



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.935

Volume 15, Issue 10, October 2026

ShadowPost: A Delivery-Survivability Benchmark for Native-JPEG DCT Steganography

**Rajshri Pote, Arman Rizwan Khan, Aditya Shakya, Divyani Dinkar Waikar, Aryan Manoj Terha,
Shreya Kamlesh Prasad**

Department of Computer Science and Engineering, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

ABSTRACT: Platform image processing can invalidate a steganographic payload even when the embedding algorithm is correct. This paper presents ShadowPost, an end-to-end native-JPEG DCT steganography system with AES-256-GCM encryption, RS(48,32) error correction, native luminance-coefficient embedding, and a platform-aware preprocessing layer. The quantitative evaluation focuses on delivery survivability: 270 trials representing six delivery modes across five platforms, supplemented by offline analysis of retained stego artifacts and controlled transformations. Exact recovery was 45/45 for Discord attachments, 45/45 for WhatsApp documents, 36/45 for Telegram sendPhoto, and 0/45 for the tested X, Instagram, and standard WhatsApp image paths. The current adaptive implementation was subsequently tested on representative cases across the supported platform profiles, but these later checks did not follow the original 45-trial protocol and are therefore not reported as a second quantitative benchmark. The reported benchmark results characterize the tested account, client, and date configurations rather than the platforms universally. Together, these results provide a reproducible baseline for separating delivery-channel failure from robustness to controlled coefficient perturbations and motivate controlled evaluation of synchronization-aware adaptive methods.

KEYWORDS: Image steganography, JPEG DCT, Reed-Solomon, AES-GCM, platform recompression, delivery survivability

I. INTRODUCTION

A JPEG stego image is not delivered unchanged by many modern services. Upload pipelines may decode pixels, resample images, quantize frequency coefficients, and encode a new JPEG. These operations can be damaging to methods that assume a stable 8×8 block grid. A useful system therefore needs both a robust embedding representation and measurements taken after real delivery.

ShadowPost addresses this problem as an end-to-end pipeline. The message is authenticated and encrypted before embedding; an error-correcting code provides bounded correction; and hidden bits are represented by ordering pairs of native JPEG DCT coefficients. This study focuses on the delivery layer: how much of the encoded message remains recoverable after transmission through six practical channels.

II. RELATED WORK AND DESIGN POSITION

Digital steganography has historically been evaluated through imperceptibility, payload capacity, and resistance to statistical detection. Recent surveys emphasize the trade-off among payload, imperceptibility, robustness, and detectability [1], [2]. JPEG-domain work studies the behavior of quantized DCT coefficients under compression and their use in robust embedding [3]. Social-network image studies show that service-side manipulation can materially alter JPEG media after upload [4]. The JPEG syntax used here follows ITU-T T.81 [5].

Robustness claims depend on the distortion model. A method that survives a quality-factor change may fail after resizing, cropping, color conversion, or decode-and-reencode processing. Consequently, laboratory recompression at a known quality factor is not equivalent to uploading a file to a live service and decoding the derivative returned to a recipient.

Robust steganography increasingly models the delivery channel explicitly [6], [7], [8]. Zeng et al. minimize channel errors in online-social-network delivery, while Qiao et al. improve cover-element selection using post-processing analysis [9], [10]. Shang et al. learn robustness to JPEG compression in an invertible-neural-network framework; Pan et al. model DCT-coefficient correlations with a pairwise conditional random field; and Cheng et al. address pixel-range overflow near spatial-block boundaries and use adaptive error correction [11], [12], [13]. Steganalysis work combines DCT-domain features with learned classifiers [14], [15]. Error-correction strategies are central to robust JPEG steganography [6], [16], [13], but parity does not by itself recover a receiver stream when the decoder is no longer aligned with the embedded representation.

ShadowPost therefore makes a focused research contribution through an empirical delivery-survivability benchmark, while the implemented project extends the benchmarked core with platform-aware pre-conditioning. The benchmark intentionally evaluates the unconditioned baseline so that delivery-induced failure behavior can be characterized independently. The adaptive layer is described as a system extension and was subsequently validated on representative cases, but its effectiveness is not assigned a new recovery percentage without a controlled post-adaptation trial set.

III. SYSTEM DESIGN

Security and framing

A plaintext message is encrypted with AES-256-GCM using a scrypt-derived key [17], [19], [20]. The implementation uses $N=2^{14}$, $r=8$, $p=1$ and a fixed public derivation salt from the Phase 3 experiment. The salt is not secret, but the prototype parameters are not a production password-storage recommendation. The resulting cryptographic object is passed to the formal framing and coding pipeline in Sec. 3.

Native-DCT embedding

ShadowPost reads and writes JPEG coefficient arrays directly in the luminance channel. Each selected coefficient position pair encodes one bit by magnitude ordering. The finalized pair set is (1,3) vs. (2,2) and (1,4) vs. (4,1); the two selected pairs per block therefore provide 2B bits for B luminance DCT blocks. Extraction uses the deterministic tie rule $|A| \geq |B|$, so the decoder remains reproducible at zero or equal coefficients. This design follows the native JPEG representation defined by ITU-T T.81.

