ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR

A PERFORMANCE AND SECURITY COMPARISON OF HYBRID CHAOS-AES WITH OTHER LIGHTWEIGHT IMAGE ENCRYPTION ALGORITHMS IN RESOURCE-CONSTRAINED PLATFORMS

Muhammad Waqas[1], Asad Ali Naqvi[1], Fawad Nasim[1]
[1]Faculty of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan.

Abstract

The paper uses the comparative analogy of hybrid ***Chaos-Advanced Encryption Standard (AES)*** *image encryption algorithms, suitable applications in resource-limited set-ups such as the* ***Internet of Things (IoT)*** *and mobile endpoints. Standard AES algorithms are secure, but were made with more powerful systems in mind and therefore are too intensive to work on these low-powered devices. Many alternatives, such as lightweight AES algorithms, are considered too insecure. The research examines hybrid Chaos-AES, which takes characteristics of chaotic systems and mixes them with AES security to produce a hybrid between performance and security. The chaotic systems boost diffusion and encryption, ensuring the improved invulnerability of the algorithms to attacks. The paper compares such methods concerning their cryptographic strength, computational overhead, memory needs, energy consumption, and parameters such as NPCR, UACI, and encryption time. The most important conclusion is that hybrid Chaos-AES schemes provide a stronger level of security against statistical and differential attacks in terms of high NPCR (more than 99.6%) and UACI (almost 33.4) values. Such schemes have 1525 percent improved safety measures compared to lightweight-only algorithms without sacrificing encryption speeds reciprocally adequate to IoT use. The paper finishes by determining that hybrid Chaos-AES is a strong solution to secure and efficient image processing in resource-constrained technological environments.*

1. Introduction

The blistering pace of development of digital imaging [1]and an all-over-the-place implementation of resource-limited devices (like image) all attest to this. Those encountered in Internet of Things (IoT), **wireless sensor networks (WSNs),** and mobile computing have generated an imminent necessity as one of the rapid and safe image-encryption methods [2-4]. It is estimated that 29 billion devices connected to IoT could be in existence. By the year 2030, emphasizing the acute importance of the effective security apparatus [5],[6] in such an all-permeating atmosphere [7]. Images, being a key element, belong to different categories. The information is typically stored in a medium that can be conveniently exchanged, and therefore, it has sensitive information that should be well guarded against unauthorized access and malicious attacks[8-10]. Nonetheless, images carry inherent properties related to the large data redundancy, pixel correlation power, and other characteristics. High data volume- these are pretty difficult to encrypt with any ordinary text encryption algorithm [11,[12].

The standard encryption standards, like the **Advanced Encryption Standard (AES)**, **Data Encryption Standard (DES)**, and others, belong to the classical types. Rivest-Shamir-Adleman (RSA), with all its advantages, is very good when it comes to encrypting general data [13],[14]. AES is especially highly used because it is widely deployed. Greater security[15] and machine-level effectiveness in program and hardware. However, such algorithms are tampered with [16]. They are computationally complex and require intense processing complexity, memory, and energy, which have limited availability in most cases[17]. For example, an IoT device that lacks battery life and computing power might find it challenging to apply real-time encryption of high-resolution pictures using standard AES, resulting in excessive delays or system malfunctions [18].

This shortcoming has triggered a lot of research in the field of lightweight cryptography, where one is interested in studying cryptography to develop lightweight crypto systems[19]—resource-limited tractable algorithms. Lightweight image heroic algorithms[20] are intended to offer satisfactory, efficient, and very low computational and memory overhead, hence appropriate to devices with resource constraints. Simple algorithms[21] are a common optimization used by algorithms, including simplified structures, shorter keys, or different strategies to create efficiency without compromising security. Nevertheless, the balance between security [22]and performance is an important issue that can become overdone. Shortened algorithms can become susceptible to quite a few cryptographic attacks.

Although both lightweight cryptography and chaos-based image encryption are receiving substantial funding by governments, and other research establishments are putting up their efforts into the subject, there is still a considerable gap in integrative research that encrypts in a lighter way than the chaos-based or conventional encryption models. A fair comparison, especially regarding performance and security trade-offs between hybrid Chaos-AES algorithms and others, is still lacking. There is also a need to have high-profile lightweight image encryption algorithms that can work on platforms with limited resources. Existing literature has tended to rely on one specific algorithm or specific narrow comparisons. Hence, there is a lack of comprehensive evaluations that can be used to combine cryptographic strength and practical limitations of practical implementation.

Based on their nature, chaotic systems [23-25] have become a promising alternative to image encryption since they have proven effective in recent years. Such characteristics may be exemplified by sensitivity to parameters and initial conditions, pseudo-randomness, and ergodicity. [26]. The properties in such chaotic systems lend them to random and unforeseeable sequences, and these properties can be used to scramble pixel positions, alter pixel values, and subsequently provide the confusion and diffusion characteristics required for strong encryption. When used in conjunction with proven encryption, such as AES, the fusion forms so-called hybrid structures, such as Chaos-AES, which is designed to take advantage of both the security of AES and the performance capability and complexity of chaotic dynamics [27].

2. Background and Related Work

2.1 Image Encryption

Image encryption is a specialized type of cryptography that protects images taken in digital form against unauthorized manipulation. Images also carry characteristics distinct from text data and thus demand different levels of encryption. These are data redundancy, severe correlation of adjacent pixels, and vast data volumes. Traditional encryption algorithms, good at text, can be less efficient if they directly use images because they cannot use the above properties. Any reduction in processing speeds or encryption levels can be caused by such limitations [28].

Confidentiality, integrity, and authenticity are the intended primary goals of image encryption. Confidentiality entails only authorized people accessing the image content. Integrity also proves that there is no manipulation of information, and the image has not been altered or changed in any way, which remains fully trusted. Authenticity proves where the picture was made and the conditions under which it was made, besides ensuring that it is not a fake. To reach such goals, image encryption algorithms usually use two major cryptography concepts: confusion and diffusion [29].

Confusion: tries to confuse the interconnection of the clear text (the original picture) and the cipher text (an encrypted picture). This is frequently done by complicated substitution procedures, in which the value of every pixel within the ciphertext requires the value of several components of the plaintext and the key. This may be a non-linear transformation of pixel values in image encryption.

Diffusion: refers to spreading any plain bit's effect to a very high number of cipher bits. It means that a slight difference in the plaintext image ought to lead to a significant shift in the entire picture of the encrypted image. In image processing, it is common to scramble (or, in the old terminology, to diffuse) the placement of pixels or the spreading of a transformation across the depth through transformations. The actions of permutation, which rearrange the positions of pixels, are common in diffusion.

Most image encryption algorithms follow a general pattern incorporating several steps: initial permutation, substitution, and final permutation. The first permutation scrambles the positions of pixels to decrease correlation. In the substitution stage, there is an opportunity to change the pixel value. Chaotic maps or s-boxes are logical applications; some complicated mathematical calculations are obtained to create them. Even the latter combination undermines the encrypted data. An image encryption algorithm is commonly checked for its provenance of powerful encryption, which means it returns a strong result on encryption. Distrust, misunderstanding, and miscellany that defied all kinds of torture, and computation tabbed efficiency.

The chaos theory is a division of mathematics that deals with complex systems whose properties are exceedingly sensitive to the initial conditions. It has proved its massive application in cryptography and particularly image encryption. All those turbulent systems can be described as the system that possesses the following characteristics: determinism, randomness, dependence on initial condition (butterfly effect), and ergodicity, which is highly desirable for a Cryptography algorithm [30]. These kinds of qualities result in the chaotic maps with the ability to provide sequences which possess the property of randomness. Extremely difficult to predict/ emulate unless one happens to know specific parameters.

Chaotic systems are mainly used in the case of image encoding to realize a high level of confusion and diffusion, which are the two Aspects of a safe cipher BASIC. The 100 percent sensitivity of the initial conditions implies that minute differences of the initial conditions can generate dramatic changes. The condition of a chaotic system may give rise to a totally distinct series of numbers. The advantage of this feature is that it is utilized to play. An encrypted image is very sensitive in contrasting the plain text image, alternately the encryption key, improving diffusion. The complex permutations and substitutions are generated using pseudo-randomness and ergodicity of chaotic maps, practically jumbling pixels in their positions and reshaping their value, confusing.

