ENGINEERING Information Technology & Electronic Engineering
https://www.academax.com/EITEE; https://www.engineering.org.cn
https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=11344065
E-mail: eng.itee@zju.edu.cn

Engineering Journals
Available on IEEE Xplore®

Research Article
https://doi.org/10.1631/ENG.ITEE.2025.0138

Reversible data hiding in encrypted domain based on NTRU and Chinese remainder theorem

Xinyue ZHANG[§], Kunyi LAI[§], Xin TANG[✉]

School of Cyber Science and Engineering, University of International Relations, Beijing 100091, China

Abstract: Reversible data hiding in the encrypted domain (RDH-ED) based on homomorphic encryption provides a promising approach for privacy-preserving data sharing, yet existing methods based on the N^{th}-degree truncated polynomial ring unit (NTRU) face a fundamental conflict between embedding capacity and reversibility, often requiring preprocessing of plaintext, which in turn compromises randomness of the ciphertext obtained. To address these issues, a novel RDH-ED scheme integrating the Chinese remainder theorem (CRT) with the NTRU cryptosystem is proposed in this study. The proposed scheme operates without any preprocessing of the plaintext and constructs multichannel redundancy in the ciphertext domain, thereby fully preserving the original polynomial structure of the plaintext. By employing a CRT-based encoding, multiple bits of information are enabled to be carried by a single polynomial coefficient, achieving an embedding capacity of 503 bits per polynomial with moderate-sized parameters. Moreover, the embedded data can be extracted before decryption via pre-negotiated coprime parameters, offering greater operational flexibility. Rigorous mathematical constraints ensure that the redundancy term is automatically eliminated during decryption, thereby guaranteeing lossless recovery of the original content. Experimental results demonstrate that the proposed scheme achieves a substantially higher embedding capacity compared to predominant RDH-ED methods based on NTRU, Paillier, and ElGamal cryptosystems, without compromising security or efficiency.

Key words: Reversible data hiding; NTRU cryptosystem; Chinese remainder theorem (CRT); Multichannel redundancy

Unedited

1 Introduction

With the increasing demand for information security and the acceleration of digital transformation, protecting sensitive data while enabling efficient information sharing has become a critical issue. In the plaintext domain, reversible data hiding (RDH) technology has achieved significant progress. For instance, Tang et al. (2020) proposed a weighted average-based complexity calculation for block selection, which improves embedding efficiency. Their subsequent work (Tang et al., 2022a, 2022b) further enhanced block selection strategies based on pixel value ordering and prediction error expansion. However, these methods typically require direct access to the original plaintext data, rendering them unsuitable for privacy-preserving applications.

Against this backdrop, RDH in the encrypted domain (RDH-ED) has been widely adopted. This technique allows additional information to be embedded into encrypted data without compromising confidentiality, while supporting lossless extraction of the hidden data and full recovery of the original content. Specifically, the redundant space in the ciphertext domain is employed to carry additional data. It is especially promising in privacy-critical applications such as medical image transmission and digital rights management. Fig. 1 illustrates different technical frameworks in RDH-ED categorized according to their respective cryptosystems.

Early schemes built on symmetric cryptography (Ma et al., 2013; Liu JF et al., 2015; Yi and Zhou, 2017) often follow a reserving room before encryption (RRBE) strategy, in which embedding space is created in the plaintext domain prior to encryption. In such schemes, RDH is performed by the content owner rather than the data hider. This requirement limits the practicality of these schemes in scenarios where the content owner lacks sufficient processing capability or when the data hiding process is expected to be imperceptible to the content owner, thereby restricting their applicability in flexible encrypted-domain settings. In contrast, public-key

✉ Xin TANG, xtang@uir.edu.cn
Xinyue ZHANG, https://orcid.org/0009-0003-8978-0292
Kunyi LAI, https://orcid.org/0009-0003-7274-8253
Xin TANG, https://orcid.org/0000-0002-5056-124X
CLC number: TP309.7

Received: Nov. 14, 2025; Revision accepted: Mar. 7, 2026;
Crosschecked: Mar. 17, 2026

© The Authors 2026. Published by Zhejiang University Press Co., Ltd. This is an open access article distributed under the terms of the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/)

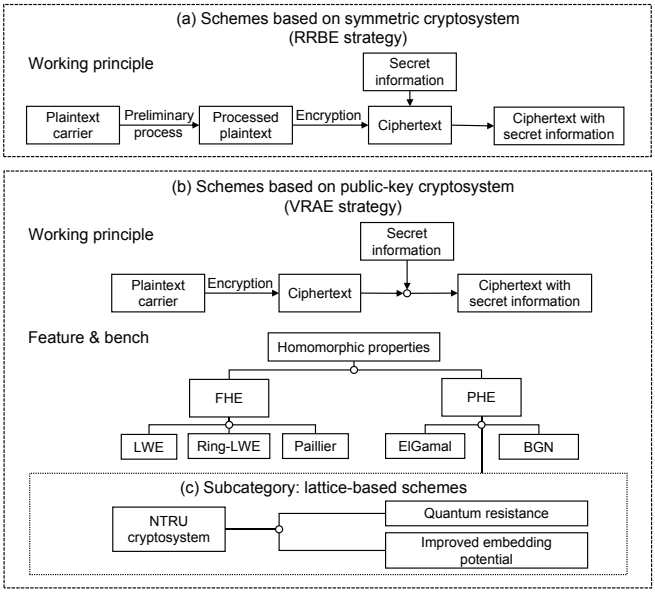

Fig. 1 Technical schemes classified by encryption methods in RDH-ED

cryptosystems, particularly those endowed with homomorphic properties, have been shown to enhance security by enabling data embedding directly in the encrypted domain, and are therefore more closely aligned with the vacating room after encryption (VRAE) paradigm (Qi et al., 2023; Zhou ZY et al., 2024). While these approaches (Ke et al., 2016; Zhang MQ et al., 2016; Zhang XP et al., 2016; Lin et al., 2021; Malik et al., 2022; Kong et al., 2024; Wu et al., 2025) support broader applications, they exhibit low embedding rates and are vulnerable to quantum attacks.