Formal pipeline and capacity

The complete formal pipeline is summarized in Fig. 3. The capacity model explains why a payload that fits the original cover may fail after delivery transformation. Let M be the plaintext message. ShadowPost first derives a 256-bit key K from a passphrase using scrypt:

$$\text{passphrase} \rightarrow \text{scrypt} \rightarrow K$$

AES-GCM then produces ciphertext C and authentication tag T using a fresh 96-bit nonce N :

$$(C, T) = \text{AES-GCM}_K(M, N)$$

The framed container is $L||N||C||T$, where L is a two-byte plaintext length field. The framed byte stream is partitioned into data blocks D_i of 32 bytes and encoded as 48-byte Reed–Solomon codewords:

$$\text{Length}(D_i) = 32 \text{ bytes}; D_i \rightarrow \text{RS}(48,32) \rightarrow W_i; \text{Length}(W_i) = 48 \text{ bytes}$$

With bounded symbol errors, parity permits correction. When the coefficient grid is displaced, however, extracted symbols are samples from a different coordinate system, so RS correction may fail or produce an unauthenticated ciphertext.

For an image with B luminance DCT blocks, the two selected pair positions provide two ordering decisions per block, giving

$$2B \text{ bits}$$

before framing and code overhead. For requested message length m , the number of codewords is

$$\lceil (2 + 12 + m + 16) / 32 \rceil$$

and the encoded requirement is $384 \times [(2 + 12 + m + 16) / 32]$ bits. A payload that fits the original cover may not fit a transformed derivative; that is a capacity failure, not a BER measurement.

Platform-aware adaptive extension

The current ShadowPost application exposes platform profiles for Instagram Feed, Twitter/X, Telegram Photo, Discord Attachment, and WhatsApp Document. For lossy image-delivery paths, the encoder can pre-condition the cover by applying the profile's canvas bounds, optional aspect-ratio crop, 16-pixel dimension alignment, and target JPEG quality before native-DCT embedding. The lossless file-attachment profiles preserve the original canvas and do not apply pre-compression. These mechanisms form part of the implemented system, but the canonical 270-trial dataset was generated with the unconditioned benchmark configuration and is consequently treated as the baseline evaluation.

Subsequent manual validation of the adaptive implementation recovered the embedded payload in representative tests across the supported profiles. Because only a small number of cases were checked after the project update, these observations are presented as implementation validation rather than as a statistically comparable recovery-rate result. A controlled baseline-versus-adaptive benchmark remains future quantitative work.

IV. EVALUATION METHOD

Trial cohorts

The canonical CSV contains 270 rows. Telegram, Discord, and WhatsApp Document use the structured 15-cover matrix with 10-byte, 100-byte, and image-specific near-capacity payloads. X (formerly Twitter), Instagram, and WhatsApp Image each contain 45 fixed 100-byte trials. This distinction is retained because the source datasets do not have identical payload distributions.

Mode	Client/API or workflow	Date (UTC)
Discord	webhook attachment	2026-08-22
Telegram	sendPhoto	2026-08-22
X	manual image post	2026-09-15
Instagram	manual image post	2026-09-15
WA Image	manual image upload	2026-09-15
WA Doc	document upload	2026-09-15

TABLE 1. EXPERIMENTAL CONDITIONS SUPPORTED BY THE REPOSITORY ARTIFACTS.

The recorded delivery conditions are summarized in Table 1.

Metrics and controlled transformations

We report exact recovery rate, Wilson 95% confidence intervals, and bit error rate (BER). BER is computed only when a meaningful aligned bit comparison exists. Trials rejected before delivery have no BER and are excluded from the corresponding mean. The controlled study transforms retained Phase 3 AES-GCM stego JPEGs locally with quality factors 95, 75, and 50, plus two resize and two crop conditions. JPEG-only conditions represent coefficient noise; resize and crop conditions are measured geometric transformations that test the fixed block-grid assumption. The payload-class design is reported in Table 5; the recorded delivery conditions are summarized in Table 1.

Visual quality and artifact analysis

PSNR and SSIM are proxies for visual quality; learned perceptual metrics also exist [18]. Cover-to-stego quality is measured with PSNR and a local RGB SSIM approximation [21]. For retained X and Instagram artifacts, thumbnails are used only to form a one-to-one source/return assignment; source images are resized to returned dimensions before aligned PSNR and SSIM are computed. This is an artifact-level quality analysis, not a row-level join to the canonical CSV. The checked-in pairing artifact records unchanged dimensions for 44/45 X pairs and 42/45 Instagram pairs, so the observed failures cannot be attributed to resizing alone in those pairs. Direct JPEG metadata inspection was not performed because the sent and returned JPEG bytes are not available in the paper-build workspace.

V. RESULTS

The canonical recovery results are summarized in Table 2. Fig. 1 visualizes the six delivery-mode rates.

