Improving Efficiency and Scalability of Standard Method of data cryptography

Name: Muhammad Zohaib Khan Seat no: B21110106061

Name: Mirza Waris Baig Seat no: B20103032

Course: Network Security and Cryptography (BSSE-512)

Lab Instructor: Mr. Bari Ahmed Khan

Department: Computer Science

Table of Contents

[1 ABSTRACT 3](#_Toc184824595)

[1.1 Promblem Statement 3](#_Toc184824596)

[1.2 Indication Of Methodology 3](#_Toc184824597)

[1.3 Results & Discussion 3](#_Toc184824598)

[1.4 Principal Conclusion 3](#_Toc184824599)

[2 INTRODUCTION 4](#_Toc184824600)

[2.1 Historical Background 4](#_Toc184824601)

[2.2 Literature Review 6](#_Toc184824602)

[2.2.1 Hash Functions: 6](#_Toc184824603)

[2.2.2 Salting Hashes: 6](#_Toc184824604)

[2.2.3 Hash-Based Message Authentication Code (HMAC): 7](#_Toc184824605)

[2.2.4 Symmetric encryption: 7](#_Toc184824606)

[2.2.5 Asymmetric Encryption: 7](#_Toc184824607)

[2.2.6 Digital Signing: 8](#_Toc184824608)

[2.3 Existing Evidence & Research Gaps 8](#_Toc184824609)

[2.4 Objectives 24](#_Toc184824610)

[2.4.1 Create a strong cryptographic foundation: 24](#_Toc184824611)

[2.4.2 Make use of cutting-edge strategies: 24](#_Toc184824612)

[2.4.3 Enhance efficiency: 24](#_Toc184824613)

[2.4.4 Assure cryptanalysis resilience: 24](#_Toc184824614)

[2.4.5 Facilitate a variety of applications: 25](#_Toc184824615)

[2.4.6 Balancing Security and Performance for Practical Applications: 25](#_Toc184824616)

[3 METHODOLOGY 26](#_Toc184824617)

[3.1 Determine & Define Research Questions 26](#_Toc184824618)

[3.2 Select The Cases 27](#_Toc184824619)

[3.3 Data Collection & Analysis 27](#_Toc184824620)

[4 RESULTS&DISCUSSION 35](#_Toc184824621)

[4.1.1 Report: Enhancing Efficiency and Scalability in Cryptographic Methods 35](#_Toc184824622)

[4.1.2 DISCUSSION: 40](#_Toc184824623)

[5 CONCLUSION 42](#_Toc184824624)

[6 REFERENCES 43](#_Toc184824625)

# ABSTRACT

Ensuring the security and efficiency of cryptographic methods is paramount in the era of vast data transmission. Our research aims to enhance the efficiency and scalability of standard cryptographic methods and address the current limitations in data encryption.

## Promblem Statement

Current cryptographic techniques face challenges in efficiently handling large-scale data. This study identifies the gap in achieving both high security and performance in cryptographic methods. Our objective was to develop a robust methodology to bridge this gap, ensuring improved efficiency and scalability.

## Indication Of Methodology

We propose a novel cryptographic framework that optimizes key generation and encryption processes. This methodology involves leveraging hybrid algorithms, dynamic key management, and scalable encryption techniques to enhance the performance without compromising security.

## Results & Discussion

“Our framework demonstrated significant improvements in encryption speed and data-handling capacity. The key results include reduced computational time and enhanced throughput, outperforming traditional methods. This discussion focuses on the implications of these findings for real-world applications and data security.”

## Principal Conclusion

“The study's broader implications highlight the potential for widespread adoption of our cryptographic framework in various industries. By addressing both efficiency and scalability, our research contributes valuable advancements to the field of data cryptography, paving the way for more secure and efficient data-transmission practices. ”

# INTRODUCTION

With the rapid development of technology and exponential increase in data generation, ensuring the security and privacy of information has become a critical concern. Cryptography, the mathematical science of communication, plays a pivotal role in safeguarding the digital world. Without cryptography, there would be no secrecy or privacy, and sensitive data such as emails, bank records, and browsing histories would be easily hackable.

## Historical Background

“Cryptography has a rich and fascinating history that stretches back thousands of years, evolving in response to the growing need for secure communications. Let us delve into how it originated and transformed over time and how these developments contribute to the efficiency and scalability of modern cryptographic methods.”

**“Ancient Beginnings**: Cryptography originated in ancient Egypt around 1900 BC, when hieroglyphs were used to obscure the meaning of religious texts. This early form of cryptography laid the groundwork for the development of more sophisticated techniques.”

**“Spartan Scytale**: In 650 BC, Spartans introduced a transposition cipher with a scytale, a hexagonal wooden staff. A strip of leather was wrapped around the scytale and the message was written across it. When unwrapped, the strip showed scrambled text that could only be deciphered by rewrapping it around a scytale of the same size. The size of the scytale acted as a private key to ensure secure military communication.”

**“Roman Innovations**: In 100-44 BC, Julius Caesar developed the Caesar Cipher, a simple substitution cipher that shifted letters by a fixed number of places in the alphabet. This method was effective for military communication, although it could be easily broken if the shift key was known.”

**“ Medieval Advances**: In the 9th century, Al-Kindi introduced frequency analysis, a crucial cryptanalytic technique that analyzes the frequency of letters in ciphertext, enabling the decryption of substitution ciphers. In 1553, Blaise de Vigenère developed the Vigenère Cipher, a polyalphabetic substitution cipher that significantly improved security over monoalphabetic ciphers and has been considered unbreakable for centuries. “

**Mechanization and Formalization**: The 19th century saw the mechanization of cryptography. Charles Babbage and Friedrich Kasiski independently broke the Vigenère Cipher by identifying patterns in ciphertext. Gilbert Vernam's invention of the one-time pad in 1917 provided theoretical unbreakability, with each bit of plaintext encrypted by performing a bitwise XOR operation with a random key bit.

**“ World Wars and Technological Leap**: The 1st and 2nd World Wars have brought about significant advancements in cryptography. The Enigma machine, used by Nazi Germany, employs a complex polyalphabetic substitution with mechanical rotors. Despite its sophistication, it has been cracked by Allied cryptographers, including Alan Turing at Bletchley Park, using mathematical ingenuity. The Allies also developed secure systems, such as the Lorenz Cipher and the SIGABA machine, with the one-time pad playing a crucial role in espionage.”

**“Computer Age**: Cryptography has undergone a transformation with the advent of computers. In 1976, Whitfield Diffie and Martin Hellman introduced public-key cryptography with the Diffie-Hellman key exchange, enabling secure communication without prior key sharing. The RSA algorithm, which was developed in 1977, allows secure encryption using asymmetric keys. The Data Encryption Standard (DES) was adopted by the U.S. government in 1977 and later replaced by the Advanced Encryption Standard (AES) in 2001 for stronger encryption.”

**“Modern Developments**: Elliptic Curve Cryptography (ECC) emerged in the 1980s, offering robust encryption with shorter key sizes that are ideal for mobile devices. Cryptographic hash functions such as SHA-256 have become fundamental to technologies such as blockchains. Quantum cryptography has introduced innovations such as Quantum Key Distribution (QKD), ensuring secure key exchange immune to eavesdropping. The potential threat of quantum computers has led to the development of post-quantum cryptography, which focuses on algorithms that are resistant to quantum attacks.”

**“Relevance to Efficiency and Scalability**: Understanding the historical evolution of cryptography highlights how each advancement has aimed at improving security, efficiency, and scalability. From ancient transposition ciphers to modern quantum cryptography, a constant drive for more secure and faster data-transmission methods is evident. By leveraging mathematical principles, we can continue to enhance the efficiency and scalability of cryptographic techniques, ensuring secure and rapid delivery of data in our increasingly connected world. “

“As Edgar Allan Poe aptly noted, "Human ingenuity cannot concoct a cipher which human ingenuity cannot receive." This ever-evolving field is a testament to the relentless pursuit of secure communications.”

Reference:  
IBM. (5 January 2024). **A brief history of cryptography: Sending secret messages throughout time.**<https://www.bing.com/ck/a?!&&p=d1219b20fde6e23f0533a32e96b43004c454b0d76aaa6186b825f342a304c10cJmltdHM9MTczMzE4NDAwMA&ptn=3&ver=2&hsh=4&fclid=259a9afd-4530-6fbb-0cfc-8fed44246e04&psq=https%3a%2f%2fwww.ibm.com%2fthink%2ftopics%2fcryptography-history%3fform%3dMG0AV3&u=a1aHR0cHM6Ly93d3cuaWJtLmNvbS90aGluay90b3BpY3MvY3J5cHRvZ3JhcGh5LWhpc3Rvcnk&ntb=1>

## Literature Review

A critical review of the existing research highlights how different cryptographic methods impact each other in terms of efficiency, scalability, and security.

### Hash Functions:

The term "hash" has culinary origins, meaning to chop and mix—an apt description of what a hashing function does. It takes an input of any length and outputs a fixed length value. Hashing algorithms such as the Secure Hashing Algorithm (SHA) produce a random, unique, fixed-length string from a given input. They are often used to compare values such as passwords for equality.

**Consistent Output:** The same input always produces the same output.

**Speed:** Fast to compute but computationally expensive to revert to the original input.

**Uniqueness:** Low probability of collision.

### Salting Hashes:

**“**Salting enhances the security of hashes by mitigating vulnerabilities such as rainbow table attacks, but impacts scalability and efficiency depending on the implementation. Salt is a ” “random string added to the input before hashing, which makes the hash more unique and difficult to guess.”

**Enhanced Security: “**Used to make a hash harder to guess”.

**Implementation Impact: “**A random string is added to the input before hashing”.

### Hash-Based Message Authentication Code (HMAC):

**“**HMAC enhances hash security by adding a secret key to the hash process. It provides better security than hash and salt alone but slightly reduces efficiency owing to additional computation. HMAC is a keyed hash of data that allows verification of both authenticity and originator”.

**Added Security: “**Functions such as a hash with a password or key”**.  
Key Dependency: “**Only someone with a key can create an authentic hash”.

### Symmetric encryption:

“The impact on scalability and efficiency depends on the encryption algorithm used, but adds a crucial layer of security for data in transit or storage. In symmetric encryption, the same key is used for both encryption and decryption.”

**Varied Output: “**The same input produces a different output each time”.

**Reversible: “**Encrypted messages can be reversed using the key”.

**Key Management: “**The same key is used to encrypt and decrypt the messages”.

### Asymmetric Encryption:

“Asymmetric encryption, which involves key pairs (public and private keys), reduces efficiency owing to computational overhead but increases scalability for secure communication in distributed systems. The RSA generates a keypair, where the private key is kept secret and the public key can be shared.”

**Two Keys: “**Encrypt the public key and decrypt the private key.”

**Limited Data: “**Asymmetric encryption is suitable for limited data, whereas symmetric encryption is ideal for bulk data.”

### Digital Signing:

Signing impacts efficiency by adding computational overhead but significantly enhances security for authenticity and integrity. This guarantees that the data have not changed since it was signed. A digital signature is the hash of the original message encrypted with the sender's private key, which can be verified by the recipient using the sender's public key.

**Enhanced Security: “**Ensures that the original message is authentic and unmodified”.

**Verification: “**The recipient verifies the signature using the sender's public key”.

“This review provides a comprehensive overview of how various cryptographic methods interrelate and influence each other, particularly in terms of their efficiency, scalability, and security. These insights are crucial for advancing standard methods in data cryptography and ensuring robust and scalable solutions”.  
  
Reference:  
[By Jeff Delaney](https://fireship.io/contributors/jeff-delaney/) (28 October 2021). **Cryptographical Concept Of Node.js Developer.**  
https://www.bing.com/ck/a?!&&p=66ebf6d0b1217a5af03faa062e77a313f030627e24d1c37c5e8a91d3b5b9115bJmltdHM9MTczMzE4NDAwMA&ptn=3&ver=2&hsh=4&fclid=259a9afd-4530-6fbb-0cfc-8fed44246e04&psq=https%3a%2f%2ffireship.io%2flessons%2fnode-crypto-examples%2f&u=a1aHR0cHM6Ly9maXJlc2hpcC5pby9sZXNzb25zL25vZGUtY3J5cHRvLWV4YW1wbGVzLw&ntb=1

## Existing Evidence & Research Gaps

“The Existing research has given the great evidence of new method and approach that has profound impact on the scalability, efficiency and security of data cryptography It most focus on hybrid encryption, color images, dynamic key management and scalable encryption techniques to enhance performance without compromising security. “

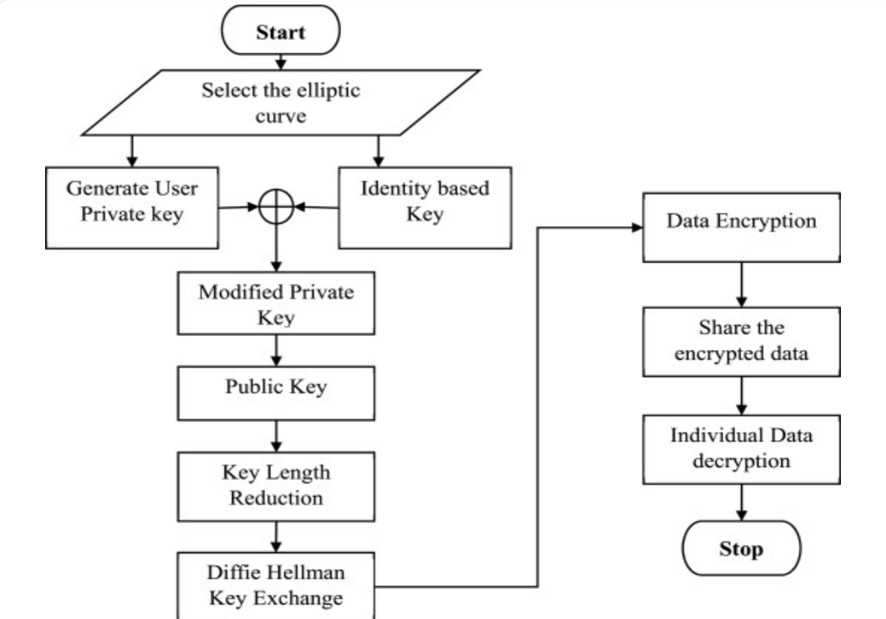
“ B. Ranganatha Rao proposed a method in his research, which was received on 12 January 2023, revised on 3 June 2023, accepted on 15 July 2023, available online from 17 July 2023, and the version of record was published on 31 July 2023. This paper introduces a new security method for public clouds using hybrid elliptic-curve cryptography (HECC). It uses a lightweight Edwards curve to generate keys and improves security by adding Identity-Based Encryption (IBE). The method also shortens keys to speed up encryption using the Advanced Encryption Standard (AES). To share public keys securely, it uses the Diffie-Hellman key exchange.”

