The ISC Int'l Journal of Information Security

ISeCure

October 2025, Volume 17, Number 3 (pp. 1–10)

http://www.isecure-journal.org

Presented at the ISCISC'2025 in Tehran, Iran.

Dual-Layered Quantum-Secure Concealing: Steganography over Quantum Key Distribution **

Donya Sadat Rezaeishad [1], and Hossein Bahramgiri [2,*]

[1] *Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran*

[2] *Faculty of Electrical and Computer Engineering, Malek-Ashtar University of Technology, Tehran, Iran*

ARTICLE INFO.

Keywords:
Cryptography, Information hiding, Quantum communication, Quantum key management, Security.

Type:

doi:

Abstract

In the quantum computing era, classical encryption faces unprecedented vulnerabilities, while Quantum Key Distribution (QKD) alone remains insufficient for top-secret data transmission due to practical hardware flaws. In this paper, a novel dual-layered framework that integrates steganography with QKD is proposed to enhance security and concealment. The proposed protocol embeds encrypted messages within QKD keys during post-processing, leveraging existing infrastructure without requiring hardware modifications. The message is first compressed, encoded, and encrypted using a pre-shared QKD key via one-time-pad encryption. A block-based search mechanism then hides message bits within the sifted key while preserving statistical randomness. Crucially, this approach provides two-layer security: information-theoretic encryption via QKD and undetectable message existence. Evaluations confirm ultra-low failure probabilities of embedding (below 10^{-12} for 1000-bit messages) and minimal deviations in sifted key length (under 1% for typical blocks). The solution enables eavesdropper detection, maintaining full compatibility with standard QKD post-processing. By unifying steganographic stealth with QKD's theoretical security, this work establishes a practical solution for transmitting top-secret data against evolving quantum threats.

1 Introduction

In today's digital landscape, information security has become increasingly critical due to the rise of extensive cyberattacks and electronic warfare. The advent of quantum computers has rendered classical encryption systems significantly vulnerable. The seminal introduction of Shor's quantum algorithm in 1994 [1] demonstrably compromised the security foundation of RSA cryptography, which relies on the computational complexity of integer factorisation. Moreover, while some classical cryptographic algorithms remain unbroken by current quantum computers, no guarantee exists for their unconditional security against future advancements [2]. A fundamental limitation persists: legitimate communicating parties, conven-

* Corresponding author.

**The ISCISC'2025 program committee effort is highly acknowledged for reviewing this paper.

Email addresses: ds.rezaeishad@ec.iut.ac.ir, bahramgiri@mut.ac.ir

ISSN: 2008-2045

tionally termed Alice and Bob, lack definitive awareness of an eavesdropper's (Eve) presence within the communication channel.

Conversely, QKD has emerged as a theoretically promising solution, offering information-theoretic (unconditional) security based on the principles of quantum mechanics [3, 4]. However, practical implementations of QKD confront significant vulnerabilities stemming from non-ideal hardware components. These imperfections enable sophisticated attacks, including zero-error attacks, which can covertly compromise security without leaving detectable traces [5–7]. Devising comprehensive countermeasures against all known attacks within a QKD system is inherently infeasible. Consequently, post-processing techniques like privacy amplification are typically employed to reduce Eve's information about the generated key. Furthermore, while Measurement-Device-Independent (MDI) QKD protocols [8, 9] offer resistance against specific receiver-side attacks (e.g., detector blinding), they possess inherent limitations: their security guarantees are restricted to detector-side vulnerabilities, and their secure key rates over practical channel distances (short-to-medium range) are significantly lower compared to conventional QKD protocols. Therefore, given the exploitation of all potential security loopholes in electronic warfare scenarios, the transmission of top-secret messages demands a more robust and layered security approach than what standalone QKD can provide.

This critical need for enhanced security serves as the primary motivation for our work. A core vulnerability we aim to address is that an adversary who partially compromises a QKD key is still aware of possessing a valuable cryptographic asset. To mitigate this, we propose integrating a second layer of security that conceals the very existence of the sensitive message.

Steganography—the ancient art of concealing a secret message within an innocuous cover medium (e.g., text, audio, image, or video)—presents a complementary strategy [10, 11]. Unlike cryptography, where the focus is on obscuring the content of the message, the primary objective of steganography is to keep the existence of the message itself hidden. The synergistic integration of steganography with cryptographic techniques has demonstrated significant potential to enhance overall security resilience.

The concept of transmitting a message via steganography and then encrypting it with a key from a QKD protocol has been explored in the literature [12–16]. However, in this paper, we go a step further: we perform steganography over a QKD process. Specifically, we not only utilize encryption with a key from one QKD protocol but also embed the secret message within the post-processing stage of another, separate QKD protocol. This approach provides a clear superiority over existing techniques by leveraging the strengths of both methodologies, ensuring that not only is the content of the message secured and the presence of a potential eavesdropper theoretically detectable (and many eavesdropping attacks are practically detectable), but that its very existence remains undetectable to potential adversaries. By employing this dual-layered strategy, we aim to create a more robust framework for safeguarding sensitive communications in an increasingly hostile digital environment. Similar to how secret information can be imperceptibly embedded into an image's least significant bits (LSB) in classical steganography, our method introduces a novel quantum steganographic approach where a hidden message is embedded within specific positions of a QKD key during its post-processing phase. Despite the randomness of QKD-generated keys, we carefully select locations that allow for embedding deterministic message bits without significantly altering the key's statistical properties.