Mode	Cohort	N	Exact	Rate	95% CI	BER	Terminal class
Discord	15×3	45	45	100.0%	92.1–100.0%	0.0000	success
WA Doc	15×3	45	45	100.0%	92.1–100.0%	0.0000	success
Telegram	15×3	45	36	80.0%	66.2–89.1%	0.0274	capacity / RS
X	45×100 B	45	0	0.0%	0.0–7.9%	n/a	fixed-grid extraction
Instagram	45×100 B	45	0	0.0%	0.0–7.9%	n/a	fixed-grid extraction
WA Image	45×100 B	45	0	0.0%	0.0–7.9%	n/a	fixed-grid extraction

TABLE 2. EXACT RECOVERY RESULTS FROM THE CANONICAL DATASET. BER IS N/A WHEN EXTRACTION FAILS AND ALIGNED COMPARISON IS UNDEFINED.

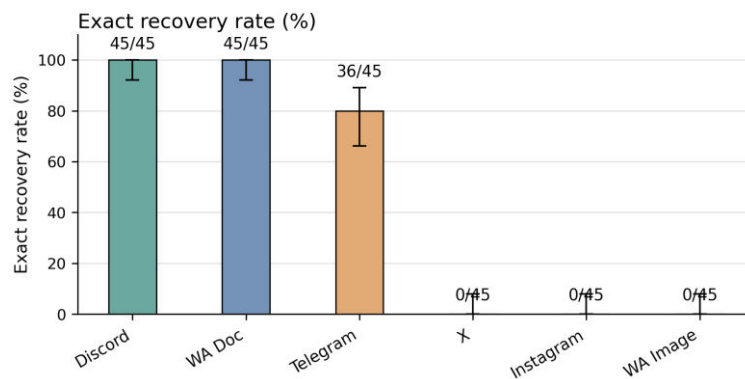


FIG. 1. EXACT RECOVERY RATE BY DELIVERY MODE.

Discord and WhatsApp Document achieved 45/45 exact recoveries with zero recorded BER, consistent with byte-preserving file transfer. Telegram recovered 36/45 messages. Its failures include capacity failures for near-capacity payloads and RS-decode failures; the stored benchmark does not establish resizing as the cause of the latter. X, Instagram, and WhatsApp Image recorded 0/45 exact recoveries; all rows have undefined BER because extraction failed.

Channel analysis

Discord is the strongest channel in this study. All 45 messages were recovered exactly, including near-capacity cases. The zero BER result indicates that the tested attachment path retained the JPEG coefficient stream sufficiently for the native decoder. This does not mean Discord is intrinsically lossless for every client or future policy; it means the tested path did not introduce a transformation that disturbed the selected DCT relationships.

WhatsApp Document also recovered all 45 messages with zero BER. The document mode is evaluated as file transfer rather than ordinary image presentation. The document result should be interpreted together with the image-mode result, not averaged into a generic WhatsApp score: the two modes expose different server behaviors.

Telegram produced 36 exact recoveries out of 45 trials. Its failures separate into three terminal classes: RS decode when aligned BER is measurable and near 0.5, capacity when the requested payload does not fit the delivered grid, and fixed-grid extraction when no aligned stream can be formed. In the canonical CSV, Telegram has two RS-decode failures, seven capacity failures, and no fixed-grid extraction failures. The payload-class breakdown is shown in Table 5 and Fig. 2.

X contains 45 fixed 100-byte trials and recovered no messages. Every failed row is recorded with fixed-grid extraction failure. The result characterizes the tested public image-post path only. Instagram likewise recovered 0/45 fixed 100-byte trials; the stored rows classify the failures as fixed-grid extraction failures; direct JPEG metadata inspection is needed to distinguish recompression, subsampling, resampling, or other transformations. Standard WhatsApp image delivery recovered 0/45 fixed 100-byte trials, contrasting sharply with WhatsApp Document and showing why the media subtype is part of the experimental condition.

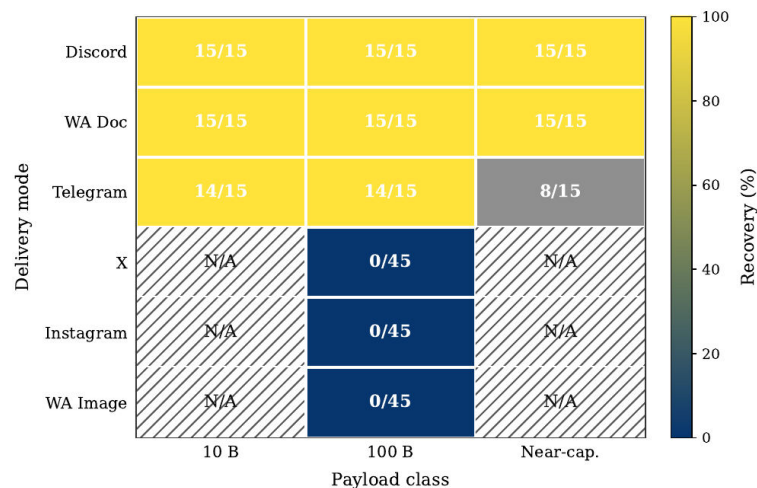


FIG. 2. PAYLOAD MATRIX SHOWING EXACT RECOVERY OVER TOTAL TRIALS; BLANK CELLS ARE N/A BECAUSE THOSE PAYLOAD CLASSES WERE ABSENT FROM THE COHORT DESIGN.