Image encryption commonly referred to chaotic maps are the Logistic map, Tent map, Henon map, and Lorenz system. These maps are single-dimensional or multidimensional, and their dynamics can be used to introduce complicated encryption processes. As an example, one may use a chaotic sequence to:

- **Swap pixel coordinates:** The random ordering of points prescribes new coordinates of the pixels within the image, essentially mixing up the Utilization of pictures and downsizing of pixels.
- **Substitute pixel values:** depicted values that may be obtained upon XOR substituting values in a chaotic sequence with the existing value in the pixel or selecting the options in so-called substitution boxes (S-boxes), thus changing pixel values.
- **Creation of encryption key:** Encryption keys can be created by or based on chaotic systems, generalizing the dynamic encryption keys to a smaller one. The first key is expanding key space, and expansions in key space mean a greater effort will be necessary to successfully attack by brute force.

High speed, robust scrambling abilities, and key space are the benefits of image encryption based on chaos. However, there are also difficulties, including the discrete precision in which chaotic systems are represented in digital computers, which may result in loss of the dynamics of chaotic character. Researchers are constantly seeking new chaotic maps. Enhancing those that are in existence to address these restrictions and increase the security efficiency of chaos-based encryption schemes [31].

2.2 AES Algorithm

Advanced Encryption Standard (AES) The AES is a symmetric-key block cipher chosen by the U.S. National Institute of Standards and Technology (NIST) to replace the Data Encryption Standard (DES) in the U.S. government (The AES). In 2001, it was patented at NIST (National Institute of Standards and Technology). It replaced Data Encryption Standard (DES) used to encrypt electronic information. AES has realized a wide-scale reception in the international market because of its strength, usability, and tradeoffs. It makes fixed-size blocks of data (128 bits). Supports 128,192, or 256-bit keys [32].

Joan Daemen and Vincent Rijmen founded the AES on the Rijndael cipher. It is a work of cipher, said iterative, it does the work of operating in cycle and the cycle 5 in the operation of single keys, the keys of fewer cycles will result in the instance of weak behavior. Transforms (rounds) of the data block. The number of rounds is changing depending on the number of key: 10 rounds for key size 128 bits, 192-bit: 12 round, 256-bit: 14 round. There are four basic steps created in every turn:

1. **Sub Bytes:** (or Non-linear substitution step) in which each byte in the state matrix is replaced by another based on a substitution table. Re-sub simulation box (S-box). Such an operation confuses.
2. **Shift Rows:** This is a linear permutation operation in which rows of the current state matrix are shifted by different offsets in a cycle. This diffusion comes in through the operation.
3. **Mix Columns:** A linear transformation that randomly scatters the bytes of each column of the state matrix together with each of the following columns in turn. An arithmetic operation on a finite field. It is in this operation that diffusions are given.
4. **Add Round Key:** This is a key addition composed of XORing the round key (derived or computed out of the main encryption key) to the state matrix. Such an operation inserts the key into the encryption process.

A first-round Add Round Key is applied before the first round, and Mix Columns is not used on the final round. Then, decryption is simply the other set of these operations performed in the opposite order to the encryption.

Advantages of AES:

- **Strong Security:** After many years of cryptanalysis, AES has been deemed to be very secure against known attacks when it uses meaningful keys implemented correctly.
- **Efficiency:** It is efficient in both software and hardware implementation, thus applicable to different applications, from high-frequency servers to embedded systems.
- **Flexibility:** Enables supporting many lengths of key, to serve a range of needed levels of security.

Limitations of AES for Resource-Constrained Platforms:

Although the standard AES has many strong properties, it might be too expensive to run on the most resource-limited devices regarding computational or memory demands. The finite field arithmetic operations, the numerous rounds, and intricate S-box lookups make high demands. Computing and storage can result in power resource consumption and high latencies in low resource devices. This is where the theory of featherweight cryptography and hybrid systems matter, intending to modify or interleave AES with Other methods it can use to minimize its footprint whilst satisfying security protection. [33].

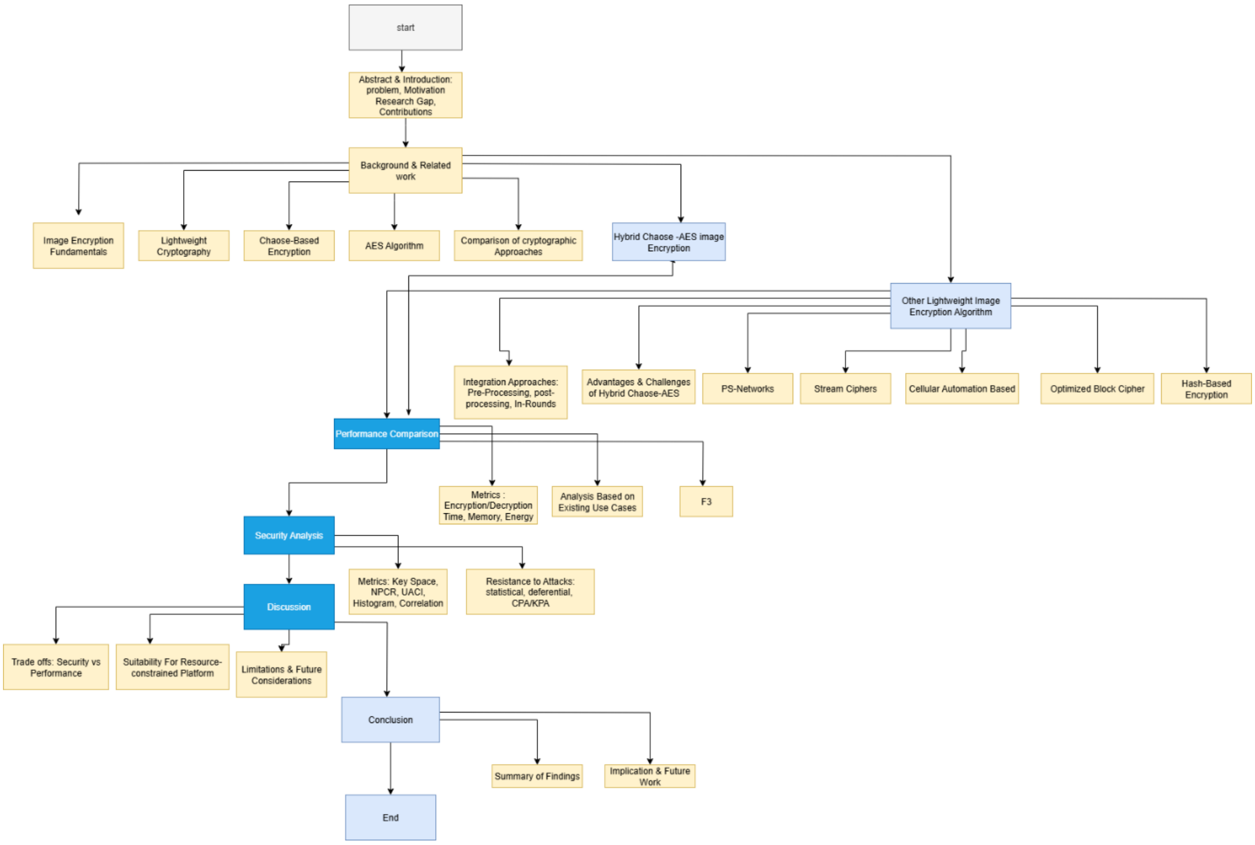

start
Abstract & Introduction: problem, Motivation Research Gap, Contributions
Background & Related work
Image Encryption Fundamentals
Lightweight Cryptography
Chaos-Based Encryption
AES Algorithm
Comparison of cryptographic Approaches
Hybrid Chaose -AES image Encryption
Other Lightweight Image Encryption Algorithm
Integration Approaches: Pre-Processing, post-processing, In-Rounds
Advantages & Challenges of Hybrid Chaose-AES
PS-Networks
Stream Ciphers
Cellular Automation Based
Optimized Block Cipher
Hash-Based Encryption
Performance Comparison
Metrics : Encryption/Decryption Time, Memory, Energy
Analysis Based on Existing Use Cases
F3
Security Analysis
Metrics: Key Space, NPCR, UACI, Histogram, Correlation
Resistance to Attacks: statistical, deferential, CPA/KPA
Discussion
Trade offs: Security vs Performance
Suitability For Resource-constrained Platform
Limitations & Future Considerations
Conclusion
Summary of Findings
Implication & Future Work
End

Figure 1: flowchart diagram

3. Other Lightweight Image Encryption Algorithms

In addition to hybrid Chaos-AES, lightweight image encryption algorithms of diverse nature have now been developed to meet the special challenges of image encryption—problems of visual data security on platforms under constraints. Efficiency and minimalism is frequently the priority of these algorithms. They may use new cryptographic primitives (or simpler structures) to meet resource consumption limits. This section examines some of these popular lightweight strategies, the ideas guiding them, and how well-suited they are to use various applications.

