Image Encryption and Decryption

Anoop BR[1], Prof. Swetha C S[2]

[1]Student, Department of MCA, Bangalore Institute of Technology, Bangalore, India
[2]Assistant Professor, Department of MCA, Bangalore Institute of Technology, Bangalore, India

---***---

ABSTRACT

In the digital age of today, organizations look up to secure, scalable, and efficient encryption techniques ensuring the protection of multimedia data and confidential communication. This paper offers a comparative study on symmetric cryptographic algorithms—DES, AES, and Blowfish—evaluated for their performance in image encryption and decryption. The analysis considers key size, rounds, encryption/ decryption speed, and overall security, demonstrating how these algorithms safeguard image data from unauthorized access. Experimental surveys highlight the strengths of AES in robustness, Blowfish in speed and flexibility, and DES in legacy use, but with vulnerabilities. The system-level evaluation provides insights into how cryptographic algorithms can be applied in real-world applications such as military communication, medical imaging, and secure internet transmission. Overall, the study demonstrates the critical role of encryption algorithms in enhancing confidentiality, maintaining integrity, and enabling secure multimedia communication—making it appropriate for environments seeking modernized image security frameworks.Overall, the solution demonstrates the power of Blowfish as a secure and performance-optimized algorithm—making it appropriate for systems seeking modernized encryption capabilities

1. INTRODUCTION

In the era of digital communication, where multimedia data such as images are transmitted and stored extensively, security has emerged as a critical concern. Images often carry sensitive information in domains such as medical imaging, defense intelligence, financial systems, and personal communications. If intercepted or manipulated, such data can lead to privacy violations, strategic disadvantages, or misuse of confidential records. Hence, encryption of images has become an indispensable requirement to ensure confidentiality, integrity.

Traditional cryptographic methods like the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) have been widely used in securing digital communication. DES, though historically significant, suffers from vulnerabilities due to its limited key size, making it prone to brute-force attacks. AES, on the other hand, offers higher security levels with larger key sizes and widespread adoption in modern applications. However, both algorithms pose challenges when dealing with large-scale multimedia content, where performance, processing speed, and adaptability become crucial .Blowfish, designed by Bruce Schneier, has emerged as a fast and efficient alternative. It is a symmetric block cipher employing a 64-bit Feistel structure and variable key sizes ranging from 32 to 448 bits. Its design simplicity, license-free usage, and resistance to known cryptanalytic attacks make it a compelling choice for secure image encryption. Furthermore, Blowfish is particularly suitable for environments where keys do not change frequently, and high-speed encryption is required. Its computational efficiency, especially on 32-bit microprocessors, makes it competitive with and often faster than AES and DES .Recent research emphasizes both theoretical evaluation and practical implementation of cryptographic algorithms for images. Comparative studies show the advantages and drawbacks of DES, AES, and Blowfish, while implementation-based work in MATLAB highlights the practical feasibility of Blowfish for encrypting grayscale and color images across multiple formats. The combination of performance analysis and real-world implementation underscores the importance of selecting algorithms that balance speed, security, and adaptability.Overall, this research focuses on consolidating a review of symmetric key algorithms with an applied study of Blowfish in MATLAB. It highlights the strengths and weaknesses of the leading cryptographic techniques and demonstrates how Blowfish provides a practical and secure solution for real-time image encryption and decryption in modern multimedia systems.

Beyond conventional text encryption, image encryption introduces unique challenges due to the larger data size, pixel correlation, and redundancy within image structures. Unlike plain text, where bit changes are easily distributed, images require specialized handling to ensure that encrypted outputs are statistically unrecognizable from the original data. Cryptographic strength is measured not only by resistance to brute-force and differential attacks but also by statistical analysis of histograms, correlation coefficients, and entropy. For this reason, image encryption demands algorithms that deliver both computational efficiency and strong statistical security measures
.

