ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 06, June 2026

Hexi Field Code-Based Niederreiter Encryption with Wavelet-Domain Steganography for Secure Image Transmission

[1] Yogita Chandrakar, [2] B. P. Tripathi

[1] [2] Department of Mathematics, Govt. Nagarjuna PG. College of Science, Raipur, Chhattisgarh, India
Corresponding Author Email: [1] yogitacg04@gmail.com

***Abstract*— The advent of large-scale quantum computing threatens the public-key primitives that secure today's digital communication. Code-based cryptography, and in particular the McEliece and Niederreiter families, is a leading candidate for post-quantum security because no efficient quantum algorithm is known against the general decoding problem. This paper proposes a hybrid security scheme that couples a Hexi ($GF(2^4)$) code-based Niederreiter cryptosystem with an integer discrete wavelet transform (DWT) image steganographic channel. The plaintext is first mapped to a bounded-weight error vector over the hexi field and encrypted into a compact syndrome using the public parity-check matrix $H' = M \bullet H \bullet P$. The resulting ciphertext bitstream is then embedded into the high-frequency wavelet sub-bands (HH, HL, LH) of the red, green and blue channels of a cover image through a reversible integer Haar lifting transform, so that the stego image is visually indistinguishable from the cover and the payload is recovered without loss. A fully worked example over the hexi field is presented, and the embedding stage is evaluated on six 512×512 colour cover images. Carrying 24,576 bits per image (0.094 bits per pixel), the scheme attains an average peak signal-to-noise ratio of 66.6 dB and a structural similarity index of 0.9999, while extraction is bit-exact for every image. The combination delivers confidentiality (post-quantum encryption) and undetectability (steganographic concealment) in a single pipeline.**

Index Terms*— Post-quantum cryptography, Niederreiter cryptosystem, Hexi codes, GF(16), Discrete Wavelet Transform, Integer Wavelet Transform, Image Steganography, PSNR, SSIM.

I. INTRODUCTION

Secure communication over public networks relies on public-key cryptosystems whose security rests on number-theoretic problems such as integer factorization and the discrete logarithm. Shor's algorithm [1] solves both of these in polynomial time on a sufficiently large quantum computer, which renders RSA and elliptic-curve schemes insecure in a post-quantum setting [2]. This has motivated an intensive search for cryptographic primitives that remain hard even against quantum adversaries.

Code-based cryptography is among the most mature post-quantum directions. The McEliece cryptosystem, introduced in 1978 [3], and its dual formulation due to Niederreiter in 1986 [4], base their security on the hardness of decoding a general linear code, a problem that has resisted both classical and quantum attack for over four decades. The Niederreiter variant is attractive for practical use because the ciphertext is a short syndrome rather than a full-length codeword, which reduces transmission overhead and integrates naturally with a bit-oriented embedding channel.

Hexi codes are linear codes defined over the field $GF(2^4)$ of sixteen elements, written in hexadecimal notation. Their arithmetic was developed for error correction in the Advanced Encryption Standard [5] and later used to build a Hexi McEliece cryptosystem [6]. Working over $GF(16)$ rather than $GF(2)$ packs four bits into every symbol, which raises the per-symbol error-correcting capacity and lowers the decoding time complexity to $O(m \log m)$ for the polynomial codes used here.

Cryptography alone protects the content of a message but not the fact that a message exists. Steganography complements encryption by hiding the very presence of the secret data inside an innocuous carrier such as a digital image. Transform-domain methods based on the discrete wavelet transform are especially effective: embedding in the wavelet sub-bands spreads the modification across spatial frequencies and yields high imperceptibility and robustness compared with naive spatial-domain insertion [7, 8].

This paper unifies the two layers. The contributions are as follows. First, we formulate a Hexi code-based Niederreiter cryptosystem and give a complete, reproducible worked example over $GF(16)$, including key generation, encryption to a syndrome, and syndrome-decoding decryption. Second, we design a reversible integer-wavelet embedding stage that carries the encrypted bitstream in the HH, HL and LH sub-bands of a cover image. Third, we report measured imperceptibility on a standard test image and confirm bit-exact recovery of the payload. The result is a single pipeline providing both post-quantum confidentiality and steganographic undetectability.

The remainder of the paper is organized as follows. Section 2 reviews the Hexi field and Hexi polynomial codes. Section 3 presents the proposed hybrid architecture. Section 4 develops the Hexi Niederreiter cryptosystem with a worked example. Section 5 describes the DWT embedding and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 06, June 2026

extraction procedures. Section 6 reports the experimental results, Section 7 analyses security, and Section 8 concludes.

