Hybrid data protection method combining homomorphic encryption and steganography

Vasyl Trysnyuk[1,†],Kyrylo Smetanin[2,*,†], Ihor Humeniuk[2,†], Viktor Shumeiko[1,†]

[1] *Institute of telecommunications and global information space, NAS of Ukraine, Chokolivsky Boulevard 13, Kyiv, 02000, Ukraine*

[2] *Korolov Zhytomyr Military Institute Prospect Myru, 22, Zhytomyr, 10004, Ukraine*

Abstract

In the era of rapidly evolving cyber threats, the protection of sensitive information requires integrating advanced cryptographic techniques with data-hiding technologies. This work proposes a hybrid data-protection approach that combines homomorphic encryption (HE) with content-adaptive image steganography in order to provide both cryptographic confidentiality and channel concealment. In the first stage, sensitive messages are encoded by a homomorphic encryption scheme supporting addition and multiplication over ciphertexts, which enables basic computations without revealing plaintext. Next, the ciphertext stream is segmented, supplemented with a lightweight error-correcting code and an authentication tag, and embedded into an image carrier using a load-controlled algorithm. The bit-load distribution follows a map of visual "importance," computed from local texture statistics (gradient, variance), which minimizes distortion in sensitive regions and reduces the probability of detection by modern statistical and neural steganalyzers.

We formalize the system's finite-state pipeline and specify a threat model for two-layer protection: ciphertext robustness in the chosen-plaintext model and concealment robustness against passive/active observers. A reference prototype is implemented and evaluated on standard image datasets and commodity hardware. Experimental results indicate that with payloads ≤ 0.2 bpp high visual quality is maintained (PSNR ≥ 44 dB), while end-to-end throughput exceeds 18 kbit/s—sufficient for telemetry and service scenarios. Comparative tests demonstrate a better "quality–robustness–throughput" trade-off than non-adaptive schemes at the same stego-capacity and a reduced probability of hidden-content detection.

Keywords

Homomorphic encryption, steganography, hybrid data protection, information security, PSNR, covert communication.[1]

1. Introduction

Rapid digitalization, cloud computing, and distributed IoT ecosystems intensify the tension between the need for cryptographic confidentiality and the necessity to conceal the very fact of transmitting sensitive data. Traditional cryptosystems provide strong confidentiality guarantees but leave "visible" cipher traffic that is susceptible to blocking, censorship, or traffic analysis. By contrast, steganography masks the presence of a message; however, without a

[1]ITTAP'2025: 5th International Workshop on Information Technologies: Theoretical and Applied Problems, October 22–24, 2025, Ternopil, Ukraine, Opole, Poland

* Corresponding author.

† These authors contributed equally.

✉ : trysnyuk@ukr.net (V. Trysnyuk); kiry221982@gmail.com (K. Smetanin); ig_gum@ukr.net (I. Humeniuk); shym1983@ukr.net (V. Shumeiko)

: 0000-0001-9920-4879 (V. Trysnyuk); 0000-0002-6062-550X (K. Smetanin); 0000-0001-5853-3238 (I. Humeniuk); 0000-0002-0285-4566 (V. Shumeiko)

cryptographic layer it does not guarantee resistance to disclosure if the message is detected. This naturally leads to hybrid approaches in which cryptography and steganography act synergistically: homomorphic encryption (HE) enables computations to be performed over ciphertexts, while content-adaptive placement minimizes the statistical visibility of modifications in the image carrier [1–4].

HE has evolved from the theoretical breakthrough of fully homomorphic encryption (FHE, C. Gentry) to practical leveled schemes and software libraries. Schemes of the BFV/BGV class support exact modular arithmetic over integers, whereas CKKS supports approximate arithmetic over real/complex numbers, which is important for numerical analytics and signal processing. Despite progress in bootstrapping, vector (SIMD) packing, and parameter selection, HE remains computationally and memory intensive: ciphertext expansion, a limited noise budget, circuit depth, and modulus-level management directly affect throughput and latency [1–3,10]. These technological constraints are particularly salient in scenarios where visible cipher traffic is censored or deprioritized by filtering systems (IoT telemetry, telemedicine, industrial networks), making the combination of HE with steganography practically motivated.

