http://dx.doi.org/10.62762/TISC.2025.186894

PERSPECTIVE

Singularity Cipher: A Topology-Driven Cryptographic Scheme Based on Visual Paradox and Klein Bottle Illusions

Abraham Itzhak Weinberg [1,*]

[1] AI-WEINBERG, AI Experts, Tel-Aviv, Israel

Abstract

This paper presents the Singularity Cipher, a novel cryptographic-steganographic framework that integrates topological transformations and visual paradoxes to achieve multidimensional security. Inspired by the non-orientable properties of the Klein bottle—constructed from two Möbius strips—the cipher applies symbolic twist functions to simulate topological traversal, producing high confusion and diffusion in the ciphertext. The resulting binary data is then encoded using perceptual illusions, such as the missing square paradox, to visually obscure the presence of encrypted content. Unlike conventional ciphers that rely solely on algebraic complexity, the Singularity Cipher introduces a dual-layer approach: symbolic encryption rooted in topology and visual steganography designed for human cognitive ambiguity. This combination enhances both cryptographic strength and detection resistance, making it well-suited for secure communication, watermarking, and plausible deniability in adversarial environments. The paper formalizes the architecture, provides encryption and decryption algorithms, evaluates security properties, and compares the method against classical, post-quantum, and steganographic approaches. Potential applications and future research directions are also discussed.

Keywords: topological cryptography, visual steganography, klein bottle cipher, post-quantum security, cognitive encryption.

1 Introduction

In the modern digital landscape, cryptographic systems must balance not only mathematical strength but also resistance to increasingly subtle forms of analysis, such as pattern recognition, statistical inference, and even human visual inspection [1]. Traditional cryptosystems, such as Advanced Encryption Standard (AES) [2], Rivest–Shamir–Adleman (RSA) [3], and post-quantum candidates like Kyber [4], focus predominantly on algebraic hardness assumptions. However, they often lack perceptual or structural

Academic Editor:
Donghua Jiang

Submitted: 08 July 2025
Accepted: 31 July 2025
Published: 19 August 2025

Vol. 1, **No.** 1, 2025.
10.62762/TISC.2025.186894

***Corresponding author:**
✉ Abraham Itzhak Weinberg
aviw2010@gmail.com

Citation
Weinberg, A. I. (2025). Singularity Cipher: A Topology-Driven Cryptographic Scheme Based on Visual Paradox and Klein Bottle Illusions. *ICCK Transactions on Information Security and Cryptography*, 1(1), 38–53.

obfuscation mechanisms that would prevent a message from being detected in the first place [5].

Recent efforts to expand the cryptographic design space have included the integration of chaotic dynamics and data motion [6]. One notable example is the Database in motion Chaos Encryption (DaChE) Algorithm[7], which applies chaos theory to Not only SQL (NoSQL) [1] database systems to introduce dynamic data transformation and enhance security through unpredictable structural evolution. This highlights a broader shift toward multidimensional and structural cryptographic models [8].

This paper introduces the Singularity Cipher, a novel hybrid cryptographic-steganographic approach that combines two rarely integrated domains: topological transformation and visual paradox encoding. Inspired by the geometric structure of the Klein bottle—a non-orientable surface [2] formed by gluing together two Möbius strips [9]—the cipher employs symbolic twist functions to simulate traversal over such a surface, thereby achieving nonlinear confusion and diffusion of plaintext characters.

Following this symbolic encryption, the resulting ciphertext is mapped into a binary form and visually encoded using geometrically paradoxical figures such as the "missing square illusion" [3] [10]. These illusions not only obscure the presence of data but also exploit cognitive biases in human perception [11], introducing a layer of plausible deniability and visual complexity that traditional steganography methods often lack [12].

By combining the mathematical richness of non-orientable topological spaces [13] with the deceptive power of visual illusions [14], the Singularity Cipher aims to extend the cryptographic landscape into new multidimensional territory. While the scheme is not a replacement for established post-quantum cryptography [15], it offers a unique augmentation: an encryption paradigm where visual structure, spatial logic, and topological transformation serve as active components in data protection and concealment. This aligns with emerging frameworks like QUASAR[16], which advocate for adaptable, forward-looking architectures to manage quantum-era risks, emphasizing the need for diversified strategies beyond algebraic hardness.

This paper formalizes the construction of the Singularity Cipher, presents a detailed algorithm, discusses its potential integration with post-quantum cryptographic primitives, and compares it to existing cryptographic and steganographic techniques in terms of functionality, obscurity, and resistance to visual and analytical attacks [17].

1.1 Definition: Singularity Cipher

Singularity Cipher is a novel hybrid cryptographic-steganographic scheme that encodes and encrypts information through a dual-layer system inspired by:

1. **Topological transformations**, particularly Möbius strip twists and Klein bottle traversal [18];
2. **Geometric-paradox-based visual encoding**, such as the missing square illusion [19].

It combines a symbolic twist-based cipher with a visual illusion-based bit encoding to obscure both the presence and the semantic content of a message.

Structure

The cipher operates in two interconnected layers:

1. Topological Cipher Layer (Klein Bottle Simulation): Each symbol $c \in \mathcal{A}$ from a finite alphabet is processed through two Möbius-style modular transformation functions T_i, where $i = 1, 2$, such that:

$$E(c) = T_2(T_1(c)), \quad D(c) = T_1^{-1}(T_2^{-1}(c))$$

This models traversal on a Klein bottle, where orientation and position change non-trivially due to non-orientability [9].

2. Paradox Encoding Layer (Visual Steganography): Binary representations of encrypted data are visually encoded using geometric illusions [19]:

- A `0`-bit is represented by a standard geometric arrangement (e.g., a valid triangle).
- A `1`-bit is represented by a paradoxical arrangement (e.g., a missing square illusion).

[1] NoSQL refers to a database design approach that stores and retrieves data using models other than the traditional table-based structure found in relational databases.

[2] On non-orientable surfaces like the Möbius strip, the lack of a well-defined 'inside' and 'outside' makes it impossible to assign a consistent directional orientation to the boundary.

[3] The missing square puzzle is an optical illusion that exploits the unreliability of visual perception in geometric analysis, making it an ideal candidate for encoding information that appears visually consistent but contains hidden contradictions.

Features

- Nonlinear, reversible symbol transformation inspired by topological surfaces [20].
- Visual obfuscation of data via perceptual paradoxes [21].
- Supports human-verifiable decryption or puzzle-based interfaces [22].
- Can be layered with post-quantum cryptography for added obfuscation [23].

Purpose

Singularity Cipher is designed to:

- Provide an alternative encryption model based on topological and perceptual complexity [24].
- Serve as a covert communication method through visual or physical media [25].
- Explore foundational ideas for future post-quantum steganographic methods [26].

1.2 Uniqueness of This Work

The Singularity Cipher offers a distinctly novel approach to data protection by fusing two rarely connected paradigms: symbolic topological transformations and visual cognitive illusions [27]. Unlike conventional encryption algorithms that operate purely on numeric or algebraic operations [28], this cipher simulates traversal over a Klein bottle—a non-orientable topological surface—using key-based twist functions. Furthermore, it encodes the resulting ciphertext into a visual domain through geometric paradoxes that deceive the observer's perception [29].

This dual-layer mechanism offers not only encryption strength but also stealth and ambiguity. While post-quantum schemes resist decryption by quantum computers [30], they remain visible as encrypted content. In contrast, the Singularity Cipher hides in plain sight, challenging both machines and humans to detect that a message exists at all [31]. This combination of symbolic complexity, visual disguise, and cognitive misdirection defines a new dimension in secure communication and sets this work apart from prior cryptographic and steganographic efforts [32].

To formally capture this multidimensional encryption framework, we coin the term Singularity Cipher to describe the integration of topological symbol manipulation with visual-paradox-based steganography. A formal definition of the Singularity Cipher is presented above.

Paper Organization

The remainder of this paper is organized as follows. Section 2 provides an overview of related work in cryptography, steganography, and topological methods. Section 3 introduces the motivation and theoretical justification for the proposed approach. In Section 4, we describe the system architecture and methodology of the Singularity Cipher. Section 5 details the encryption and decryption algorithms. Section 6 analyzes the security properties of the scheme, while Section 7 compares it with existing cryptographic and steganographic approaches. Section 8 outlines practical applications and use cases. Finally, Section 9 concludes the paper and discusses the directions for future work.

