System-Level Secure Key Management For DNA-Based Image Cryptography Using Ephemeral ECDH and HKDF-SHA256

Bagus Satrio Waluyo Poetro
Doctoral Program in Information Systems, Postgraduate School, Universitas Diponegoro, Semarang, Indonesia
bagussatriowp@students.undip.ac.id (corresponding author)

Kusworo Adi
Department of Physics, Faculty of Science and Mathematics, Universitas Diponegoro, Semarang, Indonesia
kusworoadi@lecturer.undip.ac.id

Aris Puji Widodo
Department of Informatics, Faculty of Science and Mathematics, Universitas Diponegoro, Semarang, Indonesia
arispw@gmail.com

Received: 17 January 2026 | Revised: 15 March 2026, 24 March 2026, and 9 April 2026 | Accepted: 17 April 2026

 DOI: https://doi.org/10.48084/etasr.17609

ABSTRACT

The increasing transmission of digital images over untrusted networks requires encryption mechanisms that combine strong statistical protection with secure key management. Although DNA-based image cryptography integrated with chaotic systems achieves high confusion and diffusion performance, most existing approaches rely on static or deterministically derived keys, lacking forward secrecy and structured session isolation. This paper proposes a system-level secure key management architecture for DNA-based image encryption. The framework integrates ephemeral Elliptic Curve Diffie–Hellman (ECDH) over Curve25519 (X25519) to establish session-specific shared secrets and employs RFC 5869-compliant HKDF-SHA256 for domain-separated subkey derivation. The derived subkeys are independently assigned to permutation, DNA rule selection, and diffusion stages, preventing key reuse and entropy overlap. Security analysis under a Dolev-Yao adversarial model demonstrates improved resistance to session compromise and public-key substitution in authenticated exchange. Experimental results confirm that the integration of structured key management preserves the statistical performance of the encryption engine, achieving NPCR above 99.6%, UACI near 33.4%, and entropy values approaching 7.99. The proposed framework enhances the practical security of DNA-based image cryptosystems by bridging statistical encryption techniques with modern secure key establishment protocols.

Keywords-DNA cryptography; ephemeral key agreement; perfect forward secrecy; system-level security; Key Derivation Function (KDF); chaotic image encryption

I. INTRODUCTION

The rapid proliferation of distributed computing environments, cloud infrastructures, and data-intensive applications has significantly increased the volume of high-resolution multimedia data transmitted across untrusted communication networks. Digital images, which are extensively utilized in domains such as telemedicine, remote sensing, and intelligent surveillance systems, introduce unique security challenges due to their high dimensionality, strong inter-pixel correlation, and inherent redundancy. These characteristics limit the effectiveness of conventional encryption schemes originally designed for textual data, as such schemes do not explicitly account for the statistical and structural properties of multimedia signals [1, 2]

In response, chaos- and DNA-based image encryption techniques have emerged as promising approaches for addressing the structural complexity of multimedia data. Chaotic dynamical systems exhibit properties such as sensitivity to initial conditions, ergodicity, and pseudo-randomness, which are well-suited for constructing

permutation and diffusion mechanisms within image encryption pipelines [1, 3]. Complementarily, DNA-based encoding introduces additional confusion through nucleotide mapping rules and Watson-Crick complementarity, enabling multi-level symbolic transformations that enhance resistance to statistical and differential attacks [4, 5]. Recent studies demonstrate that hybrid DNA-chaos frameworks can achieve near-ideal entropy and low pixel correlation, indicating strong statistical robustness against classical cryptanalysis [6-7].

Despite these algorithmic advances, existing research predominantly adopts an algorithm-centric perspective, focusing on maximizing statistical randomness while largely neglecting system-level security considerations, particularly in relation to key management and secure communication lifecycle integration. Many DNA-based image encryption schemes derive chaotic parameters and encoding rules from static passphrases, deterministic hashing, or plaintext-dependent transformations [4, 8]. Although such approaches introduce variability, they fail to provide essential cryptographic guarantees required in modern distributed information systems, including forward secrecy, secure session isolation, and resistance to key compromise propagation [9, 10]. As a result, compromise of a single long-term secret may expose multiple encryption sessions, leading to significant confidentiality risks in sensitive applications such as medical image transmission and cloud-based diagnostics [2, 11].

Furthermore, most existing DNA-chaos encryption frameworks do not incorporate formally defined asymmetric key establishment mechanisms. Under adversarial models such as the Dolev-Yao model, the absence of authenticated key exchange exposes systems to active attacks, including public-key substitution, replay attacks, and session hijacking [10, 12]. Although modern cryptographic protocols extensively employ secure key agreement mechanisms such as Elliptic Curve Diffie-Hellman (ECDH) to ensure robust session-level security, these mechanisms are rarely integrated into multimedia encryption pipelines [12, 13]. This disconnect reveals a fundamental gap between cryptographic protocol design and multimedia encryption implementation, particularly in system-level security architecture.

From an information systems perspective, this gap reflects a broader misalignment between algorithmic security performance and organizational trust requirements in distributed environments. Contemporary information systems emphasize not only data confidentiality, but also trust assurance, risk mitigation, and secure decision-making under uncertainty [11]. In such contexts, encryption mechanisms must be embedded within a structured key lifecycle that supports secure negotiation, isolation, and revocation of cryptographic material across sessions. Without such integration, even statistically strong encryption algorithms may fail to provide adequate protection at the system level.

