Things (IoT) of the future has been made possible by the convergence of the physical and digital domains through the conventional Internet. By linking items like RFID tags, mobile phones, sensors, and actuators to the Internet, the Internet of Things seeks to close the gap between the physical and digital worlds. These items can communicate and improve system performance because to their connectedness. Machine-to-Machine (M2M), Human-to-Machine (H2M), Human-to-Human (H2H), and Machine in/or Humans (MiH) communications are among the many communication modalities that are included in the Internet of Things. Because smart devices have limited resources, the rise of the Multimedia Internet of Things (M-IoT) presents issues that need for more bandwidth and processing power to handle multimedia data.

Smart objects with limited energy, memory, and processing power are a part of the machine intelligence (IoT). These devices process multimedia data, which includes picture, video, and audio, requiring an effective network topology. The transfer of large, unstructured multimedia data over limited networks necessitates a new strategy known as M-IoT. Feature extraction, event processing, encoding/decoding, energy-conscious computing, lightweight routing, and QoS upkeep are all part of this adaption. M-IoT has practical uses in emergency response systems, smart cities, traffic monitoring, and healthcare [50]. Many of the security issues that arise in the Internet of Things domain are not unique to this technology. Due to the intrinsic simplicity and affordability of IoT devices—such as temperature or humidity sensors—which may find it difficult to manage complex security procedures, protecting IoT presents a challenging issue.

With advancements in mathematical modeling and the transformative techniques applied to images, chaos-based encryption has proved to be a viable alternative to traditional image encryption schemes. The chaotic system possesses multiple features conducive to encryption, such as ergodicity, randomness, and sensitivity [5]. In a chaos-based encryption scheme, the source of confusion and diffusion is provided using chaotic maps, representing specific statistical measurements of the physical system based on the chaotic model. The chaotic system requires a set of values known as the initial conditions/parameters to generate such maps. These initial parameters provide the basis for the values generated by the chaotic system's behavior. If these parameters are within an optimal threshold, then the encrypted image is virtually impossible to be recreated by an adversary without the secret chaotic map or the initial parameters. Most existing image encryption schemes that employ chaotic maps or chaos systems vary their application in the type of chaotic map used/generated, the algorithm's structure, and the order of transformative processes that the scheme employs. While chaotic systems and the maps generated from such models display a high degree of uncertainty, which is highly regarded in an encryption scheme, encryption schemes based on these systems/maps are subject to certain drawbacks which result from the ex-act nature of these systems. Firstly, the conditions in which the chaotic maps are generated are primarily owed to the set of the initial parameters applied to the chaos system to generate the same. Suppose an adversary can influence the selection of values for the initial parameters. In that case, the chaotic map can generate a less-than-optimal chaotic map, exhibiting low randomness and visual characteristics, which can influence the encrypted image. Secondly, all encryption algorithms should achieve the basic properties of confusion and diffusion. Confusion refers to the property by which the encrypted data is void of similarities to the input data in any form (text, image, audio, etc.).

Diffusion refers to the property in which one change to the input data results in multiple changes to the encrypted data at seemingly random points. In most image encryption algorithms utilizing some form of a chaotic map, these maps are applied in such a manner that the chaotic map is used to achieve only one of two cryptographic primitives, i.e.,

either confusion or diffusion, but not them together. This requires that the encryption algorithm needs additional stages of transformative operations on the input image to produce a cipher image that is non-trivial to decipher without the original secret. Thirdly, when subjected to cryptanalysis, multiple chaos-based image encryption algorithms reveal deficiencies in their internal structure, thus lowering the algorithm's security [6]. Therefore, with the weaknesses that may decrease the potential security of chaos-based image encryption schemes, we design and present MMCBIE where image encryptions are based on chaotic patterns and attempts to overcome issues in chaos-based image encryptions.

While many alternatives for image encryption in IoT environments have been presented, there is a pressing need to overcome the shortcomings of current systems. Although useful, the assessed works left gaps in assuring full security for digital images in the constantly developing area of the Internet of Things. Recognizing the shortcomings of existing approaches, we want to make a substantial contribution to this field by presenting MMCBIE, a revolutionary image encryption technology. Our approach is motivated by the realization that the increase in networked devices creates potential weaknesses, particularly in the context of data breaches and security threats. MMCBIE goes beyond traditional cryptographic techniques to develop a strong encryption framework by using the power of multiple chaotic maps. We clearly define the fundamental features of digital images and adjust our technique to address problems including pixel correlations, color space complexities, and image compression effects. We show that MMCBIE not only fills current holes in image encryption for IoT applications, but also surpasses other specialized techniques in comprehensive security testing. As a result, our research not only emphasizes the shortcomings of current approaches, but also promotes MMCBIE as a substantial and efficient alternative for improving image security in the dynamic Internet of Things environment.

We make the following contributions to this research:

- We design and introduce MMCBIE, a chaos-based image encryption scheme that utilizes multiple chaotic maps to create a more robust image encryption scheme for IoT.
- We analyze the visual properties of the encrypted images using this scheme alongside other notable image encryption schemes that utilize chaotic systems. The results show noise-like solid characteristics, making the encrypted images virtually indistinguishable from complete visual noise.
- We also conduct security analysis on the scheme and show that the scheme achieves a high degree of security, thus achieving confidentiality.

In this paper, we first explore the topic of Internet of Things (IoT) security, looking at how it's set up, the challenges it faces, and the different ways it's used. We then dive into the latest developments and the problems that come with them. We also take a close look at image encryption, symmetric and asymmetric key cryptography, attribute-based encryption (ABE), and chaos-based image encryption. The next parts of the paper talk about what other researchers have done in the same field which can be seen in Section III. In section IV we suggest a design that combines a Henon Chaotic Map, key mixing, 2D-logistic Chaotic Transform, and a key structure. Section V is the most important part of our paper where we present our results and compare it with other works. We use different measures like NPCR, UACI, MSE, RMSE, PSNR, SSIM, PCC, Shannon's Entropy, GLCM Matrix Entropy, Auto Correlation Plot, and Color Component Intensity Analysis using RGB Histogram to see how well our solution works and finally our paper is concluded in section VI.

II. BACKGROUND

A. ARCHITECTURE AND CHALLENGES IN IOT

The basic architecture of IoT comprises three main layers [16]. The first layers are hardware layers which include sensors and actuators along with embedded architectures and circuitry. The second layer includes devices' storage, resource allocations, and optimizations. The third and final layer is the presentation or perception layer, which handles legitimate representations of collected data and processes for end users.

Even though IoT's underlying architecture is constructed of the three layers mentioned above, researchers are constantly discovering and developing new ways to formulate improved and efficient architectural standards depending on their functionalities. Further development in this area will improve scalability, energy efficiency, storage optimization, and secure data transmission. Even though IoT has the potential to bestow several benefits and applications to help humankind, there are several limitations and challenges in terms of its deployment and communication strategies that hinder its progress. One of the best examples of these challenges is energy consumption and optimization. The IoT devices and appliances deployed in the field are primarily battery-powered in household environments or industries. Therefore, capturing data, processing, and transmission to the end-user should be energy efficient. Also, the embedded processors that handle these tasks should strive to use as minimal power as possible. Recent works have tried to address these challenges by constructing energy-efficient protocols, harvesting techniques [17], [18], and more. As handling vast chunks of data from multiple IoT end nodes is highly demanding in terms of the power consumed, maintaining the energy efficiency of the data centers is also a significant concern for wide-range IoT deployment [19]. As a result, different optimization techniques that employ machine learning or novel fusion techniques should be developed to address these issues. Another challenge for IoT is to create a universal and standard platform architecture and protocols. The IoT devices that exist right now are based on distinct sets of protocols and architecture based on their manufacturers,

making the connection and communication between them tedious and challenging.

Hence, there is a need to develop universal protocols and algorithms that are efficient and scalable. One of the most critical challenges in dire need of addressing is security in IoT platforms. Due to their power and performance constraints, IoT platforms are susceptible to various attacks like eavesdropping, interference, physical compromising of nodes, and tampering of data and man-in-the-middle attacks. The highly volatile nature of nodes in IoTs and consistent additions of new nodes also create complex issues in the security of underlying networks. Therefore, the nodes and the data transmitted among the nodes should be tamper-proof, properly authenticated, and encrypted. But then, conventional cryptographic algorithms use many encryption rounds and complex algorithms to ensure the security of the data transmitted. And, if the key size, the number of rounds is reduced, or the algorithm is less complex, these systems are ineffective in ensuring sufficient security. As a result, most conventional cryptographic algorithms cannot ensure adequate security without consuming more energy and bandwidth.

Moreover, the data handled by IoT devices, for example, digital images, and videos, require specific encryption algorithms to disintegrate the pixel redundancy and correlation, which the classical cryptographic algorithms fail to deliver. Accordingly, researchers have developed many cryptographic schemes for IoT over recent years that are lightweight [20] and contemplate the distinctive properties of the data transmitted [21]. Over the recently developed schemes that employ chaos theory, DNA cryptography, or more refined encryption schemes, chaotic encryption consistently performs better mainly due to their randomization, ergodicity, and increasing sensitivity toward initial parameters.

B. APPLICATIONS OF IOT

The Internet of Things and its wide variety of applications promise considerable improvements in the human lifestyle, both in terms of effortlessness and practicality. In households, IoT plays a significant role not only in automating and interconnecting various appliances but in securing the home as well. This includes remote surveillance and alarm systems which act as intrusion detection system that alerts and informs home-owners of any potential trespassing, even if they are far away from their homes. In smart transportation systems or ''Automotive IoTs,'' the applications range from automated traffic and accident alerts, remote vehicle health reporting, maintenance, automated fleet management in industrial trucks, and more. IoT provides security, logistics and packaging optimization, quality assurance, product management, and more regarding agricultural and industrial enhancements. It also reduces the production and maintenance costs in industries by reducing the number of human work forces needed for repetitive work. As a result, this shifts the focus of the personnel from meaningless tasks to exploring and creating new ideas for future innovation and betterment of the world. Another important and emerging area for IoT deployment is health care. IoT systems in healthcare bring forth remote patient monitoring, automated reporting, smart ambulances, and much more, thereby ensuring faster diagnosis, better independent drug management, and improved treatment standards. Image processing, or the manipulation of digital images using various tools and techniques, has been gaining popularity over recent years. Image processing in IoT plays a significant role in most if not all, applications mentioned above. The digitally captured images are usually passed through digital signal processing techniques, which include sampling and quantizing the images for more accessible enhancement and analysis. Then, they are analyzed to extract information from or to restore the corrupted portions or even compress the images for more accessible storage and transport. Some of the examples for these analyses include motion detection, separation and extraction of the edges, and texture analysis. For effective image compression, the redundancy of the adjacent pixels is exploited to reduce the bytes to store the pixel values. One of the prime examples of the image acquiring and processing using IoT is remote surveillance and motion detection [7]. Using various sophisticated image analysis techniques, the embedded processors in IoT devices can detect unrecognized movement even in the dark.

There is an increasing proliferation of IoT devices connected to the internet as a result of the rapid growth of IoT technology, which has enhanced the sharing of information. However, this growth also creates brand-new issues with data security and privacy in IoTs and specifically in times of image transmissions in green IoT which face two main challenges. Firstly, in order to reduce costs, green IoT devices often have very little computational power, which limits their ability to perform highly precise calculations. The second requirement is that any encryption scheme used on these devices must be effective enough to guarantee continued device operation.

CES Blocks were used as a remedy to problems with traditional methods of generating highly random keys, encryption procedures, authentication, confidentiality, and integrity when sharing medical images. By utilizing the difficulties of determining the time series generated by the high-rise dynamic hybrid chaotic system, their suggested approach attempts to deliver an extraordinarily secure transmission. The authors present a cutting-edge method for ensuring the safe transfer of medical images in an IoT setting. The approach they suggest, dubbed CES Blocks, is based on a chaotic encryption strategy that makes use of a high-rise dynamic hybrid chaotic system to produce time series with a high level of randomness. This system is made to have strong randomization properties ideal for highly efficient image data encryption. The authors also discuss IoT device constraints in terms of memory and computational power, and they suggest improvements to mitigate potential security flaws. They talk on the need for improvisation to defend against

potential threats. The authors conduct analyses in terms of performance, secret key analysis, histogram analysis, correlation of neighboring pixel points, and information entropy analysis to examine the chaotic encryption scheme's privacy-preserving properties. Overall, this work offers a novel strategy for safely transferring medical images in an IoT setting. It proposes the blockchain-based CES Blocks system, a revolutionary chaotic encryption scheme that promises to improve the security and privacy of medical image transmission [13].

C. IOT ADVANCEMENTS AND CHALLENGES

Smart devices or embedded systems commonly utilize specialized processors, featuring limited memory and constrained power capacity, typically provided by batteries. In order to protect against malicious attacks, it is crucial to secure the end-to-end communication channels by implementing encryption and authentication algorithms that offer strong cryptographic capabilities. To address this challenge and provide practical encryption technology, ongoing development efforts are focused on Lightweight Cryptography (LWC) methods. These methods aim to optimize the sustained workload of such networks, prioritizing low power consumption, continuous availability, and computational resource constraints.

D. IMAGE ENCRYPTION

The rise of interest in chaotic dynamics around the 1960s and 1970s can be linked to the increasing processing capabilities of digital computers where many non-linear systems were examined for the first time. The presence of odd attractors and varying trajectory environments around attractors were the key features of such systems. These characteristics work together to create time series that, although totally deterministic, look random. Encryption is a process that transforms valuable information into unrecognizable forms for safeguarding them against unauthorized access. The high redundancy, capacity, and correlation of the bit pixels in the picture content necessitate the use of an encryption method, the main goal of which is to send the image safely [22]. In other words, the relevant actual information is hidden by encryption algorithms that transform plain images into cipher images. The picture can then be safely transmitted across the network without being able to be decrypted by an unauthorized party. Hence, decryption is used to convert cipher images back to their original forms. Moreover, images are combined with keys during image encryption and decryption help in decoding these encrypted images and for restoring the original images. The two basic types of keys used in image encryption and decryption are asymmetric and symmetric keys (Refer Figure 2). In symmetric keys (private keys) based cryptography, encryption and decryption utilize the same keys, whereas in asymmetric keys (public keys) based cryptography, distinct keys are used, requiring private and public keys for operations.

E. SYMMETRIC KEY CRYPTOGRAPHY

Given only one key for encryption and decryption of images, symmetric key cryptography can be referred to as encryption based on private or secret keys [23]. A private key generated by the sender and used to encrypt the picture is then transmitted to the recipient through the transmission medium. The same private key used in the encryption of images is used in decryption. Computing costs and resource needs are lower for symmetric key cryptography. Symmetric encryption may be further divided into Block and Stream Ciphers, as seen in Figure 1. In most cases, stream ciphers operate by encrypting a single bit of data at a time. Lightweight stream ciphers, such as Grain, Trivium, and Micky, are examples of lightweight stream ciphers which encrypt faster than block ciphers including Advanced Encryption Standard (AES) [24], Triple Data Encryption Standard (3-DES) [25], CLEFIA [26], and PRESENT [27] are a few examples of block ciphers. They encrypt data in blocks of specified sizes. Initialization vectors are used by block ciphers as additional layers of protection against brute force assaults. AES, known for its efficiency and security, is commonly employed in both Internet of Things (IoT) and non-IoT images. 3DES, though suitable for non-IoT images, may pose resource constraints for certain IoT devices. CLEFIA and PRESENT, as lightweight block ciphers, are apt choices for IoT images. In the realm of stream ciphers, Grain and Trivium emerge as lightweight alternatives suitable for IoT applications.

F. ASYMMETRIC KEY CRYPTOGRAPHY

In contrast to symmetric key encryption, asymmetric cryptography is often referred to as public key encryption. The picture is encrypted and decrypted using two different keys when using public key encryption [28]. Public and private keys are a set of keys that are held by each sender and recipient. While the sender only has access to the public key, the private key is kept confidential. The sender encrypts the picture using the public key before sending it to the recipient. With their private key, the recipient then decrypts the picture. Asymmetric encryption costs more to compute and uses more resources. Asymmetric key cryptography techniques include Digital Signature Algorithm (DSA), ECDSA, Rivest-Shamir-Adleman (RSA), and Diffie-Hellman. The spatial, transform, and spatiotemporal domains are only a few of the several areas in which picture encryption may be used. Fig. 3 shows how picture encryption systems are categorized. The next sub-sections go into great detail about these picture encryption methods. RSA, a widely-used algorithm, is commonly applied in non-IoT scenarios where computational resources are less constrained. Diffie-Hellman, primarily employed for key exchange, is versatile and can be utilized in both IoT and non-IoT contexts. On the other hand, ECDSA (Elliptic Curve Digital Signature Algorithm) and DSA (Digital Signature Algorithm) are more suited for non-IoT images due to their utilization of elliptic curve cryptography.

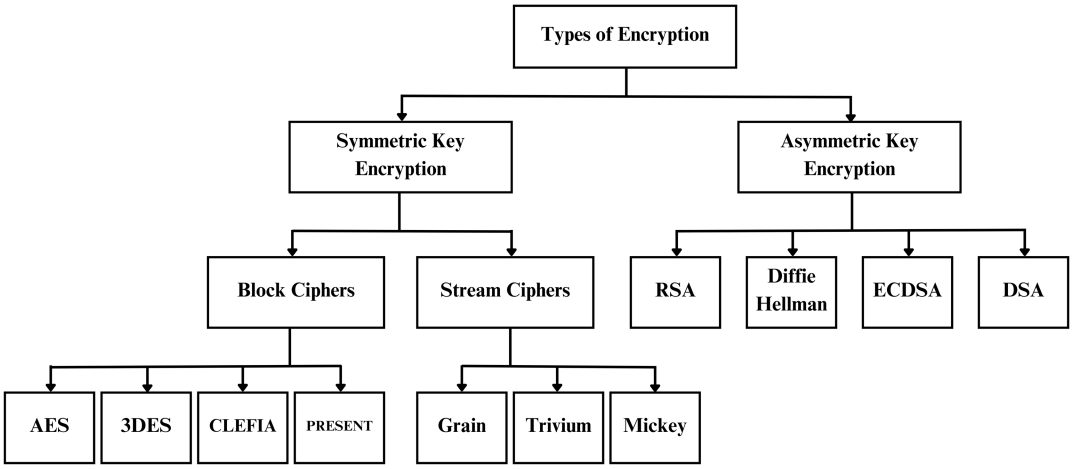


FIGURE 1. Types of image encryption algorithms.