2 Background and Related Work

This section outlines prior work and theoretical foundations related to the Singularity Cipher, specifically in the domains of cryptography, steganography, topological data transformation, and visual paradoxes.

2.1 Cryptography and Nonlinear Transformations

Traditional symmetric-key ciphers such as AES rely heavily on substitution-permutation networks to achieve confusion and diffusion [33, 34]. Post-quantum algorithms, including lattice-based cryptography (e.g., Kyber [4]), code-based schemes [35], and multivariate polynomial systems [36], focus on algebraic structures that are resistant to quantum algorithms like Shor's [37] or Grover's [38].

While effective against brute-force and quantum attacks, these systems do not typically address data obfuscation at the structural or perceptual level [39]. Research into chaotic maps and non-linear geometries for cryptographic use has been limited but growing [6], with some work exploring toroidal and hyperbolic data spaces [40].

2.2 Steganography and Visual Encoding

Steganography focuses on concealing the existence of communication rather than encrypting the message itself [41]. Techniques range from Least Significant Bit (LSB) image embedding [42] to more advanced transformations in the frequency or wavelet domains [43, 44]. However, many of these methods can be detected through statistical steganalysis [45, 46].

The Singularity Cipher differs by using visual paradoxes—specifically illusions involving area and geometry—as a medium of binary encoding [14]. This form of visual encoding resists both automated detection and human suspicion by presenting data as part of a believable, familiar visual structure [63].

2.3 Topological Structures in Computation

Topological concepts have been used in quantum computing (e.g., topological qubits) [47] and in error-correcting codes [48, 49], but they are underutilized in classical cryptography [50]. The Möbius strip and Klein bottle are well-known non-orientable surfaces that exhibit unique traversal properties [51]. When mapped to symbolic data transformations, they provide an opportunity to design reversible but disorienting encryption functions [52].

Some prior research has investigated the use of braid groups and knot theory in cryptographic contexts [53, 54], leveraging their non-commutative properties for key exchange [55]. However, these approaches differ from the current work, which uses topology not for algebraic hardness but for structural encryption and symbol flow disruption [56].

2.4 Cognitive Illusions and Perceptual Security

Visual illusions, such as the "missing square" paradox [10] or Penrose triangle [57], exploit the human visual system's assumptions about geometry, depth, and area [58]. While these illusions have been studied extensively in psychology [59, 60], their application in security is rare [61]. A few steganographic systems have used optical illusions as distraction mechanisms [14], but none have formally encoded binary data within paradoxical constructs [62].

The Singularity Cipher bridges this gap by directly encoding binary digits using illusions whose geometry is locally plausible but globally inconsistent [64]. This creates a system where information is protected not only mathematically but cognitively [65].

3 Motivation

As digital communication becomes increasingly ubiquitous, so does the means and sophistication of adversarial analysis [66]. Traditional cryptographic systems, while mathematically sound, are often optimized solely for computational hardness and do not address deeper structural or perceptual vulnerabilities [67]. Adversaries may not always aim to break a cipher directly; instead, they may seek to detect the presence of encrypted communication, classify it, or infer its metadata through statistical, visual, or behavioral cues [68].

In parallel, the development of quantum computing presents a growing threat to widely deployed cryptographic primitives [69]. While post-quantum cryptography offers strong alternatives grounded in lattice problems, error-correcting codes, or multivariate polynomials [70], it still generally conforms to classical notions of message representation and transmission. There is an emerging need for encryption methods that go beyond mathematical complexity alone—methods that incorporate cognitive misdirection, geometric transformation, and visual ambiguity to protect not just the contents but also the existence of sensitive information [41].

The Singularity Cipher addresses this need through a dual-layer design that draws from distinct disciplines. The topological layer introduces algebraic complexity using the properties of non-orientable surfaces such as the Möbius strip and Klein bottle, known for their non-trivial paths and symmetry-breaking properties that provide cryptographic confusion and diffusion [20]. The visual paradox layer exploits cognitive and perceptual vulnerabilities by hiding binary information inside geometric illusions, leveraging limitations in both human and machine interpretation [71, 72] to make ciphertext not only encrypted but also visually obfuscated.

This multidimensional approach aims to redefine the boundaries of encryption by integrating principles from topology, cognitive science, and optical illusion into cryptographic design [73]. By obscuring not only what is encrypted, but whether anything is encrypted at all, the Singularity Cipher serves as a foundation for systems that are inherently stealthy, obfuscated, and structurally unpredictable—qualities that may prove critical in the post-quantum era and in adversarial environments where data must survive not just decryption attempts, but also detection [74].

4 Singularity Cipher Architecture

The Singularity Cipher is a hybrid cryptographic-steganographic system that integrates both topological and perceptual obfuscation mechanisms across two sequential transformation layers [75]. This section describes the end-to-end data transformation process and outlines the mathematical and visual logic underlying each stage.

4.1 System Overview

Figure 1 illustrates the overall structure of the proposed Singularity Cipher, which operates through two distinct layers:

1. **Topological Cipher Layer**: This layer simulates a Klein bottle traversal by passing each plaintext symbol m through two Möbius-style modular transformations, T_1 and T_2 [9, 76]. These transformations are key-dependent cyclic mappings over a symbol alphabet $\mathcal{A}$ that introduce orientation confusion and nonlinear diffusion [34]. The resulting ciphertext c is structurally resistant to simple inversion without knowledge of both twist parameters.
2. **Paradox Encoding Layer**: The encrypted message c is converted to its binary representation and mapped onto visual elements using perceptual encoding [77]. Each binary digit is rendered as a geometric object: a standard triangle for bit '0', or a paradoxical triangle (e.g., the "missing square" illusion) for bit '1' [10, 59]. This enables steganographic embedding in diagrams, puzzles, or illustrations while leveraging human visual perception ambiguity as concealment [78].

The final output is a composite visual image that not only hides the original message but also embeds structural ambiguity, making detection and decoding by adversaries more complex [79]. The dual-layer approach provides redundant security mechanisms—even if the visual encoding is detected, the underlying topological encryption maintains message protection [80].

4.2 Topological Cipher Layer: Klein Bottle Simulation

The first layer introduces algebraic and spatial complexity through two Möbius-style permutation functions, T_1 and T_2, defined over a finite alphabet $\mathcal{A}$ [81, 82]:

$$E(c) = T_2(T_1(m)), \quad D(c) = T_1^{-1}(T_2^{-1}(c)) \tag{1}$$

Each twist function T_i represents a key-dependent cyclic permutation that may include bitwise reversal, modular shifting, and position-dependent character scrambling [83, 84]. The non-orientable properties of the Klein bottle are simulated by ensuring that applying both T_1 and T_2 introduces irreversible confusion without access to both inverse functions [51]. The traversal mimics the Klein bottle's global self-intersection by causing symbol paths to cross or invert depending on position and context [85].

4.3 Paradox Encoding Layer: Binary-to-Visual Mapping

The ciphertext c is converted to its binary representation b, and each bit is embedded in a visual structure according to the following encoding scheme [86]:

- A bit value of `0` is represented by a standard geometric shape, such as a consistent right triangle.
- A bit value of `1` is represented by a paradoxical image, such as the "missing square" illusion, where the area appears unchanged after rearrangement, despite the presence of a hidden void [87].

These representations are selected for their cognitive plausibility; the visual patterns appear structurally valid but contain implicit contradictions that conceal the data while maintaining plausible deniability [88, 89].

4.4 Visual Assembly and Output Generation

Once the entire binary sequence has been transformed into visual symbols, the output is assembled into a single composite image or diagram [90]. The resulting image can be embedded in physical print, digital documents, or multimedia contexts, enabling both transmission and passive concealment [91].

The system supports both automated and human-decodable decryption, where an observer with prior knowledge of the cipher rules can visually interpret and reconstruct the original binary stream from the image [92, 93]. The encoded message is thus protected by both mathematical permutation and perceptual masking, creating a cryptographic method that operates simultaneously in computational and perceptual domains [94].

