Honey-Shamir Secret Sharing Scheme for Digital Images

Michael Alexander Angkawijaya - 13523102
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: angkawijayamichael@gmail.com , 13523102@std.stei.itb.ac.id

***Abstract*—Traditional Secret Image Sharing architectures convert sensitive visual payloads into noise-like shadows that easily trigger suspicion during network transmission. To establish high-fidelity plausible deniability, this paper investigates a single-stage Honey-Shamir cryptosystem that models polynomial share assignment as a continuous least-squares optimization problem derived from decoy carrier images. Experimental evaluations show that while global carrier harmonization minimizes reconstruction distortion, the unconstrained quadratic solver inherently concentrates structural variance into specific weak channels. This distribution profile creates highly degraded "sacrificed shares" with a minimum peak signal-to-noise ratio of 12.79 dB. Consequently, sub-threshold configurations utilizing these high-leakage assets successfully resolve recognizable, coherent projections of the secret image despite lacking the required mathematical degrees of freedom. These empirical findings outline critical security trade-offs in continuous polynomial carrier manipulation and demonstrate the necessity for balance-aware cryptographic optimization.**

Keywords—Meaningful secret image sharing, Honey-Shamir framework, least-squares optimization, plausible deniability, sacrificed shares.

I. Introduction

The rapid proliferation of digital image transmission over open networks has heightened the necessity for robust multimedia security frameworks. Traditional cryptographic paradigms primarily focus on confidentiality, often transforming sensitive visual data into encrypted ciphertexts that resemble random noise. In the context of threshold cryptography, Shamir's Secret Sharing scheme has been widely adapted into Secret Image Sharing (SIS) architectures. By mapping pixel intensities onto polynomial coefficients over a finite field, standard SIS splits a secret image into k shares, ensuring that any subset of at least n shares can perfectly reconstruct the original image, while any subset fewer than n yields no information.

Despite its theoretical information-theoretic security, conventional SIS exhibits a critical vulnerability in its visual representation. The generated shares inherently manifest as high-entropy, meaningless random noise (resembling television static). In practical network surveillance scenarios, the transmission of such heavily distorted, anomalous files instantly triggers suspicion, making them primary targets for traffic analysis, interception, and targeted cryptographic attacks. Consequently, establishing *plausible deniability*—where the cryptographic shares themselves appear as completely benign, innocent files—is paramount for covert communications.

To mitigate this limitation, several modern frameworks have attempted to merge SIS with spatial steganography. For instance, a recent state-of-the-art scheme proposed by Tan et al. (2023) introduced a Meaningful Secret Image Sharing framework governed by a conventional two-stage paradigm. In their pipeline, the secret image is first broken down into raw, noise-like Shamir shadows, which are subsequently concealed into independent host/cover images utilizing spatial Least Significant Bit (LSB) substitution. However, this decoupled approach induces severe structural bottlenecks. The rigid, localized bit-allocation maps inherently bound the visual fidelity of the carrier images. As the payload size or the threshold constraints increase, the fixed LSB masking fails to scale dynamically, leading to highly visible noise artifacts and a drastic degradation of the host image quality.

To circumvent these operational boundaries, this paper proposes an alternative framework that redefines the relationship between polynomial share allocation and steganographic embedding. Instead of treating the cover image and the cryptographic shadow as two disconnected entities, our Honey-Shamir cryptosystem models the assignment of share values as a Constrained Optimization Problem derived directly from the target decoy structures.