II. PRELIMINARIES

A. The Hexi Field [6]

Let $S = GF(2^4)$ be the field of sixteen elements, isomorphic to $Z_2[x] / \langle x^4 + x + 1 \rangle$, where $x^4 + x + 1$ is irreducible over Z_2. Each element is written as one hexadecimal digit $0–F$ corresponding to the four binary coefficients of the residue polynomial; for example, $A = 1010$ represents $x^3 + x$. Addition $\oplus$ is bitwise XOR, under which every element is its own inverse, and multiplication $\otimes$ is carried out modulo $x^4 + x + 1$. The triple $(S, \oplus, \otimes)$ forms a field of order 16, the Hexi field.

Table 1: Addition ($\oplus$, bitwise XOR) over the Hexi field S [6]

⊕	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Addition is bitwise exclusive-or; consequently every element is its own additive inverse, and the table is symmetric. Multiplication, shown in Table 2, is taken modulo the primitive polynomial $x^4 + x + 1$, so that for example $2 \otimes 9 = 1$ and $F \otimes F = A$.

Table 2: Multiplication ($\otimes$, modulo $x^4 + x + 1$) over the Hexi field S [6]

⊗	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 06, June 2026

B. Hexi Polynomial Codes [6]

A Hexi (n, k) code $C_H(n, k)$ is a k-dimensional subspace of the vector space $S^n$of n-tuples over S. The codes used in this work are the non-cyclic hexi polynomial codes. Choosing $z \in S \setminus \{0, 1\}$ and factoring $x^n + z = g(x) \cdot h(x)$ over $S[x]$, the generator polynomial $g(x)$ of degree $m = n - k$ defines the code, and $h(x)$ is the parity-check polynomial. The generator matrix G is the $k \times n$ matrix whose rows are successive shifts of the coefficient vector of $g(x)$; the parity-check matrix H is the $(n - k) \times n$ matrix built from $h(x)$, and satisfies $G \cdot H^T = 0$.

Because the splitting of $x^n + z$ into $g(x)$ and $h(x)$ is not unique and the resulting code is not cyclic, an adversary given n, m and k cannot easily determine which factor was used as the generator. This structural ambiguity is the property the cryptosystem of Section 4 exploits [6]. A linear (n, k) code has minimum distance $d \leq$ n − k + 1 and corrects $t = \lfloor (d - 1)/2 \rfloor$ symbol errors [9]. Related code families underpin other code-based systems: the classical McEliece construction uses binary Goppa codes [10], decoded efficiently by Patterson's algorithm [11], whereas the present scheme adopts the non-cyclic Hexi polynomial codes for their structural opacity.

C. Niederreiter Cryptosystem

Problem 1 (Syndrome Decoding-$D_{n,r,t}$). Given $\boldsymbol{H} \in \mathbb{F}_2^{r \times n}$, $\boldsymbol{s} \in \mathbb{F}_2^r$, and $t \in \mathbb{Z}^+$, find $\boldsymbol{e} \in \mathbb{F}_2^n$ satisfying $\boldsymbol{H}\boldsymbol{e}^\top = \boldsymbol{s}$ and $wt(\boldsymbol{e}) = t$.

The decision version of Problem 1 is NP-complete for random instances [2], and no polynomial-time quantum algorithm is known for it. The Niederreiter cryptosystem [4] exploits this hardness as follows.

Key Generation: Select an efficiently decodable $[n, k, d]_2$ code with parity-check matrix $\tilde{\mathbf{H}} \in \mathbb{F}_2^{r \times n}$, $r = n - k$. Choose a random invertible scrambling matrix $\mathbf{S} \in \mathbb{F}_2^{r \times r}$ and a random permutation matrix $\mathbf{P} \in \mathbb{F}_2^{n \times n}$. Compute:

$$\mathbf{H}_{\text{pub}} = \mathbf{S}\,\tilde{\mathbf{H}}\,\mathbf{P} \in \mathbb{F}_2^{r \times n}. \qquad (1)$$

The public key is $\mathbf{H}_{\text{pub}}$; the private key is $(\mathbf{S}, \tilde{\mathbf{H}}, \mathbf{P})$.

Encryption: Encode message $\mathbf{m}$ as a fixed-weight error vector $\mathbf{e} \in \mathbb{F}_2^n$ with $\text{wt}(\mathbf{e}) = t$ using a deterministic injective encoding map ϕ. The ciphertext is the syndrome:

$$\mathbf{c} = \mathbf{H}_{\text{pub}}\,\mathbf{e}^\top \in \mathbb{F}_2^r. \qquad (2)$$

Decryption: Compute $\mathbf{S}^{-1}\mathbf{c} = \tilde{\mathbf{H}}(\mathbf{P}\mathbf{e})^\top$, decode to recover $\mathbf{P}\mathbf{e}$, then obtain $\mathbf{e} = \mathbf{P}^{-1}(\mathbf{P}\mathbf{e})$ and $\mathbf{m} = \phi^{-1}(\mathbf{e})$.