5 Algorithm Description

This section formally defines the core procedures of the Singularity Cipher: the encryption and decryption algorithms. Each message is first passed through a symbolic topological transformation layer and then visually encoded using geometric paradoxes.

Let the plaintext be denoted as $m \in \mathcal{A}^*$, where $\mathcal{A}$ is a finite alphabet. Let $K = (k_1, k_2)$ represent

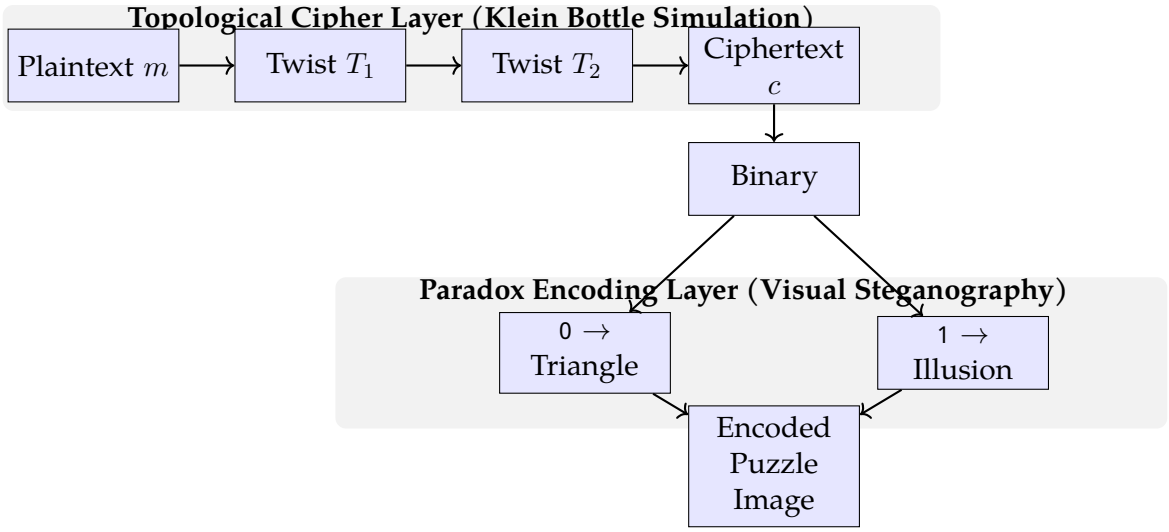

Figure 1. Structure of the Singularity Cipher: a two-layer hybrid encryption scheme combining topological Möbius transformations and visual paradox encoding.

the encryption key, consisting of two permutation parameters defining twist functions T_1 and T_2.

5.1 Encryption Algorithm

Algorithm 1: Singularity Cipher Encryption

Input: Plaintext m, Key $K = (k_1, k_2)$
Output: Visual Cipher Image $\mathcal{I}$

Apply Möbius-style transformation:
$c_1 \leftarrow T_1(m, k_1)$ `// First twist (symbolic reordering)`
$c_2 \leftarrow T_2(c_1, k_2)$ `// Second twist (non-orientable traversal)`
Convert to binary:
$b \leftarrow$ `toBinary`(c_2)
$n \leftarrow$ `length`(b)
foreach *bit* b_i *in* b **do**
  if $b_i = 0$ **then**
    $v_i \leftarrow$ `RenderTriangle()` `// Normal triangle`
  else
    $v_i \leftarrow$ `RenderParadoxIllusion()`
    `// Geometric illusion (e.g., missing area)`
  end
end
$\mathcal{I} \leftarrow$ `AssembleImage`$(v_1, v_2, \ldots, v_n)$
return $\mathcal{I}$

5.2 Decryption Algorithm

The decryption process reverses the encryption procedure by first analyzing the visual cipher image to extract embedded binary information, and then applying inverse topological transformations to recover the original plaintext. The algorithm begins by examining each visual element in the cipher image to distinguish between normal geometric shapes (representing binary 0s) and paradoxical illusions (representing binary 1s). This binary string is then converted back to symbolic form and subjected to inverse Möbius-style transformations, applied in reverse order to systematically undo the topological scrambling performed during encryption.

Algorithm 2: Singularity Cipher Decryption

Input: Visual Cipher Image $\mathcal{I}$, Key $K = (k_1, k_2)$
Output: Recovered Plaintext m

Extract binary string from visual symbols:
$b \leftarrow$ `DecodeBinaryFromImage`$(\mathcal{I})$
Convert binary to ciphertext symbols:
$c_2 \leftarrow$ `fromBinary`(b)
Apply inverse topological transformation:
$c_1 \leftarrow T_2^{-1}(c_2, k_2)$
$m \leftarrow T_1^{-1}(c_1, k_1)$
return m

6 Security Analysis

The security of the Singularity Cipher derives from a combination of symbolic transformation using topological permutation functions and perceptual encoding via geometric paradoxes [95, 96]. This section analyzes its resilience against classical and perceptual attacks.

6.1 Confusion and Diffusion

The topological cipher layer simulates traversal over a non-orientable surface (the Klein bottle), using two key-dependent twist functions T_1 and T_2 [13]. These transformations ensure both confusion and diffusion [34]:

- **Confusion**: Symbol relationships are obscured due to position-dependent permutation and inversion patterns [97]. The non-orientable nature of the Klein bottle makes it difficult to trace the original symbol flow [98].
- **Diffusion**: A single-bit change in the input propagates through both twists, altering multiple output bits due to the nonlinear nature of the permutations [99, 100].

These properties mirror those sought in modern block ciphers, such as avalanche effect and key sensitivity [101, 102].

6.2 Key Space and Resistance to Brute Force

The cipher uses two keys (k_1, k_2), each defining a permutation of the message space. For an alphabet $\mathcal{A}$ of size n, the number of possible permutations is $n!$, making the combined key space size $(n!)^2$ [103].

Even for small alphabets (e.g., $n = 256$), the key space becomes computationally infeasible to exhaust via brute-force search, ensuring high entropy and key unpredictability [104, 105].

6.3 Resistance to Known Plaintext and Ciphertext-Only Attacks

In a ciphertext-only attack, the visual representation of the ciphertext offers little statistical regularity due to the paradox encoding [106, 107]. Known plaintext attacks are also challenging because [108]:

- The symbolic transformation is nonlinear and reversible only with both k_1 and k_2 [109].
- The binary encoding obfuscates character boundaries [110].
- The visual paradoxes disguise data presence, thwarting alignment-based inference [111].

6.4 Steganographic Robustness

Unlike LSB or frequency-domain steganography, the paradox encoding layer does not embed data in noise-prone image features [42, 44]. Instead, it hides data in the semantics of the image itself, using illusions that appear innocuous but carry structured meaning to the receiver [14, 112].

This offers resistance to:

- **Statistical steganalysis**, which typically relies on detecting minor image perturbations [46, 113].
- **Visual inspection**, where the illusion camouflages the presence of any information at all [46, 114].

6.5 Limitations and Assumptions

- The security of the cipher depends on the secrecy of the transformation keys and the correct rendering of paradox images [115, 116].
- Optical distortions, compression artifacts, or automatic image filtering may degrade the ability to decode symbols reliably [117–119].
- The visual encoding assumes that the receiver can correctly interpret geometric illusions; for machine interpretation, trained models may be needed [120, 121].

7 Comparison with Existing Approaches

To contextualize the Singularity Cipher within the broader landscape of cryptographic and steganographic research, we compare its characteristics against several representative systems, including classical encryption schemes, post-quantum algorithms, and visual steganography methods [5, 122]. This analysis reveals the unique positioning of our approach at the intersection of cryptographic security and perceptual concealment.

7.1 Evaluation Framework

We evaluate cryptographic and steganographic systems across five key dimensions that capture both traditional security properties and novel perceptual characteristics [123]:

- **Security Basis**: The underlying mathematical or perceptual foundation providing cryptographic strength [124].
- **Quantum Resistance**: Robustness against quantum attacks, particularly Shor's and Grover's algorithms [37, 38].
- **Visual/Perceptual Layer**: Integration of human perception mechanisms for additional security through cognitive concealment [125].