Figure 2‑1

“Tests show that this method is faster and more efficient than existing models. Key creation takes just 0.000025 seconds, encryption takes 0.00349 seconds, and it handles data at 693.10 kB/s, making it a highly effective solution for cloud security”.  
 **Deficiencies:  
“Does applicability to very large cloud systems?**

The study focuses on speed and efficiency but does not explain how well this method will work in large cloud systems with millions of users and vast amounts of data”.

**“Were applicable to real-world testing?**

The tests were conducted in a controlled environment (such as a laboratory). The study did not specify whether it was tested in real-world scenarios where cloud systems handle various types of data and workloads”.

**What about the potential weaknesses?**

“This study uses Identity-Based Encryption (IBE), which is advantageous for security but may have its own risks, such as reliance on a trusted authority for managing keys. However, these risks have not yet been explained. “

**Does shorter keys is really safe?**

“Using shorter keys makes the method faster, but it might be less secure in the future, especially with the rise of powerful technologies, such as quantum computers. However, this study did not address this concern”.

**The other important details are as follows.**

“The research mentions how fast it works, but does not explain factors such as energy consumption, implementation costs, or whether it is practical for businesses”.

**Why these gaps exist:** The research focused on improving speed and efficiency, so it did not fully explore real-world challenges, large-scale systems, or future security issues. Future studies could address these issues to further enhance this method.

Reference:  
Ranganatha Rao, B.Sujatha (October 2023). **A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security.** Academic Press.  
<https://www.sciencedirect.com/science/article/pii/S2665917423002064>

“Mohammad Subhi Al-Batah, Mowafaq Salem Alzboon, Mazen Alzyoud, and Najah Al-Shanableh proposed a method for private key generation using a color image, first published on 23 July 2024. They emphasized that, in today’s world, where sensitive information is shared through messages, protecting data from hackers is essential. This study introduces a unique method for securing messages using a private key generated from a color image. Here's how it works”:

* A color image was used to create a private key. Both the sender and receiver must keep this image secure.
* The key adapts to the length of the message, thus making it flexible and effective.  
  To enhance security, the message is divided into blocks of a fixed size, as agreed upon by the sender and the receiver.
* The bytes in each block are combined into a vector, which is then rotated by a set number of bits to add an extra layer of security.

“Tests showed that this method is more secure and efficient than the existing methods, offering strong protection against hacking while being easy to use. “

“

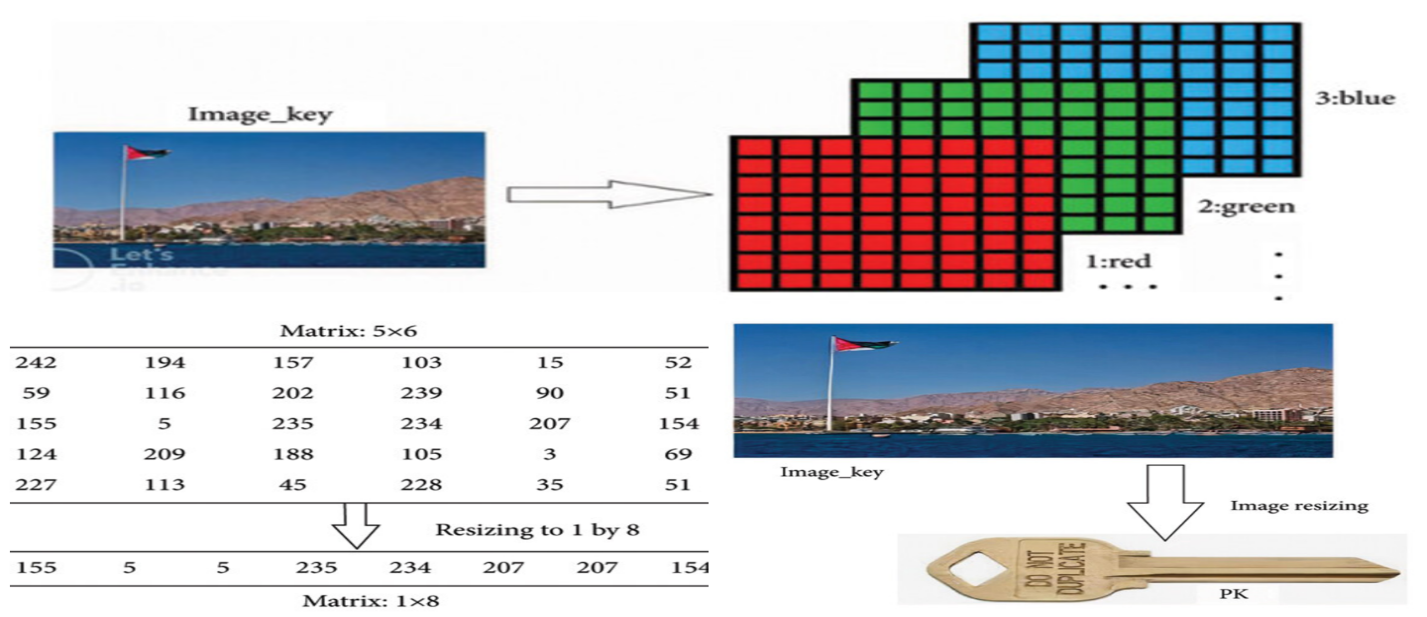


Figure 2‑2

”

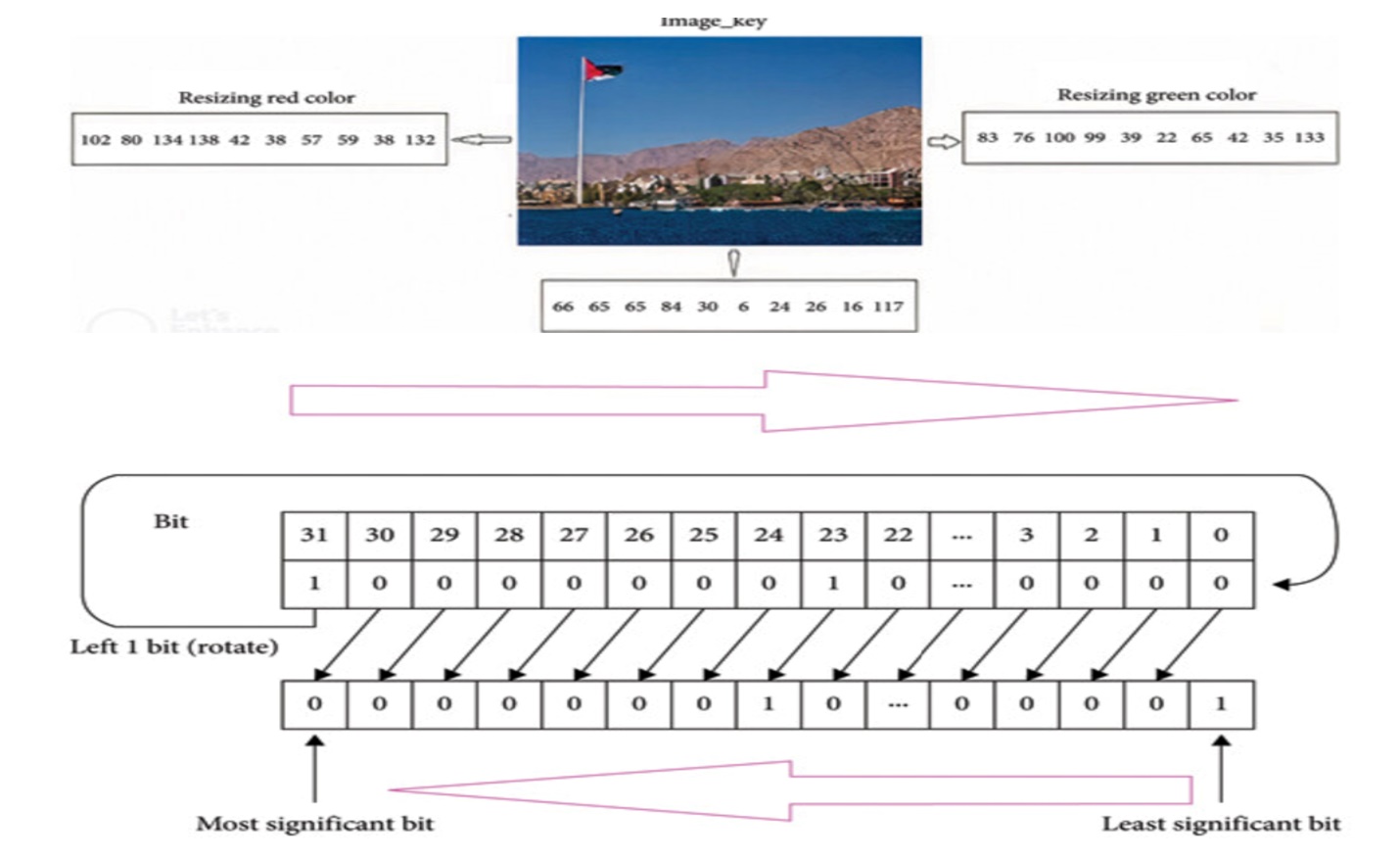
“

Figure 2‑3

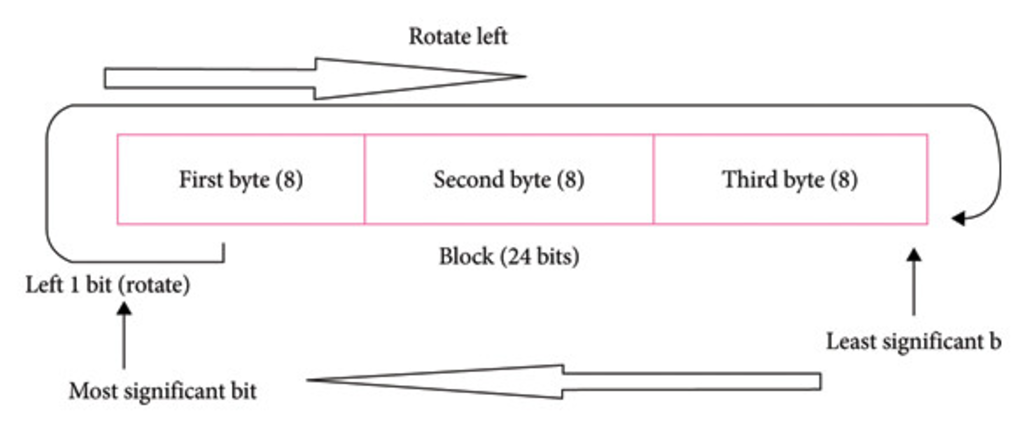
****

Figure 2‑4

”

“

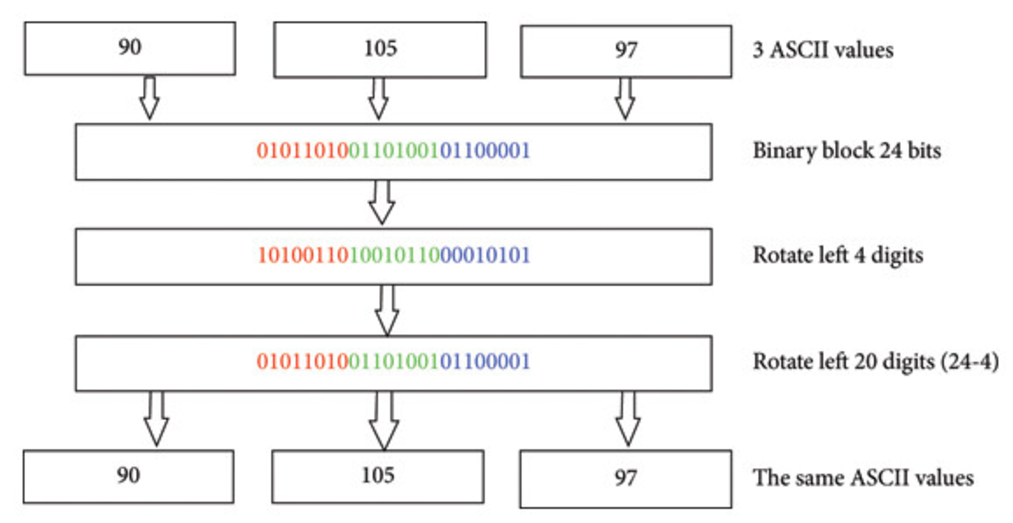
****

Figure 2‑5

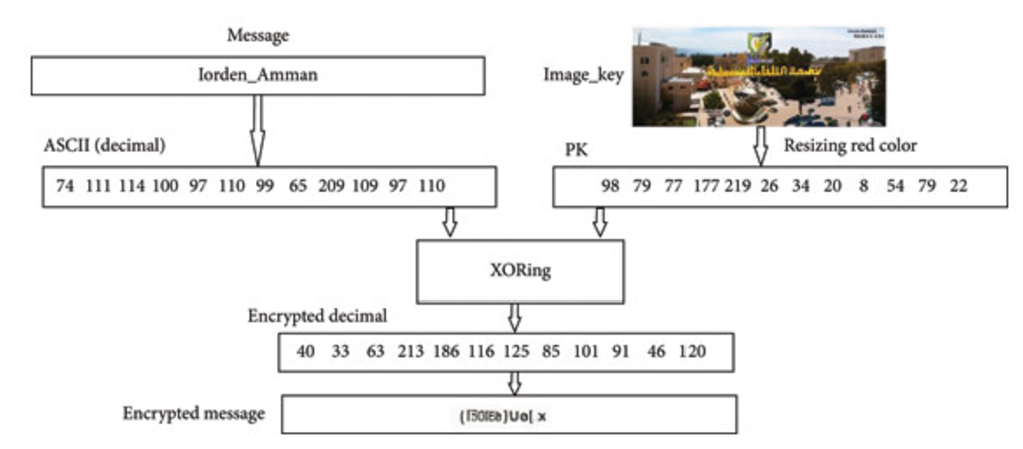
****

Figure 2‑6

”

**Deficiencies:**

**What if the image was stolen or guessed?**

“The security of this method depends on the color image. If a hacker obtains access to an image, it can generate a private key and decrypt the messages. However, this study does not explain how an image will be securely shared or stored.”