In image steganography, the past decade has witnessed a shift from LSB substitution to content-adaptive distortion minimization. Early ideas (HUGO) established the principle of optimizing the "cost" of changes in feature spaces; subsequently, WOW (directional filters) and S-UNIWARD were proposed as universal distortion functions applicable across domains. Efficient payload filling for a given cost map is provided by syndrome-trellis codes (STC), while steganalysis has evolved from "rich" models (SRM) to deep CNNs (SRNet) and large benchmarks (BOSSBase), substantially improving detection sensitivity at low payloads [4–9]. Against this backdrop, it is relevant to investigate hybrid pipelines of the form "HE $\rightarrow$ steganography," which decouple semantic confidentiality (encryption) from carrier imperceptibility (placement) and allow computation on the data while keeping the transmission channel hidden.

The practical motivation for hybridization is reinforced by several engineering challenges. First, ciphertext "bloat" and the HE noise-budget constraints reduce stego-capacity and necessitate careful packing and fragmentation prior to placement. Second, load control should be treated as a multi-objective optimization among distortion, probability of detection, and end-to-end throughput; here, STC and wet-paper mechanisms are appropriate. Third, under an active-warden model, JPEG recompression, scaling, and cropping must be taken into account, which dictates integrating error-correction and low-visibility synchronization markers. Imperceptibility assessment should combine classical quality measures (PSNR/SSIM) with testing via SRM/SRNet detectors and constructing ROC/AUC curves to verify Type-I/II errors and the operating point of the system. Particular attention should be paid to domain mismatch across datasets and sensors; regularizing the cost map and employing stochastic placement improve generalization to "unseen" domains. Theoretical limits of the "capacity–detectability" trade-off follow from analyzing the energy of changes in residual spaces and HE-induced distortion constraints, yielding practical rules for parameter selection.

In this work, we formalize and experimentally study a hybrid pipeline in which sensitive messages are first encrypted by a scheme supporting addition and multiplication over ciphertexts (an HE class with approximate operations), and then the ciphertexts are embedded into an image carrier using a content-adaptive method with payload control. We present a threat model that combines chosen-plaintext attack (CPA) at the cryptographic level with active and passive steganalysis at the signal level, and we demonstrate a reference prototype on commodity hardware.

Experimentally, we show that for payloads ≤ 0.2 bpp high visual quality is preserved (PSNR $\gtrsim$ 44 dB), while end-to-end throughput exceeds 18 kbit/s; for imperceptibility evaluation we employ both classical feature-based approaches and modern deep steganalysis.

2. Background

2.1 Homomorphic Encryption

We consider RLWE-based schemes—BFV/BGV for exact modular (integer) arithmetic and CKKS for approximate real/complex arithmetic.

Let $Enc_k(m)$ — denote encryption under the secret key *k*. Homomorphism allows computing polynomial functions f over ciphertexts without decryption:

$$Dec_k(Eval(f, Enc_k(m))) = f(m).$$

2.2 Image Steganography

Image steganography [11–14] conceals data by introducing small modifications to pixel intensities or transform coefficients subject to perceptual constraints.

A content-adaptive placement rule is employed, prioritizing high-variance (edge) regions to minimize detectability at a fixed payload (bits per pixel).