Lattice-based schemes represent a recent advancement in RDH-ED by offering quantum resistance through security mechanisms based on the shortest vector problem (SVP) and closest vector problem (CVP). From the perspective of redundancy generation, these lattice-based approaches can be regarded as VRAE-based RDH-ED methods. Among these, schemes based on the N^{th}-degree truncated polynomial ring unit (NTRU) cryptosystem (Zhou N et al., 2020; Zhang TJ and Li, 2022; Liu DC et al., 2023; Wu et al., 2024) have demonstrated improved embedding potential by using homomorphic properties or noise components. However, a fundamental challenge persists in the inherent conflict between embedding capacity and reversibility. Reversibility requires preserving sufficient unmodified inherent noise for correct decryption, thereby establishing a minimum noise threshold. Conversely, high embedding capacity is achieved by replacing noise with embedded data, creating direct competition for the same noise coefficients. Consequently, embedding capacity is fundamentally limited by the minimum noise required for lossless decryption.

In this context, to substantially improve the embedding capacity while ensuring reversibility, we propose a novel RDH-ED scheme that integrates the Chinese remainder theorem (CRT) with the NTRU cryptosystem. This integration enables high-capacity data embedding through multibit encoding within a single polynomial coefficient. Our contributions can be summarized as follows:

1. We put forward a novel embedding framework based on a multichannel redundancy strategy, which enables multibit data encoding within a single noise coefficient. In this case, it becomes possible to inject structured redundancy that satisfies specific congruence constraints directly into the ciphertext during the standard NTRU encryption process.

2. Then, we focus on designing a separable data extraction and carrier recovery scheme under the proposed framework. Specifically, data extraction is accomplished directly via simple modular arithmetic, while carrier recovery is achieved automatically through standard NTRU decryption by dissolving redundancy terms, with both processes operating independently. Furthermore, the entire process requires no additional complex computations, significantly reducing storage and transmission overhead.

3. We conduct security analysis and experiments on image and text carriers. Both theoretical and experimental results demonstrate that our scheme exhibits significant advantages in security, reversibility, and embedding capacity.

2 Related works

2.1 RDH-ED based on homomorphic public-key cryptosystems

By leveraging homomorphic properties, specific computations can be performed directly on ciphertexts while maintaining plaintext consistency. Existing homomorphic encryption-based RDH-ED methods fall into two categories: fully homomorphic encryption (FHE) and partially homomorphic encryption (PHE).

FHE supports arbitrary computations but faces practical limitations due to high computational overhead. Zhang MQ et al. (2016) proposed a learning with erorrs (LWE)-based RDH-ED method using homomorphic operations, while Ke et al. (2016) introduced a multibit RDH scheme based on Ring-LWE with improved embedding capacity. PHE, supporting either additive or multiplicative homomorphism, offers greater efficiency. The Paillier cryptosystem has been widely adopted in RDH-ED due to its additive homomorphic property. A series of studies has developed Paillier-based RDH-ED schemes by exploiting ciphertext expansion and homomorphic operations (Lin et al., 2021; Malik et al., 2022). Beyond Paillier, other public-key homomorphic encryption schemes have also been investigated for RDH-ED such as ElGamal (Kong et al., 2024) and Boneh–Goh–Nissim (BGN) (Wu et al., 2025).

However, most PHE solutions rely on traditional number-theoretic assumptions vulnerable to quantum attacks, prompting exploration of post-quantum alternatives, which offer both quantum resistance and practical homomorphic properties.

2.2 RDH-ED based on NTRU cryptosystem

Existing NTRU-based approaches generally follow two methodologies: one emphasizing homomorphic properties and the other focusing on direct utilization of noise components.

Regarding homomorphic properties, Zhou N et al. (2020) pioneered this domain by proposing schemes that convert decimal pixel pairs into binary plaintext, pre-process it via difference expansion, and embed information using NTRU's additive homomorphism. However, this approach achieves a

Unedited

maximum embedding rate of only 31 bits per polynomial (bpp) and requires decryption to extract the information, compromising privacy. Zhang TJ and Li (2022) later proposed an NTRU-based reversible dual-watermarking algorithm that enables different users to embed two separate watermarks into the same encrypted image at different stages. While allowing lossless recovery of the original image and full extraction of both watermarks, this method still relies primarily on additive homomorphism without fully exploiting the noise space potential.

In contrast, Liu DC et al. (2023) proposed an RDH-ED scheme based on polynomial partitioning (PP) for NTRU, directly embedding information by modifying redundant segments of the ciphertext polynomial. Each polynomial in the NTRU ring with dimension N can conceal up to $(N-8)$ bits and supports a two-stage operation. Building on this, Wu et al. (2024) introduced polynomial encoding (PE) and polynomial modulation (PM) approaches. PE encodes bitstreams as NTRU-compliant random polynomials, while PM aligns ciphertext coefficient parity with embedded bits. Although PE improves noise term utilization by embedding one bit per coefficient, further enhancement of per-coefficient efficiency remains possible.

3 Preliminaries on NTRU cryptosystem

The NTRU public-key cryptosystem (Hoffstein et al., 1998, 2003), proposed by Hoffstein, Pipher, and Silverman, is recognized as one of the fastest public-key cryptosystems. It is defined over a truncated polynomial ring $R=\frac{\mathbb{Z}[x]}{x^N-1}$, where N is prime and $\mathbb{Z}[x]$ denotes polynomials with integer coefficients. The set R contains all polynomials of degree at most $N-1$, with a general representation:

$$a(x)=a_0+a_1x+\cdots+a_{N-1}x^{N-1}. \tag{1}$$

Here, $a_i\in\mathbb{Z}$ for $i=0,1,\ldots,N-1$. This can also be expressed in coefficient vector form:

$$a(x)=\sum_{i=0}^{N-1}a_ix^i=[a_0,a_1,\ldots,a_{N-1}]. \tag{2}$$

Two fundamental algebraic operations are defined on the ring R: addition and multiplication. For polynomials $a(x)=[a_0,a_1,\ldots,a_{N-1}]$ and $b(x)=[b_0,b_1,\ldots,b_{N-1}]$, addition is performed by summing the corresponding coefficients of like terms:

$$a(x)+b(x)=[a_0+b_0,a_1+b_1,\ldots,a_{N-1}+b_{N-1}]. \tag{3}$$

Multiplication is defined by convolution, denoted as $\otimes$. For $c(x)=a(x)\otimes b(x)=\sum_{k=0}^{N-1}c_kx^k$, the coefficients are given by

$$\begin{aligned}c_k&=\sum_{i=0}^{k}a_ib_{k-i}+\sum_{i=k+1}^{N-1}a_ib_{N+k-i}\\&=\sum_{i+j\equiv k\pmod N}a_ib_j.\end{aligned} \tag{4}$$

3.1 Parameter setting

The construction of the NTRU public-key cryptosystem relies on several core parameters that define the algebraic structure, key space, and security strength. These parameters include:

The polynomial degree N, typically a prime number, defines the polynomial ring $R=\frac{\mathbb{Z}[x]}{x^N-1}$, where all operations are performed as coefficient-modular N^{th}-order cyclic convolution.