Our significant contributions to the area include presenting an innovative hybrid protocol for quantum steganography that features the following characteristics:

- *Two Layers of Security*: Designed for the transmission of top-secret information to enhance overall security.
- *Hidden Message Transmission During QKD Process*: The protocol allows for the transfer of a hidden message during the QKD process, where message transmission is not typically expected. The QKD process is usually employed for sharing a completely random key. Consequently, even if an eavesdropper obtains partial information about the key, they will not be aware that the key actually contains a message.
- *Detection of Eavesdroppers*: In the presence of an eavesdropper, legitimate users can theoretically detect their presence, and in many practical cases, the presence of an eavesdropper is identifiable.
- *No Need for New Hardware*: The protocol can be implemented using existing QKD systems without requiring new hardware. Additionally, once the QKD process is completed, the secret message is transmitted without any delay in the transfer of the message from Alice to Bob.

The paper is structured as follows: Section 2 reviews existing work in quantum steganography. Section 3 details our steganography algorithm. Section 4 evaluates our QKD scheme. Section 5 discusses criti-

cal implementation considerations. Finally, Section 6 concludes.

2 Related Work

Quantum steganography has emerged as a promising paradigm for enhancing information security. It leverages principles of quantum mechanics to conceal data within cover media. Current research in this field encompasses the following key directions, among others:

(1) Utilising Quantum Circuits with Classical encryption: Employing quantum circuits in both the embedding and extraction phases to accelerate processing speed or to improve the embedding capacity of information [17–20];
(2) Incorporating QKD-Generated Keys: Combining steganography with keys generated via QKD to achieve theoretically unconditional (information-theoretically secure) encryption [12–16];
(3) Quantum Direct Steganography: Securely transmitting the cover medium using Quantum Secure Direct Communication (QSDC) [21, 22];
(4) Integration with Post-Quantum Cryptography (PQC): Combining quantum steganography with PQC techniques to strengthen cryptographic security [23, 24];
(5) Any Combination of the Above Items.

Recent studies highlight various advancements in this field. Tudorache et al. propose a quantum steganography protocol that adapts the B92 QKD scheme to hide secret messages within grayscale images using the Novel Enhanced Quantum Representation (NEQR) framework, implemented on IBM Quantum Experience via Qiskit [12]. Biswas et al. explore quantum-steganographic security for IoT-enabled smart cities, establishing quantum-secured channels through QKD [13]. Arumugam et al. present a hybrid framework that integrates QKD, Caesar cipher encryption, and LSB steganography to strengthen security against quantum attacks, with particular emphasis on the role of QKD in enhancing the encryption of cover media [14]. Djordjevic integrates covert classical communication channels into the error reconciliation phase of the BB84 QKD protocol, significantly increasing the secret-key rate by preventing eavesdroppers from accessing parity-bit information [15]. Finally, Sykota et al. utilise a dual-layered security system that processes the key through a secure hash algorithm and employs deep learning-based steganography to embed secrets into cover images, further strengthening data security [16].

In this paper, we employ a steganography technique within the QKD process. First, we encrypt the top-secret data using a key generated through QKD. Then, we embed this encrypted data into *another* QKD key and communicate it implicitly during the post-processing phase of the QKD protocol. Our proposed scheme improves both security and stealth by embedding top-secret messages directly within the QKD key exchange process, setting it apart from previous hybrid methods. This approach facilitates undetectable data transfer while also allowing for eavesdropper detection, all without the need for hardware modifications.

3 Proposed Quantum Steganography Scheme

Consider that Alice wants to embed a top-secret message into the QKD key, which serves as the cover medium, using a steganographic technique to share it with Bob. To achieve this, a QKD protocol that incorporates a basis matching phase is selected. This phase involves the selection of keys that correspond to identical bases while discarding those that do not. Notable examples of such protocols include BB84, six-state, E91, and MDI. For conceptual clarity, we employ the widely used BB84 protocol in our scheme; however, the extension to other protocols is straightforward.

Initially, the quantum phase of the protocol is executed. After the completion of the quantum transmission through the quantum channel, the post-processing phase begins via the classical channel. Consider that during the quantum phase, Alice transmits N_0 quantum states to Bob through the quantum channel (All symbols used throughout this paper are summarised in Table 1). Let N denote the number of successful detection events at Bob's receiver. Bob communicates the timing of successful detections along with the bases used during those time slots to Alice through the authenticated channel. Then, Alice compares the bases reported by Bob with her own bases and retains the keys corresponding to identical bases, without disclosing them to Bob. At this point, the embedding process of the top-secret message into the key begins.