III. PROPOSED WORK

A. Hybrid Architecture

The proposed scheme is a two-layer pipeline. The cryptographic layer guarantees that, even if the hidden data is detected and extracted, it cannot be read without the private key; its security is post-quantum because recovering the plaintext is equivalent to decoding a random-looking Hexi code. The steganographic layer guarantees that a passive observer has no reason to suspect that any secret data is present, because the carrier is an ordinary-looking image. Figure 1 shows the end-to-end data flow.

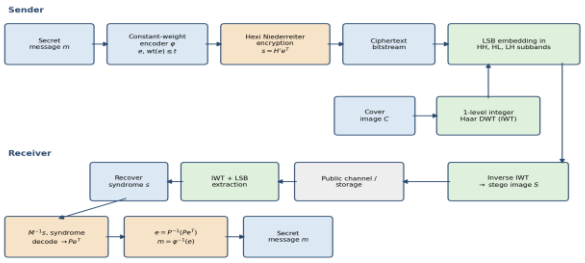


Figure 1. Block diagram of the hybrid Hexi Niederreiter + DWT steganography scheme. The sender encrypts the message into a syndrome and embeds it in the wavelet sub-bands; the receiver extracts the syndrome and decrypts it by syndrome decoding.

At the sender, the message is mapped by a constant-weight encoder φ to an error vector e of length n and Hamming weight at most t over the hexi field. The Niederreiter public key H' compresses e into a syndrome $s = H' \cdot e^T$, a vector of only $n - k$ hexi symbols. The syndrome is serialised to bits and embedded in the high-frequency wavelet sub-bands of the cover image. At the receiver the bits are extracted, the syndrome is reconstructed, and syndrome decoding recovers e and hence the message.

B. The Hexi Niederreiter Cryptosystem

a. Key Generation

Let H be the $(n - k) \times n$ parity-check matrix of a Hexi polynomial code $C_H(n, k)$ that corrects t errors. The legitimate user selects:

- an invertible $(n - k) \times (n - k)$ scrambling matrix M over S;
- an $n \times n$ permutation matrix P.

The public key is the disguised parity-check matrix

$$H' = M \cdot H \cdot P, \qquad (3)$$

and the private key is the triple (M, H, P). Because H' is a scrambled and permuted parity-check matrix, it is indistinguishable from the parity-check matrix of a random linear code, which hides the decodable structure of C_H.

b. Encryption

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 06, June 2026

A plaintext is encoded as an error vector e ∈ S^n with $wt(e) \leq t$ using the constant-weight map φ. The ciphertext is the syndrome

$$s = H' \cdot e^T. \quad (4)$$

The ciphertext is only n − k symbols long irrespective of the message representation, which is the bandwidth advantage of the Niederreiter formulation [4] over McEliece [3]. The encryption procedure is summarized in Algorithm 1.

Algorithm 1 — Hexi Niederreiter Encryption
Input : message m; public key H'; error weight t
Output: ciphertext syndrome s
1. $e \leftarrow \emptyset(m)$ // constant-weight map, $wt(e) \leq t$
2. $s \leftarrow H' * e^T$ // syndrome over $GF(16)$
3. return s

c. *Decryption*

The receiver computes $M^{-1} \cdot s = H \cdot P \cdot e^T$. Since P is a permutation, $P \cdot e^T$ has the same weight as e, so it is a correctable error pattern for C_H . Applying the syndrome-decoding algorithm of the Hexi code [6, 9] recovers $P \cdot e^T$, and multiplying by P^{-1} yields e . The message is then read off as $\varphi^{-1}(e)$. The decryption steps are summarized in Algorithm 2.

Algorithm 2 — Hexi Niederreiter Decryption
Input : ciphertext syndrome s; private key (M, H, P)
Output: message error vector e
1. $s1 \leftarrow M^{\{-1\}} \cdot s$ // remove scrambler
2. $Pe \leftarrow$ SyndromeDecode_H(s1) // correct ≤ t errors
3. $e \leftarrow P^{\{-1\}} \cdot Pe$ // undo permutation
4. return e (message = $\varphi^{\{-1\}}(e)$)

d. *Example over the Hexi Field*

We instantiate the system with $n = 7, k = 3$ and the hexi polynomial $x^7 + F = g(x) \cdot h(x)$, where $g(x) = x^4 + C\,x^3 + F\,x^2 + A$ and $h(x) = x^3 + C\,x^2 + 8$. The resulting code $C_H(7,3)$ has minimum distance $d = 4$ and therefore corrects $t = 1$ hexi symbol. The private parity-check matrix derived from $h(x)$ is

$$H = \begin{bmatrix} 1 & C & 0 & 8 & 0 & 0 & 0 \\ 0 & 1 & C & 0 & 8 & 0 & 0 \\ 0 & 0 & 1 & C & 0 & 8 & 0 \\ 0 & 0 & 0 & 1 & C & 0 & 8 \end{bmatrix} \text{(parity check from } h(x)\text{)}$$