The small modulus p, usually a small prime such as $p=3$, defines the plaintext polynomial set $\mathcal{L}_\text{m}$:

$$\mathcal{L}_\text{m}=\left\{m(x)\in R:-\frac{p}{2}<m_i\le\frac{p}{2}\right\}, \tag{5}$$

resulting in $m_i\in\{-1,0,1\}$ when $p=3$.

The large modulus q, a positive integer significantly larger than p with $\gcd(p,q)=1$ and $\gcd(N,q)=1$, serves as the modulus for encryption and decryption processes. Here, gcd denotes the greatest common divisor of integers.

The coefficient distribution parameters d_f, d_g, and d_r define polynomials with coefficients in $\{-1,0,1\}$, where $T(\alpha,\beta)$ denotes the set of polynomials with exactly α coefficients equal to 1, β coefficients equal to -1, and $N-\alpha-\beta$ coefficients equal to 0:

$$\begin{aligned}f(x)&\in\mathcal{L}_\text{f}=T(d_\text{f}+1,d_\text{f}),\\g(x)&\in\mathcal{L}_\text{g}=T(d_\text{g},d_\text{g}),\\r(x)&\in\mathcal{L}_\text{r}=T(d_\text{r},d_\text{r}).\end{aligned} \tag{6}$$

These parameters collectively establish the mathematical foundation for the NTRU cryptosystem.

3.2 Key generation

As a fundamental element of public-key cryptosystems, the key generation process of NTRU is designed to produce a key pair that is mathematically related, comprising a private key that facilitates decryption and signing and a public key that enables encryption and verification. The detailed steps are outlined in Algorithm 1.

Algorithm 1 Key generation

Require: coefficient parameters N,p,q,d_f, and d_g
Ensure: public key $h(x)$ and private key $\langle f(x),F_\text{p}(x)\rangle$
1: randomly select $f(x)\in L_f=T(d_\text{f}+1,d_\text{f})$
2: compute modular inverses $F_\text{p}(x)$ modulo p and $F_\text{q}(x)$ modulo q, satisfying

$$F_\text{p}(x)\otimes f(x)\equiv 1\pmod p$$

$$F_\text{q}(x)\otimes f(x)\equiv 1\pmod q$$

3: **if** $F_\text{p}(x)$ or $F_\text{q}(x)$ does not exist **then**
4: go back to row 1
5: **end if**
6: randomly select $g(x)\in L_\text{g}=T(d_\text{g},d_\text{g})$
7: compute $h(x)=F_\text{q}(x)\otimes g(x)$
8: **return** $h(x),\langle f(x),F_\text{p}(x)\rangle$

3.3 Encryption and decryption

3.3.1 Encryption process

Given a plaintext polynomial $m(x)\in\mathcal{L}_\text{m}$ to be encrypted, the encrypting party uses the public key $h(x)$ and system parameters (N,p,q,d_r) to perform encryption according to the following steps:

Unedited

1. Randomly select $r(x) \in \mathcal{L}_{\mathrm{r}}$ according to the predetermined parameter d_{r};

2. Compute the ciphertext $c(x)$ as follows:

$$c(x) = pr(x) \otimes h(x) + m(x). \tag{7}$$

3.3.2 Decryption process

Given a ciphertext polynomial $c(x)$ to be decrypted, the receiving party uses the private key $\langle f(x), F_{\mathrm{p}}(x)\rangle$ to perform decryption according to the following steps:

1. Compute

$$a(x) = f(x) \otimes c(x) \pmod{q}, \tag{8}$$

and then adjust the coefficients of the resulting $a(x)$ to the range $\left(-\frac{q}{2}, \frac{q}{2}\right]$ through modulo operation;

2. Recover the plaintext

$$m_{\mathrm{decrypted}} = F_{\mathrm{p}}(x) \otimes a(x) = m(x) \pmod{q}, \tag{9}$$

where $m_{\mathrm{decrypted}}$ denotes the decrypted message.

3.4 Improved NTRU systems

The NTRU-Lindner–Peikert–Regev (NTRU-LPR) encryption system is an improved scheme based on NTRU (Wang et al., 2021). In the NTRU-LPR system, the encryption polynomial $c(x)$ incorporates an additional redundant term $pe(x)$. Then, the following equation is derived:

$$c(x) = pr(x) \otimes h(x) + pe(x) + m(x). \tag{10}$$

Apart from the encryption process, the system parameters, key structure, and decryption process remain consistent with those in the standard NTRU.

3.5 Motivation and limitations of NTRU-based RDH-ED schemes

As reviewed above, the NTRU cryptosystem provides several appealing properties for RDH in the encrypted domain, including inherent encryption randomness, a high-dimensional polynomial structure, and a relatively large ciphertext modulus. In particular, due to the randomized sampling in ciphertext generation, a single plaintext may correspond to multiple valid ciphertexts. This one-to-many mapping introduces intrinsic redundancy in the ciphertext space, which has motivated prior research on NTRU-based RDH-ED.

This property has been partially explored in previous studies. In particular, Wu et al. (2024) proposed a PE scheme that exploits the random sampling of the perturbation polynomial $r(x)$ to carry auxiliary information while preserving decryption correctness. These results indicate that the encryption randomness of NTRU can be leveraged for RDH.

However, from a broader perspective, the redundancy of NTRU ciphertexts is not limited to encryption randomness alone. The ciphertext is defined over a high-dimensional polynomial ring with a relatively large modulus, which inherently provides a much larger redundancy space than that exploited by randomness-based approaches. Existing schemes that rely solely on manipulating $r(x)$ therefore use only a limited portion of the available redundancy.