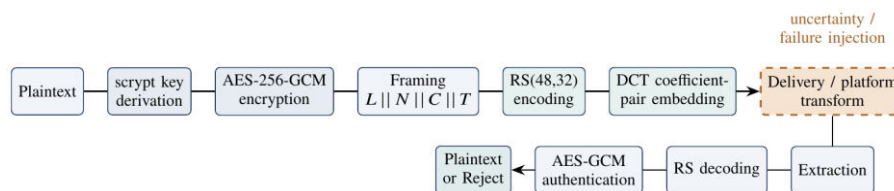


FIG. 3. SHADOWPOST END-TO-END PIPELINE; THE DELIVERY/PLATFORM TRANSFORMATION IS THE UNCERTAIN CHANNEL STAGE.

VI. ERROR MODEL AND FAILURE TAXONOMY

The benchmark uses four operational failure classes. A success produces valid extraction, RS decoding, AES-GCM authentication, and exact plaintext equality. A fixed-grid extraction failure is a decoder outcome label meaning that no usable aligned bit stream was extracted; it makes no causal claim about the platform transformation. Reed–Solomon decode and authentication failures remain separate, while capacity failures identify payloads rejected before a meaningful bit comparison. The terminal counts are reported in Table 3 and visualized in Fig. 4.

Mode	Success	Grid	RS	Capacity	Auth.
Discord	45	0	0	0	0
WA Doc	45	0	0	0	0
Telegram	36	0	2	7	0
X	0	45	0	0	0
Instagram	0	45	0	0	0
WA Image	0	45	0	0	0

Table 3. Failure taxonomy counts generated from the canonical CSV.

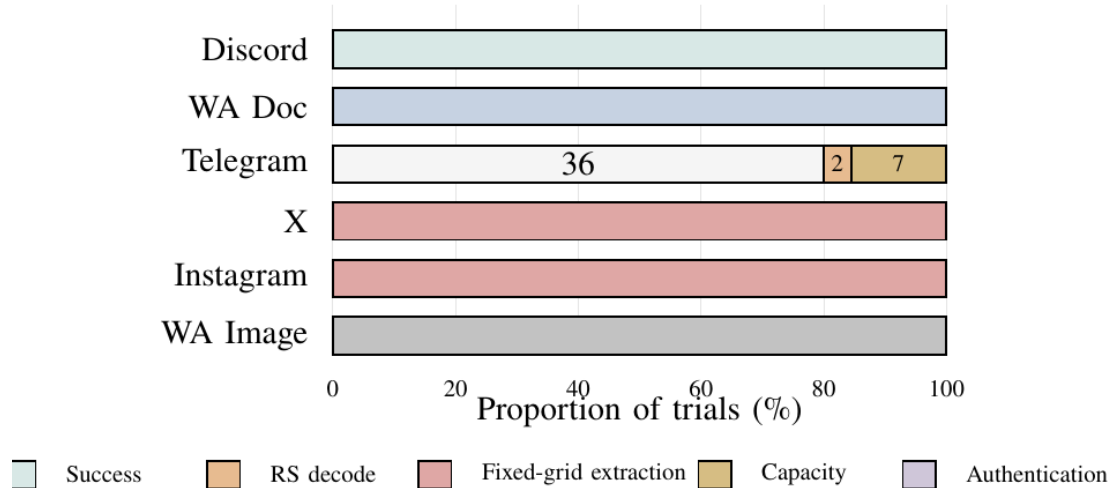


FIG. 4. FAILURE TAXONOMY BY DELIVERY MODE. TELEGRAM CONTAINS 2 REED–SOLOMON DECODE FAILURES AND 7 CAPACITY FAILURES; ALL OTHER NON-SUCCESS TRIALS ARE FIXED-GRID EXTRACTION FAILURES.

A bit error rate is useful only when the decoder can align received bit positions with transmitted positions. Under coefficient perturbation, BER summarizes damage before RS decoding. Under spatial rescaling, the receiver's index refers to a different block than the sender's index, so BER is undefined when extraction fails. The X, Instagram, and WhatsApp Image rows therefore do not have a meaningful BER measurement.

Controlled transform results

The controlled study uses the Phase 3 short payload of 384 bits (48-byte RS codeword) for the offline JPEG-quality study. The controlled study separates coefficient noise from geometric desynchronization. The JPEG-only conditions retain exact recovery for every retained stego image, while every resize and crop condition fails under the current fixed-grid extractor. Table 4 reports the recovery, BER, and aligned-quality values, and Fig. 5 visualizes the same conditions.

Transform	Mechanism	Exact	Rate	BER	Aligned PSNR (dB)	Aligned SSIM
q95	coefficient noise	15/15	100.0%	0.0000	49.1	0.993
q75	coefficient noise	15/15	100.0%	0.0000	39.2	0.967
q50	coefficient noise	15/15	100.0%	0.0003	36.2	0.940
r0.90	geometric desync	0/15	0.0%	0.4880	44.7	0.988
r0.75	geometric desync	0/15	0.0%	0.4915	37.3	0.953
c0.02	geometric desync	0/15	0.0%	0.5036	19.8	0.551
c0.05	geometric desync	0/15	0.0%	0.4967	16.3	0.474

TABLE 4. OFFLINE CONTROLLED-TRANSFORM STUDY ON RETAINED PHASE 3 STEGO JPEGs. RESIZE/CROP ROWS USE THE QUALITY FACTOR SHOWN IN THE ROW NAME.