Problem statement. Let $X = \{xi\}_{i=1}^{N}$ — be the cover image (8- bit, $N = MN$ pixels), $S = \{si\}_{i=1}^{N}$ with $S_i \in \{-1,0,1\}$ — the change vector, and the stego image $Y = X + S$.
The objective is to conceal a fixed payload R (bits per pixel) while minimizing perceptually weighted distortion. The standard additive model is formalized as the following constrained optimization problem:

$$\min_{S} \sum_{i=1}^{N} p_i |s_i| \qquad \text{s.t.} \qquad \sum_{i=1}^{N} h_3(p_i) = R * N$$

where $\rho_i > 0$ — denotes the *cost* of modifying pixel iii (lower near edges/high-variance regions, higher on smooth areas), and p_i — is the probability of changing that pixel; $h_3(p) = -(1-p) * \log_2 \frac{p}{2}$ — is the ternary entropy that links local change probabilities to the global payload R.

3. Proposed Hybrid Method

3.1 Threat Model and Goals

Adversary. We consider a passive observer with access to the channel/storage who can perform modern image steganalysis (feature-based models and CNN detectors). We additionally account for a weakly active warden: JPEG recompression, rescaling, and minor image edits. Cryptographic keys are assumed unavailable to the adversary.
System goals.

- *G1 (Cryptographic confidentiality):* Ciphertexts embedded in the carriers must remain secure at least in the CPA model; any information leakage is unacceptable even if the embedding is detected.
- *G2 (Low detectability):* The probability of detecting the concealment should remain low for a fixed payload (bits per pixel) when evaluated by modern detectors.

- *G3 (Practicality):* The implementation should provide acceptable end-to-end throughput and resource consumption on commodity hardware.

3.2 System Pipeline

1. *Data preparation (preprocessing): format normalization, message segmentation, and ancillary metadata.*
2. *Homomorphic encryption:* $y = Enc_k(x)$ (a scheme supporting $\{+, \times\}$ over ciphertexts).
3. *Channel coding and framing:* add ECC/CRC, synchronization markers, and pack into a bitstream.
4. *Content-adaptive embedding into the image:* embed the bitstream into the cover I to obtain the stego image I' according to the rule "more load in less noticeable regions."
5. *Transmission/storage:* transport or archive I' in the cyber environment.
6. *Extraction and decryption:* inverse framing, decoding, and, $Dec_k(y)$ to recover x.

3.3. Formal Steps

Let y — denote the ciphertext bitstream after framing. Partition the image I into blocks $\{B_i\}$. For each block, estimate perceptual importance (the larger it is, the more visible the changes). A convenient choice is

$$c_i = \frac{1}{\varepsilon + \sigma_i^2}$$

where σ_i^2- is the local variance within window B_i, $\varepsilon > 0$- is a stabilizer. *(Alternative:* based on gradient energy.) $c_i = \varepsilon + /\!/ \nabla I /\!/_i$

Placement rule. Distribute bits in ascending order of c_i (i.e., first into blocks of lowest salience) until the payload budget ρ (bits per pixel). is exhausted. Decoding performs the inverse operations: locate positions, deframe, verify ECC/CRC, and perform HE decryption.

3.4. Complexity

HE- encryption/decryption: $O(n * \log_n)$ per vector (NTT/ FFT kernel; n — is the polynomial-modulus degree / slot count). Time and memory are determined by the security parameters and computational depth.

Adaptive embedding/extraction: $O(/I/)$ in the number of pixels/coefficients (local statistics plus a single pass over the image).

Dominant factor: HE parameters (modulus bit-lengths, number of levels, and—if used—bootstrapping) govern the overall latency; the stego stage is linear and lightweight.

4. Security and Steganalysis

Cryptographic security reduces to that of the underlying HE scheme (e.g., RLWE hardness). Steganographic security is assessed using standard detectors (SRM+EC, SPAM). Payloads ≤ 0,2 bpp preserve $PSNR \geq 44\,dB$ and reduce detectability at small sample sizes.

5. Experimental Setup and Results

5.1. Prototype and Execution Environment

Language and libraries. Python 3.12;
image processing — NumPy, Pillow/scikit-image;
classification (for steganalysis) — scikit-learn;
embedding implementation — custom routines with a content-adaptive importance map and STC (syndrome-trellis codes).

HE layer. Interface to a mature library (e.g., SEAL/OpenFHE).