Moreover, current NTRU-based RDH-ED schemes still suffer from several practical limitations. First, data extraction and decryption are often tightly coupled, requiring access to the secret key or modifications to the standard decryption procedure. Second, some schemes impose constraints on ciphertext values or plaintext structures, reducing flexibility in real applications. Third, embedding capacity is typically restricted by the need to preserve sufficient inherent noise for correct decryption, leading to conservative utilization of the ciphertext space.

These observations indicate that, while NTRU provides a rich redundancy structure, its full potential for high-capacity and flexible RDH-ED has not yet been fully explored. This motivates us to investigate NTRU from a different perspective: Instead of further exploiting encryption randomness, we aim to systematically use the redundancy of the ciphertext coefficient space. Based on this insight, the proposed scheme is designed to achieve separable data extraction, full compatibility with standard NTRU encryption and decryption, and substantially enhanced embedding capacity, as detailed in the following section.

4 The proposed method

4.1 A multichannel redundancy embedding framework

The proposed RDH-ED scheme based on NTRU and CRT exploits the inherent noise component of the NTRU-LPR ciphertext as an information carrier. By introducing a structured redundancy construction mechanism, deep coupling between encryption and data embedding is achieved without modifying the standard NTRU encryption and decryption procedures.

First, based on standard NTRU parameter agreement, the sender and receiver pre-negotiate a set of pairwise coprime parameters and extend the modulus q.

Second, after generating the initial ciphertext via NTRU encryption, the sender employs CRT to construct redundant terms satisfying dual congruence constraints, achieving atomic deep coupling between encryption and redundancy construction.

Finally, using the pre-negotiated parameters, data extraction and carrier recovery are fully decoupled at the receiver side. The receiver can directly extract hidden information through modulo operations or automatically eliminate redundant terms via NTRU decryption to recover the original carrier, incurring zero ciphertext expansion and negligible computational overhead.

Through this framework, the proposed scheme achieves high-capacity RDH while preserving separability between information extraction and carrier recovery. The overall framework is illustrated in Fig. 2.

4.2 Parameter initialization and carrier encryption

In addition to the standard NTRU system parameters (N, p, q, d), where $d = d_{\mathrm{f}} = d_{\mathrm{g}} = d_{\mathrm{r}}$, the communicating parties pre-negotiate a set of n_{p} pairwise coprime integers $\{p_i\}_{i=1}^{n_{\mathrm{p}}}$,

Unedited

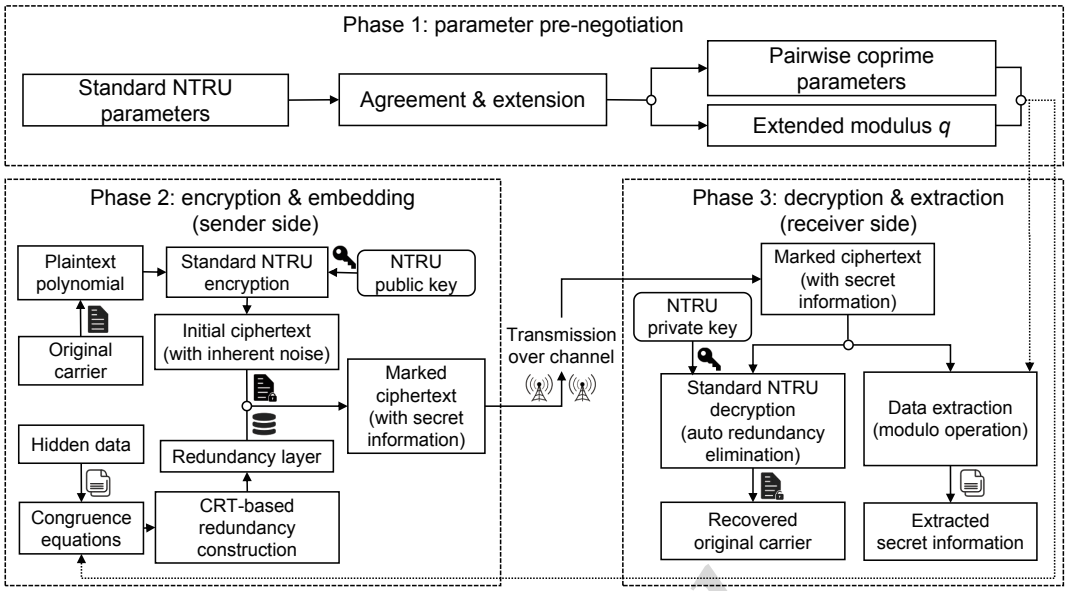

Fig. 2 Algorithm framework

Unedited

which satisfy

$$\gcd(p_i, p_j) = 1, \quad \forall i \neq j, \tag{11}$$

and

$$\gcd(p_i, p) = 1, \quad \gcd(p_i, q) = 1. \tag{12}$$

Each coprime modulus p_i defines an independent embedding channel in the ciphertext domain. Let

$$P = \prod_{i=1}^{n_\mathrm{p}} p_i \tag{13}$$

denote the composite modulus associated with the multichannel redundancy.

To guarantee correct decryption after data embedding, the ciphertext modulus q must satisfy

$$q > \big[(6d+1) + (2d+1)P\big]p. \tag{14}$$

The derivation of this constraint will be provided in Section 4.5.

Given a plaintext polynomial $m(x) \in \mathcal{L}_\mathrm{m}$, the sender generates a standard NTRU ciphertext using the public key $h(x)$ and a randomly selected perturbation polynomial $r(x) \in \mathcal{L}_\mathrm{r}$:

$$c(x) = pr(x) \otimes h(x) + m(x) \pmod q. \tag{15}$$

The resulting ciphertext can be expressed as

$$c(x) = \sum_{i=0}^{N-1} c_i x^i, \tag{16}$$

where each coefficient c_i serves as a potential embedding unit.

4.3 Data embedding via CRT

The proposed data embedding mechanism is built upon the CRT, which provides a rigorous mathematical foundation for constructing multichannel redundancy on each ciphertext coefficient. The detailed data embedding procedure is summarized as follows:

Step 1: secret data representation. The secret data to be embedded are organized into a matrix.

$$\boldsymbol{B}_{N\times n_\mathrm{p}} = \begin{bmatrix} b_{01} & b_{02} & \cdots & b_{0n_\mathrm{p}} \\ b_{11} & b_{12} & \cdots & b_{1n_\mathrm{p}} \\ \vdots & \vdots & & \vdots \\ b_{(N-1)1} & b_{(N-1)2} & \cdots & b_{(N-1)n_\mathrm{p}} \end{bmatrix}, \tag{17}$$

where $b_{ij} \in \{0, 1, \ldots, p_j - 1\}$, $(i = 0, 1, \ldots, N-1;\ j = 1, 2, \ldots, n_\mathrm{p})$. Each row of $\boldsymbol{B}_{N\times n_\mathrm{p}}$ corresponds to the information embedded into one ciphertext coefficient.

