International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 10 – Issue 08 || August 2025 || PP. 60-64

Gröbner Bases and Polynomial Ideals Used in Zero-Watermarking for Image Authentication

Anwar Khaleel Faraj[1], Areej M. Abduldaim[2], Rasha Jalal Mitlif[3], Mohammed Qasim Hamid[4]

[1, 2, 3] *Department of Mathematics and Computer Applications, College of Applied Sciences, University of Technology, Baghdad, Iraq*
[4]*Computer Department, College of Education, Al-Mustansiriyah University Baghdad,Iraq*
Areej.M.Abduldaim@uotechnology.edu.iq
rasha.j.mitlif@uotechnology.edu.iq
alamerymohamad@uomustansiriyah.edu.iq

Abstract: This paper introduces an image authentication method based on advanced algebraic structures to provide strong security and robustness. The approach maps significant DCT coefficients of image blocks into the polynomial ring $\mathbb{Z}_{256}[x]/(x^n-1)$, where features are extracted using optimization theory and Gröbner bases. These features are combined through ring symmetries and the Chinese Remainder Theorem to generate a robust binary watermark. A verification process computes the ring-theoretic distance between original and extracted watermarks, while additional enhancements such as key-dependent ring isomorphisms and non-commutative rings strengthen security. The system is well-suited for sensitive applications like medical imaging, legal evidence, and copyright protection.

1. Introduction

The digital revolution has made images a primary means of storing information, communicating, and providing evidence in vital areas such as medical diagnosis, legal proceedings, and journalism. However, this widespread availability raises significant challenges in ensuring their authenticity, integrity, and ownership. Sometimes, these can have serious consequences, such as security compromises due to unauthorized distribution or malicious modification. Digital watermarking has emerged as a pivotal technology to address these concerns by embedding a secret signal—a watermark—directly into the host's data.

Traditional watermarking techniques face a fundamental paradox: embedding a robust watermark inherently alters the original content. Such modifications are unacceptable in scenarios requiring absolute fidelity, even if changes are imperceptible, such as legal evidence or raw medical images like MRI scans and X-rays. To address this issue, non-alteration watermarking was introduced. Instead of embedding information directly, it extracts intrinsic, robust features from the image to generate a unique watermark, which is then registered with a trusted third party. This method preserves the original content entirely while still enabling authentication and copyright protection.

Most current approaches depend on statistical features, transform-domain coefficients (like DCT, DWT, and SVD), or geometric invariants. Although these methods can be effective to some extent, they often lack a strong theoretical basis, leaving them vulnerable to advanced attacks and limiting their broader applicability. The core challenge lies in developing a feature extraction mechanism that is both highly sensitive to tampering and free of any embedded watermark, while remaining robust against benign, content-preserving operations such as compression, blurring, and filtering.

Many studies use singular value decomposition (SVD) to strengthen watermarking algorithms. In [1], combining SVD with the Arnold transform provides strong robustness against diverse attacks. The authors in [2, 3] applied the Gravitational Search Algorithm (GSA) and the Shuffled Frog Leaping (SFL) Algorithm in combination with GSVD and SVD. However, SVD suffers from high computational complexity, requiring $O(n^3)$ operations for a matrix of order n, particularly when repeated computations are involved. Discret Wavelet Transform DWT is used in image watermarking to separate high- and low-frequency components. In [4], the Haar wavelet with LSB embedding secures a logo image within the original image. Chebyshev polynomials, combined with the Diffie–Hellman homogeneous method, are used in [5] to embed a watermark logo into various samples of the audio file's DCT transform.

This paper proposes a novel zero-watermarking scheme grounded in the rigorous mathematical framework of *abstract algebra*, specifically *ring theory* and **ideal theory.** By mapping image features into polynomial rings over finite fields and exploiting the algebraic properties of ideals and Gröbner bases, we develop a feature extraction and watermark construction process that is theoretically sound, highly secure, and

exceptionally robust. Our method transforms the image authentication problem into an algebraic problem, leveraging operations like ring homomorphisms and the Chinese Remainder Theorem to generate a unique, non-invertible watermark.

2. Related Work

The field of digital watermarking is vast, but can be broadly categorized into traditional and zero-watermarking techniques.

Traditional Watermarking methods embed information by modifying pixel values or transform-domain coefficients. Spatial domain techniques, such as the Least Significant Bit (LSB) substitution [6], are simple but fragile. Frequency-domain methods, leveraging transforms like the Discrete Cosine Transform (DCT) [7] and Discrete Wavelet Transform (DWT) [8], offer greater robustness against compression and noise by embedding watermarks in the perceptually significant coefficients. While these methods have been widely studied and deployed, their inherent modification of the host signal remains a critical drawback for high-fidelity applications.

Zero-Watermarking was conceived to eliminate this drawback. The foundational principle is to generate a watermark from the image's features rather than embedding one. Early and common approaches utilize robust feature sets for this construction. For instance, many schemes [9, 10] extract features from transform domains. A prevalent technique involves using the relationship between significant coefficients in the DCT domain or singular values from a Singular Value Decomposition (SVD) [11] to form a binary sequence. Other methods exploit geometric invariants [12] or image moments that are resistant to affine transformations.

