mathematics

MDPI

*Article*

# Simultaneous Decompositions of Two Sets of Five Quaternion Tensors and Applications in Color Videos Processing

**Zhuo-Heng He [1,2], Yu-Fei Jiang [1], Mei-Ling Deng [3] and Shao-Wen Yu [4,*]**

[1] Sino-European School of Technology, Shanghai University, Shanghai 200444, China; zhuohenghe@shu.edu.cn (Z.-H.H.); yfjiang@shu.edu.cn (Y.-F.J.)
[2] Department of Mathematics and Newtouch Center for Mathematics, Shanghai University, Shanghai 200444, China
[3] Department of Mathematics and Statistics, University of Nevada, Reno, NV 89557, USA; meilingd@unr.edu
[4] School of Mathematics, East China University of Science and Technology, Shanghai 200237, China
* Correspondence: yushaowen@ecust.edu.cn

**Abstract**

This paper extends the theory of equivalence canonical forms from quaternion matrices to quaternion tensors under the Einstein product. Motivated by recent results on the simultaneous decomposition of two specific configurations of five quaternion matrices, we establish a comprehensive framework for the corresponding configurations of five quaternion tensors. The core approach leverages bijective transformation maps that establish isomorphisms between quaternion tensor spaces and matrix spaces, allowing us to systematically construct invertible transformation tensors that simultaneously reduce the given tensor quintuples to canonical forms consisting solely of binary entries (0 and 1). A detailed structural analysis of the resulting canonical tensor forms is provided, including explicit dimension formulas for all identity blocks derived from precise rank conditions. To demonstrate practical utility, we integrate the proposed tensor decomposition with the discrete wavelet transform to construct a color video encryption and decryption system. Experimental results confirm perfect reconstruction (PSNR exceeding 300 dB, SSIM equal to 1) and strong security performance: NPCR of 49.8%, UACI of 49.6%, information entropy of 0.9986 bits per pixel, adjacent pixel correlation below 0.03 in absolute value, and a key space exceeding $2^{512}$. The developed theory significantly extends the existing literature on quaternion tensor decompositions and provides powerful tools for multidimensional signal processing.

**Keywords:** tensor decomposition; quaternion algebra; Einstein product; simultaneous decomposition; color video encryption; tensor quintuples

**MSC:** 15A69; 15B33

Check for updates

Academic Editor: Elena Guardo

Received: 8 April 2026
Revised: 26 April 2026
Accepted: 27 April 2026
Published: 5 May 2026

**Copyright:** © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

## 1. Introduction

Tensors, as multidimensional arrays, have become fundamental mathematical objects for representing and analyzing complex, high-dimensional data across a wide range of scientific disciplines. The rich theory of tensor decompositions has found broad applications in diverse fields, including data mining, genomic signal processing, advanced signal processing, and computer vision. Various tensor decomposition frameworks—such as Tucker decomposition, higher-order singular value decomposition (HOSVD), and several

other innovative approaches—have been extensively studied and successfully applied to real-world problems [1–4].

Quaternion algebra, introduced by Hamilton in 1843, constitutes an associative yet noncommutative division algebra over the real number field. The mathematical foundation of quaternion algebra is well-established in the literature, with its noncommutative nature presenting both challenges and opportunities for theoretical developments [5–7]. In recent years, quaternion algebra has garnered significant attention due to its powerful applications in various domains including signal processing, control theory, computer science, and quantum mechanics. Particularly in the domain of color image processing, the quaternion model provides an elegant and natural representation where the RGB components of each pixel naturally correspond to the three imaginary parts of a quaternion number [8–11].

A quaternion tensor, defined as a tensor with quaternion entries, represents a significant generalization that can encapsulate more complex structural information compared to real-valued tensors, thereby offering enhanced potential for applications in various domains. For instance, quaternion-based higher-order singular value decomposition has been successfully applied to color image processing tasks [9,12]. In a related development, the eigenvalues of quaternion tensors under the Einstein product have been investigated and applied to color video compression, demonstrating the practical utility of quaternion tensor methods [13–15].

Recent years have witnessed a surge of interest in quaternion tensor decompositions. Huo et al. [16] established a simultaneous decomposition for quaternion tensor quaternities under Einstein product, demonstrating applications in color video encryption. He et al. [14] investigated the diagonalization of two quaternion tensors via t-product and applied it to simultaneous encryption of two color videos. Yang et al. [15] developed randomized quaternion tensor UTV decompositions for efficient color image and video processing. Miao et al. [12] explored quaternion tensor left ring decomposition for color image inpainting. Furthermore, Imhogiemhe et al. [17] studied low-rank tensor decompositions for quaternion multiway arrays, while Flamant et al. [18,19] developed quaternion nonnegative matrix factorization and constrained convex quaternion optimization frameworks.