Step 2: redundancy construction via CRT. To embed the multichannel data associated with the i^{th} row of $\boldsymbol{B}_{N\times n_\mathrm{p}}$, the i^{th} ciphertext coefficient c_i is mapped into multiple residue channels defined by a set of pairwise coprime moduli $\{p_j\}_{j=1}^{n_\mathrm{p}}$. Specifically, we construct a redundancy coefficient ω_i such that the marked coefficient $c_i + \omega_i$ carries the prescribed residues in all channels.

Formally, ω_i is required to satisfy the following set of congruence constraints:

$$\begin{cases} \omega_i + c_i \equiv b_{i1} \pmod{p_1}, \\ \omega_i + c_i \equiv b_{i2} \pmod{p_2}, \\ \quad \vdots \\ \omega_i + c_i \equiv b_{in_\mathrm{p}} \pmod{p_{n_\mathrm{p}}}, \\ \omega_i \equiv 0 \pmod{p}. \end{cases} \tag{18}$$

Since the moduli $\{p_j\}_{j=1}^{n_\mathrm{p}}$ are pairwise coprime and are also coprime with the plaintext modulus p, the CRT guarantees that the above system admits a solution and that this solution is unique modulo M, where

$$M = p \prod_{j=1}^{n_\mathrm{p}} p_j. \tag{19}$$

This existence and uniqueness property ensures that each residue vector $[b_{i1}, b_{i2}, \ldots, b_{in_\mathrm{p}}]$ is mapped to exactly one redundancy coefficient, forming the mathematical basis of the proposed multichannel embedding mechanism.

Accordingly, ω_i can be explicitly computed as

$$\omega_i = \left[\sum_{j=1}^{n_\mathrm{p}} (b_{ij} - c_i)\frac{M}{p_j}\left(\frac{M}{p_j}\right)^{-1} \bmod p_j\right] \bmod M, \tag{20}$$

where $\left(\frac{M}{p_j}\right)^{-1} \bmod p_j$ denotes the modular multiplicative inverse.

Step 3: marked ciphertext generation. After computing all redundancy coefficients, the redundancy polynomial is formed as

$$\omega(x) = \sum_{i=0}^{N-1} \omega_i x^i. \tag{21}$$

The marked ciphertext with embedded data $c'(x)$ is then obtained by

$$\begin{aligned} c'(x) &= c(x) + \omega(x) \\ &= pr(x) \otimes h(x) + m(x) + \omega(x). \end{aligned} \tag{22}$$

4.4 Separable data extraction and carrier recovery

The proposed scheme is fully separable in the sense that data extraction and carrier recovery can be performed independently, without requiring one operation as a prerequisite for the other.

Case 1: data extraction without cipher decryption. When only the embedded data are required, the receiver directly applies modular reduction to each marked ciphertext coefficient using the pre-negotiated coprime parameters. Specifically, for the i^{th} coefficient, the embedded information is obtained as

$$b_{ij} \equiv c'_i \pmod{p_j}, \quad j = 1, 2, \ldots, n_p. \tag{23}$$

Since the redundancy term is constructed to satisfy the congruence relations in Section 4.3, all embedded data can be extracted directly from the ciphertext without performing NTRU decryption or accessing the private key.

Case 2: carrier recovery without data extraction. When only the original carrier is required, the receiver performs standard NTRU decryption on the marked ciphertext $c'(x)$. Specifically, the decryption process is given by

$$a(x) = f(x) \otimes c'(x) \pmod{q}, \tag{24}$$

followed by coefficient centering and plaintext recovery:

$$\begin{aligned} m_{\mathrm{decrypted}} = F_p(x) \otimes a(x) &\equiv m(x) + \omega(x) \\ &\equiv m(x) \pmod{p}. \end{aligned} \tag{25}$$

Since the redundancy term satisfies $\omega(x) \equiv 0 \pmod{p}$ by construction, it is automatically eliminated during the modulo-p reduction step, thereby ensuring perfect recovery of the original carrier without requiring data extraction.

4.5 Solvability condition

The correctness of NTRU decryption relies on bounding the coefficient magnitude of

$$f(x) \otimes c(x) = pr(x) \otimes g(x) + m(x) \otimes f(x). \tag{26}$$

For standard NTRU encryption, correct decryption is guaranteed if

$$q > (6d + 1)p. \tag{27}$$

After embedding, the ciphertext becomes $c'(x) = c(x) + \omega(x)$, which yields

$$f(x) \otimes c'(x) = f(x) \otimes c(x) + f(x) \otimes \omega(x). \tag{28}$$

Since $\omega(x) = pe(x)$ and the maximum coefficient magnitude of $f(x) \otimes e(x)$ is bounded by $(2d+1)P$, correct decryption is ensured if

$$q > \big[(6d + 1) + (2d + 1)P\big]p, \tag{29}$$

which is identical to the constraint given in inequality (14).

Accordingly, with the polynomial length N unchanged, the modulus expansion ratio before and after embedding is

$$\frac{q'}{q} = 1 + \frac{(2d + 1)P}{6d + 1}. \tag{30}$$

5 Experimental results and analysis

5.1 Feasibility verification

To verify the feasibility and reversibility of the proposed scheme, experiments are conducted on both image and text carriers. The objective is to demonstrate lossless recovery of the original carrier after decryption and error-free extraction of the embedded data.

For image experiments, the baboon image is selected as the carrier image and the Lena image as the embedded secret image, as shown in Fig. 3. After decryption, the recovered carrier image in Fig. 3c is identical to the original carrier one shown in Fig. 3a. Owing to the mathematically exact coefficient-level recovery, the mean squared error (MSE) is zero, leading to an infinite peak signal-to-noise ratio (PSNR). Similarly, the extracted secret image in Fig. 3d perfectly matches the original secret one in Fig. 3b.

To further validate generality, text data are also tested, as illustrated in Fig. 4. The decrypted carrier text is fully restored without any distortion, and the embedded secret text is extracted without errors. These results confirm that the proposed scheme supports perfectly RDH across different data types.