These limitations highlight the need for a protocol-aware cryptographic architecture that integrates secure session establishment with structured key management in DNA-based image encryption systems. In such architectures, entropy sources must be independent of static parameters and plaintext-derived inputs to prevent deterministic key reuse. Additionally, negotiated session secrets should be expanded into multiple cryptographically independent subkeys through domain-separated key derivation mechanisms, ensuring entropy isolation across functional stages such as permutation, encoding, and diffusion [14, 15]. This design principle aligns with modern secure communication protocols, where key separation and context binding are essential to prevent cross-layer entropy leakage and compositional vulnerabilities.

To address these challenges, this study proposes a system-level secure key management framework for DNA-based image encryption. The proposed architecture integrates an ephemeral ECDH key exchange mechanism over Curve25519 (X25519) to establish session-specific shared secrets between communicating entities in untrusted environments [13]. The use of ephemeral key exchange ensures forward secrecy and eliminates the reliance on static initialization parameters. The negotiated shared secret is subsequently processed using a Hash-based Key Derivation Function (HKDF) with SHA-256, following the extract-and-expand paradigm defined in modern cryptographic standards [14]. This process produces multiple domain-separated subkeys that are independently assigned to permutation, DNA encoding rule selection, and diffusion stages, thus preventing entropy reuse and enhancing compositional security.

By embedding standardized key agreement and structured key derivation into the DNA-based encryption pipeline, the proposed framework bridges the gap between statistical multimedia encryption techniques and modern cryptographic protocol design. Consequently, this architecture not only preserves the statistical robustness of DNA-chaos encryption but also enhances system-level security properties, including forward secrecy, session isolation, and resistance to active adversarial attacks. This integration advances DNA-based image cryptography toward deployment-ready secure information systems capable of supporting high-stakes applications such as medical data transmission and cloud-based analytics.

II. RELATED WORK AND IDENTIFIED GAP

Chaos- and DNA-based image encryption techniques have been extensively explored to address the intrinsic structural properties of digital images, including high spatial redundancy and strong inter-pixel correlation [1, 5]. Chaotic dynamic systems are widely utilized due to their sensitivity to initial conditions, ergodicity, and pseudo-random behavior, enabling effective permutation and diffusion processes that enhance statistical randomness in encrypted images [3]. In parallel, DNA-based encoding introduces additional confusion through nucleotide mapping and Watson-Crick complementary pairing rules, enabling multi-symbol substitution and increasing non-linearity through dynamic rule selection and hybrid encoding strategies [4, 7].

Hybrid DNA-chaos frameworks further combine chaotic permutation with DNA-based diffusion to disrupt spatial correlations and improve resistance to statistical and differential attacks, often achieving near-ideal entropy values and near-zero pixel correlation coefficients [6, 16]. Robustness against differential attacks is commonly evaluated using

metrics such as NPCR and UACI, which quantify sensitivity to small perturbations in plaintext images [17]. However, despite these strong statistical properties, existing approaches remain predominantly algorithm-centric and exhibit critical limitations in key management and entropy design. Many schemes derive chaotic parameters and DNA rule configurations from static passphrases, deterministic hash functions, or plaintext-dependent transformations, which fail to provide forward secrecy, secure key rotation, and session isolation required in modern distributed systems [4, 8-10]. Additionally, entropy reuse across multiple functional stages, such as permutation, encoding, and diffusion, introduces potential statistical dependencies due to the absence of domain-separated key derivation, thus weakening compositional security [5, 17, 18]. In contrast, modern cryptographic systems emphasize secure key establishment and lifecycle management through asymmetric protocols such as ECDH and authenticated key exchange schemes, which provide strong security guarantees against active adversarial attacks [12, 13].

When combined with standardized key derivation mechanisms such as HKDF, these approaches enable the generation of cryptographically independent subkeys and enforce domain separation, as widely adopted in secure communication protocols, including transport-layer security architectures [14, 19]. Furthermore, recent studies in Internet of Medical Things (IoMT) and smart infrastructure highlight the importance of integrating cryptographic mechanisms with system-level considerations such as trust, risk management, and secure decision-making [2, 11]. Nevertheless, these protocol-level security mechanisms are rarely integrated into DNA-based image encryption frameworks, and existing hybrid approaches that incorporate ECC or HKDF still treat key management as a secondary component rather than a core architectural element [6, 15, 20]. Consequently, a clear research gap exists in the lack of protocol-aware, system-level cryptographic architectures that integrate secure session-based key establishment, domain-separated key derivation, and structured entropy management within DNA-based image encryption systems. Addressing this gap requires a shift from purely algorithmic optimization toward a unified architecture that aligns statistical encryption performance with modern cryptographic protocol design and information system security requirements.

III. PROPOSED SYSTEM ARCHITECTURE

A. System Overview

To address the identified gap in integrating secure key management with DNA-based image encryption, this study proposes a protocol-aware system architecture that explicitly separates cryptographic negotiation from internal encryption operations. The design is structured to enforce entropy isolation, session independence, and functional modularity across different stages of the encryption process. The architecture consists of three main layers: Key Establishment, Key Derivation, and DNA Encryption, each with distinct responsibilities and controlled interactions.