Assuming N_s bases match between Alice and Bob out of N total detections; for large N, we expect $N_s/N \approx 1/2$ due to random basis selection. Let $\boldsymbol{K}$ denote the sifted key corresponding to matching bases. Embedding the top-secret message into $\boldsymbol{K}$ presents three critical considerations:

- Key transmission constraint: During the quantum phase, Alice shares a raw key with Bob. Subsequent post-processing (basis sifting, error correction, and privacy amplification) does not permit retransmission of specific key segments for direct bit replacement. To resolve this, we

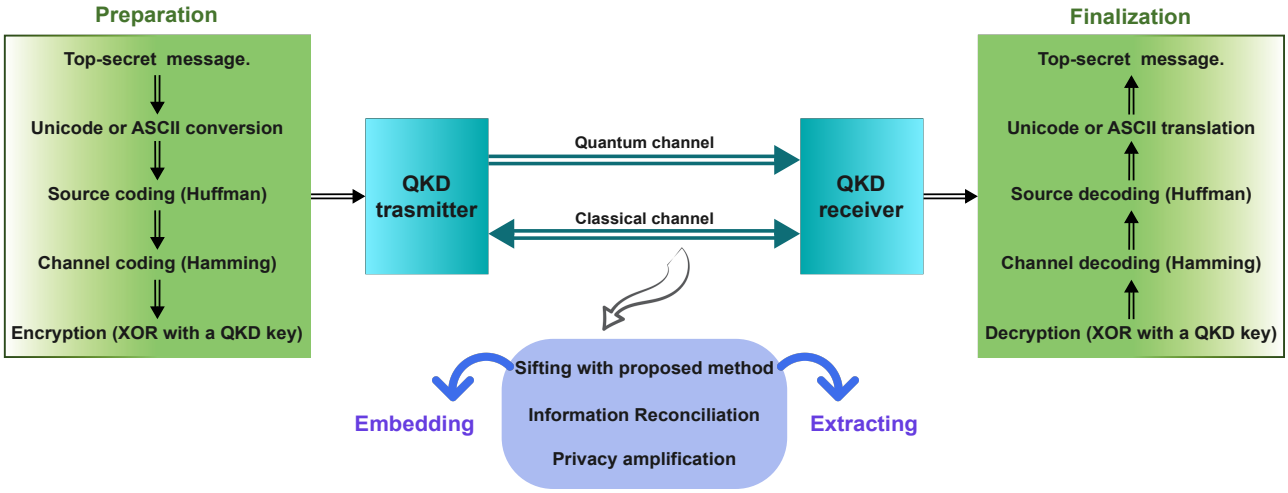

Figure 1. Proposed Quantum Steganography Scheme.

Table 1. List of Symbols Used in the Paper.

Symbol	Description
N_0	Number of transmitted quantum states
N	Number of successful detections events
N_s	Number of bases match
$\boldsymbol{K}$	Sifted key sequence corresponding to matching bases with length N_s
$\boldsymbol{M}$	Secret message after preparation (binarization, compression, channel coding, encryption)
len	Length of sequence $\boldsymbol{M}$
$\boldsymbol{K'}$	Truncated sifted key sequence
N'_s	Number of $\boldsymbol{K'}$
p	Position of prepared secret message in each block
ℓ_{block}	Length of each block in the sequence $\boldsymbol{K'}$
$s_{\max}$	Maximum search threshold
$\boldsymbol{M}^B$	Extracted message sequence with length len
p_{fail}	Failure probability of message embedding
μ	Alice's mean photon number per pulse
Q_μ	Overall detection gain
Y_i	yield of an i-photon state
Y_0	Background rate (including detector dark counts)
η	Overall transmittance
l	Channel length
α	Channel loss coefficient
t_{Bob}	Transmittance of Bob's optical components
η_{D}	Detector efficiency
ℓ_j^{req}	Number of bits from $\boldsymbol{K}$ required to construct the j-th block of $\boldsymbol{K'}$

introduce a novel search mechanism detailed in the following.

- Error correction requirement: Quantum channel imperfections may introduce errors in top-secret bits. An appropriate error-correcting code must be exclusively applied to these bits before steganographic embedding.
- Randomness preservation: Key bits exhibit true quantum randomness. Therefore, if we directly embed the bits of the top-secret message, the key will no longer remain completely random, jeopardising its security. Consequently, we will randomise the encoded message bits by employing a One-Time Pad (OTP) encryption method, utilising XOR with a key previously generated by QKD. Crucially, as with all steganographic systems, the primary security objective remains concealing the existence of the message within the stego-media (shared key).

Figure 1 represents the proposed quantum steganography scheme, which comprises the following steps:

3.1 Preparation phase

Alice first converts the secret message into a binary sequence using, for example, ASCII or Unicode encoding, optionally adding start/end delimiters. The secret message undergoes the following preprocessing steps prior to embedding:

(1) Source coding: Apply lossless compression (e.g., Huffman coding) to minimise the bit-length of the sequence, optimising embedding efficiency.
(2) Channel coding: Implement error-correcting codes (e.g., Hamming codes) to enhance robustness against transmission errors.
(3) Encryption: Perform XOR-based one-time-pad encryption using a pre-shared QKD key, simul-

taneously enhancing security and preserving cryptographic randomness.

The resultant sequence is denoted as $\boldsymbol{M} = \{m_1, m_2, \ldots, m_{\text{len}}\}$ with length len.