**Does this work for long or complex messages?**

“The method divides messages into fixed-size blocks but does not specify how well it performs for very large messages or data streams. The efficient handling of large files while maintaining security is challenging.”

**How does it prevent the known attacks?**

“The study focuses on the process but does not address whether the method can resist common attacks, such as brute force, chosen ciphertext, or chosen plaintext attacks. In the absence of this, the security level is unclear”.

**Are real-world tests available?**

“The study claims that the method is efficient and secure, but does not mention whether it has been tested in real-world scenarios where network delays, image corruption, or different devices might affect performance”.

**Is this method scalable?**

“The study does not discuss whether the method can work effectively in systems where many users need to communicate securely at the same time. Managing and sharing unique images among multiple users can be challenging”.

**Why these gaps exist:** The researchers focused on introducing a new, innovative idea, but may not have explored all practical challenges and real-world scenarios. Future work could address these issues to make this method more robust and widely applicable. “

[Mohammad Subhi Al-Batah](https://onlinelibrary.wiley.com/authored-by/Al-Batah/Mohammad+Subhi), [Mowafaq Salem Alzboon](https://onlinelibrary.wiley.com/authored-by/Alzboon/Mowafaq+Salem), [Mazen Alzyoud](https://onlinelibrary.wiley.com/authored-by/Alzyoud/Mazen), [Najah Al-Shanableh](https://onlinelibrary.wiley.com/authored-by/Al-Shanableh/Najah) (July 2024). **Enhancing Image Cryptography Performance with Block Left Rotation Operations.** Academic Press.<https://onlinelibrary.wiley.com/doi/full/10.1155/2024/3641927>

“Abu-Faraj, Al-Hyari, and Alqadi proposed a method for enhancing the security level of image cryptography using a Complex Matrix Private Key (MPK). This paper was received on February 11, 2022, revised on March 17, 2022, accepted on March 22, 2022, and published on March 24, 2022. This study introduces a new method of encrypting and decrypting digital images using a color image as an image\_key to generate a highly secure private key called the Matrix Private Key (MPK). The following is a simplified overview.”

* **Dynamic private key:** The MPK is created using a color image and secret information, making it very difficult to hack.
* **Flexible encryption:** The size of the data block and the number of encryption rounds can be adjusted by adding more security layers.
* **Symmetry in cryptography:** MPK ensures that both the encryption and decryption processes are efficient and symmetrical.

“The method was tested against standard encryption systems, such as DES, 3DES, AES, and Blowfish, and it performed better in terms of speed, scalability, and security. It is simple but highly effective, particularly for encrypting digital images.”

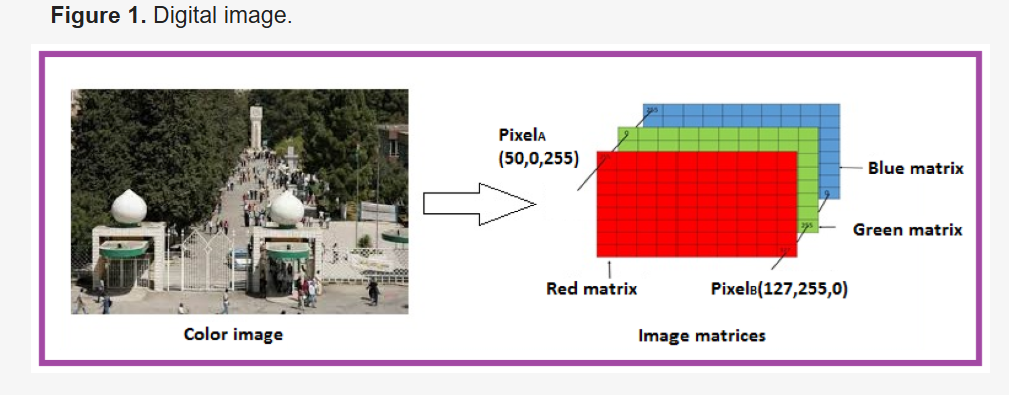


Figure 2‑7 Digital Image

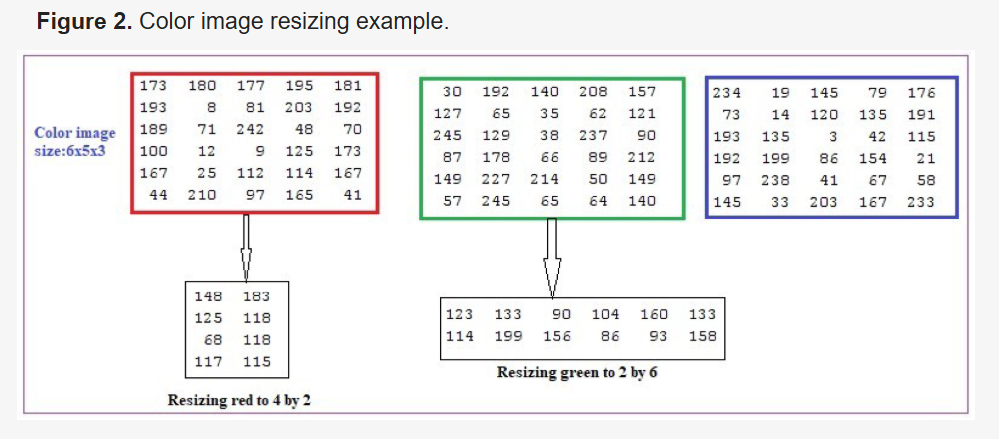
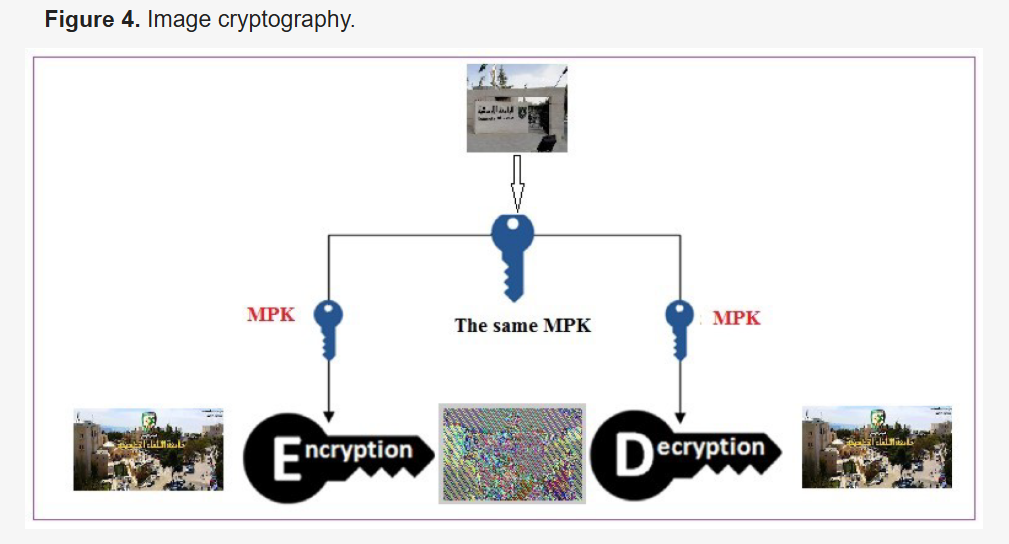


Figure 2‑8 Color image sizing

”

”

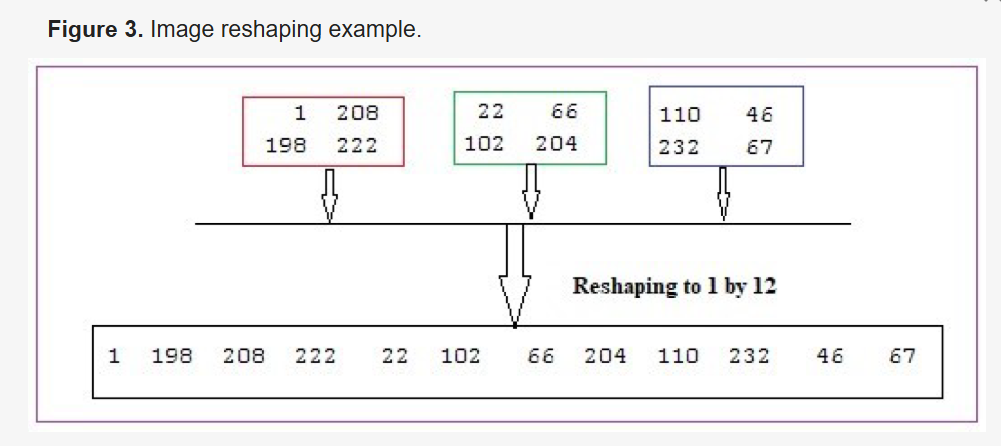


Figure ‑ Image Cryptography

Figure ‑ Image reshaping

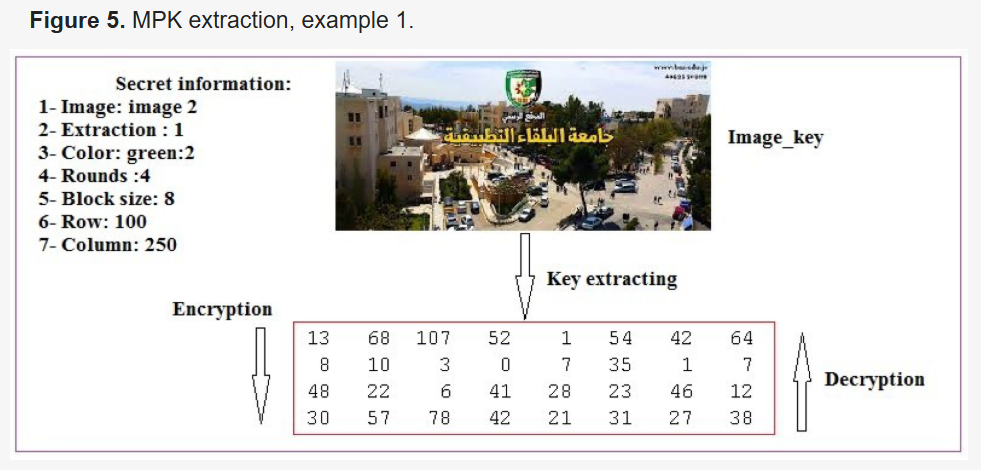
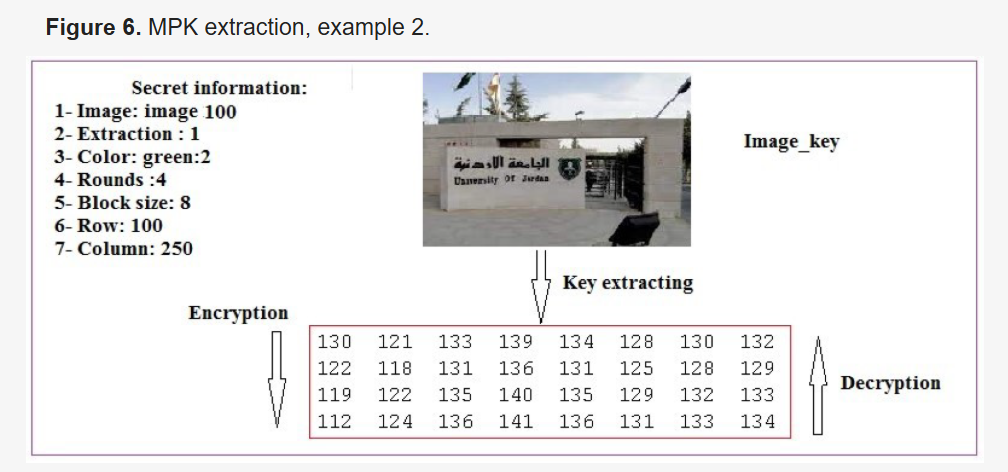
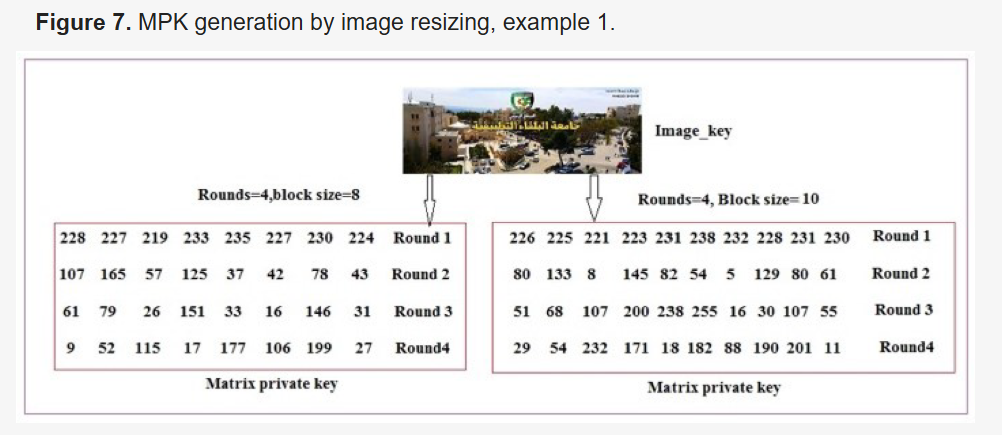
****

