

Paper Type: Correction

Correction to: An Enhanced Hybrid Video Encryption Scheme Using Sine-Transformed 3D ILM and AES-GCM

Worud Mahdi Saleh 

General Directorate of Diyala Education, Ministry of Education, Diyala, Iraq.

Correspondence: worud.m.saleh@alsalam.edu.iq

Published online: 15 October 2026

Correction to: Neutrosophic Optimization and Intelligent Systems (2026), Volume 11, pp. 26–36. <https://doi.org/10.61356/j.nois.2026.11669>

The published article contains discrepancies between numerical values stated in its abstract and those reported in its tables, inaccurate technical terminology, and statements that exceed the evidence presented. With the author's authorization, the following corrections and clarifications are issued to ensure an accurate and appropriately qualified publication record.

1 | Numerical Corrections

The summary values below are derived from Tables 3–5 of the original article. The corrected entropy, NPCR, and UACI means are the arithmetic means of the three video-sequence values reported in the corresponding tables. The processing-time means and standard deviations are reproduced from Table 5; the original experimental runs were not available for independent reanalysis.

Quantity	Published abstract	Corrected value / interpretation
Mean ciphertext entropy	7.9997	7.9995 (from Table 3)
Mean NPCR	99.61%	99.6172% (from Table 4)
Mean UACI	45.33%	33.4662% (from Table 4)
Mean encryption time	29 ms per frame	28.30 ± 0.95 ms per 720p frame (Table 5)
Mean decryption time	Not stated	28.90 ± 1.02 ms per 720p frame (Table 5)
Frame-rate claim	“exceeding 35 FPS” from 29 ms	$1000/28.30 \approx 35.34$ FPS as the reciprocal of the reported mean encryption time only; not measured end-to-end video throughput



Corresponding Author: worud.m.saleh@alsalam.edu.iq



<https://doi.org/10.61356/j.nois.2026.12680>



Licensee **Neutrosophic Optimization and Intelligent systems**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

2 | Technical terminology and scientific interpretation

The expression “128-slice authentication tag” in the abstract is corrected to “128-bit GCM authentication tag,” consistent with the description in Section 3.3 of the original article. The expressions “periodic non-lawless fenestella’s,” “perfectly uniform pseudo-random sequences,” and “strongest attainable protection” are withdrawn because they are technically unclear or unsupported as stated.

In Section 3.1, the assertion that applying a sine transformation and reduction modulo 1 guarantees uniform output distribution is replaced by the clarification that such operations do not, by themselves, prove uniformity, cryptographic unpredictability, or the absence of periodic behavior.

In Sections 3.2–3.6, references to a 96-bit AES-GCM initialization vector describe its specified length but do not establish that a unique nonce is guaranteed for each encryption under the same key. Likewise, nonce length and authentication tags alone do not establish replay resistance. Secure use of AES-GCM requires correct key and nonce management and verification of the authentication tag; the published description does not independently demonstrate these implementation properties.

In Sections 4.2–4.4, the reported chi-square statistics, entropy, NPCR, and UACI are descriptive results for the tested frames. Their values do not, on their own, demonstrate resistance to all statistical, differential, chosen-plaintext, or other cryptanalytic attacks. In particular, the corrected UACI value replaces the inconsistent abstract figure without creating a new experimental result.

In Sections 4.5 and 5, the reported mean encryption time is corrected to 28.30 ± 0.95 ms per 720p frame. Its reciprocal is approximately 35.34 frames per second for the measured encryption operation, without accounting for all stages of an end-to-end streaming system. Accordingly, claims of demonstrated throughput in ultra-high-definition or multi-stream deployment are withdrawn; those operating conditions were not evaluated in the reported experiments.

3 | Corrected Abstract

This study examines a hybrid video-encryption approach combining a Sine-Transformed Three-Dimensional Improved Logistic Map (ST-3D-ILM) with the Advanced Encryption Standard in Galois/Counter Mode (AES-GCM). The proposed architecture uses a chaos-based mechanism to derive per-frame cryptographic inputs and AES-GCM to provide authenticated encryption of video-frame data. The article reports an experimental evaluation involving three video sequences—Foreman, Akiyo, and Coastguard—processed at a resolution of 1280×720 pixels. According to the published results tables, the mean ciphertext information entropy is 7.9995, the mean Number of Pixels Change Rate (NPCR) is 99.6172%, and the mean Unified Average Changing Intensity (UACI) is 33.4662%. The reported encryption and decryption times are 28.30 ± 0.95 ms and 28.90 ± 1.02 ms per 720p frame, respectively. These measurements describe the observed statistical properties and processing times of the reported implementation under the stated test conditions. They do not independently establish cryptographic security, correct nonce management, resistance to all attack models, or end-to-end performance in higher-resolution deployments. Further implementation-level validation is needed before such conclusions can be drawn.

4 | Scope and record of the correction

This notice corrects numerical reporting, terminology, and the interpretation of the original article’s published findings. The corrected summary statistics are calculated from values already present in the article; no new measurements, experiments, or independent validation of its cryptographic implementation are introduced. Claims of comprehensive security and wider deployment performance that were not established by the reported tests should not be relied upon. The original article should be read together with this correction notice.

References

- [1] Dworkin, M. J. (2007). Sp 800-38d. recommendation for block cipher modes of operation: Galois/counter mode (gcm) and gmac. National Institute of Standards & Technology. <https://doi.org/10.6028/NIST.SP.800-38D>

The original article can be found online at <https://doi.org/10.61356/j.nois.2026.11669>

Disclaimer/Publisher's Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.