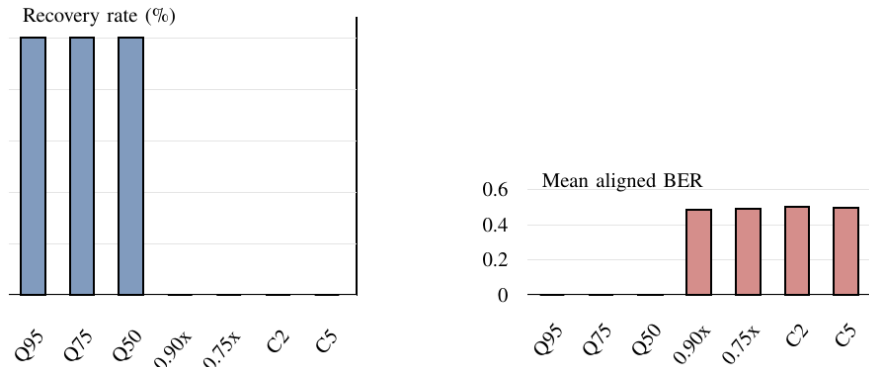


FIG. 5. OFFLINE TRANSFORM STUDY. THE X-AXIS TICK MAPPING IS Q95/Q75/Q50 = Q95/Q75/Q50; 0.90x/0.75x = R0.90/R0.75; C2/C5 = C0.02/C0.05, AS IN TABLE 4.

Capacity and payload robustness

The structured cohort provides three payload classes for Discord, Telegram, and WhatsApp Document. The capacity data are reported in Table 5.

Mode	Payload class	Bytes	Exact	Mean observed BER
Discord	10 B	10	15/15	0.0000
Discord	100 B	100	15/15	0.0000
Discord	near capacity	641–21,569	15/15	0.0000
Telegram	10 B	10	14/15	0.0359
Telegram	100 B	100	14/15	0.0335
Telegram	near capacity	641–21,569	8/15	0.0001
WA Doc	10 B	10	15/15	0.0000
WA Doc	100 B	100	15/15	0.0000
WA Doc	near capacity	641–21,569	15/15	0.0000

TABLE 5. RECOVERY AND OBSERVED BER BY STRUCTURED PAYLOAD CLASS.

Visual quality and artifact pairing

Across the 15 retained cover–stego pairs, the mean cover-to-stego PSNR is 46.6 dB and mean local RGB SSIM is 0.988. The artifact-level pairing summary is reported in Table 6. “Identical” is counted exactly as in `offline_paper_analysis.py`: `stego_to_delivered_psnr` is inf or infinity, meaning the aligned pixel MSE is exactly zero after the source image is resized to the returned dimensions.

Mode	Pairs	Identical	PSNR	SSIM	Width ratio
Instagram	45	37	31.0	0.946	0.971
X	45	41	33.0	0.995	0.989

TABLE 6. RETAINED VISUAL-QUALITY AND ARTIFACT-PAIRING SUMMARY. “IDENTICAL” MEANS INF PSNR, I.E., ZERO ALIGNED MSE AFTER SOURCE RESIZING.

TABLE 7 REPORTS THE ARTIFACT-LEVEL DIMENSION-DATA CAVEAT.

Mode	CSV dims	Artifact pairs	Width ratio	Interpretation
Discord	0	0	–	no CSV dimensions
Telegram	0	0	–	no CSV dimensions

Mode	CSV dims	Artifact pairs	Width ratio	Interpretation
WA Doc	0	0	–	no CSV dimensions
X	0	45	0.989	artifact pairs only
Instagram	0	45	0.971	artifact pairs only
WA Image	0	0	–	no CSV dimensions

TABLE 7. DIMENSION-DATA COVERAGE AND ARTIFACT-LEVEL PAIRING CAVEAT.

The checked-in pairing CSV establishes 41/45 pixel-identical X pairs and 37/45 pixel-identical Instagram pairs; it does not establish byte identity. Because dimensions are unchanged in 44/45 X pairs and 42/45 Instagram pairs, those failures cannot be attributed to resizing alone. Direct JPEG metadata inspection was not performed because the sent and returned JPEG bytes are not available in the paper-build workspace.

Basic detectability screening

The transparent paired coefficient-statistic screen is not a rich-model steganalysis benchmark and is not a security certificate. The four runs in Table 8 all obtain 53.3%, near chance; statistical power is low (n=15 pairs), so this is not evidence of undetectability.

Run	Bits	Cover TN	Stego TP	Balanced acc.
Phase 1 all pairs	512	8/15	8/15	53.3%
Phase 1 0,2	256	8/15	8/15	53.3%
Phase 1 0,2 tie-fixed	256	8/15	8/15	53.3%
Phase 3 AES-GCM	384	8/15	8/15	53.3%

TABLE 8. PAIRED COEFFICIENT-STATISTIC DETECTABILITY SCREEN. ALL FOUR RUNS OBTAIN 53.3%, NEAR CHANCE; THE RESULT IS NOT A SECURITY CERTIFICATE. STATISTICAL POWER IS LOW (N=15 PAIRS).