- **Steganographic Capability**: Ability to hide the existence of encrypted data within seemingly innocent visual content [41].
- **Confusion and Diffusion**: Effectiveness in obscuring input-output relationships through algebraic or topological transformations [34].

7.2 Comparative Analysis

Table 1 presents a comprehensive comparison of the Singularity Cipher against existing cryptographic and steganographic approaches, highlighting the distinctive features of each method.

7.3 Discussion and Implications

The comparative analysis reveals distinct advantages and limitations across different approaches. Classical encryption schemes like AES and RSA provide strong algebraic security through substitution-permutation networks and number-theoretic problems, respectively [2, 3]. However, they lack visual concealment capabilities and are vulnerable to quantum cryptanalysis [126]. Their high confusion and diffusion properties make them excellent for traditional cryptographic applications but render encrypted data easily identifiable [127].

Post-quantum cryptographic algorithms such as Kyber and FrodoKEM address quantum vulnerabilities through lattice-based constructions, offering proven resistance against Shor's algorithm [4, 128, 129]. Despite their quantum robustness, these methods operate within conventional algebraic frameworks and provide no mechanism for visual obfuscation or perceptual concealment [130].

Steganographic approaches like LSB manipulation excel at hiding data existence but offer minimal cryptographic protection [42, 131]. Visual cryptography provides both concealment and some level of security through image-based secret sharing, yet remains vulnerable to various image processing attacks and statistical analysis [132, 133].

The Singularity Cipher occupies a unique position by integrating topological transformations with perceptual illusions, creating a dual-layer security model [94]. This approach combines strong symbolic transformation through Möbius and Klein bottle mappings with cognitive concealment via paradox-based steganography [134, 135]. While its quantum resistance remains theoretically unproven, the topological foundation suggests potential robustness against both classical and quantum attacks [136].

Furthermore, the Singularity Cipher's design philosophy enables hybrid deployment scenarios where it can be combined with established post-quantum algorithms [137, 138]. This layered approach would inherit the computational robustness of proven Post Quantum Cryptography (PQC) schemes while adding structural and visual stealth capabilities unique to our method [139].

The analysis demonstrates that while the Singularity Cipher may not replace high-throughput traditional encryption systems, it offers compelling advantages for scenarios requiring covert, cognitively shielded communication [25, 140]. Its integration of cryptographic strength with perceptual invisibility makes it particularly suitable for applications where both security and concealment are paramount, opening new avenues for secure communication in adversarial environments [141, 142].

8 Applications and Use Cases

The Singularity Cipher offers a unique integration of symbolic encryption and visual steganography, making it particularly well-suited for environments that require both security and covert communication [25]. This section outlines key application domains where the cipher provides distinctive advantages.

8.1 Covert Communication in High-Risk Environments

In authoritarian regimes or conflict zones, the ability to hide not just the content but the very presence of encrypted communication is critical [143, 144]. The Singularity Cipher allows messages to be embedded in seemingly innocent diagrams or illustrations, evading censorship and detection [145]. Since the visual output resembles mathematical puzzles or artwork, it offers plausible deniability [89, 146].

8.2 Steganographic Watermarking for Intellectual Property Protection

The visual paradox layer can be used to encode ownership or licensing metadata directly into scientific illustrations, technical drawings, or architectural blueprints [147, 148]. These hidden watermarks are difficult to detect and remove without specific knowledge of the encoding scheme, providing a novel form of content authentication [149, 150].

Table 1. Comprehensive Comparison of Cryptographic and Steganographic Approaches

Approach	Security Basis	Quantum Resistance	Visual/Perceptual Layer	Steganographic Use
Singularity Cipher (ours)	Topological illusion, Möbius/Klein transformation	Unproven	✓	✓
AES (Symmetric)	Block cipher, substitution-permutation	✗	✗	✗
RSA / ECC	Integer factorization, elliptic curves	✗	✗	✗
Kyber (PQC)	Lattice (MLWE)	✓	✗	✗
FrodoKEM (PQC)	Standard lattice (LWE)	✓	✗	✗
LSB Steganography	Bit-plane manipulation	✗	✗	✓
Visual Cryptography	Image-based XOR sharing	✗	✓	✓
Braid Group Cryptography	Non-abelian algebra / topology	Partial	✗	✗
Chaos-based Crypto	Dynamical systems / sensitivity	Partial	✗	✗
Ambiguous Illusion Encoding	Human perception trick	✗	✓	✓

8.3 Secure Instruction Encoding in Printed or Visual Media

In espionage or intelligence contexts, visual steganography allows instructions or data to be embedded in public media such as posters, packaging, or digital art [151, 152]. The use of paradoxical geometry makes the encoded data accessible only to viewers with specific decoding instructions, adding a layer of obfuscation that is resistant to machine detection [153, 154].

8.4 Human-Perceptual Cryptography for Cognitive Interfaces

The cipher could serve in secure human-machine interfaces where visual illusions trigger specific responses or actions [72, 155]. For example, in Augmented Reality (AR) or heads-up displays, paradoxical encodings may serve as secure tokens that are recognized by trained human agents but remain undecipherable to automated systems [156–158].

8.5 Augmenting Post-Quantum Encryption with Structural Obfuscation

Though not a replacement for standard post-quantum cryptographic algorithms, the Singularity Cipher can augment them by encoding their outputs into paradoxical visual structures [159, 160]. This provides additional defense in depth that combines computational intractability with perceptual stealth [161, 162].

9 Conclusion

This paper introduced the Singularity Cipher, a novel hybrid encryption and steganographic scheme that integrates topological transformations inspired by the Klein bottle with visual paradox-based data encoding. By leveraging symbolic permutations across non-orientable geometries and embedding binary data in perceptually deceptive visual structures, the cipher offers multidimensional security that goes beyond traditional mathematical hardness assumptions.

We demonstrated that the cipher provides strong confusion and diffusion, a large key space, and enhanced stealth through cognitive and perceptual obfuscation. In contrast to classical and post-quantum cryptographic systems, which focus primarily on algorithmic complexity, the Singularity Cipher also addresses the growing need for concealment and plausible deniability in adversarial environments.

The architecture supports applications in covert communication, watermarking, and secure visual

interfaces, particularly where data needs to remain hidden in plain sight. Moreover, the cipher can be combined with post-quantum primitives to create a multi-layered defense strategy that is both computationally secure and visually elusive.

Future work includes formalizing the cipher's resistance to machine learning-based steganalysis, developing automated visual encoders and decoders, and exploring other topological surfaces—such as higher-genus manifolds—as symbolic spaces for encryption. We also anticipate the potential for adaptation in augmented reality and human-centric cryptography, where visual cognition becomes part of the secure communication channel.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Kendhe, A. K., & Agrawal, H. (2013). A survey report on various cryptanalysis techniques. *International Journal of Soft Computing and Engineering (IJSCE), 3*(2), 287-293.

[2] Dworkin, M. J., Barker, E., Nechvatal, J. R., Foti, J., Bassham, L. E., Roback, E., & Dray Jr, J. F. (2001). Advanced encryption standard (AES). *National Institute of Standards and Technology (NIST)*. [CrossRef]

[3] Imam, R., Areeb, Q. M., Alturki, A., & Anwer, F. (2021). Systematic and critical review of rsa based public key cryptographic schemes: Past and present status. *IEEE Access, 9*, 155949–155976. [CrossRef]

[4] Maram, V., & Xagawa, K. (2023). Post-quantum anonymity of Kyber. In *IACR International Conference on Public-Key Cryptography* (pp. 3–35). Springer. [CrossRef]

[5] Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital image steganography: A literature survey. *Information Sciences, 609*, 1451–1488. [CrossRef]

[6] Zhang, B., & Liu, L. (2023). Chaos-based image encryption: Review, application, and challenges. *Mathematics, 11*(11), 2585. [CrossRef]

[7] Weinberg, A. I. (2025). Dynamic Data Defense: Unveiling the Database in motion Chaos Encryption (DaChE) Algorithm–A Breakthrough in Chaos Theory for Enhanced Database Security. *arXiv preprint arXiv:2501.03296*.