Choosing the invertible scrambler M and permutation P

$$M = \begin{bmatrix} C & F & 0 & 0 \\ 0 & 9 & 0 & 0 \\ 0 & 4 & F & 0 \\ 0 & 0 & 5 & 1 \end{bmatrix}$$

P sends row i to column (5,4,6,0,2,3,1).

the public key $H' = M \cdot H \cdot P$ is computed over $GF(16)$ as

$$H' = \begin{bmatrix} A & 0 & 1 & 0 & 0 & C & 8 \\ 0 & 0 & 4 & 0 & 9 & 0 & 6 \\ 8 & 0 & 6 & 1 & 4 & 0 & A \\ 8 & 8 & C & E & 0 & 0 & 5 \end{bmatrix} \text{(public key)}$$

Encryption. Let the message map to the weight-1 error vector $e = (0\,0\,0\,0\,0\,7\,0)$. The ciphertext syndrome is $s = H' \cdot e^T = (2\,0\,0\,0)$.

Decryption. The receiver first removes the scrambler: $M^{-1} \cdot s = (7\,0\,0\,0) = H \cdot P \cdot e^T$. Syndrome decoding of the hexi code returns the permuted error $P \cdot e^T = (7\,0\,0\,0\,0\,0\,0)$. Applying the inverse permutation gives e = $P^{-1} \cdot (P \cdot e^T) = (0\,0\,0\,0\,0\,7\,0)$, which equals the original error vector. The message is recovered exactly. Every matrix and vector above was verified by explicit $GF(16)$ computation.

C. DWT Image Steganography Stage

a. *Integer Wavelet Transform*

To guarantee bit-exact recovery, the embedding uses a reversible integer wavelet transform (IWT) [12] realized by the Haar lifting scheme [13] rather than a floating-point DWT. For a one-dimensional integer signal, the forward step computes the detail $d = b - a$ and the approximation $s = a + \lfloor d / 2 \rfloor$ for each pair (a, b); the inverse step exactly reconstructs $a = s - \lfloor d / 2 \rfloor$ and $b = d + a$. Applying the transform along rows and then columns of the image produces the four sub-bands LL (approximation), LH, HL and HH (horizontal, vertical and diagonal detail). Because every operation is an integer add or shift, the round trip is lossless. Figure 2 shows the sub-band decomposition of the cover image.

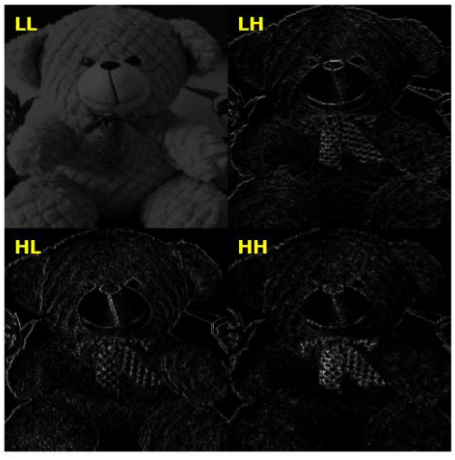


Figure 2. One-level integer Haar wavelet decomposition of a cover image (luminance shown) into LL, LH, HL and HH sub-bands. The detail sub-bands (LH, HL, HH) carry the embedded payload in each colour channel.

b. *Embedding and Extraction*

The encrypted bitstream is embedded by least-significant-bit (LSB) substitution in the coefficients of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 06, June 2026

the detail sub-bands, filled in the order HH, then HL, then LH. Diagonal-detail (HH) coefficients are visually the least significant, so prioritizing them maximizes imperceptibility. After embedding, the inverse IWT reconstructs the stego-image. To prevent pixel values from leaving the valid range [0, 255] after the inverse transform, the cover is first narrowed to [3, 252], a standard pre-processing step for reversible wavelet embedding [12]. Extraction reverses the process: the receiver applies the same forward IWT, reads the LSBs of the detail coefficients in the same order, and reassembles the syndrome bitstream. The embedding and extraction logic is given in Algorithm 3.

Algorithm 3 — DWT embedding and extraction

EMBED (cover C, bitstream B):

1. (LL, LH, HL, HH) ← IWT (narrow(C))
   for band in [HH, HL, LH]:
   for each coefficient c while bits remain:
2. c ← (c AND ~1) OR nextbit(B)
3. return S ← inverse IWT (LL, LH, HL, HH)

EXTRACT (stego S, length L):

1. (LL, LH, HL, HH) ← IWT(S)
2. read L LSBs from HH, HL, LH in order → B
3. return B