VII. SECURITY AND PRIVACY ANALYSIS

Confidentiality is provided by AES-GCM rather than visual concealment [19], [20]. An observer who extracts coefficient orderings without the passphrase obtains ciphertext and cannot recover authenticated plaintext under the cryptographic assumptions of AES-GCM and script. The nonce is stored with the ciphertext because it is required for decryption but is not secret.

Integrity is equally important. A platform transformation that changes hidden bits should not silently produce plausible plaintext. GCM authentication rejects modified ciphertext, and the application reports decode failure instead of returning unauthenticated bytes. Reed–Solomon improves availability under bounded corruption but does not replace authentication; corrected data is accepted only after GCM verification.

The system does not claim steganalytic undetectability. Relative coefficient ordering leaves a statistical footprint, and repeated use of the same coefficient positions could be detectable by a sufficiently trained analyst. The evaluated contribution is delivery survivability under known platform transforms, not resistance to a dedicated detector.

A deployment must separate passphrases from media distribution. Operational security therefore depends on key handling, account security, and platform metadata exposure in addition to the DCT payload.

VIII. REPRODUCIBILITY PROCEDURE

The repository contains the encoder/decoder, phase experiments, delivery-mode CSVs, canonical master CSV, and returned media. The returned-media evidence includes downloaded/twitter and downloaded/instagram. A reproduction should preserve the passphrase/message generator and the trial metadata. Downloaded derivatives are evidence files; never re-encode before decoding. The repository README should hold the longer reproduction sequence and environment details.

IX. COMPARISON WITH COMMON DESIGN ALTERNATIVES

Pixel-domain LSB embedding is simple on untouched bitmaps, but JPEG decoding and recompression operate in another representation. Native-DCT embedding aligns the representation with JPEG compression, explaining partial Telegram survival and strong attachment results.

A pure DCT payload without authentication can yield false-positive readable output after bit damage. ShadowPost instead authenticates the encrypted object. Larger error-correcting codes may improve bounded coefficient-noise recovery, but cannot solve arbitrary geometric resampling and also reduce payload capacity; RS(48,32) is therefore a controlled baseline rather than a globally optimal parity rate.

X. LIMITATIONS AND VALIDITY THREATS

The benchmark is limited to the accounts, clients, image files, and dates represented by the stored artifacts. Social platforms can change image processing without notice. A later run may produce different dimensions or quantization behavior, so timestamps and downloaded derivatives are part of the experiment provenance.

The cohorts are intentionally not collapsed into one perfectly balanced design. The structured cohort tests payload scaling; the feed/media cohort tests a repeated 100-byte message under delivery paths that were already known to produce derivatives. This supports a practical channel comparison but does not support a claim that every platform has been evaluated at every payload size.

The offline extension measures sender-side PSNR/SSIM, selected returned-media quality, and a transparent coefficient-statistic screen, but it does not provide a full rich-model detector benchmark, computational latency study, or key-search analysis. Only one embedding method was evaluated, with no baseline method evaluated under the same delivery matrix. It also does not evaluate video, animated media, PNG delivery, or alternative client applications. Returned-media quality joins are artifact-level assignments, and the canonical CSV has zero populated dimension rows; therefore no platform-wide dimension-ratio correlation is claimed.

The Wilson 95% intervals in Fig. 1 are calculated from 45 trials per delivery mode. For the structured Discord, Telegram, and WhatsApp Document cohorts, the 45 trials reuse 15 cover images across three payload classes; therefore, the independence assumption is imperfect and the intervals should be interpreted descriptively. In the canonical CSV, Telegram's nine non-successes comprise two Reed–Solomon decode failures and seven capacity failures, as summarized in Table 3.

XI. DISCUSSION

The results separate payload robustness from channel preservation. RS parity is sufficient for bounded coefficient perturbations in preserved-grid conditions, but the cause of the X, Instagram, and WhatsApp Image failures remains undetermined. JPEG-only quality changes remained recoverable in the offline controlled study, while the tested file-attachment modes preserved the coordinate system and Telegram occupied an intermediate regime with capacity and RS failures. The feed/image paths produced fixed-grid extraction failures, which is a decoder outcome rather than a causal attribution.

The main design opportunity is synchronization. Synchronization-aware pilots, multi-scale registration, or a spatial fallback should be evaluated before increasing RS redundancy. The present paper does not claim such a mitigation has been implemented; it establishes the failure boundary that a mitigation must address. A requirement such as “works on WhatsApp” is underspecified because the document and image paths had opposite outcomes in this dataset.

The benchmark findings motivated the platform-aware preprocessing implemented in the current ShadowPost application. That extension targets known delivery constraints through canvas normalization, 16-pixel alignment, aspect-ratio handling, and target-quality pre-conditioning. Representative manual tests after this implementation successfully recovered payloads across the supported profiles, but those tests were not conducted with the original 45-trial protocol. The present study therefore does not claim a quantitative improvement in recovery rate from the adaptive layer. The current application view of these adaptive profiles is shown in Fig. 6. Figure 6 documents the application interface; promotional wording visible in the screenshot, including “world’s first” and “4.9/5 Reliability,” is not independently validated by the benchmark and is not treated as an experimental finding in this paper.