5.2 Scheme performance

5.2.1 Embedding capacity analysis

The embedding capacity of the proposed scheme is determined by the polynomial degree N and the number of CRT channels n_p. According to the embedding construction in Eq. (18), for each ciphertext coefficient c_i, one residue symbol is embedded independently in each CRT channel. Therefore, each coefficient can carry n_p embedding symbols.

Since an NTRU ciphertext polynomial contains N coefficients, the total embedding capacity C (measured in symbols per ciphertext polynomial) is given by

$$C = Nn_\mathrm{p}. \tag{31}$$

As shown in Table 1, the embedding capacity increases linearly with both the polynomial degree N and the number

Unedited

Fig. 3 Experimental results using image data: (a) original carrier image; (b) original secret image; (c) decrypted carrier image; (d) extracted secret image

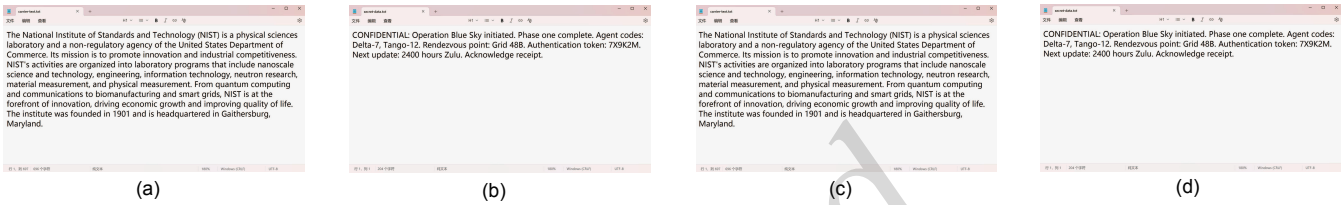

Fig. 4 Experimental results using text data: (a) original carrier text; (b) original secret text; (c) decrypted carrier text; (d) extracted secret text

Unedited

Table 1 Embedding capacity with different parameter configurations

N	n_{p}	d	q	Capacity (bpp)
107	1	5	97	107
		8	151	
		10	191	
		30	547	
107	2	5	229	214
		8	359	
		10	439	
		30	1279	
503	1	55	997	503
		90	1627	
		110	1987	
		160	2887	
503	2	55	2333	1006
		90	3803	
		110	4639	
		160	6761	

of CRT channels n_{p}. For example, when $N = 503$ and $n_{\mathrm{p}} = 1$, the proposed scheme embeds 503 symbols per ciphertext polynomial. When $n_{\mathrm{p}} = 2$, the capacity doubles to 1006 symbols, demonstrating the scalability of the proposed multichannel embedding strategy.

The increase in embedding capacity is accompanied by an increase in the modulus q, as required by the solvability condition in inequality (29), where $P = \prod_{j=1}^{n_{\mathrm{p}}} p_j$. The corresponding choices of q for different parameter settings, reflecting the required modulus expansion, are summarized in Table 1.

This design allows embedding capacity to be flexibly scaled by adjusting n_{p}, while keeping the modulus expansion controlled and compatible with standard NTRU parameter selection.

5.2.2 Security analysis

The proposed scheme is built upon the NTRU cryptosystem, whose security relies on the hardness of lattice problems, such as the SVP and CVP, which are believed to be resistant to both classical and quantum attacks.

The CRT-based redundancy term $\omega(x)$ does not alter the public key, encryption structure, or decryption algorithm of NTRU. By construction, each coefficient satisfies $\omega_i \equiv 0 \pmod{p}$, ensuring automatic elimination during decryption. Therefore, the correctness and security guarantees of standard NTRU decryption are fully preserved.

It is worth noting that $\omega(x)$ is deterministically derived from the embedded payload via CRT. Any statistical characteristics present in $\omega(x)$ directly correspond to the unknown secret data and do not introduce additional exploitable patterns beyond the ciphertext. Consequently, the proposed embedding mechanism does not weaken the ciphertext indistinguishability of NTRU under standard threat models.

5.2.3 Computational complexity

The computational complexity of the proposed scheme is analyzed and compared with the PE and PM algorithms, as summarized in Table 2. Note that X denotes the embedding capacity per polynomial.

Table 2 Comparison of computational complexity

Method	Capacity (bpp)	Computational complexity	
		Embedding	Extraction
CRT	503	$O(NY)$	$O(NY)$
PE	220	$O(NY)$	$O(NY)$
PM	10	$O(2^X Y)$	$O(XY)$

For the proposed scheme, both the embedding and extraction processes exhibit linear time complexity of $O(NY)$, where Y represents the number of carrier units. This linear complexity arises from coefficient-wise modular arithmetic operations without iterative or exponential search procedures.

The experimental results further validate the linear scaling behavior. As illustrated in Fig. 5, the processing time grows approximately linearly with the size of the embedded message. In addition, Fig. 6 demonstrates stable performance across multiple trials, indicating that both embedding and extraction operations exhibit consistent execution time behaviors under identical parameter settings.

Compared with the PE algorithm, the proposed scheme preserves the same linear-time computational complexity while achieving more than twice the embedding capacity. More importantly, unlike the PM algorithm, which incurs exponential embedding complexity of $O(2^X Y)$ due to coefficient-wise modulation and search operations, the proposed method avoids exponential growth entirely. This leads to a favorable balance between computational efficiency and practical embedding capacity.

Overall, the proposed scheme achieves high-capacity RDH with low computational overhead, making it particularly suitable for practical scenarios with constrained computational resources.