3.2 Embedding phase

From the sifted key sequence $\boldsymbol{K} = \{k_1, k_2, \ldots, k_{N_s}\}$, Alice constructs a truncated sequence $\boldsymbol{K'} = \{k'_1, k'_2, \ldots, k'_{N'_s}\}$ where $N'_s < N_s$. The embedding positions are determined such that the j-th message bit m_j occupies the p-th position within the j-th block of $\boldsymbol{K'}$. It is assumed that the length of each block in the sequence $\boldsymbol{K'}$ is equal to ℓ_{block}. The parameters p and ℓ_{block} are mutually agreed upon by Alice and Bob prior to the initiation of the protocol.

For the first block, Alice sequentially transfers bits $\{k_1, \ldots, k_{p-1}\}$ from $\boldsymbol{K}$ to $\boldsymbol{K'}$. If $k_p = m_1$, it is appended to $\boldsymbol{K'}$; otherwise, Alice scans subsequent bits in $\boldsymbol{K}$ until locating $k_i = m_1$ (which is appended to $\boldsymbol{K'}$), discarding all intervening bits. After finding the p-th bit in the sequence $\boldsymbol{K'}$, the remainder of the block is completed based on the sequence $\boldsymbol{K}$. This process repeats for subsequent blocks.

The resulting sequence $\boldsymbol{K'}$ comprises $\lceil N'_s/\ell_{\text{block}} \rceil$ blocks of length ℓ_{block}, except for the last block which may be shorter. When the message length len is less than the number of blocks $\lceil N'_s/\ell_{\text{block}} \rceil$, random padding bits are appended to $\boldsymbol{M}$ to ensure complete block coverage. Explicit start and end delimiters embedded within $\boldsymbol{M}$ enable precise message demarcation during extraction. This structure guarantees unambiguous message recovery by Bob while maintaining statistical consistency with genuine QKD keys. The complete embedding procedure is formalised in Algorithm 1.

To prevent excessive computational overhead, a maximum search threshold $s_{\max}$ is enforced. If any m_j cannot be matched within $s_{\max}$ attempts, the steganographic process aborts, and standard QKD proceeds without embedding. Figure 2 illustrates an example of a successful quantum steganography scheme, while Figure 3 demonstrates a failed scheme.

If Algorithm 1 succeeds, Alice sends the basis list corresponding to the positions of $\boldsymbol{K'}$ If Algorithm 1 fails, Alice instead announces the basis list corresponding to the full sifted key $\boldsymbol{K}$.

If the $\boldsymbol{K'}$ sequence is successfully constructed, Alice announces the bases corresponding to the elements of $\boldsymbol{K'}$ to Bob. In case the steganography scheme fails, Alice announces the bases corresponding to the keys in $\boldsymbol{K}$ to Bob. Here, the sifting stage is completed.

Algorithm 1 Generate Stego-Key from Sifted Key

Input: $\boldsymbol{K}$, $\boldsymbol{M}$, ℓ_{block}, p, $s_{\max}$
Output: $\boldsymbol{K'}$ or "protocol fail"

$j \leftarrow 1$, $i' \leftarrow 1$, $s \leftarrow 0$
for $i = 1, 2, 3, \ldots, N_s$ **do**
  if $i' < (j-1) * \ell_{\text{block}} + p$ **then**
    $k'_{i'} \leftarrow k_i$
    $i' \leftarrow i' + 1$
  else if $i' == (j-1) * \ell_{\text{block}} + p$ **then**
    $s \leftarrow s + 1$
    if $m_j == k_i$ **then**
      $k'_{i'} \leftarrow k_i$
      $i' \leftarrow i' + 1$
      $j \leftarrow j + 1$
      $s \leftarrow 0$
    else if $s \geq s_{\max}$ **then**
      return "protocol fail"
      break
    end if
  end if
end for

3.3 Extracting phase

After Alice announces matching bases via the authenticated channel, Bob retains the keys corresponding to the identical bases and discards the rest (similar to the key sifting stage in conventional QKD). He then partitions the resulting key into blocks of length ℓ_{block} and extracts the p-th bit from each block as the embedded secret message bits.

3.4 Finalization Phase

The remaining bits in the key follow the standard QKD protocol, including the information reconciliation (error correction) and privacy amplification stages [25]. However, for the extracted message sequence, denoted as $\boldsymbol{M}^B = \{m_1^B, m_2^B, \ldots, m_{\text{len}}^B\}$, the following steps are performed to recover the top-secret message:

(1) Decryption: XOR the extracted bits with the encryption key generated in the Section 3.1 to obtain the decrypted message.
(2) Channel decoding: Error correction via syndrome computation using the channel coding scheme (e.g., Hamming code) specified during preparation. This reconciles discrepancies between Alice's original message bits and Bob's extracted bits.
(3) Apply source decoding (e.g., Huffman decoding), followed by delimiter removal, to reconstruct the original secret message.

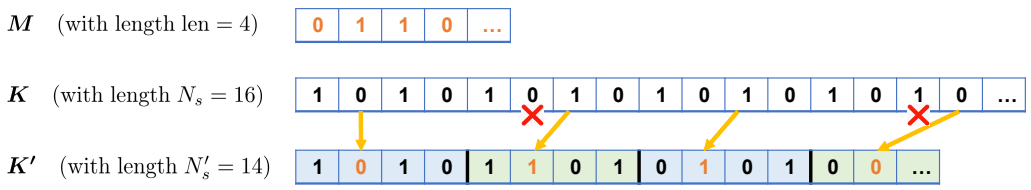

Figure 2. A successful quantum steganography scheme with $p = 2$, $\ell_{\text{block}} = 4$ and $s_{\max} = 5$.