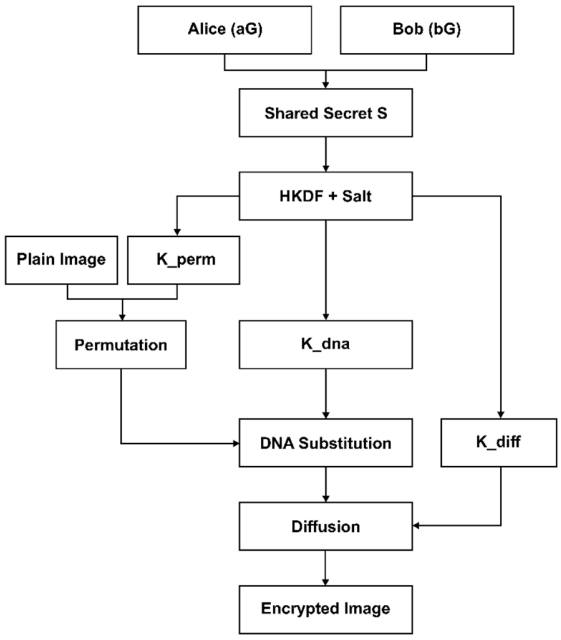

Fig. 1. Layered architecture of the proposed ECDH-HKDF-DNA image encryption framework.

As shown in Figure 1, the Key Establishment Layer is responsible for generating a session-specific shared secret using ephemeral asymmetric cryptography. The Key Derivation Layer transforms this secret into multiple domain-separated subkeys, while the DNA Encryption Layer utilizes these subkeys to control the permutation, encoding, and diffusion processes. This separation ensures that cryptographic negotiation remains independent from data transformation mechanisms, thereby preventing entropy reuse and improving system-level robustness.

B. Ephemeral ECDH Key Establishment

To ensure secure session initialization over untrusted communication channels, the proposed system employs an ephemeral ECDH protocol based on Curve25519. This mechanism enables both communicating parties to derive a shared secret without directly transmitting sensitive key material, thereby reducing exposure to interception.

$$\alpha, b \in R\, \mathbb{Z}_q \tag{1}$$

are ephemeral private scalars, and G is the elliptic curve base point. The public keys are computed as:

$$A = aG, \quad B = bG \tag{2}$$

The shared secret is then derived as:

$$S = aB = bA = abG \tag{3}$$

As illustrated in Figure 2, both parties independently compute the same shared secret S. Since the private scalars are generated per session and discarded after use, the protocol provides forward secrecy and prevents compromise propagation across sessions.

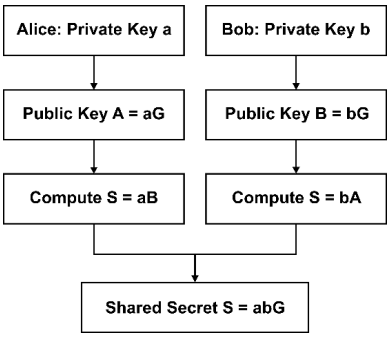

Fig. 2. X25519 ECDH handshake and shared secret derivation.

C. HKDF-SHA256 Key Derivation

Following secure key establishment, the shared secret must be transformed into structured cryptographic material suitable for multi-stage encryption. Direct use of the shared secret may introduce bias or unintended correlations; therefore, a standardized key derivation process is required.

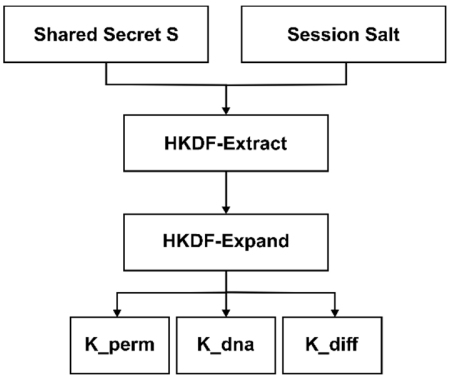

Fig. 3. Domain-separated key derivation architecture.

The shared secret S is processed using the extract-and-expand paradigm:

$$PRK = HMACSHA - 256(salt, S) \quad (4)$$

$$K_i = HMACSHA - 256(PRK, info_i \parallel i) \quad (5)$$

where $info_i \parallel i$ defines the functional context of each subkey. As shown in Figure 3, this process produces multiple independent subkeys:

$$K_{perm}, K_{dna}, K_{diff} \quad (6)$$

The use of domain separation ensures that each operational stage receives an independent entropy source, eliminating cross-stage dependencies and improving compositional security.

D. Subkey Mapping and DNA Encryption Pipeline

After deriving independent subkeys, the next step is to integrate them into the DNA-based encryption workflow. Unlike conventional designs that reuse a single chaotic sequence, the proposed system assigns distinct subkeys to each functional stage to enforce entropy isolation.

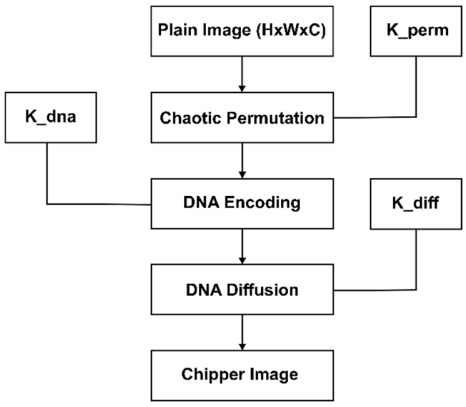

Fig. 4. Subkey-driven DNA encryption workflow.

The mapping is defined as follows:

1. Permutation Stage

$$x_{n+1} = f(x_n, \mu) \quad (7)$$

The subkey K_{perm} initializes a chaotic map to generate a permutation index P, which reorders pixel positions.