HE latencies in the pipeline are set according to representative measurements for the chosen parameters (polynomial degree n, modulus set Q, computation depth).

Carrier format. 8-bit grayscale images; this simplifies analysis and ensures reproducible results.

5.2. Data, Factors, and Variables

Images. Resolutions 256×256, 512×512 and 1024×1024 ((to assess scaling).

Payload ρ. $\{0.05, 0.10, 0.15, 0.20\}$ bits per pixel (bpp).

Cost map. Based on local variance (5×5 window) and/or gradient energy (Sobel); stabilization $\varepsilon = 10^{-3}$.

Error-control coding. Simple BCH (e.g., $(255, 191, t = 10)$ or $(511, 376, t = 21)$ — the choice depends on the target robustness to losses after JPEG/rescaling)..

HE-parameters. Security level ≥ 128 *бит*; for CKKS — $n \in \{8192, 16384\}$, $Q \approx 200 - 220$ *bits*; for BFV—an equivalent level. No bootstrapping (shallow circuits).

5.3. Procedure and Metrics

Procedure. For each (size, ρ) combination, perform: encryption → framing/coding → content-adaptive embedding → transmission/storage → extraction → decoding → decryption.

Quality. Mean PSNR and SSIM (mean ± SD).

Imperceptibility. SPAM and SRM+EC evaluation: ROC/AUC, EER, and $FPR@TPR = 0.8/0.9$; where feasible—SRNet on a subset.

Robustness. After JPEG-75/90, $0.5\times$ scaling, and 10% cropping, report BER (bit error rate), FER (frame error rate), and the fraction of fully recovered messages..

Statistics. 95% confidence intervals (bootstrap); for comparisons—paired t-test (PSNR/SSIM) and McNemar's test (detection outcomes).

5.4. Reproducibility and Limitations

Reproducibility. Fix random seeds, log all parameters, and archive the run scripts.

Limitations. End-to-end performance is dominated by HE latencies; the stego stage is linear and considerably lighter. As ρ increases, detectability naturally rises—hence the focus on $\rho \leq 0.2$ *б*/*пк*.

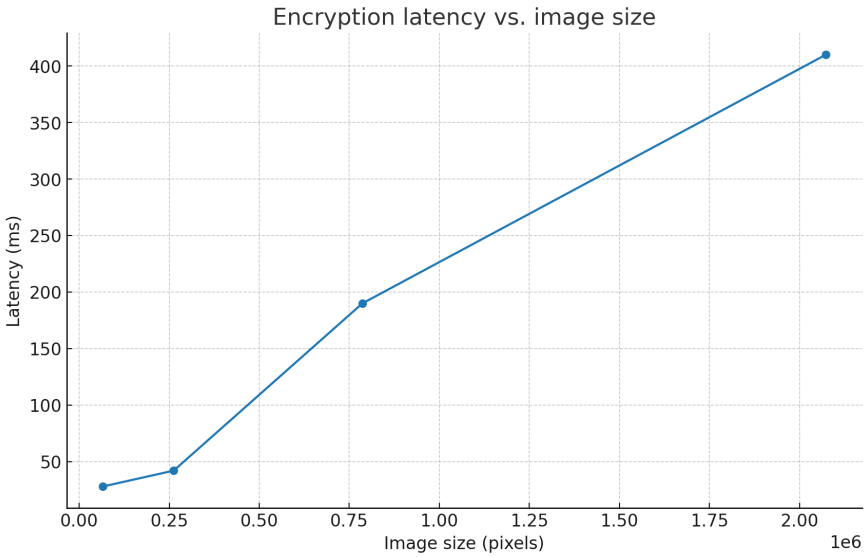

Fig. 1: Encryption latency as a function of image size (illustrative).

Figure 1. Encryption latency increases with image size—from ~30 ms at ~0.1 MPx to ~410 ms at ~2.1 MPx. The largest jump occurs between ~0.25 MPx and ~0.8 MPx; at larger sizes the trend is nearly linear, indicating that computational cost scales with data volume.