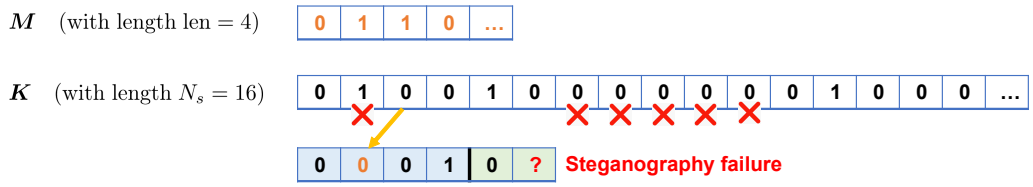

Figure 3. A failed quantum steganography scheme with $p = 2$, $\ell_{\text{block}} = 4$ and $s_{\max} = 5$.

4 Evaluation

This section analyses the proposed QKD-based method for sharing the top-secret message.

4.1 Failure Probability

Protocol failure occurs if, for any message bit m_j, no matching bit is found within the $s_{\max}$ consecutive bits of the sifted key sequence $\boldsymbol{K}$. This happens with probability $2^{-s_{\max}}$ per message bit. Since blocks are independent, the total failure probability is given by

$$p_{\text{fail}} = 1 - \left(1 - 2^{-s_{\max}}\right)^{\text{len}} \approx \frac{\text{len}}{2^{s_{\max}}}, \tag{1}$$

where len is the length of the sequence $\boldsymbol{M}$ to be shared, and the approximation is valid for relatively large $s_{\max}$. For example, with a message length of len = 1000 and a maximum search length of $s_{\max} = 50$, the failure probability is less than 8×10^{-13}.

Note that this failure probability concerns only the embedding of the top-secret message within the QKD key and is independent of the failure probability of the QKD protocol, which is determined by the Quantum Bit Error Rate (QBER) after sifting and subsequent error-correction and privacy-amplification steps.

4.2 Quantum Resource Estimation

The choice of $s_{\max}$ in Section 4.1 must ensure that the len bits of $\boldsymbol{M}$ can be successfully embedded within the QKD key $\boldsymbol{K}$ of length N_s, which is possible if

$$N_s > (\ell_{\text{block}} - 1 + s_{\max})\,\text{len}. \tag{2}$$

The key point here is that Equation 2 represents the worst-case scenario, and the actual required length of $\boldsymbol{K}$ may be smaller than this upper bound, depending on the specific distribution of the message $\boldsymbol{M}$ and the QKD key $\boldsymbol{K}$.

Consider a QKD setup using Weak Coherent Pulses (WCPs) with randomised phases. The photon number per pulse follows a Poisson distribution with parameter μ, representing Alice's expected photon number. The overall detection gain is given by [26]

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} = Y_0 + 1 - e^{-\eta\mu}, \tag{3}$$

where $Y_i = Y_0 + 1 - (1-\eta)^i$ denotes the yield of an i-photon state, Y_0 is the background rate including detector dark counts. Moreover, the overall transmittance is given by

$$\eta = t_{\text{Bob}}\, \eta_{\text{D}}\, 10^{-\alpha l/10}. \tag{4}$$

Here, l represents the channel length, α is the channel loss coefficient (dB/km), while t_{Bob} and η_{D} denote the transmittance of Bob's optical components and detector efficiency, respectively.

For N_0 transmitted signals, the detected pulse count is $N \approx Q_\mu N_0$. With a sifting factor of $\frac{1}{2}$, $\frac{N_s}{N} \approx \frac{1}{2}$. Combining with Equation 2, the required N_0 is

$$N_0 > \frac{2\,(\ell_{\text{block}} - 1 + s_{\max})\,\text{len}}{Q_\mu}. \tag{5}$$

For instance, if $\ell_{\text{block}} = 100$, $s_{\max} = 50$, len = 1000, and $Q_\mu = 0.001$, Equation 5 yields $N_0 > 2.98 \times 10^8$ quantum signals.

If the number of transmitted signals N_0 is fixed and the secret message length len cannot be embedded within a single shared key according to condition Equation 5, the protocol may be extended to multiple QKD rounds so as to accumulate adequate key length for embedding.

4.3 Steganalysis

This section analyses modifications of the QKD protocol introduced by the proposed steganographic scheme. Since the message $\boldsymbol{M}$ is random, the statistical properties of the key sequence bits remain unaffected. Crucially, alterations are confined to the

key-sifting stage, while subsequent processing of the protocol remains unchanged.

The only distinction between the steganographic scheme and the standard QKD implementation lies in the number of shared bases between Alice and Bob, which changes from N_s to N_s'. In what follows, we analytically derive $N_s - N_s'$.