IoT images are often defined as images that are taken or processed by IoT devices, which are defined by resource limitations such as low memory, computing power, and energy. On the other hand, non-IoT photos originate from more durable technologies like traditional computers or cameras. The distinction resides in the attributes and capabilities of the devices engaged in processing or generating the images, rather than inherent properties of the images themselves.

G. ATTRIBUTE BASED ENCRYPTION (ABE)

The typical ABE architecture is depicted in Figure 2. This system has several data producers (or simply producers) who create information, numerous data consumers (or simply consumers) who consume such information, and some data storage where information is either temporarily or permanently stored. A data producer is a piece of sensing equipment that is used to measure physical quantities or detect environmental events. They frequently feature limited computational and communication capabilities and are battery-powered. Single-board computers (like the Raspberry Pi) and mobile devices are examples of data generators that can be more resourceful. Data consumers are often either actuators—devices that automatically carry out activities depending on the information—or display information to humans. They might be powerful mobile devices such as smartphones, watches, tablets, or even full-fledged computers with superior connectivity and computing capabilities than the average data generator. Data consumers can also be constrained to devices like single-board computers or battery-powered actuators. Data storage can be achieved in multiple ways including high-end mainframes that provide cloud services to users to data producers who temporarily keep observed data onboard. Data storage takes the shape of edge nodes, MQTT broker devices, and others between these two. Additionally, a lot of modern IoT systems, like Ethereum [29], [30], store data in blockchain data structures. For a number of reasons, the conventional ABE system in the literature views all data storage as being unreliable. In fact, external organizations with offices abroad frequently handle cloud servers. Additionally, edge servers and cloud servers are always susceptible to software and hardware assaults due to their Internet connectivity [31]. Onboard storage is viewed as unreliable since it is frequently vulnerable to hacking attempts or is physically accessible and un-managed, as in wireless sensor networks. Finally, since data stored on a blockchain are by nature public, encryption is required to maintain their confidentiality [32].

For all of the reasons stated above, it is pertinent to encrypt data while in storage. Attribute-Based Encryption (ABE) demonstrates its efficacy in systems that demand guaranteed data secrecy while incorporating robust access controls. Certain ABE approaches recognize data storage as semi-trusted, acknowledging the potential for malicious activities. Trust paradigms within these categories have undergone thorough examination. Devices, such as concealed nodes facilitating data connections (e.g., network gateways or Internet routers), function as non-data storage points. Despite being untrusted, their impact can be mitigated. Figure 3 delineates key performance indicators essential for ABE in Internet of Things (IoT) applications, aligning with protocols like Datagram Transport Layer Security (DTLS). DTLS is commonly employed to secure communication in IoT devices, necessitating a focused consideration of specific performance indicators for optimal ABE implementation. The designation of ''producer bandwidth efficiency'' as a key factor underscores the importance of optimizing bandwidth resource utilization by entities generating data in the IoT ecosystem. This emphasis on bandwidth efficiency becomes particularly crucial in IoT applications with numerous devices engaged in communication and data sharing. Effectively managing bandwidth ensures reduced latency, enhanced overall system performance, and seamless data flow, especially in resource-constrained environments. Furthermore, the inclusion of a key authority, deemed

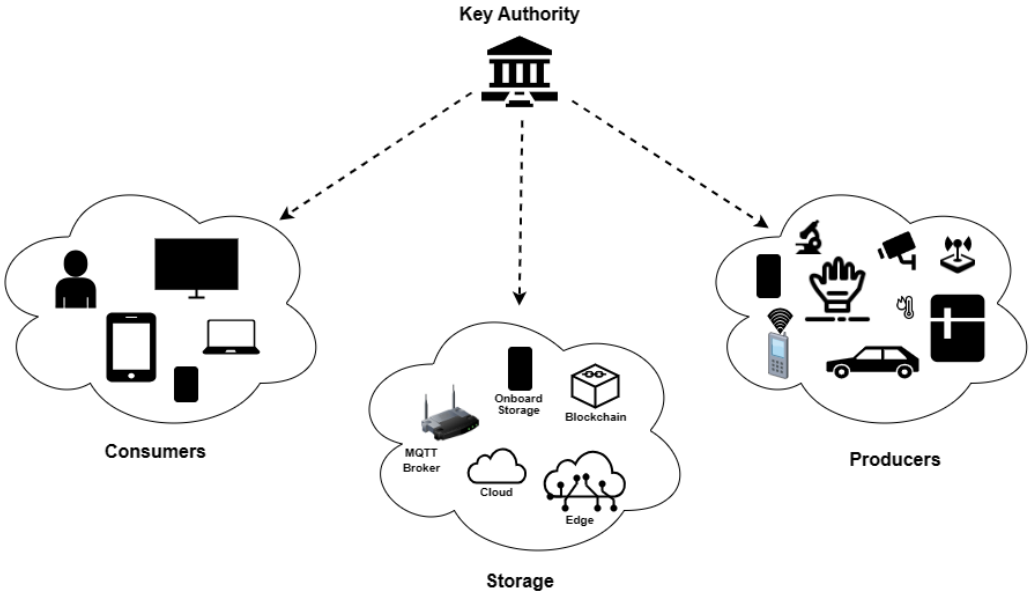


FIGURE 2. ABE architecture [58].

reliable by other entities, becomes imperative in ABE architecture. This key authority oversees the generation, distribution, updating, and revocation of ABE keys during key management operations. Importantly, key authorities, often intermittent PCs, only establish connections when key management operations are required. The key performance indicators for ABE encompasses pivotal factors contributing to the effectiveness of ABE in IoT applications, with a specific emphasis on ''producer bandwidth efficiency'' due to its significance in optimizing network resources and ensuring streamlined data transfer among IoT devices [58].

H. CHAOS-BASED IMAGE ENCRYPTION

The study of correlations between chaotic systems and cryptography, aiming to provide secure image encryption and communications during attacks, has been ongoing [34]. Chaotic cryptography, described as a balanced fusion of encryption and chaotic theories, exhibits a primary distinction from cryptosystems in that chaotic systems are defined on real numbers, while cryptosystems are mapped on an infinite set of integers. Traditional ciphers like AES and DES, effective for text encryption, prove ineffective for picture encryption due to repeating data in related images. Chaos-based encryption methods address this issue by generating uniformly dispersed random keys, covering picture data in cipher images. The close relationship between chaotic systems and cryptographic ideas yields a combination of enhanced performance, high security levels, and practical applications such as the use of pseudo-random numbers in creating stream and block ciphers, secure communications, image and video encryption, and more. According to one theory, chaotic systems, a collection of dynamical equations changing over time, may be discrete or continuous [35], comparable to confusion and diffusion in effective cryptosystems.

Numerous chaotic image encryption algorithms have been proposed, driven by advancements in image encryption and crypt-analysis. Choosing chaotic maps for chaos-based algorithms is a crucial and challenging stage [36]. Early attempts using simple chaotic maps with limited key spaces proved insufficient, leading to the proposal of chaotic maps with larger dimensions for faster, more secure, and higher-quality cryptosystems. Chaotic maps such as the Henon map, Tinkerbell map, Logistic map 1D, Logistic map 2D, Tent map, and a 5D Hyper-chaotic map have been researched for image encryption. The first attempt at a chaotic system-based image encryption scheme was proposed by Fridrich [37]. Though initially considered efficient and secure, further crypt-analysis revealed its insecurity. However, this scheme laid the foundation for many chaos-based image encryption algorithms by introducing a method to apply chaos maps generated from chaotic systems in transformative operations.

The Logistic-Sine-Cosine Image Encryption Scheme (LSC-IES) is a chaos-based image encryption scheme addressing the problem of non-optimal initial parameters. This scheme combines two seed maps (sine and logistic chaos maps) with assigned weights, performing a cosine transform on the resultant chaos map. This process resolves the issue of low randomness/non-ideal chaos for maps generated to achieve confusion. After transformation, diffusion is achieved through high-efficiency scrambling and rotation, repeated multiple times to produce the final cipher image. The encryption scheme demonstrates high resistance to differential attacks, as indicated by consistent scores in NPCR and UACI tests. The uniqueness of LSC-IES lies in the use of two chaotic maps to counteract non-ideal chaotic behavior.

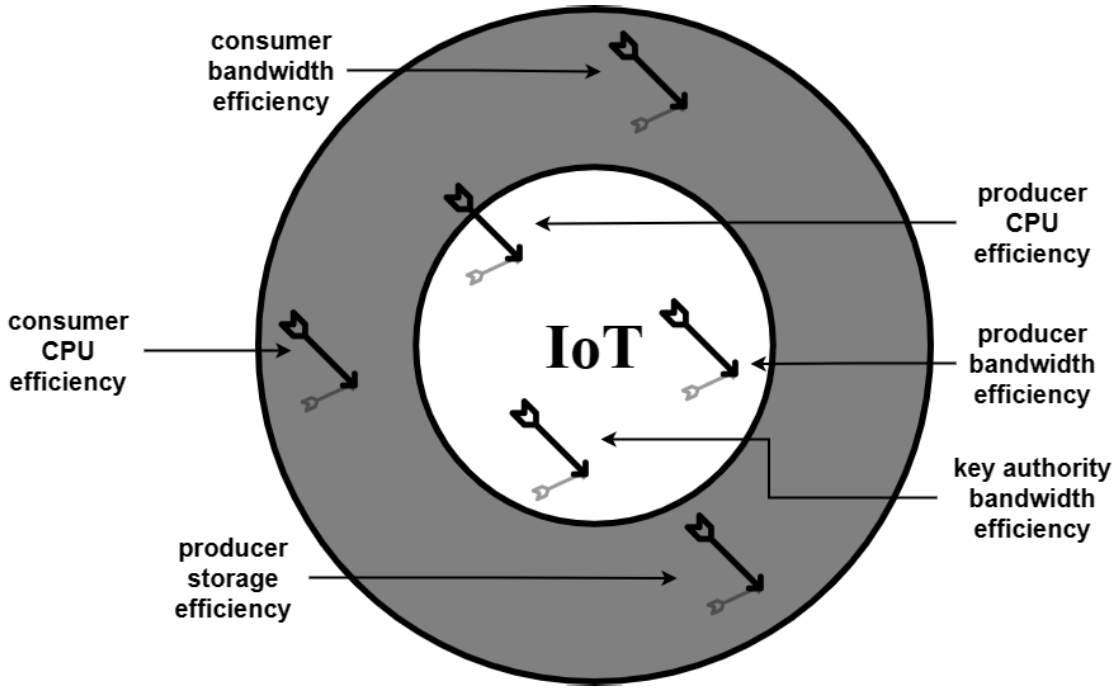


FIGURE 3. Key performance indicators for ABE in IoTs [58].

The adoption of chaotic maps has proven effective for secure communication in the Internet of Things (IoT), exemplified by the development of MMCBIE. This groundbreaking picture encryption method enhances encryption resilience and addresses IoT-specific challenges by utilizing the dynamics of multiple chaotic maps. The incorporation of chaotic maps adds complexity, significantly improving the security of encrypted photos. Furthermore, under MMCBIE, visually analyzing encrypted images reveals a unique property: the images exhibit a solidity similar to noise, making them nearly indistinguishable from random visual noise. This innovation elevates the confidentiality of transmitted images, advancing the encryption paradigm for secure communication in the IoT environment.

III. RELATED WORK

Different works have been proposed over the years that deal with fall detection using IoT. These IoT systems use deep learning or convolution neural networks, motion sensing, and image processing techniques to predict, detect and alert falls, mainly for the elderly who are home alone [8], [9]. Another prominent use case scenario of IoT image processing is smart agriculture. Different implementations have been proposed that employ IoT pesticide and irrigation drones that can detect crops accurately using image recognition and machine learning, which reduces wastage and increases productivity [10]. The above examples show that digital images and their collection, transmission, and analysis are an essential part of emerging innovative IoT applications.

Trujillo-Toledo et al. in [11] created a cryptosystem with four chaotic maps using pseudo-random number generators (PRNG) with mod 1023 functions mainly for generating unpredictable sequences. They evaluated their enhancements with bifurcation diagrams, maximal Lyapunov exponents, and statistical tests including NIST SP 800-22 and TestU01. The study's PRNG encrypted RGB images using machine-to-machine (M2M) mechanisms where encryption procedures used message queuing telemetry transport (MQTT) protocol between WiFi networks and the Internet. The proposed scheme withstood assaults including differential attacks. The proposed cryptosystem, built with enhanced sequences derived using Logistic 1D maps, obtained throughputs of up to 47.44 Mbit/s on desktop computers, and 10.53 Mbit/s on Raspberry Pi 4. Thus, it demonstrated improved security for RGB images transmitted between WiFi networks and Internet.

In order to overcome the challenges of increasing proliferation of IoT devices and limited computational power, Gu et al. have suggested the encryption method PSBP, which makes use of a parallel chaotic system. With a 16-bit precision limit, the PSBP comprises of the Piecewise Linear Chaotic Map (PWLCM), Skew Tent Map (STM), and Bernoulli map. This approach efficiently creates an efficient key matrix for encryption. A cost-effective picture encryption technique called IEPSBP, based on the PSBP system, has also been introduced by the researchers. IEPSBP uses rows or columns as fundamental units for permutation and diffusions in place of bits or bytes. It has been shown through security research and performance testing that

TABLE 1. Summary of related work section.

Authors	Chaotic Maps / Encryption Algorithms Used	Security
Guan et al. [5]	Combined Arnold's Cat Map and Chen's Chaotic systems	Input image are shuffled
		Numeric value used degree of pixel-shuffling
		Pixels encrypted with transform maps generated from Chen's chaotic system
DA Trujillo-Toledo, OR López-Bonilla [11]	Logistic 1D Map	Resistant to Known Attacks
		Protection Against Various Attacks
		Enhanced Randomness in Sequences
		Robust Against Cryptanalysis Attacks
		Efficient Throughput, Desktop: 47.44 Mbit/s, Raspberry Pi 4: 10.53 Mbit/s
		Ideal for Secure Image Transmission via WiFi and the Internet
R Durga, E Poovammal, K Ramana, RH Jhaveri [13]	High-rise Dynamic Hybrid Chaotic System, CES Blocks	Highly secure transmission
		Chaotic encryption strategy
		Strong randomization properties
		Privacy-preserving properties
		Improvements for IoT device constraints
		Performance and privacy analysis conducted
P Kumari, B Mondal [32]	Grain Stream Cypher, Chaos, GKSG, PWLCM	Protection of image data in IoT networks
		Thorough analysis of encryption methods
		Creation of PRNS using GKSG and PWLCM
		Efficacy and reliability of suggested approach demonstrated
KN Singh, OP Singh, N Baranwal, AK Singh [39]	Combination of Confusion and Diffusion Techniques, Chaotic Maps	Efficient and secure image encryption
		Improved effectiveness
		NPCR and UACI scores close to optimal values
		Overcoming shortcomings of existing research
		Robustness and confidentiality of encrypted images
CM Kumar, R Vidhya, M Brindha [40]	Enhanced Thorp Shuffle, Zig-zag Scan Convolution	Plain image relevance
		Strong diffusion
		Nullification of NPCR and UACI critical values
		One-time key for added security
		Resistance against differential attacks
		Experimental validation of security and performance metrics
W Alexan, YL Chen, LY Por, M Gabr [41]	Hyperchaotic Maps, Single Neuron Model, Substitution-Permutation Networks (SPNs)	Two hyperchaotic maps combined with SNM
		Three-stage encryption process
		S-boxes and encryption keys generated using hyperchaotic maps and SNM
		High level of confusion and diffusion
		Good NPCR and UACI values
Zhongyun Hua et al. [44]	2D-PPCS	Robust chaotic behavior
		Better performance
		Generate higher randomness pseudorandom numbers
Zhang, Yinxing et al. [45]	*n*-dimensional hyperchaotic map (nD-HCM)	Robust hyperchaotic behaviors
		Better performance
		Resist transmission noise
Zhongyun Hua et al. [46]	S-Box Latin Square	High performance
		High security level
		Outperform several state-of-the-art encryption algorithms

IEPSBP ensures cost-effectiveness and security in the context of green IoT [12].

To prioritize less memory usage and quicker communication amongst these devices, Manish Gupta, Vibhav Prakash Singh, Kamlesh Kumar Gupta, and Piyush Kumar Shukla presented a revolutionary image encryption approach specifically designed for IoT devices. Their goal is to make image transmission within IoT-enabled devices safe and error-free. The suggested method employs a two-level security strategy by fusing watermarking and cryptography methods. The discrete wavelet transform (DWT) methodology is used by the authors as the watermarking method at the first level of security. The decision to use DWT was driven by its comparatively lower processing needs when compared to other watermarking systems. The watermark is the main component of this level of protection. The authors provide a hybrid strategy that combines a 1-dimensional logistic chaotic map and the crossover operator from a genetic encryption method for the second degree of security. The technique's overall security is improved by this combination. The authors assert that by using a smaller key size and fewer encryption rounds to encrypt sparse amounts of private data, their suggested method achieves a higher level of security. However, to support these claims, a thorough examination or examination of the method is required. The report gives a detailed explanation of the suggested methodology along

with experimental findings based on numerous evaluation criteria. The authors examine the comparative results in great detail as they compare their method to currently used methods. This makes it possible to compare the effectiveness and performance of the suggested method to those of other strategies. On its whole, the study introduces a powerful image encryption solution that combines watermarking and cryptographic methods and is specifically created for safe image transfer between IoT-enabled devices. The authors' strategy solves memory use and communication speed issues, laying the groundwork for improved security in IoT environments [14].