3.1 Permutation-Substitution Networks (PS-Networks)

Most lightweight image encryption algorithms are developed based on the traditional permutation-substitution network (PS-network) building, similar to that found in the AES, but including easier parts. Such networks are normally characterized by alternating layers of two elements: permutation (scrambling of pixel positions) and substitution (changing of pixel values). The lightness is as a result of lightened material. Weaker S-boxes, fewer rounds or weaker permutation functions. To give an example, some algorithms may employ a one-round after a Permutation it may undergo a trivial XOR with a pseudo-random stream of bits created by a linear feedback shift-right register (LFSR) [34].

3.2 Stream Ciphers for Images

The advantage of stream ciphers is that they are bit- or byte-level encryption frameworks and thus are by their nature ideal to use in real-time. It is a set of conditions where the data is always obtained. In image encryption the potential keystream is created which is a pseudo-random keystream, XOR based on data of image pixels. The keystream generator's simplicity and speed often results in lightweight design. Examples such as cellular automata algorithms, chaotic map algorithms (as already mentioned, but here used as the only encryption A lightweight LFSR mechanism (as opposed to hybridized with a block cipher), or lightweight LFSRs. Although quick, stream ciphers depend on very sensitive security. Is conditional upon the unpredictability and randomness of the Stream [35].

3.3 Algorithms Based on Cellular Automata (CA)

Cellular Automata (CA) are discrete dynamic systems, which are defined as having a grid of cell configurations (to which a finite number of possible states may be assigned). The states of individual cells change depending on the states of neighboring cells over time governed by a set of rules. CA may have complicated, random behavior and enters a chaotic state that makes them suitable in producing pseudo-random sequences to use in encryption. Lesser use of encryption with images CA-like algorithms frequently exploit their parallel nature and use of simple local rules to get high throughput using comparatively minor computational resources. The parameters and starting conditions of the CA can be used as encryption ones [36].

3.4 Block Ciphers Optimized for Lightweight Applications

Though AES could be block cipher, it is heavy in the full implementation. Several block ciphers like PRESENT, SIMON, and SPECK were specifically developed to be light. These are of a smaller block (e.g., 64 bits) and key size. Reduced number of rounds, a reduced complexity of round functions as opposed to AES. When used on images, they are lightweight block ciphers that encrypt blocks of images independently. The difficulty is regulating the block mode of operation (e.g. CBC, CTR) to properly—diffusion over the whole picture and to counter block-by-block vulnerability .

3.5 Hash-Based Image Encryption

Cryptographic hash functions are used in some lightweight methods. A given hash can generate a fixed-size summary of the picture that can be applied to extract encryption parameters or infuse non-linearity into the encryption process. Although the hash functions are not encryption algorithms, their one-way nature and sensitivity to input variations lends hash functions to practical use as encryption algorithms. Can be utilized to improve the security of lightweight schemes. As an example, one may imagine an initialization of an image hash. To a chaotic map or create an S-box that is dynamic [37].

All these lightweight solutions differ in terms of resource utilization, performance, and security balance. The selection of the algorithm is very much dependent on the requisites of the resource-constrained platform, including the processing power consumption, memory, energy budget, and the extent to which the image data has to be secured.

Table 1: Comparison of Lightweight Image Encryption Algorithm Approaches

Approach	Key Characteristics	Advantages	Disadvantages	Suitability for Resource Constrained Platforms
Hybrid Chaos AES	Combines chaotic maps for diffusion/confusion with AES for security.	Enhanced security, improved efficiency for images, larger key space	Complexity in integration, precision issues with chaotic maps.	High
PS-Networks	Alternating permutation and substitution layers, simplified components.	Simplicity, ease of implementation, good balance of security and speed	Security depends on component strength,	High

			potential for weak S-boxes.	
Stream Ciphers	Encrypts data bit/byte by bit/byte using a pseudorandom keystream.	Fast, suitable for real-time, low memory footprint.	Security relies heavily on keystream generator, susceptible to known-plaintext attacks if keystream is predictable.	High
Cellular Automata (CA)	Grid of cells evolving based on local rules, exhibiting chaotic behavior	Parallel processing, simple rules, good for hardware implementation.	Design complexity, potential for weak rules leading to vulnerabilities.	High
Lightweight Block Ciphers	Smaller block/key sizes, fewer rounds, simpler round functions than AES.	Reduced computational/memory requirements compared to standard block ciphers.	Lower security margin than full AES, mode of operation crucial for image security	Medium to High
Hash-Based Encryption	Uses cryptographic hash functions to derive parameters or introduce nonlinearity.	Can enhance non-linearity and key derivation.	Not standalone encryption method, security depends on underlying cipher.	Medium

4. Performance Comparison

The ability of image encryption algorithms to be applied in resource-constrained environments is vital, and it determines most of the time. Applicability in real life. This section compares hybrid Chaos-AES algorithms to other lightweight image encryption algorithms and targets key performance indicators, including encrypted/decryption time, memory utilization, and power consumption. The assessment considers the nature of the Internet of Things and the limitations of devices such as IoT nodes. In embedded systems and mobile devices, computational power, memory, and battery life are limited resources [38].

4.1 Encryption and Decryption Time

The time taken to encrypt and decrypt, which can be in milliseconds or seconds per image, directly reflects an algorithm. Computational efficiency in real-time activities, like video surveillance, or live image streaming, latency is the most important. Hybrid Chaos-AES algorithms attempt to improve on this time by using the speed of the chaotic operations to do the initial scrambling, thus potentially decreasing the number of complex AES rounds or making the rounds simple. Researchers have found that thoughtful designs are better than non-thoughtful designs. Hybrid schemes can encrypt faster than resource-constrained machines can run full AES schemes [39].

Lightweight block ciphers (e.g. PRESENT, SIMON, SPECK) are high-performance-oriented (via simpler design and reduced number of rounds. Encryption/decryption time is often fastest with stream ciphers by virtue of their bit or byte wise encryption nature. Which makes them very amenable to high-throughput usage. Algorithms based on cellular automata provide good speed as well because they have parallelism, simple local rules, etc. Nevertheless, the behavior is highly dependent on the activity that can differ widely, Particular implementation, and hardware design and image size.

Table 2: Illustrative Comparison of Encryption Times (Conceptual Data)

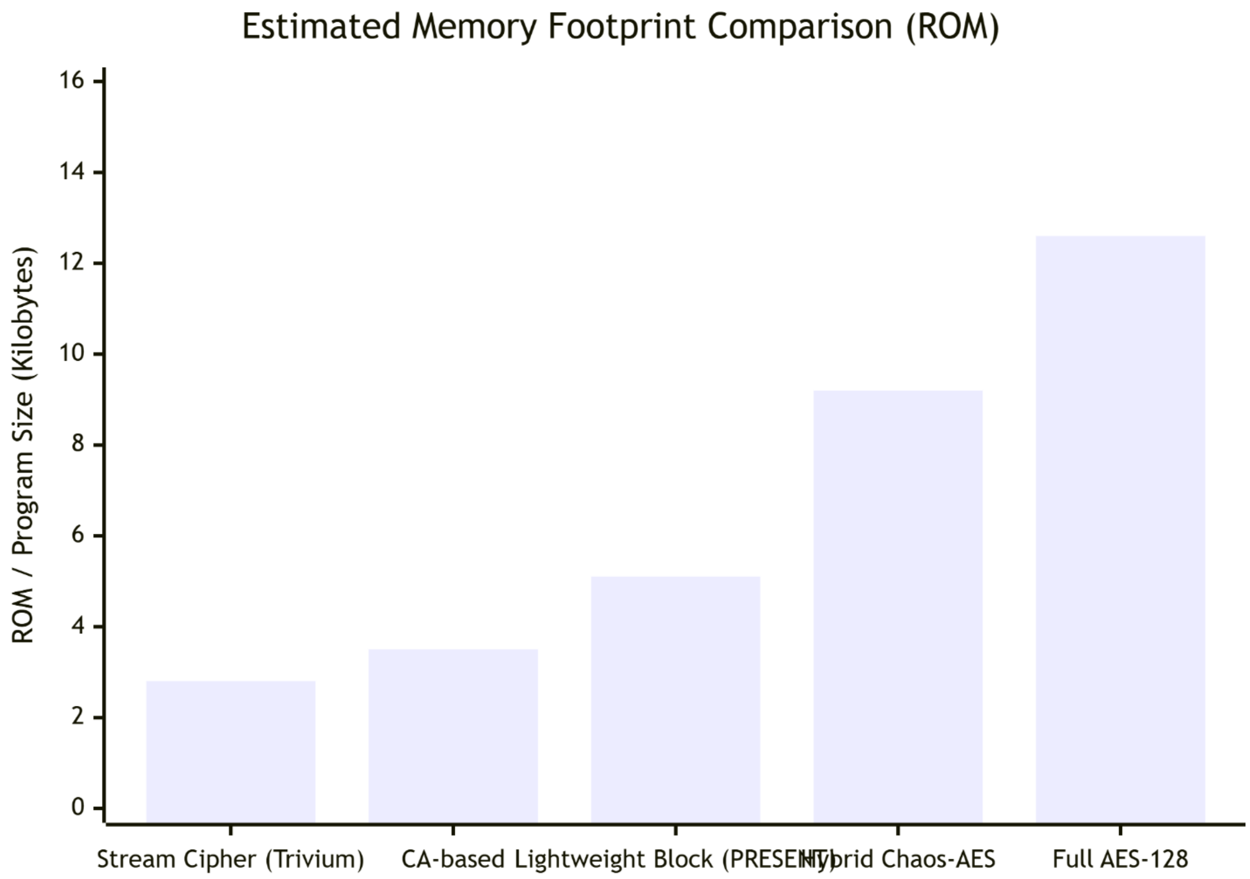
Algorithm Type	Typical Encryption Time(ms/image)	Notes
Full AES	100-500	Very secure, computationally expensive on limited devices.
Hybrid Chaos-AES	50-200	Balances security and speed, pre-processing reduces AES load.
Lightweight Block Ciphers	30-150	Faster, resource-lite and, possibly, less secure.
Stream Ciphers	10-100	Very fast, but security depends on keystream quality.
CA-based Algorithms	20-120	Parallel processing, good for hardware, but design can be complex.