In the broader context of secure communication, several approaches have been studied that combine traditional symmetric cryptography with advanced techniques such as permutation methods, biometric-based key generation, and hybrid models. Studies show that algorithms like the Hyper Image Encryption Algorithm (HIEA), Hill Cipher modifications, and elliptic curve cryptography offer enhancements in reliability and robustness. However, the complexity of these models often increases computational overhead, making them less feasible for real-time or resource-constrained systems. Against this background, Blowfish strikes a balance between security and performance, offering modularity, adaptability, and feasibility for large-scale image processing

. Practical implementations reinforce the theoretical advantages of Blowfish. Simulation in MATLAB demonstrates how images of different formats—such as BMP, JPEG, PNG, and TIFF—can be encrypted and decrypted with minimal computational delay, while preserving the fidelity of the original image upon decryption.

2. RELATED WORK

• Over the years, numerous researchers have contributed to the development and analysis of cryptographic techniques for securing digital images. Early work on the Data Encryption Standard (DES) established a foundation for symmetric encryption, but its limited key size and vulnerability to brute-force attacks highlighted the need for more advanced techniques. The Advanced Encryption Standard (AES) was introduced as a successor, offering higher flexibility with key sizes of 128, 192, and 256 bits. AES has since been widely adopted for its robustness and efficiency in both hardware and software implementations. Comparative studies indicate that while AES offers strong security guarantees, the computational demand for multimedia data can be significant .Blowfish, introduced by Bruce Schneier in 1993, has gained attention as a fast, free, and secure alternative to DES. It employs a 64-bit block size and supports variable key lengths ranging from 32 to 448 bits. Unlike DES, Blowfish was designed for efficient software implementation and demonstrates strong resistance against known cryptanalytic attacks.

• Several studies have also focused on specialized image encryption methods beyond traditional cryptographic standards. Techniques such as the Hyper Image Encryption Algorithm (HIEA), advanced Hill cipher models, and hybrid cryptographic protocols combining RSA, ECC, and hash functions have been introduced to address challenges in image security. These models improve aspects like robustness, authentication, and integrity, but often at the cost of increased algorithmic complexity and execution time. In contrast, Blowfish remains notable for maintaining a balance between strong encryption and computational efficiency, making it suitable for real-time scenarios where performance is critical

. Practical implementations of Blowfish for image encryption further validate its efficiency. MATLAB-based experiments demonstrate how both grayscale and color images of multiple formats can be encrypted and decrypted with minimal processing delay. The results show that encrypted images have randomized histograms, making them resistant to statistical analysis, while decrypted images retain complete fidelity with the originals. Studies confirm that Blowfish's 16-round Feistel network structure provides high diffusion and confusion, ensuring that even small changes in input keys or plaintext result in significantly different ciphertext outputs. These outcomes reinforce Blowfish's viability as a strong candidate for secure multimedia communication

.

Researchers have also explored comparative frameworks to benchmark the performance of DES, AES, and Blowfish across multiple parameters such as key size, number of rounds, encryption speed, and decryption efficiency. Results consistently indicate that DES is outdated and insecure for modern applications, while AES provides high security but at the cost of processing overhead. Blowfish, in contrast, emerges as highly competitive, demonstrating faster encryption times and flexibility in key size, which allows users to adapt the algorithm based on their performance and security requirements. This adaptability makes Blowfish particularly useful in scenarios where both speed and confidentiality are paramount .

In addition to theoretical studies, several experimental implementations have reinforced Blowfish's relevance. For example, MATLAB-based simulations show that the algorithm efficiently encrypts large datasets of images without compromising quality upon decryption. Histogram analysis of encrypted images reveals that Blowfish successfully disperses pixel intensity values, resulting in encrypted outputs with minimal resemblance to the original image. This transformation protects against statistical attacks, ensuring that unauthorized entities cannot derive meaningful insights from the cipher image. Such findings validate Blowfish as a practical solution for multimedia systems that demand a tradeoff between simplicity and security.

3. PROBLEM STATEMENT

The rapid growth of multimedia applications and digital communication has made image security a pressing challenge. While text-based encryption has been extensively studied and standardized, images pose additional complexities due to their size, redundancy, and pixel correlation.

