



Security Hardening of OptiSecure-3D: A Nonce-Diversified and Authenticated Framework for Compressed Latent-Image Protection

Akshat Tiwari¹, Dr. Prachi Diwan², Dr. Tarundhar Diwan³

¹Research Scholar, Atal Bihari Vajpayee University, Bilaspur, Chhattisgarh, India

²prachidiwan5@gmail.com, ³taruntech@gmail.com

Abstract

A previously published OptiSecure-3D architecture combines stacked-autoencoder compression, offline Differential Evolution and a three-dimensional Arnold map for image protection. Its lightweight online path motivates a deployment question that is not resolved by entropy, correlation, NPCR or UACI alone: a deterministic XOR mask reused across messages permits algebraic cancellation and does not provide ciphertext integrity. This technical note formalizes that threat and specifies OptiSecure-3D-H, a security-hardened profile that preserves latent-space compression and optional three-dimensional permutation while moving confidentiality and authenticity to standard cryptographic primitives. A 256-bit master secret is separated with HKDF; a fresh 96-bit nonce drives per-image permutation parameters; the canonical header is bound as associated data; and AES-256-GCM encrypts and authenticates the permuted latent bytes. Decryption verifies the authentication tag before inverse permutation or neural decoding. The paper provides an explicit invertible 3D matrix, packet format, encryption and decryption algorithms, failure rules and a leakage-controlled evaluation protocol. The analysis shows why the repeated-mask construction fails under known- or chosen-plaintext access and explains how nonce uniqueness, key separation, metadata authentication and fail-closed verification address those weaknesses. The chaotic transform is deliberately treated as reversible preconditioning rather than as the source of cryptographic security. No unsupported speed or attack-resistance result is asserted; empirical claims are reserved for a reproducible implementation study.

Keywords: authenticated encryption; image encryption; stacked autoencoder; latent compression; 3D Arnold map; differential evolution; HKDF; AES-GCM; nonce; chosen-plaintext attack.

1. Introduction

Secure image transport requires confidentiality, integrity and unambiguous processing of dimensions, model versions and compression parameters. Image-specific statistics can be useful diagnostics, but they do not replace a cryptographic security argument. Shannon's confusion–diffusion principles motivated many image ciphers [1] and two- and three-dimensional chaotic maps have subsequently been used as reversible permutations [2], [3]. Cryptanalytic studies nevertheless show that sensitivity, high entropy and low adjacent-pixel correlation do not by themselves establish resistance to known- or chosen-plaintext attacks [4]–[6].



Tiwari et al. published OptiSecure-3D in 2025 as a hybrid of stacked-autoencoder (SAE) compression, optimized three-dimensional chaotic mapping and an encryption/decryption module [7]. The present paper does not claim that architecture or its reported empirical values as a new contribution. It instead studies a narrow deployment risk raised by deterministic mask reuse and presents an independently specified security-hardening profile. This positioning is essential because the original title, architecture and headline results are already part of the scientific record [7].

The contributions of this technical note are:

- A concrete multi-message attack model for deterministic permutation-plus-XOR encryption, including known- and chosen-plaintext recovery paths.
- OptiSecure-3D-H, a nonce-diversified construction with HKDF key separation, HMAC-based permutation derivation, AES-256-GCM authenticated encryption and authenticated metadata.
- An explicitly invertible 3D Arnold-family matrix, canonical packet structure and complete forward and inverse algorithms with fail-closed behavior.
- A reproducibility protocol that separates SAE training, DE tuning, held-out evaluation and cryptographic conformance testing; it also prevents timing comparisons across incompatible platforms.
- A claim boundary: chaos-derived statistics are reported, if at all, as supplementary behavior; confidentiality and integrity are attributed only to the authenticated-encryption layer.

Finally, Section 8 sets out a concrete evaluation protocol for OptiSecure-3D-H, specifying the minimum empirical evidence (datasets, baselines, metrics and ablation studies) that must accompany any future performance or robustness claims. This protocol is an integral part of the contribution, framing how the construction should be tested in practice rather than serving as an optional appendix.

2. Relationship to OptiSecure-3D and Prior Work

2.1 Positioning relative to OptiSecure-3D

Our work does not re-propose OptiSecure-3D as originally specified in [7]; instead, it treats OptiSecure-3D as a starting point and proposes a protocol-level hardening profile, OptiSecure-3D-H. Table 1 summarizes which components of the original architecture are retained, which are re-scoped and which security responsibilities are moved to standard AEAD and key-derivation mechanisms. The contribution of this paper is therefore not a new “chaotic cipher,” but a hardened construction that (i) removes fixed-mask vulnerabilities under the threat model of Section 3 and (ii) aligns the design with well-analyzed, nonce-based authenticated encryption.



Table 1. Scope of the security-hardening contribution relative to the published OptiSecure-3D architecture.