2. DNA Encoding Stage

$$r_n = g(K_{dna}, n) \quad (8)$$

3. Diffusion Stage

$$k_n = h(K_{diff}, n) \quad (9)$$

$$C_n = E_n \oplus k_n \quad (10)$$

The overall encryption transformation is expressed as:

$$I \rightarrow B \rightarrow P(B) \rightarrow D(O(B)) \rightarrow C \quad (11)$$

As shown in Figure 4, the pipeline ensures that each stage operates under independent entropy sources derived from the session-specific shared secret. Consequently, identical plaintext images encrypted under different sessions produce distinct ciphertext outputs:

$$C(1) = C(2) \quad (12)$$

This property significantly enhances resistance against replay, known-plaintext, and statistical attacks, while maintaining the high entropy and decorrelation properties required for secure image encryption.

IV. SECURITY ANALYSIS

The security of the proposed framework was analyzed under the Dolev-Yao adversarial model, where the communication channel was assumed to be fully controlled by an active adversary capable of intercepting, modifying, injecting, and replaying messages. The adversary was considered computationally bounded, and the security of the key establishment phase relied on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP) over Curve25519. Given public keys $A = aG$ and $B = bbG = bBG = bG$, it is computationally infeasible to recover the private scalars a or b, or to derive the shared secret $S = abG$, ensuring confidentiality of the negotiated session key.

The use of ephemeral private scalars in each session guarantees forward secrecy, such that compromise of long-term credentials or previously observed communication does not reveal past session keys. Each execution of the protocol produces an independent shared secret, which is subsequently transformed through HKDF-SHA256 into multiple domain-separated subkeys. This design enforces strict entropy isolation across functional stages of the encryption pipeline, ensuring that the permutation, DNA encoding, and diffusion processes operate using computationally independent key material. Under the pseudorandomness assumptions of HKDF and HMAC-SHA256, leakage in one stage does not provide a feasible pathway for deriving subkeys associated with other stages.

Although standard ECDH protects against passive adversaries, it is inherently vulnerable to active key substitution attacks. To address this limitation, the proposed architecture assumes authentication of ephemeral public keys using digital signatures (e.g., Ed25519), ensuring that only legitimate parties can participate in the key exchange. Under this assumption, the system achieves resistance against man-in-the-middle attacks, preventing adversaries from injecting malicious key material or impersonating communicating entities.

From a system-level perspective, the proposed architecture enforces strict session isolation by deriving all operational parameters from a fresh shared secret for each encryption instance. Consequently, identical plaintext inputs encrypted under different session keys yield distinct ciphertext outputs, formally expressed as $S^{(1)} \neq S^{(2)} \Longrightarrow C^{(1)} \neq C^{(2)}$. This property ensures that the encryption process is strongly dependent on the session-specific secret, thereby preventing deterministic behavior across sessions. As a result, the scheme effectively mitigates replay and known-plaintext attacks, since the ciphertext generated in one session cannot be reused or exploited in another.

The overall security strength of the system is bounded by the 256-bit key space of X25519, yielding a search space of size 2256, which is computationally infeasible to exhaust under current computational capabilities. Although multiple subkeys are derived for different functional stages, they originate from a single high-entropy shared secret, and thus the effective security level remains 256 bits while ensuring proper entropy distribution through domain-separated derivation.

In addition to cryptographic guarantees, the statistical security of the encryption pipeline is preserved. Experimental evaluation demonstrates entropy values approaching the theoretical maximum and near-zero correlation between adjacent pixels in the ciphertext image. These results indicate that the integration of protocol-level key management does not degrade the statistical randomness of the DNA-based encryption process, but instead strengthens its resistance against both statistical and structural cryptanalysis.

V. EXPERIMENTAL RESULTS

A. Experimental Setup

Experimental evaluation was conducted using 30 chest radiograph images selected from the publicly available Tuberculosis (TB) Chest X-ray Database, originally introduced in [21]. This dataset is widely used in medical imaging research and contains 700 tuberculosis-positive and 3500 normal chest X-ray images collected from multiple international repositories, including the NLM Montgomery and Shenzhen datasets, the Belarus dataset, and the NIAID TB portal [22]. From this dataset, a subset of images was randomly selected and further augmented using four geometric transformations, which are 90° rotation, 180° rotation, horizontal flip, and vertical flip, resulting in a corpus of 30 radiograms. This augmentation strategy preserves intrinsic pixel distribution characteristics while introducing controlled structural diversity.

All images were converted to grayscale and normalized to a uniform spatial resolution to ensure consistent experimental conditions. The use of radiographic imagery is deliberate: such images exhibit high spatial redundancy, low local variance in soft tissue regions, and strong inter-pixel correlation, making them a stringent benchmark for evaluating chaos-based encryption systems. All experiments were conducted on a 64-bit Windows workstation using Python 3.10. The proposed system integrates X25519-based ECDH for session-level key establishment and HKDF-SHA256 for domain-separated key derivation. A fresh 256-bit random salt was generated for each encryption session using a cryptographically secure random generator. The evaluation metrics include Shannon entropy, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), spatial correlation coefficients, execution time, and memory consumption.

To ensure statistical robustness, each image was subjected to 30 independent Chosen-Plaintext Attack (CPA) trials, resulting in a total of 900 NPCR and UACI evaluations. Mean (μ) and standard deviation (σ) values were computed across the dataset. The sample size of 30 images follows common practice in image encryption evaluation, where statistical reliability is achieved through repeated perturbation-based testing rather than large-scale dataset expansion.

B. Visual Encryption Validation

Plaintext-Ciphertext-Decryption Verification involves verifying the correctness of the end-to-end encryption pipeline by selecting a representative radiogram to illustrate the transformation across the three stages of plaintext, ciphertext, and decrypted reconstruction.