Blowfish emerges as a potential candidate to address these challenges, but its practical performance in real-world applications must be evaluated. While theoretical studies highlight its advantages in speed, variable key length, and resistance to cryptanalysis, there is limited integration of comparative analysis and experimental implementation. Existing research often isolates comparative reviews of DES, AES, and Blowfish from practical system-level demonstrations, such as MATLAB-based encryption and decryption of images. This separation prevents a holistic understanding of how Blowfish can outperform or complement existing standards when applied in modern multimedia environments.

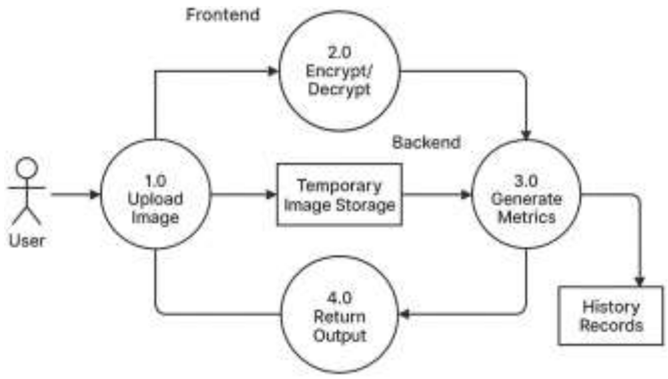
Therefore, the problem addressed in this research is the identification and validation of an encryption algorithm that provides a strong balance between security, adaptability, and computational efficiency for image data.

4. PROPOSED SYSTEM

The proposed system focuses on combining a comparative review of symmetric key algorithms—DES, AES, and Blowfish—with a practical implementation of Blowfish in MATLAB for secure image encryption and decryption. The design leverages the theoretical strengths of AES and Blowfish while identifying the weaknesses of DES, thereby positioning Blowfish as an efficient and adaptable solution for real-time multimedia applications. The system is structured to analyze the performance of these algorithms against factors such as encryption and decryption speed, key size flexibility, robustness against attacks, and suitability for handling large-scale image data.

At the core of the proposed system lies the Blowfish algorithm. Blowfish operates as a symmetric block cipher with a 64-bit block size and supports variable key lengths up to 448 bits. It utilizes a 16-round Feistel network, where operations such as permutation, substitution, XOR, and modular addition are iteratively applied to achieve diffusion and confusion. In the MATLAB-based implementation, the system reads an input image, processes it into pixel matrices, and applies Blowfish encryption to generate cipher images.

The system architecture is designed to support different image formats including BMP, PNG, JPEG, and TIFF, as well as both grayscale and color images. Histogram analysis of encrypted outputs validates the randomness introduced by Blowfish, ensuring that the cipher images bear no statistical resemblance to the original. Furthermore, correlation analysis of adjacent pixels and entropy measurements confirm the robustness of the encryption process. By integrating MATLAB simulations with theoretical comparisons of AES and DES, the proposed system bridges the gap between abstract cryptographic analysis and practical multimedia implementation. In addition, the system emphasizes scalability and adaptability for real-world use cases. For high-security applications such as defense communication, telemedicine.



5. METHODOLOGY

Algorithm Selection and Analysis

The first phase involves identifying and studying the most widely used symmetric key cryptographic algorithms—DES, AES, and Blowfish. DES, although historically significant, is analyzed for its limitations, such as its small 56-bit key size and vulnerability to brute-force attacks.AES is studied for its robustness and support for multiple key sizes (128, 192, 256 bits), making it highly secure but computationally demanding for multimedia data. Blowfish is examined for its unique features, including a variable key length of 32–448 bits, a 64-bit block size, and efficiency in software implementation.

System Design

The proposed system is designed around the Blowfish algorithm's Feistel structure, which applies 16 iterative rounds of encryption to ensure diffusion and confusion. The system architecture separates image header information from pixel data to maintain compatibility with standard image formats. Only the pixel matrix is encrypted, while the image header remains unchanged, ensuring the encrypted output retains the structure of the original file. This design supports multiple image formats such as BMP, PNG, JPEG, and TIFF, as well as both grayscale and color images. The modular design also ensures that the system can be extended to analyze other encryption algorithms in the future.