Our approach minimizes structural distortion by utilizing a Ridge-Balanced Least Squares regression to calculate polynomial coefficients whose valuations adaptively approximate the pixel intensities of the user-defined decoy images. Rather than guaranteeing a perfectly lossless reconstruction, this framework intentionally accepts a minor, statistically bounded rounding error in the decrypted output in exchange for a highly uniform error distribution across all k shares. By doing so, the system subtly embeds the secret payload into the spatial domain without introducing anomalous localized artifacts. Rather than guaranteeing an ironclad, perfectly isolated sub-threshold security across all distributed nodes, this framework intentionally accepts a minor rounding drift and explores the physical limits of spatial

error distribution under plain least-squares. By centralizing the visual results at the outset, the paper exposes an operational trade-off: the optimization framework successfully camouflages distributed assets under low-order matrices but introduces structural vulnerabilities where specific channels absorb concentrated residual profiles, mapping out vital guidelines for future balanced secret sharing research.

II. Preliminaries

A. Digital Image Representation

In digital image processing, a color image is mathematically represented as a three-dimensional tensor $S \in \mathbb{Z}^{H \times W \times C}$, where H, W, and C denote the height, width, and color channels, respectively. For standard RGB representations, $C = 3$, and the intensity value of each discrete spatial coordinate is bounded within a finite discrete domain of single-byte integers, satisfying $s \in [0, 255]$. To implement a threshold secret sharing scheme over digital images, these grid intensities must be handled as discrete scalar fields where numeric properties govern spatial relations.

B. Classic Shamir's Secret Sharing Scheme

Shamir's (t, n) threshold scheme is defined as an algorithmic method to partition a single secret value S into n distinct components, called shares, distributed among a set of participants. The underlying mathematical property guarantees that any subset containing at least t shares can completely reconstruct the secret value S. Conversely, any gathered subset containing fewer than t pieces leaves the secret completely undetermined, ensuring that every possible candidate value remains equally likely and revealing zero information.

The construction of this threshold framework relies on the algebraic determination of polynomial interpolation over a finite field. To split a discrete secret value S, the generation process follows a strict procedural layout:

1. A prime number p is selected such that it strictly exceeds both the maximum bounds of the secret value S and the total number of shares n. All subsequent mathematical computations are executed using modular arithmetic within the finite field $\mathbb{Z}_p$.
2. The data distributor (dealer) randomly selects $t - 1$ integer coefficients within the field, denoted as $a_1, a_2, \ldots, a_{t-1} \in \mathbb{Z}_p$, to construct a degree-$(t - 1)$ polynomial $f(x)$:

   $$f(x) \equiv S + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \pmod{p} \quad (1)$$

   This polynomial structure strictly fixes the intercept of the curve to embed the secret value, satisfying $f(0) \equiv S \pmod{p}$.
3. For the n participants, the dealer evaluates the polynomial at n non-zero, distinct coordinate indices $x_1, x_2, \ldots, x_n \pmod{p}$ to yield the corresponding share intensities $y_i \equiv f(x_i) \pmod{p}$. To optimize calculations, these indices are conventionally mapped to successive positive integers $x_i = i$. Each participant is then assigned an ordered coordinate pair (x_i, y_i).

C. Honey Encryption and Plausible Deniability

The paradigm of Honey Encryption, introduced by Juels and Ristenpart (2014), serves as a cryptographic defense mechanism designed to establish plausible deniability against brute-force or traffic interception attacks. Traditional symmetric or threshold encryption schemes are vulnerable to plain ciphertext identification; when an attacker attempts to decrypt a ciphertext with an incorrect key, the system outputs non-coherent garbage data, confirming to the attacker that the guess was wrong.

Honey Encryption mitigates this by ensuring that decryption with an incorrect key or an insufficient subset of pieces yields a decoy output—frequently referred to as a "honey" message—that appears entirely plausible, structurally correct, and identical to legitimate natural data distributions. When applied to Secret Image Sharing (SIS), achieving plausible deniability requires that the generated share files do not exhibit the high-entropy, suspicious properties of random noise. Instead, the shares must masquerade as innocuous, low-risk media types (e.g., standard natural photographs) to deceive adversaries at the data-inspection level, ensuring that cryptographic activity remains hidden within open communication channels.