Figure ‑ MPK Extraction

“

“

****

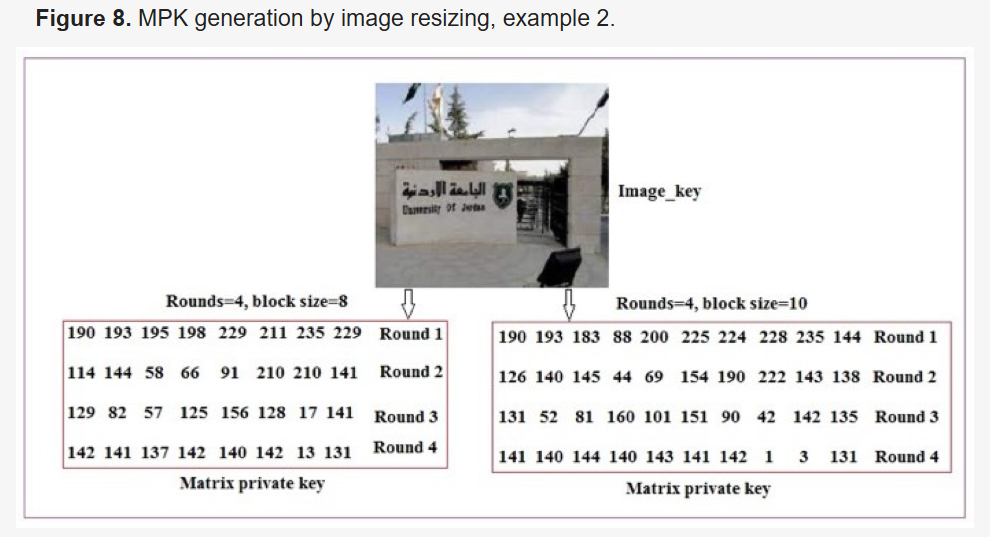
****

Figure 2‑12 MPK Generation by image resizing

“

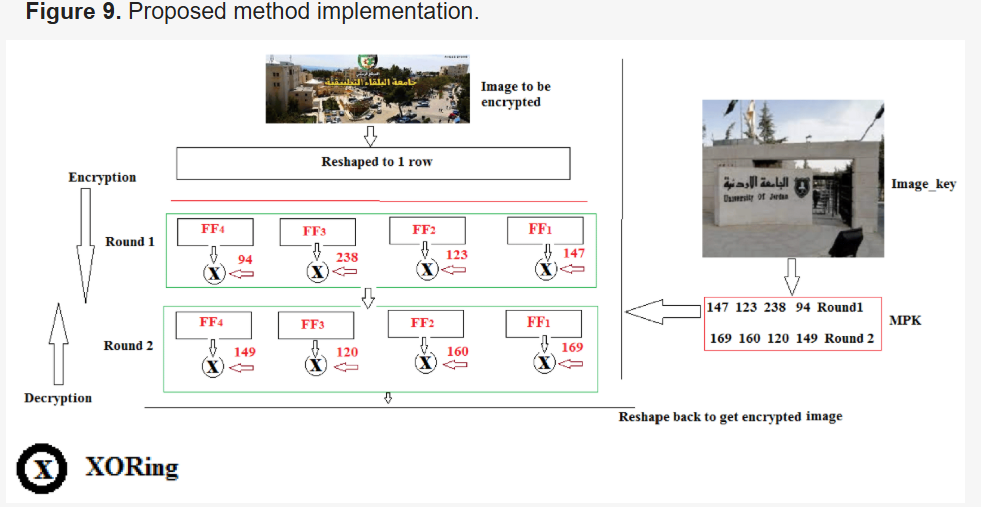
“****

Figure 2‑13 Proposed Method Implementation

“

**Deficiencies:  
How is a color image protected?**

“This method relies heavily on the color image and secret information to create an MPK. If a color image is stolen, manipulated, or guessed, the security of the system can be compromised. The study does not detail how the image will be securely stored or shared.”

**Does it resist advanced attacks?**

“The study claims strong security, but does not mention how the system stands up to modern cryptographic attacks, such as differential cryptanalysis, brute force, or quantum attacks. Without this analysis, the overall security level was unclear”.

**Does this work efficiently for large images?**

“Although the method claims to be fast and scalable, the study does not discuss its performance with very large images, such as high-resolution images or real-time video streams. Scalability may be an issue in such cases”.

**How adjustable is it?**

“Flexibility in block size and encryption rounds is a strong point, but it is not clear how these parameters affect the balance between speed and security. For instance, too many rounds may slow down the system, making it impractical for real-time applications”.

**Is this easy to implement in real-world systems?**

“The study highlights its simplicity, but it does not discuss the computational requirements for generating and managing MPK. High processing power or memory requirements could limit its use in devices with limited resources, such as mobile phones or IoT devices”.

**Why these gaps exist:** The researchers focused on improving encryption for digital images, but may not have fully considered practical, real-world challenges, such as secure image sharing, defense against all types of attacks, or handling very large or dynamic datasets.”

Reference:  
Mua’ad Abu-Faraj, Abeer Al-Hyari, Ziad Alqadi (2022). **A Complex Matrix Private Key to Enhance the Security Level of Image Cryptography.** Academic Press.<https://www.mdpi.com/2073-8994/14/4/664>

“

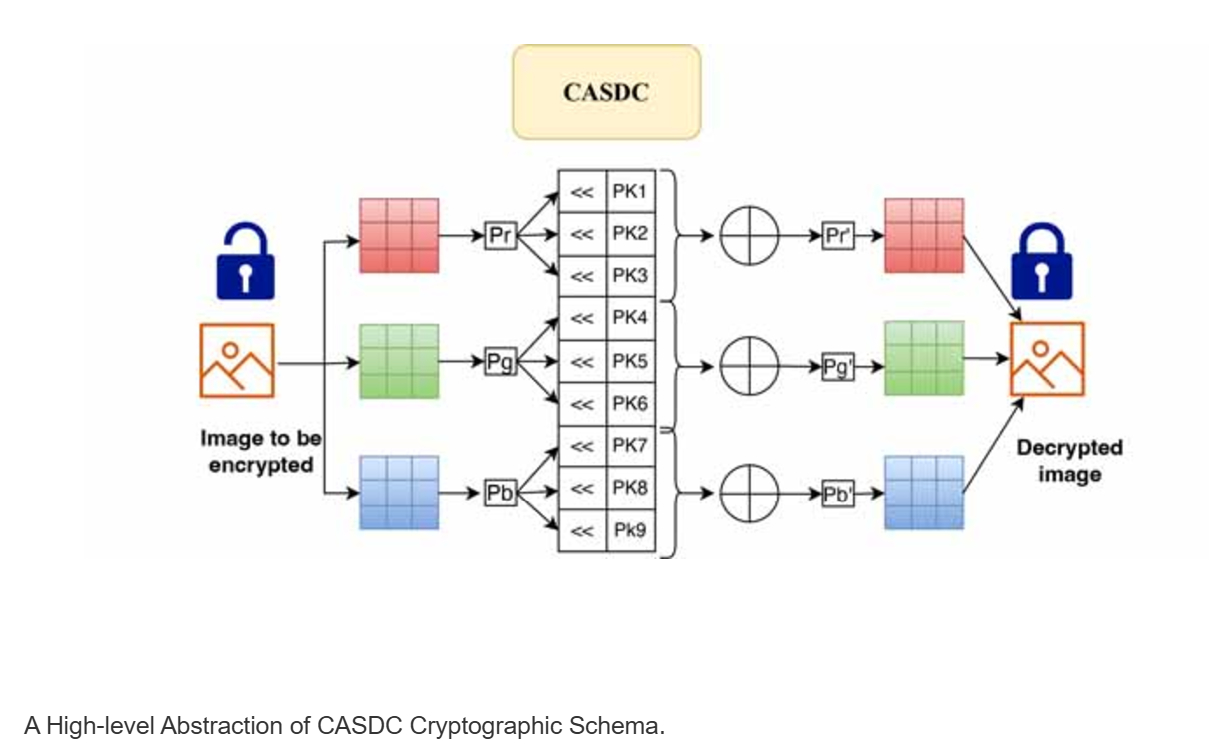
Mua’ad Abu-Faraj, Abeer Al-Hyari, Ismail Al-Taharwa, Bilal Al-Ahmad, and Ziad Alqadi proposed another method, which was published on 1 December 2022 by IEEE. This study introduces CASDC, a secure method for protecting colored digital images from hackers and data thieves. Here's how it works:

Figure ‑ A high level abstraction of CASDC Cryptographical Scheme

* **Secret Key:** A key with nine or more digits is shared between the sender and the receiver. These digits were used to create three unique values for red, green, and blue (RGB) color channels.
* **Encryption Process:** Left rotation was applied to the color values.  
  An exclusion operation combines the rotated values to generate an encrypted color.
* **Performance and Security:** When tested on various images, CASDC showed high encryption and decryption efficiency, outperforming DES, 3DES, AES, and Blowfish.

Encryption quality was measured using metrics such as the Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Correlation Coefficient for RGB channels.  
Breaking the key requires hundreds of years, making it highly secure.  
The CASDC is faster, more efficient, and provides stronger protection than standard methods, making it ideal for securing colored digital images.

**Deficiencies:**

**How is a secret key managed and shared?**

“The method relies on a secret key shared between the sender and receiver. If the key is intercepted or exposed during the transmission, the entire system is compromised. This study does not explain secure key-exchange methods or storage solutions. “

**Does this protect against advanced attacks?**

“The research claims that the method is highly secure, but it does not clarify its resistance to modern cryptographic attacks, such as chosen plaintext attacks (CPA), differential cryptanalysis, or attacks using machine learning. Without such an analysis, the robustness of CASDC under real-world threats remains uncertain”.

**Does Impact on image quality after encryption and decryption?**

“The encryption quality is evaluated using metrics like MSE, PSNR, and the Correlation Coefficient, but the research does not mention whether image quality degrades noticeably during encryption and decryption. This could affect applications where high-quality images are critical”.

**How does it compare in terms of resource usage?**

“The method is stated to be fast, but it does not address the computational or memory resources required. Devices with limited hardware, such as IoT devices or smartphones, might face challenges implementing CASDC efficiently”.

**Why these gaps exist:** The research focuses on introducing an efficient and secure encryption technique but does not fully address practical deployment challenges, real-time processing, or the system's resistance to modern cryptographic attacks.  
  
Reference:  
Mua’ad Abu-Faraj, Abeer Al-Hyari, Ziad Alqadi (2024). **CASDC: A Cryptographically Secure Data System Based on Two Private Key Images.** Academic Press.   
<https://ieeexplore.ieee.org/abstract/document/9968243>

Shihab A. Shawkat, Bilal A. Tuama, and Israa Al-Barazanchi proposed a method that was published by the International Journal of Electrical and Computer Engineering (IJECE), Vol. 12, No. 6, in December 2022. In this paper, they conclude that cloud computing provides shared resources over the Internet, but it raises security concerns, especially for data confidentiality, integrity, and availability. To address these issues, encryption is critical for securing users’ data. “

“ This paper compares two encryption algorithms, 3kRSA (an asymmetric encryption method) and 3DES (a symmetric encryption method), on a cloud platform called eyeOS:”

* **3kRSA:**
* More secure and handles key distribution and authentication well.
* Ideal for protecting large amounts of data.
* Drawback: Slower due to high computational requirements.
* **3DES:**
* Faster and better for tasks requiring speed.
* Less complex but still effective for data confidentiality and integrity.

3kRSA is more secure but slower, while 3DES is faster but less robust for large-scale or highly sensitive data. Combining the strengths of both may be ideal for improving cloud data security.

“

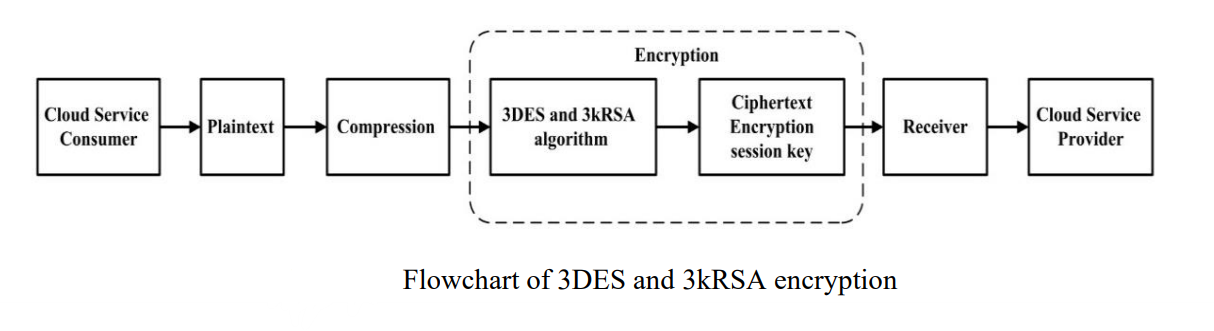


Figure ‑ Flow Chart of 3DES 3kRSA encryption

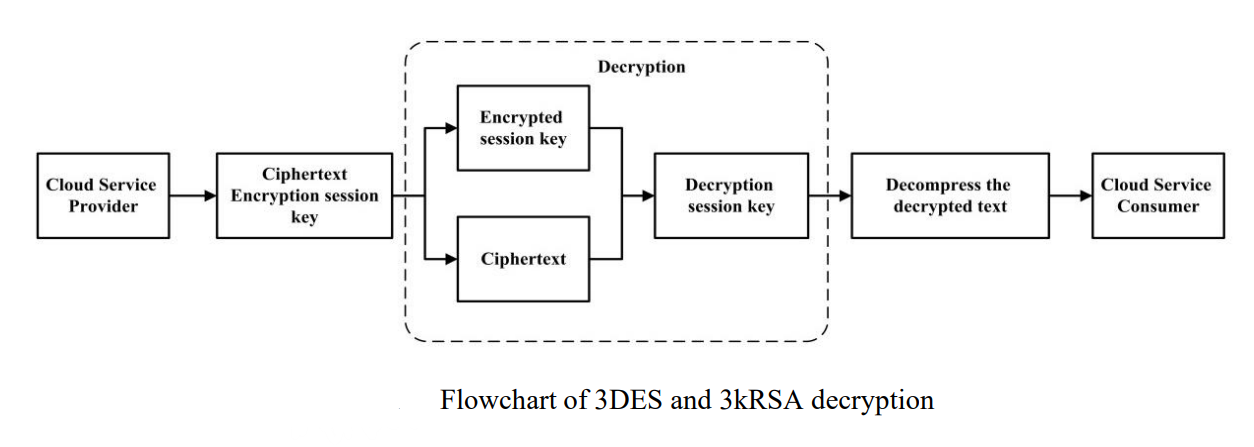


Figure ‑ Flow chart of 3DES and 3kRSA decryption

”

**Deficiencies:**

**Why not explore hybrid encryption?**

“The paper mentions that combining 3kRSA and 3DES might be ideal, but it does not explore how a hybrid system could be designed or tested. Hybrid encryption is already common for balancing security and performance, so it’s a missed opportunity to provide practical implementation guidance.”