Implementation Process

- Image Input and Preprocessing:
  The process begins by selecting an input image (grayscale or color) and loading it into MATLAB. The image is then converted into a pixel matrix, ensuring compatibility with the block-based structure of the Blowfish algorithm.

- Block Division and Key Preparation:
  The pixel matrix is divided into 64-bit blocks, consistent with the Blowfish block size. A secret key of variable length (ranging from 32 to 448 bits) is chosen, and subkeys are generated during the initialization phase.

- Encryption Phase:
  Each 64-bit block undergoes 16 rounds of the Feistel network operations, including substitution, permutation, XOR, and modular addition. This transforms the plain pixel values into encrypted cipher values, ensuring diffusion and confusion.

- Decryption Phase:
  To recover the original image, the same secret key is applied, but the subkeys are used in reverse order. This ensures lossless reconstruction of the image, maintaining identical quality between the decrypted and original versions.

- Output Generation and Validation
  The system produces three outputs: the original image, the encrypted image, and the decrypted image. Histogram analysis of the encrypted image is performed to confirm statistical randomness, while a visual comparison verifies the accuracy of the decryption process.

Evaluation Metrics

The evaluation of the proposed system relies on several performance-oriented and security-oriented metrics that provide a holistic understanding of how encryption algorithms behave with image data. The first key metric is encryption and decryption time, which directly impacts the feasibility of real-time applications. Blowfish consistently demonstrates faster processing speeds compared to DES, largely due to its efficient Feistel structure and flexible key size design. AES also performs strongly but tends to consume more computational resources, particularly when applied to large image datasets. By comparing encryption and decryption times across these algorithms, it becomes evident that Blowfish provides an optimal balance between performance and security, making it a reliable choice for systems requiring quick response times.

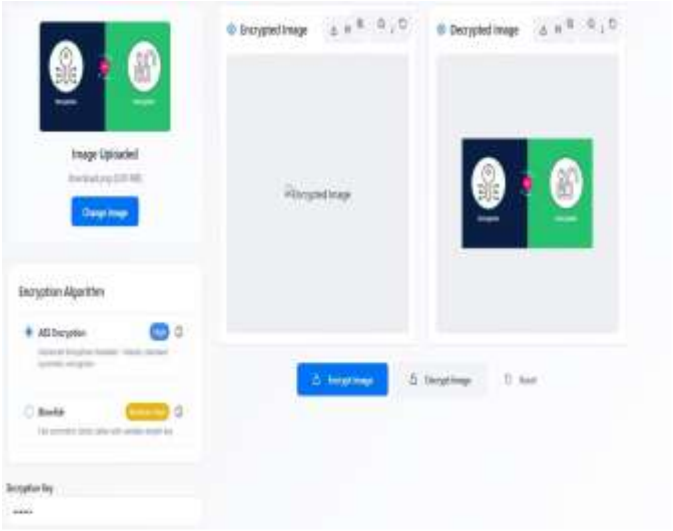
A second critical metric is histogram analysis, which evaluates the statistical distribution of pixel intensities in encrypted images. An ideal encryption system produces a uniform histogram where the frequency of pixel values appears evenly distributed. This randomness ensures that attackers cannot derive meaningful insights from the cipher image by studying its statistical features. In MATLAB simulations, Blowfish-generated encrypted images exhibited significantly randomized histograms compared to the original, confirming its ability to obscure visual and statistical patterns effectively. Such results indicate strong resistance against statistical attacks, a key requirement in multimedia security.

Another important aspect of evaluation is correlation analysis between adjacent pixels. Original images typically show high correlation between neighboring pixels, which attackers can exploit. A secure encryption algorithm must reduce this correlation to near zero. Results confirmed that Blowfish successfully minimizes pixel correlation in encrypted images, producing outputs where adjacent pixels appear completely independent. This decorrelation property strengthens Blowfish's resistance against differential attacks, ensuring that even small variations in the input image or key produce entirely different ciphertext outputs.