Let ℓ_j^{req} denote the number of bits from $\boldsymbol{K}$ required to construct the j-th block of $\boldsymbol{K'}$, assuming successful embedding in the quantum steganographic scheme. The possible cases are

- $m_j = k_i$ with probability $\frac{1}{2}$, yielding $\ell_j^{\text{req}} = \ell_{\text{block}}$;
- $m_j \neq k_i$ and $m_j = k_{i+1}$ with probability $\frac{1}{2^2}$, yielding $\ell_j^{\text{req}} = \ell_{\text{block}} + 1$;
- ...
- $m_j \neq k_i, k_{i+1}, \ldots, k_{i+s_{\max}-2}$ and $m_j = k_{i+s_{\max}-1}$ with probability $\frac{1}{2^{s_{\max}}}$, yielding $\ell_j^{\text{req}} = \ell_{\text{block}} - 1 + s_{\max}$.

The expected value for ℓ_j^{req} is therefore

$$\begin{aligned}
\mathbb{E}[\ell_j^{\text{req}}] &= \sum_{s=1}^{s_{\max}} \frac{\ell_{\text{block}} - 1 + s}{2^s} \\
&= (\ell_{\text{block}} - 1) \sum_{s=1}^{s_{\max}} \frac{1}{2^s} + \sum_{s=1}^{s_{\max}} \frac{s}{2^s} \\
&= (\ell_{\text{block}} - 1) \left(1 - \frac{1}{2^{s_{\max}}}\right) + 2 - \frac{s_{\max} + 2}{2^{s_{\max}}} \\
&= \ell_{\text{block}} \left(1 - \frac{1}{2^{s_{\max}}}\right) - \frac{s_{\max} + 1}{2^{s_{\max}}} + 1 \\
&\lesssim \ell_{\text{block}} + 1, \qquad (6)
\end{aligned}$$

where the approximation is valid for relatively large $s_{\max}$. Given the values of message length len and block's length ℓ_{block}, the length of sequence $\boldsymbol{K'}$ is

$$N_s' \simeq \ell_{\text{block}} \times \text{len}. \qquad (7)$$

Utilizing Equation 6, the expected length of sequence $\boldsymbol{K}$ is bounded as

$$\mathbb{E}[N_s] \lesssim (\ell_{\text{block}} + 1) \times \text{len}. \qquad (8)$$

Therefore,

$$\mathbb{E}[N_s - N_s'] < \text{len}, \qquad (9)$$

and the fractional distance is

$$\frac{\mathbb{E}[N_s - N_s']}{\mathbb{E}[N_s]} < \frac{1}{\ell_{\text{block}} + 1}. \qquad (10)$$

For instance, in the aforementioned example with $\ell_{\text{block}} = 100$, $s_{\max} = 50$, len $= 1000$, the exact value of $\mathbb{E}[\ell_j^{\text{req}}]$ from Eq.(6) is $\mathbb{E}[\ell_j^{\text{req}}] = 100.\overline{9} \simeq 101$. Moreover, $\mathbb{E}[N_s - N_s'] < 1000$, and the fractional distance is less than 0.01.

4.4 Comparative Evaluation

To rigorously position our proposed protocol within the existing landscape of quantum-safe communication solutions, a comprehensive comparative evaluation is conducted. This analysis benchmarks our dual-layered QKD-based steganography scheme against several alternative approaches, focusing on key criteria: security layer, need for new hardware, quantum attack resistance, eavesdropper detection capability, and practicality. The results are summarised in Table 2.

Our protocol's most significant advantage is its dual security layer, which combines steganographic hiding with QKD-based encryption, while requiring no new hardware. This sets it apart from other methods. Specifically:

- Compared to B92-Inspired Quantum Steganography [12], which offers a single security layer and requires quantum imaging hardware, our approach provides a more practical and cost-effective solution with higher practicality.
- Against classical steganography with QKD encryption [13, 14, 16], our protocol integrates steganography directly within the QKD process, enhancing stealth without additional hardware, whereas these methods rely on classical steganography techniques.
- Unlike classical steganography with PQC [19, 23, 27], which lacks eavesdropper detection and offers only a single security layer, our protocol inherently includes eavesdropper detection through QKD and provides dual-layer security.
- While classical steganography with QSDC [28] offers eavesdropper detection, it requires specialised hardware and has medium practicality, whereas our protocol achieves high practicality with no new hardware needs.

The primary trade-off for our protocol is the initial requirement for a pre-shared QKD key for OTP encryption. Additionally, the embedding process slightly reduces the sifted key rate, though this impact is minimal ($< 1\%$). Future work could focus on optimising key management and embedding efficiency further.

5 Discussion

This section addresses critical implementation considerations and potential vulnerabilities, followed by an assessment of the protocol's practical advantages.

5.1 Steganalysis Countermeasures

As established in Section 4.3, the average decrease in the number of matched-basis bits caused by our embedding procedure is bounded by the message

Table 2. Comparative Analysis of Quantum-Secure Steganography Protocols.

Criterion/Method	Proposed Protocol	B92-Inspired Quantum Steganography [12]	Classical steganography with QKD encryption [13, 14, 16]	Classical steganography with PQC [19, 23, 27]	Classical steganography with QSDC [28]
Security Layer	Dual	Single	Single	Single	Single
New Hardware	No	Yes	No	No	Yes
Quantum Resistance	Yes	Yes	Yes	Yes	Yes
Eavesdropper Detection	Yes	Yes	Yes	No	Yes
Practicality	High	Medium	High	High (software-based)	Medium

length len, and the fractional deficit does not exceed $1/(\ell_{\text{block}} + 1)$. To prevent statistical detectability, it suffices to select ℓ_{block} such that this fractional deficit remains below the natural finite-size fluctuations of the sifting stage.