Component	Published OptiSecure-3D [7]	OptiSecure-3D-H contribution
Latent representation	SAE-based compression	Retained as a pluggable, versioned compressor; its model identifier is authenticated.
Offline optimization	DE tunes chaotic parameters	Retained only for engineering objectives; training/validation data are separated from test data.
Per-image variation	Not made a formal security invariant	Fresh nonce is mandatory; permutation parameters are derived per image.
Confidentiality	Chaotic processing and XOR are central	AES-256-GCM is the confidentiality boundary.
Integrity	Not specified as a complete AEAD packet	Header and ciphertext are authenticated; failures return no plaintext.
Security claims	Image statistics and attack tests	Standard cryptographic assumptions plus explicit operational conditions.

2.2 Related image-encryption and compressible-encryption work

Beyond OptiSecure-3D, our work relates to a broader body of image-encryption and compressible-encryption constructions, many of which also combine permutation, diffusion and transform-domain processing. We briefly situate OptiSecure-3D-H within this landscape to clarify what is inherited, what is deliberately discarded and where our threat-model and evaluation focus differs.

Related work spans vectorized hyperchaotic encryption, compressible image ciphers and chaotic-map-driven key streams combined with diffusion and substitution layers.

The redesign retains the engineering idea of compressing before protection and allows an offline-optimized 3D permutation. It changes the security boundary. Differential Evolution remains a parameter-search method [8], while the SAE is a lossy compressor grounded in standard autoencoder methodology [9]–[12]. Neither component is treated as a substitute for a reviewed authenticated-encryption scheme.

Related work spans vectorized hyperchaotic encryption [24], compressed-sensing and scrambling designs [25], chaos-based compression–encryption [26] and cryptanalysis of complex DNA/Feistel constructions [27]. Learnable and compressible image-encryption research also emphasizes the distinction between privacy transformations and standard cryptography [28]. These studies motivate careful benchmarking, but they do not remove the need for authenticated encryption and explicit key/nonce management.



3. Threat Model and Requirements

The adversary may observe many packets, know image formats and model architecture, obtain selected plaintext–ciphertext pairs, submit malformed packets, reorder or replay valid packets and modify any unauthenticated field. The master key, implementation endpoint and random-number generator are assumed uncompromised. Side-channel and endpoint compromise are outside the construction-level analysis and require separate implementation controls.

Table 2. *Threat capabilities, requirements and enforcement boundaries.*

Adversarial capability	Required protection	Mechanism / boundary
Passive multi-message observation	No algebraic mask cancellation or cross-image leakage	Unique nonce and AEAD encryption.
Known/chosen plaintext	No reusable equivalent key	Standard encryption key remains secret; permutation seed changes per nonce.
Ciphertext header modification	Detect before decoding	GCM tag authenticates ciphertext and canonical header.
Replay reordering /	Application-level detection	Authenticated sequence or frame identifier plus receiver replay state.
Malformed dimensions / resource exhaustion	Bounded parsing	Validate version, lengths, dimensions and model identifier before allocation.
Nonce accident	Avoid catastrophic failure	Persistent uniqueness state; AES-GCM-SIV is an optional misuse-resistant profile [17].

Replay resistance is not supplied by AEAD alone. A sender identifier and monotonic sequence number SHOULD be included in the authenticated header and the receiver SHOULD reject previously accepted values within its operational replay window. Availability, traffic analysis, image dimensions exposed in the header and a compromised encoder are not hidden by this design.

3.1 Assumptions for subsequent analysis

The security arguments in Sections 4–7 are made under the following assumptions. (i) The master key, salts and derived keys remain confidential and are handled using side-channel-resistant implementations of AES-GCM and HKDF; we do not address leakage or fault attacks. (ii) Nonces are generated and enforced so that no key/nonce pair is ever reused for different plaintexts, including across sessions and devices. (iii) Header validation, replay protection and resource-usage limits are correctly enforced by the surrounding protocol and system, so that invalid or repeated packets cannot be exploited to escalate attacks beyond the model of Section 3. (iv) Standard cryptographic hardness assumptions for AES and HMAC hold. If any of these assumptions is violated, the guarantees claimed for OptiSecure-3D-H no longer apply.



4. Fixed-Mask Failure

We consider an adversary that can obtain (i) at least one plaintext–ciphertext pair (M_1, C_1) under a fixed permutation–mask pair (P, S) and (ii) observe further ciphertexts (C_i) of the same length produced under the same configuration. Under these conditions, the deterministic construction

$$C_i = P(M_i) \oplus S. \quad (1)$$

is insecure for confidentiality across messages, even if (P) appears complex and (S) has high empirical entropy.

For two ciphertexts encrypted with the same (P) and (S) , XOR cancels the mask:

$$C_1 \oplus C_2 = P(M_1) \oplus S \oplus P(M_2) \oplus S = P(M_1) \oplus P(M_2). \quad (2)$$

Once (S) is recovered as $(S = C_1 \oplus P(M_1))$ from any known or chosen plaintext–ciphertext pair, the adversary can compute $[M_i = P^{-1}(C_i \oplus S)]$ for every same-length ciphertext generated under the same $((P, S))$ configuration, so cross-message confidentiality fails completely.