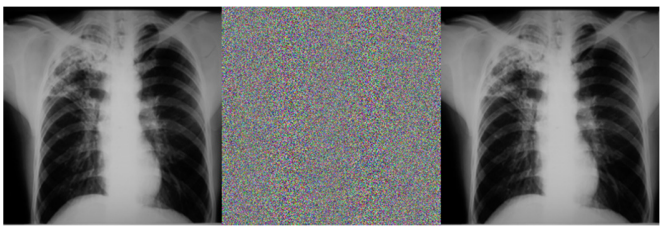

Fig. 5. Visual demonstration of the proposed architecture operating on medical radiogram Tuberculosis-343: (a) plaintext, (b) DNA-ciphertext, and (c) lossless decrypted output.

As shown in Figure 5, the ciphertext exhibits noise-like characteristics with no visually discernible anatomical structures, indicating effective visual obfuscation. The decrypted image is identical to the original plaintext,

confirming the correctness and reversibility of the DNA-based permutation-diffusion pipeline combined with HKDF-based key management. Histogram analysis involves analyzing the statistical distribution of pixel intensities to evaluate resistance against histogram-based attacks that exploit non-uniform intensity distributions in natural images.

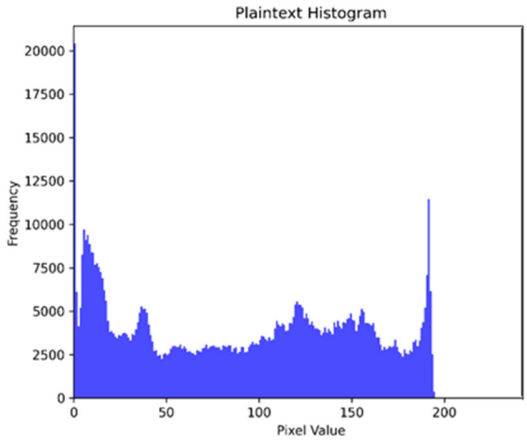

Fig. 6. Plaintext pixel intensity histogram.

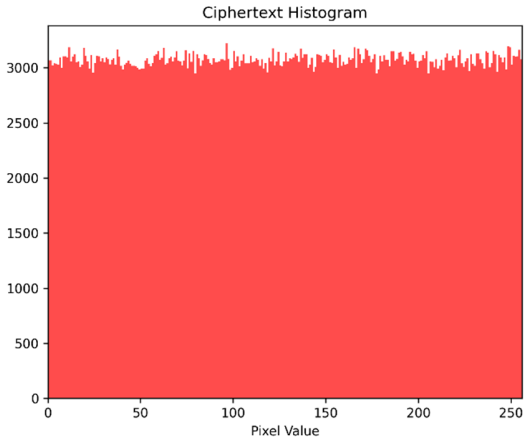

Fig. 7. Ciphertext pixel intensity histogram.

The plaintext histogram (Figure 6) exhibits clustered peaks corresponding to different tissue densities, reflecting strong statistical non-uniformity. In contrast, the ciphertext histogram (Figure 7) approaches a uniform distribution over the full intensity range [0, 255], indicating that the encryption process effectively removes statistical patterns present in the original image.

Correlation analysis involves evaluating the spatial correlation between adjacent pixels to measure the effectiveness of the diffusion stage in eliminating predictable spatial dependencies. The plaintext correlation plot (Figure 8) shows strong linear clustering, indicating high spatial redundancy. After encryption, the ciphertext plot (Figure 9) exhibits a uniform dispersion of points with near-zero correlation, demonstrating effective spatial decorrelation.

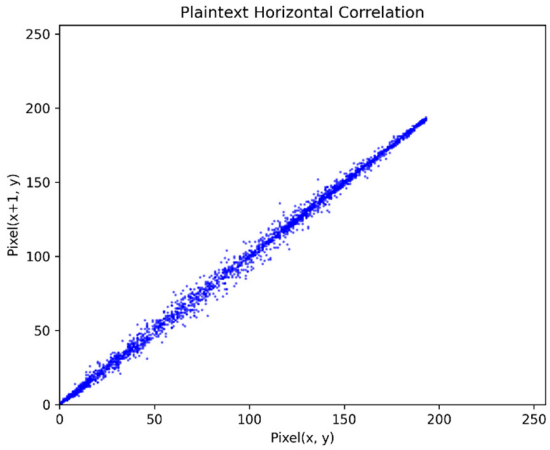

Fig. 8. Plaintext adjacent-pixel correlation scatter plot.

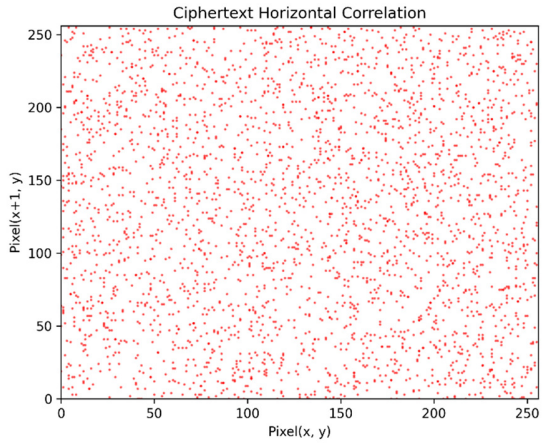

Fig. 9. Ciphertext adjacent-pixel correlation scatter plot.