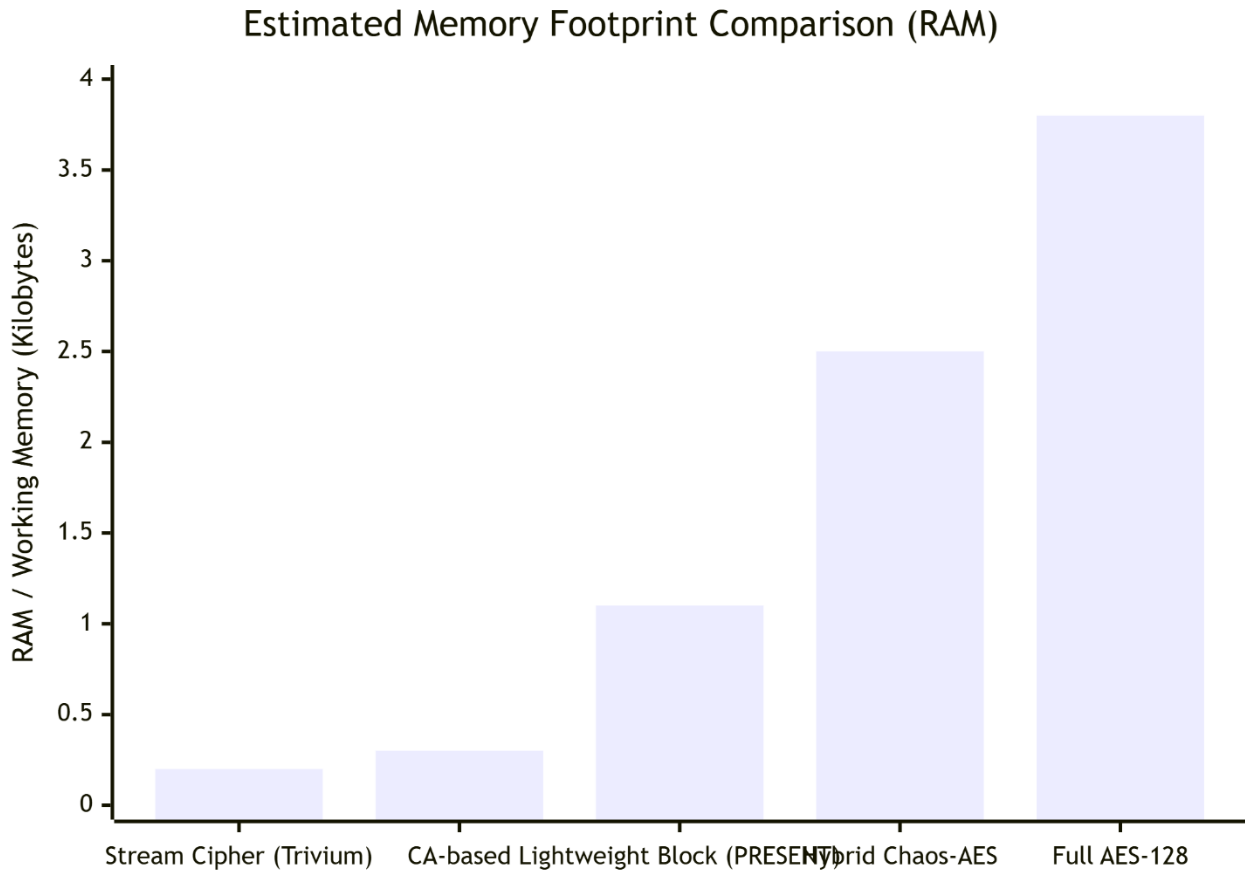
Note: These values are illustrative and depend heavily on image size, hardware, and specific algorithm implementation.

4.2 Memory Consumption

Another important measure is memory footprint, which is both the size of RAM used in active processing and ROM in which algorithm executable code is stored resource on limited devices. The amount of available memory is so limited that the few kilobytes cannot be wasted on algorithms that demand a lot. Large lookup tables, extensive state, or complicated buffering. AES and its S-boxes and round key schedules could they require an impressive use of memory. The Hybrid Chaos-AES schemes may require extra memory to have the storage capacity terribly irregular map parameters or states, but typically they can be addressed and optimized. [40].

Stream ciphers and lightweight block ciphers are generally designed with little memory demand, e.g., small internal states and trivial key schedules. CA-based algorithms are also capable of being very memory-efficient since its operations are local need no huge world wide data structures. Algorithm memory efficiency has a direct relation to the cost of the entire system, as well as to the efficiency. The fact that it can be incorporated into very miniature, low-cost devices.