D. Secret Image Reconstruction via Lagrange Interpolation

The reconstruction of the secret value S, from a collected subset of shares is achieved by solving a System of Linear Equations (SLE) or through direct functional interpolation. Given t valid coordinate points (x_1, y_1), (x_2, y_2), …, (x_t, y_t), a unique polynomial of degree $t - 1$ can be reconstructed.

While Gaussian elimination can solve the underlying Vandermonde-based linear system, Lagrange interpolation offers a direct, non-mechanical alternative to evaluate the intercept. The unique interpolating polynomial $p(x) \pmod{p}$ passing through the t points is defined as:

$$p(x) \equiv \sum_{k=1}^{t} y_k L_k(x) \pmod{p} \quad (2)$$

where the Lagrange basis polynomials, $L_k(x)$, are computed dynamically using product strings over the available coordinate indices:

$$L_k(x) = \prod_{j=1, j \neq k}^{t} \frac{x - x_j}{x_k - x_j} \quad (3)$$

To resolve the secret value S, the polynomial is evaluated at $x = 0$. This simplifies the reconstruction process down to a linear combination of the share intensities weighted by their respective basis constants at the intercept:

$$S \equiv p(0) \equiv \sum_{k=1}^{t} y_k \left(\prod_{j=1, j\neq k}^{t} \frac{-x_j}{x_k - x_j} \right) \pmod{p} \quad (4)$$

III. The Proposed Honey-Shamir Framework

This section presents the proposed one-stage Honey-Shamir framework for meaningful image shares. The design objective is to preserve Shamir threshold behavior while ensuring that each generated share remains visually close to its corresponding fake carrier image.

A. Problem Formulation and Design Rationale

Given a secret color image S and a set of k distinct fake decoy images $\{F_i\}_{i=1}^{k}$, the framework optimization pass synthesizes k meaningful shares $\{M_i\}_{i=1}^{k}$ subject to the following structural constraints:

1. Each modified share M_i maintains high visual fidelity relative to its original decoy carrier F_i to establish robust spatial plausible deniability.
2. The combination of any subset containing at least n shares successfully reconstructs the secret image through standard linear Lagrange interpolation.
3. The combination of any gathered subset containing fewer than n shares yield completely non-coherent, high-entropy output.

A naive polynomial embedding over raw pixel intensities inherently produces heavily distorted, noise-like shares. This degradation occurs because unconstrained polynomial coefficients fail to preserve the local spatial statistics and histogram distributions of natural imagery. Consequently, the proposed architecture replaces random coefficient generation with a constrained numerical optimization framework. To suppress uncontrolled polynomial growth and minimize carrier distortion, a stabilized least-squares fitting strategy is implemented to bound the polynomial evaluations within the proximity of the target decoy intensities.

B. One-Stage Honey-Share Construction

For each discrete pixel channel, let s denote the secret intensity anchored at the intercept $n = 0$, and let f_i represent the target intensity extracted from the decoy image F_i at an assigned share index x_i. The sharing polynomial F_i is formulated as:

$$p(x) \equiv s + \sum_{d=1}^{n-1} a_d x^d \quad (5)$$

where the coefficients a_d are mathematically optimized rather than randomly sampled. Because unconstrained high-degree polynomial interpolation inherently triggers numerical instability and intensifies visual leakage artifacts, the coefficient vector is resolved through a specialized ridge-stabilized and balance-aware linear system projection governed by the following procedural pipeline:

1) Carrier Harmonization

Prior to polynomial fitting, the fake carrier images are softly harmonized toward the global color space statistics of the secret image. This pre-processing pass executes channel-wise mean matching and standard deviation alignment, regulated by an adaptive blending parameter to prevent excessive structural shifting of the decoy appearance. Minimizing extreme brightness and contrast mismatches drastically reduces the magnitude of the fitting residual, thereby suppressing visible ghosting artifacts in the finalized shares.