C. Quantitative Statistical Evaluation

The entropy values approach the theoretical maximum for 8-bit grayscale images, indicating strong global randomness. Correlation coefficients converge toward zero, confirming effective removal of spatial dependencies. However, the NPCR and UACI values being lower than the ideal standard reflect the characteristics of the architecture that uses domain-separated subkeys because each stage, such as permutation, DNA encoding, and diffusion, operates on independent entropy sources, so that the layered amplification of the avalanche effect does not occur as it does in monolithic chaos architectures. Recent DNA-chaos encryption studies typically report entropy values in the range of 7.98–7.999, NPCR values above 99%, and UACI values around 33%. These results are generally achieved using tightly coupled architectures where permutation and diffusion share the same entropy source. In contrast, the proposed framework enforces HKDF-based domain separation, generating independent subkeys for each functional stage. This structural separation reduces implicit cross-layer amplification effects, resulting in moderated NPCR and UACI values.

However, the entropy and correlation metrics remain aligned with established benchmarks, indicating that global statistical unpredictability is preserved and, more importantly,

the proposed architecture introduces system-level security properties such as session isolation and forward secrecy that are absent in conventional DNA chaos designs.

TABLE I. AGGREGATED CRYPTOGRAPHIC PERFORMANCE METRICS

Evaluation Metric	Mean (μ)	Std. dev. (σ)	Theoretical ideal
Shannon Entropy	7.9866	9.82×10^{-3}	≈ 8.0000
NPCR (%)	16.7251	9.68	≥ 99.6094
UACI (%)	6.3289	4.38	≈ 33.4635
Corr (R–G)	0.000799	-	≈ 0
Corr (R–B)	-0.000258	-	≈ 0
Encryption Time (s)	3.99	0.88	-
Protocol peak memory (MB)	518.92	-	-

D. Key Sensitivity Analysis

To evaluate key sensitivity, a single Least Significant Bit (LSB) was modified in the derived key material before encryption. The resulting ciphertext exhibits widespread non-linear divergence, demonstrating that even minimal changes in key material propagate throughout the encryption pipeline. This confirms that the system is highly sensitive to key variations and resistant to key-related attacks.

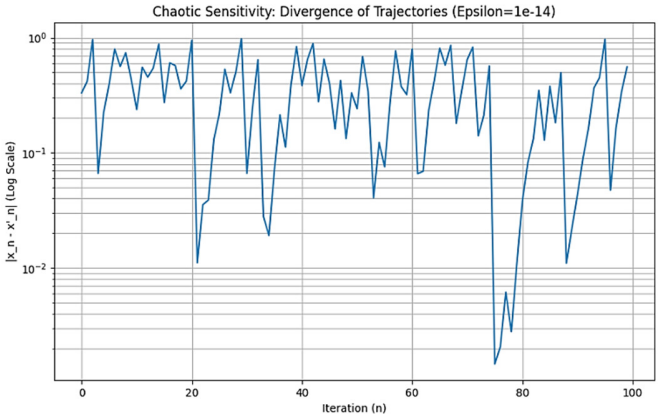

Fig. 10. Differential map showing ciphertext variation under one-bit key perturbation.

E. Computational Performance Analysis

The average encryption time per radiogram is 3.99 s, with observed variance depending on image size and CPA simulation overhead. Profiling indicates that ECDH key establishment and HKDF derivation contribute minimally to total execution time. The primary computational cost arises from chaotic sequence generation and DNA encoding/decoding operations. Despite the integration of cryptographic key management, the system maintains acceptable performance for offline or semi-real-time applications.

F. Protocol-Oriented Security Validation

Beyond statistical evaluation, protocol-level security properties were validated through controlled experiments. Forward secrecy was verified by executing 100 independent encryption sessions, each generating a unique shared secret with no observed collisions. Cross-session replay resistance was confirmed by injecting ciphertext from one session into another, resulting in deterministic decryption failure due to mismatched key material. Additionally, an active Man-In-The-Middle (MITM) scenario was simulated by substituting the ephemeral public key. Signature verification failed before key agreement, confirming that authenticated key exchange prevents unauthorized key substitution.

G. Architectural Trade-Off Discussion

Traditional DNA-chaos encryption frameworks rely on monolithic chaotic systems where all encryption stages share a single entropy source. While this design maximizes avalanche propagation, it lacks session isolation and formal key management. In contrast, the proposed architecture adopts a different approach by enforcing domain-separated key derivation and session-based key establishment. This design prioritizes forward secrecy, entropy independence, and resistance to cross-session attacks. As illustrated in Figure 11, the proposed system sacrifices some degree of avalanche amplification in exchange for stronger system-level security guarantees. Despite this trade-off, entropy and correlation metrics remain close to theoretical ideals, confirming that statistical security is preserved.

VI. DISCUSSION

A. Interpretation of Statistical and Differential Results

The results indicate strong global statistical performance, with entropy approaching the theoretical 8-bit limit and near-zero spatial correlation, confirming effective removal of structural redundancy. However, NPCR (≈16.7%) and UACI (≈6.3%) are lower than conventional DNA-chaos schemes. This is not a weakness but a consequence of HKDF-based domain separation, where each stage operates with independent subkeys. As a result, perturbation propagation is confined to the diffusion layer, reflecting intrinsic diffusion capability rather than amplified multi-layer effects.

B. Architectural Implications

The proposed system shifts DNA-based encryption from an algorithm-centric approach to a protocol-aware architecture. By integrating ephemeral ECDH and HKDF-SHA256, it ensures session isolation, forward secrecy, and independent key derivation. Unlike conventional designs, this framework combines strong statistical performance with formal key management, demonstrating that cryptographic robustness and statistical security can coexist within a unified system.