A research study by Kumari and Mondal in [15] describes an encryption method that uses the Grain Stream Cipher and Chaos to protect the privacy of image data sent through IoT networks. The paper is divided into several sections, including a thorough analysis of different encryption methods, the creation of pseudo-random number sequences (PRNS) using the GKSG and PWLCM, the proposed encryption scheme, security analysis tests, and a discussion of the results. The authors draw attention to the fact that IoT-enabled devices can collect data and establish device-to-device communication via wireless technologies like Bluetooth and Wi-Fi. However, this communication is vulnerable to security risks that could endanger the confidentiality of picture data sent across IoT networks. The authors suggested encryptions using Grain Stream Ciphers and Chaos to safeguard transmitted image data on IoT networks. The suggested encryption technique is thoroughly described in the paper, along with its main parts and workings. The authors also provided security analyses to demonstrate the efficacy and reliability of their suggested approach. The data and results were carefully analyzed and discussed. The research article provides insightful information regarding the use of encryption methods for protecting image data sent through IoT networks in its conclusion. The suggested method, which makes use of the Grain Stream Cipher and Chaos, enhances the privacy and security of images in IoTs.

A well-known chaos-based image encryption technique was proposed by Guan et al. [5]. This approach combines two chaotic systems: Arnold's cat map and Chen's chaotic system. First, the input image is shuffled using a transform generated by Arnold's cat map. This generation procedure accepts a numeric value for the degree of pixel-shuffling operations it is to perform. Next, the resulting image with the shuffled pixels is then encrypted with the transform map generated from Chen's chaotic system. This was an approach that combined a one-dimensional and a three-dimensional chaotic system to encrypt an image. However, further cryptanalysis proved that the algorithm was not secure against chosen-plain text and known-plain text attacks. These attacks could retrieve the secret parameters of the chaotic systems, which constituted the secret key used for encryption. A method that uses the Hénon chaotic system to encrypt images was proposed by Mursi et al. [38]. The authors conduct a statistical analysis of the range of values in which the Hénon chaotic system displays optimal randomness. They modify the Hénon chaotic system, creating five chaotic systems with different ranges for the initial parameters. The resulting scheme works by applying fractional Fourier transform on the input image, applying Arnold's cat map to introduce confusion, and applying one of the five Hénon-based chaotic systems to achieve diffusion. This scheme proves the strength of the Hénon chaotic system and its preferred properties like high randomness. The logistic chaos system is based on the logistic equation introduced by Pierre François Verhulst in 1845. While this represents a one-dimensional mapping of arbitrary points, an approach that uses a two-dimensional version of the logistic chaos map was proposed by Yang et al. This system uses a two-dimensional logistic sequence generator to provide a chaotic map input into a permutation-substitution network, thus achieving both confusion and diffusion using a single chaos system. The authors analyze the behavior of the two-dimensional logistic chaos system, including phase, trajectory, and complexity, under different value ranges of the input parameters and define the optimal range of the system in which it displays ideal chaotic behavior. They prove that the encryption algorithm shows high resistance against differential crypt-analysis attacks and key-specific attacks. This approach is unique since it manages to achieve confusion and diffusion using chaotic systems.

The research presented in [39] proposes a secure method for encrypting images using chaos as the underlying principle. The proposed algorithm combines confusion and diffusion techniques to ensure the security of the encrypted images. To assess the algorithm's performance, the authors employed NPCR and UACI scores, which yielded results very close to the optimal values. These results surpassed the outcomes of recent studies, indicating improved effectiveness. The primary objective of the proposed scheme is to achieve efficiency and security in image encryption for smart city applications. It specifically addresses the shortcomings of existing image encryption research, such as computational overhead and inadequate security measures. The paper delves into the encryption and decryption processes employed in the proposed scheme. Chaotic maps are utilized to generate keys for both scrambling and diffusion operations, thereby ensuring the robustness and confidentiality of the encrypted images.

An innovative image encryption algorithm that incorporates the Enhanced Thorp shuffle and Zig-zag Scan Convolution (ETS-ZSC) operation. The algorithm aims to enhance the security of image encryption by achieving plain image relevance, strong diffusion, theoretical critical value nullification in NPCR and UACI, as well as an additional layer of security through a one-time key. The Enhanced Thorp shuffle contributes to confusion through permutation-based techniques, while the Zig-zag Scan Convolution enhances diffusion. By achieving high entropy values that closely align with theoretical values and reducing the correlation

between adjacent pixel values, the proposed method exhibits resistance against differential attacks. The article also presents experimental results that validate the effectiveness of the proposed algorithm, assessing security and performance metrics such as NPCR, UACI, entropy value, correlation coefficient, and visual quality [40].

A paper presented in [41], focused on the application of hyper-chaotic maps and a single-neuron model. The paper introduces a novel framework for encrypting images, which combines two hyper-chaotic maps with the single neuron model (SNM). This framework consists of three sequential stages, where each stage involves the utilization of a substitution box (S-box) followed by XOR operations with an encryption key. The generation of S-boxes and encryption keys is accomplished using numerical solutions obtained from the hyper-chaotic maps and the SNM. By employing Substitution-Permutation Networks (SPNs) in image encryption, this approach offers various benefits, including a high level of confusion and diffusion, aligning with the principles of secure communication as defined by Shannon. The proposed encryption technique achieves good NPCR and UACI values, which are comparable to an innovative method for encrypting medical images where chaotic maps (Baker's and 2D-Logistic Sine Coupling maps) were utilized, to introduce confusion, while employing image scrambling to achieve diffusion. In order to assess the security of this encryption scheme, a comprehensive analysis was performed, comparing it with three other well-established algorithms. The objective of this analysis was to evaluate the algorithm's security in terms of the encryption and decryption keys, the histogram of the encrypted image, Shannon's entropy, differential attack, and contrast analysis. Through various tests such as NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity), the proposed scheme exhibited a favorable balance between performance and security. However, it should be noted that, like any encryption scheme, there is a possibility of undiscovered vulnerabilities.

In the paper proposed in [44], a two-dimensional parametric polynomial chaotic system (2D-PPCS) as a solution to shortcomings in current chaotic systems for engineering applications was introduced. By using modular chaotification on initialized parametric polynomials, the 2D-PPCS generates robust chaos with customized Lyapunov exponents, addressing issues of discontinuous parameter ranges and chaos degradation. The approach is validated through theoretical analysis and numerical experiments, showcasing its ability to outperform representative 2D chaotic maps in generating highly random pseudo-random numbers. Another paper proposed in [45] introduces a method for generating n-dimensional hyper-chaotic maps (nD-HCM) with desired dynamics and robust behaviors. This method employs the Gershgorin-type theorem to formulate the nD-HCM using parametric polynomials. The resulting map exhibits n positive Lyapunov exponents, ensuring robust hyper-chaotic behavior. Theoretical analysis supports this claim. Examples of hyper-chaotic maps are provided, demonstrating the effectiveness of the method in producing complex behaviors and outperforming representative high-dimensional chaotic maps. The nD-HCM is also applied to a secure communication scheme, displaying superior noise resistance compared to other high-dimensional chaotic maps.

The research presented by Hua et al. in [46] presents a novel approach to constructing substitution boxes (S-boxes) for symmetric key encryption. The method combines chaotic sequences from a chaotic system to generate a complete Latin square, which is then used to create the S-box. The resulting S-box exhibits strong resistance to various security attacks and demonstrates high performance. The approach is applied to image encryption, resulting in an algorithm that effectively encrypts different image types with uniform histogram distributions. Security analyses confirm its robustness against attacks, while performance evaluations indicate its superiority over existing encryption algorithms.

In the research by Hadi Shahriar et al. Pyramid interconnection networks [47], exemplified by the Non-Flat Surface Level (NFSL) pyramids like NFSL-T and NFSL-Q, introduce a compelling paradigm for diverse applications such as image processing and data mining. Their hierarchical data abstraction, mirroring the human vision system, offers significant advantages, particularly in handling multidimensional datasets simultaneously. NFSL pyramids, constructed from L-level A-lateral-base pyramids, present a novel approach with their apex node surrounded by level-one surfaces—the closest nodes to the apex in basic pyramids. This architecture caters to the growing demand for symmetric and expandable interconnection networks, crucial for systems processing data from various directions. The proposed NFSL pyramid structure stands out as a powerful method to decrease computations for IoT devices. Its effectiveness is highlighted through the study of two topologies, NFSL-T and NFSL-Q, originating from Trilateral-base and Quadrilateral-base basic pyramids. To gauge the innovation's impact, essential network properties are meticulously evaluated and compared with those of standard pyramid networks and their variants. This research contributes not only to the advancement of interconnection network designs but also aligns with the evolving needs of efficient computing in IoT applications.

The fat-tree interconnection network as proposed in the research [48] stands out as a widely adopted choice in massively parallel processing systems, due to its advantageous features like deterministic routing, in-order delivery, and performance comparable to adaptive routing methods. However, challenges arise during high traffic workloads due to deterministic routing and simultaneous use of switch links, leading to Head of Line (HoL)-blocking in buffers. To address this issue, this paper introduces an innovative strategy involving switch buffer blocking paths. The strategy involves combining packets with different blocked paths

to alleviate congestion through packet exchange. Short and medium depth buffers are employed for packet exchange, considering consecutive and non-consecutive exchanging states. This approach strikes a balance between enhancing performance and reducing buffer depths without altering packet delivery order. Simulation results indicate a notable improvement, with a 22% and 33% reduction in average network latency using consecutive and non-consecutive exchanging states, respectively. Additionally, buffer depths in each switch decrease by 43.75% and 37.5% compared to multiple buffers, showcasing the potential to decrease power consumption in IoT devices through efficient packet routing methods.

In the paper by Li et al., the authors proposed a new image encryption scheme called CIES-DVEM. The scheme combines dynamic vector-level operations and a 2D-enhanced logistic modular map to achieve efficient and secure image encryption. The CIES-DVEM scheme utilizes a dynamic binary diffusion algorithm to diffuse the pixel values of the image. It also incorporates a logistic modular map to generate chaotic sequences that are used for encryption. The scheme aims to provide high security, good encryption performance, and resistance against various attacks. However, the paper does not explicitly mention the drawbacks of the proposed scheme. It focuses more on the technical details and experimental results of CIES-DVEM. To fully understand the limitations or drawbacks of the scheme, further analysis and evaluation would be required [51].

The paper by Wen et al. proposes a joint compression-encryption scheme for protecting the privacy of digital images. The approach combines image compression and encryption techniques to achieve high compression ratio, high image recovery quality, and a high level of security against cryptographic attacks. The scheme utilizes techniques such as pixel value complement, color component interchange, and dynamic chaotic sequences to enhance security. It also introduces a mechanism for associating plaintext and intermediate ciphertext to generate chaotic sequences that resist cryptographic attacks effectively. One of the advantages of the proposed scheme is that it reduces the computational complexity of the encrypted object, improving efficiency. The simulation results demonstrate that the scheme has a high compression ratio, high image recovery quality, and a fairly high security level against common cryptographic attacks. Overall, the joint compression-encryption scheme presented in the paper is a promising method for protecting the privacy of digital images in the era of big data. The joint compression-encryption scheme proposed in the paper can be used for IoT security by protecting the privacy and confidentiality of digital images transmitted in IoT systems. With the rapid development of IoT technology, a large amount of data, including digital images, is generated and transmitted in IoT networks. However, the transmission of these images can be vulnerable to security threats. The proposed scheme combines compression and encryption techniques to address the security issues in IoT systems. It utilizes chaos-based block permutation and two-round row-column diffusion algorithms for image encryption. This encryption algorithm enhances the security of the digital images by resisting various cryptographic attacks. Furthermore, the scheme employs joint compression-encryption, which reduces the computational complexity of the encrypted objects and improves the efficiency of the encryption process. This is crucial for IoT systems, as they often require real-time communication and efficient processing of data. By implementing the joint compression-encryption scheme, IoT systems can ensure the confidentiality and integrity of the digital images transmitted within the network. This enhances the overall security of the IoT system and protects against unauthorized access and data breaches. Overall, the proposed joint compression-encryption scheme provides a preferred and promising method for securing digital images in IoT systems, addressing the security challenges associated with image transmission in IoT networks [52].

In the paper by Kun et al., the authors proposed an image encryption scheme called IES-M-BD (Image Encryption Scheme based on Memristive Chaotic System, Bidirectional Bit-level Cyclic Shift, and Dynamic DNA-level Diffusion). The scheme utilizes a memristive chaotic system to generate chaotic sequences, which are then used to perform a bidirectional bit-level cyclic shift on the plaintext image. The hash value of the plaintext image is also used to influence the cyclic shift and dynamic DNA-level diffusion operations. The shifted matrix is then encoded dynamically using DNA encoding rules and subjected to DNA-level diffusion and permutation. Finally, the encrypted image is obtained after dynamic DNA decoding. The authors conducted simulation tests and security analyses to evaluate the performance of the encryption scheme. The results showed that the proposed scheme has a high security level and can resist various attacks. However, there are some drawbacks to consider. The paper does not provide a detailed analysis of the computational complexity of the proposed scheme, which could be a limitation in practical implementations. Additionally, the paper does not discuss the potential impact of noise or errors in the memristive chaotic system on the encryption process. In terms of IoT security, this method could be useful for securing image data transmitted or stored in IoT devices. By utilizing a memristive chaotic system and combining it with bidirectional bit-level cyclic shift and dynamic DNA-level diffusion, the proposed scheme offers enhanced security and resistance to attacks. This can help protect sensitive image data in IoT applications, ensuring the privacy and integrity of the transmitted or stored images [53].

In another paper proposed by Wen et al., the authors explains the QCMDC-IEA algorithm, which combines quantum chaotic maps and DNA coding, has inherent security defects. The pixel permutation and DNA substitution

components of the algorithm can be broken separately. The algorithm suffers from two fatal security flaws: the existence of an equivalent key and the lack of confusion and diffusion in the DNA domain encryption. The paper proposes an attack method that combines chosen-plaintext attack and differential analysis to completely crack the QCMDC-IEA algorithm with low complexity. However, the algorithm is vulnerable to chosen-plaintext attacks, which means an attacker can achieve complete decipherment with low complexity. The DNA domain encryption component of the algorithm lacks proper confusion and diffusion properties, which further weakens its security. In terms of applying the findings to IoT security, the paper does not explicitly discuss the application of the QCMDC-IEA algorithm to IoT security. However, the insights gained from the cryptanalysis of the algorithm can be used to inform the design and evaluation of encryption algorithms used in IoT devices. The paper highlights the importance of systematic cryptanalysis and the need to consider the security contributions of different components, such as DNA encoding and chaotic systems, in encryption algorithms. This can help in developing more secure encryption algorithms for IoT devices to protect sensitive data and ensure the integrity of communications. The QCMDC-IEA algorithm, which combines DNA coding and quantum chaotic mapping, was analyzed for its security aspects through cryptanalysis. The analysis revealed two major security defects in the algorithm. Firstly, the existence of an equivalent key was identified. This means that different keys can produce the same encryption result, compromising the security of the algorithm. This flaw arises from the fact that all chaos-based pseudo-random number sequences (PRNS) used in QCMDC-IEA are independent of the plain image. Secondly, it was found that the DNA domain encryption in QCMDC-IEA lacks both confusion and diffusion. This makes the algorithm vulnerable to cryptographic attacks. The DNA domain encryption process essentially involves a 2-bit data substitution, which can be simplified and exploited. To crack QCMDC-IEA, a combination of chosen-plaintext attack and differential analysis was proposed. This attack method takes advantage of the identified security defects and achieves complete decipherment with low complexity, revealing the underlying security mechanism of the algorithm. Based on the insights gained from the cryptanalysis, recommendations for security enhancement were provided. These recommendations include improving the design of DNA-encoded modules to enhance their security contribution to encryption algorithms and assessing the security contribution of chaotic systems from a cryptographic perspective. In summary, the cryptanalysis of QCMDC-IEA revealed the presence of equivalent keys and the lack of confusion and diffusion in the DNA domain encryption. The proposed attack method effectively cracks the algorithm, highlighting the need for security enhancements in similar image encryption algorithms based on DNA coding and chaos [54].

Another paper proposed by Wen et al. focuses on the cryptanalysis of a color image cipher called ICIC-DNA. The authors perform a detailed analysis of the algorithm and identify several security flaws. They propose a chosen-plaintext attack method to break the encryption process of ICIC-DNA. The drawbacks of ICIC-DNA include the existence of equivalent keys, the simplification of the diverse DNA operations, and the vulnerability of the substitution and permutation processes. These flaws make ICIC-DNA insecure and susceptible to chosen-plaintext attacks. The paper emphasizes the importance of examining the security aspects of image encryption algorithms, particularly those based on DNA coding and chaos theory. It suggests that the security of such algorithms should be assessed from a cryptanalytic perspective rather than relying solely on formal security measures. In terms of IoT security, the insights gained from the cryptanalysis of ICIC-DNA can contribute to the development of more secure encryption algorithms for IoT devices. By identifying the vulnerabilities and flaws in existing algorithms, researchers can design and implement stronger security mechanisms to protect sensitive data in IoT applications. Overall, the paper highlights the need for a systematic and in-depth study of the security mechanisms in image encryption algorithms. It emphasizes the importance of cryptanalysis in assessing the security of these algorithms and provides suggestions for improving their security. After conducting a thorough cryptanalysis of ICIC-DNA, several security flaws were identified. These flaws undermine the overall security of the image cipher. Equivalent Keys: Despite the use of multiple chaotic systems, the encryption sequences generated by ICIC-DNA are independent of the plaintext. This means that equivalent keys exist, which significantly weakens the security of the cipher. The diverse DNA operations employed in ICIC-DNA can be essentially simplified to a 2-bit data substitution process. This simplification makes it easier for attackers to analyze and break the encryption. ICIC-DNA incorporates both substitution and permutation of DNA domains. However, based on the equivalent simplification operation, these processes can be attacked separately using divide-and-conquer strategies. Based on these security vulnerabilities, a chosen-plaintext attack method was proposed to exploit the weaknesses in ICIC-DNA. The attack method involves using differential analysis to break the DNA-base permutation process, eliminating the DNA domain encryption, and ultimately using the equivalent key to achieve complete cracking. It is important to address these security aspects to enhance the overall security of image ciphers based on chaos theory and DNA encoding. By avoiding equivalent keys, assessing the security contribution of DNA coding, and ensuring the randomness of chaotic encryption sequences, the security of such algorithms can be improved [55].