The algebraic failures in Section 4 therefore give us three non-negotiable design constraints: (i) no reusable or linearly related mask may ever be applied across distinct images or blocks; (ii) secrecy must not depend on keeping a fixed permutation structure hidden; and (iii) any “chaotic” component must be treated purely as a pre- or post-processing layer, not as the source of cryptographic guarantees. Section 5 translates these constraints into concrete parameter-derivation rules and a revised permutation design and Section 6 then embeds this permutation within an AEAD-based construction that cleanly separates compression, permutation and authenticated encryption.

5. OptiSecure-3D-H Construction

5.1 Design principles

OptiSecure-3D-H separates compression, reversible permutation and cryptographic protection. The SAE reduces representation size; a nonce-derived 3D map optionally changes spatial arrangement; AES-GCM supplies confidentiality and integrity under NIST SP 800-38D [14]. HKDF supplies domain-separated subkeys [16]. AEAD processing follows the interface model in RFC 5116 and the formal separation of plaintext, ciphertext, nonce and associated data [15], [18].

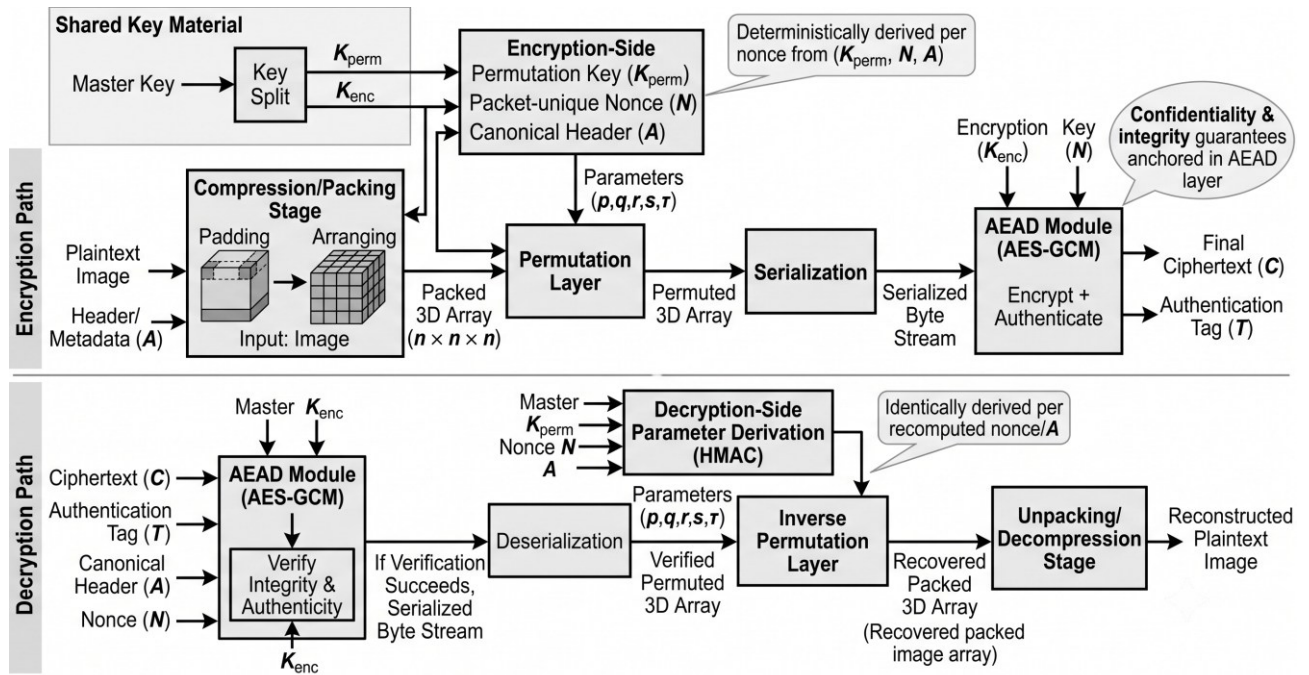


Figure 1. High-level OptiSecure-3D-H processing pipeline.

5.2 Notation and keys

Table 3. Principal notation.

Symbol	Meaning
K	256-bit master secret retained in a protected keystore.
Sdev	Non-secret installation salt stored with the key record.
K _{perm} , K _{aead}	32-byte permutation and AEAD subkeys derived by HKDF.
N	Fresh 96-bit nonce, unique for each packet under K _{aead} .
H, A	Packet header and its canonical byte encoding used as associated data.
Z, M	Real-valued latent tensor and deterministic quantized byte string.
P π , P π^{-1}	Forward and inverse nonce-derived permutations.
C, T	Ciphertext and 128-bit authentication tag.