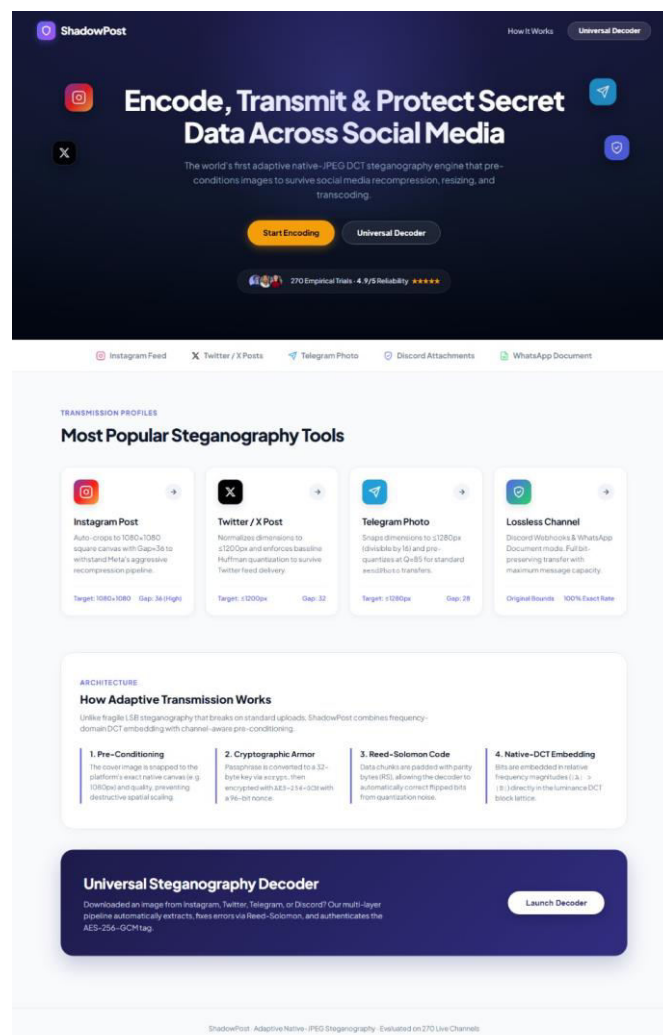


FIG. 6. CURRENT SHADOWPOST ADAPTIVE PLATFORM PROFILES AND THEIR PLATFORM-AWARE PREPROCESSING TARGETS.

XII. CONCLUSION

ShadowPost is a broader adaptive native-JPEG DCT steganography system whose research evaluation in this paper focuses on delivery survivability. Across the canonical 270-trial baseline, exact recovery was 45/45 on Discord attachments, 45/45 on WhatsApp documents, 36/45 on Telegram, and 0/45 on the tested X, Instagram, and WhatsApp image paths. The offline analysis shows that coefficient-level noise can remain recoverable, whereas the cause of the tested feed/image failures remains undetermined. The implemented system additionally provides platform-aware pre-conditioning, which was manually validated on representative cases after the benchmark was completed. Because those later checks did not use the same controlled trial protocol, they are not presented as 45-trial recovery rates. A future controlled baseline-versus-adaptive study would quantify the mitigation effect directly.

Responsible Use.

ShadowPost is intended for authorized research, resilience testing, and defensive evaluation of image-delivery channels. Hidden channels may violate platform terms or applicable policies, so experiments should use accounts, media, and recipients for which the researchers have authorization.

Data Availability. The implementation, canonical benchmark CSV, returned media, and paper-generation artifacts are available in the ShadowPost repository at the canonical benchmark commit [22]. The repository also contains the later adaptive platform profiles and application code; these later implementation changes should not be interpreted as modifications to the historical 270-trial dataset.

APPENDIX A. COVER MANIFEST

retro/preview.jpg; ricepod/preview.jpg; sheep/preview.jpg; shimmering_particles/preview.jpg; techno/preview.jpg.
demon_core/preview.jpg; dna_fragment/preview.jpg; eagleflag/preview.jpg; fantasticcar/preview.jpg;
neon_sunset/preview.jpg;
arsenal/preview.jpg; audiophile/preview.jpg; beach/preview.jpg; corsair_collection/dotted.fabeb454b273c6d2398a.jpg;
deep_space/preview.jpg;

The structured cohort uses these 15 cover identifiers.

APPENDIX B. DATA DICTIONARY

The compact field dictionary is given in Table 9.

Field	Meaning
platform	delivery mode
trial	per-mode sequence number
cover_name	source or returned media filename
payload_size bytes	plaintext length requested by the encoder
cover_width, cover_height, delivered_width, delivered_height	image dimensions when captured; historical manual rows may be empty
success	true only for exact plaintext recovery
ber	measured bit error rate when aligned comparison is available
failure_reason	standardized terminal class
timestamp	trial event time

TABLE 9. COMPACT DATA DICTIONARY.