The paper proposed by Feng et al. analyzed and identified problems in an image encryption scheme called IES-FD. The authors focused on the encryption processing for gray images

and identified several security, feasibility, and practicability problems related to the secret key of IES-FD. The original paper described multiple entities as the secret key, including the hash value of the plain image generated by the Keccak algorithm, a DNA sequence downloaded from the GenBank database, and x', y', z', w' values. This inconsistency and lack of clarity in defining the secret key pose a problem. It suggests using a DNA sequence as the secret key, which is as long as $6 \times M \times N$, where M and N represent the size of the plain image. However, transmitting such a long DNA sequence securely is not practical and feasible, rendering this approach unusable. The paper claims that using the hash value of the plain image as the secret key ensures a key space of 2^{512}, effectively resisting brute force attacks. However, the actual possible values of the hash value and the resulting key space are much smaller, around 2^{28}. Similarly, the claim of a key space of 10^{100} when using x', y', z', w' as the secret key is also incorrect. The paper identified several problems with the IES-FD image encryption scheme, including vague and inconsistent description of the secret key, impracticality of using a DNA sequence as the key, and inaccurate claims about the key space. After conducting cryptanalysis, there are several security aspects that can be examined in a focused and deliberate manner. These aspects can build on the insights gained from the cryptanalysis and help improve the security of an image encryption scheme. The design of the secret key should be carefully analyzed to ensure it is practical and reasonable. Random values or secret parameters should be avoided, and the key should be defined in a standardized binary bit sequence format. The generation process of equivalent key streams should be thoroughly analyzed and verified. It is important to avoid situations where different secret keys produce the same equivalent key streams. Each encryption step should be carefully analyzed to determine its necessity, feasibility, and practicality. Redundant or meaningless encryption steps should be avoided, and the encryption structure should be a complete and self-contained iterative structure with necessary cryptographic primitives. The relationship between the input and output of each encryption step should be analyzed. It is important to consider whether this relationship will degrade or be simplified under specific attack conditions. When verifying the security of an image encryption scheme, it is crucial to analyze and evaluate the entire encryption scheme from the perspective of an attacker. In-depth and comprehensive analysis should be conducted for each encryption step. By examining these security aspects in a focused and deliberate manner, it is possible to identify vulnerabilities and weaknesses in the image encryption scheme and make necessary improvements to enhance its security.

The proposed paper by Choi and Yu on secure image encryption system is based on compressed sensing (CS) with a scrambling mechanism. Compressed sensing is a technique that allows for the efficient acquisition and reconstruction of sparse signals. In this system, a sparse measurement matrix is used for encryption, where the nonzero elements are generated by a linear feedback shift register (LFSR) based keystream generator. To enhance the security and diffusion of the encrypted image, data scramblers based on LFSR are attached behind the CS-encryption. These scramblers introduce additional randomness and complexity to the encrypted image, making it more resistant to attacks. The use of multiple pairs of scramblers further enhances the diffusion process. The proposed system is designed for the context of multimedia Internet-of-Things (IoT) applications. With the increasing use of IoT devices and the generation of large amounts of multimedia data, it is crucial to ensure the security and privacy of these data. The secure image encryption system based on CS and scrambling provides a reliable and efficient method for encrypting multimedia data in IoT applications. By combining the advantages of CS, such as efficient data acquisition and reconstruction, with the scrambling mechanism for diffusion, the proposed system offers a secure and robust encryption solution for multimedia IoT. It ensures the confidentiality and integrity of the transmitted or stored images, protecting them from unauthorized access and attacks. Overall, the proposed system provides a secure image encryption solution that is suitable for the context of multimedia IoT, addressing the need for secure data transmission and storage in IoT applications [59].

The proposed paper by Hedayati and Mostafavi on lightweight image encryption algorithm is used in Multimedia Internet of Things (M-IoT) to provide secure communication while considering the resource constraints of IoT devices. The algorithm focuses on reducing encryption complexity and improving data communication performance. It achieves this by encrypting significant and insignificant pixels of an image using different algorithms, reducing the computational complexity. Additionally, the algorithm extracts significant parts of an image and reduces the transmitted data by correlating the insignificant data with the significant ones. By implementing this algorithm, the power consumption of devices and packet rate in M-IoT can be decreased by 15% and 26% respectively, compared to existing algorithms. This paper offers several advantages for secure communication. The algorithm focuses on encrypting significant image pixels, reducing the encryption complexity. This allows resource-constrained IoT devices to perform encryption with minimal processing power. The algorithm also employs a selective pixel encryption approach and block compression to reduce the amount of data exchanged between nodes. This results in improved data communication performance and reduced bandwidth usage. By reducing the computational complexity and data transmission volume, the algorithm contributes to a decrease in power consumption of IoT nodes. On average, the power consumption of devices is reduced by 15% compared to existing algorithms. The algorithm also ensures end-to-end secure communication by providing a desirable level of security. It achieves this by encrypting both significant and insignificant pixels of an image with different algorithms, reducing

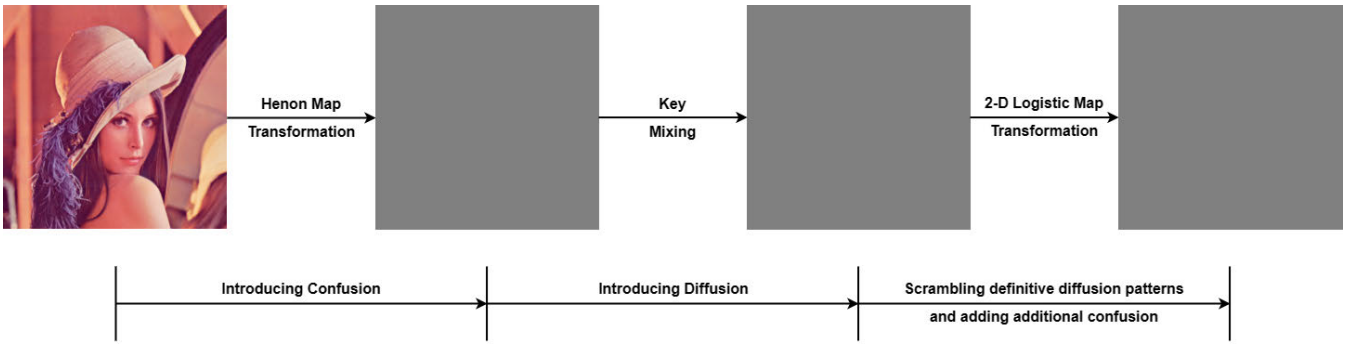


FIGURE 4. A visualization of the stages of MMCBIE.

the risk of unauthorized access. Overall, the proposed lightweight image encryption algorithm in M-IoT offers a balance between security and resource efficiency, making it suitable for secure communication in resource-limited IoT devices [60].

In conclusion, this paper presents an effective approach to encrypting medical images, employing both confusion and diffusion techniques to enhance security while maintaining a satisfactory performance-to-security ratio. The above-mentioned chaos-based image encryption schemes provide the most well-known and utilized techniques of applying chaotic systems to encrypt visual information while retaining the secrecy of the visual domain's two-dimensional information. However, most existing chaotic image encryption schemes employ chaos maps in only one encryption domain, such as diffusion or component-based confusion. Also, non-optimal choice of initial conditions can cause the generation of chaos maps whose distribution can be deterministic in nature. Therefore, we need an encryption scheme that introduces confusion and diffusion into the algorithm and solves the security deficiencies of the current schemes.

Table 1 shows the summary of the related works.

IV. PROPOSED DESIGN

A high-level overview of the proposed image encryption methodology is explained here. The original image is fed into the encryption algorithm. Hénon Chaotic Transform block represents the first step of the algorithm, where the Hénon chaotic map is applied to the input image. It generates a transformation map that is XORed with the input image. In Key Mixing step, a 192-bit key is used to perform cyclic RGB modulus addition with the output of the Hénon transform. This process is mathematically defined by equations (3). 2D-Logistic Chaotic Transform involves the use of a 2D logistic system, where subkeys x_L, y_L, and R contribute to the initial values and chaotic parameters. The generated 2D logistic map is XORed with the output of the Key Mixing stage. The final encrypted image is produced after applying all three transformation steps. The resulting image is highly secure due to the chaotic nature of the transformations.

The proposed design is an image encryption algorithm that processes the images in a set of transformative steps as listed below:

- Hénon Chaotic Transform
- Key Mixing
- 2D-Logistic Chaotic Transform

A sample of intermediate outputs detailing the overall stages of MMCBIE is shown in Figure 4.

Figure 5 displays the architecture's block diagram. The architecture of chaos-based image cryptosystems encompasses confusion and diffusion phases. The confusion phase, also known as the pixel permutation, occurs when the image is rendered unrecognizable by re-arranging the pixel positions over the whole image while leaving the pixel values the same. Because the previous phase is insecure and easily exploited by an attacker, the diffusion phase is employed. As a consequence, when the diffusion phase is performed with the help of a chaotic map, the chaotic systems' sequence alters the values of the pixels throughout the whole image sequentially. The confusion-diffusion technique is continued until an acceptable level of security is achieved.

The ongoing development of multimedia technology has improved digital data accessibility, including pictures, video, and audio data, via the Internet and public networks. In order to safeguard the enormous volume of data generated through the Internet every day, network security has therefore become a difficult problem. Images have several characteristics that set them apart from textual data, such as high data redundancy, dispersed information, big data sizes, a significant correlation between neighboring pixels, and bulk data capacity [42]. The encryption of two-dimensional images needs to be converted into one-dimensional data streams which are then encrypted using text-based cryptosystems. Text-based encryption results in identical decrypted texts and hence, bits must be retrieved with extreme precision in order to decrypt original messages. Digital multimedia applications do not, however, need to meet this condition because a little change in a pixel's property does not significantly impair the quality of the image. Additionally, the intensity values in an image's pixel data range from [0, 255]. The encrypted value for a pixel is established when

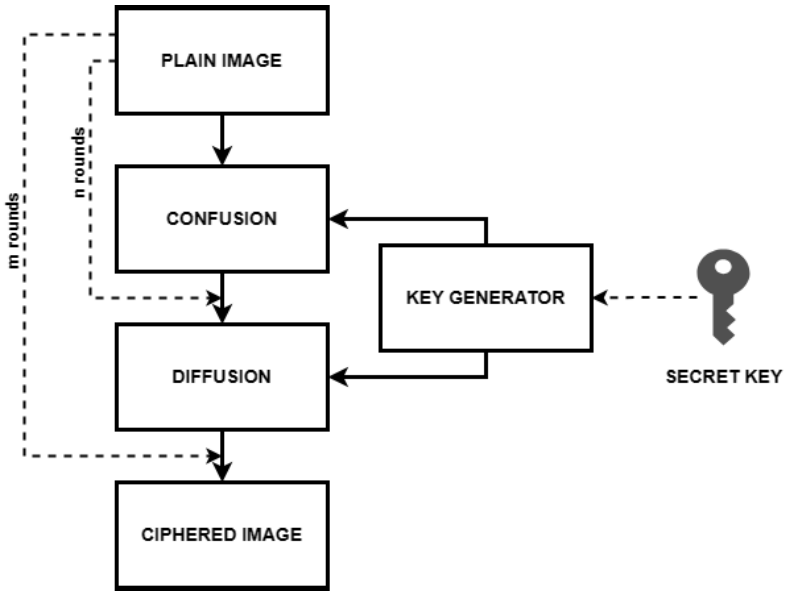


FIGURE 5. Chaos-based image cryptosystem architecture.

converting photos using traditional techniques according to the encryption key used, and because the pixel value appears several times in an image (data redundancy), the attacker may readily estimate that value. The optimal encryption method is one that requires the least amount of computing time without compromising security. Unfortunately, textual data is typically more effectively protected by traditional cryptographic techniques like AES, DES, TDES, IDEA, and RSA [43]. Due to the inherently unstable nature of pictures, these approaches are not appropriate for real-time image encryption. Furthermore, when carried out by commercial software, these procedures are difficult to execute and demand substantial computational resources.

A. HÉNON CHAOTIC TRANSFORM

The Hénon chaotic map, a two-dimensional chaotic map known for its well-defined entropy and verified chaotic behavior, is a pivotal component of our design. It is mathematically defined by the following equations:

$$x_{i+1} = 1 - ax_i^2 + y_i \tag{1}$$

$$y_{i+1} = bx_i, \tag{2}$$

where x and y are the pixel coordinates; a and b are the initial parameters of the chaotic map generation; i refers to the index of the pixel which takes values like 0, 1, 2 .... The optimal values which the Henon map displays are $a = 1.4$ and $b = 0.3$. For value ranges other than that specified, the maps generated display either a repetitive iteration or a diminishing iteration pattern that is easily recognizable. The part of the key that is provided to the Hénon map is the values of x_0 and y_0, from the subkeys x_H and y_H. Each value of x_0 and y_0 results in a unique chaotic map generated. The Hénon map is generated with the same dimensions as that of the input image. The generated Hénon transform map is used in a pixel-based XOR operation with the input image. This means that each input image pixel is XORed with the corresponding pixel value from the Hénon transform map.

Algorithm 1 Hénon/2D-Logistic Chaotic Transform

```
Input  : image, key
Output: Encrypted image
Transform(image,key)
ImageMatrix = Gen_Image_Matrix(image);
M,N = Get_Dimension(ImageMatrix);
ChaosMatrix = Gen_Chaos_Map(Dimension,key);
EncMatrix = [];
for i in range(M) do
    for j in range(N) do
        if color = RGB then
            for k in ImageMatrix[i][j] do
                Enc_Row = k ⊕ ChaosMatrix[i][j];
            end
        else if color = BW then
            Enc_Row = ImageMatrix[i][j] ⊕
              ChaosMatrix[i][j];
    end
end
EncMatrix = EncMatrix.append(Enc_Row);
EncImage = reshape(EncMatrix, Dimension);
return EncImage;
```

Figure 6 shows the trajectory path followed by the Hénon Map and Algorithm 1 shows the process followed by Hénon/2D-Logistic Chaotic Transform in encrypting an image.

Two scenarios are considered in this process: one for color images and another for black-and-white images. For color images, the RGB color space is utilized to transform the input image. Each pixel is divided into its red, green, and blue color components, and the corresponding values of each color component are XORed with the corresponding values from the generated Hénon transform map. In the case of a black-and-white image, the intensity value of each pixel is XORed with the value from the corresponding pixel from the Hénon intensity map.

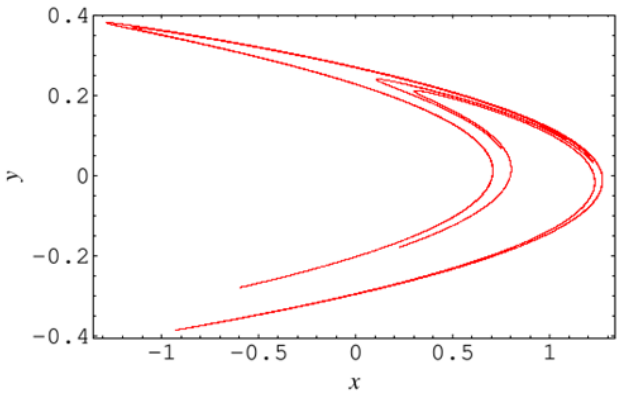


FIGURE 6. Trajectory of Hénon Map.

B. KEY MIXING

The key mixing stage consists of using a 192-bit key. The key is split into eight 24-bit parts, in which each 24-bit value corresponds to the RGB intensity values of a pixel. The output image obtained from the Hénon chaotic transform is fed as the input to this image. Then all the pixels of the image are treated as a one-dimensional array (in row-major order). This array undergoes cyclic RGB modulus addition with the key in a chaining order. This is mathematically expressed by the set of the following equations:

$$p_x[i] = \begin{cases} (p_Y[i] + p_Y[i-8]) \mod (L) & if\, i \geq 8 \\ (P_Y[i] + MK_Y[i]) \mod (L) & if\, i < 8 \end{cases}, \tag{3}$$

where $p_X[i]$ and $p_Y[i]$ denote the intensity value of the red, green, and blue color component at the i^{th} pixel in the image, and when X is R, then Y is G, when X is G, then Y is B, and when X is B, then Y is R; L denotes the maximum intensity value of each color component in the input image, which has a value of 2^{B-1} where B is the bit depth (this results in a value of 255); MK denotes the sub-key that is used for the key-mixing stage. The output of this stage is then fed as the input to the 2D-Logistic chaotic transform stage. Algorithm 2 depicts the process.