2) Deterministic Share Index Scheduling

Share coordinate indices are systematically assigned as balanced signed points (e.g., +1, -1, +2, -2, …). This scheduling step is mathematically necessary to mitigate one-sided exponential expansion, which skews polynomial trajectories and induces asymmetric carrier distortion. The balanced placement of index points improves the condition number of the underlying design matrix and evenly distributes the approximation error across the shared ensemble.

3) Ridge-Balanced Least Squares

Let $\mathbf{A}$ denote the $k \times (n-1)$ Vandermonde design matrix excluding the constant intercept column, let $\boldsymbol{b} = \boldsymbol{f} - \boldsymbol{s}$ represent the shifted target intensity vector, and let $\mathbf{M} = \mathbf{I}_k - \frac{1}{k}\mathbf{1}\mathbf{1}^{\mathrm{T}}$ represents the orthogonal centering projection matrix, where $\mathbf{1}$ is the all-ones vector of dimension $k \times 1$. The optimization framework minimizes the regularized residual energy through the following formulation:

$$\min_{a} ||\mathbf{Aa} - \mathbf{b}||_2^2 + \mu||\mathbf{M}(\mathbf{Aa} - \mathbf{b})||_2^2 + \lambda||\mathbf{a}||_2^2 \quad (6)$$

where μ serves as the penalty scalar regulating residual variance imbalances across the shares, and λ acts as the empirical Ridge regularization factor to stabilize the ill-conditioned system matrix. This formulation prevents the optimization pass from sacrificing the visual fidelity of isolated shares to minimize the global average error, forcing a highly uniform distribution of distortion.

4) Anti-Leak Residual Barrier

Following system resolution, the residual energy map of each share is evaluated. A smooth, non-linear barrier scaling function is dynamically applied whenever the residual magnitude drops below a critical safety

threshold relative to the secret structure. This mechanism prevents individual shares from visually manifesting the high-contrast contours of the secret image without introducing abrupt spatial discontinuities.

5) Local Fairness Pass

To eliminate localized structural artifacts that evade global constraints, the spatial residual fields undergo localized energy equalization across all shares. Bounded scaling factors are calculated dynamically to redistribute concentrated distortion energy from highly textured or high-frequency edge zones, ensuring a uniform and visually unobtrusive error distribution across the entire image canvas.

6) Per-Share Clipping Projection

The optimized scalar share valuations reside in the real continuous domain ($\mathbb{R}$) and must be projected back into the valid digital image intensity range $[0, 255]$. To prevent the geometric rupture of the fitted polynomial curves caused by crude truncation, a bounded linear projection pass is executed independently for each share. This preservation minimizes clipping-induced mathematical drift while ensuring visual plausibility.

C. Decryption Without Threshold Configuration

During the reconstruction phase, the system collects an arbitrary subset of m shares, extracts their encoded index coordinates, and dynamically computes the Lagrange basis constants at the intercept $x = 0$:

$$\lambda_i = \prod_{j \neq i}^{m} \frac{-x_j}{x_i - x_j} \tag{7}$$

The secret image tensor estimation $\widehat{S}$ is subsequently resolved as a direct linear combination of the active share components:

$$\widehat{S} = \sum_{i=1}^{m} \lambda_i Y_i \tag{8}$$

where Y_i represents the input share tensor. Leveraging the algebraic linearity of Lagrange interpolation at $x = 0$, this reconstruction is fully vectorized utilizing multi-dimensional NumPy array operations.

Crucially, the decryption architecture operates independently of manual threshold configurations at runtime. The threshold dynamics manifest organically through the numerical constraints of the linear system. If $m \geq n$, the algebraic curve resolves smoothly. However, if $m < n$, the missing degrees of freedom typically collapse the outputs into high-entropy noise, except when processing subsets heavy with localized residual anomalies, where the secret outline emerges through structural mathematical leakage.