However, despite these advances, the theory of simultaneous decomposition for multiple tensors over quaternion algebra remains relatively underdeveloped compared with its real-valued counterpart. This theoretical gap is particularly notable, as numerous important results over the real numbers cannot be directly extended to the quaternion setting due to its inherent noncommutativity [5,6]. Recent work has begun to address this gap by establishing simultaneous decompositions for two sets of quaternion tensor triplets under the Einstein product, with applications in color video processing [13]. Nevertheless, the more intricate case of simultaneous decomposition for quintuples of quaternion tensors has remained an open challenge to date.

The present work is directly motivated by a recent seminal contribution that established equivalence canonical forms for two specific configurations of five quaternion matrices [20]. Their work addressed the matrix configurations:

$$(1)\quad \begin{pmatrix} A & 0 & 0 \\ B & C & D \\ 0 & 0 & E \end{pmatrix}, \qquad (2)\quad \begin{pmatrix} A & 0 \\ B & C \\ 0 & D \\ 0 & E \end{pmatrix}.$$

and provided complete characterizations of their equivalence canonical forms under simultaneous equivalence transformations.

In this paper, we undertake a systematic generalization of these matrix-level results to the tensor domain. Our main contribution is the development of a comprehensive theory

for the simultaneous decomposition of two corresponding configurations of quaternion tensor quintuples under the Einstein product. Specifically, we extend the matrix configurations (1) and (2) to their tensor analogs and establish their canonical forms through the construction of appropriate invertible transformation tensors. The mathematical approach leverages transformation maps that establish isomorphisms between quaternion tensors and quaternion matrices, thereby allowing us to bridge the matrix and tensor theories in a rigorous manner [21,22].

Beyond the theoretical developments, we demonstrate the practical utility of our tensor decomposition framework by integrating it with the discrete wavelet transform to construct a novel system for color video encryption and decryption. This integrated approach achieves the dual objectives of simultaneous encryption and compression while providing enhanced security features, thereby addressing important practical challenges in multimedia security [23–25]. In this context, "color video processing" is interpreted in a broad sense throughout this paper, referring to the complete pipeline that integrally combines wavelet-based video analysis, tensor-based structural transformations, and encryption. The framework immediately delivers concrete processing functionalities—including multiresolution decomposition and structured data reorganization—beyond the encryption application itself, and does not depend on future compression extensions to be effective.

The remainder of this paper is organized as follows. In Section 2, we present essential mathematical preliminaries including notations, fundamental results about quaternion algebra, tensor theory, and Einstein product. In Section 3, we provide a comprehensive review of the matrix-level simultaneous decomposition results that serve as the foundation for our tensor generalizations. Section 4 presents our main theoretical contributions: the simultaneous decomposition theories for two configurations of quaternion tensor quintuples, including detailed constructions of the canonical forms and thorough structural analyses. In Section 5, we demonstrate the application of our theoretical framework to color video encryption and decryption, presenting both the methodological framework and experimental validation. Finally, Section 6 concludes the paper with a summary of contributions and directions for future research.

## 2. Preliminaries

### *2.1. Quaternion Algebra and Basic Notations*

**Definition 1** (Quaternion Algebra [5,6]). *The quaternion algebra $\mathbb{H}$ is defined as:*

$$\mathbb{H} = \{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \mid \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1,\ a_0, a_1, a_2, a_3 \in \mathbb{R}\}.$$

*Quaternion algebra is associative but noncommutative, with the multiplication rules:*

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

**Definition 2** (Quaternion Tensor [1,13]). *A tensor $\mathcal{A} = (a_{i_1,\ldots,i_N})_{1\le i_j\le I_j}$ (for $j = 1,\ldots,N$) is a multi-dimensional array with $I_1 I_2 \cdots I_N$ entries, where $N$ is called the order of $\mathcal{A}$. We denote $\mathbb{H}^{I_1\times\cdots\times I_N}$ as the set of all the $N$-order quaternion tensors of dimensions $I_1 \times \cdots \times I_N$.*

**Definition 3** (Diagonal and Unit Tensors [26,27]). *A tensor $\mathcal{D} = (d_{i_1,\ldots,i_N,j_1,\ldots,j_N}) \in \mathbb{H}^{I_1\times\cdots\times I_N\times I_1\times\cdots\times I_N}$ is called a diagonal tensor if all of its entries are zero except for $d_{i_1,\ldots,i_N,i_1,\ldots,i_N}$. If all the $d_{i_1,\ldots,i_N,i_1,\ldots,i_N} = 1$, then $\mathcal{D}$ is called a unit tensor and denoted by $\mathcal{I}$.*