C. 2D-LOGISTIC CHAOTIC TRANSFORM

A two-dimensional logistic system is a chaotic system that provides superior entropy and security [4] over its one-dimensional counterpart and other well-known two-dimensional chaotic systems. It is mathematically expressed as:

$$x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \tag{4}$$

$$y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i), \tag{5}$$

where (x_i, y_i) is the x-coordinate and y-coordinate obtained at the i^{th} iteration; r is the initial parameter of the chaotic system. This stage uses the x_L, y_L, and r sub-keys from the primary key. The x_0 and y_0 values for the initial iteration are obtained from x_L and y_L respectively.The initial parameter r is the value of the r sub-key. Each combination of these three values creates a unique chaotic map. The generated

Algorithm 2 Key Mixing Stage

```
Function KEY_MIX (image, key) :
    ImageMatrix = Gen_Image_Matrix(image);
    M, N = Get_Dimension(ImageMatrix);
    for i in range(M) do
        for j in range(N) do
            1D_ImageMatrix = ImageMatrix[i][j];
        end
    end
    for k in range(M x N) do
        if color = RGB then
            if k < 8 then
                RowR=mod((RowG[k]+MKG[k]),L);
                RowG=mod((RowB[k]+MKB[k]),L);
                RowB=mod((RowR[k]+MKR[k]),L);
            end
            else
                RowR=mod((RowG[k]+MKG[k-
                  8]),L);
                RowG=mod((RowB[k]+MKB[k-
                  8]),L);
                RowB=mod((RowR[k]+MKR[k-
                  8]),L);
            end
            Enc_Row = merge(RowR, RowG, RowB);
        end
        else if color = BW then
            if k < 8 then
                Enc_Row = mod((Row[k] =
                  MK[k]),L);
            end
            else
                Enc_Row = mod((Row[k] =
                  MK[k-8]), L);
            end
        end
    end
    EncMatrix = EncMatrix.append(Enc_Row);
    EncImage = reshape(EncMatrix, Dimension);
return EncImage
```

2D logistic transform map is used in a pixel-based XOR operation with the output of the second stage. Color images are handled similarly to the way the first stage handles the XOR operation. The resulting image is the final cipher image. Figure 7 shows the trajectory path followed by the 2D-Logistic Chaotic Transform.

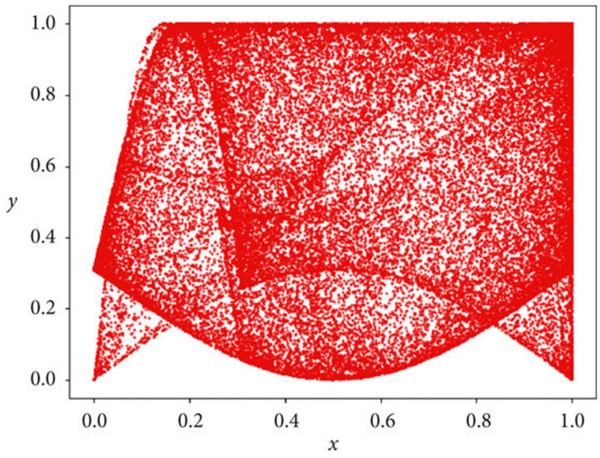


FIGURE 7. Trajectory of 2D-LSCM Map.

D. KEY STRUCTURE

The key is composed of six subkeys as shown in Figure 8, where x_H and y_H denote the initial values used in the Hénon chaotic transform stage; MK denotes the subkey used in the key-mixing stage; x_L, y_L, and R denote the initial values provided in order to generate the two-dimensional logistic map in the final stage. The only restriction on the values of any of the subkeys is on the value of R; keeping the value inside the range of 1.11 - 1.19 for optimal chaos [4] behavior is recommended.

In summary, the proposed image encryption method, called MMCBIE, involves three key transformation stages: Hénon Chaotic Transform, Key Mixing, and 2D-Logistic Chaotic Transform. The Hénon Chaotic Transform utilizes a two-dimensional chaotic map to generate a transformation map that is XORed with the input image. The Key Mixing stage involves a 192-bit key, which is cyclically added to the output of the Hénon transform, enhancing security. Finally, the 2D-Logistic Chaotic Transform employs a 2D logistic system, contributing to the confusion and diffusion phases for encryption. The entire process ensures the security of the encrypted image through chaotic transformations. The key structure comprises six subkeys, each playing a specific role in different stages of the encryption algorithm. The proposed design addresses the challenges of safeguarding multimedia data, considering the unique characteristics of images and the limitations of traditional cryptographic techniques in real-time image encryption.

V. EVALUATION

This section shows the performance and security of the proposed algorithm using end-to-end time analysis, key

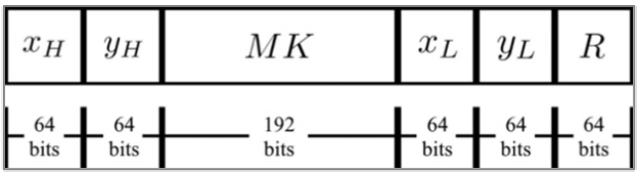


FIGURE 8. Key structure of MMCBIE.

sensitivity analysis, differential crypt-analysis, and much more. The results are compared with mainstream chaotic image encryption techniques spanning one-dimensional and two-dimensional chaotic systems. The analyses are grouped into four. First is the performance analysis in which the algorithm is tested against existing schemes on a dataset of images with varying sizes, from 64×64 to 1024×1024. The second group consists of the key space and the key sensitivity analysis. These results are obtained from the theoretical analysis of the key characteristics used in the encryption algorithm. The third group consists of all the tests that provide a metric score. In this group, testing is done on a dataset containing open-access images obtained from professional photography databases. These images are chosen in such a manner to have a variety of characteristics in structural information, color component intensity distribution, overall brightness and contrast, and saturation. The fourth group consists of all the tests that provide a plot/graph of the characteristics of the cipher image. In this group, testing is done on a 512×512 Lena image and the respective cipher images.

We explain the experimental analysis of the image encryption scheme we've put forward. To assess the algorithm's performance and security, we carried out a series of tests using a dataset sourced from professional photography databases. This dataset encompassed various image characteristics, including structural information, color component intensity distribution, brightness, contrast, and saturation. Our experiments aimed to highlight the stability and reliability of our proposed approach. Executing the code on numerous images revealed minimal variations in the results, indicating the consistency of our methodology. In terms of performance analysis, our focus zeroed in on the total time taken for encrypting and decrypting images using the proposed scheme. We compared the efficiency of our algorithm with other existing chaotic encryption schemes, underscoring the necessity for an efficient encryption algorithm tailored for IoT devices with power and performance constraints, as outlined in the paper [57]. The image encryption scheme proposed in [57] is rooted in chaos and incorporates a fusion of confusion and pixel scrambling methods to bolster security. The algorithm employs a secret key to generate initial states, permutation to shuffle pixel values, diffusion, and pixel scrambling in the matrix representation of pixels. We benchmarked this scheme against other algorithms such as 2DLSCM, Logistic tent map, and PWLCM. The study also suggests that further strides in security can be made by

TABLE 2. Performance analysis of various algorithms.

End-to-End Run-time Analysis of Various Algorithms (in seconds)						
Image Size	**Generic 1D Chaotic System (Arnold)**	**Generic 2D Chaotic System (Henon)**	**S-Box using complete Latin Square**	**Arnold's Cat & 2D-LSCM**	**Improved Baker's Map & Logistic Map**	**MMCBIE**
64 x 64	0.7842	1.2135	0.5067	1.74	0.2639	0.112
128 x 128	3.4678	4.9823	1.7391	6.868	2.5649	0.564
512 x 512	6.8245	12.4321	4.3498	28.76	4.6574	1.349
1024 x 1024	14.9834	27.5946	6.8321	113.75	12.3088	2.0251

integrating different chaos algorithms, employing additional chaos techniques, and increasing the number of iterations for confusion. Additionally, it proposes a runtime analysis of the encryption and decryption processes and advocates the use of different algorithms for enhanced performance. Our algorithm's results, as presented in this document, encompass a variety of tests conducted on the cipher images. These tests involve metrics such as Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM). We also conducted a comparative analysis of our algorithm's performance against other encryption techniques based on these metrics. In summary, the experimental content of this document serves to underscore the effectiveness, efficiency, and security of our proposed image encryption scheme.

All images utilized in this paper were sourced from LHQ (Landscapes High Quality). LHQ represents a comprehensive image dataset featuring high-resolution landscape images. Comprising 90,000 images with a resolution of 1024×1024, the dataset encompasses a diverse array of natural and urban landscapes. This dataset is made available under the CC0: Public Domain license [49]. For the purposes of our analysis, we dynamically transformed these images into sizes of 64 × 64 pixels, 128 × 128 pixels, and 512 × 512 pixels. Our assessment of the dataset indicates its suitability, as evidenced by consistent results across multiple images. To showcase the stability of our approach, we executed the code on numerous images, choosing to display only 10 representative samples. Through this experimentation, we observed minimal variations in results, affirming the reliability of our methodology based on prior experience.

A. PERFORMANCE ANALYSIS

This test explores and corroborates the total time taken to encrypt and decrypt images using the proposed scheme. The algorithm must be efficient for an IoT encryption scheme and consume less time to encrypt and decrypt the data due to its power and performance limitations. Therefore, a test like this will prove that the algorithm is more efficient than the other existing chaotic encryption schemes and can be a good candidate for securing the sensitive images transmitted among IoT devices.

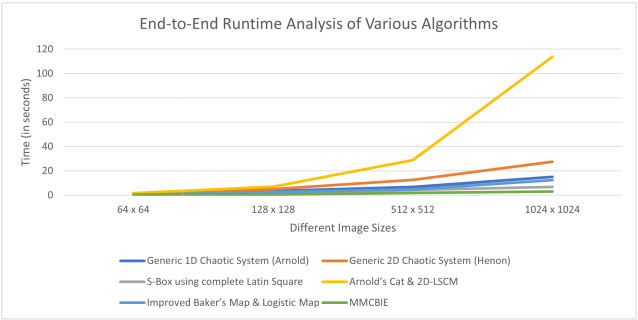


FIGURE 9. Performance analysis of various encryption algorithms.

From Table 2 and Figure 9, it is evident that the proposed MMCBIE scheme is significantly more efficient than the other comparable multi-chaotic map-based schemes, making it a viable option for a standardized IoT image encryption scheme.

B. KEY SPACE ANALYSIS

This analysis examines and confirms that the secret key used in the scheme is properly defined and of sufficient size. The primary key for encrypting the input image is a 512-bit key divided into six parts, as discussed before. The largest sub-key is the key used in the key-mixing stage. Its key length (192 bits) is on par with and/or better than other standard symmetric algorithms for data encryption, such as AES, DES, and other symmetric encryption variants. By induction, Brute force attacks [57] and other attacks relying on an insufficient or small key space of the algorithm are effectively resisted.

C. KEY SENSITIVITY ANALYSIS

This is an overall analysis of the change induced by a unit change in the key that is used to encrypt the input image or a unit change in the input image itself. Changing one bit of the key can be applied to any of the sub-keys, i.e., the one-bit change will be applied as a change to either one of the sub-keys x_H, y_H, MK, x_L, y_L or R, while the other sub-keys remain unchanged. A change in x_H or y_H completely changes the output of the Hénon chaotic system, resulting in a chaotic map that is different from the original map, which results in the output of the first stage of MMCBIE being different. Similarly, a change in x_L, y_L, or R

TABLE 3. NPCR score comparison between various encryption schemes.

NPCR Scores						
Image	**Generic 1D Chaotic Scheme (Arnold)**	**Generic 2D Chaotic Scheme (Henon)**	**S-Box using complete Latin Square**	**Arnold's Cat & 2D-LSCM**	**Improved Baker's Map & Logistic Map**	**MMCBIE**
1	99.0322	99.9819	99.6201	99.5407	99.5727	99.6015
2	99.0597	99.9917	99.6094	99.4158	99.4582	99.6127
3	99.2549	99.818	99.6399	99.4280	99.4063	99.6078
4	99.4	99.9558	99.6460	99.5884	99.6322	99.608
5	99.3888	99.8109	99.5850	99.2396	99.3089	99.6099
6	98.9775	99.701	99.6133	99.4598	99.6116	99.6088
7	98.4908	99.9102	99.6051	99.4756	99.6037	99.6131
8	99.2968	99.9991	99.6318	99.2527	99.6030	99.6098
9	98.4138	100	99.5359	99.2493	99.2019	99.6099
10	98.8291	99.7961	99.6288	99.3545	99.4032	99.611
Average	**99.0144**	**99.8965**	**99.66153**	**99.4004**	**99.4036**	**99.6093**

significantly changes the output of the 2D logistic chaotic system, resulting in a chaotic map that is different from the original map, which results in the output of the last stage of MMCBIE being different. If the change is applied to MK, this results in a different additive value being compounded over each pixel and cycled overall color components (red, blue, and green). This results in a significantly differing output of the second stage compared with the output generated with the original value of MK. This ensures the security of the image encryption scheme against sensitive-key attacks. This is further shown using the NPCR and UACI tests, whose respective scores show that the algorithm is resistant to key-sensitive attacks.

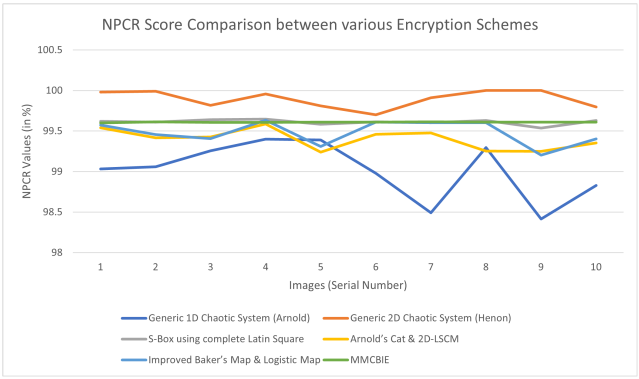


FIGURE 10. NPCR score comparison between generic chaos-based image encryption and MMCBIE.

D. NUMBER OF PIXEL CHANGING RATE (NPCR)

In this test for differential crypt-analysis, the original image and the cipher image are compared to find the number of pixels that are different at each point in the image grid. The NPCR test scores are shown in Table 3 and Figure 10. From the table, we can see that all the algorithms maintain a high degree of resistance toward chosen-plain text differential attacks by virtue of being able to manipulate a high value of pixels with a unit change in the input image or the key. While the generic 2D chaotic encryption scheme does have a marginally higher score than MMCBIE, this is negligible as this measure the actual percentage of pixels that is subject to change and not the difference between the intensity of those pixels. NPCR is given by the following equation:

$$NPCR(E_1, E_2) = \sum_{i=1}^{I} \sum_{j=1}^{J} \frac{W(i,j)}{N} \times 100, \tag{6}$$

where E_1 and E_2 are two encrypted images, N represents the total number of pixels in an image and $W(i,j)$ is defined by the following equation:

$$W(i,j) = \begin{cases} 0, & E_1(i,j) = E_2(i,j) \\ 1, & E_1(i,j) \neq E_2(i,j), \end{cases} \tag{7}$$

E. UNIFIED AVERAGE CHANGED INTENSITY (UACI)

This test is a form of differential crypt-analysis that provides a method to evaluate the strength of an image encryption scheme by measuring the averaged difference between the input image and the cipher image, measuring the average change in intensity of a pixel value over the whole pixel grid. The UACI test scores are shown in Table 4 and Figure 11. This result shows an insufficient change in averaged intensity change across the 1D chaotic encryption scheme, while the 2D chaotic encryption scheme and MMCBIE maintain higher scores. This shows that both of these algorithms will be able to resist differential attacks that specifically target intensity change instead of positioning (which is indicated by NPCR). UACI is given by the following equation:

$$UACI(E_1, E_2) = \sum_{i=1}^{I} \sum_{j=1}^{J} \frac{|E_1(i,j) - E_2(i,j)|}{N \times Q} \times 100, \tag{8}$$

where Q is the maximum possible value of a pixel in an image.

TABLE 4. UACI score comparison between various encryption schemes.

UACI Scores						
Image	**Generic 1D Chaotic Scheme (Arnold)**	**Generic 2D Chaotic Scheme (Henon)**	**S-Box using complete Latin Square**	**Arnold's Cat & 2D-LSCM**	**Improved Baker's Map & Logistic Map**	**MMCBIE**
1	22.9231	36.6868	33.6123	33.0887	33.2721	34.9803
2	17.6944	32.0461	33.4635	33.3712	33.2801	28.5709
3	21.3578	35.1223	33.4320	33.3485	33.7577	33.0088
4	28.6208	33.8617	33.4381	33.4026	33.7287	31.3456
5	30.3043	35.956	33.4671	33.3761	33.1388	33.9177
6	30.7203	37.9271	34.5613	33.0898	33.1140	36.9721
7	18.4805	30.6655	33.5432	33.2521	33.4040	28.3811
8	26.1823	37.326	33.4215	33.1619	33.4474	35.8712
9	12.5976	34.3134	33.5147	33.7421	33.6199	32.0123
10	12.228	35.3592	33.4502	33.0827	33.8273	33.7685
Average	**22.1109**	**34.9264**	**33.58939**	**33.2916**	**33.4590**	**32.8828**

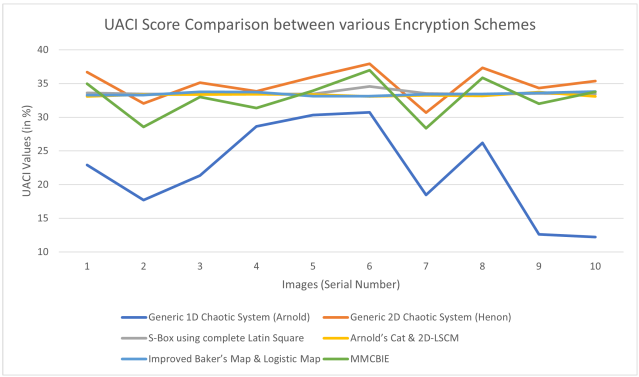


FIGURE 11. UACI Score comparison between generic Chaos-based image encryption and MMCBIE.