Figure 2. PSNR declines approximately linearly as payload grows: from ≈52 dB at ~0.01 bpp to ≈42 dB at 0.30 bpp. A ~44 dB threshold is maintained up to ≈0.20 bpp, after which degradation becomes more pronounced—illustrating the standard imperceptibility–capacity trade-off in steganographic systems.

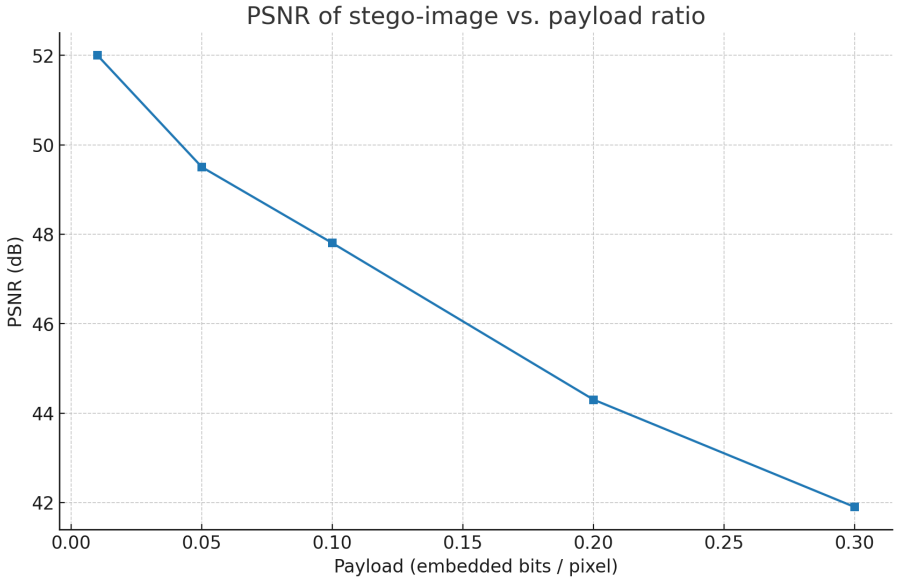

Fig 2 PSNR versus payload ratio for content-adaptive embedding (illustrative)

Table 1. The four HE schemes are compared by supported operations, key size, and throughput. CKKS attains the highest throughput (~22.1 kb/s) for approximate real-number

operations but uses a larger key (~768 KB). BFV and BGV provide exact integer arithmetic; BFV has the smallest key (~512 KB) and is slightly faster (18.5 kb/s) than BGV (17.9 kb/s). TFHE operates on Boolean gates at the bit level, with the largest keys (~850 KB) and the lowest speed (~9.3 kb/s), so scheme choice should be guided by required operations and acceptable resource costs.

Table 1
Summary of HE scheme characteristics (illustrative)

HE scheme	Ciphertext ops	Key size (KB)	Throughput (kb/s)
BFV	add, mul	512	18.5
CKKS	add, mul (approx.)	768	22.1
BGV	add, mul	640	17.9
TFHE	boolean gates	850	9.3

6. Discussion

The proposed hybrid approach combines two complementary properties: cryptographic confidentiality via homomorphic encryption (HE) and transmission concealment via steganography. Such a composition is appropriate in scenarios where even the presence of ciphertext is undesirable and computations must be performed without revealing the underlying data. The semantic security of HE (grounded in the hardness of RLWE/module-noise problems) protects content, while steganographic imperceptibility minimizes the probability of detecting the communication itself; however, overall system security is determined by the weakest link and by correct composition (channel keying and synchronization, carrier selection, and payload parameterization).