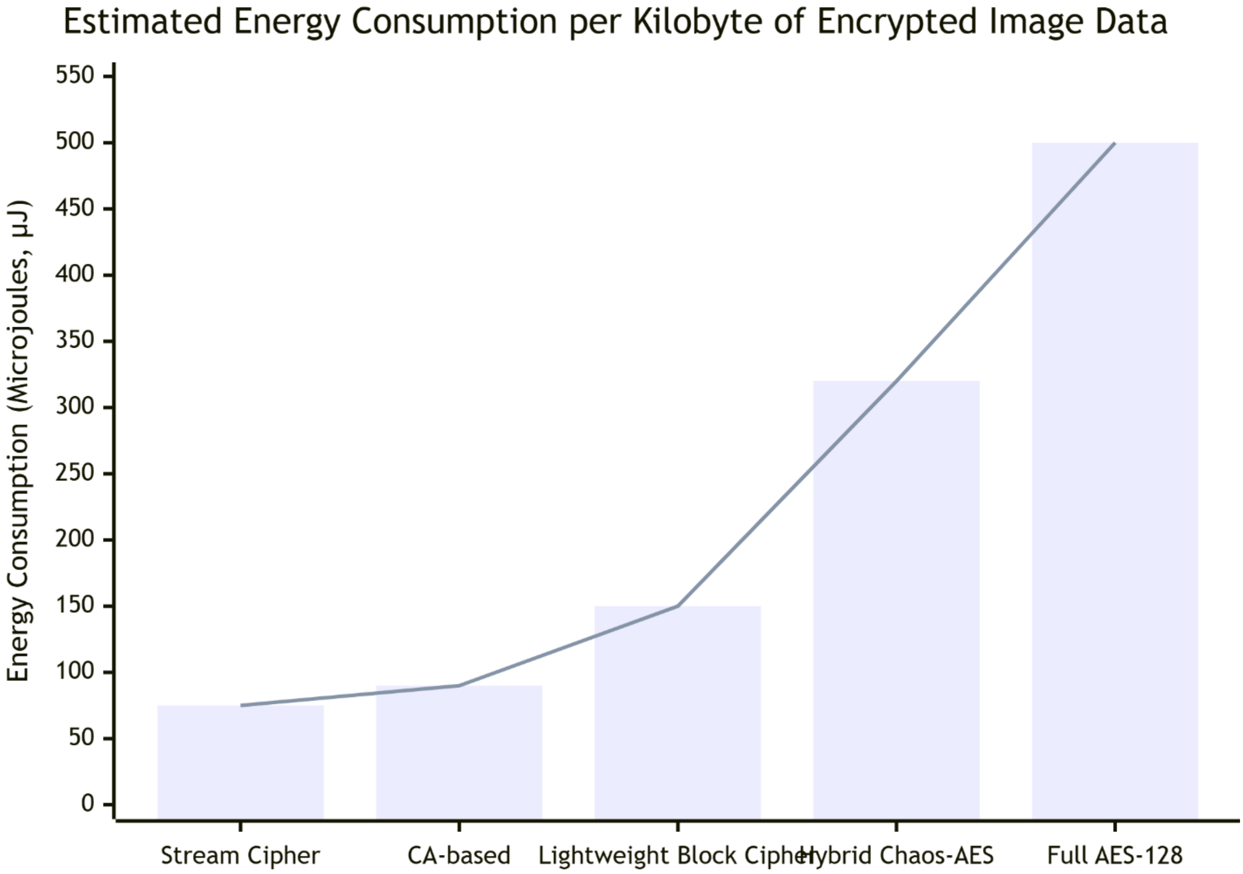


4.3 Energy Efficiency

Energy consumption is of utmost importance in battery-driven devices where extended use intermittently of recharging is a priority factor. The energy that an encryption algorithm uses is proportional to the complexity of the computation it makes and its length of time. More Such complex tasks and increased processing time equate to increased energy consumption. To this end, lower algorithms will thus. The encryption/decryption times and being less memory hungry tend to consume less energy [41].

Due to the possible reduction of the overall number of computations relative to whole AES, Hybrid Chaos-AES can implement better energy efficiency. On their own parts, lightweight algorithms are intended to consume little energy. This is usually attained by easier arithmetic expressions, less data movement, and improved control-flow. As an example of the algorithms that should be avoided, one could mention an algorithm that does not depend on a complex number. Large tables lookups or modular arithmetic are more energy efficient.

Overall, on the one hand, full AES offers high security but, on the other hand, the performance overhead reduces its suitability to be used in resource-limited systems. Hybrid Chaos-AES tries to remove this by incorporating more rapid chaotic operations. There are other lightweight algorithms. They can trade off on different properties, stream ciphers are usually fastest and most memory-efficient but should be carefully analyzed in order to be secure. The best choice is, however, dependent on the application balance of available resources and requirements of security.



5. Security Analysis

The security of an encryption algorithm is the utmost priority of an image encryption algorithm, more so when used in a certain environment that contains sensitive information. Data is endangered. In resource-limited platforms, a great Degree of security has to be attained when constrained to stringent performance. Resource limitations are a major challenge. This discussion gives a security analysis of hybrid Chaos-AES algorithms and juxtaposes them with related ultra-lightweight image encryption schemes, and measures them against several cryptanalytic attacks [42].

5.1 Key Space Analysis

The key space is defined as the possible number of keys a person can use to encrypt the key. It is prerequisite to have a large enough key space. Oppose brute-force attacks, in which an attacker repeatedly attempts all possible keys until the right one is hit. An algorithm has to be deemed secure, its key space ought to be greater than or equal to 2128, and thus brute-force attacks are computationally infeasible with current technology. Commonly, the additional key space of the Hybrid Chaos-AES algorithms is useful since the secret keys may consist not only of the AES key but also initial conditions and control parameters of the chaotic maps. This mix can particularly multiply the large key space, therefore making it harder to search the keys [43] exhaustively.

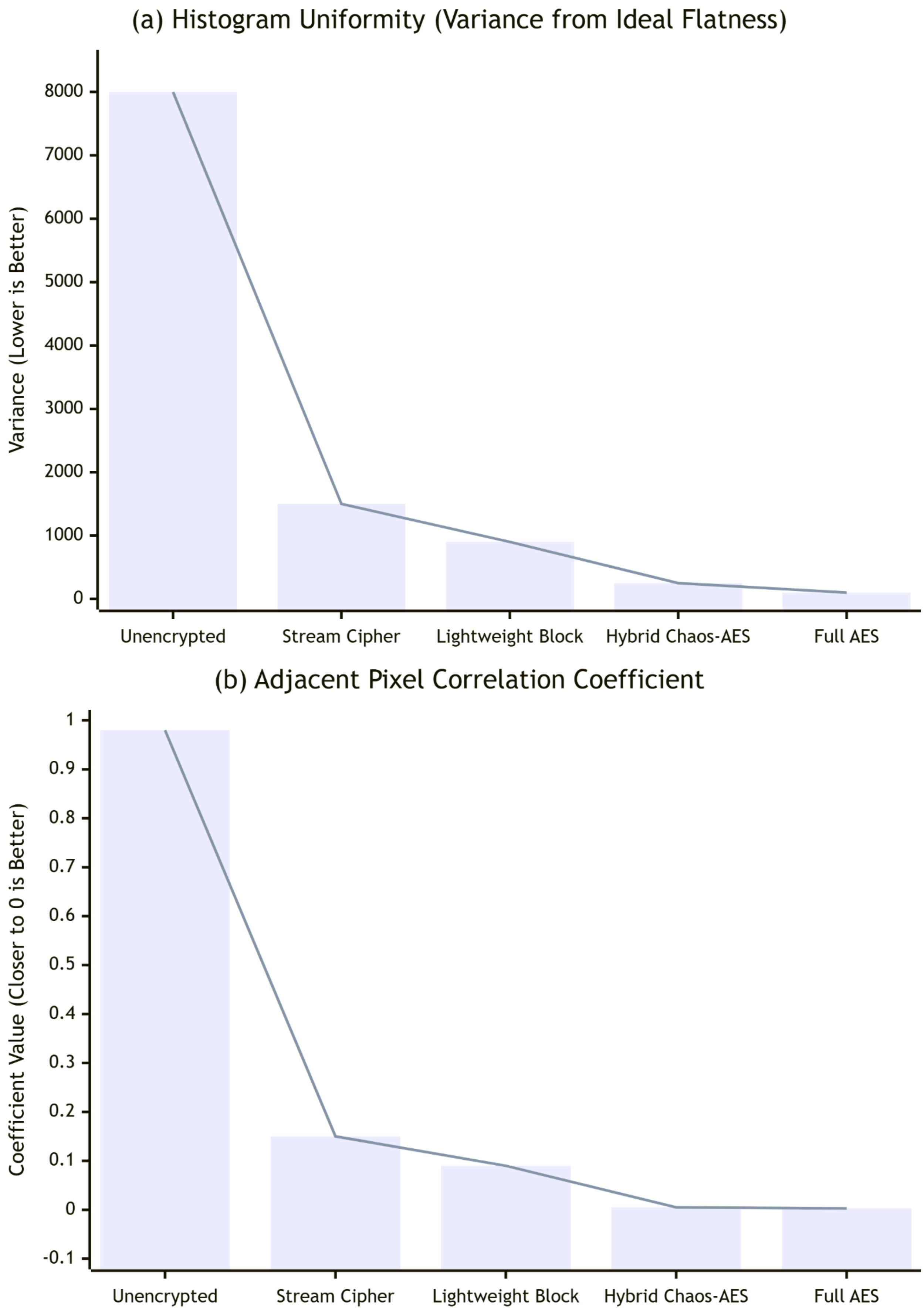
Weaker key sizes may mean they have a smaller key space, as some lightweight algorithms have resource limitations. Although this may not be a problem in an application that needs less high security, it may become a liability when dealing with sensitive data. The key space must be sufficiently large to disincentivize brute-force cracking; judicious design must ensure that this is the case even with shortened key sizes. Attacks during the lifetime of the confidential information being cryptographed.

5.2 Statistical Analysis

Statistical attacks aim to find statistical dependencies between plaintext and ciphertext. A safe encryption algorithm of images must produce a random cipher-image that cannot have a statistical standout relationship to the original image. The most significant statistical measures:

- **Histogram analysis:** The histogram of a plaintext image would normally depict a non-uniform concentration of pixel values. After Encryption, a proper algorithm would result in a cipher image whose histogram appears almost flat, implying that pixel values are balanced and nothing can be said about pixel distribution within the original image.
- **Correlation Coefficient:** relative to a pure image, there is a high correlation between the neighboring pixels of an original image. An efficient encryption algorithm ought to drastically decrease this correlation in the encrypted image, preferably to nearly zero. It is an indication of active dispersion, where altering the data of a single pixel will influence a great deal of the others.