F. MEAN SQUARED ERROR (MSE)

This test is employed to assess the visual disparity between the input image and the cipher image. It involves calculating the squared difference of each pixel in the pixel grid between the original image and the cipher image and the cipher image, which is then divided by the number of pixels of the image. The mean squared error compared to the input and cipher images of each algorithm is shown in 5 and Figure 12. This comparison shows that the 2D chaotic encryption algorithm provides the more quantified difference between the input and cipher images, followed by MMCBIE and then the 1D chaotic encryption algorithm. However, it is worth noting that this difference in scores will not be consistently reflected across all input values and input images. To account for this variation in scores across a different scenario, we also utilize RMSE score comparison, shown in the next subsection. MSE is given by the following equation:

$$MSE = \frac{1}{N} \times \dot{}[(P(x,y) - E(x,y))^2], \tag{9}$$

In the given context, N represents the total number of pixels in the image, $P(x,y)$ represents the pixel intensity of the corresponding pixel in the input image, and $E(x,y)$ represents the pixel intensity of the corresponding pixel in the encrypted image.

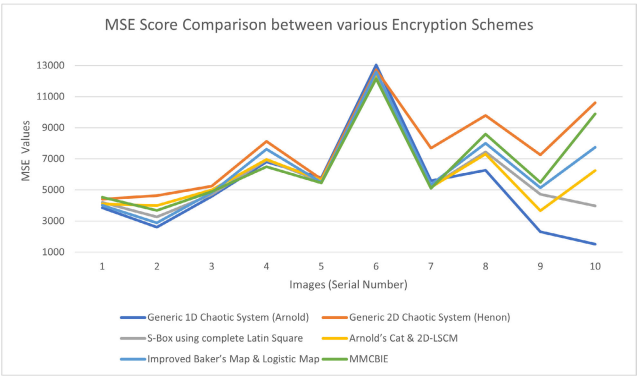


FIGURE 12. MSE score comparison between generic chaos-based image encryption and MMCBIE.

G. ROOT MEAN SQUARED ERROR (RMSE)

RMSE is derived from the square root of the MSE, offering a more comprehensive measure of the relative difference between two images under specific conditions. The root-mean-squared error compared with the input and cipher image of each algorithm is shown in 6 and Figure 13. This comparison shows a higher difference between the original and cipher images in the 2D chaotic encryption algorithm and MMCBIE. In comparison, the 1D chaotic encryption algorithm shows a significantly weaker difference. Compared to the mean squared error comparison, this shows a lesser score deviation over different input scenarios. Root Mean Square (RMSE) is given by the following equation:

$$RMSE = \sqrt{\frac{1}{N} \times \dot{}[(P(x,y) - E(x,y))^2]}, \tag{10}$$

TABLE 5. MSE score comparison between various encryption schemes.

MSE Scores						
Image	**Generic 1D Chaotic Scheme (Arnold)**	**Generic 2D Chaotic Scheme (Henon)**	**S-Box using complete Latin Square**	**Arnold's Cat & 2D-LSCM**	**Improved Baker's Map & Logistic Map**	**MMCBIE**
1	3852.4445	4410.1854	4201.7536	4087.5618	4012.1193	4524.9394
2	2607.7634	4626.5659	3254.9867	3987.2365	2872.6489	3681.8771
3	4575.9326	5248.3631	4703.8185	4992.1402	4826.5797	4885.2061
4	6794.8915	8130.9825	6923.7436	6956.5309	7615.2467	6494.9525
5	5787.4087	5697.7712	5543.1123	5631.2679	5479.6345	5440.4422
6	13035.2457	12727.9066	12432.7342	12318.2211	12584.6903	12159.0055
7	5582.5632	7684.5585	5227.8901	5175.2678	5343.1892	5098.5247
8	6269.8801	9783.3022	7446.1234	7310.9876	7998.4567	8592.179
9	2312.8878	7247.637	4725.3012	3658.8765	5142.6453	5477.1221
10	1515.6126	10611.5439	3978.2354	6247.8872	7732.4198	9899.9489
Average	**5233.4630**	**7616.8816**	**5993.77088**	**6927.65185**	**7270.76587**	**6625.4198**

Here, N represents the total number of pixels in the image, $P(x, y)$ denotes the pixel intensity of the corresponding pixel in the input image, and $E(x, y)$ signifies the pixel intensity of the corresponding pixel in the encrypted image.

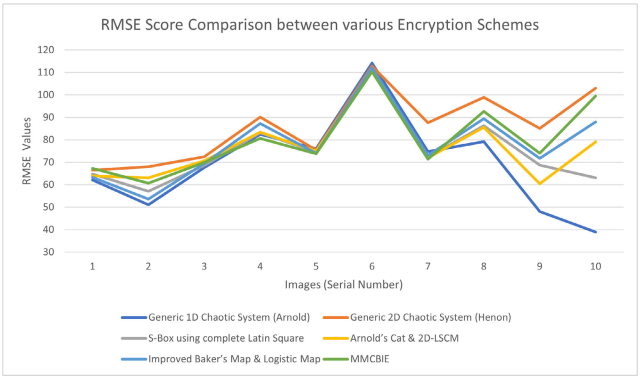


FIGURE 13. RMSE score comparison between generic chaos-based image encryption and MMCBIE.

H. PEAK SIGNAL-TO-NOISE RATIO (PSNR)

This test measures the degradation caused by trans-formative processes, such as compression, enhancement, reconstruction, and more, on images. This process finds the quality of such trans-formed images with reference to the original image.

If the value obtained is high, it means that the reconstructed image is similar to the original image. The peak signal-to-noise ratio comparison of the cipher images is given in 7 and Figure 14. The lower the signal-to-noise ratio is, the higher the strength of encryption since the cipher image is perceived to have more noise when compared to the original image. However, all the cipher images in this comparison have ratios that do not show a clear advantage over one another and are quite close to one another. This shows that each image appears to be well-randomized from the original image with regard to the PSNR criterion. Peak Signal-To-Noise Ratio (PSNR) is defined using the following equation:

$$PSNR = 20 \times \log_{10}(Q) - 10 \times \log_{10}(MSE), \quad (11)$$

where Q denotes the maximum potential pixel intensity value of the image, and MSE refers to the Mean Square Error, as defined by equation (9), which quantifies the difference between the original image and the encrypted image.

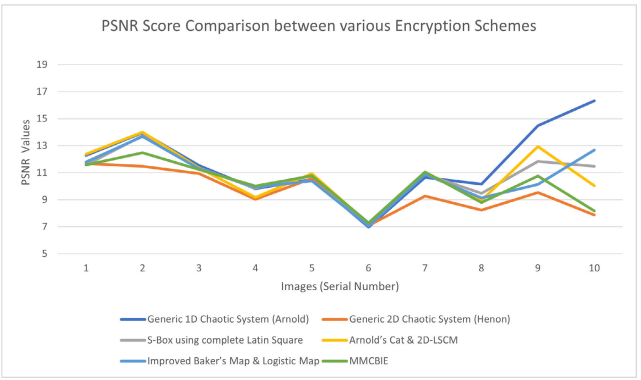


FIGURE 14. PSNR score comparison between generic chaos-based image encryption and MMCBIE.

I. STRUCTURAL SIMILARITY INDEX (SSIM)

The comparison between Structural Similarity Index values for each cipher image is given in 8 and Figure 15. A lower value obtained in the Structural Similarity Index test shows a lack of image features found in the cipher image when compared to the other cipher images. However, in this comparison, all cipher images have sufficient deviance from the visual features in regard to the structural information that is perceived from the original image. However, this does not account for similarities or dissimilarities in color,

TABLE 6. RMSE score comparison between various encryption schemes.

RMSE Scores						
Image	**Generic 1D Chaotic Scheme (Arnold)**	**Generic 2D Chaotic Scheme (Henon)**	**S-Box using complete Latin Square**	**Arnold's Cat & 2D-LSCM**	**Improved Baker's Map & Logistic Map**	**MMCBIE**
1	62.0681	66.4092	64.8209	63.9340	63.3413	67.2677
2	51.0663	68.0189	57.0525	63.1446	53.5971	60.6785
3	67.6456	72.4456	68.5844	70.6551	69.4736	69.8942
4	82.4311	90.172	83.209	83.4058	87.2654	80.5913
5	76.075	75.4836	74.4521	75.0418	74.0246	73.7594
6	114.172	112.818	111.5022	110.9875	112.1815	110.2679
7	74.7166	87.6616	72.3041	71.9393	73.0971	71.404
8	79.1826	98.9106	86.2909	85.5043	89.4341	92.694
9	48.0925	85.1331	68.7408	60.4886	71.7122	74.0076
10	38.9309	103.0123	63.0733	79.0436	87.9342	99.4985
Average:	**69.4381**	**86.0065**	**75.003**	**76.4145**	**78.2061**	**80.0063**

TABLE 7. PSNR score comparison between various encryption schemes.

PSNR Scores						
Image	**Generic 1D Chaotic Scheme (Arnold)**	**Generic 2D Chaotic Scheme (Henon)**	**S-Box using complete Latin Square**	**Arnold's Cat & 2D-LSCM**	**Improved Baker's Map & Logistic Map**	**MMCBIE**
1	12.2734	11.6862	11.5748	12.3712	11.7912	11.5747
2	13.9681	11.4782	13.745	14.002	13.678	12.4701
3	11.5260	10.9306	11.3525	11.3652	11.2894	11.2420
4	9.8090	9.0294	9.8447	9.1623	9.9306	10.0050
5	10.5060	10.5738	10.7746	10.9347	10.4024	10.7745
6	6.9796	7.0832	7.1234	7.2007	7.0425	7.2818
7	10.6625	9.2746	10.8912	10.9807	10.8763	11.0564
8	10.1582	8.2259	9.4786	8.9612	9.1247	8.7898
9	14.4893	9.5288	11.8436	12.9327	10.1275	10.7453
10	16.3249	7.8730	11.4726	10.0397	12.6754	8.1745
Average:	**11.6697**	**9.5684**	**10.70484**	**10.89688**	**10.79386**	**10.2114**

which will be shown in RGB histogram analysis. The Structural Similarity Index (SSIM) can be represented using the following equation:

$$SSIM(x, y) = P(x, y) \times C(x, y) \times S(x, y) \tag{12}$$

The brightness similarity between the plain image and the encrypted image is shown in the context by $P(x, y)$, whereas the contrast and structural similarities are indicated by $C(x, y)$ and $S(x, y)$, respectively. These three factors, which are determined using the following formulae, together yield the overall SSIM score.

$$E(x, y) = \frac{2 \times \mu_x \times \mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \tag{13}$$

$$C(x, y) = \frac{2 \times \sigma_x \times \sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \tag{14}$$

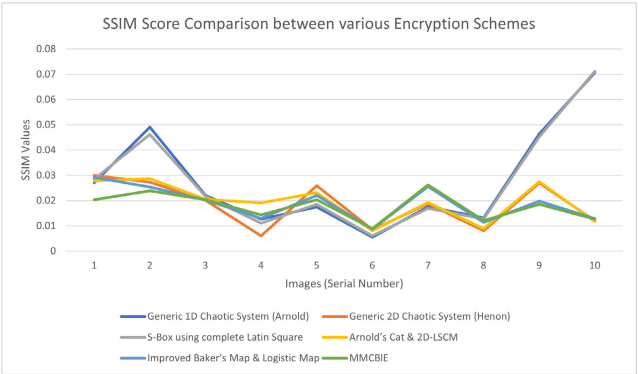


FIGURE 15. SSIM score comparison between generic chaos-based image encryption and MMCBIE.

$$S(x, y) = \frac{\sigma_{xy} + C_3}{\sigma_x \times \sigma_y + C_3} \tag{15}$$

TABLE 8. SSIM score comparison between various encryption schemes.

SSIM Scores						
Image	**Generic 1D Chaotic Scheme (Arnold)**	**Generic 2D Chaotic Scheme (Henon)**	**S-Box using complete Latin Square**	**Arnold's Cat & 2D-LSCM**	**Improved Baker's Map & Logistic Map**	**MMCBIE**
1	0.0271	0.03	0.0285	0.0278	0.0292	0.0203
2	0.0491	0.0273	0.0462	0.0287	0.0254	0.0238
3	0.022	0.0201	0.0217	0.0205	0.0202	0.0203
4	0.0126	0.006	0.011	0.019	0.013	0.0143
5	0.0174	0.0259	0.0185	0.0231	0.0220	0.0203
6	0.0055	0.0085	0.0060	0.0080	0.0087	0.0089
7	0.0175	0.0187	0.0169	0.0193	0.0256	0.0262
8	0.0132	0.008	0.0127	0.0089	0.0113	0.0121
9	0.0464	0.0269	0.0452	0.0275	0.0198	0.0185
10	0.0706	0.012	0.0712	0.0117	0.0129	0.0126
Average:	**0.0281**	**0.0183**	**0.02669**	**0.01855**	**0.01881**	**0.0177**

In the aforementioned situation, x and y stand for the means of the plain and encrypted images, respectively, while x and y stand for their corresponding standard deviations. The covariance between the plain image and the encrypted image is also shown by the symbol σ_{xy}. The minuscule constants C_1, C_2, and C_3 are added to prevent division by zero.

J. PEARSON'S CORRELATION COEFFICIENT (PCC)

This test measures the degree of correlation between two data sources. When this test is conducted on a cipher image and the respective input image, the coefficient should be close to zero for the image encryption algorithm to be considered sufficiently secure.

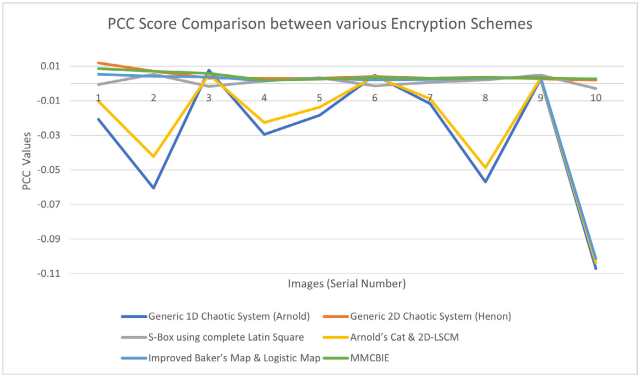


FIGURE 16. PCC score comparison between generic chaos-based image encryption and MMCBIE.

The comparison between Pearson's correlation coefficients for each cipher image is given in 9 and Figure 16. The equation that defines the Pearson's Correlation Coefficient (PCC) is as follows:

$$PCC = \frac{Covariance(P, E)}{\sigma_P, \sigma_E} \tag{16}$$

The correlation between the input image and the cipher image is stronger when using the 1D chaotic encryption technique, which has a higher absolute value. Contrarily, the correlation coefficients produced from the MMCBIE and 2D chaotic encryption techniques are nearer to 0, indicating that there is no obvious connection between the cipher image and the input image. However, the RGB histogram analysis will look at colour disparities and similarities, which are not considered in this analysis.

The covariance between the pixel intensities of the plain image and the encrypted image is represented in the context by $Covariance(P, E)$. The standard deviations of the pixel intensities in the plain image and the encrypted image, respectively, are also indicated by the letters P and E.

K. SHANNON'S ENTROPY

Local Shannon's entropy is given by the following equation:

$$H(E) = -\sum_{n=1}^{N} P(n) \times \log_2(P(n)), \tag{17}$$

where $P(n)$ is the likelihood that a given pixel in the image exists and $H(E)$ is the local Shannon entropy of the encrypted image.

The entropy of any data source refers to the degree of uncertainty or randomness encountered from the source's data. This measure of randomness, when run on a cipher image encrypted with a sufficiently secure encryption algorithm, should provide a high value. The comparison for scores obtained from the Shannon entropy test across the cipher images is shown in 10 and Figure 17. In this test, it is observed that MMCBIE performs better than the 1D and the 2D chaotic encryption schemes by providing a cipher image that is more characteristically like a completely random data stream.

TABLE 9. PCC score comparison between various encryption schemes.

PCC Scores						
Image	**Generic 1D Chaotic Scheme (Arnold)**	**Generic 2D Chaotic Scheme (Henon)**	**S-Box using complete Latin Square**	**Arnold's Cat & 2D-LSCM**	**Improved Baker's Map & Logistic Map**	**MMCBIE**
1	-0.0207	0.012	-0.0005	-0.0102	0.0054	0.0086
2	-0.0605	0.0071	0.0054	-0.0423	0.0042	0.0071
3	0.0077	0.0032	-0.0017	0.0053	0.0038	0.0058
4	-0.0294	0.003	0.0015	-0.0225	0.0017	0.002
5	-0.0183	0.0031	0.00342	-0.0137	0.00305	0.0025
6	0.0047	0.0042	-0.00127	0.0041	0.0021	0.0035
7	-0.0116	0.0031	0.00076	-0.0089	0.0024	0.003
8	-0.0569	0.0036	0.00215	-0.0487	0.0030	0.0035
9	0.0026	0.0027	0.00493	0.0031	0.0036	0.0032
10	-0.1071	0.002	-0.00288	-0.1039	-0.1015	0.0028
Average:	**-0.029**	**0.0043**	**0.000880**	**-0.02339**	**0.002762**	**0.0042**

TABLE 10. Shannon's entropy score comparison between various encryption schemes.

Shannon's Entropy Scores						
Image	**Generic 1D Chaotic Scheme (Arnold)**	**Generic 2D Chaotic Scheme (Henon)**	**S-Box using complete Latin Square**	**Arnold's Cat & 2D-LSCM**	**Improved Baker's Map & Logistic Map**	**MMCBIE**
1	7.4458	7.5419	7.7235	7.9887	7.8998	7.6611
2	6.9917	7.6186	7.4000	7.9874	7.8883	7.608
3	7.445	7.5226	7.3785	7.9974	7.3032	7.6826
4	7.8042	7.8874	7.6215	7.9974	7.3871	7.761
5	7.6668	7.581	7.7091	7.9993	7.8993	7.6655
6	7.1514	7.8059	7.3542	7.9993	6.5503	7.8899
7	6.6984	7.6156	7.2763	7.9992	7.8887	7.5699
8	7.4353	7.8073	7.6771	7.9987	7.9992	7.7853
9	6.8183	7.7516	7.8302	7.9998	7.9993	7.7009
10	6.6997	7.8815	7.7554	7.9998	7.9997	7.9289
Average:	**7.2157**	**7.7014**	**7.61268**	**7.9967**	**7.6815**	**7.7253**

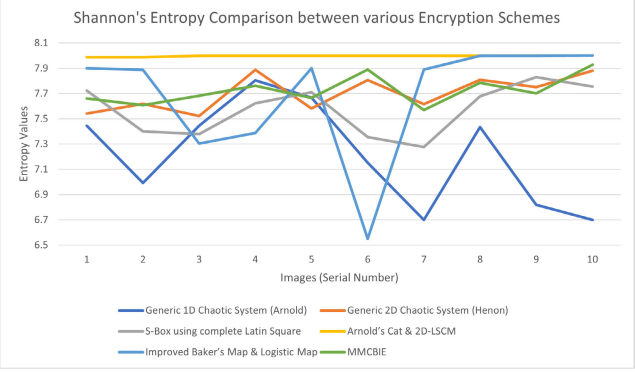


FIGURE 17. Shannon's entropy score comparison between generic chaos-based image encryption and MMCBIE.