Key separation is performed once per key record:

$$PRK = HKDF - Extract(Sdev, K), \quad (3)$$

$$K_{perm} = HKDF - Expand(PRK, "OptiSecure - 3D - H/perm", 32), \quad (4)$$

$$K_{aead} = HKDF - Expand(PRK, "OptiSecure - 3D - H/aead", 32). \quad (5)$$

The labels, protocol version and lengths are fixed ASCII or canonical binary values. They MUST NOT be replaced by ambiguous language-dependent strings. AES permits 256-bit keys under FIPS 197 [13].



5.3 Compressor and serialization

The encoder produces $Z = \text{Enc}\theta(I)$. A deterministic quantizer Q and canonical serializer convert Z to M . The header records the compressor model identifier, quantizer identifier and parameters original dimensions, latent dimensions, color representation, padding length, protocol version, sender identifier and sequence number. The exact SAE architecture is an implementation profile, not a cryptographic parameter. A receiver MUST reject an unknown model identifier rather than silently substitute a different decoder.

For a lossy SAE, $\text{Dec}\theta(Q^{-1}(M))$ reconstructs an approximation of I . Consequently, PSNR and SSIM measure compression–reconstruction fidelity, not encryption strength [22], [23]. Model cards and dataset documentation provide useful reporting structures for the trained compressor and its data provenance [29], [30].

5.4 Nonce-derived 3D permutation

Pad M deterministically to a cubic array B of side n , where n^3 is at least $|M|$. The padding length is authenticated in H . Compute $D = \text{HMAC} - \text{SHA} - 256(K_{\text{perm}}, \text{label} \parallel N \parallel A)$, expand D as necessary with counter-mode HMAC and parse unbiased integers p, q, r, s and a positive round count τ . Rejection sampling avoids modulo bias when bounded values are required.

One convenient integer matrix family is

$$A_3(p, q, r, s) = [[1, p, 0], [q, pq + 1, 0], [r, s, 1]], \det(A_3) = 1. \quad (6)$$

Its integer inverse is

$$A_3^{-1} = [[pq + 1, -p, 0], [-q, 1, 0], [-pqr + qs - r, pr - s, 1]]. \quad (7)$$

Because the determinant is one, the matrix is invertible modulo every positive n . For each coordinate vector $v = (x, y, z)^T$, the forward and inverse rounds are

$$v' = A_3 v \bmod n, v = A_3^{-1} v' \bmod n. \quad (8)$$

Apply τ rounds to obtain π and reorder bytes accordingly. This permutation may improve diffusion of local latent structure and preserve continuity with 3D-map research [2], [3], but it is not assigned independent cryptographic strength. Security remains conditional on AEAD and correct key/nonce handling.

Using HMAC over the fixed label, nonce (N) and canonical header (A) ensures that the permutation parameters are uniquely tied to each packet, remain unpredictable to an adversary without (K_{perm}) and avoid modulo bias through rejection sampling.

5.5 Authenticated packet

Serialize the header canonically as A . Encrypt the permuted byte string $M' = P\pi(M)$ using AES-256-GCM with Kead, nonce N and associated data A . The transmitted packet is $H \parallel N \parallel C \parallel T$. The recommended tag length is 128 bits; truncation is not used in this profile.



Table 4. Canonical packet profile.

Field	Status	Required contents / validation
H	Authenticated, not encrypted	Version, algorithms, model/quantizer IDs, dimensions, padding, sender ID, sequence.
N	Public, unique	96-bit value unique under Kaead; checked against sender policy.
C	Encrypted and authenticated	Permuted serialized latent bytes.
T	Authentication output	128-bit GCM tag; constant-time verification.