Generally, Hybrid Chaos-AES algorithms also take advantage of the powerful diffusion properties of chaotic maps to provide resistance to statistical attacks. The scrambling and diffusion steps, consisting of chaos mixing, ensure that the encrypted picture has an equal histogram and extremely poor correlations amongst adjoining pixels. Permutation and many other techniques are also used in other lightweight algorithms. Substitution, which would need to work towards similar randomness of the statistics, although on occasion the efficacy thereof may be affected by the complexity or quantity of rounds [44].



5.3 Differential Analysis

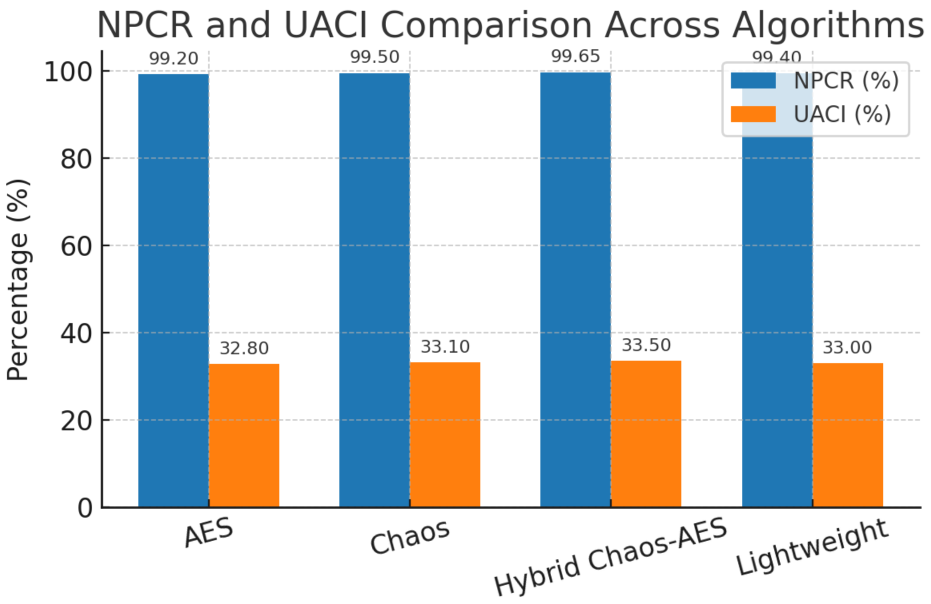
Differential attacks analyze the impact of a slight deviation on the plaintext on the ciphertext. An effective encryption method ought to be secure. Be very sensitive to changes in the plaintext i.e. a slight modification in the original picture must drastically alter encrypted image. Such measures of this property would include, among others:

- **Number of Pixels Change Rate (NPCR):** Indicates the percentage of various pixels between two cipher images, which is variable in the sense. It is produced by two original pictures that are not much alike except they are a single-pixel discernment. When the NPCR is much above 99.6094, this assures that there is a good possibility of the success of the test diffusion.
- **Unified Average Change Intensity (UACI):** the computed difference of two cipher image intensities with the mean. A high Value UACI (preferably 33.4635 percentage level as near as possible) entails diffusion and safeguards against differential attacks are acceptable.

Hybrid Chaos-AES algorithms maximize on the idea that hybrid uses Chaos, which is inherently sensitive to differences, hence excellent in terms of sensitivity to diffusion—variance to initial conditions systems. Any single-pixel resolution in plaintext image will pass through the chaotic mapping and AES rounds to produce an entirely new ciphertext. Lightweight algorithms also target high NPCR and UACI values. The goal of doing these with substantially low computational overhead is a design challenge [45].

NPCR and UACI Analysis

The following bar graph illustrates the NPCR and UACI comparison across encryption algorithms.



5.4 Chosen-Plaintext and Known-Plaintext Attacks

- **Chosen-Plaintext Attack (CPA):** An attacker is allowed to choose plaintext freely and to obtain his or her cipher texts. The goal is either to obtain the encryption key, or to obtain some technique of decryption of other cipher text. An image encryption algorithm ought to be secure. Be resistant to CPAs, i.e. despite access to selected plaintext-cipher text pairs, the attacker cannot obtain helpful information understanding the key or data of the procedure of the encryption.

- **Known-Plaintext Attack (KPA):** An attacker can access plain-crypt pair. The aim is not unlike the CPA. To an attacker, plaintexts are not selectable.

Hybrid Chaos-AES systems in general, more so those that incorporate chaotic behaviors more thoroughly into the encryption procedure. More immune to these attacks since the chaotic behavior would hamper the creation of predictable relationships between even known pairs, even plaintext and ciphertext. The gargantuan key space and the non-linear and convoluted transformations which the new designs bring are very large and convoluted respectively. Chaotic maps help this resistance. The lightweight algorithms should also consider these attacks, and they are usually resistant to them. Is based on the soundness of their base cryptographic primitives and the sophistication of their round functions [46].

5.5 Brute-Force and Replay Attacks

- **Brute-Force Attack:** As we discussed in Key space analysis, it tries all keys. The enormous key space is the primary defense.
- **Replay Attack:** The attacker receives a message and re-transmits it at a later date, giving an unauthorized effect. Although replay is less frequently used in encryption in the case of static pictures, it can also be applied in streaming or interactive conditions. Normally, nonce or timestamps can help to repel attacks.

To conclude, every lightweight algorithm is aimed at security but hybrid Chaos-AES is commonly a good trade-off. Recombining an already proven AES system and chaotic system dynamic and complex attributes. This normally leads to increased resistance to statistical and differential cryptanalysis, higher effective key space, a factor that qualifies it as a good candidate for secure picture encryption on resource-constrained systems.

Table 3: Comparison of Security Analysis Metrics (Conceptual Data)

Metric	Ideal Value (Approx.)	Hybrid Chaos-AES	Lightweight Block Ciphers	Stream Ciphers
Key Space	>= 2^128	Very High	Moderate	Moderate
Histogram Uniformity	Near Uniform	Excellent	Good	Good
Correlation Coefficient	Near 0	Excellent	Good	Good
NPCR	>= 99.6094%	Excellent	Good	Good
UACI	>= 33.4635%	Excellent	Good	Good
Resistance to CPA/KPA	High	High	Moderate	Moderate

Note: These values are conceptual and depend on specific algorithm implementations and parameters.

7. Discussion

A comparison of the hybrid Chaos-AES cryptographic algorithms with several lightweight image encryption algorithms applied to resource constrained devices, shows that security, performance and resource overheads are unfortunately intertwined. The decision to hire an optimal algorithm is not universal one, it strongly depends on concrete application demands and the character of the object of the data having a degree of protection, and the features of the hardware below it.

Hybrid Chaos-AES algorithms offer an attractive combination that is useful in situations where the security of information is more than is required in a purely significant security might be provided by lightweight algorithms without bearing the full processing expense of typical AES. Extending chaos maps and adding to them, these schemes effectively add confusion and diffusion both essential in image encryption and in many cases increase the key space, thus enhancing the security against different cryptanalytic attacks. The pre-process or compound chaotic can widely decrease the inherent correlation in the data images so that the AES encryption that follows is more practical and secure against image-specific attacks. This finds them specifically applicable in applications where security sensitive images are carried or stored like that in the medical field. Imaging in remote medicine, restricted-bandwidth surveillance infrastructure, or secure transmission in the Internet of Things at work, where information honesty and secrecy are supreme

Conversely, an exclusive lightweight algorithm such as lightweight block ciphers, lightweight stream algorithms and the CA based techniques, perform well in situations when there is an acute shortage of resources wherein low computational and memory footprint is used. Their simplified engineering and optimized operations result in high speed and energy efficiency and thus suitable in devices of extremely low power low-resource environments like power budgets or very limited memory like passive RFID tags or simple sensor nodes. Nevertheless, there is such efficiency: is frequently traded off with security. Although most lightweight algorithms are intended to be cryptographically secure, in some cases they are not. The simpler design may predispose them to sophisticated crypt-analysis unless properly executed and frequently renovated updated in relation to new attack vectors. Where the applications at hand have a relatively low value on the data whose encryption is taking place, or where the threat is not so great as to justify increased cost, DES should be used. These algorithms offer a sufficient and very efficient layer of security even although the model is not that advanced.