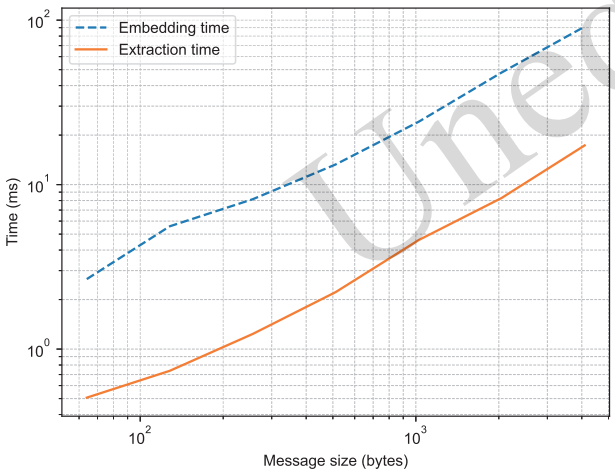

Fig. 5 Processing time trend with respect to message size

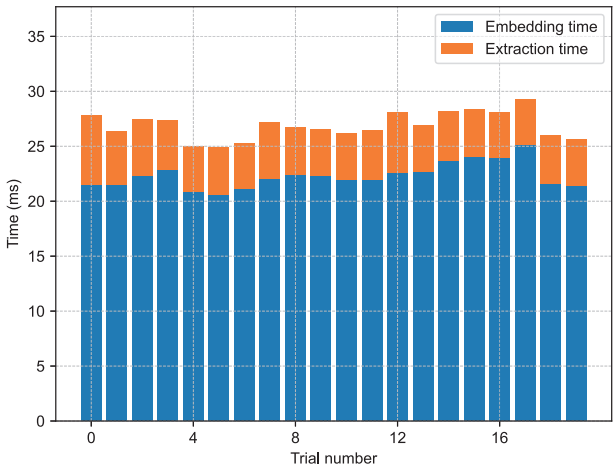

Fig. 6 Performance stability across multiple trials

5.3 Comparison with other homomorphic schemes

Table 3 presents a comprehensive comparison between the proposed CRT-based RDH-ED scheme and representative homomorphic encryption-based approaches, including Paillier-based (Lin et al., 2021; Malik et al., 2022), ElGamal-based (Kong et al., 2024), and NTRU-based schemes (Zhou N et al., 2020; Liu DC et al., 2023; Wu et al., 2024).

From a functional perspective, similar to Paillier 2022 (Malik et al., 2022), ElGamal-based scheme (Kong et al., 2024), and the NTRU-PM scheme (Wu et al., 2024), the proposed method supports direct data extraction in the encrypted domain without requiring ciphertext decryption or any modification to the standard decryption process. In contrast, Paillier 2021 (Lin et al., 2021) and several NTRU-based schemes such as NTRU (Zhou N et al., 2020) and NTRU-PP (Liu DC et al., 2023), rely on customized decryption procedures, which compromise cryptographic transparency and limit compatibility with existing cryptosystems.

From the viewpoint of redundancy utilization, existing NTRU-based RDH-ED methods exploit only limited portions of the available ciphertext redundancy. NTRU-PP scheme (Liu DC et al., 2023) reserves embedding space in the plaintext domain before encryption, which weakens encryption strength and inevitably causes ciphertext length expansion. NTRU-PE approach (Wu et al., 2024) embeds data by exploiting the random perturbation polynomial $r(x)$, making its embedding capacity inherently constrained by the NTRU parameter d_r. The NTRU-PM scheme (Wu et al., 2024) relies on random coefficient modulation to match target patterns; however, this trial-and-error mechanism results in low embedding efficiency and severely limited capacity.

In contrast, the proposed method exploits redundancy from a different perspective. Instead of relying on encryption randomness or plaintext manipulation, it preserves the original ciphertext format and introduces modulus expansion. Specifically, modulus q is required to satisfy the solvability condition after adding structured redundancy to the ciphertext. In practice, modulus q in NTRU-based schemes is typically chosen to be larger than the minimum bound required for correct decryption, primarily for security considerations. This security-driven margin naturally introduces redundant space in the ciphertext domain, which can be directly exploited for reversible data embedding. Consequently, when this existing margin already meets or nearly meets the solvability requirement of the proposed method, the embedded redundancy can be accommodated with little or no additional expansion of q. As a result, the proposed approach does not require any modification to the standard encryption or decryption procedures, and the practical increase of the ciphertext modulus remains limited.

As a direct consequence, the proposed scheme achieves a substantially higher embedding capacity than all compared methods. For instance, when $N = 503$ and $n_p = 1$, the embedding capacity reaches at least 503 bpp, significantly exceeding the capacities of existing Paillier-, ElGamal-, and NTRU-based RDH-ED schemes. This gain arises from the structured exploitation of the ciphertext modulus space enabled by the CRT-based design, rather than ad hoc redundancy manipulation.

Unedited

Table 3 Comparison of different RDH-ED algorithms ($N = 503$ for NTRU schemes)

Algorithm	Does extraction require decryption	Modify decryption process	Ciphertext expansion	Carrier restrictions	Capacity (bpp)
Paillier 2021 (Lin et al., 2021)	No	Yes	Length expansion	None	2
Paillier 2022 (Malik et al., 2022)	No	No	None	None	1
ElGamal (Kong et al., 2024)	No	No	None	None	1.5
NTRU (Zhou N et al., 2020)	No	Yes	None	Some	$\leq$31
NTRU-PP (Liu DC et al., 2023)	No	Yes	Length expansion	None	$\leq$495
NTRU-PE (Wu et al., 2024)	Yes	No	None	None	220
NTRU-PM (Wu et al., 2024)	No	No	None	None	10
Proposed scheme	No	No	Modulus expansion	None	$\geq$503

It should be noted that although the embedding capacity can be theoretically increased by enlarging the number of CRT channels n_{p}, doing so requires a corresponding increase in the modulus q to maintain solvability. Since the size of the ciphertext space grows rapidly with q, excessive modulus expansion leads to diminished efficiency in storage and transmission. Therefore, the proposed scheme is most effective when a moderate number of CRT channels is selected, striking a balance between embedding capacity and practical efficiency.

Overall, the proposed CRT-based RDH-ED scheme provides a favorable balance among embedding capacity, cryptographic compatibility, and operational flexibility, making it a practical and scalable solution for high-capacity RDH in encrypted domains.

6 Conclusions and future work

This study proposes a novel RDH scheme for the NTRU cryptosystem based on the CRT, which addresses the fundamental limitation between reversibility and embedding capacity. With the help of CRT, multichannel redundancy is constructed in the ciphertext domain, enabling multibit embedding per polynomial coefficient without modifying the standard encryption structure. Through rigorous mathematical constraints, the embedded redundancy is automatically eliminated during decryption, ensuring perfect recovery of the original content. Experimental evaluations confirm higher embedding capacity compared to existing NTRU-based RDH techniques, without ciphertext length expansion or security degradation.

Future research will focus on extending the CRT framework to other post-quantum cryptographic systems and enhancing computational efficiency.