### 2.2. Einstein Product and Transformation Maps

**Definition 4** (Einstein Product [26,28]). *For two tensors with compatible sizes* $\mathcal{A} = (a_{i_1,\ldots,i_N,j_1,\ldots,j_N}) \in \mathbb{H}^{I_1\times\cdots\times I_N\times J_1\times\cdots\times J_N}$ *and* $\mathcal{B} = (b_{j_1,\ldots,j_N,k_1,\ldots,k_M}) \in \mathbb{H}^{J_1\times\cdots\times J_N\times K_1\times\cdots\times K_M}$, *the Einstein product of* $\mathcal{A}$ *and* $\mathcal{B}$ *is defined by the operation* $*_N$ *via*

$$(\mathcal{A} *_N \mathcal{B})_{i_1,\ldots,i_N,k_1,\ldots,k_M} = \sum_{j_1,\ldots,j_N} a_{i_1,\ldots,i_N,j_1,\ldots,j_N} b_{j_1,\ldots,j_N,k_1,\ldots,k_M}.$$

*Thus,* $(\mathcal{A} *_N \mathcal{B}) \in \mathbb{H}^{I_1\times\cdots\times I_N\times K_1\times\cdots\times K_M}$.

**Definition 5** (Transformation Map [26,27]). *Define the transformation*

$$f_{I_1,\ldots,I_N,J_1,\ldots,J_N} : \mathcal{A} \in \mathbb{H}^{I_1\times\cdots\times I_N\times J_1\times\cdots\times J_N} \to A \in \mathbb{H}^{I_1\cdot I_2\cdots I_{N-1}\cdot I_N\times J_1\cdot J_2\cdots J_{N-1}\cdot J_N}$$

*with* $f_{I_1,\ldots,I_N,J_1,\ldots,J_N}(\mathcal{A}) = A$ *defined entry-wise as*

$$(\mathcal{A})_{i_1,\ldots,i_N,j_1,\ldots,j_N} \xrightarrow{f_{I_1,\ldots,I_N,J_1,\ldots,J_N}} (A)_{\left[i_1+\sum_{k=2}^{N}(i_k-1)\prod_{s=1}^{k-1} I_s\right],\left[j_1+\sum_{k=2}^{N}(j_k-1)\prod_{s=1}^{k-1} J_s\right]}.$$

**Lemma 1** (Transformation Properties). *The transformation map* $f$ *defined in Definition 5 satisfies:*

1. *For any* $\mathcal{A} \in \mathbb{H}^{I_1\times\cdots\times I_N\times J_1\times\cdots\times J_N}$, *the map* $f_{I_1,\ldots,I_N,J_1,\ldots,J_N}$ *is bijective with well-defined inverse* $f^{-1}$.
2. *For* $\mathcal{A} \in \mathbb{H}^{I_1\times\cdots\times I_N\times J_1\times\cdots\times J_N}$ *and* $\mathcal{B} \in \mathbb{H}^{J_1\times\cdots\times J_N\times K_1\times\cdots\times K_N}$:

$$f(\mathcal{A} *_N \mathcal{B}) = f(\mathcal{A}) \cdot f(\mathcal{B}),$$

   *where* $\cdot$ *denotes standard matrix multiplication.*
3. $f(\mathcal{I}) = I$, *where* $\mathcal{I}$ *is the unit tensor and* $I$ *is the identity matrix.*
4. $f(\mathcal{A}^{-1}) = f(\mathcal{A})^{-1}$ *for any invertible tensor* $\mathcal{A}$.

**Proof.** (1) The bijectivity of $f$ follows from the fact that the index mapping $(i_1,\ldots,i_N,j_1,\ldots,j_N) \mapsto (i,j)$ with

$$i = i_1 + \sum_{k=2}^{N}(i_k-1)\prod_{s=1}^{k-1} I_s, \quad j = j_1 + \sum_{k=2}^{N}(j_k-1)\prod_{s=1}^{k-1} J_s$$

is a bijection between the multi-index and linear index sets (cf. Lemma 6). Hence $f$ is invertible with $f^{-1}$ mapping the linear indices back to the original tensor indices.

(2) For $\mathcal{A} \in \mathbb{H}^{I_1\times\cdots\times I_N\times J_1\times\cdots\times J_N}$ and $\mathcal{B} \in \mathbb{H}^{J_1\times\cdots\times J_N\times K_1\times\cdots\times K_N}$, let $A = f(\mathcal{A})$, $B = f(\mathcal{B})$. The $(i,k)$-th entry of $A \cdot B$ is

$$(A\cdot B)_{ik} = \sum_{j=1}^{J} A_{ij}B_{jk},$$

where $J = J_1\cdots J_N$. Under the inverse index mapping, each linear index $j$ corresponds uniquely to a multi-index $(j_1,\ldots,j_N)$. Therefore,

$$(A\cdot B)_{ik} = \sum_{j_1,\ldots,j_N} a_{i_1,\ldots,i_N,j_1,\ldots,j_N}\, b_{j_1,\ldots,j_N,k_1,\ldots,k_N},$$

which is precisely the $(i_1,\ldots,i_N,k_1,\ldots,k_N)$-th entry of $\mathcal{A} *_N \mathcal{B}$ mapped by $f$. Thus $f(\mathcal{A} *_N \mathcal{B}) = f(\mathcal{A})\cdot f(\mathcal{B})$.