[8] Lv, X., Zhong, Y., & Tan, Q. (2020). A study of bitcoin de-anonymization: Graph and multidimensional data analysis. In *2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)* (pp. 339–345). IEEE. [CrossRef]

[9] Putz, M. V., & Ori, O. (2020). Topological symmetry transition between toroidal and klein bottle graphenic systems. *Symmetry, 12*(8), 1233. [CrossRef]

[10] Ninio, J. (2014). Geometrical illusions are not always where you think they are: a review of some classical and less classical illusions, and ways to describe them. *Frontiers in Human Neuroscience, 8*, 856. [CrossRef]

[11] Pohl, R. F. (2022). What are cognitive illusions? In *Cognitive Illusions* (pp. 3–23). Routledge. [CrossRef]

[12] Anderson, R. J., & Petitcolas, F. A. P. (1998). On the limits of steganography. *IEEE Journal on Selected Areas in Communications, 16*(4), 474–481. [CrossRef]

[13] Fuladi, N., Hubard, A., & de Mesmay, A. (2024). Short topological decompositions of non-orientable surfaces. *Discrete & Computational Geometry, 72*(2), 783–830. [CrossRef]

[14] Jiao, S., & Feng, J. (2021). Image steganography with visual illusion. *Optics Express, 29*(10), 14282–14292. [CrossRef]

[15] Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature, 605*(7909), 237–243. [CrossRef]

[16] Weinberg, A. I. (2025). Preparing for the Post Quantum Era: Quantum Ready Architecture for Security and Risk Management (QUASAR)–A Strategic Framework for Cybersecurity. *arXiv preprint arXiv:2505.17034*.

[17] Shamir, A. (1998, May). Visual cryptanalysis. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 201-210). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[18] Clack, C. D., & Courtois, N. T. (2019). Distributed Ledger Privacy: Ring Signatures, Möbius and CryptoNote. *arXiv preprint arXiv:1902.02609*.

[19] Ponticorvo, M., & Miglino, O. (2010). Encoding geometric and non-geometric information: a study with evolved agents. *Animal Cognition, 13*, 157–174. [CrossRef]

[20] Yao, B., & Mu, Y. (2018, December). Mathematical Problems From Topological Graphic Passwords of Cryptography. In *2018 IEEE 4th Information Technology*

and Mechatronics Engineering Conference (ITOEC) (pp. 1897-1903). IEEE. [CrossRef]

[21] Chen, J. W., Chen, L. J., Yu, C. M., & Lu, C. S. (2021). Perceptual indistinguishability-net (pi-net): Facial image obfuscation with manipulable semantics. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 6478-6487). [CrossRef]

[22] Yang, C. N., Sun, L. Z., Yan, X., & Kim, C. (2016). Design a new visual cryptography for human-verifiable authentication in accessing a database. *Journal of Real-Time Image Processing, 12*, 483–494. [CrossRef]

[23] Edwards, M., Mashatan, A., & Ghose, S. (2020). A review of quantum and hybrid quantum/classical blockchain protocols. *Quantum Information Processing, 19*(6), 184. [CrossRef]

[24] Polovnikov, K., Kazakov, V., & Syntulsky, S. (2020). Core–periphery organization of the cryptocurrency market inferred by the modularity operator. *Physica A: Statistical Mechanics and its Applications, 540*, 123075. [CrossRef]

[25] Makhdoom, I., Abolhasan, M., & Lipman, J. (2022). A comprehensive survey of covert communication techniques, limitations and future challenges. *Computers & Security, 120*, 102784. [CrossRef]

[26] Gabriel, A. J., Alese, B. K., Adetunmbi, A. O., & Adewale, O. S. (2013). Post-quantum crystography: a combination of post-quantum cryptography and steganography. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)* (pp. 449–452). IEEE. [CrossRef]

[27] Myers, A., Kvinge, H., & Emerson, T. (2023). TopFusion: Using topological feature space for fusion and imputation in multi-modal data. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 600–609). [CrossRef]

[28] Yegireddi, R., & Kumar, R. K. (2016). A survey on conventional encryption algorithms of Cryptography. In *2016 International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1–4). IEEE. [CrossRef]

[29] Ryu, D., Abernethy, B., Park, S. H., & Mann, D. L. (2018). The perception of deceptive information can be enhanced by training that removes superficial visual information. *Frontiers in Psychology, 9*, 1132. [CrossRef]

[30] Kappler, S. A., & Schneider, B. (2022). Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms. *Proceedings of the Society, 84*, 61–71. [CrossRef]

[31] Baluja, S. (2017). Hiding images in plain sight: Deep steganography. *Advances in Neural Information Processing Systems, 30*. [CrossRef]

[32] Taha, M. S., Mohd Rahim, M. S., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of steganography and cryptography: A short survey. In *IOP Conference Series: Materials Science and Engineering* (Vol. 518, No. 5, p. 052003). IOP Publishing. [CrossRef]

[33] Dhall, S., & Yadav, K. (2024). Cryptanalysis of substitution-permutation network based image encryption schemes: a systematic review. *Nonlinear Dynamics, 112*(17), 14719–14744. [CrossRef]

[34] Qayyum, A., Ahmad, J., Boulila, W., Rubaiee, S., Masood, F., Khan, F., ... & Buchanan, W. J. (2020). Chaos-based confusion and diffusion of image pixels using dynamic substitution. *IEEE Access, 8*, 140876–140895. [CrossRef]

[35] Overbeck, R., & Sendrier, N. (2009). Code-based cryptography. In *Post-quantum cryptography* (pp. 95–145). Springer. [CrossRef]

[36] Dey, J., & Dutta, R. (2023). Progress in multivariate cryptography: Systematic review, challenges, and research directions. *ACM Computing Surveys, 55*(12), 1–34. [CrossRef]

[37] Ugwuishiwu, C. H., Orji, U. E., Ugwu, C. I., & Asogwa, C. N. (2020). An overview of quantum cryptography and shor's algorithm. *Int. J. Adv. Trends Comput. Sci. Eng, 9*(5). [CrossRef]

[38] Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2016). Applying Grover's algorithm to AES: quantum resource estimates. In *International Workshop on Post-Quantum Cryptography* (pp. 29–43). Springer. [CrossRef]

[39] Horváth, M., & Buttyán, L. (2020). *Cryptographic Obfuscation: A Survey*. Springer.

[40] Gençoğlu, M. T. (2017). Cryptanalysis of a new method of cryptography using laplace transform hyperbolic functions. *Communications in Mathematics and applications, 8*(2), 183.

[41] Ke, Y., Liu, J., Zhang, M. Q., Su, T. T., & Yang, X. Y. (2018). Steganography security: Principle and practice. *IEEE Access, 6*, 73009–73022. [CrossRef]

[42] Bansal, K., Agrawal, A., & Bansal, N. (2020). A survey on steganography using least significant bit (lsb) embedding approach. In *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)* (pp. 64–69). IEEE. [CrossRef]

[43] Yadahalli, S. S., Rege, S., & Sonkusare, R. (2020). Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques. In *2020 5th international conference on communication and electronics systems (ICCES)* (pp. 1325–1330). IEEE. [CrossRef]

[44] Joshi, S. V., Bokil, A. A., Jain, N. A., & Koshti, D. (2012). Image steganography combination of spatial and frequency domain. *International Journal of Computer Applications, 53*(5), 25–29.

[45] De La Croix, N. J., Ahmad, T., & Han, F. (2024).

Comprehensive survey on image steganalysis using deep learning. *Array*, 100353. [CrossRef]

[46] Fridrich, J., & Goljan, M. (2002). Practical steganalysis of digital images: state of the art. *Security and Watermarking of Multimedia Contents IV, 4675*, 1–13. [CrossRef]

[47] Stern, A., & Lindner, N. H. (2013). Topological quantum computation—from basic concepts to first experiments. *Science, 339*(6124), 1179–1184. [CrossRef]

[48] de Albuquerque, C. D., da Silva, E. B., & Soares, W. S. (2022). *Quantum Codes for Topological Quantum Computation*. Springer.