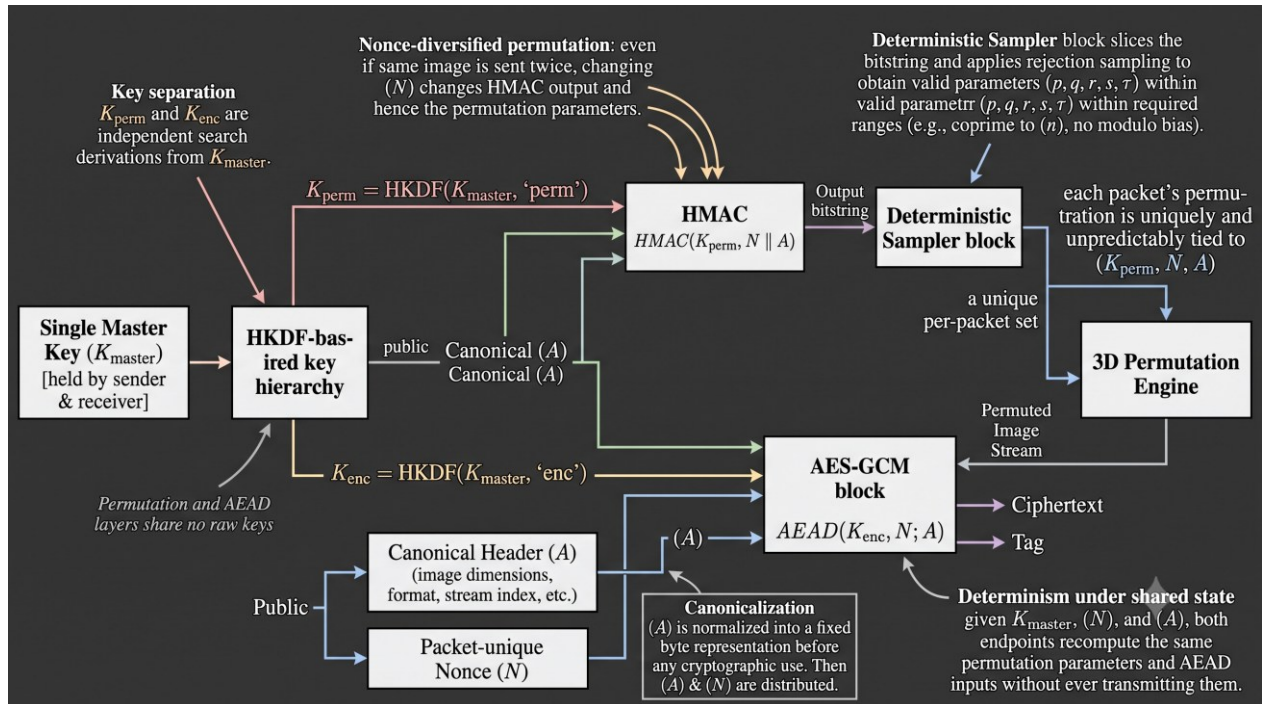


Figure 2. Packet structure and authenticated header fields in OptiSecure-3D-H.

6. Algorithms

6.1 Encryption

Input: image I , frozen encoder $Enc\theta$, key record ($K, Sdev$), fresh nonce N , metadata H

- 1 Validate input dimensions and select the registered compressor profile.
- 2 $Z \leftarrow Enc\theta(I); M \leftarrow \text{Serialize}(Q(Z))$; update H with dimensions, IDs and padding.
- 3 $A \leftarrow \text{CanonicalEncode}(H)$; derive K_{perm} and K_{aead} using (3)–(5).
- 4 $d \leftarrow \text{HMAC} - \text{SHA} - 256(K_{perm}, \text{"map"} \parallel N \parallel A)$; derive p, q, r, s, τ without modulo bias.
- 5 $M' \leftarrow P\pi(M)$ using (6)–(8).
- 6 $(C, T) \leftarrow \text{AES} - 256\text{-GCM-Encrypt}(K_{aead}, N, A, M')$.
- 7 Return packet $H \parallel N \parallel C \parallel T$; commit N /sequence state atomically.



Nonce allocation and packet emission MUST be atomic: after a crash or retransmission, a sender must not reuse a nonce with a different plaintext under the same K_{ae}. If robust uniqueness cannot be engineered, the AES-GCM-SIV profile in RFC 8452 is preferable because it is designed to reduce the consequences of accidental nonce reuse [17].

6.2 Decryption

Input: packet $H \parallel N \parallel C \parallel T$, key record (K, S_{dev}) , registered decoder Dec_{θ}

- 1 Parse fixed-size fields; validate version, lengths, dimensions, IDs and resource limits.
- 2 $A \leftarrow CanonicalEncode(H)$; derive K_{perm} and K_{ae} using (3)–(5).
- 3 $M' \leftarrow AES - 256\text{-GCM-Decrypt}(K_{ae}, N, A, C, T)$.
- 4 If authentication fails: erase intermediates, return one generic error and stop.
- 5 Check replay state; derive p, q, r, s, τ from $HMAC(K_{perm}, "map" \parallel N \parallel A)$.
- 6 $M \leftarrow P\pi^{-1}(M')$; verify and remove authenticated padding.
- 7 $Z \leftarrow Q^{-1}(Deserialize(M)); \hat{I} \leftarrow Dec_{\theta}(Z); return \hat{I}$.

Verification precedes inverse permutation and neural decoding. This order prevents attacker-controlled unauthenticated bytes from reaching complex parsing or model code. Implementations should use constant-time tag verification, uniform errors, bounded allocations and zeroization of temporary key material where the platform permits.

7. Security Analysis

This section returns to the central claim of the paper: that fixed-mask OptiSecure-3D is structurally insecure because deterministic mask reuse enables algebraic cancellation under the threat model of Section 3 and that OptiSecure-3D-H eliminates this class of failures by replacing ad-hoc masking with nonce-diversified AEAD and disciplined key/nonce handling. Sections 5 and 6 defined how permutation parameters and AEAD keys are derived and applied; here we make explicit how those choices block the attacks from Section 4 and what security properties are obtained under the stated assumptions.