C. Deployment Considerations and Limitations

The added cryptographic layers introduce minimal overhead, with total processing time dominated by DNA-chaos operations, supporting practical deployment for secure medical image transmission. However, NPCR and UACI remain lower due to isolated diffusion, the security model relies on computational assumptions rather than formal verification, and evaluation is limited to grayscale radiograms. Future work should extend validation to broader data modalities and formal protocol analysis.

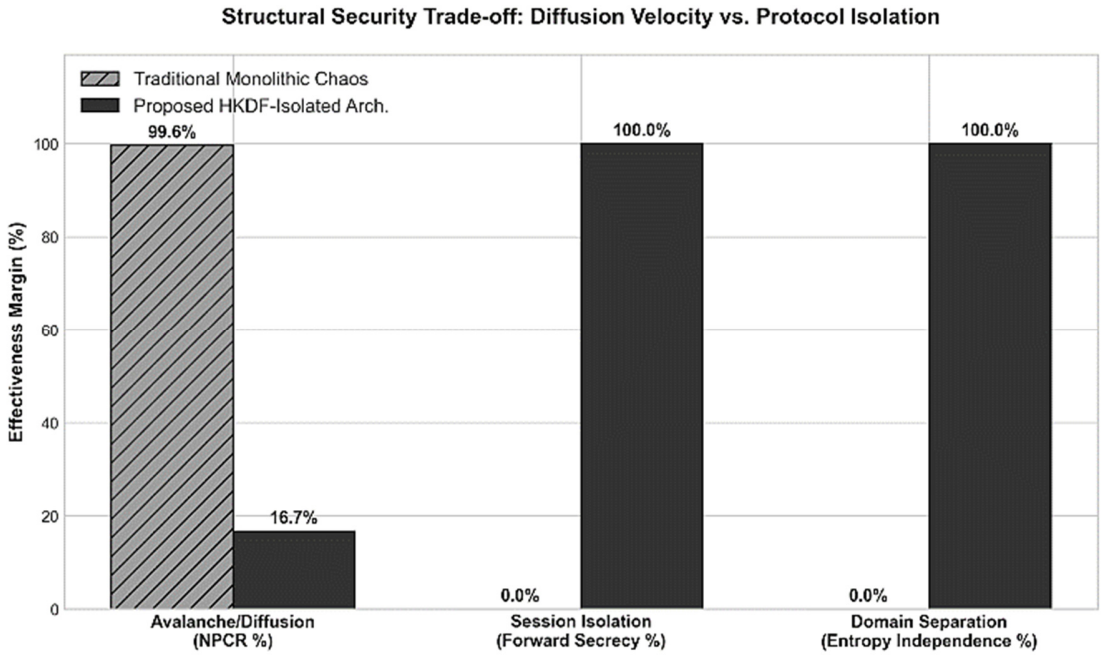

Fig. 11. Illustration of the distinction between monolithic entropy coupling and domain-separated session architecture.

VII. CONCLUSION

This study proposed a protocol-aware DNA-based image encryption framework that integrates ephemeral X25519 ECDH and HKDF-SHA256 for session-based key establishment and domain-separated subkey derivation. Unlike conventional DNA-chaos schemes, the proposed architecture enforces entropy isolation across permutation, substitution, and diffusion stages through independent subkeys. Experimental results demonstrate high entropy and near-zero spatial correlation, confirming strong statistical security, while adversarial simulations validate session uniqueness and replay resistance. Although NPCR and UACI are lower than monolithic designs, this reflects controlled diffusion under domain separation rather than reduced security. Overall, the proposed framework shows that modern cryptographic key management can be effectively combined with DNA-based encryption, advancing it toward a more robust, deployment-ready, and protocol-aligned security architecture.

DECLARATION OF COMPETING INTERESTS

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ACKNOWLEDGMENT

The authors would like to thank Universitas Islam Sultan Agung (UNISSULA) and the Faculty of Industrial Technology (FTI UNISSULA) for supporting this research.

DATA AVAILABILITY

This study used the Tuberculosis (TB) Chest X-ray Database provided by researchers from Qatar University, the University of Dhaka, and their collaborators. The dataset is publicly available and can be accessed through the corresponding dataset repositories [22] and the NIAID TB portal. The data supporting this study are available from the corresponding author upon reasonable request.

AI USE AND DECLARATION OF GENERATIVE AI USE

During the preparation of this work, the authors used OpenAI ChatGPT and Anthropic Claude to assist with proofreading and grammar improvement. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

REFERENCES

[1] Y. Sanjalawe, A. Al-Daraiseh, S. Al-E'mari, and S. N. Makhadmeh, "FileCipher: A Chaos-Enhanced CPRNG-Based Algorithm for Parallel File Encryption," *Algorithms*, vol. 19, no. 2, Feb. 2026, Art. no. 119, https://doi.org/10.3390/a19020119.

[2] V. N. S. Kumaran, T. Manikandan, R. K. Dhanaraj, T. Al-Shehari, N. A. Alsadhan, and S. Selvarajan, "A secure medical image encryption technique based on DNA cryptography with elliptic curves," *Scientific Reports*, vol. 15, no. 1, June 2025, Art. no. 20003, https://doi.org/10.1038/s41598-025-03898-5.

[3] A. Hennache, M. L. Hennache, and S. M. A. Ghaly, "Improving the RSA Encryption for Images by Introducing DNA Sequence Encoding," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 17786–17791, Dec. 2024, https://doi.org/10.48084/etasr.8557.

[4] H. Zhang, X. Feng, J. Sun, and P. Yan, "Chaotic Image Security Techniques and Developments: A Review," *Mathematics*, vol. 13, no. 12, June 2025, Art. no. 1976, https://doi.org/10.3390/math13121976.