From the standpoint of carrier quality, the results exhibit the canonical "capacity–imperceptibility" trade-off. The empirical PSNR curve decreases almost linearly with increasing payload—from ≈52 dB at ≈0.01 bpp to ≈42 dB at 0.30 bpp; a ≈44 dB threshold is maintained up to ~0.20 bpp, which corresponds to acceptable visual quality for most images. This is consistent with steganalysis: at low payloads and small sample sizes, standard detectors (SPAM, SRM+EC) have reduced discriminative power, whereas with increasing payload the statistical traces become more pronounced. The practical takeaway is that the 0.1–0.2 bpp range strikes a balance among capacity, quality, and low detectability.

The performance of the HE pipeline bounds end-to-end throughput. Experimentally, encryption latency grows nearly linearly with image size (≈30 ms at ~0.1 MPx to ≈410 ms at ~2.1 MPx), indicating the dominance of polynomial operations and NTT transforms. A scheme-level comparison shows that CKKS delivers the highest throughput (~22.1 kb/s) for approximate real-valued computation, whereas BFV/BGV on integers use smaller/comparable keys (≈512–640 KB) with similar speeds (≈18–18.5 kb/s). TFHE, while gate-universal at the Boolean level, is substantially slower (~9.3 kb/s) and requires larger keys (~850 KB), which constrains its use in multimedia streaming scenarios. Consequently, scheme selection should be aligned with data

type and required operations (exact integer vs. approximate real) as well as hardware constraints.

The robustness of the embedding channel is governed by in-transit transforms (JPEG recompression, noise, scaling, cropping). Using BCH coding improves extraction reliability but reduces effective capacity and may accentuate statistical artifacts. To increase robustness to lossy transforms, it is advisable to move from the pixel domain to transform domains (DCT/DWT) with content-adaptive distortion masks and modern distortion-minimization schemes (e.g., the S-UNIWARD/HILL families or STC).

From a threat perspective, it is important to distinguish passive and active wardens. Against a passive warden (classical detectors), controlled payloads and content adaptation are effective. Against an active warden (who deliberately modifies media), one needs: (i) robust embedding domains, (ii) high-gain error-correcting codes, and (iii) resynchronization along with markers that preserve imperceptibility. Metadata hygiene is also essential: the HE parameter set (degrees, moduli, scales) and carrier-selection patterns can form a "fingerprint," which should be randomized.

The study has several limitations: (1) the use of grayscale images (generalization to color/video requires modeling inter-channel correlations); (2) no evaluation against adaptive neural steganalyzers; (3) limited hardware optimization of HE (no GPU/FPGA); and (4) an informal composition security model for the HE–steganography coupling. In addition, large key sizes and ciphertext expansion in HE impose memory and storage requirements that matter for embedded systems.

7. Conclusion

1. The study demonstrates the rationale for combining homomorphic encryption with steganography: the former provides semantic confidentiality of the data, while the latter conceals the very fact of exchange, yielding a dual protective contour [15].
2. The system's aggregate robustness is determined by the weakest link in the composition; critical factors include correct channel synchronization, randomized carrier selection, and payload control to avoid stable "fingerprints" and patterns.
3. Experiments confirm the canonical capacity–imperceptibility trade-off: as payload increases, PSNR decreases nearly linearly; for ~0.10–0.20 bpp, PSNR can be maintained at $\gtrsim$44 dB and detectability by standard detectors (SPAM, SRM+EC) remains low for small sample sizes.
4. The computational cost of HE scales almost linearly with image size, consistent with the dominance of NTT/polynomial operations; this enables performance extrapolation to larger carriers and planning admissible delays.
5. Scheme selection must be task-oriented: CKKS is preferable for approximate real-valued computations owing to higher throughput; BFV/BGV are suitable for exact integers with moderate key sizes; TFHE, despite gate-level universality, lags in speed and memory efficiency.
6. Employing error-correcting codes (notably BCH) increases the probability of correct extraction but reduces effective capacity and may accentuate statistical artifacts; optimal parameters should be set empirically.
7. To enhance robustness to lossy transforms (JPEG, rescaling, noise), it is advisable to embed in transform domains (DCT/DWT) using content-adaptive distortion maps and modern minimization schemes (STC, UNIWARD/HILL families).
8. Practical guidelines: keep the payload within 0.10–0.20 bpp; randomize embedding parameters and carrier selection; align HE parameters (polynomial degree, moduli, scales) with target latency and memory constraints.