[49] Yao, X. C., Wang, T. X., Chen, H. Z., Gao, W. B., Fowler, A. G., Raussendorf, R., ... & Pan, J. W. (2012). Experimental demonstration of topological error correction. *Nature, 482*(7386), 489–494. [CrossRef]

[50] Song, S., & Li, H. (2025). Can topological transitions in cryptocurrency systems serve as early warning signals for extreme fluctuations in traditional markets? *Physica A: Statistical Mechanics and its Applications, 657*, 130194. [CrossRef]

[51] Polthier, K. (2003). Imaging maths-Inside the Klein bottle. Retrieved from http://plus.maths.org/content/imaging-maths-inside-klein-bottle.

[52] Micciancio, D., & Panjwani, S. (2005). Adaptive security of symbolic encryption. In *Theory of Cryptography Conference* (pp. 169–187). Springer. [CrossRef]

[53] Dehornoy, P. (2004). Braid-based cryptography. *Contemp. Math, 360*(5), 33.

[54] Sconza, S., & Wildi, A. (2024). Knot-based Key Exchange protocol. *Cryptology ePrint Archive*.

[55] Ko, K. H., Lee, S. J., Cheon, J. H., Han, J. W., Kang, J. S., & Park, C. (2000). New public-key cryptosystem using braid groups. In *Advances in Cryptology—CRYPTO 2000* (pp. 166–183). Springer. [CrossRef]

[56] Barthe, G., Grégoire, B., Jacomme, C., Kremer, S., & Strub, P. Y. (2019). Symbolic methods in computational cryptography proofs. In *2019 IEEE 32nd Computer Security Foundations Symposium (CSF)* (pp. 136–13615). IEEE. [CrossRef]

[57] Draper, S. W. (1978). The Penrose triangle and a family of related figures. *Perception, 7*(3), 283–296. [CrossRef]

[58] Marr, D. (2010). *Vision: A computational investigation into the human representation and processing of visual information*. MIT press.

[59] Jonsson, D. (2022). *Deceptive geometries: Spatial analysis and design through the study of visual illusions*.

[60] Coren, S., & Girgus, J. (2020). *Seeing is deceiving: The psychology of visual illusions*. Routledge. [CrossRef]

[61] Hayashi, E., Dhamija, R., Christin, N., & Perrig, A. (2008). Use your illusion: secure authentication usable anywhere. In *Proceedings of the 4th Symposium on Usable Privacy and Security* (pp. 35–45). [CrossRef]

[62] Goldwasser, S., Micali, S., & Rivest, R. L. (2019). A "paradoxical" solution to the signature problem. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali* (pp. 265–284). [CrossRef]

[63] Bresciani, S., & Eppler, M. J. (2015). The pitfalls of visual representations: A review and classification of common errors made while designing and interpreting visualizations. *Sage Open, 5*(4), 2158244015611451. [CrossRef]

[64] Abbe, E. A. (2008). *Local to global geometric methods in information theory* (Doctoral dissertation, Massachusetts Institute of Technology).

[65] Patel, V. L., Arocha, J. F., & Shortliffe, E. H. (2000). Cognitive models in training health professionals to protect patients' confidential information. *International Journal of Medical Informatics, 60*(2), 143–150. [CrossRef]

[66] Arcos, R., & Smith, H. (2021). Digital communication and hybrid threats. *Revista ICONO 14. Revista científica de Comunicación y Tecnologías emergentes, 19*(1), 1–14. [CrossRef]

[67] Vignesh, R. S., Sudharssun, S., & Kumar, K. J. J. (2009). Limitations of quantum & the versatility of classical cryptography: a comparative study. In *2009 Second international conference on environmental and computer science* (pp. 333–337). IEEE. [CrossRef]

[68] Basyoni, L., Fetais, N., Erbad, A., Mohamed, A., & Guizani, M. (2020). Traffic analysis attacks on tor: A survey. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 183–188). IEEE. [CrossRef]

[69] Faruk, M. J. H., Tahora, S., Tasnim, M., Shahriar, H., & Sakib, N. (2022). A review of quantum cybersecurity: threats, risks and opportunities. In *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (pp. 1–8). IEEE. [CrossRef]

[70] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature, 549*(7671), 188–194. [CrossRef]

[71] Ibrahim, D. R., Teh, J. S., & Abdullah, R. (2021). An overview of visual cryptography techniques. *Multimedia Tools and Applications, 80*, 31927–31952. [CrossRef]

[72] Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications, 48*, 102352. [CrossRef]

[73] Al Maliky, S. B. S., & Abbas, N. A. (2014). Multidisciplinary in Cryptology. In *Multidisciplinary Perspectives in Cryptology and Information Security* (pp. 1–28). IGI Global. [CrossRef]

[74] Bloch, M. (2015). A channel resolvability perspective on stealth communications. In *2015 IEEE international*

symposium on information theory (ISIT) (pp. 2535–2539). IEEE. [CrossRef]

[75] Jassim, K. N., Nsaif, A. K., Nseaf, A. K., Hazidar, A. H., Priambodo, B., Naf'an, E., ... & Putra, Z. P. (2019). Hybrid cryptography and steganography method to embed encrypted text message within image. In *Journal of Physics: Conference Series* (Vol. 1339, No. 1, p. 012061). IOP Publishing. [CrossRef]

[76] Arnold, D. N., & Rogness, J. P. (2008). Möbius transformations revealed. *Notices of the American Mathematical Society, 55*(10), 1226–1231.

[77] Rauschenberger, R., & Yantis, S. (2006). Perceptual encoding efficiency in visual search. *Journal of Experimental Psychology: General, 135*(1), 116. [CrossRef]

[78] Xiang, T., Yang, Y., Liu, H., & Guo, S. (2019). Visual security evaluation of perceptually encrypted images based on image importance. *IEEE Transactions on Circuits and Systems for Video Technology, 30*(11), 4129–4142. [CrossRef]

[79] Cruse, D. A. (2001). Crypto-ambiguity. *Recherches anglaises et nord-américaines, 34*(1), 5–18.

[80] Lord, S., & Nunes-Vaz, R. (2013). Designing and evaluating layered security. *International Journal of Risk Assessment and Management, 17*(1), 19–45. [CrossRef]

[81] Li, S., Li, C., Chen, G., Bourbakis, N. G., & Lo, K. T. (2008). A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Processing: Image Communication, 23*(3), 212–223. [CrossRef]

[82] Tesler, G. (2000). Matchings in graphs on non-orientable surfaces. *Journal of Combinatorial Theory, Series B, 78*(2), 198–231. [CrossRef]

[83] Hehn, T., Milenkovic, O., Laendner, S., & Huber, J. B. (2008). Permutation decoding and the stopping redundancy hierarchy of cyclic and extended cyclic codes. *IEEE Transactions on Information Theory, 54*(12), 5308–5331. [CrossRef]

[84] Ye, G. (2010). Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognition Letters, 31*(5), 347–354. [CrossRef]

[85] Chas, M., & Lalley, S. P. (2012). Self-intersections in combinatorial topology: statistical structure. *Inventiones Mathematicae, 188*(2), 429–463. [CrossRef]

[86] Lin, K. T. (2012). Based on binary encoding methods and visual cryptography schemes to hide data. In *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 59–62). IEEE. [CrossRef]

[87] Dabrowski, A., Weippl, E. R., & Echizen, I. (2013). Framework based on privacy policy hiding for preventing unauthorized face image processing. In *2013 IEEE International Conference on Systems, Man, and Cybernetics* (pp. 455–461). IEEE. [CrossRef]

[88] Halevi, S. (2005). A plausible approach to computer-aided cryptographic proofs. *Cryptology ePrint Archive*.

[89] Chapman, M., & Davida2, G. (2002). Plausible deniability using automated linguistic stegonagraphy. In *International Conference on Infrastructure Security* (pp. 276–287). Springer. [CrossRef]

[90] Dani, P., & Chaudhuri, S. (1995). Automated assembling of images: Image montage preparation. *Pattern Recognition, 28*(3), 431–445. [CrossRef]

[91] Shehab, D. A., & Alhaddad, M. J. (2022). Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research. *Symmetry, 14*(1), 117. [CrossRef]

[92] Khoo, K., Lee, E., Peyrin, T., & Sim, S. M. (2017). Human-readable proof of the related-key security of AES-128. *IACR Transactions on Symmetric Cryptology*, 59–83.