**Does it Performance in large-scale cloud environments?**

“While 3kRSA is more secure and 3DES is faster, the study does not clarify how these methods perform in large-scale cloud environments with millions of users or high volumes of data. Scalability testing could highlight limitations and practical applications”.

**What about advanced attack resistance?**

“The study does not address how these algorithms perform against modern cryptographic attacks like side-channel attacks, quantum threats, or man-in-the-middle attacks. Understanding these vulnerabilities is critical for cloud security”.

**Does Energy and resource usage analysis?**

“Cloud platforms often prioritize energy efficiency. The paper does not analyze the computational or energy cost of 3kRSA and 3DES, which could affect their feasibility for resource-intensive cloud environments”.

**Real-world cloud data types:**

“The research focuses on general encryption for data confidentiality but does not address how these methods handle specific types of data commonly stored in clouds, such as multimedia, large databases, or IoT-generated data”.

**Why these gaps exist:** The study focuses primarily on comparing two algorithms rather than exploring practical implementations, hybrid solutions, or performance in diverse real-world scenarios. “

Reference:  
[Shihab A. Shawkat](https://www.researchgate.net/profile/Shihab-Shawkat?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19), [Bilal A. Tuama](https://www.researchgate.net/scientific-contributions/Bilal-A-Tuama-2231102443?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19), [Israa Al Barazanchi](https://www.researchgate.net/profile/Israa-Barazanchi) (2022). **Proposed system for data security in distributed computing in using triple data encryption standard and Rivest Shamir Adlemen.** Academic Press.   
<https://www.researchgate.net/profile/Israa-Barazanchi/publication/363691763_Proposed_system_for_data_security_in_distributed_computing_in_using_triple_data_encryption_standard_and_Rivest_Shamir_Adlemen/links/632f24b3694dbe4bf4b9db71/Proposed-system-for-data-security-in-distributed-computing-in-using-triple-data-encryption-standard-and-Rivest-Shamir-Adlemen.pdf>

“

## Objectives

The Objectives of our research on Cryptographic is to:

### Create a strong cryptographic foundation:

* Improve the security, scalability, and effectiveness of the encryption and decryption procedures.
* Examine the shortcomings of conventional cryptography techniques.

### Make use of cutting-edge strategies:

* Optimize performance by integrating hybrid algorithms.
* Make use of dynamic key management to improve security.

### Enhance efficiency:

* Prioritize quicker encryption, decryption, and key generation.
* Reduced computational overhead and good throughput are guaranteed.

### Assure cryptanalysis resilience:

* Create the framework to successfully fend off cryptographic attacks.

### Facilitate a variety of applications:

* Make secure data transfer possible for cloud computing.
* Pay attention to scalable solutions for the security of sensitive data and image encryption.

### Balancing Security and Performance for Practical Applications:

* Maintain strong protection while increasing processing speed for practical applications by striking a balance between security and efficiency. “

# METHODOLOGY

## Determine & Define Research Questions

**1.** **How can hybrid encryption methods improve the efficiency and security of key generation processes in large systems?**

**2. What are the key challenges in implementing cryptographic methods in real-world scenarios, and how can they be addressed?**

**3. How can shorter key lengths impact the overall security and efficiency of cryptographic systems?**

**4. What techniques can be used to enhance the scalability of cryptographic methods to handle large-scale data and high-resolution images?**

**5. How can energy consumption and implementation costs of cryptographic methods be minimized without compromising security and efficiency?**

**6. What strategies can be employed to protect cryptographic systems from modern cryptographic attacks, such as quantum attacks and cryptanalysis?**

## Select The Cases

**List all the cases (research papers) want to study:**

* + Case 1: HECC-AES-DH
  + Case 2: Image-based private key generation
  + Case 3: CASDC method
  + Case 4: 3DES-2KRSA hybrid

Table 3‑1 Summarization Of Cases

|  |  |  |  |
| --- | --- | --- | --- |
| Case | Method | Strengths | Deficiencies |
| Case 1 | Shorter keys, AES with DH key exchange | Faster key generation, increased speed | Scalability issues, unclear energy cost |
| Case 2 | Image-based private key generation | Novel approach, layered security | Unclear image sharing/storage, brute force gaps |
| Case 3 | XOR with RGB rotations | High security (100 years to break key) | Secret key reliance, practical challenges |
| Case 4 | Combines AES (fast) and RSA (secure) | Balanced efficiency and security | Scalability not well-tested |

## Data Collection & Analysis

**Case 1:**

Table 3‑2 Data Of Case 1(HECC-AES-DH)

|  |  |  |  |
| --- | --- | --- | --- |
| Test | Aspect | Results | Detail |
| Efficiency | Encryption Time | 0.00349s | - |
|  | Decryption Time | 0.002138s | - |
|  | Key Generation Time | 0.000025s | Key generation is faster than traditional methods, resulting in high data throughput. |
| Performance | Throughput | 693.10 KB/Sec | - |
| Scalability | Total Key Size | 807.625 bytes | Not work well with large systems where millions of users are involved. |
|  | Real world applications | Not perform tested in real world scenario | - |
| Security | Avalanche effect | Above 50% | Effective against brute force, but a shorter key is less secure for the future. |
| Challenge | Implementation | High Implementation cost and unclear energy efficiency | - |

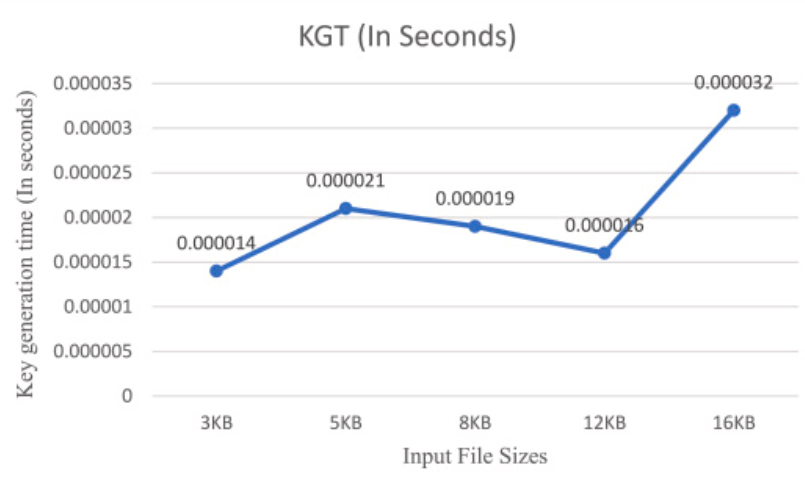
****

Figure 3‑1

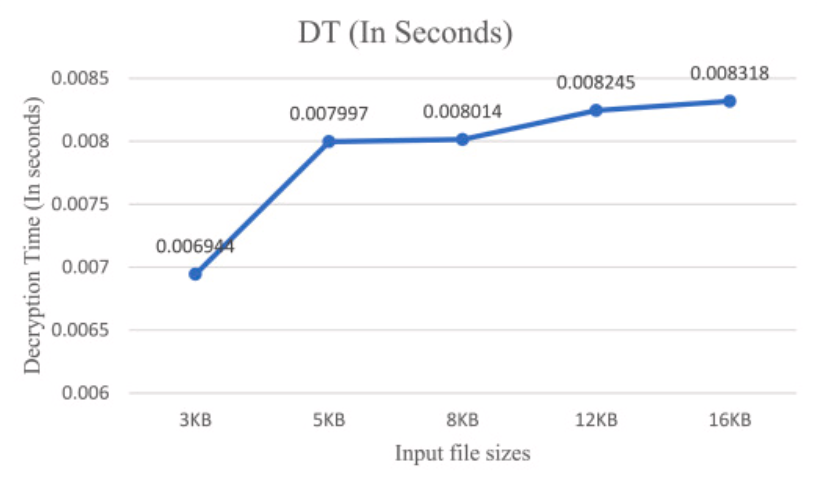
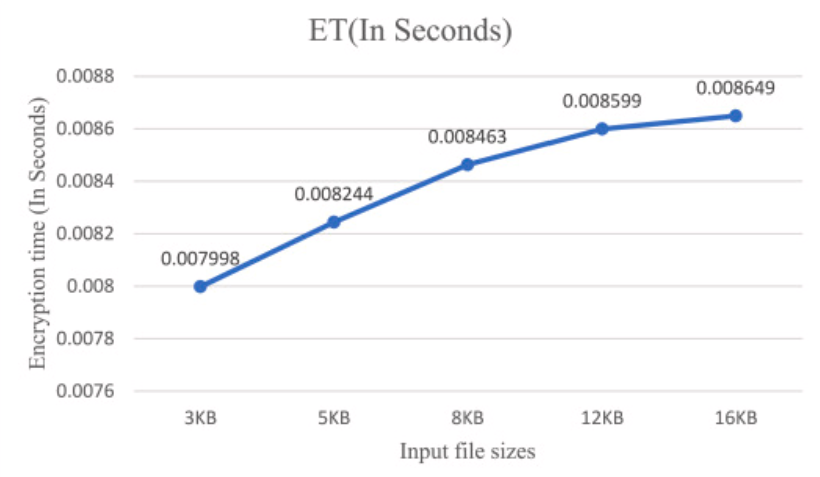
****

Figure ‑

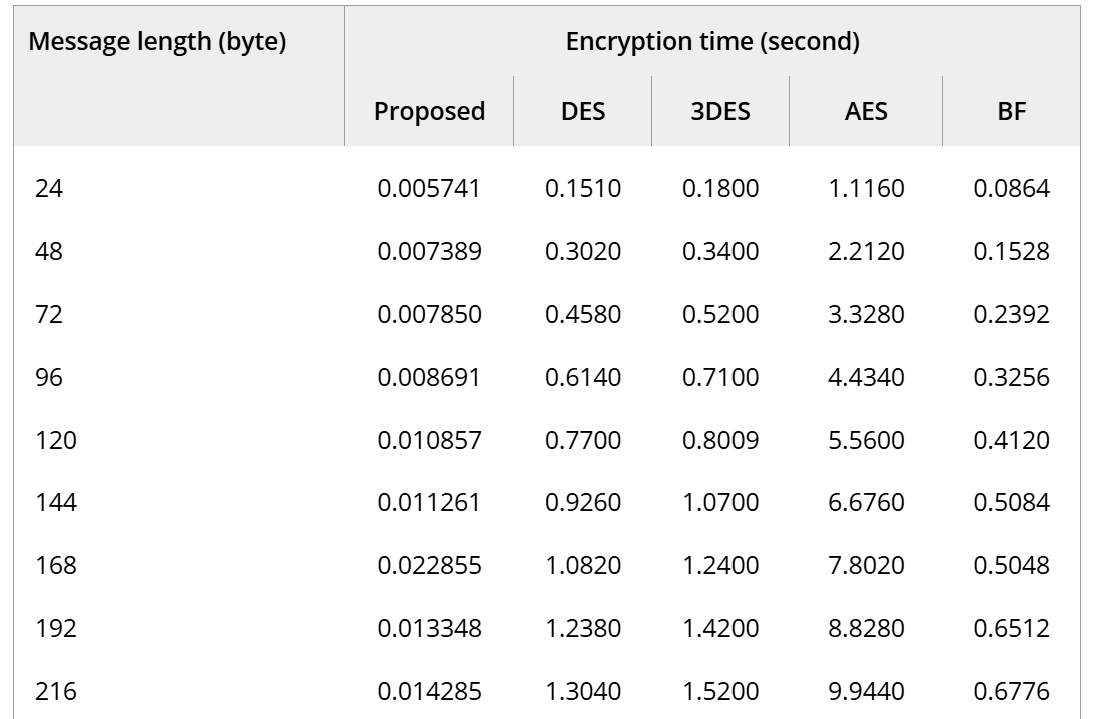
Figure ‑

Reference:  
Ranganatha Rao, B.Sujatha (October 2023). **A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security.** Academic Press.  
<https://www.sciencedirect.com/science/article/pii/S2665917423002064>  
 **Case 2:**

Table ‑ Data Of Case2 (Image Based Private Key Generation)

|  |  |  |  |
| --- | --- | --- | --- |
| **Test** | **Aspect** | **Results** | **Detail** |
| Efficiency | Encryption Time | Message of size 240 byte can be encrypted in only 0.015784 second | By comparing encryption time between the proposed method and standard method the proposed method is faster than standard method. |
| Performance | - | Not explain does perform well user communicate same time. | - |
| Scalability | Message Size | The method is effective for small and medium-sized messages or data stream, but does not perform well for large messages or data stream. | - |
| Security | Image Secure | Unclear image sharing/storage, brute force gaps | If a hacker gets the image, it can easily get the original text. |
| Challenge | Real world Application | Test in real world where image correction or difference devices might affect performance | - |