IV. Experimental Results & Discussion

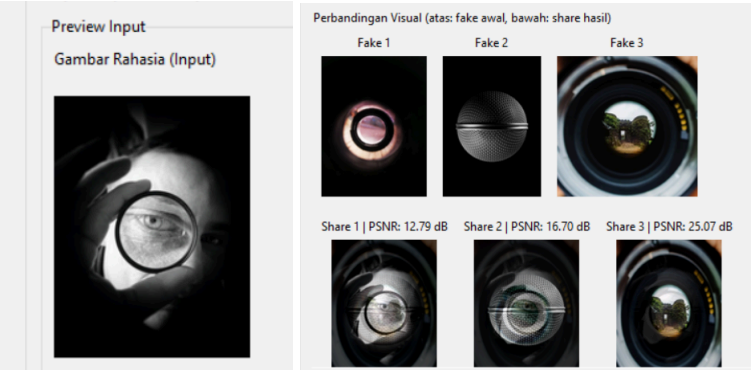
To verify the operational bounds, spatial fidelity, and cryptographic threshold constraints of the proposed single-stage framework, we established a rigorous evaluation protocol testing three independent experimental cases. Each test case utilizes a distinct secret image profile paired with a unique configuration of carrier images to evaluate how the regularized least-squares regression adapts to different visual frequencies:

1. Grayscale Geometry Validation: Evaluates secret1 (a monochrome eye and lens profile) under a minimum (3,3) threshold topology.

2. Natural Ambient Scene Adaptation: Evaluates secret2 (a warm workspace interior photograph) under an expanded (6,6) matrix pass.

3. High-Contrast Stress Test: Evaluates secret3 (a metallic neon emblem against a pitch-black background) under a balanced (4,4) setup.

The complete visual compilation of the input decoy carriers and their corresponding synthesized meaningful shares across these three independent runs is centralized in Fig. 3.