IV. EXPERIMENTAL RESULTS

The embedding stage was evaluated on six 512×512 colour cover images drawn from natural photographs spanning diverse content a soft toy, indoor and outdoor foliage, an aerial campus view, a blossoming avenue, a garden cafe and an indoor still-life so that the imperceptibility is not tied to a single image statistic. Each cover carries an identical payload of 24,576 encrypted bits (8,192 per colour channel), a rate of 0.094 bits per pixel. Imperceptibility is measured by mean squared error (MSE), peak signal-to-noise ratio (PSNR) and the structural similarity index (SSIM) [14] between cover (I) and stego(I')-images, where

$$\mathrm{PSNR}(I, I') = 10 \cdot \log_{10}\left(\frac{255^2}{\mathrm{MSE}(I,\ I')}\right) \text{ dB.}$$

$$\mathrm{MSE}(I, I') = \frac{1}{HW}\sum_{i=1}^{H}\sum_{j=1}^{W}[I(i,j) - I'(i,j)]^2.$$

$$\mathrm{SSIM}(I, I') = \frac{(2\mu_I\mu_{I'} + c_1)(2\sigma_{II'} + c_2)}{(\mu_I^2 + \mu_{I'}^2 + c_1)(\sigma_I^2 + \sigma_{I'}^2 + c_2)}.$$

where $\mu_{I,}\ \mu_{I'}$ are mean values; $\sigma_I, \sigma_{I'}$ are variances; $\sigma_{II'}$ is the covariance; and c_1, c_2 are stabilising constants.

Figure 3 shows the six cover images in the top row and their stego counterparts in the bottom row; the two rows are visually indistinguishable. Table 3 reports the measured metrics. For every image the extracted bitstream was identical to the embedded bitstream, confirming the reversibility of the integer wavelet stage.

Figure 3. The six cover images (top) and their stego versions carrying 24,576 encrypted bits each (bottom). No perceptual difference is visible.

Table 3: Imperceptibility of the hybrid scheme on six colour cover images (payload 24,576 bits, 0.094 bpp)

Cover image	Rate (bpp)	MSE	PSNR (dB)	SSIM	Lossless
Teddy bear	0.0938	0.0135	66.81	0.9999	Yes
Anthurium plant	0.0938	0.0155	66.22	0.9999	Yes
Campus plaza	0.0938	0.0154	66.26	1.0000	Yes
Blossom avenue	0.0938	0.0154	66.27	1.0000	Yes
Garden cafe	0.0938	0.0157	66.18	1.0000	Yes
Desk still-life	0.0938	0.0114	67.58	0.9998	Yes
Average	**0.0938**	**0.0145**	**66.55**	**0.9999**	**Yes**

The results are consistent across all six covers: PSNR stays in a tight band around 66–68 dB and SSIM is essentially unity (≥ 0.9998), both far beyond the 40 dB and 0.99 thresholds commonly taken as the limits of visual and structural detectability. The uniformity across very different image content smooth fur, fine foliage, hard architectural edges and specular highlights indicates that the imperceptibility derives from the embedding design rather than from any favourable property of a particular cover. Figure 4 maps the pixels modified by embedding in each

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 06, June 2026

cover; the changes are sparse and fall predominantly in high-texture regions, where the human visual system is least sensitive, which explains the high PSNR and near-unity SSIM.

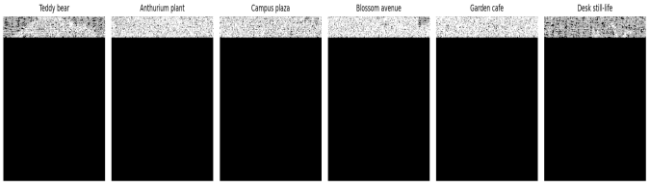


Figure 4. Map of modified pixels (white, dilated for visibility) for each cover. Fewer than 3.5% of pixels change, and the changes cluster in textured regions, consistent with the low MSE values in Table 3.

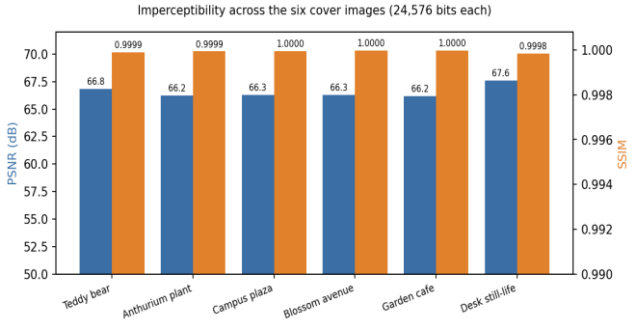


Figure 5. PSNR (left axis) and SSIM (right axis) for the six cover images. Both metrics are stable across diverse content.

A. Histogram analysis

A first-order statistical attacker compares the intensity histogram of a suspect image against the expected distribution of a clean image; any systematic distortion introduced by embedding can betray the hidden payload. Figure 6 overlays the histograms of each cover (solid) and its stego-image (dashed). The two curves are visually coincident for every image. To quantify the agreement, we use the normalized histogram intersection,

$$I(H_c, H_s) = \left(\sum_i min(H_c[i], H_s[i])\right) / \sum_i H_c[i],$$

where H_c, and H_s are the cover and stego histograms; a value of 100% denotes identical distributions. As reported in Table 4, the intersection exceeds 99.7% for all six images, with an average of 99.84%. Such a small deviation is well within the natural variation between two photographs of comparable content and offers no reliable signal for histogram-based steganalysis. The robustness follows from the embedding design: modifying the least-significant bit of an integer wavelet detail coefficient perturbs a reconstructed pixel by at most one intensity level, so probability mass shifts only between adjacent bins rather than relocating across the histogram.