Table ‑ Encryption Time

****

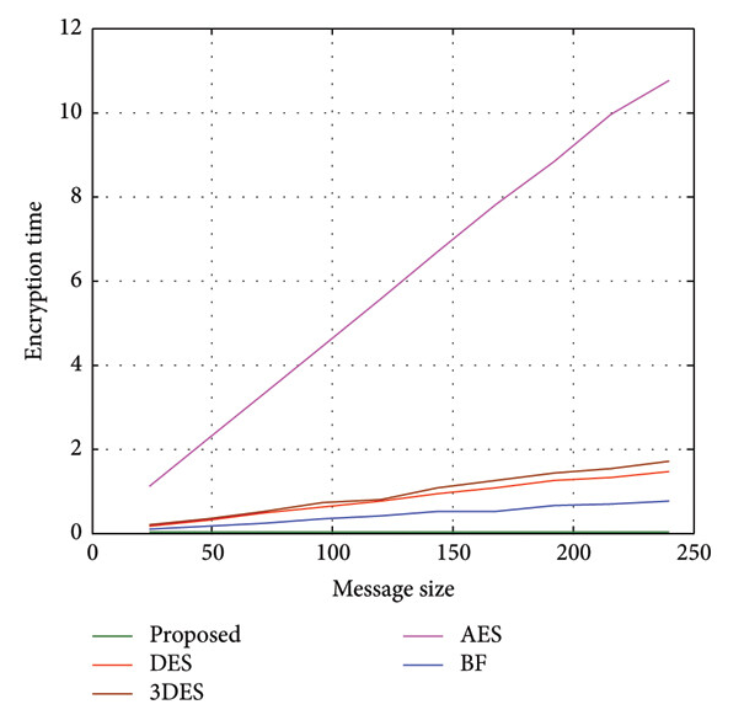
**Reference:**[Mohammad Subhi Al-Batah](https://onlinelibrary.wiley.com/authored-by/Al-Batah/Mohammad+Subhi), [Mowafaq Salem Alzboon](https://onlinelibrary.wiley.com/authored-by/Alzboon/Mowafaq+Salem), [Mazen Alzyoud](https://onlinelibrary.wiley.com/authored-by/Alzyoud/Mazen), [Najah Al-Shanableh](https://onlinelibrary.wiley.com/authored-by/Al-Shanableh/Najah) (July 2024). **Enhancing Image Cryptography Performance with Block Left Rotation Operations.** Academic Press.<https://onlinelibrary.wiley.com/doi/full/10.1155/2024/3641927>

Figure 3‑4 Encryption Time Comparison

**CASE 3:**

Table ‑ Data Of case 3

|  |  |
| --- | --- |
| **Aspect** | **Result** |
| Efficiency | “Average penetration (hacking) time per attempt = 509.6630 sec. Total number of attempts = 79 = 40353607.  Hacking time (best case) =(40353607×509.6630) sec. =(40353607×509.6630)/(60×60×24×365.25) years. = **651.7207 years**.” |
| Throughput | The method provide good throughput was equal to 3237.2 byte per second. |
| Scalability | Image Quality Degrade |
| Security | More secure because special key that are used to generate three value for each the three channel |

Table ‑ Throughput Summary

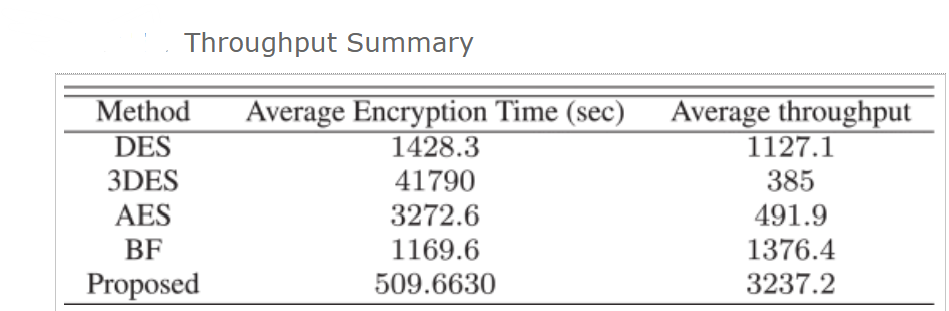
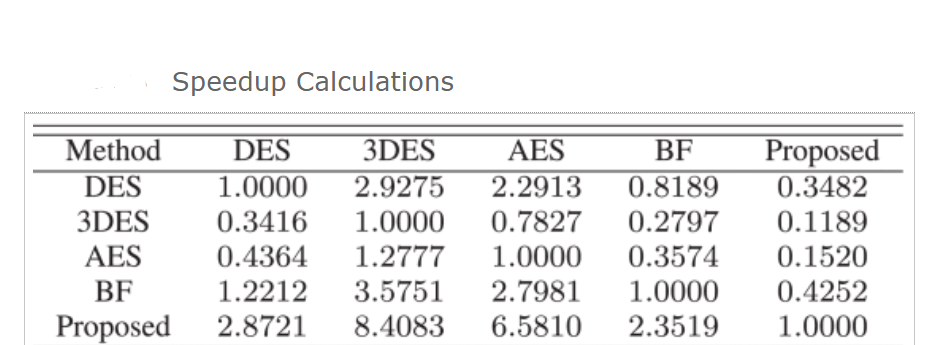
****

Table 3‑7 Speed Calculations

****

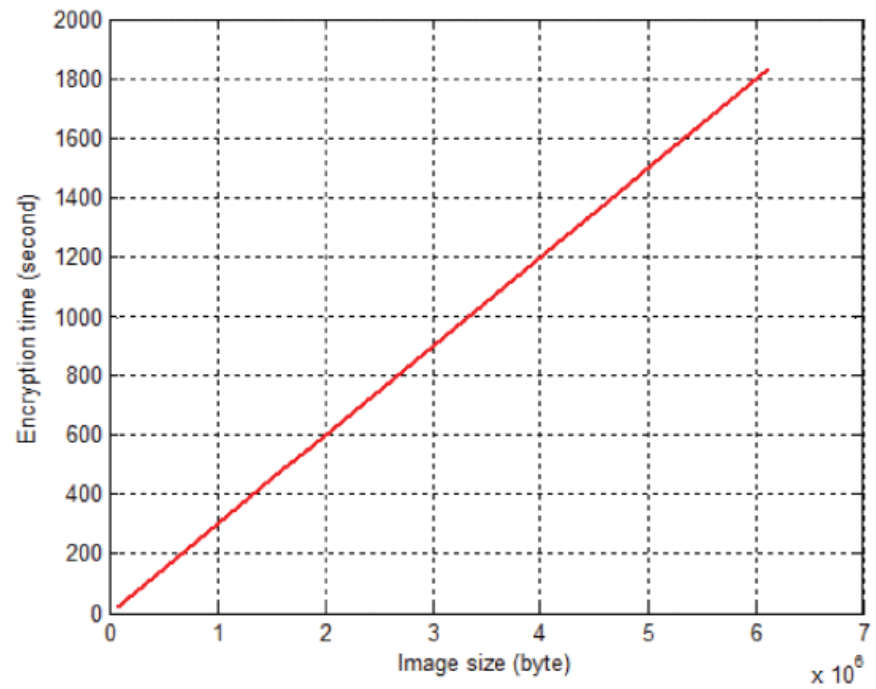
****

Figure ‑ Encryption Time and Image size

**Reference:**Mua’ad Abu-Faraj, Abeer Al-Hyari, Ziad Alqadi (2024). **CASDC: A Cryptographically Secure Data System Based on Two Private Key Images.** Academic Press.   
<https://ieeexplore.ieee.org/abstract/document/9968243>

**Case 4**

Table ‑ Data Of Case 4

|  |  |
| --- | --- |
| **Aspect** | **Result** |
| Efficiency | 3DES ensures fast encryption; 3KRSA is slower for key exchange. |
| Scalability | Limited scalability for large datasets; not tested on distributed systems. |
| Security | Strong resistance to brute force; quantum security depends on 3KRSA key size. |

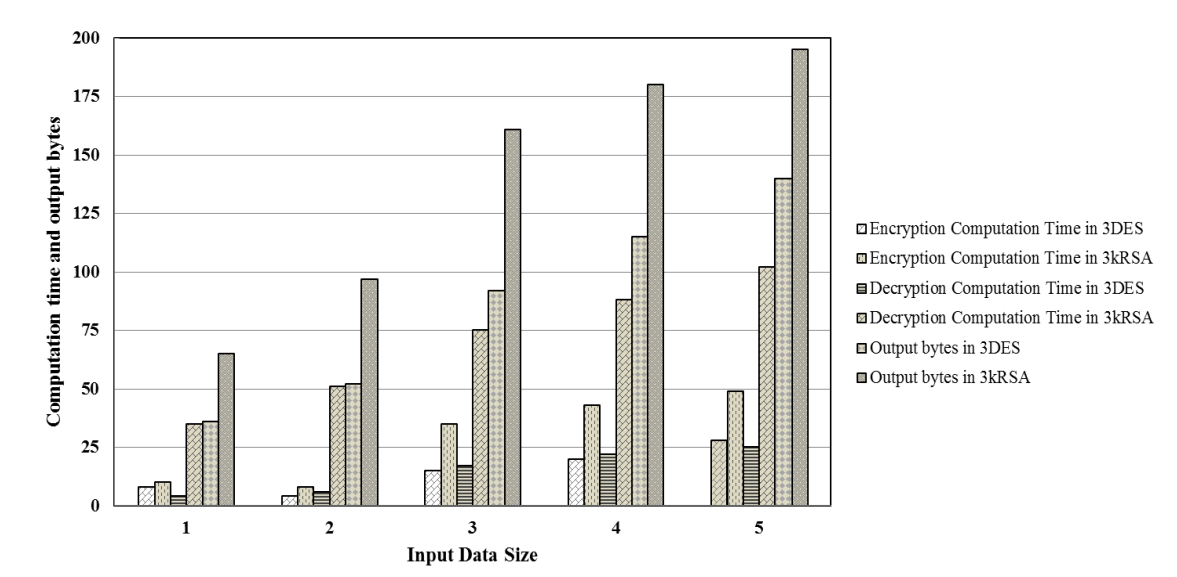
****

Figure ‑ 3DES and 3KRSA Computation Time of Encryption Decryption and Output Bytes

**Reference:**[Shihab A. Shawkat](https://www.researchgate.net/profile/Shihab-Shawkat?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19), [Bilal A. Tuama](https://www.researchgate.net/scientific-contributions/Bilal-A-Tuama-2231102443?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19), [Israa Al Barazanchi](https://www.researchgate.net/profile/Israa-Barazanchi) (2022). **Proposed system for data security in distributed computing in using triple data encryption standard and Rivest Shamir Adlemen.** Academic Press.   
<https://www.researchgate.net/profile/Israa-Barazanchi/publication/363691763_Proposed_system_for_data_security_in_distributed_computing_in_using_triple_data_encryption_standard_and_Rivest_Shamir_Adlemen/links/632f24b3694dbe4bf4b9db71/Proposed-system-for-data-security-in-distributed-computing-in-using-triple-data-encryption-standard-and-Rivest-Shamir-Adlemen.pdf>

# RESULTS&DISCUSSION

### Report: Enhancing Efficiency and Scalability in Cryptographic Methods

“ Enhancing cryptographic techniques for increasing security, scalability, and efficiency is the main and primary goal of this paper. In order to satisfy the requirements of modern data systems, the research investigates interesting approaches such as hybrid encryption, dynamic key management, and shorter keys by discussing important issues.6 key research question serves as the soul for the methodological structure and offer a framework for analysis and solution development”.

#### Increasing/Improving Efficiency and Security in Key Generation:

* “How in big systems key generations be made more secure and efficient by using hybrid encryption techniques Point of view(pov):
  + Hybrid encryption i.e. RSA (for secure key exchange),AES (for bulk data) mixes symmetric and asymmetric techniques.
  + elliptical curves also other shorter keys increases performance without crucially sacrificing security.
  + Dynamic key management assures flexibility and reduces the possibility of key theft”.