7.1 Confidentiality and cross-message separation

Section 7.1 first shows how the OptiSecure-3D-H parameter derivation breaks the algebraic structure exploited in Section 4, ensuring that no reusable mask or fixed permutation remains available to an adversary. Under the standard security assumptions for AES-GCM and provided that nonces are unique under K_{ae}, plaintext confidentiality no longer depends on secrecy of the 3D matrix, DE objective, SAE architecture or image statistics [14], [15]. Because each packet uses a fresh nonce and derives an independent permutation and AEAD key context, the algebraic cancellation in (2) no longer applies across messages.

7.2 Integrity and metadata binding

GCM authenticates both C and A. Any modification to model ID, dimensions, padding, sequence number, ciphertext or tag causes verification failure except with the bounded forgery probability associated with the AEAD security limit. Implementers must observe the key and data-volume limits applicable to their GCM library and deployment [14]. A successful tag is necessary before



allocation-intensive decoding, but applications must still enforce conservative dimension and packet-size limits. This per-packet nonce and key diversification prevent any reuse of a fixed mask across messages, so the structural attack in (2) cannot be mounted against OptiSecure-3D-H under the stated assumptions.

7.3 Replay and nonce discipline

A unique nonce prevents dangerous reuse but does not prove packet freshness. The authenticated sender and sequence fields support replay detection when the receiver stores acceptance state. Random 96-bit nonces can be used only with a collision-risk analysis and key-rotation policy; a persistent counter or a sender-unique prefix plus counter is easier to audit. Nonce reuse under GCM is a protocol failure, not an image-quality degradation.

7.4 Role of chaos metrics

These metrics are therefore treated strictly as supplementary behavior checks; they play no role in the formal confidentiality or integrity argument, which depends solely on the AEAD construction and the associated key/nonce discipline.

7.5 Claim boundaries

Table 5. *Explicit boundaries on security and performance claims.*

Claim	Status in this manuscript
The repeated fixed-mask form is unsafe	Established algebraically by (1)–(2).
The 3D matrix is invertible modulo n	Established by $\det(A_3)=1$ and explicit inverse (7).
Header/ciphertext tampering is detected	Conditional on correct AES-GCM implementation and key/nonce rules.
Replay is prevented	Only when receiver replay state and authenticated sequence numbers are used.
The method is faster than alternatives	Not claimed; requires same-platform benchmark data.
The SAE preserves diagnostic or perceptual content	Not claimed; requires dataset-specific PSNR/SSIM and task evaluation.
The chaotic layer is not relied upon for cryptographic security;	it is outside the claimed security guarantees

8. Reproducible Evaluation Protocol

A future empirical version should pre-register the following protocol. The goal is to evaluate engineering cost and compression quality without using image statistics as substitutes for cryptographic evidence. Dataset provenance, split hashes, model configuration, optimization settings, source revision, environment and raw outputs must be archived.

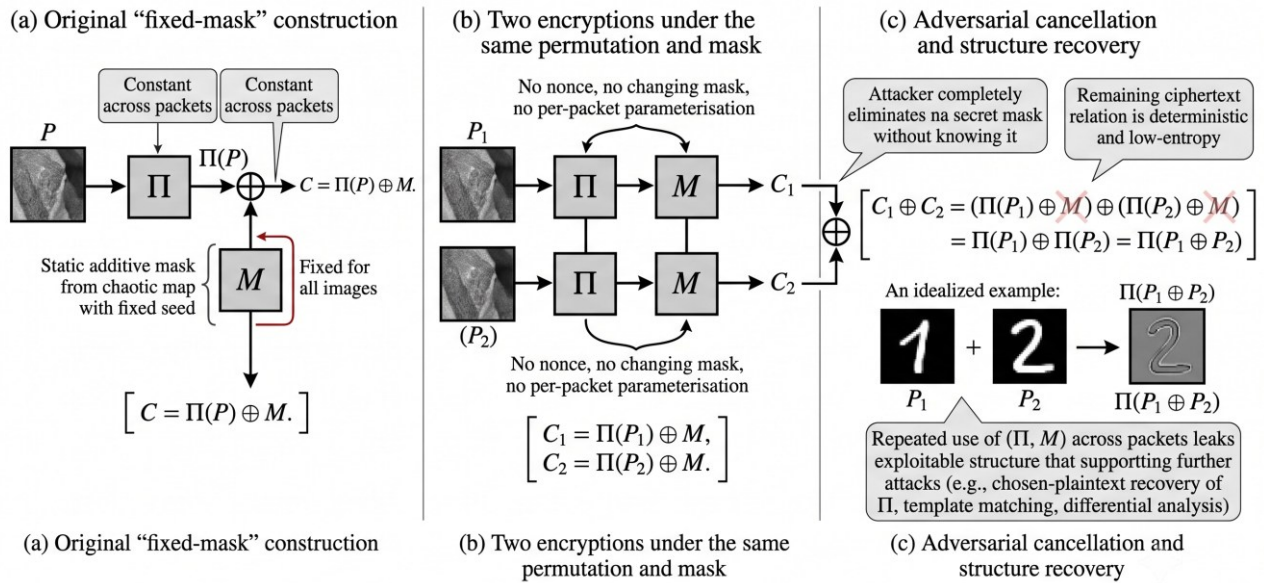


Figure 3. Algebraic failure of fixed-mask image encryption under mask reuse.