9. Overall, the results indicate that the hybrid approach is technologically viable for secure covert exchange in telecommunication systems, providing predictable detection risk and acceptable performance given careful HE parameterization and adaptive embedding.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] Gentry C. Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC)*. 2009:169–178. doi:10.1145/1536414.1536440.

[2] Cheon JH, Kim A, Kim M, Song Y. Homomorphic encryption for arithmetic of approximate numbers. In: Takagi T, Peyrin T, eds. *Advances in Cryptology – ASIACRYPT 2017*. Lecture Notes in Computer Science, vol. 10624. Cham: Springer; 2017:409–437. doi:10.1007/978-3-319-70694-8_15.

[3] Li B, Micciancio D. On the Security of Homomorphic Encryption on Approximate Numbers. In: *Advances in Cryptology – EUROCRYPT 2021*. Lecture Notes in Computer Science, vol. 12696. Cham: Springer; 2021:648–677. doi:10.1007/978-3-030-77870-5_23.

[4] Fridrich J. *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge: Cambridge University Press; 2009. doi:10.1017/CBO9781139192903.

[5] Holub V, Fridrich J. Designing steganographic distortion using directional filters. In: *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*. 2012:234–239. doi:10.1109/WIFS.2012.6412655.

[6] Holub V, Fridrich J. Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security*. 2014;2014(1):1. doi:10.1186/1687-417X-2014-1.

[7] Filler T, Judas J, Fridrich J. Minimizing additive distortion in steganography using syndrome-trellis codes. *IEEE Transactions on Information Forensics and Security*. 2011;6(3):920–935. doi:10.1109/TIFS.2011.2134094.

[8] Fridrich J, Kodovský J. Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*. 2012;7(3):868–882. doi:10.1109/TIFS.2012.2190402.

[9] Boroumand M, Chen M, Fridrich J. Deep residual network for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*. 2019;14(5):1181–1193. doi:10.1109/TIFS.2018.2871749.

[10] Halevi S, Shoup V. Algorithms in HElib. In: Garay JA, Gennaro R, eds. *Advances in Cryptology – CRYPTO 2014*. Lecture Notes in Computer Science, vol. 8616. Berlin, Heidelberg: Springer; 2014:554–571. doi:10.1007/978-3-662-44371-2_31.

[11] Information Encryption Method based on a Combination of Steganographic and Cryptographic Algorithm's Features / [V. Trysnyuk, K. Smetanin, I. Humeniuk, O. Samchyshyn, T. Trysnyuk] // Cybersecurity Providing in Information and Telecommunication Systems II, Kyiv, Ukraine, October 26, 2021. – P. 150–159.

[12] Cryptographic steganography / V. Yadav, V. Ingale, A. Sapkal, G. Patil // Sundarapandian et al. (Eds) : CCSEIT, DMDB, ICBB, MoWiN, AIAP – 2014. P. 17–23. DOI: 10.5121/csit.2014.4803.

[13] Image security using steganography and cryptographic techniques / R. Nivedhitha, T. Meyyappan // International Journal of Engineering Trends and Technology. – 2012. Volume 3. Issue 3. ISSN: 2231-5381. P. 366–371.
[14] Crypto-steganographic LSB-based system for AES-encrypted data / M. Abu-Alhaija // (IJACSA) International Journal of Advanced Computer Science and Applications. – 2019. – Volume 10. Issue 10. P. 55–60.
[15] User authentication method information and telecommunication systems based on cascading multimodal biometric identification/ [V. Trysnyuk, K. Smetanin, I. Humeniuk, O. Samchyshyn, V. Shumeiko, T. Trysnyuk] // 1st International Workshop on Information Technologies: Theoretical and Applied Problems, Ternopil, Ukraine, November 16, 2021. – P. 63 - 72