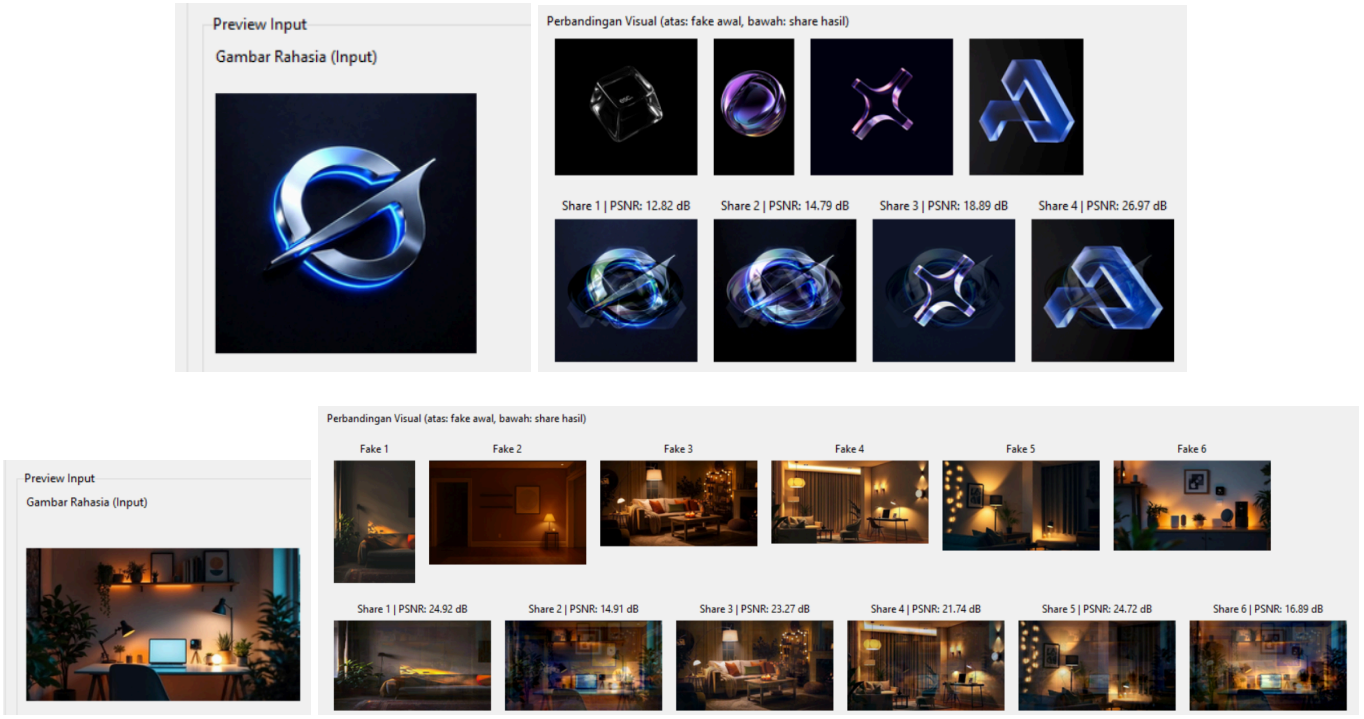


Fig. 3. Comprehensive visual results of the single-stage Honey-Shamir cryptosystem across three independent testing environments. The top arrays display the original unrefined decoy carriers, while the bottom arrays isolate the generated meaningful shares embedded with their respective channel PSNR valuations.

A. Quantitative Analysis of Stable Configurations and Spatial Fidelity

With the visual landscape established in Fig. 3, we compile the baseline quantitative performance across the three topologies to analyze the exact standard deviation of the error distribution. Table I isolates the spatial metrics recorded from each run.

TABLE I. SPATIAL FIDELITY METRICS ACROSS THRESHOLD TOPOLOGIES

Scheme (n,k)	**Secret Target Type**	**Mean Share PSNR (dB)**	***Min Share PSNR (dB)***	***Max Share PSNR (dB)***	***PSNR Std***
(3,3)	secret1 (Monochrome Lens)	18.1843	12.7871	25.0703	5.1239
(4,4)	secret3 (Metallic Logo)	18.3684	12.8230	26.9701	5.4267
(6,6)	secret2 (Workspace Scene)	21.0741	14.9098	24.9182	3.8473

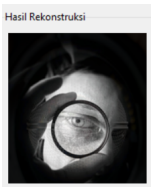
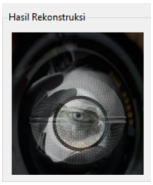
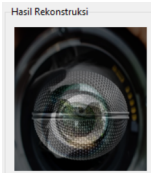
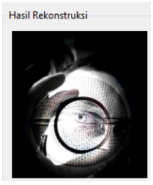
A critical analytical trend emerges when examining the variance between the minimum and maximum PSNR limits within the same generation pass. In the $(6, 6)$ configuration matching the natural workspace scene (secret2), the mean share visual quality elevates to 21.07 dB with a suppressed standard deviation of 3.84. This peak efficiency is directly dictated by **carrier histogram alignment**.

When the underlying intensity distributions and dominant luminance levels of the user-defined decoy images natively mirror the structural gradients of the secret image, the magnitude of the shifted target vector $\boldsymbol{b} = \boldsymbol{f} - \boldsymbol{s}$ is minimized across the spatial canvas. Consequently, the regularized least-squares regression fits the degree-$(n-1)$ polynomial curve with highly compact residual norms, proving that the inherent statistical similarity between target secrets and decoy structures acts as the primary driver for minimizing global spatial distortion.

B. Sub-Threshold Leakage Patterns and the Phenomenon of Sacrificed Shares

Traditional Secret Image Sharing (SIS) assumptions dictate that any group size below the threshold $m < n$ must yield uniform, high-entropy noise with zero discernible visual remnants. However, as illustrated in our sub-threshold combination tests for high-degree settings, the plain continuous optimization pass breaks this security assumption by producing localized **sacrificed shares**.