It is important to emphasise that finite-size effects alone do not expose the existence of hidden data. Even if message presence were somehow suspected, both the positions and the values of the hidden bits remain indistinguishable to an adversary: the positions are selected secretly (described below), and the values are one-time-pad encrypted with an independent QKD key.

However, to further strengthen the dual-layer security architecture, we propose the following protocol modifications:

(1) Reincorporating discarded matched-basis bits: To conceal the deficit in sifted key length introduced by message embedding, Alice reincorporates len bits selected from $\boldsymbol{K}$ but excluded from $\boldsymbol{K'}$ during the search phase. This approach not only masks the embedding-induced reduction, thereby preserving indistinguishability from standard QKD runs, but also increases the effective sifted key length by avoiding the loss of these len bits. Since the p-th bit in each block may not correspond to the embedded message bit, Alice must communicate the hidden message locations to Bob through an authenticated classical channel.

(2) Utilising mismatched-basis bits: Alice appends bits corresponding to basis choices where Alice and Bob initially disagreed (absent in $\boldsymbol{K}$). Since these bits may disagree, Alice and Bob can discard these bits in the post-processing procedure.

5.2 QKD Abortion

A critical consideration involves Quantum Bit Error Rate (QBER) assumptions under active attacks like intercept-resend, where elevated QBER typically triggers protocol abortion. Since message embedding occurs during sifting—prior to QBER estimation—abortion risks partial message compromise. We address this through dual countermeasures: First, the dual-layered security architecture ensures message protection even if $\boldsymbol{M}$ is partially intercepted. Second, we can implement adaptive embedding to enhance robustness. Rather than fixed-position p embedding, this approach utilises random per-block embedding positions. Specifically, prior to protocol execution, Alice generates a random position sequence $\boldsymbol{P} = \{p_1, p_2, \ldots, p_{\text{len}}\}$ where $1 \leq p_j \leq \ell_{\text{block}}$, securely shared with Bob using the proposed fixed-position embedding scheme. If QBER remains within acceptable limits, each message bit m_j is embedded at position p_j of block j in a new random per-block embedding scheme. Should elevated QBER trigger protocol abortion, the system restarts with a newly generated random position sequence.

This adaptive strategy significantly increases security by preventing attackers from predicting embedding locations across protocol iterations, while legitimate parties maintain synchronisation through pre-shared positional keys. The trade-off, however, is a modest increase in overhead: one round of fixed-position embedding is first required to communicate the random position map $\boldsymbol{P}$, followed by the actual message transmission using adaptive embedding. Upon successful protocol completion without abortion, the stego-key is transmitted using the agreed adaptive embedding positions.

5.3 Quantum Secure Direct Communication

The third critical consideration is that secure quantum transmission of messages is achievable using QSDC methods [28]. As discussed in Section 4.4, since QKD has reached a greater level of maturity and both small and large-scale QKD networks are operational globally, the proposed method offers an ideal solution for dual-layer security in the transmission of top-secret messages, utilizing *current technology* without the need for a new quantum experimental setup, thereby enhancing security and increasing the concealment of information through the established QKD setup.

6 Conclusion

This work establishes a novel dual-layered quantum steganographic protocol that fundamentally enhances the security of top-secret data transmission against quantum threats. By embedding encrypted messages directly within QKD keys during post-processing, our approach delivers two critical advancements: (1) *information-theoretic security* via QKD and (2) *undetectable concealment* of the message's existence. Crucially, the protocol achieves this without hardware modifications or transmission delays, leveraging existing QKD infrastructure. Key results include:

- A *Block-based embedding mechanism* preserving cryptographic randomness with ultra-reliable message hiding (failure probability below 10^{-12} for 1,000-bit messages)
- *Low statistical deviations in sifted keys* (under 1% for 100-bit blocks), ensuring compatibility with standard QKD post-processing
- *Inherent eavesdropper detection* capabilities combined with steganographic stealth to prevent adversarial awareness.

This framework sets a new standard for practical quantum-secure communication, offering immediate deployability for high-sensitivity applications. Future work will focus on optimising adaptive embedding parameters and large-scale network integration.

References

[1] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. IEEE, 1994.

[2] Pramode K Verma, Mayssaa El Rifai, and Kam Wai Clifford Chan. *Multi-photon Quantum Secure Communication*. Springer, 2019.

[3] Charles H Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. In *Conf. on Computers, Systems and Signal Processing ,(Bangalore) India*, volume 175, 1984.

[4] Ramona Wolf. *Quantum key distribution*, volume 988. Springer, 2021.

[5] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301–1350, 2009.

[6] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2):025002, 2020.

[7] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *Advances in optics and photonics*, 12(4):1012–1236, 2020.

[8] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical review letters*, 108(13): 130503, 2012.

[9] Marco Lucamarini, Zhiliang L Yuan, James F Dynes, and Andrew J Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705): 400–403, 2018.