[93] Jena, P. C., & Das, N. K. (2008). A survey on visual cryptography using image encryption and decryption. *Int. J. Emerg. Technol. Adv. Eng*.

[94] Mahalingam, H., Veeramalai, T., Menon, A. R., Subashanthini, S., & Amirtharajan, R. (2023). Dual-domain image encryption in unsecure medium—A secure communication perspective. *Mathematics, 11*(2), 457. [CrossRef]

[95] Yao, B., Wang, X., Ma, F., & Wang, H. (2021). New Encryption Techniques From Lattice Thought In Topological Cryptography. In *2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)* (Vol. 5, pp. 467–473). IEEE. [CrossRef]

[96] Vargas-Olmos, C., Murguia, J. S., Ramírez-Torres, M. T., Mejía, M. C., Rosu, H. C., & Gonzalez-Aguilar, H. (2016). Perceptual security of encrypted images based on wavelet scaling analysis. *Physica A: Statistical Mechanics and its Applications, 456*, 22–30. [CrossRef]

[97] Behnia, S., Akhshani, A., Ahadpour, S., Akhavan, A., & Mahmodi, H. (2009). Cryptography based on chaotic random maps with position dependent weighting probabilities. *Chaos, Solitons & Fractals, 40*(1), 362–369. [CrossRef]

[98] Stone, L. (2014). Metaphors for Abstract Concepts: Visual Art and Quantum Mechanics. *Studio Research, 2*, 14–29.

[99] Liu, J., Zhang, M., Tong, X., & Wang, Z. (2021). Image compression and encryption algorithm based on compressive sensing and nonlinear diffusion. *Multimedia Tools and Applications, 80*, 25433–25452. [CrossRef]

[100] Wu, J., Liao, X., & Yang, B. (2018). Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation. *Signal Processing, 142*, 292–300. [CrossRef]

[101] Ramanujam, S., & Karuppiah, M. (2011). Designing an algorithm with high avalanche effect. *IJCSNS International Journal of Computer Science and Network Security, 11*(1), 106–111.

[102] Bogdanov, A. (2010). *Analysis and design of block cipher constructions*. Citeseer.

[103] Bogdanov, A., Knudsen, L. R., Leander, G., Standaert, F. X., Steinberger, J., & Tischhauser, E. (2012). Key-alternating ciphers in a provable setting: encryption using a small number of public permutations. In *Advances in Cryptology–EUROCRYPT 2012* (pp. 45–62). Springer. [CrossRef]

[104] Pospíšil, J., & Novotný, M. (2012). Lightweight cipher resistivity against brute-force attack: Analysis of PRESENT. In *2012 IEEE 15th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)* (pp. 197–198). IEEE. [CrossRef]

[105] Zhang, B., & Jin, C. (2008). Cryptanalysis of a chaos-based stream cipher. In *2008 The 9th International Conference for Young Computer Scientists* (pp. 2782–2785). IEEE. [CrossRef]

[106] Jiao, S., Lei, T., Gao, Y., Xie, Z., & Yuan, X. (2019). Known-plaintext attack and ciphertext-only attack for encrypted single-pixel imaging. *IEEE Access, 7*, 119557–119565. [CrossRef]

[107] Gao, Y., Wang, Y., Yuan, Q., Wang, T., Wang, X., & Guo, L. (2018). Methods of differential fault attack on LBlock with analysis of probability. In *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)* (pp. 474–479). IEEE. [CrossRef]

[108] Hariss, K., & Noura, H. (2022). Towards a fully homomorphic symmetric cipher scheme resistant to plain-text/cipher-text attacks. *Multimedia Tools and Applications, 81*(10), 14403–14449. [CrossRef]

[109] Hussain, I., & Shah, T. (2013). Literature survey on nonlinear components and chaotic nonlinear components of block ciphers. *Nonlinear Dynamics, 74*, 869–904. [CrossRef]

[110] Popov, I. V., Debray, S. K., & Andrews, G. R. (2007). Binary Obfuscation Using Signals. In *USENIX Security Symposium* (pp. 275–290).

[111] Bagdasaryan, E., Jha, R., Shmatikov, V., & Zhang, T. (2024). Adversarial Illusions in Multi-Modal Embeddings. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 3009–3025).

[112] Huo, Y., Xiang, S., Luo, X., & Zhang, X. (2024). Image Semantic Steganography: A Way to Hide Information in Semantic Communication. *IEEE Transactions on Circuits and Systems for Video Technology*. [CrossRef]

[113] Agarwal, A., Singh, R., Vatsa, M., & Ratha, N. (2020). Image transformation-based defense against adversarial perturbation on deep learning models. *IEEE Transactions on Dependable and Secure Computing, 18*(5), 2106–2121. [CrossRef]

[114] Troscianko, T., Benton, C. P., Lovell, P. G., Tolhurst, D. J., & Pizlo, Z. (2009). Camouflage and visual perception. *Philosophical Transactions of the Royal Society B: Biological Sciences, 364*(1516), 449–461. [CrossRef]

[115] Dagdelen, Ö., Fischlin, M., Gagliardoni, T., Marson, G. A., Mittelbach, A., & Onete, C. (2013). A cryptographic analysis of OPACITY. In *Computer Security–ESORICS 2013* (pp. 345–362). Springer. [CrossRef]

[116] Mabry, F. J., James, J. R., & Ferguson, A. J. (2007). Unicode steganographic exploits: maintaining enterprise border security. *IEEE Security & Privacy, 5*(5), 32–39. [CrossRef]

[117] Kim, K., Kim, J., Song, S., Choi, J. H., Joo, C., & Lee, J. S. (2021). Light lies: Optical adversarial attack. *arXiv preprint arXiv:2106.09908*.

[118] Gschwandtner, M., Uhl, A., & Wild, P. (2007). Transmission error and compression robustness of 2D chaotic map image encryption schemes. *EURASIP Journal on Information Security, 2007*(1), 048179.

[119] Wang, H. J., Guo, C., Simon, D. R., & Zugenmaier, A. (2004). Shield: Vulnerability-driven network filters for preventing known vulnerability exploits. In *Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications* (pp. 193–204). [CrossRef]

[120] Westheimer, G. (2008). Illusions in the spatial sense of the eye: Geometrical–optical illusions and the neural representation of space. *Vision Research, 48*(20), 2128–2142. [CrossRef]

[121] Hu, Y., Yang, S., Yang, W., Duan, L. Y., & Liu, J. (2020). Towards coding for human and machine vision: A scalable image coding approach. In *2020 IEEE International Conference on Multimedia and Expo (ICME)* (pp. 1–6). IEEE. [CrossRef]

[122] Sarveswaran, S., Shangkavi, G., Gowthaman, N., & Vasanthaseelan, S. (2021). Cryptography techniques and internet of things applications–A modern survey. *Int. J. of Aquatic Science, 12*(2), 2338–2371.

[123] Ramakrishna, D., & Shaik, M. A. (2024). A Comprehensive analysis of Cryptographic Algorithms: Evaluating Security, Efficiency, and Future Challenges. *IEEE Access*. [CrossRef]

[124] Lindell, Y. (2017). *Tutorials on the Foundations of Cryptography*. Springer.

[125] Yang, Y., Xiang, T., Lv, X., Guo, S., & Zeng, T. (2023). The illusion of visual security: Reconstructing perceptually encrypted images. *IEEE Transactions on Circuits and Systems for Video Technology, 34*(5), 3998–4010. [CrossRef]

[126] Mitra, S., Jana, B., Bhattacharya, S., Pal, P., & Poray, J. (2017). Quantum cryptography: Overview, security issues and future challenges. In *2017 4th international conference on opto-electronics and applied optics (optronix)* (pp. 1–7). IEEE. [CrossRef]

[127] Abd, A. J., & Al-Janabi, S. (2019). Classification and identification of classical cipher type using artificial neural networks. *Journal of Engineering and Applied Sciences, 14*(11), 3549–3556. [CrossRef]

[128] Guo, Q., Johansson, T., & Nilsson, A. (2020). A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM. In *Annual International Cryptology Conference* (pp. 359–386). Springer. [CrossRef]

[129] Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. *ACM Computing Surveys (CSUR), 51*(6), 1–41. [CrossRef]

[130] Hosseini, S. M., & Pilaram, H. (2024). A Comprehensive Review of Post-Quantum Cryptography: Challenges and Advances. *Cryptology ePrint Archive*.