Figure 3. Algebraic weakness of fixed-mask image encryption: when the same permutation and static mask are reused, XORing two ciphertexts cancels the mask and yields a permuted difference image $(\Pi(P_1 \oplus P_2))$, exposing exploitable structure and demonstrating structural insecurity under multi-ciphertext observation.

8.1 Data and model disclosure

- List every dataset, version, license, image identifier, checksum, color space, resolution policy and exclusion rule. Publish the exact train/validation/test manifest.
- Disclose every encoder/decoder layer, tensor shape, activation, quantizer, loss, optimizer, learning rate, batch size, epoch limit, random seed, checkpoint rule and model hash.
- Disclose DE population size, mutation strategy and factor, crossover rate, generation limit, parameter bounds, objective normalization, objective weights, data partition, seed and stopping rule.
- Freeze the compressor and DE-selected engineering parameters before the held-out test set is opened. Never optimize entropy or correlation on the reported test images.

8.2 Cryptographic conformance

- Use published AES-GCM and HKDF known-answer tests, plus round-trip tests for every supported tensor shape.
- Test one-bit modifications independently in H, N, C and T; every modified packet must fail without producing a decoded image.
- Generate at least the maximum operational packet count in a nonce-state test and confirm no duplicate under a key record.



- Test restart, rollback, retransmission, counter exhaustion, key rotation, unknown model IDs, oversized dimensions, malformed padding and replay-window behavior.
- Use property-based tests to verify $P\pi^{-1}(P\pi(M)) = M$ for random dimensions, parameters, round counts and byte strings.

8.3 Quality, size and speed

Report PSNR and SSIM between the original image and the authenticated-decryption reconstruction, stratified by dataset and compression ratio [22], [23]. Report total packet size, latent payload size, header and tag overhead and decoder failure rate. Timing must be end-to-end and stage-resolved: encoding, quantization/serialization, permutation, AEAD, inverse processing and decoding.

Table 6. Minimum evidence required before quantitative claims are introduced.

Category	Minimum report
Platform	CPU/GPU model, memory, OS, library versions, compiler/interpreter, thread count.
Timing	Warm-up, number of images, repetitions, clock method, mean, SD, median, p95, confidence interval.
Quality	PSNR, SSIM, compression ratio, per-dataset distributions, failure cases.
Security conformance	Known-answer tests, tamper rejection, replay tests, nonce audit, parser limits.
Statistics (supplementary)	Entropy, local entropy, NPCR/UACI with critical tests, correlations; no standalone security claim.
Reproducibility	Code commit, configuration, seeds, raw CSV, environment lockfile, figure-generation scripts.

Comparative speedups are valid only when all baselines are executed on the same hardware, software stack, image set, resolution, color representation and timing boundary. Values copied from unrelated papers must remain a literature summary rather than being converted into a percentage speedup.

9. Limitations and Deployment Considerations

OptiSecure-3D-H does not hide packet length, dimensions, sender identity, timing or traffic volume. Lossy compression may be unsuitable for applications requiring exact reconstruction and domain shift may degrade SAE outputs. Authenticated encryption cannot compensate for a compromised endpoint, weak random-number source, leaked master key, unsafe model loader or side-channel leakage. The optional 3D permutation increases implementation complexity and therefore requires tests demonstrating that its engineering value exceeds its cost.

The construction has not been accompanied here by new measured throughput, energy, PSNR, SSIM or embedded-device results. This technical note therefore confines its contribution to a protocol-level hardening and evaluation protocol; any future submission claiming performance benefits must treat Section 8 as a minimum evidentiary baseline.



10. Conclusion

The main weakness of deterministic latent permutation followed by a reusable XOR mask is structural: repeated masking permits cancellation and equivalent-key recovery regardless of favorable image statistics. OptiSecure-3D-H retains compression and optional nonce-diversified 3D permutation but assigns confidentiality and integrity to a standards-based AEAD layer. HKDF-separated keys, a fresh nonce, authenticated metadata, fail-closed verification and replay state provide a clearer and auditable security boundary. The specification, algorithms, figures and evaluation protocol make the redesigned method implementable without overstating what has been empirically demonstrated.

Declarations

Ethics approval: Not applicable to the protocol-level analysis presented in this blinded manuscript; confirm against the target journal and any future dataset use.

Data and code availability: No new experimental dataset or measured result is reported. An implementation and raw benchmark package should accompany any empirical revision.

Author contributions, funding, acknowledgments and competing interests: supplied separately with the non-blinded title page and journal forms.