[10] Frank Y Shih. *Digital watermarking and steganography: fundamentals and techniques*. CRC press, 2017.

[11] Sabyasachi Pramanik, Mangesh Manikrao Ghonge, Renjith V Ravi, and Korhan Cengiz. *Multidisciplinary approach to modern digital Steganography*. IGI Global, 2021.

[12] Alexandru-Gabriel Tudorache, Vasile Manta, and Simona Caraiman. Quantum steganography based on the b92 quantum protocol. *Mathematics*, 10(16):2870, 2022.

[13] Sujit Biswas, Rajat Subhra Goswami, and K Hemant Kumar Reddy. Advancing quantum steganography: a secure iot communication with reversible decoding and customized encryption technique for smart cities. *Cluster Computing*, 27(7):9395–9414, 2024.

[14] Adhavan Arumugam, Bibin Eswaran, Logavasigaran Ramesh, and C Nallusamy. Quantum-integrated steganography for secure communication using qkd and lsb techniques. In *2025 International Conference on Electronics and Renewable Systems (ICEARS)*, pages 977–983. IEEE, 2025.

[15] Ivan B Djordjevic. Covert/stealth/low-probability of detection communications and qkd. In *Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography*, pages 507–540. Springer, 2025.

[16] Arman Sykot, Md Shawmoon Azad, Wahida Rahman Tanha, BM Monjur Morshed, Syed Emad Uddin Shubha, and MRC Mahdy. Multi-layered security system: Integrating quantum key distribution with classical cryptography to enhance steganographic security. *Alexandria Engineering Journal*, 121:167–182, 2025.

[17] Gaofeng Luo, Ri-Gui Zhou, and WenWen Hu. Efficient quantum steganography scheme using inverted pattern approach. *Quantum Information Processing*, 18(7), 2019.

[18] RS Randhawa, Amey R Hasabnis, and Sanghmitra Rai. Quantum-based colour image steganography. In *2023 10th IEEE Uttar Pradesh Section*

International Conference on Electrical, Electronics and Computer Engineering (UPCON), volume 10, pages 1447–1452. IEEE, 2023.

[19] Aksaj Kumar Bharatwaj and Amey R Hasabnis. Steganography in the quantum era. In *2024 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pages 1–5. IEEE, 2024.

[20] Hao-Ming Dang, Hong-Mei Yang, Dong-Huan Jiang, Bin Yan, Jia-Hao Huang, Xiao-Tong Sun, and Xiang-Hao Yang. A lsb quantum steganography algorithm based on hash encryption. *Quantum Information Processing*, 24(7):1–26, 2025.

[21] Zhi-Guo Qu, Xiu-Bo Chen, Xin-Jie Zhou, Xin-Xin Niu, and Yi-Xian Yang. Novel quantum steganography with large payload. *Optics Communications*, 283(23):4782–4786, 2010.

[22] Ahmed A Abd El-Latif, Bassem Abd-El-Atty, M Shamim Hossain, Samir Elmougy, and Ahmed Ghoneim. Secure quantum steganography protocol for fog cloud internet of things. *IEEE access*, 6:10332–10340, 2018.

[23] Arome Junior Gabriel, Boniface Kayode Alese, Adebayo O Adetunmbi, and Olumide S Adewale. Post-quantum crystography: a combination of post-quantum cryptography and steganography. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, pages 449–452. IEEE, 2013.

[24] Aykut Karakaya and Ahmet Ulu. A survey on post-quantum based approaches for edge computing security. *Wiley Interdisciplinary Reviews: Computational Statistics*, 16(1):e1644, 2024.

[25] Yi Luo, Xi Cheng, Hao-Kun Mao, and Qiong Li. An overview of postprocessing in quantum key distribution. *Mathematics (2227-7390)*, 12(14), 2024.

[26] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Physical Review A*, 72(1):012326, 2005.

[27] Priya Sharma, Vrinda Gupta, and Sandeep Kumar Sood. Post-quantum cryptography research landscape: A scientometric perspective. *Journal of Computer Information Systems*, 65(1):119–140, 2025.

[28] Dong Pan, Gui-Lu Long, Liuguo Yin, Yu-Bo Sheng, Dong Ruan, Soon Xin Ng, Jianhua Lu, and Lajos Hanzo. The evolution of quantum secure direct communication: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*, 26(3):1898–1949, 2024.

Donya Sadat Rezaeishad received her B.Sc. and M.Sc. degrees in Electrical Engineering from Isfahan University of Technology (IUT), Isfahan, Iran, in 2017 and 2019, respectively. She received her Ph.D. in Electrical Engineering from IUT, Isfahan, Iran, in 2025. Her research interests include Quantum Communications (Quantum Key Distribution, Quantum Internet, Quantum Information Theory, Quantum Error Correction), Quantum Random Number Generation, FPGA, and Image Processing.

Hossein Bahramgiri received the B.S. and M.S. degrees in 2000 and 2003, respectively, from Sharif University of Technology, Tehran, Iran, and a PhD degree in 2010 from the University of Tehran, Iran, all in Electrical Engineering. He has been an assistant professor at the Malek-Ashtar University of Technology since 2016, and his research area includes information theory, security and communication networks.