[5] A. Saini and R. Sehrawat, "Enhancing Data Security through Machine Learning-based Key Generation and Encryption," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 14148–14154, June 2024, https://doi.org/10.48084/etasr.7181.

[6] H. Nguyen, T. Hoang, and L. Tran, "Efficient Hardware Implementation of Elliptic-Curve Diffie–Hellman Ephemeral on Curve25519," *Electronics*, vol. 12, no. 21, Oct. 2023, Art. no. 4480, https://doi.org/10.3390/electronics12214480.

[7] M. Altaf, W. Gaoud Alghabban, N. M. Nazar, M. Ayadi, and K. E. Hindi, "CryptoShield–multilayered cryptographic framework for

enhanced security and robust communication systems," *Scientific Reports*, vol. 15, no. 1, Dec. 2025, Art. no. 44046, https://doi.org/10.1038/s41598-025-29474-5.

[8] C. Bhaya, M. Zain, and A. K. Singh, "A DNA-based color image cryptosystem using chaotic maps, spiral mixing and non-linear binary operator," *Scientific Reports*, vol. 15, no. 1, Sept. 2025, Art. no. 33813, https://doi.org/10.1038/s41598-025-04021-4.

[9] S. Joshi, K. Crowther, and J. Robinson, "Tradeoffs in Key Rotation Strategies for Industrial Internet of Things Devices and Firmware," *Applied Sciences*, vol. 14, no. 21, Oct. 2024, Art. no. 9942, https://doi.org/10.3390/app14219942.

[10] J. Helen, A. Selvi, and T. Rajendran, "DNA Encoding and Chaos based Image Encryption Technique for Cloud Storage and Communications," *Indian Journal Of Science And Technology*, vol. 18, no. 9, pp. 734–744, Mar. 2025, https://doi.org/10.17485/IJST/v18i9.3557.

[11] R. Serrano, C. Duran, M. Sarmiento, C. K. Pham, and T. T. Hoang, "ChaCha20–Poly1305 Authenticated Encryption with Additional Data for Transport Layer Security 1.3," *Cryptography*, vol. 6, no. 2, June 2022, Art. no. 30, https://doi.org/10.3390/cryptography6020030.

[12] H. Zhiqiang, A. Rauf, A. Nazir, F. Tchier, A. Aslam, and K. A. Tola, "Design and analysis of a secure image encryption algorithm using proposed non-linear RN chaotic system and ECC/HKDF key derivation with authentication support," *Scientific Reports*, vol. 15, no. 1, Nov. 2025, Art. no. 39951, https://doi.org/10.1038/s41598-025-23592-w.

[13] A. Manasrah, H. Al-Aqrabi, Q. Yaseen, and T. Khdour, "A provably secure two-way authenticated key agreement protocol for IIoT environments," *Egyptian Informatics Journal*, vol. 32, Dec. 2025, Art. no. 100833, https://doi.org/10.1016/j.eij.2025.100833.

[14] L. Huang, C. Ding, Z. Bao, H. Chen, and C. Wan, "A DNA Encoding Image Encryption Algorithm Based on Chaos," *Mathematics*, vol. 13, no. 8, Apr. 2025, Art. no. 1330, https://doi.org/10.3390/math13081330.

[15] M. Samiullah *et al.*, "An Image Encryption Scheme Based on DNA Computing and Multiple Chaotic Systems," *IEEE Access*, vol. 8, pp. 25650–25663, 2020, https://doi.org/10.1109/ACCESS.2020.2970981.

[16] V. Tanksale, "Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices," *Electronics*, vol. 13, no. 18, Sept. 2024, Art. no. 3631, https://doi.org/10.3390/electronics13183631.

[17] W. Robert *et al.*, "A Comprehensive Review on Cryptographic Techniques for Securing Internet of Medical Things: A State-of-the-Art, Applications, Security Attacks, Mitigation Measures, and Future Research Direction," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol. 2024, pp. 135–169, Nov. 2024, https://doi.org/10.58496/MJAIH/2024/016.

[18] Z. Xia, T. Liu, J. Wang, and S. Chen, "A secure and efficient authenticated key exchange scheme for smart grid," *Heliyon*, vol. 9, no. 7, July 2023, Art. no. e17240, https://doi.org/10.1016/j.heliyon.2023.e17240.

[19] C. W. Chuah, N. Z. Harun, and I. R. A. Hamid, "Key derivation function: key-hash based computational extractor and stream based pseudorandom expander," *PeerJ Computer Science*, vol. 10, Aug. 2024, Art. no. e2249, https://doi.org/10.7717/peerj-cs.2249.

[20] B. S. W. Poetro, K. Adi, and A. P. Widodo, "Autonomous Key Generation and Management using HKDF-SHA256 for Secure DNA-based Image Cryptography," in *2025 3rd International Conference on Computer System, Information Technology, and Electrical Engineering (COSITE)*, Dec. 2025, pp. 381–384, https://doi.org/10.1109/COSITE68330.2025.11414297.

[21] T. Rahman *et al.*, "Reliable Tuberculosis Detection Using Chest X-Ray With Deep Learning, Segmentation and Visualization," *IEEE Access*, vol. 8, pp. 191586–191601, 2020, https://doi.org/10.1109/ACCESS.2020.3031384.

[22] T. Rahman, A. Khandakar, and M. E. H. Chowdhury, "Tuberculosis (TB) Chest X-ray Database." IEEE DataPort, Oct. 20, 2020, https://doi.org/10.21227/MPS8-KB56.