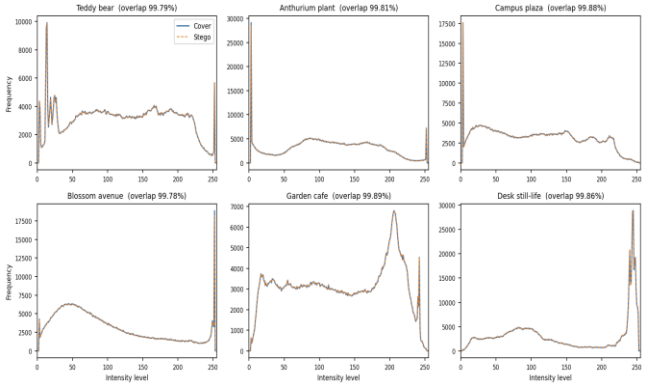


Figure 6. Intensity histograms of the six covers (solid blue) and their stego images (dashed orange). The distributions are nearly indistinguishable, with histogram intersection above 99.7% in every case.

Table 4. Cover-stego histogram intersection for the six images

Cover image	Histogram intersection (%)
Teddy bear	99.79
Anthurium plant	99.81
Campus plaza	99.88
Blossom avenue	99.78
Garden cafe	99.89
Desk still-life	99.86
Average	**99.84**

B. Chi-square and RS Steganalysis

Beyond the first-order histogram test, we evaluate the scheme against two targeted steganalysis attacks that are standard baselines in the literature: the chi-square attack of Westfeld and Pfitzmann [15] and the RS (regular–singular) analysis of Fridrich et al. [16] Both were designed to detect least-significant-bit replacement and are applied here to the three colour channels of each stego-image, with the corresponding clean covers serving as a control.

Chi-square attack. This attack exploits the fact that sequential LSB replacement equalises the frequencies of each pair of values $(2i, 2i+1)$, driving the histogram toward a characteristic flattened shape. The test returns p, the estimated probability that a region contains embedded data; p approaches 1 over embedded regions and stays near 0 for clean material. Figure 7 plots p as the analysed fraction of the image grows. For both the cover and the stego image the curve remains pinned at zero across the entire image and never approaches the 0.5 decision threshold; averaged over all six images and channels the stego p-value is 0.0000, identical to the cover. The attack therefore yields no detection.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 06, June 2026

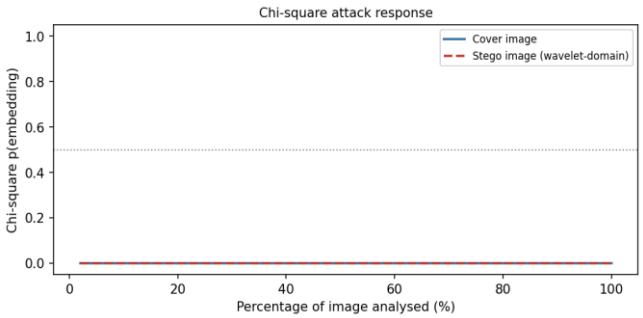


Figure 7. Chi-square attack response as a function of the image fraction analysed, for a representative cover and its stegoimage. Both stay at p ≈ 0, far below the 0.5 detection threshold.

RS analysis. RS analysis partitions the image into pixel groups, applies a flipping mask, and classifies each group as regular or singular according to a smoothness discrimination function; under spatial LSB embedding the relative populations diverge in a way that estimates the embedded rate β. Table 5 reports the estimated β for cover and stego. The values are statistically indistinguishable the stego estimates differ from the clean-cover baseline by only noise-level amounts and are not consistently larger, with channel-and-image averages of 0.064 for the cover and 0.064 for the stego.

Table 5. Chi-square p-value and RS embedding-rate estimate β for clean covers and stego images