References

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
- [2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998, doi: 10.1142/S021812749800098X.
- [3] G. Chen, Y. Mao and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solitons Fractals*, vol. 21, no. 3, pp. 749–761, 2004, doi: 10.1016/j.chaos.2003.12.022.
- [4] G. Álvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006, doi: 10.1142/S0218127406015970.
- [5] K. J. Persohn and R. J. Povinelli, "Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation," *Chaos Solitons Fractals*, vol. 45, no. 3, pp. 238–245, 2012, doi: 10.1016/j.chaos.2011.12.006.
- [6] H. Wen and Y. Lin, "Cryptanalyzing an image cipher using multiple chaos and DNA operations," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 7, 2023.
- [7] A. Tiwari, P. Diwan, T. D. Diwan, M. Miroslav and S. P. Samal, "A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication," *Sci. Rep.*, vol. 15, art. 14151, 2025, doi: 10.1038/s41598-025-95995-8.
- [8] R. Storn and K. Price, "Differential evolution A simple and efficient heuristic for global optimization over continuous spaces," *J. Global Optim.*, vol. 11, pp. 341–359, 1997, doi: 10.1023/A:1008202821328.



- [9] I. Goodfellow, Y. Bengio and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016, ch. 14.
- [10] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” in Proc. 3rd Int. Conf. Learning Representations (ICLR), 2015.
- [11] X. Glorot and Y. Bengio, “Understanding the difficulty of training deep feedforward neural networks,” in Proc. 13th Int. Conf. Artificial Intelligence and Statistics, vol. 9, 2010, pp. 249–256.
- [12] L. Prechelt, “Early stopping but when?” in Neural Networks: Tricks of the Trade, G. B. Orr and K.-R. Müller, Eds. Berlin, Germany: Springer, 1998, pp. 55–69, doi: 10.1007/3-540-49430-8_3.
- [13] National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” FIPS 197-upd1, May 2023, doi: 10.6028/NIST.FIPS.197-upd1.
- [14] M. Dworkin, “Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC,” NIST Special Publication 800-38D, Nov. 2007, doi: 10.6028/NIST.SP.800-38D.
- [15] D. McGrew, “An interface and algorithms for authenticated encryption,” RFC 5116, Jan. 2008, doi: 10.17487/RFC5116.
- [16] H. Krawczyk and P. Eronen, “HMAC-based Extract-and-Expand Key Derivation Function (HKDF),” RFC 5869, May 2010, doi: 10.17487/RFC5869.
- [17] S. Gueron, A. Langley and Y. Lindell, “AES-GCM-SIV: Nonce misuse-resistant authenticated encryption,” RFC 8452, Apr. 2019, doi: 10.17487/RFC8452.
- [18] P. Rogaway, “Authenticated-encryption with associated-data,” in Proc. 9th ACM Conf. Computer and Communications Security, 2002, pp. 98–107, doi: 10.1145/586110.586125.
- [19] A. Rukhin et al., “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” NIST Special Publication 800-22 Rev. 1a, Apr. 2010, doi: 10.6028/NIST.SP.800-22r1a.
- [20] Y. Wu, J. P. Noonan and S. S. Agaian, “NPCR and UACI randomness tests for image encryption,” J. Sel. Areas Telecommun., pp. 31–38, Apr. 2011.
- [21] Y. Wu, Y. Zhou, G. Saveriades, S. S. Agaian, J. P. Noonan and P. Natarajan, “Local Shannon entropy measure with statistical tests for image randomness,” Inf. Sci., vol. 222, pp. 323–342, 2013, doi: 10.1016/j.ins.2012.07.049.
- [22] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, 2004, doi: 10.1109/TIP.2003.819861.
- [23] A. Horé and D. Ziou, “Image quality metrics: PSNR vs. SSIM,” in Proc. 20th Int. Conf. Pattern Recognition, 2010, pp. 2366–2369, doi: 10.1109/ICPR.2010.579.
- [24] B. Ge et al., “Secure and fast image encryption algorithm using hyper-chaos-based key generator and vector operation,” IEEE Access, vol. 9, pp. 137635–137654, 2021.



- [25] J. Choi and N. Y. Yu, “Secure image encryption based on compressed sensing and scrambling for internet-of-multimedia things,” *IEEE Access*, vol. 10, pp. 10706–10718, 2022.
- [26] H. Wen, Y. Huang and Y. Lin, “High-quality color image compression-encryption using chaos and block permutation,” *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, art. 101660, 2023.
- [27] W. Feng et al., “Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding,” *IEEE Access*, vol. 9, pp. 145459–145470, 2021.
- [28] H. Kiya, “Progress and challenges in compressible and learnable image encryption for privacy-preserving image encryption and machine learning,” in *Proc. 12th Int. Conf. Knowledge and Smart Technology*, 2020, p. XV, doi: 10.1109/KST48564.2020.9059423.
- [29] M. Mitchell et al., “Model cards for model reporting,” in *Proc. Conf. Fairness, Accountability and Transparency*, 2019, pp. 220–229, doi: 10.1145/3287560.3287596.
- [30] T. Gebru et al., “Datasheets for datasets,” *Commun. ACM*, vol. 64, no. 12, pp. 86–92, 2021, doi: 10.1145/3458723.