While these feature-based methods have demonstrated success, they often operate on heuristic principles. Their robustness is empirically verified rather than mathematically guaranteed, potentially leaving them exposed to adversarial attacks designed to specifically target the chosen statistical features. Furthermore, the process of binarizing continuous features to form a watermark can sometimes lead to a loss of discriminative information.

Our work distinguishes itself by moving beyond heuristic feature extraction. We draw inspiration from the application of algebraic structures in cryptography and coding theory. The use of polynomial rings and ideals, particularly in the context of Gröbner bases, has been explored for cryptography (e.g., in the design of multivariate cryptosystems) and for error correction [13]. However, its application to digital watermarking, and specifically zero-watermarking, remains largely unexplored.

Recent pioneering work has begun to bridge this gap. For example, [14] proposed a watermarking scheme based on commutative ring ideals. Our approach significantly extends this line of inquiry by constructing a more complex algebraic structure: the quotient ring $\mathbb{Z}_{256}[x]/(x^n-1)$, which is intimately related to cyclic codes. AGr¨obner basis for ideal I is a set of non-zero polynomials $G = \{a_1, \ldots, a_t\} \subseteq I$if for all ƒ ∈ 𝕀 such that f is not zero 0, then$lp(a_i)$ divides $lp(ƒ)$ for some$i \in \{1, \ldots, t\}$.The systematic extraction of a Gröbner basis for the ideal generated by the image's feature polynomial provides a canonical and robust representation of the image block. The S-Polynomial of $\hbar$and$\ell$is the polynomial S($\hbar$, ℓ) = L /lt($\hbar$) ·$\hbar$− L lt(ℓ) ·ℓ such that L = lcm(lp($\hbar$), lp(ℓ)) and $\hbar$, $\ell$are non zeropolynomails in k[x_1, ..., x_n]. This algebraic foundation allows us to formally define security enhancements through ring automorphisms and isomorphisms, and to rigorously analyze the algorithm's complexity and robustness, offering a theoretically superior alternative to existing empirical methods.

This algorithm presents a novel zero-watermarking approach for image authentication using algebraic ring structures. Unlike traditional watermarking, zero-watermarking doesn't modify the host image but constructs a watermark from the image's intrinsic features.

3. Mathematical Preliminaries

We utilize the following ring-theoretic concepts:

1. **Ring of Integers Modulo n (Z_n):** For pixel value manipulations
2. **Polynomial Rings:** For feature representation
3. **Ideal Decomposition:** For feature extraction
4. **Ring Homomorphisms:** For mapping operations

Algorithm Components

1. Preprocessing Phase

Input: Original image I of size M×N

Steps:

1. Convert image to grayscale if necessary ($I \rightarrow I_g$)
2. Divide image into k×k blocks (typical k=8)
3. For each block B:

- Apply 2D Discrete Cosine Transform (DCT)
- Select significant coefficients C = $\{c_1, c_2, ..., c_m\}$

2. Ring Construction

For each block's coefficients:

1. Define the base ring $\mathbb{Z}_{256}$ (for 8-bit images)
2. Construct polynomial ring $R[x]/(x^n - 1)$ where *n* is the number of significant coefficients
3. Create feature polynomial for block B_{ij} :
   $P_{ij}(x) = \Sigma\ (c_k mod p)\ x^{k-1}$, with p is prime less than 256.

3. Ideal-Based Feature Extraction

1. For each$P_{ij}\ (x)$, compute its principal ideal:
   $I_{ij}(x) = \left(P_{ij}(x)\right)\{r(x)P_{ij}(x): r(x) \in R[x]/(x^n - 1)\}$.
2. Compute the reduced Gröbner basis $G_{ij}\ (x)$ for each ideal I_{ij}
3. Extract feature vector F_{ij} from G_{ij} :
   - Leading coefficients
   - Degrees of basis polynomials
   - Number of basis elements

4. Watermark Generation

1. Construct master feature matrix:
   $F=[F_{11},F_{12},\ldots,F_{1n},F_{21},\ldots,F_{2n},\ldots,F_{m1},\ldots,F_{mn}]$
2. Apply ring homomorphism φ:R→S where S is a specially constructed quotient ring
3. Compute the kernel of φ to extract invariant features
4. Apply Chinese Remainder Theorem to combine features from different rings
5. Generate binary watermark W by thresholding the invariant features

5. Verification Process

Input: Suspected image I', original watermark W

Steps:

1. Repeat preprocessing and feature extraction on I'
2. Generate candidate watermark W'
3. Compute similarity measure using ring-theoretic distance: $d(W, W') = \Sigma\varphi^{-1}(W_i \oplus W_{i'}) \bmod p$, where φ^{-1} is the inverse homomorphism
4. Accept as authentic if $d(W, W') < threshold\ \tau$