L. GLCM MATRIX ENTROPY (SHANNON)

This provides a method to highlight the features of an image by a matrix in which each value indicates the number of times a pair indicated by the gray levels is separated by the specified distance vector used to generate the matrix. The generated matrix is analyzed for randomness by means of the Shannon entropy test. The comparison for scores obtained from the Shannon entropy test on the matrix of grey-level co-occurrence across the cipher images is shown in 11 and Figure 18.

This test shows that MMCBIE performs better than the 1D chaotic encryption scheme and is on par with the 2D chaotic encryption algorithm. This is because MMCBIE provides a cipher image whose grey-level co-occurrence matrix shows more random characteristics. By induction, the features extracted from the image by means of the matrix of grey-level co-occurrence are random.

M. AUTO-CORRELATION PLOT

To measure the degree to which these similarities are reduced, a graph of adjacent pixels is plotted, which displays their correlation. A cipher image plot produced by a strong

TABLE 11. GLCM matrix entropy score comparison between various encryption schemes.

GLCM Matrix Entropy Scores						
Image	**Generic 1D Chaotic Scheme (Arnold)**	**Generic 2D Chaotic Scheme (Henon)**	**S-Box using complete Latin Square**	**Arnold's Cat & 2D-LSCM**	**Improved Baker's Map & Logistic Map**	**MMCBIE**
1	2.9516	3.0812	3.0204	3.0578	3.0087	3.0796
2	2.0118	3.1736	2.7324	3.1239	2.3456	3.2157
3	4.0274	4.3363	4.2567	4.1723	4.3221	4.3886
4	6.2424	6.1487	6.1832	6.1917	6.2258	6.1465
5	6.1772	6.3191	6.2948	6.2013	6.2827	6.2801
6	5.7097	6.31	5.8451	5.7389	5.8646	5.9802
7	4.642	6.3407	4.9813	5.7742	5.2531	6.3372
8	6.2326	6.3507	6.1798	6.1573	6.2189	6.1151
9	4.8599	6.4111	5.7584	5.1123	5.9846	6.228
10	4.1566	6.2958	6.3592	4.5327	6.5681	6.7768
Average:	**4.7011**	**5.4767**	**5.09713**	**4.93427**	**5.10386**	**5.4548**

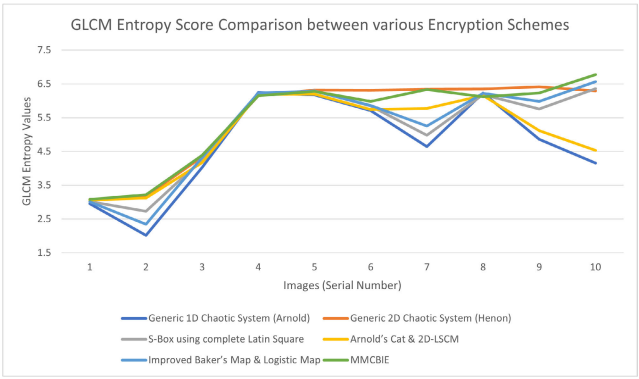


FIGURE 18. GLCM matrix entropy score comparison between generic chaos-based image encryption and MMCBIE.

image encryption algorithm should not reveal any groups of localized points and should be as random as possible.

The two images are displayed in the Figure 19 plots together with the neighboring pixel auto-correlation plot of the original image (Figure 19 (a)). A way to see the intensity pairs of the neighboring pixels in an image is via the adjacent-pixel auto-correlation graphic. The original image's plot displays a group of points grouped linearly. This shows that the image contains many adjacent pixel pairs with similar intensity levels.

The plot of the 1D chaotic encryption scheme shows a perceptive 'widening' of the plot of the original image to the axes. However, it is to be noted when comparing the plot of the original image and that of the 1D chaotic encryption that the individual pixel intensities do not change, which is apparent from the movement of the points of the plot linearly (parallel to either of the axes), indicating a change in adjacent pixel value but not the original pixel.

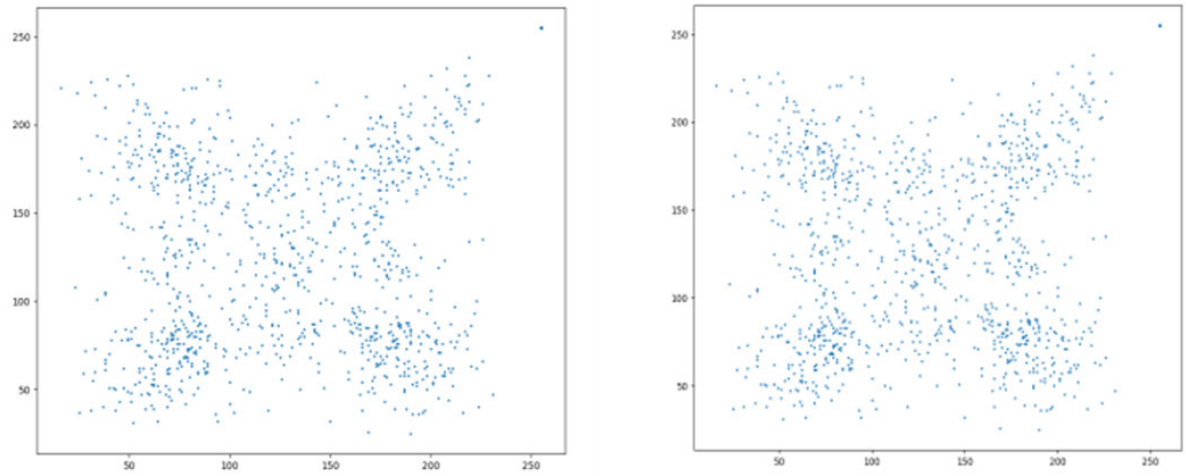
When comparing the original image's plot to that of the 2D chaotic encryption, we see some localization of certain points in some areas of the plot of the 2D chaotic encryption scheme. This shows that the pixels of varying intensities are not distributed uniformly over the image, suggesting a lack of randomness or possible extraction of visual information from the cipher image.

From the auto-correlation plot of the cipher image generated by MMCBIE, the scattered nature of the points indicate that the pixels of varying intensities are distributed uniformly over the cipher-image, which is required for the security of the visual information of the original image.

N. COLOR COMPONENT INTENSITY ANALYSIS USING RGB HISTOGRAM

Color component intensity analysis of cipher images ages is analogous to letter frequency and dictionary analysis for cipher texts. The histogram depicts the intensity distribution of the different color components of the image. A robust image encryption algorithm should generate cipher images with uniformly distributed histograms for each color component. One component's average intensity should not overshadow another component's average intensity. The RGB intensity histograms of the three cipher images (Figures 20b), 20(c), and 20(d)) and the original image's original image are shown in the Figure 20 plots. The RGB intensity histogram provides a simple method by which one can perform color-component analysis.

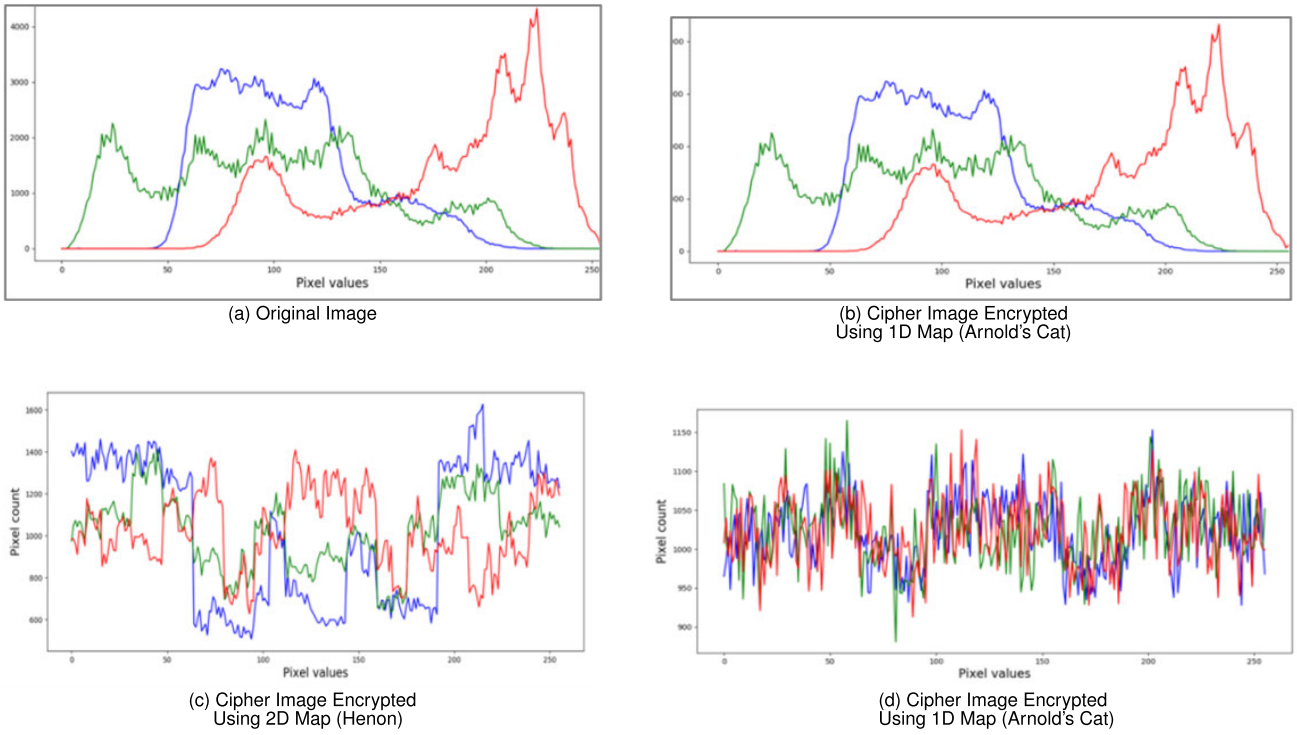
The original image's histogram, shown in Figure 20a, shows distinct values for the red, green, and blue color components. Even without having direct access to the original image, certain qualities of the image can be inferred by analyzing the intensity of each component. The histogram in Figure 20b shows the cipher images created using the 1D chaotic encryption method. When comparing this histogram with the original image, it is observed that the histograms are like each other. This means that while the 1D chaotic encryption scheme achieves confusion by transposing pixels across the image grid, it does not modify



(a) Original Image

(b) Cipher Image Encrypted Using 1D Map (Arnold's Cat)

FIGURE 19. Adjacent pixel auto-correlation plot of the original image and the three cipher-Images.



(a) Original Image

(b) Cipher Image Encrypted Using 1D Map (Arnold's Cat)

(c) Cipher Image Encrypted Using 2D Map (Henon)

(d) Cipher Image Encrypted Using 1D Map (Arnold's Cat)

FIGURE 20. RGB intensity histogram of the original image and the three cipher-images.

the intensity of the color components. The absence of the substitution/modification of these values shows the weakness of the algorithm. The histogram of the generated with the help of 2D chaotic encryption method is shown in Fig 20c. When comparing this histogram with the original image, it is observed that the histograms do not pose any similarity. From this observation, it can be inferred that the 2D chaotic encryption scheme applies substitution/modification of intensity values of color components in the original image. While providing higher strength when compared to the 1D chaotic encryption scheme, the histogram does not show the ideal uniformity required for higher strength. Fig. 20d shows the histogram of the cipher picture produced by MMCBIE. As discussed earlier, for an image encryption scheme that handles colors, the intensity histogram of the color components should be as uniformly distributed as possible. The intensity histogram of this scheme does not only bear any resemblance to that of the original image but also

TABLE 12. Summary of all security analysis.

Results (Average)	Generic 1D Chaotic Scheme (Arnold)	Generic 2D Chaotic Scheme (Henon)	S-Box using complete Latin Square	Arnold's Cat & 2D-LSCM	Improved Baker's Map & Logistic Map	MMCBIE	Performed Better? (Y/N)
NPCR	99.014	99.8965	99.6615	99.4004	99.4036	99.6093	Y
UACI	22.1109	34.9264	33.5894	33.2916	33.4590	32.8828	Y
MSE	5233.463	7616.8816	5993.7709	6927.6519	7270.7659	6625.4198	Y
RMSE	69.4381	86.0065	75.003	76.4145	78.2061	80.0063	Y
PSNR	11.6697	9.5684	10.7048	10.8969	10.7939	10.2114	Y
SSIM	0.0281	0.0183	0.0267	0.0185	0.0188	0.0177	Y
PCC	-0.029	0.0043	0.0008	-0.0233	0.0027	0.0042	Y
Shannon's Entropy	7.2157	7.7014	7.6127	7.9967	7.6815	7.7253	Y
GLCM	4.7011	5.4767	5.0971	4.9342	5.1039	5.4548	Y

shows a highly uniform distribution of each color component across the full range of intensity (0-255). Table 12, shows a summary of the security analysis tests conducted and in which analysis, our proposed algorithm performs better.

VI. RESULTS AND DISCUSSION

We provide a thorough analysis of our proposed design's performance metrics by emphasizing not only its efficacy but also its efficiency in real-world scenarios. To substantiate our claims, we conducted multiple iterations of the code, consistently obtaining unchanged values, thereby attesting to the accuracy and reliability of our results.

Unlike other methods, MMCBIE turns encrypted images into something that looks like random visual noise, making it really tough to distinguish from the original. This unique trait makes MMCBIE a standout in protecting digital images in the world of IoT. We tested MMCBIE thoroughly to make sure it's not just good in theory but in practical situations. Our tests show that MMCBIE has excellent security features, making it strong against potential attacks and decoding attempts. By paying close attention to the special traits of digital images and showcasing MMCBIE's unparalleled security, our solution can be considered reliable for keeping images secure in IoT applications.

A summary of all the results obtained in the previous section can be found below and also in Table 12.

MMCIE's improved performance is due to its optimized multi-chaotic map-based methodology, which ensures faster image data processing and makes it a viable competitor for safeguarding sensitive images in IoT communications. In comparison to other symmetric encryption alternatives, the painstaking design of MMCBIE's key structure, with an emphasis on suitable size and complexity, improves its resistance to attacks, offering a safe foundation for data encryption. The secure connection between the essential components of MMCBIE, such as Hénon chaotic system parameters and 2D logistic chaotic system variables, strengthens its resistance to critical sensitivity attacks. This, together with the varying impact of key modifications at different phases, contributes to the algorithm's better security. MMCIE's ability to maintain a high NPCR score demonstrates its ability to withstand differential attacks, protecting the integrity of the encrypted image by intentionally altering pixel changes. Despite a minor difference from a generic method, MMCBIE's general resilience in protecting against chosen-plain text differential attacks remains clear.

MMCIE's higher UACI score indicates its ability to withstand attacks directed primarily at changing pixel intensity, demonstrating its superiority over the 1D chaotic encryption technique. The outcome from NPCR underscores MMCBIE's complete encryption methodology, providing powerful security against differential attacks that may leverage differences in pixel intensity throughout the full image grid.

MMCIE's strong result in the MSE test, which nearly matches the 2D chaotic encryption technique, demonstrates its ability to reduce visual disparity. The varied nature of MSE scores emphasizes MMCBIE's versatility across many input conditions, validating its success in retaining image quality while offering a solid encryption framework. MMCIE's higher performance in the RMSE test, particularly when compared to the 1D chaotic encryption technique, demonstrates its use in giving a complete assessment of relative changes across images. MMCBIE's consistency in scoring across varied input conditions demonstrates its capacity to reduce visual discrepancies and maintain the integrity of encrypted images.

MMCIE's comparable PSNR results indicate its success in retaining image quality during encryption, agreeing with other methods in terms of reconstructed cipher images' resemblance to their originals. MMCBIE's efficacy is based on its capacity to maintain image accuracy, which is critical in encryption quality, even in the lack of a clear improvement in PSNR over the comparable methods. MMCIE's good result in the SSIM test highlights its ability to create appropriate deviance in visual elements while keeping the structural integrity of the original image. This is consistent with the broader theme of MMCBIE's effectiveness in preserving image characteristics, despite the fact that SSIM specifically focuses on structural similarities without taking color aspects into account. MMCIE's success in minimizing correlation coefficients reflects its strong encryption security, in contrast to the 1D chaotic encryption technique, which has a stronger

correlation. MMCBIE's emphasis on reducing correlation contributes to its overall strength in obscuring the relationship between the cipher image and the original input image, which aligns with the goal of a secure image encryption process.

MMCIE's superior performance in the Shannon entropy test demonstrates its ability to improve cipher image randomness, distinguishing it from both 1D and 2D chaotic encryption schemes. The result highlights MMCBIE's success in meeting the criteria for a secure encryption algorithm by introducing more uncertainty and randomness into the encrypted data. In the GLCM Matrix Entropy test, MMCIE outperformed the 1D chaotic encryption scheme and closely aligned with the 2D chaotic encryption algorithm, demonstrating its ability to introduce randomness into the grey-level co-occurrence matrix.