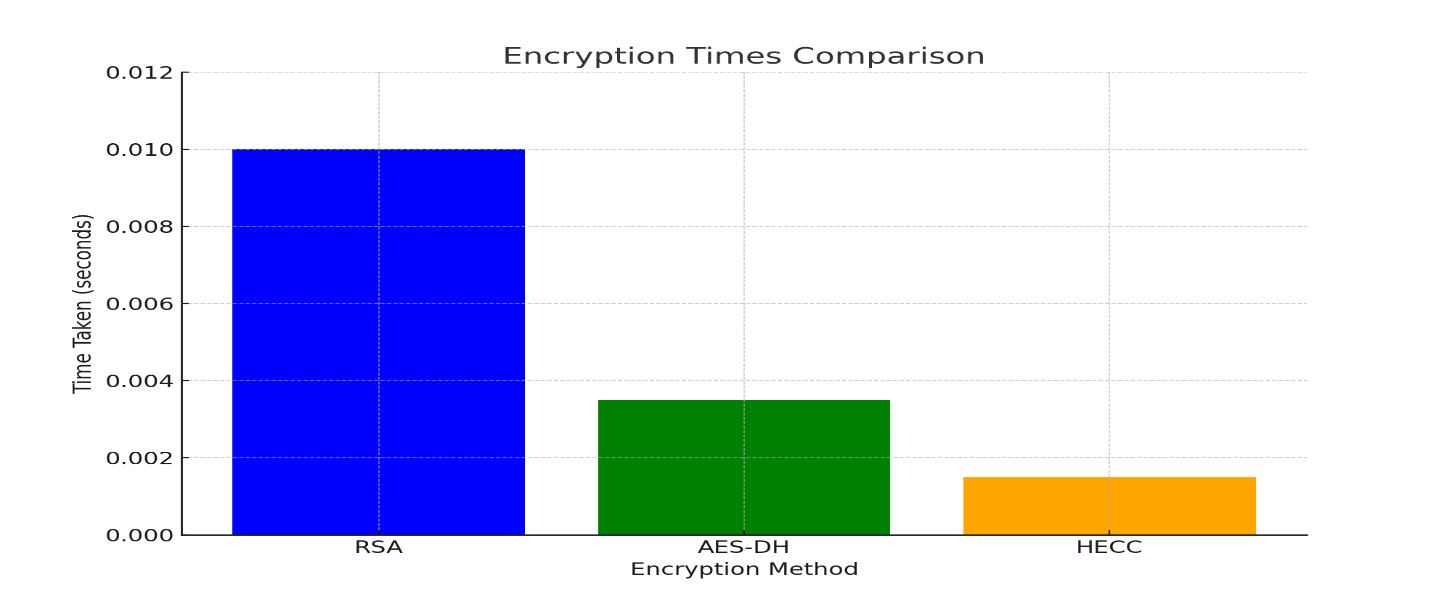
**“Graphical Illustration:”**

Figure ‑ Encryption Time Comparison

#### Moving on to Real-World Cryptographic Challenges:

* “ What are the main hurdles to apply cryptographic techniques in practical settings and how may they be control  
  **Challenges:**   
  • Broad-scale cloud system scalability, manageability.   
  • Safe n secure key management and sharing.   
  • Resource n assets limitations and energy efficiency.   
  **Answers:**   
  Distributed key management systems should be used.   
  Perform, manage practical testing in multiple variations of settings.   
  For low end devices maximize computational productivity. “

**“Graphical Illustration:**

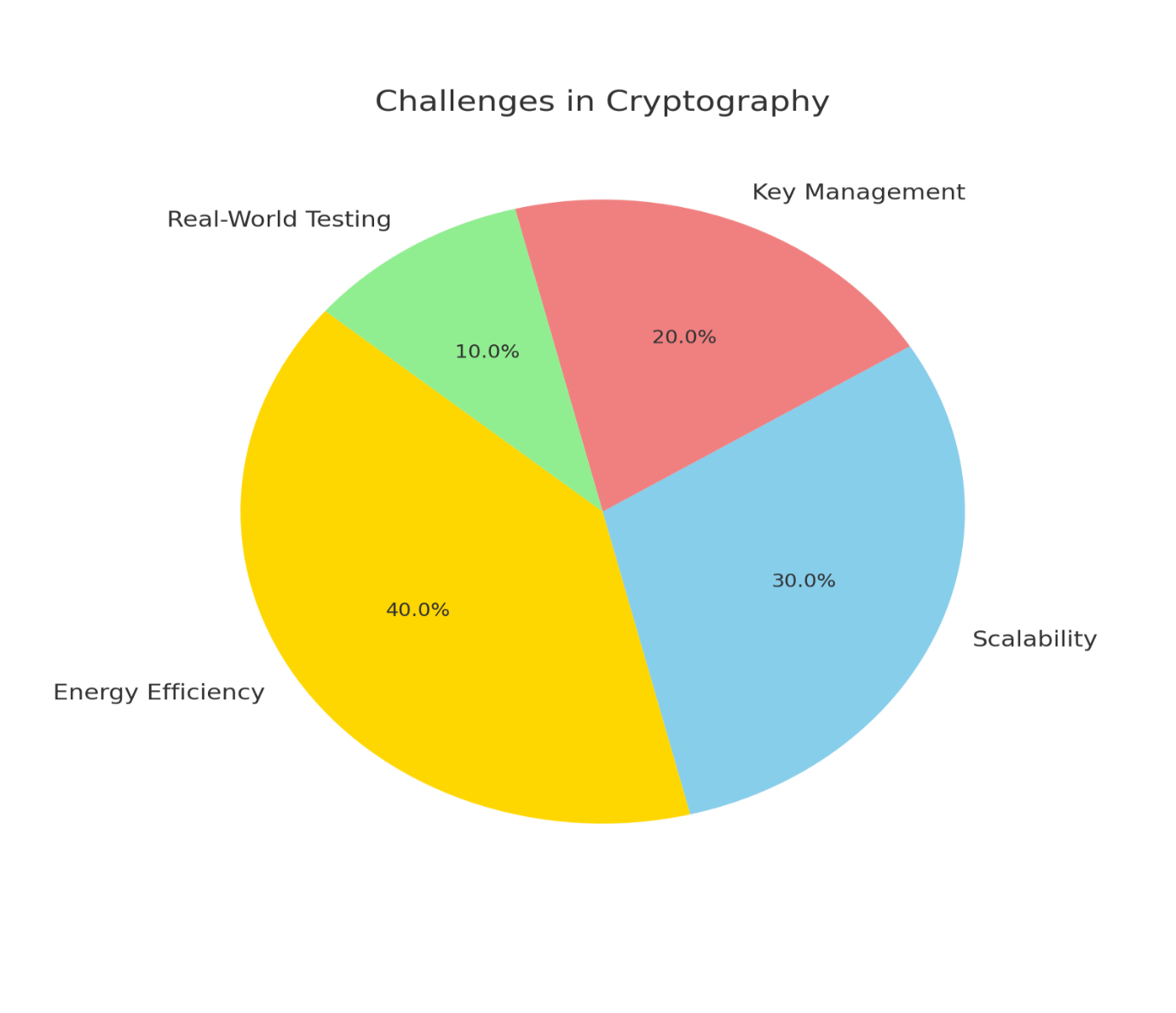
****

Figure ‑ Changes in Cryptography”

#### Inspecting Trade-Offs for Key Length:

* “What effects might lower key lengths have on the general productiveness and security of cryptographic systems”  
  “Point of view(pov):   
  • Despite the fact that shorter keys (like HECC) enhance throughput and speed they may be unsafe to quantum assault in the future.   
  • Post-quantum cryptography uses algorithms that are resistant to the dangers of quantum computing hence assures security”.

**“Graphical Illustration:**

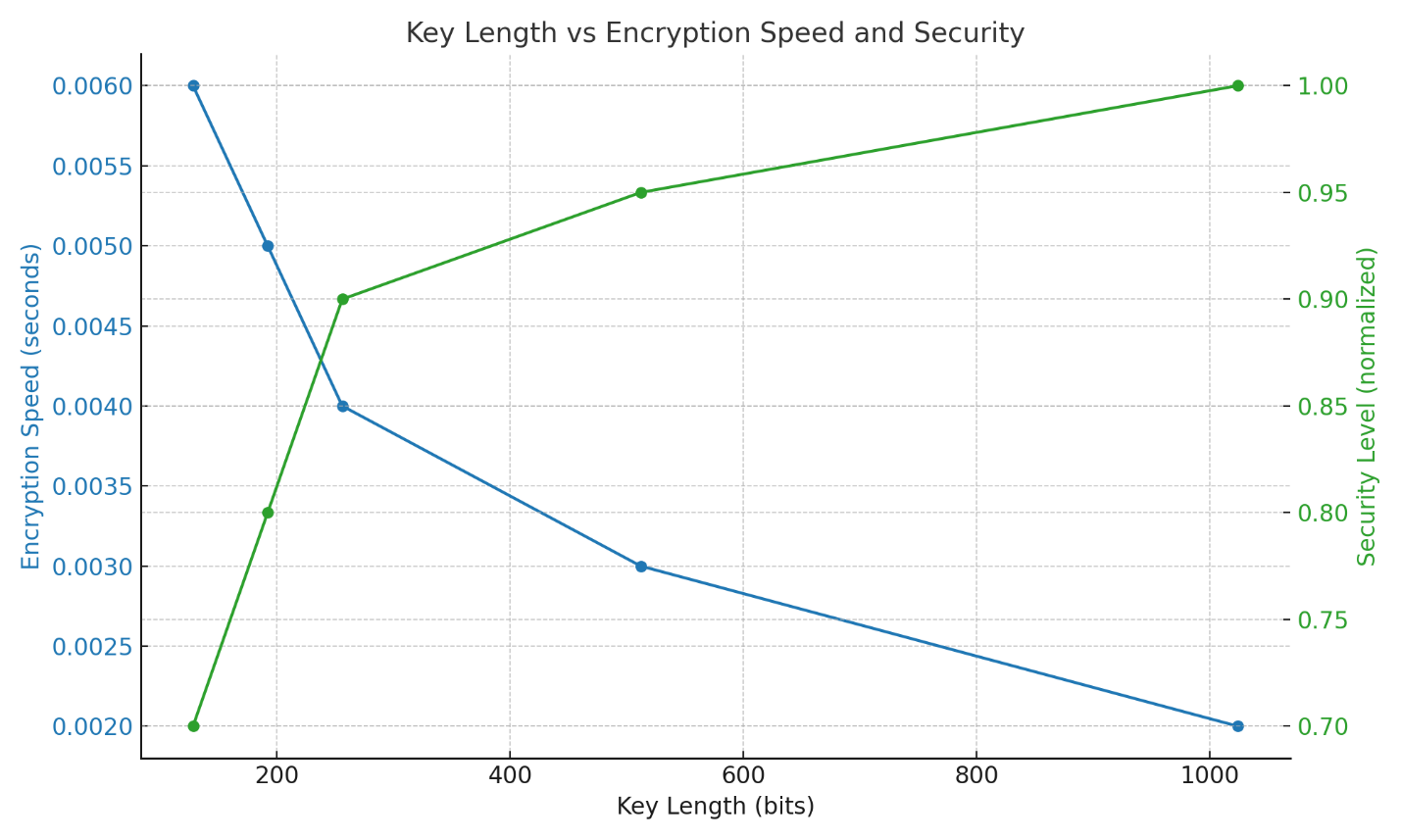
****”

Figure ‑ Key Length vs Speed and Security

#### Enhancing Scalability for Big Data:

* “ How can cryptographic advances be made more adjustable, approachable to handle high resolution photos and enormous amounts of data? “  
  **“Techniques:**   
  • To operate data in parallel also divide it into smaller units.   
  • For immense files use RGB based picture encryption.   
  • Flexible scalability in terms of dynamic key management. “

**“Graphical Illustration:**

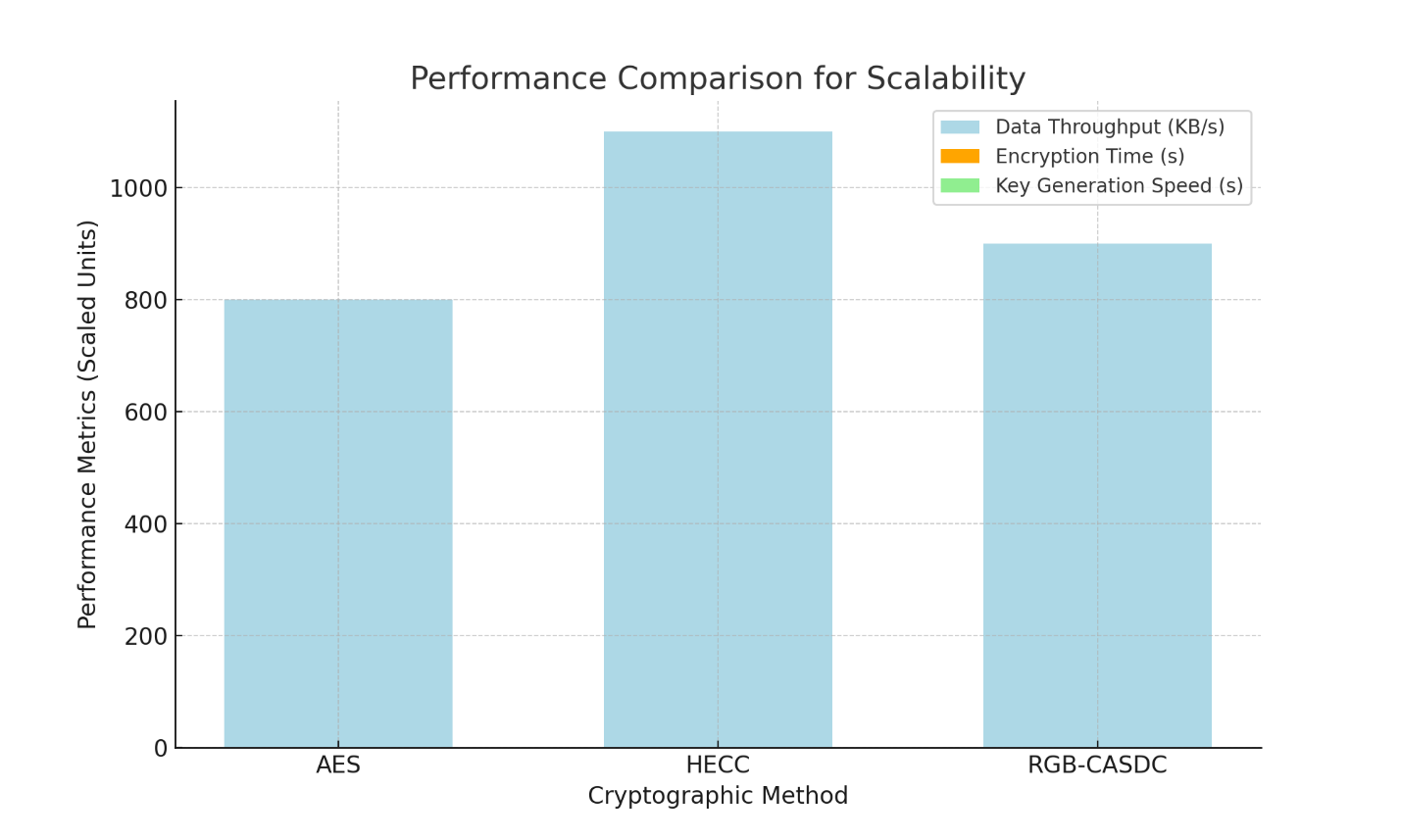
****”

Figure ‑ Performance Comparison for Scalability

#### Minimizing Implementation and Execution Expenses and Energy Use:

* “ What a cryptographic techniques energy usage, execution and implementation expenses be reduced without giving up or sacrificing effectiveness and security?”  
  **“Answers:**   
  • Utilize energy saving techniques i.e. AES and ECC.   
  • For IOT related devices use lightweight cryptography.   
  With effective usage of hybrid methodologies computational expenses can be decreased.”