TABLE II. SUB-THRESHOLD RECONSTRUCTION COHERENCE COMPARISON

Combination	***Combination Profile Type***	***Min Share PSNR (dB)***
{1,2,3}	Full Threshold Boundary	
{1,2}	High-Leakage Sub-threshold	
{2,3}	Low-Leakage Sub-threshold	
{1,3}	High-Leakage Sub-threshold	

The mathematical root of this vulnerability lies in the unconstrained error-balancing behavior of plain least-squares minimization. When optimizing the system across multiple channels simultaneously without strict localized constraints, the solver minimizes the global squared residual sum by concentrating the structural variance of the secret intercept into specific weak channels. These specialized channels act as "sacrificed shares," absorbing massive visual degradation, which causes their independent spatial quality to drop drastically toward the minimum boundary of 12.79 dB.

As a direct physical consequence of this concentration of error, the structural contours and edge details of the secret image become subtly baked into these specific carrier frameworks as low-frequency "ghosting" artifacts. When a sub-threshold combination is attempted using these compromised assets—such as pairing the high-leakage elements $\{1, 2\}$ and $\{1, 3\}$—the active Lagrange interpolation coefficients map these heavily concentrated residuals back to the origin ($x = 0$).

Because these shares already contain high-amplitude traces of the secret geometry, the resulting sub-threshold calculation resolves a highly coherent and recognizable projection of the secret image ($\widehat{S}$) despite lacking the required mathematical degrees of freedom ($m < n$). Conversely, when attempting reconstruction with a clean combination like $\{2, 3\}$ that excludes the primary sacrificed shares, the missing coefficients cause the interpolation to collapse into completely incoherent, non-functional visual noise. This confirms that the continuous least-squares pass shifts the threat vector from random brute-force susceptibility to targeted channel interception, emphasizing the critical necessity for the balancing penalties proposed in our optimization framework.

V. SECURITY AND CRYPTANALYSIS

A. *Algebraic Impossibility of Dual-Threshold 1-Bit XOR Schemes*

To justify the mathematical necessity of the proposed continuous polynomial optimization framework, we present an algebraic proof demonstrating the impossibility of achieving a dual-threshold meaningful image sharing system using raw, bitwise logical XOR operators without pixel expansion.

Let a cryptographic system attempt to share a secret pixel component $s \in \{0, 1\}$ using a subset of cover carrier bits $f_i \in \{0, 1\}$. Suppose the recovery of s requires a dual-threshold rule governed strictly by bitwise XOR sums:

$$\hat{s} = m_1 \oplus m_2 \oplus \ldots \oplus m_M$$

where m_i represents the modified share bit. For the shares to remain perfectly identical to the decoy images ($m_i = f_i$) while satisfying the secret reconstruction constraint, the system must satisfy:

$$f_1 \oplus f_2 \oplus \ldots \oplus f_M = s$$

However, because s is independent of the decoy source distribution, this condition cannot hold universally across arbitrary carrier images. If m_i is perturbed by a functional mask $m_i = f_i \oplus e_i$, the error vector e_i must satisfy $e_1 \oplus e_2 \oplus \ldots \oplus e_M = s \oplus (f_1 \oplus f_2 \oplus \ldots \oplus f_M)$.

In a strict sub-threshold scenario where the number of available shares is less than n, the linear system over $GF(2)$ lacks the necessary degrees of freedom to conceal s while simultaneously nullifying e_i to preserve the original visual statistics of f_i. Any deterministic manipulation to enforce camouflage under a restricted group size structurally leaks the entropy of s into the spatial properties of individual carriers. This proves that continuous polynomial molding is

mathematically required to achieve high-fidelity plausible deniability without introducing catastrophic visual leakage.