[131] Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective, 30*(2), 63–87. [CrossRef]

[132] Vyas, C., & Lunagaria, M. (2014). A review on methods for image authentication and visual cryptography in digital image watermarking. In *2014 IEEE International Conference on Computational Intelligence and Computing Research* (pp. 1–6). IEEE. [CrossRef]

[133] Talhaoui, M. Z., Wang, Z., Midoun, M. A., Smaili, A., Mekkaoui, D. E., Lablack, M., & Zhang, K. (2025). Vulnerability Detection and Improvements of an Image Cryptosystem for Real-Time Visual Protection. *ACM Transactions on Multimedia Computing, Communications and Applications, 21*(3), 1–23. [CrossRef]

[134] Peng, S. L., & Zhang, X. S. (1998). Second topological conjugate transformation in symbolic dynamics. *Physical Review E, 57*(5), 5311. [CrossRef]

[135] Yang, Z., Xiang, L., Zhang, S., Sun, X., & Huang, Y. (2021). Linguistic generative steganography with enhanced cognitive-imperceptibility. *IEEE Signal Processing Letters, 28*, 409–413. [CrossRef]

[136] Tzalenchuk, A., Lara-Avila, S., Kalaboukhov, A., Paolillo, S., Syväjärvi, M., Yakimova, R., ... & Kubatkin, S. (2010). Towards a quantum resistance standard based on epitaxial graphene. *Nature nanotechnology, 5*(3), 186–189. [CrossRef]

[137] Fedorov, A. K. (2023). Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together. *Frontiers in Quantum Science and Technology, 2*, 1164428. [CrossRef]

[138] Scientific, L. L. (2025). A multilayered security scheme for data encryption and decryption for stronger security towards post-quantum cryptography in cloud computing. *Journal of Theoretical and Applied Information Technology, 103*(11).

[139] Mikic, M., Srbakoski, M., & Praska, S. (2025). Post-Quantum Stealth Address Protocols. *arXiv preprint arXiv:2501.13733*.

[140] Singh, B., & Cheema, S. S. (2024). Psychological Defenses in Cyberspace: Unveiling the Significance of Cognitive Shields in Cybersecurity. *International Journal of Advanced Networking and Applications, 16*(1), 6291–6295.

[141] Schaefer, R. F., Boche, H., & Poor, H. V. (2015). Secure communication under channel uncertainty and adversarial attacks. *Proceedings of the IEEE, 103*(10), 1796–1813. [CrossRef]

[142] Shamsi, Z., Waikhom, L., Saha, A. K., Patgiri, R., Singha, M. F., & Laiphrakpam, D. S. (2024). Visually meaningful cipher data concealment. *Digital Signal Processing, 155*, 104717. [CrossRef]

[143] Dal, A., & Nisbet, E. C. (2022). Walking through firewalls: Circumventing censorship of social media and online content in a networked authoritarian context. *Social Media+ Society, 8*(4), 20563051221137738. [CrossRef]

[144] Chamales, G., & Baker, R. (2011). Securing crisis maps in conflict zones. In *2011 IEEE Global Humanitarian Technology Conference* (pp. 426–430). IEEE. [CrossRef]

[145] Khan, F., & Gutub, A. (2007). *Message concealment techniques using image based steganography*.

[146] Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer, 31*(2), 26–34. [CrossRef]

[147] Evsutin, O., Melman, A., & Meshcheryakov, R. (2020). Digital steganography and watermarking for digital images: A review of current research directions. *IEEE Access, 8*, 166589–166611. [CrossRef]

[148] Sengupta, A., & Rathor, M. (2019). IP core steganography for protecting DSP kernels used in CE systems. *IEEE Transactions on Consumer Electronics, 65*(4), 506–515. [CrossRef]

[149] Kadian, P., Arora, S. M., & Arora, N. (2021). Robust digital watermarking techniques for copyright protection of digital data: A survey. *Wireless Personal Communications, 118*, 3225–3249. [CrossRef]

[150] Muhammad, K., Ahmad, J., Rho, S., & Baik, S. W. (2017). Image steganography for authenticity of visual contents in social networks. *Multimedia Tools and Applications, 76*, 18985–19004. [CrossRef]

[151] Zebari, D. A., Zeebaree, D. Q., Saeed, J. N., Zebari, N. A., & Adel, A. Z. (2020). Image steganography based on swarm intelligence algorithms: A survey. *people, 7*(8), 9.

[152] Hall, S. (2014). Encoding and decoding the message. In *The discourse studies reader: Main currents in theory*

and analysis (pp. 111–121). John Benjamins.

[153] Kamitani, Y., & Tong, F. (2005). Decoding the visual and subjective contents of the human brain. *Nature neuroscience, 8*(5), 679–685. [CrossRef]

[154] Barkhi, M., Pourhossein, J., & Hosseini, S. A. (2024). Integrating fault detection and classification in microgrids using supervised machine learning considering fault resistance uncertainty. *Scientific Reports, 14*(1), 28466. [CrossRef]

[155] Lin, S., Zhu, J., Yu, W., Wang, B., Sabet, K. A., Zhao, Y., ... & Lin, H. (2022). A touch-based multimodal and cryptographic bio-human–machine interface. *Proceedings of the National Academy of Sciences, 119*(15), e2201937119. [CrossRef]

[156] Syed, T. A., Siddiqui, M. S., Abdullah, H. B., Jan, S., Namoun, A., Alzahrani, A., ... & Alkhodre, A. B. (2022). In-depth review of augmented reality: Tracking technologies, development tools, AR displays, collaborative AR, and security concerns. *Sensors, 23*(1), 146. [CrossRef]

[157] Goyal, V., Ishai, Y., Sahai, A., Venkatesan, R., & Wadia, A. (2010). Founding cryptography on tamper-proof hardware tokens. In *Theory of Cryptography: 7th Theory of Cryptography Conference, TCC 2010* (pp. 308–326). Springer. [CrossRef]

[158] Kaminska, A. (2018). Storing Authenticity at the Surface and into the Depths: Securing Paper with Human-and Machine-Readable Devices 1. *Intermédialités, 32*. [CrossRef]

[159] Gordienko, Y., Trochun, Y., Taran, V., Khmelnytskyi, A., & Stirenko, S. (2025). HNN-QC n: Hybrid Neural Network with Multiple Backbones and Quantum Transformation as Data Augmentation Technique. *AI, 6*(2), 36. [CrossRef]

[160] Sengupta, A., & Rathor, M. (2020). Structural obfuscation and crypto-steganography-based secured JPEG compression hardware for medical imaging systems. *IEEE Access, 8*, 6543–6565. [CrossRef]

[161] Yendamury, G., & Mohankumar, N. (2021). Defense in depth approach on AES cryptographic decryption core to enhance reliability. In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1–7). IEEE. [CrossRef]

[162] Mollicchi, S. (2017). Flatness versus depth: A study of algorithmically generated camouflage. *Security Dialogue, 48*(1), 78–94. [CrossRef]

Abraham Itzhak Weinberg Dr. Weinberg has spent over 30 years in the fields of software and information systems. He had served for six years in the IAF (Israeli Air Force) and retired as a Captain. In recent years, he has managed a BI (business intelligence) unit and data warehousing projects and has consulted data science projects as well as projects integrating big data and cybersecurity. His academic background consists of a BSc in industrial engineering and management as well as computer science, and an MSc in industrial engineering. Dr. Weinberg obtained his PhD in Software and Information Systems Engineering. He also completed his post-doctorate in the United Kingdom. As a lecturer, he had the opportunity to teach BI courses, facilitate seminars, and contribute to the publication of papers in esteemed journals and conferences. His main research interests are focused on Artificial intelligence, Generative AI, data science, Explainable Artificial Intelligence (XAI), big data, quantum finance, and cyber security. (Email: aviw2010@gmail.com)