Acknowledgments

This work was supported by the Fundamental Research Funds for the Central Universities, University of International Relations (No. 3262026T52), the National Natural Science Foundation of China (No. 62102113), and the Academic Support Programme for Undergraduate Students of University of International Relations (No. 3262025SWA03).

Author contributions

Xinyue ZHANG and Kunyi LAI contributed equally to this work. Xinyue ZHANG took the lead in writing and editing the paper. Kunyi LAI was responsible for the design of the algorithm and experimental validation. Xin TANG, as the corresponding author, participated in reviewing and finalizing the paper. All the authors discussed the results and contributed to the final version.

Conflict of interest

All the authors declare that they have no conflict of interest.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declaration on the use of generative AI tools

During the preparation of this work, the authors used ChatGPT to improve language. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the published article.

References

Hoffstein J, Pipher J, Silverman JH, 1998. NTRU: a ring-based public key cryptosystem. Int Algorithmic Number Theory Symp, p.267-288. https://doi.org/10.1007/BFb0054868

Hoffstein J, Howgrave-Graham N, Pipher J, et al., 2003. NTRUSign: digital signatures using the NTRU lattice. Topics in Cryptology—CT-RSA, p.122-140. https://doi.org/10.1007/3-540-36563-X_9

Ke Y, Zhang MQ, Su TT, 2016. A novel multiple bits reversible data hiding in encrypted domain based on R-LWE. *J Comput Res Dev*, 53(10):2307-2322 (in Chinese). https://doi.org/10.7544/issn1000-1239.2016.20160444

Kong YJ, Zhang MQ, Jiang ZB, et al., 2024. A fine-grained reversible data hiding in encrypted domain based on the cipher-text redundancy of encryption process. *Heliyon*, 10(11):e31542. https://doi.org/10.1016/j.heliyon.2024.e31542

Lin WB, Zhang MQ, Guo S, et al., 2021. Separable reversible data hiding in encrypted domain based on Paillier. *Appl Res Comput*, 38(10):3161-3165 (in Chinese). https://doi.org/10.19734/j.issn.1001-3695.2021.01.0065

Liu DC, Wu HT, Zhuang ZW, et al., 2023. Reversible data hiding scheme in NTRU encrypted domain based on polynomial partition. *Comput Sci*, 50(8):294-303 (in Chinese). https://doi.org/10.11896/jsjkx.220800245

Liu JF, Han T, Tian YG, et al., 2015. Reversible data hiding in encrypted images using recompression. *J Commun*, 36(9):13-25 (in Chinese).

Ma KD, Zhang WM, Zhao XF, et al., 2013. Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Trans Inform Forens Secur*, 8(3):553-562. https://doi.org/10.1109/TIFS.2013.2248725

Malik A, Ashraf A, Wu HZ, et al., 2022. Reversible data hiding in encrypted text using Paillier cryptosystem. Asia-Pacific Signal and Information Processing Association Annual Summit and Conf, p.1495-1499. https://doi.org/10.23919/APSIPAASC55919.2022.9979998

Qi KL, Zhang MQ, Di FQ, et al., 2023. High capacity reversible data hiding in encrypted images based on adaptive quadtree partitioning and MSB prediction. *Front Inform Technol Electron Eng*, 24(8):1156-1168. https://doi.org/10.1631/FITEE.2200501

Unedited

Tang X, Zhou LN, Liu D, et al., 2020. Reversible data hiding based on improved rhombus predictor and prediction error expansion. IEEE 19th Int Conf on Trust, Security and Privacy in Computing and Communications, p.13-21. https://doi.org/10.1109/TrustCom50675.2020.00016

Tang X, Zhou LN, Tang G, et al., 2022a. Improved fluctuation derived block selection strategy in pixel value ordering based reversible data hiding. Proc 20th Int Workshop on Digital Forensics and Watermarking, p.163-177. https://doi.org/10.1007/978-3-030-95398-0_12

Tang X, Zhou YT, Cheng YX, et al., 2022b. Weighted average-based complexity calculation in block selection oriented reversible data hiding. *Secur Commun Netw*, 2022:5225978. https://doi.org/10.1155/2022/5225978

Wang C, Han YL, Duan XW, et al., 2021. NTRU-type proxy re-encryption scheme based on RLWE difficult assumption. *J Cryptol Res*, 8(5):909-920 (in Chinese). https://doi.org/10.13868/j.cnki.jcr.000486

Wu HT, Cheung YM, Tian ZH, et al., 2024. Lossless data hiding in NTRU cryptosystem by polynomial encoding and modulation. *IEEE Trans Inform Forens Secur*, 19:3719-3732. https://doi.org/10.1109/TIFS.2024.3362592

Wu HT, Chen YQ, Cheung YM, et al., 2025. BGN encryption based lossless data hiding by random number replacement and partitioning. *IEEE Trans Depend Secur Comput*, 22(8):8043-8055. https://doi.org/10.1109/TDSC.2025.3603618

Yi S, Zhou YC, 2017. Binary-block embedding for reversible data hiding in encrypted images. *Signal Process*, 133:40-51. https://doi.org/10.1016/j.sigpro.2016.10.017

Zhang MQ, Ke Y, Su TT, 2016. Reversible steganography in encrypted domain based on LWE. *J Electron Inform Technol*, 38(2):354-360 (in Chinese).

Zhang TJ, Li ZC, 2022. Research on image reversible double watermarking algorithm in ciphertext domain based on NTRU. *Softw Eng Appl*, 11(3):504-515 (in Chinese). https://doi.org/10.12677/SEA.2022.113053

Zhang XP, Long J, Wang ZC, et al., 2016. Lossless and reversible data hiding in encrypted images with public-key cryptography. *IEEE Trans Circ Syst Video Technol*, 26(9):1622-1631. https://doi.org/10.1109/TCSVT.2015.2433194

Zhou N, Zhang MQ, Tang HQ, et al., 2020. Reversible data hiding algorithm in encrypted domain based on NTRU. *Sci Technol Eng*, 20(32):13285-13294 (in Chinese). https://doi.org/10.3969/j.issn.1671-1815.2020.32.029

Zhou ZY, Wang CY, Yan KX, et al., 2024. Reversible data hiding in encrypted images based on additive secret sharing and additive joint coding using an intelligent predictor. *Front Inform Technol Electron Eng*, 25(9):1250-1265. https://doi.org/10.1631/FITEE.2300750

Unedited