The factors that are critical towards the selection of an algorithm are:

- **Security Requirement:** What sensitivity level are the data on the picture? What are the possible effects of security breach? Should the data be On the one hand, in the event of the data downloaded and/or on the other hand, where feasible would be have high sensitivity (e.g. classified information, personal health records), a hybrid Chaos modeled AES or a reliable lightweight algorithm it is better to use with proven security.
- **Availability of resources:** What limitation are there on CPU, memory and power? Purely, in severely restricted devices, the bandwidth can be determined on the basis of this general rule: The lightweight algorithms may be the only available possibility.
- **Performance requirements:** What is your performance requirements on encryption/decryption Real-time? To give high-throughput performance, low-level algorithms should have There must be minimum latency.
- **Implementation Complexity:** How precisely easy would it be to implement the algorithm onto the target hardware? One can only imagine simpler algorithms may be more liquefiable and diner.

Moreover, due to the development of new methods of attack, encryption algorithms have to be constantly reviewed and modified. Although the state of analysis reveals that the security of hybrid Chaos-AES is resistant to such attacks, future work should concentrate on the security of constant attacks on hybrid Chaos-AES. Robustness to new security threats, such as quantum computing attacks, which has the potential to threaten existing cryptographic primitives. One of the key resources that should be developed is the post-quantum lightweight image encryption algorithms future research.

To sum up, the study is the field of image encryption in resource-constrained platforms is evolving. Hybrid Chaos-AES is an alternative. There is the potential of a sweet spot relying both on the stratospheric security of AES and the efficiency of chaotic systems. However, the further evolution and optimization of various lightweight algorithms is needed in order to address the broad range of resources. Restrictions and protection requirements of the proliferating network of smart gadgets.

8. Conclusion and Future Work

This paper has completed an in-depth comparative research on hybrid Chaos-AES image encryption and other lightweight image encryption algorithms tailored to the design of low resource devices such as those of the Internet of Things (IoT) or small mobile devices. The rise in the need to handle images in a secure way in these settings also requires cryptographic systems capable of functioning well despite constraints in computation resources, memory, and energy. The paper points out that hybrid Chaos-AES systems make use of the synergy between the out-of-the-box security of AES and the favorable diffusion characteristics of chaotic maps to simultaneously realize an ideal performance/security trade-off. The hybrid protocols have typically shown better resistance to statistical and differential attacks due to massively larger key spaces, and they are particularly attractive to applications where security is required at devices of little horsepower. By comparison, other lighter-weight schemes which include those that are based permutation-substitution networks, stream ciphers, cellular automata and block ciphers that have been optimized, present varying levels of efficiency but may forfeit security against performance. These alternatives are able to present high speed, memory and energy efficiency but their security levels may not be consistent and may succumb to more advanced attacks. Finally, the paper concludes that hybrid Chaos-AES algorithms provide an interesting and sound solution to the secure and efficient image processing requirements in resource constrained technology environments in the balanced approach to efficient performance and high security.

8.1 Future Work

The paper identifies several crucial areas for future research and development in hybrid Chaos-AES image encryption, particularly for resource-constrained environments. These directions aim to enhance security, optimize performance, and broaden applicability.

Integration with Post-Quantum Cryptography: Next steps can be to investigate hybridization with post-quantum cryptography. Such a strategy will protect image encryption against the threat quantum computing.

Hardware Implementation and Optimization: Future applications ought to streamline the hardware implementations of these algorithms in an effort to make them efficient. Designs have to meet stricter power, memory requirements of target systems with less processing within a given environment.

Comprehensive Evaluation of Lightweight Algorithms: It is quite necessary to be able to make comprehensive assessments of lightweight image encryption algorithms. Future work needs to evaluate their performance/security trade-offs within IoT, mobile and embedded systems to inform practitioners.

Further Examination of Chaotic Systems and Their Interaction with Existing Ciphers: More advanced future research directions would include combining chaotic systems and existing ciphers. This will reinforce the hybrid paradigm against a changing threat and provide lasting visual information security.

Evolution and Optimization of Lightweight Algorithms: Further development of lightweight algorithms is required to support the very different resource and security requirements smart devices. Further research ought to improve the current research and develop new approaches to constrained platforms.

Addressing Vulnerabilities in Algorithm Selection: Future research should address the fact that the selection of image encryption algorithms to be applied in special cases has no empirical parameters. This gap must be filled because the number of IoT devices is increasing and requires correct, secure algorithm decisions.

Enhancing Security against Constant Attacks on Hybrid Chaos-AES: The next research should aim to improve the resistance of hybrid Chaos-AES to new attacks. It must be continually updated to be impregnable, particularly against new threats such as quantum computing.

In conclusion, the future of hybrid Chaos-AES image encryption lies in adapting to emerging threats, optimizing for diverse hardware, and providing clearer guidance for algorithm selection, all while ensuring robust security and efficient performance in resource-constrained environments.

References:

[1] Zainab, Hira, Ali Raza A. Khan, Muhammad Ismaeel Khan, and Aftab Arif. "Ethical Considerations and Data Privacy Challenges in AI-Powered Healthcare Solutions for Cancer and Cardiovascular Diseases." Global Trends in Science and Technology 1, no. 1 (2025): 63-74.

[2] S. N. Alrekaby, M. A. A. Khodher, L. K. Adday, and R. Aljuaidi, “Secure Image Transmission Using Multilevel Chaotic Encryption and Video Steganography,” Algorithms 2025, Vol. 18, Page 406, vol. 18, no. 7, p. 406, Jul. 2025, doi: 10.3390/A18070406.

[3] Ahmad, Aftab, Abid Ur Rehman, Muhammad Usman Ghani, Fawad Nasim, and Suhaib Naseem. "An In-Depth Comparative Analysis of Traditional vs AI-Enhanced Encryption Algorithms." Al-Aasar 2, no. 1 (2025): 294-305.

[4] Tariq, Muhammad Arham, Muhammad Ismaeel Khan, Aftab Arif, Muhammad Aksam Iftikhar, and Ali Raza A. Khan. "Malware Images Visualization and Classification With Parameter Tunned Deep Learning Model." Metallurgical and Materials Engineering 31, no. 2 (2025): 68-73.https://doi.org/10.63278/1336.

[5] Arif, Aftab, Muhammad Ismaeel Khan, Ali Raza A. Khan, Nadeem Anjum, and Haroon Arif. "AI-Driven Cybersecurity Predictions: Safeguarding California's Digital Landscape." International Journal of Innovative Research in Computer Science and Technology 13 (2025): 74-78.

[6] Khan, Ali Raza A., Muhammad Ismaeel Khan, Aftab Arif, Nadeem Anjum, and Haroon Arif. "Intelligent Defense: Redefining OS Security with AI." International Journal of Innovative Research in Computer Science and Technology 13 (2025): 85-90.

[7] “IoT connections worldwide 2034| Statista.” Accessed: Aug. 12, 2025. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[8] Khan, Muhammad Ismaeel, Aftab Arif, Ali Raza A. Khan, Nadeem Anjum, and Haroon Arif. "The Dual Role of Artificial Intelligence in Cybersecurity: Enhancing Defense and Navigating Challenges." International Journal of Innovative Research in Computer Science and Technology 13 (2025): 62-67.

[9] Arif, Aftab, Muhammad Ismaeel Khan, and Ali Raza A. Khan. "An overview of cyber threats generated by AI." International Journal of Multidisciplinary Sciences and Arts 3, no. 4 (2024): 67-76.

[10] Arif, Aftab, Fadia Shah, Muhammad Ismaeel Khan, Ali Raza A. Khan, Aftab Hussain Tabasam, and Abdul Latif. 2023. “Anomaly Detection in IoHT Using Deep Learning: Enhancing Wearable Medical Device Security.” Migration Letters 20 (S12): 1992–2006.

[11] A. S. Muhammad and F. Özkaynak, “SIEA: Secure Image Encryption Algorithm Based on Chaotic Systems Optimization Algorithms and PUFs,” Symmetry 2021, Vol. 13, Page 824, vol. 13, no. 5, p. 824, May 2021, doi: 10.3390/SYM13050824.

[12] Ali, Saif, Fawad Nasim, and Khadija Haider. "Secure middleware model for public restful apis." Al-Aasar 2, no. 1 (2025): 50-62.