6. RESULTS AND EVALUATION

SAMPLE RECORDS

Analysis shows that DES is significantly slower in both encryption and decryption due to its hardware-oriented design and small 56-bit key size, which also makes it insecure against brute-force attacks. AES demonstrates strong security with large key sizes (128, 192, and 256 bits) and faster performance than DES, but it is computationally heavier for large-scale image data. Blowfish, by contrast, combines speed and flexibility, offering fast encryption and decryption with key sizes ranging from 32 to 448 bits. It proves particularly efficient in software implementations, outperforming DES.



The MATLAB implementation of Blowfish provided practical validation of its efficiency. Both grayscale and color images, in formats such as BMP, JPEG, PNG, and TIFF, were encrypted and decrypted successfully. The system generated three outputs: the original image, the encrypted cipher image, and the decrypted image. Results confirmed that Blowfish produced perfectly lossless decryption, where the reconstructed image was identical to the original. This outcome demonstrates that Blowfish not only provides strong security but also preserves data integrity, which is crucial for applications in medical imaging, defense systems, and secure communication.

Statistical analysis of the encrypted outputs further reinforced Blowfish's security strength. Histogram analysis of encrypted images revealed uniformly distributed pixel intensities.

Histogram analysis was applied to the sample records to study the statistical properties of the encrypted images. Original images showed non-uniform distributions with clear peaks, corresponding to recurring intensity values, especially in areas of smooth texture. By contrast, encrypted images generated using Blowfish displayed randomized and uniform histograms. This randomness ensured that attackers could not use statistical analysis to gain insights into the original content. The results confirmed that Blowfish effectively removes visible and statistical correlations in sample records, reinforcing its robustness against statistical attacks.

Another critical observation from the sample records was the correlation analysis of adjacent pixels. In the original images, neighboring pixels exhibited high correlation, which is a common characteristic of unencrypted image data. After encryption, this correlation was significantly reduced, with adjacent pixels appearing statistically independent. This outcome demonstrated that Blowfish provides strong diffusion, ensuring that even small changes in the input image or encryption key produced significantly different ciphertexts. The avalanche effect observed in the sample records confirmed Blowfish's suitability for applications where high sensitivity to input variation is crucial.

Entropy calculations for the encrypted sample records further validated the effectiveness of the algorithm. Original images typically exhibited entropy values lower than the theoretical maximum, reflecting predictable patterns in pixel intensities. Encrypted images, however, achieved entropy values close to the ideal, indicating a high degree of randomness and unpredictability. This ensured that the ciphertext contained no exploitable patterns, enhancing security against brute-force and cryptanalytic attacks. The results from the sample records confirmed that Blowfish is capable of producing secure ciphertext images across multiple formats and data sizes.

Finally, the analysis of the sample records highlighted the efficiency of Blowfish in terms of computational performance. Encryption and decryption times were measured for each image, showing that Blowfish performed consistently faster than DES and with comparable or superior efficiency to AES. This efficiency, combined with its strong security properties, makes Blowfish a practical algorithm for real-world environments where rapid processing of multimedia data is required. Overall, the sample records provided comprehensive validation of Blowfish as a secure, efficient, and reliable encryption technique for image data.

DES, in contrast, is largely obsolete, serving primarily as a benchmark in comparative studies. By consolidating both theoretical analysis and experimental results, this research confirms that Blowfish is not only a secure algorithm but also a practical solution for multimedia encryption. These outcomes validate the relevance of Blowfish in advancing secure image transmission systems, offering a blend of speed, simplicity, and robustness that aligns with the growing demands of modern digital communication.