**“Graphical Illustration:**

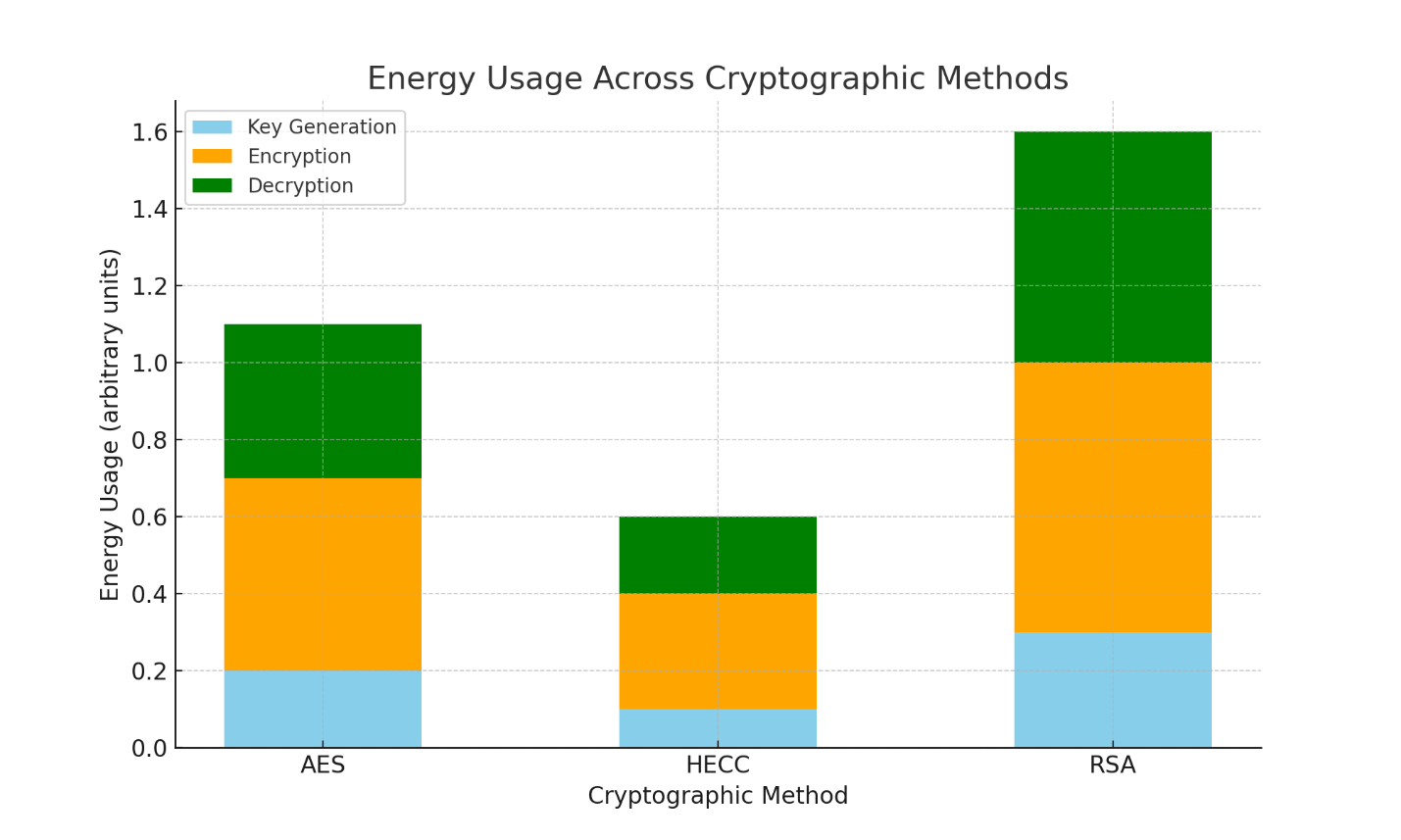
“****

Figure ‑ Energy Usage Across Cryptographic Methods”

“

#### Protecting Against Modern Attacks:

* “What kind of strategies must be used to guard cryptographic systems from modern attacks like cryptanalysis and quantum attack? “

**“ Strategies:**• To cope against quantum attacks and employ post quantum cryptography.   
• To cope off side channel, brute force assaults and use numerous encryption levels.   
• With time evolve, update and improve algorithms to keep up with new threats. “

**“Graphical Illustration:**

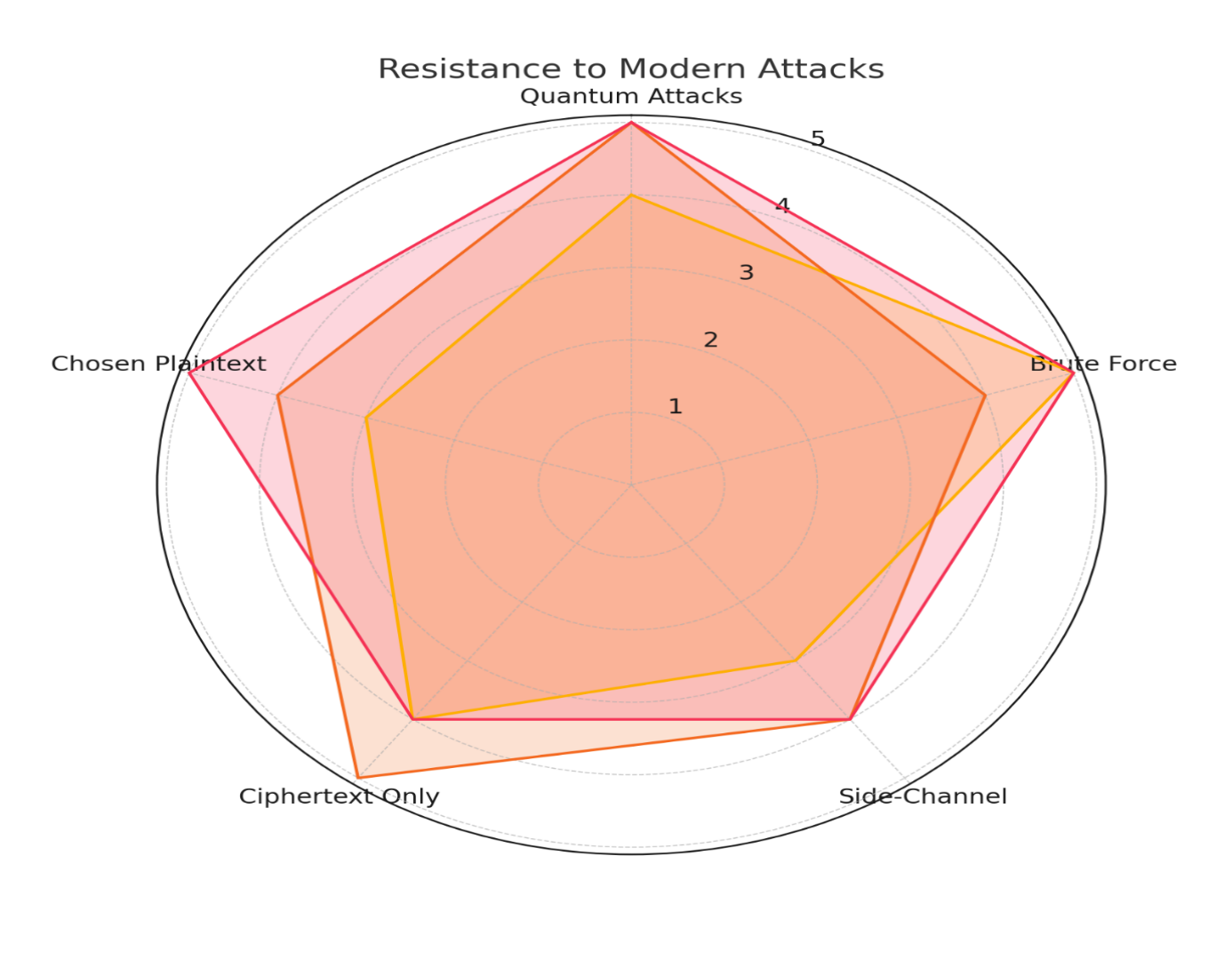
****”

Figure ‑ Resistance to modern attacks

### DISCUSSION:

“The study highlights updates, advancements and upgrades in cryptographic methods to improve efficiency, scalability and security. Hybrid techniques i.e. AES-DH and HECC enhances encryption speed, agility and key generation also addressing scalability for huge and enormous datasets using variety of techniques like data partitioning and RGB based encryption. Energy efficient algos i.e. ECC decreases costs, making cryptography satisfactory for IoT devices. As well as techniques like post quantum cryptography, layered encryption strength against upcoming and rising threats also including quantum and brute force attacks.” “ While the discovery show notable improvements also further research is to be carried in terms of addressing real world scalability, quantum vulnerabilities and large-scale implementation challenges.”

# CONCLUSION

“In conclusion this document illustrates that enhancing, updating and improving cryptographic methods with time using strategies i.e. hybrid encryption, dynamic key management and energy efficient algorithms can remarkably improve both security and performance. The incorporation of scalable methods for large datasets and the acquisition of post-quantum cryptography positions these methods to tackle modern and future threats. While the suggested solution promises more distant study into real world applications, huge scale systems and quantum resistance is important to fully enhance and improve cryptographic techniques for the evolving digital landscape. The advancement presented tops the pathway for more secure, efficient and scalable data privacy techniques in diverse industries. “

# REFERENCES

Ranganatha Rao, B.Sujatha (October 2023). **A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security.** Academic Press.  
<https://www.sciencedirect.com/science/article/pii/S2665917423002064>

[Mohammad Subhi Al-Batah](https://onlinelibrary.wiley.com/authored-by/Al-Batah/Mohammad+Subhi), [Mowafaq Salem Alzboon](https://onlinelibrary.wiley.com/authored-by/Alzboon/Mowafaq+Salem), [Mazen Alzyoud](https://onlinelibrary.wiley.com/authored-by/Alzyoud/Mazen), [Najah Al-Shanableh](https://onlinelibrary.wiley.com/authored-by/Al-Shanableh/Najah) (July 2024). **Enhancing Image Cryptography Performance with Block Left Rotation Operations.** Academic Press.<https://onlinelibrary.wiley.com/doi/full/10.1155/2024/3641927>

Mua’ad Abu-Faraj, Abeer Al-Hyari, Ziad Alqadi (2022). **A Complex Matrix Private Key to Enhance the Security Level of Image Cryptography.** Academic Press.<https://www.mdpi.com/2073-8994/14/4/664>

Mua’ad Abu-Faraj, Abeer Al-Hyari, Ziad Alqadi (2024). **CASDC: A Cryptographically Secure Data System Based on Two Private Key Images.** Academic Press.   
<https://ieeexplore.ieee.org/abstract/document/9968243>

[Shihab A. Shawkat](https://www.researchgate.net/profile/Shihab-Shawkat?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19), [Bilal A. Tuama](https://www.researchgate.net/scientific-contributions/Bilal-A-Tuama-2231102443?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19), [Israa Al Barazanchi](https://www.researchgate.net/profile/Israa-Barazanchi) (2022). **Proposed system for data security in distributed computing in using triple data encryption standard and Rivest Shamir Adlemen.** Academic Press.   
<https://www.researchgate.net/profile/Israa-Barazanchi/publication/363691763_Proposed_system_for_data_security_in_distributed_computing_in_using_triple_data_encryption_standard_and_Rivest_Shamir_Adlemen/links/632f24b3694dbe4bf4b9db71/Proposed-system-for-data-security-in-distributed-computing-in-using-triple-data-encryption-standard-and-Rivest-Shamir-Adlemen.pdf>

[Mua’ad Abu-Faraj](https://www.researchgate.net/profile/Muaad-Abu-Faraj?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19), [Ziad A.A Al Qadi](https://www.researchgate.net/profile/Ziad-Al-Qadi?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19). **Improving the Efficiency and Scalability of Standard Methods for Data Cryptography.** Academic Press.  
<https://www.researchgate.net/publication/357240780_Improving_the_Efficiency_and_Scalability_of_Standard_Methods_for_Data_Cryptography>

IBM. (5 January 2024). **A brief history of cryptography: Sending secret messages throughout time.**<https://www.bing.com/ck/a?!&&p=d1219b20fde6e23f0533a32e96b43004c454b0d76aaa6186b825f342a304c10cJmltdHM9MTczMzE4NDAwMA&ptn=3&ver=2&hsh=4&fclid=259a9afd-4530-6fbb-0cfc-8fed44246e04&psq=https%3a%2f%2fwww.ibm.com%2fthink%2ftopics%2fcryptography-history%3fform%3dMG0AV3&u=a1aHR0cHM6Ly93d3cuaWJtLmNvbS90aGluay90b3BpY3MvY3J5cHRvZ3JhcGh5LWhpc3Rvcnk&ntb=1>

[By Jeff Delaney](https://fireship.io/contributors/jeff-delaney/) (28 October 2021). **Cryptographical Concept Of Node.js Developer.**  
https://www.bing.com/ck/a?!&&p=66ebf6d0b1217a5af03faa062e77a313f030627e24d1c37c5e8a91d3b5b9115bJmltdHM9MTczMzE4NDAwMA&ptn=3&ver=2&hsh=4&fclid=259a9afd-4530-6fbb-0cfc-8fed44246e04&psq=https%3a%2f%2ffireship.io%2flessons%2fnode-crypto-examples%2f&u=a1aHR0cHM6Ly9maXJlc2hpcC5pby9sZXNzb25zL25vZGUtY3J5cHRvLWV4YW1wbGVzLw&ntb=1