Complete Algorithm Pseudocode

```
function ZeroWatermarkEmbedding(I):
    // Input: Image I
    // Output: Watermark W
    // Step 1: Preprocessing
I_gray = RGB2Gray(I) if needed
    blocks = PartitionImage(I_gray, k=8)
DCT_blocks = ApplyDCT(blocks)
    // Step 2: Ring Construction
    R = IntegerModRing(256)
    S = PolynomialRing(R, 'x').quotient(x^n - 1)
feature_matrix = []
    for each block B in DCT_blocks:
        C = SelectSignificantCoefficients(B)
        P = ConstructPolynomial(C, S)
        I = Ideal(P)
        G = GroebnerBasis(I)
        F = ExtractFeatures(G)
feature_matrix.append(F)
    // Step 3: Watermark Generation
    F = Matrix(feature_matrix)
    φ = ConstructHomomorphism(R, S)
```

```
    invariants = Kernel(φ)
    W = ApplyCRT(invariants)
    return Binary(W)
function VerifyWatermark(I', W_original):
W_candidate = ZeroWatermarkEmbedding(I')
    d = RingTheoreticDistance(W_original, W_candidate)
    return d < threshold
```

Security Enhancements

1. **Secret Key Incorporation:**
   - Use key-dependent ring isomorphisms
   - Apply random automorphisms to the polynomial rings
2. **Non-commutative Rings:**
   - Employ matrix rings for additional security
   - Use quaternion algebras for robust feature representation
3. **Dynamic Parameter Selection:**
   - Choose modulus p based on image characteristics
   - Adapt polynomial degree n per image block

Robustness Considerations

1. **Error-Correcting Codes:**
   - Encode watermark using ring-based codes
   - Utilize ideals as error-correcting structures
2. **Multiple Ring Representations:**
   - Create watermarks in different rings (Z_p,$Z_p[x]$, etc.)
   - Combine results for increased robustness
3. **Feature Selection:**
   - Prioritize mid-frequency DCT coefficients
   - Use ring invariants resistant to common attacks

Complexity Analysis

The algorithm's complexity is dominated by:

1. O(MN)for image preprocessing
2. O(k^2log$k$)per block for DCT (k is block size)
3. O(n^3)per block for Gröbner basis computation
4. O(m^2) for matrix operations (m is feature dimension)

Overall complexity is approximately O($MN + N$- blocks×(k^2log$k$+n^3)+m^2)

Applications

1. Image authentication in sensitive domains (medical, legal)
2. Copyright protection without image modification
3. Tamper detection in surveillance systems
4. Multimedia forensics

This algorithm provides a theoretically sound approach to zero-watermarking by leveraging the rich structure of rings in abstract algebra, offering both security and robustness while preserving the original image data.

References

[1]. Heng Zhang, Chengyou Wang, and Xiao Zhou, A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain, Future Internet 2017, 9, 45; doi:10.3390/fi9030045.

[2]. A. M .Abduldaim, A. K. Faraj, Combining Algebraic GSVD and Gravitational Search Algorithm for Optimizing Secret Image Watermark Sharing Technique, International Journal of Mathematics and Computer Science, 17, (2022), 2, 753-774.

[3]. Waleed, J., Abduldaim, A.M., Alyas, H.H., Mohammed, A.Q., An Optimized Zero-Watermarking Technique Based on SFL Algorithm 2nd International Conference on Electrical, Communication, Computer, Power and Control Engineering, ICECCPCE 2019, 2019, pp. 171–175, 9072723.

[4]. Hussain, R.A., Abdulmunem, M.E., Abdul-Hossen, A.M.J., Propose Image Encryption Watermarking Algorithm Based on Frequency and Geometric Transform, SCCS 2019 - 2019 2nd Scientific Conference of Computer Sciences, 2019, pp. 143–147, 8852591.
[5]. H . B. Abdul Wahab, A. J. Abdul-Hossen, S. A. Kadhom, Encrypted Image Watermark in Audio Files Using Homogenous Deffie-Hellman with Chebyshev Polynomial, Eng. & Tech. Journal, 34, (2016).
[6]. W. Bender, et al., "Techniques for data hiding," *IBM Systems Journal*, 1996.
[7]. I. J. Cox, et al., "Secure spread spectrum watermarking for multimedia," *IEEE TIP*, 1997.
[8]. D. Kundur, D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," *IEEE ICASSP*, 1998.
[9]. Q. Wen, et al., "A zero-watermarking scheme based on DWT and chaotic modulation," *Proc. CISW*, 2004.
[10]. Y. Liu, et al., "A zero-watermarking algorithm for medical images based on SVD and chaotic encryption," *IEEE Access*, 2020.
[11]. R. Liu, T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE TMM*, 2002.
[12]. C.-S. Lu, et al., "Geometric distortion-resilient image watermarking using invariant moments," *IEEE IP*, 2002.
[13]. D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer, 2007.
[14]. X. Li, et al., "A Novel Watermarking Scheme Based on Ring Theory and Ideal Decomposition," *Proc. ICASSP*, 2021.