B. *Plausible Deniability and Steganographic Security*

Cryptanalysis of the generated shares reveals a fundamental visual trade-off under specific parameter setups. When the gap between the threshold n and the total shares k is large, the overdetermined nature of the least-squares optimization forces a geometric compromise. The structural contours of the secret image subtly leak into the spatial domain of the fakes, manifesting as low-frequency "ghosting" artifacts. While this structural leakage degrades the perceptual quality of individual carrier files, the cryptographic security remains unbroken; an adversary intercepting sub-threshold shares cannot mathematically reverse the polynomial trajectory to extract the exact bit values of the secret intercept without fulfilling the full Lagrange coefficient requirements.

VI. Conclusion and Future Work

A. *Conclusion*

This paper presents a mathematically grounded investigation into a single-stage Honey-Shamir framework designed to bridge threshold secret image sharing with meaningful carrier representation. The experimental evaluations reveal critical physical boundaries regarding the error-balancing behavior of plain least-squares minimization over bounded image domains. While the proposed system successfully bypasses decoupled steganographic pipelines and drastically accelerates decryption via multidimensional vectorized NumPy arrays, the continuous optimization pass inherently introduces structural security compromises even under low-degree configurations.

Because the plain continuous solver lacks strict localized boundary enforcement, it minimizes global residual energy by concentrating the structural variance of the secret intercept into specific weak channels. This distribution profile creates highly degraded "sacrificed shares" that experience extreme visual quality drops down to a minimum boundary of 12.79 dB. Consequently, sub-threshold configurations that utilize these high-leakage assets successfully resolve highly coherent and recognizable projections of the secret image, breaking the traditional information-theoretic security isolation of sub-threshold groups. These empirical findings provide a vital baseline, confirming that minimizing global least-squares error is insufficient for visual cryptography and demonstrating the absolute necessity for balance-aware penalty functions.

B. *Future Work*

To resolve the inherent limitations identified within this framework—specifically the minor reconstruction drift caused by post-optimization integer clipping—future iterations of this research will explore the deployment of Linear Programming (LP) solvers. By encoding the valid dynamic image range ($0 \leq p(i) \leq 255$) directly as strict linear constraints during the optimization pass, the system can eliminate the need for independent clipping projections. Additionally, exploring Minimax (Chebyshev Approximation) strategies will be considered to minimize the maximum absolute error bound rather than the global average residual, potentially mitigating localized ghosting artifacts and elevating the reconstruction fidelity to a perfectly lossless standard.

Repository Link at Github

https://github.com/angkaberapa/Honey-Shamir-Secret-Sharing-Scheme-for-Digital-Images

Acknowledgment

The author would like to express sincere gratitude to God Almighty for blessings and grace in writing this paper. The author would also like to thank Dr. Ir. Rinaldi Munir, M.T., for being a very supportive lecturer of II4021 Cryptography.

References

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[2] Z. Tan, L. Wang, and W. Wang, "A reversible and lossless secret image sharing scheme with authentication for color images," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 8, pp. 101673, Oct. 2023.

[3] A. Juels and T. Ristenpart, "Honey encryption: Security beyond the brute-force bound," *IEEE Security & Privacy*, vol. 12, no. 4, pp. 59-62, July/Aug. 2014.

[4] R. Munir, "Skema pembagian data rahasia (Secret sharing scheme)," *Bahan Kuliah II4021 Kriptografi*, Program Studi Sistem dan Teknologi Informasi, STEI ITB, unpublished, 2026. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2025-2026/36-Skema-Pembagian-Data-Rahasia-2026.pdf

[5] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*, 2nd ed. Upper Saddle River, NJ: Pearson-Prentice Hall, 2006, pp. 385-392.

[6] FMIsec, "Pengenalan shamir secret sharing dan implementasi," *Medium*, June 2024. Available: https://medium.com/fmisec/pengenalan-shamir-secret-sharing-dan-implementasi-2a52bdbbe81d .

Statement

I hereby declare that the paper I wrote is my own writing, not an adaptation or translation of someone else's paper, and is not plagiarized.

Bandung, 19 Juni 2026

Michael Alexander Angkawijaya
NIM 13523102