The results validate MMCBIE's ability to generate cipher images with enhanced random characteristics, ensuring the unpredictability of extracted features and reaffirming its position as a strong image encryption scheme. The scattered point distribution of MMCIE ensures uniformity in the distribution of pixels with varying intensities, resulting in superior performance in the Auto-Correlation Plot. This feature distinguishes MMCBIE from 1D and 2D chaotic encryption schemes by ensuring the security of visual information in the original image. The dispersed arrangement of MMCBIE's points emphasizes its ability to increase randomness while also securing the visual content in the encrypted image. MMCIE's ability to generate uniformly distributed RGB intensity histograms demonstrates its ability to effectively modify intensity values, ensuring a higher level of security. In contrast, the 1D chaotic encryption scheme lacks intensity modification, and the 2D scheme, while stronger than the 1D scheme, falls short of achieving the ideal uniformity required for higher strength. The ability of MMCBIE to meet these criteria demonstrates its strength in color component analysis, which contributes to its overall superiority in security analysis tests.

VII. CONCLUSION

We displayed a chaos-based encryption of image scheme that utilizes multiple 2-dimensional chaos systems in tandem, which can handle grey-scale and color images. This chaotic image encryption scheme introduces an approach wherein the chaos map generated from the first 2-dimensional chaotic system is used to apply confusion to the image, which is then followed by key-mixing in a cyclic manner, thereby shuffling the order of intensities of the subsequent pixels. Finally, the chaos map generated from the second 2-dimensional chaos system is applied to randomize the diffusion introduced in the key-mixing stage and to provide additional confusion. The scheme is compared with other image encryption schemes that use 1-dimensional and 2-dimensional chaos systems using various performance and security analyses. The results from these comparative tests show that MMCBIE displays significantly better performance and security to be a strong candidate for standardized IoT image encryption schemes. In conclusion, the highlighted strengths of MMCBIE position it as a robust solution for IoT image encryption, demonstrating superior performance and security in comparison to alternative schemes. Exploring MMCBIE's adaptability to evolving threats and its potential enhancements will be crucial for advancing the field of image encryption in the context of IoT security. The seamless similarity of the encrypted images to noise enhances their ability to be hidden, making MMCBIE a promising option for supporting IoT image encryption and promoting continual improvements in data protection procedures. Rigorous security analyses of MMCBIE's robustness confirm its viability and open avenues for further exploration and refinement in future research endeavors.

There are also several restrictions associated with MMCBIE. Its computational complexity is one significant drawback, which could be problematic in real-time applications using IoT devices with limited resources. Furthermore, the scheme's performance in specific scenarios may be affected by its sensitivity to initial conditions and parameters. Subsequent investigations ought to concentrate on refining MMCBIE's computing efficiency, investigating methods to reduce sensitivity to changes in parameters, and carrying out thorough assessments in a range of operational scenarios. To strengthen MMCBIE's security features, a comprehensive research into potential weaknesses and adversarial attacks is necessary. In order to ensure MMCBIE's efficacy in the ever-changing field of IoT security, researchers and industry stakeholders can work together to further develop and improve the technology.

REFERENCES

[1] K. Rarhi and S. Saha, "Image encryption in IoT devices using DNA and hyperchaotic neural network," in *Design Frameworks for Wireless Networks*, vol. 82. Singapore: Springer, 2020, pp. 347–375, doi: 10.1007/978-981-13-9574-1_15.

[2] S. Roy, U. Rawat, H. A. Sareen, and S. K. Nayak, "IECA: An efficient IoT friendly image encryption technique using programmable cellular automata," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 11, pp. 5083–5102, Nov. 2020.

[3] M. Usman, I. Ahmed, M. Imran, S. Khan, and U. Ali, "SIT: A lightweight encryption algorithm for secure Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 1, pp. 1–10, 2017.

[4] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, no. 4, pp. 403–419, Apr. 2019.

[5] Z. H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Phys. Lett. A*, vol. 346, nos. 1–3, pp. 153–157, 2005.

[6] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Process.*, vol. 132, no. 3, pp. 150–154, 2017.

[7] A. B. Dorothy, S. B. R. Kumar, and J. J. Sharmila, "IoT based home security through digital image processing algorithms," in *Proc. World Congr. Comput. Commun. Technol. (WCCCT)*, Tiruchirappalli, India, Feb. 2017, pp. 20–23.

[8] Y.-Z. Hsieh and Y.-L. Jeng, "Development of home intelligent fall detection IoT system based on feedback optical flow convolutional neural network," *IEEE Access*, vol. 6, pp. 6048–6057, 2018.

[9] L. Shen, Q. Zhang, G. Cao, and H. Xu, "Fall detection system based on deep learning and image processing in cloud environment," in *Proc. Complex, Intell., Softw. Intensive Syst.*, Matsue, Japan, 2018, pp. 590–598.

[10] A. Kapoor, S. I. Bhat, S. Shidnal, and A. Mehra, "Implementation of IoT (Internet of Things) and image processing in smart agriculture," in *Proc. Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solutions (CSITSS)*, Oct. 2016, pp. 21–26.

[11] D. A. Trujillo-Toledo, O. R. López-Bonilla, E. E. García-Guerrero, E. Tlelo-Cuautle, D. López-Mancilla, O. Guillén-Fernández, and E. Inzunza-González, "Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps," *Chaos, Solitons Fractals*, vol. 153, Dec. 2021, Art. no. 111506.

[12] Z. Gu, H. Li, S. Khan, L. Deng, X. Du, M. Guizani, and Z. Tian, "IEPSBP: A cost-efficient image encryption algorithm based on parallel chaotic system for green IoT," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 89–106, Mar. 2022.

[13] R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh, and B. Yoon, "CES blocks—A novel chaotic encryption schemes-based blockchain system for an IoT environment," *IEEE Access*, vol. 10, pp. 11354–11371, 2022.

[14] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, "An efficient image encryption technique based on two-level security for Internet of Things," *Multimedia Tools Appl.*, vol. 82, no. 4, pp. 5091–5111, Feb. 2023.

[15] P. Kumari and B. Mondal, "An encryption scheme based on grain stream cipher and chaos for privacy protection of image data on IoT network," *Wireless Pers. Commun.*, vol. 130, no. 3, pp. 2261–2280, Jun. 2023.

[16] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020.

[17] K. Shafique, B. A. Khawaja, M. D. Khurram, S. M. Sibtain, Y. Siddiqui, M. Mustaqim, H. T. Chattha, and X. Yang, "Energy harvesting using a low-cost rectenna for Internet of Things (IoT) applications," *IEEE Access*, vol. 6, pp. 30932–30941, 2018.

[18] Q. Awais, Y. Jin, H. T. Chattha, M. Jamil, H. Qiang, and B. A. Khawaja, "A compact rectenna system with high conversion efficiency for wireless energy harvesting," *IEEE Access*, vol. 6, pp. 35857–35866, 2018.

[19] "Cellular networks for massive IoT—Enabling low power wide area applications," Internet Things, Sweden, Tech. Rep., pp. 1–13, 2017. Accessed: Apr. 27, 2024. [Online]. Available: https://www.gsma.com/iot/resources/cellular-networks-for-massive-iot-enabling-low-power-wide-area-applications/

[20] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Internet-of-Things-based smart environments: State of the art, taxonomy, and open research challenges," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 10–16, Oct. 2016.

[21] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[22] N. Jeyanthi and R. Thandeeswaran, *Security Breaches and Threat Prevention in the Internet of Things*. Hershey, PA, USA: IGI Global, 2017.

[23] S. Kumari, "A research paper on cryptography encryption and compression techniques," *Int. J. Eng. Comput. Sci.*, vol. 6, no. 4, pp. 20915–20919, 2017.

[24] S. Heron, "Advanced encryption standard (AES)," *Netw. Secur.*, vol. 2009, no. 12, pp. 8–12, 2009.

[25] W. C. Barker, "Recommendation for the triple data encryption algorithm (TDEA) block cipher, Rev. 19 May 2008, Version 1.1. in NIST special publication," U.S. Dept. Commerce, Technol. Admin., Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2004.

[26] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA," in *Fast Software Encryption* (Lecture Notes in Computer Science), vol. 4593, A. Biryukov, Ed. Berlin, Germany: Springer, 2007, pp. 181–195, doi: 10.1007/978-3-540-74619-5_12.

[27] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in *Proc. Int. Workshop Cryptograph. Hardw. and Embedded Syst.* Vienna, Austria: Springer, 2007, pp. 450–466.

[28] R. Tripathi and S. Agrawal, "Comparative study of symmetric and asymmetric cryptography techniques," *Int. J. Advance Found. Res. Comput.*, vol. 1, no. 6, pp. 68–76, Jun. 2014.

[29] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *J. Ind. Inf. Integr.*, vol. 15, pp. 21–28, Sep. 2019.

[30] W. Viriyasitavat, L. D. Xu, Z. Bi, and D. Hoonsopon, "Blockchain technology for applications in Internet of Things—Mapping from system design perspective," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8155–8168, Oct. 2019.

[31] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre attacks: Exploiting speculative execution," *Commun. ACM*, vol. 63, no. 7, pp. 93–101, Jun. 2020, doi: 10.1145/3399742.

[32] A. Arena, P. Perazzo, and G. Dini, "Virtual private ledgers: Embedding private distributed ledgers over a public blockchain by cryptography," in *Proc. 23rd Int. Database Appl. Eng. Symp.*, New York, NY, USA, 2019, pp. 1–9, doi: 10.1145/3331076.3331083.

[33] M. Rasori, P. Perazzo, and G. Dini, "A lightweight and scalable attribute-based encryption system for smart cities," *Comput. Commun.*, vol. 149, pp. 78–89, Jan. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366419303913

[34] S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, "Optimizing chaos based image encryption," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 25569–25590, 2018.

[35] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated chaotic systems for image encryption," *Signal Process.*, vol. 147, pp. 133–145, Jun. 2018.

[36] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: A survey," in *Proc. 5th Int. Conf. Signal Image Process.*, Jan. 2014, pp. 102–107.

[37] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, Jun. 1998.

[38] M. F. M. Mursi, H. E. H. Ahmed, F. E. A. El-Samie, and A. H. A. El-Aziem, "Image encryption based on development of Hénon chaotic maps using fractional Fourier transform," *Int. J. Strategic Inf. Technol. Appl.*, vol. 5, no. 3, pp. 62–77, Jul. 2014.

[39] K. N. Singh, O. P. Singh, N. Baranwal, and A. K. Singh, "An efficient chaos-based image encryption algorithm using real-time object detection for smart city applications," *Sustain. Energy Technol. Assessments*, vol. 53, Oct. 2022, Art. no. 102566.

[40] C. M. Kumar, R. Vidhya, and M. Brindha, "An efficient chaos based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function," *Int. J. Speech Technol.*, vol. 52, no. 3, pp. 2556–2585, Feb. 2022.

[41] W. Alexan, Y.-L. Chen, L. Y. Por, and M. Gabr, "Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption," *Symmetry*, vol. 15, no. 5, p. 1081, May 2023.

[42] O. Georgiou and U. Raza, "Low power wide area network analysis: Can LoRa scale?" *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 162–165, Apr. 2017.

[43] K. L. Lueth, "IoT analytics research-state of IoT summer 2021," IoT Anal. GmbH, Ham-burg, Germany, Tech. Rep. 1, Mar. 2022. [Online]. Available: https://iot-analytics.com/product/state-of-iot-summer-2021

[44] Z. Hua, Y. Chen, H. Bao, and Y. Zhou, "Two-dimensional parametric polynomial chaotic system," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 7, pp. 4402–4414, Jul. 2022.

[45] Y. Zhang, Z. Hua, H. Bao, H. Huang, and Y. Zhou, "Generation of n-dimensional hyperchaotic maps using gershgorin-type theorem and its application," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 10, pp. 6516–6529, Oct. 2023, doi: 10.1109/TSMC.2023.3283433.

[46] Z. Hua, J. Li, Y. Chen, and S. Yi, "Design and application of an S-box using complete Latin square," *Nonlinear Dyn.*, vol. 104, no. 1, pp. 807–825, Mar. 2021.

[47] H. S. Shahhoseini, E. Saleh Kandzi, and M. Mollajafari, "Nonflat surface level pyramid: A high connectivity multidimensional interconnection network," *J. Supercomput.*, vol. 67, no. 1, pp. 31–46, Jan. 2014.

[48] S. M. Mohtavipour, M. Mollajafari, and A. Naseri, "A novel packet exchanging strategy for preventing HoL-blocking in fat-trees," *Cluster Comput.*, vol. 23, no. 2, pp. 461–482, Jun. 2020.

[49] I. Skorokhodov. (2023). *Landscapes Dataset (LHQ 1024×1024)*. Kaggle. [Online]. Available: https://www.kaggle.com/datasets/dimensi0n/lhq-1024

[50] A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal, and S. W. Kim, "Multimedia Internet of Things: A comprehensive survey," *IEEE Access*, vol. 8, pp. 8202–8250, 2020.

[51] H. Li, S. Yu, W. Feng, Y. Chen, J. Zhang, Z. Qin, Z. Zhu, and M. Wozniak, "Exploiting dynamic vector-level operations and a 2D-enhanced logistic modular map for efficient chaotic image encryption," *Entropy*, vol. 25, no. 8, p. 1147, Jul. 2023.

[52] H. Wen, Y. Huang, and Y. Lin, "High-quality color image compression-encryption using chaos and block permutation," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 8, Sep. 2023, Art. no. 101660.

[53] K. Qian, W. Feng, Z. Qin, J. Zhang, X. Luo, and Z. Zhu, "A novel image encryption scheme based on memristive chaotic system and combining bidirectional bit-level cyclic shift and dynamic DNA-level diffusion," *Frontiers Phys.*, vol. 10, Aug. 2022, Art. no. 963795.

[54] H. Wen and Y. Lin, "Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding," *Expert Syst. Appl.*, vol. 237, Mar. 2024, Art. no. 121514.

[55] H. Wen and Y. Lin, "Cryptanalyzing an image cipher using multiple chaos and DNA operations," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 7, Jul. 2023, Art. no. 101612.
[56] W. Feng, Z. Qin, J. Zhang, and M. Ahmad, "Cryptanalysis and improvement of the image encryption scheme based on feistel network and dynamic DNA encoding," *IEEE Access*, vol. 9, pp. 145459–145470, 2021.
[57] V. S. Nair, L. S. Mohith, and J. Kurunandan, "An improvement to 2DLSCM encryption scheme," in *Proc. 2nd Int. Conf. Augmented Intell. Sustain. Syst. (ICAISS)*, Aug. 2023, pp. 1204–1210.
[58] M. Rasori, M. L. Manna, P. Perazzo, and G. Dini, "A survey on attribute-based encryption schemes suitable for the Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8269–8290, Jun. 2022.
[59] J. Choi and N. Y. Yu, "Secure image encryption based on compressed sensing and scrambling for internet-of-multimedia things," *IEEE Access*, vol. 10, pp. 10706–10718, 2022.
[60] R. Hedayati and S. Mostafavi, "A lightweight image encryption algorithm for secure communications in multimedia Internet of Things," *Wireless Pers. Commun.*, vol. 123, pp. 1121–1143, Oct. 2022.

KURUNANDAN JAIN received the bachelor's degree in mathematics from the University of Leicester, in 2011, and the M.Sc. degree in applied mathematics and the Ph.D. degree in mathematical physics from Imperial College London, in 2017. He is currently an Assistant Professor with the Department of Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham, India. His research interests include cryptography, authentication and privacy design, cryptanalysis, digital signature, quantum cryptography and applications for Industry 4.0, 5G, 6G, and future networks.

BETRANT TITUS received the bachelor's degree in computer science from the Saintgits College of Engineering, Mahatma Gandhi University, Kottayam, in 2018, and the master's degree in cyber security from Amrita Vishwa Vidyapeetham, India, in 2020. He is a professional in the field of computer science and cybersecurity.

PRABHAKAR KRISHNAN (Senior Member, IEEE) was a Visiting Adjoint Professor with the Department of Computer Science, The University of Texas at San Antonio, USA. He is currently a Research Scientist with the Department of Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham, India. He is a member of the Core-Development Group, OpenAirInterface Software Alliance (OSA) 5G Wireless Community, Eurecom, Europe. He has over two decades of industry experience in the USA. His current research interests include cybersecurity, with a special focus on designing network security and architecture, network softwarization, SDN/NFV, cyber forensics, and the IoT standardization. He is a Senior Member of the IEEE Computer Society.

SUJITHA SUDEVAN received the bachelor's degree in computer engineering from Mumbai University, in 2018, and the master's degree in cyber security from Amrita Vishwa Vidyapeetham, India, in 2023. She is a professional in the field of cybersecurity. She has also contributed to the field through her research and has published a paper on a lightweight medical image encryption scheme based on chaotic maps and image scrambling. Her research interests include cryptography and forensics.

P. PRABU received the M.C.A. and Ph.D. degrees in computer application, specializing in software engineering, from Anna University, Chennai. He is currently an Assistant Professor with the Department of Computer Science, CHRIST (Deemed to be University), Bengaluru, Karnataka, India. With a combined experience of over 12 years in both teaching and industry, he has successfully supervised several research-oriented and application-driven projects, focusing on areas, such as ERP, mobile applications, and open-source software tools. Notably, he has an H-index of 15 and has authored more than 50 papers that have been published in renowned Scopus and SCI journals. His research interests include software engineering, security, web services, deep learning, the IoT, and mobile applications.

ALA SALEH ALLUHAIDAN received the B.Sc. degree in computer science from Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia, the M.Sc. degree in computer information systems from Grand Valley State University, Allendale, MI, USA, and the Ph.D. degree in information systems and technology from Claremont Graduate University, Claremont, CA, USA. She is currently an Assistant Professor with the Department of Information Systems, Princess Nourah Bint Abdulrahman University. Her research interests include health informatics, big data analytics, and machine learning.