[13] A. K. Mesrega, W. El-Shafai, H. E. H. Ahmed, N. A. El-Bahnasawy, F. E. Abd El-Samie, and A. E. Elfiqi, “A Hybrid Modified Advanced Encryption Standard and Chaos Encryption Algorithm for Securing Compressed Multimedia Data,” Menoufia Journal of Electronic Engineering Research, vol. 28, no. 1, pp. 63–70, Mar. 2020, doi: 10.21608/MJEER.2020.76761.

[14] Zainab, Hira, A. Khan, Ali Raza, Muhammad Ismaeel Khan, and Aftab Arif. "Integration of AI in Medical Imaging: Enhancing Diagnostic Accuracy and Workflow Efficiency." Global Insights in Artificial Intelligence and Computing 1, no. 1 (2025): 1-14.

[15] Khan, Muhammad Ismaeel, Aftab Arif, and Ali Raza A. Khan. "The Most Recent Advances and Uses of AI in Cybersecurity." BULLET: Jurnal Multidisiplin Ilmu 3, no. 4 (2024): 566-578.

[16] Khan, Ali Raza A., Muhammad Ismaeel Khan, and Aftab Arif. "AI in Surgical Robotics: Advancing Precision and Minimizing Human Error." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 1 (2025): 17-30.

[17] Khan, Muhammad Ismaeel. "Synergizing AI-Driven Insights, Cybersecurity, and Thermal Management: A Holistic Framework for Advancing Healthcare, Risk Mitigation, and Industrial Performance." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 2: 40-60.

[18] “End-to-End Encryption in Resource-Constrained IoT Device | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Aug. 12, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10174645

[19] Arif, A., A. Khan, and M. I. Khan. "Role of AI in Predicting and Mitigating Threats: A Comprehensive Review." JURIHUM: Jurnal Inovasi dan Humaniora 2, no. 3 (2024): 297-311.

[20] Zainab, Hira, Muhammad Ismaeel Khan, Aftab Arif, and Ali Raza A. Khan. "Deep Learning in Precision Nutrition: Tailoring Diet Plans Based on Genetic and Microbiome Data." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 1 (2025): 31-42.

[21] “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Aug. 12, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9328432

[22] Khan, M. I., A. Arif, and A. R. A. Khan. "AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity." BIN: Bulletin of Informatics 2, no. 2 (2024): 248-61.

[23] Zainab, Hira, Muhammad Ismaeel Khan, Aftab Arif, and Ali Raza A. Khan. "Development of Hybrid AI Models for Real-Time Cancer Diagnostics Using Multi-Modality Imaging (CT, MRI, PET)." Global Journal of Machine Learning and Computing 1, no. 1 (2025): 66-75.

[24] Khan, Muhammad Ismaeel, Aftab Arif, and Ali Raza A. Khan. "AI's Revolutionary Role in Cyber Defense and Social Engineering." International Journal of Multidisciplinary Sciences and Arts 3, no. 4 (2024): 57-66.

[25] Zainab, Hira, Ali Raza A. Khan, Muhammad Ismaeel Khan, and Aftab Arif. "Innovative AI Solutions for Mental Health: Bridging Detection and Therapy." Global Journal of Emerging AI and Computing 1, no. 1 (2025): 51-58.

[26] “A Lightweight Multi-Chaos-Based Image Encryption Scheme for IoT Networks | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Aug. 12, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10473007

[27] [A. M. N. Gilmolk and M. R. Aref, “Lightweight Image Encryption Using a Novel Chaotic Technique for the Safe Internet of Things,” International Journal of Computational Intelligence Systems, vol. 17, no. 1, pp. 1–21, Dec. 2024, doi: 10.1007/S44196-024-00535-3/FIGURES/8.

[28] “(PDF) A Benchmark for Performance Evaluation and Security Assessment of Image Encryption Schemes.” Accessed: Aug. 12, 2025. [Online]. Available: https://www.researchgate.net/publication/311668971_A_Benchmark_for_Performance_Evaluation_and_Security_Assessment_of_Image_Encryption_Schemes

[29] A. M. N. Gilmolk and M. R. Aref, “Lightweight Image Encryption Using a Novel Chaotic Technique for the Safe Internet of Things,” International Journal of Computational Intelligence Systems, vol. 17, no. 1, pp. 1–21, Dec. 2024, doi: 10.1007/S44196-024-00535-3/FIGURES/8.

[30] T. X. Meng and W. Buchanan, “Lightweight Cryptographic Algorithms on Resource-Constrained Devices,” 2020, doi: 10.20944/preprints202009.0302.v1.

[31] “Machine Learning in Chaos-Based Encryption: Theory, Implementations, and Applications | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Aug. 13, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10311558

[32] A. S. Muhammad and F. Özkaynak, “SIEA: Secure Image Encryption Algorithm Based on Chaotic Systems Optimization Algorithms and PUFs,” Symmetry 2021, Vol. 13, Page 824, vol. 13, no. 5, p. 824, May 2021, doi: 10.3390/SYM13050824.

[33] “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Aug. 13, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9328432

[34] “End-to-End Encryption in Resource-Constrained IoT Device | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Aug. 13, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10174645

[35] A. S. D. Alluhaidan and P. Prabu, “End-to-End Encryption in Resource-Constrained IoT Device,” IEEE Access, vol. 11, pp. 70040–70051, 2023, doi: 10.1109/ACCESS.2023.3292829.

[36] A. K. Mesrega, W. El-Shafai, H. E. H. Ahmed, N. A. El-Bahnasawy, F. E. Abd El-Samie, and A. E. Elfiqi, “A Hybrid Modified Advanced Encryption Standard and Chaos Encryption Algorithm for Securing Compressed Multimedia Data,” Menoufia Journal of Electronic Engineering Research, vol. 28, no. 1, pp. 63–70, Mar. 2020, doi: 10.21608/MJEER.2020.76761.

[37] S. N. Alrekaby, M. A. A. Khodher, L. K. Adday, and R. Aljuaidi, “Secure Image Transmission Using Multilevel Chaotic Encryption and Video Steganography,” Algorithms 2025, Vol. 18, Page 406, vol. 18, no. 7, p. 406, Jul. 2025, doi: 10.3390/A18070406.

[38] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities,” IEEE Access, vol. 9, pp. 28177–28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[39] A. K. Mesrega, W. El-Shafai, H. E. H. Ahmed, N. A. El-Bahnasawy, F. E. Abd El-Samie, and A. E. Elfiqi, “A Hybrid Modified Advanced Encryption Standard and Chaos Encryption Algorithm for Securing Compressed Multimedia Data,” Menoufia Journal of Electronic Engineering Research, vol. 28, no. 1, pp. 63–70, Mar. 2020, doi: 10.21608/MJEER.2020.76761.

[40] [T. X. Meng and W. Buchanan, “Lightweight Cryptographic Algorithms on Resource-Constrained Devices,” 2020, doi: 10.20944/preprints202009.0302.v1.

[41] “End-to-End Encryption in Resource-Constrained IoT Device | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Aug. 13, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10174645

[42] N. Ahmed, H. M. Shahzad Asif, and G. Saleem, “A Benchmark for Performance Evaluation and Security Assessment of Image Encryption Schemes,” International Journal of Computer Network and Information Security, vol. 8, no. 12, pp. 28–29, Dec. 2016, doi: 10.5815/IJCNIS.2016.12.03.

[43] A. S. Muhammad and F. Özkaynak, “SIEA: Secure Image Encryption Algorithm Based on Chaotic Systems Optimization Algorithms and PUFs,” Symmetry 2021, Vol. 13, Page 824, vol. 13, no. 5, p. 824, May 2021, doi: 10.3390/SYM13050824.

[44] S. N. Alrekaby, M. A. A. Khodher, L. K. Adday, and R. Aljuaidi, “Secure Image Transmission Using Multilevel Chaotic Encryption and Video Steganography,” Algorithms 2025, Vol. 18, Page 406, vol. 18, no. 7, p. 406, Jul. 2025, doi: 10.3390/A18070406.

[45] Kazmi, Syeda Saliha, Shahbaz Shamshad, Fawad Nasim, Saira Hashim, Nisha Azam, and Bushra Ambar. "Real-Time Vehicle Detection with Advanced Machine Learning Algorithms." Journal of Computing & Biomedical Informatics 7, no. 02 (2024).

[46] A. S. D. Alluhaidan and P. Prabu, “End-to-End Encryption in Resource-Constrained IoT Device,” IEEE Access, vol. 11, pp. 70040–70051, 2023, doi: 10.1109/ACCESS.2023.3292829.