The canonical master file contains 270 rows, with 45 rows per delivery mode and 126 true successes. BER is empty rather than zero when aligned comparison is unavailable, commonly because the payload cannot fit the delivered grid or extraction fails. Audit checks should verify the six 45-row cohorts, the 126 successes, and the expected payload distributions before regenerating tables or figures.

REFERENCES

- [1] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik: Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). *Signal Processing* 206, 108908 (2023). DOI: 10.1016/j.sigpro.2022.108908.
- [2] B. Song, P. Wei, S. Wu, Y. Lin, and W. Zhou: A survey on deep-learning-based image steganography. *Expert Systems with Applications* 254, 124390 (2024). DOI: 10.1016/j.eswa.2024.124390.
- [3] L. Zhu, X. Luo, C. Yang, Y. Zhang, and F. Liu: Invariances of JPEG-quantized DCT coefficients and their application in robust image steganography. *Signal Processing* 183, 108015 (2021). DOI: 10.1016/j.sigpro.2021.108015.
- [4] T. Chuman, K. Iida, W. Sirichotedumrong, and H. Kiya: Image manipulation specifications on social networking services for encryption-then-compression systems. *IEICE Transactions on Information and Systems* E102-D(1), 11–18 (2019). DOI: 10.1587/transinf.2018MUP0001.
- [5] ITU-T: Information technology – Digital compression and coding of continuous-tone still images – Requirements and guidelines, Recommendation T.81 (1992).
- [6] X. Duan, B. Li, Z. Yin, X. Zhang, and B. Luo: Robust image steganography against lossy JPEG compression based on embedding domain selection and adaptive error correction. *Expert Systems with Applications* 229, 120416 (2023). DOI: 10.1016/j.eswa.2023.120416.
- [7] J. Zhang, X. Zhao, and X. He: Robust JPEG steganography based on the robustness classifier. *EURASIP Journal on Information Security* 2023, 11 (2023). DOI: 10.1186/s13635-023-00148-x.
- [8] Y. Huang, Z. Liu, Q. Wu, and X. Liu: Robust image steganography against JPEG compression based on DCT residual modulation. *Signal Processing* 219, 109431 (2024). DOI: 10.1016/j.sigpro.2024.109431.
- [9] K. Zeng, K. Chen, W. Zhang, Y. Wang, and N. Yu: Improving robust adaptive steganography via minimizing channel errors. *Signal Processing* 195, 108498 (2022). DOI: 10.1016/j.sigpro.2022.108498.
- [10] T. Qiao, S. Wang, X. Luo, and Z. Zhu: Robust steganography resisting JPEG compression by improving selection of cover element. *Signal Processing* 183, 108048 (2021). DOI: 10.1016/j.sigpro.2021.108048.
- [11] F. Shang, Y. Lan, J. Yang, E. Li, and X. Kang: Robust data hiding for JPEG images with invertible neural network. *Neural Networks* 163, 219–232 (2023). DOI: 10.1016/j.neunet.2023.03.037.
- [12] Y. Pan, J. Ni, Q. Liu, W. Su, and J. Huang: Efficient JPEG image steganography using pairwise conditional random field model. *Signal Processing* 221, 109493 (2024). DOI: 10.1016/j.sigpro.2024.109493.
- [13] Y. Cheng, Z. Luo, and Z. Yin: Robust steganography with boundary-preserving overflow alleviation and adaptive error correction. *Expert Systems with Applications* 281, 127598 (2025). DOI: 10.1016/j.eswa.2025.127598.
- [14] M. Boroumand, M. Chen, and J. J. Fridrich: Deep residual network for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security* 14(5), 1181–1193 (2019). DOI: 10.1109/TIFS.2018.2871749.
- [15] N. J. De La Croix, T. Ahmad, and F. Han: Comprehensive survey on image steganalysis using deep learning. *Array* 22, 100353 (2024). DOI: 10.1016/j.array.2024.100353.
- [16] Y. Zhang, C. Qin, W. Zhang, F. Liu, and X. Luo: On the fault-tolerant performance for a class of robust image steganography. *Signal Processing* 146, 99–111 (2018). DOI: 10.1016/j.sigpro.2018.01.011.
- [17] National Institute of Standards and Technology: Advanced Encryption Standard (AES), FIPS 197-upd1 (2023).
- [18] J. Kim and S. Lee: Deep learning of human visual sensitivity in image quality assessment framework. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1969–1977 (2017). DOI: 10.1109/CVPR.2017.213.
- [19] National Institute of Standards and Technology: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D (2007).
- [20] C. Percival and S. Josefsson: The scrypt Password-Based Key Derivation Function. RFC 7914 (2016). DOI: 10.17487/RFC7914.
- [21] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli: Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing* 13(4), 600–612 (2004). DOI: 10.1109/TIP.2003.819861.
- [22] ShadowPost Research Team: ShadowPost platform trial datasets and implementation, project artifact (2026). Repository URL: <https://github.com/Arman-Khan-24/ShadowPost>; canonical benchmark commit: 1b0dd40704242bc525ea5edd042267d299ff6186.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details