Another important outcome of the evaluation lies in the robustness of Blowfish against cryptanalytic attacks. Studies demonstrate that no successful attack has been recorded against the full version of the algorithm. In MATLAB simulations, even when small variations were introduced in the secret key or the input image, the resulting ciphertext was entirely different from the previous output, highlighting Blowfish's strong avalanche effect. This property is critical in ensuring that any slight modification in input leads to significant changes in output, thereby making the encryption resistant to differential cryptanalysis. Such characteristics confirm Blowfish's reliability in contexts where high sensitivity to key and data variations is necessary for maintaining strong protection.Furthermore, the results highlight how Blowfish addresses the limitations of traditional algorithms in the context of modern applications. While AES provides exceptional robustness, its comparatively higher computational demand may not be ideal for lightweight systems or applications requiring rapid encryption of large image files.

7. CONCLUSION

This research consolidated both theoretical and experimental perspectives on image encryption using symmetric key algorithms, specifically DES, AES, and Blowfish. The comparative analysis revealed that DES, once a widely used standard, has become insecure due to its small key size and vulnerability to brute-force attacks. AES continues to be highly reliable, offering robust protection through larger key sizes, but it requires higher computational resources, which may limit its efficiency in processing large multimedia datasets. Blowfish emerged as a strong alternative, demonstrating superior adaptability, computational efficiency, and resistance to cryptanalysis, particularly in software-based implementations.

The MATLAB-based implementation of Blowfish further validated its practical applicability. Simulation results confirmed that Blowfish encrypts and decrypts both grayscale and color images effectively, maintaining perfect fidelity between the original and decrypted images. Histogram analysis, entropy calculations, and correlation studies reinforced the algorithm’s strength by showing that the encrypted outputs exhibit high randomness and resistance to statistical attacks. These results underline Blowfish’s ability to provide fast and reliable encryption without compromising security, making it suitable for applications in defense communication, telemedicine, secure internet transactions, and multimedia systems.

Looking forward, future work can focus on extending the implementation of Blowfish and other symmetric algorithms to multimedia data beyond images, such as audio and video. Integrating Blowfish into hybrid cryptographic frameworks alongside asymmetric methods may further enhance authentication, integrity, and scalability. Additionally, research can investigate the deployment of Blowfish in modern cloud and distributed environments, evaluating its performance under large-scale, real-time data transfer scenarios. The adaptability of Blowfish, combined with its simplicity, makes it an excellent candidate for continued exploration in emerging domains such as Internet of Things (IoT) security, smart healthcare, and military-grade secure communication.

REFERENCES

1. J. Thakur & N. Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," International Journal of Emerging Technology and Advanced Engineering (IJETAE), vol. 1, no. 2, 2011. A performance-based comparative study of DES, AES, and Blowfish algorithms.

2. A. Devi, A. Sharma & A. Rangra, "A Review on DES, AES and Blowfish for Image Encryption & Decryption," International Journal of Computer Science and Information Technologies (IJCSIT), vol. 6, no. 3, pp. 3034–3036, 2015. A survey and comparison of DES, AES, and Blowfish with focus on image encryption applications.

3. P. Singh & K. Singh, "Image Encryption and Decryption Using Blowfish Algorithm in MATLAB," International Journal of Scientific & Engineering Research (IJSER), vol. 4, no. 7, pp. 150–154, 2013. A MATLAB-based implementation of Blowfish for secure image encryption and decryption.

4. A. M. A. Al-Neaimi & R. F. Hassan, "New Approach for Modifying Blowfish Algorithm by Using Multiple Keys," International Journal of Computer Science and Network Security (IJCSNS), vol. 11, no. 3, pp. 35–41, 2011. A modified Blowfish structure using multiple keys to enhance security.

5. M. Anand Kumar & S. Karthikeyan, "Investigating the Efficiency of Blowfish and Rijndael (AES) Algorithms," International Journal of Computer Network and Information Security (IJCNIS), vol. 2, pp. 22–28, 2012. A performance evaluation of Blowfish and AES algorithms for secure communication.

6. P. Dang & P. Chau, "Image Encryption for Secure Internet Multimedia Applications," IEEE Transactions on Consumer Electronics, vol. 46, no. 3, pp. 395–403, 2000. A technique for secure image encryption in multimedia applications.