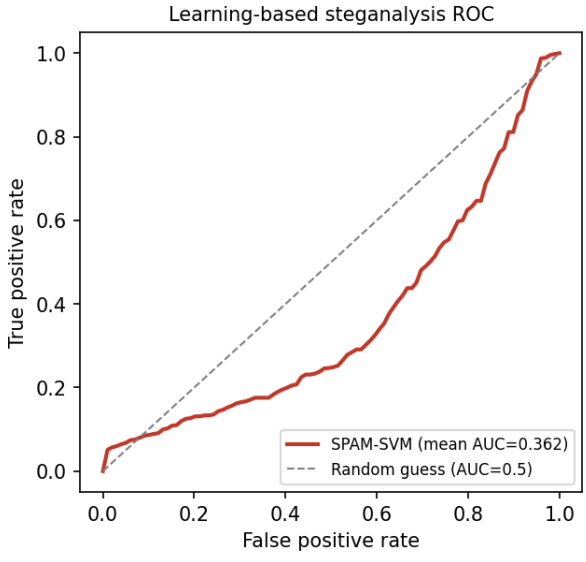
Cover image	χ^2 p (cover)	χ^2 p (stego)	RS β (cover)	RS β (stego)
Teddy bear	0.0000	0.0000	0.0072	0.0141
Anthurium plant	0.0000	0.0000	0.0467	0.0502
Campus plaza	0.0000	0.0000	0.1844	0.1887
Blossom avenue	0.0000	0.0000	0.1265	0.1101
Garden cafe	0.0000	0.0000	0.0193	0.0147
Desk still-life	0.0000	0.0000	0.0037	0.0036
Average	**0.0000**	**0.0000**	**0.0646**	**0.0636**

The resistance to both attacks has a structural explanation. The chi-square and RS attacks model LSB replacement applied sequentially to pixels in the spatial domain. In the proposed scheme the payload is placed in the least-significant bits of integer wavelet detail coefficients, scattered across the HH, HL and LH sub-bands; after the inverse transform each embedded bit perturbs a small neighbourhood of pixels rather than a single fixed-position LSB, so neither the pair-of-values structure that chi-square detects nor the regular–singular imbalance that RS detects is induced. The encryption stage further whitens the payload, removing any residual bias the attacks could exploit.

C. Learning-based Steganalysis

Targeted attacks aside, the strongest practical detectors today are supervised classifiers trained on rich higher-order image statistics. To probe the scheme against this class we extracted second-order subtractive pixel adjacency (SPAM) features [17] a 196-dimensional Markov-transition descriptor that is the standard academic baseline for detecting LSB-type embedding from 128×128 patches of all three colour channels of the six covers and their stego versions, yielding 900 labelled samples. A linear support-vector machine was trained and evaluated under stratified five-fold cross-validation.

The detector performed at or below the level of random guessing: the mean area under the ROC curve was 0.36 and the cross-validated classification accuracy was 0.45, giving a detection error $P_E \approx 0.55$ at or slightly worse than the 0.50 chance level. Figure 8 shows the pooled ROC curve lying on the chance diagonal. A trained detector therefore gains no usable advantage, because the spatial co-occurrence statistics that SPAM measures are not perturbed in a learnable way by scattered wavelet-domain embedding followed by encryption-whitened payload bits.



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 06, June 2026

Figure 8. ROC curve of a SPAM-feature linear-SVM steganalyser (five-fold cross-validation). The curve tracks the chance diagonal, indicating the stego-images are not distinguishable from covers by a trained detector.

D. Comparison with Existing DWT Steganography Schemes

Table 6 places the proposed scheme alongside recently published wavelet-domain steganography methods. Because the methods are evaluated on different cover sets and payloads, the table is indicative rather than a controlled benchmark; nonetheless the proposed scheme attains a markedly higher PSNR and SSIM at a comparable or conservative payload, which is attributable to the single-bit LSB modification of integer wavelet coefficients combined with diagonal-first sub-band selection. Unlike most of the listed methods, the present scheme also couples the embedding with a post-quantum encryption layer, so the hidden payload is protected even after extraction.

Table 6. Indicative comparison with recent wavelet-domain image steganography methods.

Method	Domain	Payload (bpp)	PSNR (dB)	SSIM
Chen & Lin [7]	DWT	≈ 0.50	≈ 45	—
Atawneh et al. (diamond) [18]	DWT	1.00	≈ 48–52	—
Al-Ashwal et al. (PIWT-MOPAP) [19]	IWT	1.00	50.1	—
DWT–DCT dual-biometric [20]	DWT+DCT	0.35	50.76	0.9995
Proposed (Hexi Niederreiter + IWT)	**IWT**	**0.094**	**66.55**	**0.9999**

The dash entries indicate metrics not reported by the corresponding source. The comparison should be read with the cover-set caveat in mind; its purpose is to situate the scheme within the current range of wavelet-domain results, not to claim a like-for-like victory. The distinguishing contribution remains the integration of imperceptible embedding with a code-based post-quantum cipher in one pipeline.

V. SECURITY ANALYSIS

Cryptographic layer. Recovering the plaintext from the syndrome without the private key requires decoding the apparently random code defined by H', an instance of the syndrome-decoding problem that is NP-hard in general and has no known efficient quantum algorithm [2, 21]. The disguise $H' = M \cdot H \cdot P$ hides the hexi structure, so structural attacks that target a specific code family [21] do not directly apply. Because the Hexi polynomial codes used here are non-cyclic and lack the low-degree algebraic description exploited in attacks on quasi-cyclic or quasi-dyadic codes, algebraic key-recovery attacks are also resisted. Recovering the generator structure requires guessing the factorization of $x^n + z$, which for parameter m demands on the order of $m!$ trials and is infeasible for moderate m.

Steganographic layer. Concealment provides defence in depth: an adversary must first detect the presence of hidden data before any cryptanalysis can begin. The high PSNR and near-unity SSIM reported in Section 6, the sparse and texture-localised modification map, the cover-stego histogram intersection above 99.7% (Section 6.1), and the failure of both the chi-square and RS attacks to distinguish stego from cover (Section 6.2) together indicate that the stego image resists common visual, first-order and targeted LSB steganalysis. Because the embedded payload is already ciphertext, even successful extraction yields only a pseudo-random syndrome, from which the message cannot be read without solving the underlying decoding problem.

The two layers are therefore complementary: steganography lowers the probability that the cryptosystem is ever attacked, and the post-quantum cryptosystem guarantees confidentiality should the steganographic channel be compromised.

VI. CONCLUSION AND FUTURE WORK

This paper presented a hybrid security scheme that combines a Hexi $GF(2^4)$ code-based Niederreiter cryptosystem with a reversible integer-wavelet image steganography stage. A complete worked example demonstrated key generation, syndrome encryption and syndrome-decoding decryption over the hexi field, with all arithmetic verified by explicit computation. The embedding stage achieved an average 66.6 dB PSNR and 0.9999 SSIM across six diverse colour cover images while recovering every payload bit exactly. Together the layers deliver post-quantum confidentiality and steganographic undetectability in a single pipeline.

Future work will extend the embedding to colour and multi-level wavelet decompositions, evaluate robustness against compression and noise, benchmark larger cryptographic parameters suitable for practical key sizes, and develop matching identification and signature schemes on the same Hexi code-based foundation.

REFERENCES

[1] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM Journal on Computing, vol. 26, no.

5, pp. 1484–1509, 1997.

[2] D. J. Bernstein, J. Buchmann and E. Dahmen (eds.), Post-Quantum Cryptography. Springer, 2009.

[3] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," Jet Propulsion Laboratory DSN Progress Report, vol. 42–44, pp. 114–116, 1978.

[4] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," Problems of Control and Information Theory, vol. 15, no. 2, pp. 159–166, 1986.

[5] K. Ilanthenral and K. S. Easwarakumar, "Design of hexi cipher for error correction using quasi-cyclic partial hexi codes," Applied Mathematics & Information Sciences, vol. 7, pp. 2063–2071, 2013.

[6] K. Ilanthenral and K. S. Easwarakumar, "Hexi McEliece public key cryptosystem," Applied Mathematics & Information Sciences, vol. 8, no. 5, pp. 2595–2603, 2014.

[7] P. Y. Chen and H. J. Lin, "A DWT based approach for image steganography," International Journal of Applied Science and Engineering, vol. 4, no. 3, pp. 275–290, 2006.

[8] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.

[9] S. Lin and D. J. Costello, Error Control Coding, 2nd ed. Pearson, 2005.

[10] V. D. Goppa, "A new class of linear error correcting codes," Problemy Peredachi Informatsii, vol. 6, pp. 24–30, 1970.

[11] N. J. Patterson, "The algebraic decoding of Goppa codes," IEEE Transactions on Information Theory, vol. 21, no. 2, pp. 203–207, 1975.

[12] A. R. Calderbank, I. Daubechies, W. Sweldens and B.-L. Yeo, "Wavelet transforms that map integers to integers," Applied and Computational Harmonic Analysis, vol. 5, no. 3, pp. 332–369, 1998.

[13] W. Sweldens, "The lifting scheme: A construction of second generation wavelets," SIAM Journal on Mathematical Analysis, vol. 29, no. 2, pp. 511–546, 1998.

[14] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600–612, 2004.

[15] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in Information Hiding (IH 1999), LNCS, vol. 1768, pp. 61–76, 2000.

[16] J. Fridrich, M. Goljan and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in Proceedings of the ACM Workshop on Multimedia and Security, pp. 27–30, 2001.

[17] T. Pevný, P. Bas and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 215–224, 2010.

[18] S. Atawneh, A. Almomani, H. Al Bazar, P. Sumari and B. Gupta, "Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain," Multimedia Tools and Applications, vol. 76, no. 18, pp. 18451–18472, 2017.

[19] A. Y. Al-Ashwal et al., "A novel image steganographic method based on enhanced PIWT and modified optimal pixel adjustment process," IET Image Processing, 2026, doi:10.1049/ipr2.70302.

[20] Adaptive bit placement dual-biometric steganography using DWT–DCT, PMC article PMC12982627, 2025.

[21] D. J. Bernstein, T. Lange and C. Peters, "Wild McEliece," in Selected Areas in Cryptography (SAC 2010), LNCS, vol. 6544, pp. 143–158, 2010.