(3) By Definition 3, the unit tensor $\mathcal{I}$ has entries 1 on the diagonal positions $(i_1,\ldots,i_N, i_1,\ldots,i_N)$ and 0 elsewhere. Under $f$, these diagonal positions map exactly to the diagonal entries of an identity matrix, so $f(\mathcal{I}) = I$.

(4) If $\mathcal{A}$ is invertible with inverse $\mathcal{A}^{-1}$, then $\mathcal{A} *_N \mathcal{A}^{-1} = \mathcal{I}$. Applying $f$ to both sides and using property (2) gives $f(\mathcal{A}) \cdot f(\mathcal{A}^{-1}) = I$, so $f(\mathcal{A}^{-1}) = f(\mathcal{A})^{-1}$. □

**Lemma 2** (Inverse Transformation Property). *For matrices* $A \in \mathbb{H}^{I_1 \cdot I_2 \cdots I_{N-1} \cdot I_N \times I_1 \cdot I_2 \cdots I_{N-1} \cdot I_N}$ *and* $B \in \mathbb{H}^{I_1 \cdot I_2 \cdots I_{N-1} \cdot I_N \times K_1 \cdot K_2 \cdots K_{N-1} \cdot K_N}$*:*

$$f^{-1}_{I_1,\ldots,I_N,K_1,\ldots,K_N}(A \cdot B) = f^{-1}_{I_1,\ldots,I_N,I_1,\ldots,I_N}(A) *_N f^{-1}_{I_1,\ldots,I_N,K_1,\ldots,K_N}(B).$$

**Proof.** Let $\mathcal{X} = f^{-1}_{I_1,\ldots,I_N,I_1,\ldots,I_N}(A)$ and $\mathcal{Y} = f^{-1}_{I_1,\ldots,I_N,K_1,\ldots,K_N}(B)$. Applying $f$ to $\mathcal{X} *_N \mathcal{Y}$ and using Lemma 1(2), we obtain

$$f(\mathcal{X} *_N \mathcal{Y}) = f(\mathcal{X}) \cdot f(\mathcal{Y}) = A \cdot B.$$

Since $f$ is bijective (Lemma 1(1)), it follows that

$$f^{-1}_{I_1,\ldots,I_N,K_1,\ldots,K_N}(A \cdot B) = \mathcal{X} *_N \mathcal{Y} = f^{-1}_{I_1,\ldots,I_N,I_1,\ldots,I_N}(A) *_N f^{-1}_{I_1,\ldots,I_N,K_1,\ldots,K_N}(B),$$

which completes the proof. □

**Definition 6** (Tensor Invertibility [13,26]). *A tensor* $\mathcal{A} \in \mathbb{H}^{I_1 \times \cdots \times I_N \times I_1 \times \cdots \times I_N}$ *is invertible if there exists* $\mathcal{X} \in \mathbb{H}^{I_1 \times \cdots \times I_N \times I_1 \times \cdots \times I_N}$ *satisfying:*

$$\mathcal{A} *_N \mathcal{X} = \mathcal{X} *_N \mathcal{A} = \mathcal{I}.$$

*In this case,* $\mathcal{X}$ *is the inverse of* $\mathcal{A}$*, denoted* $\mathcal{A}^{-1}$*.*

**Lemma 3** (Invertibility Criterion). *A tensor* $\mathcal{A} \in \mathbb{H}^{I_1 \times \cdots \times I_N \times I_1 \times \cdots \times I_N}$ *is invertible if and only if* $f(\mathcal{A})$ *is an invertible matrix. Then:*

$$\mathcal{A}^{-1} = f^{-1}(f(\mathcal{A})^{-1}).$$

**Proof.** ($\Rightarrow$) If $\mathcal{A}$ is invertible, there exists $\mathcal{A}^{-1}$ such that $\mathcal{A} *_N \mathcal{A}^{-1} = \mathcal{I}$. Applying $f$ to both sides and using Lemma 1(2)–(3) yields $f(\mathcal{A}) \cdot f(\mathcal{A}^{-1}) = I$, so $f(\mathcal{A})$ is an invertible matrix with $f(\mathcal{A})^{-1} = f(\mathcal{A}^{-1})$.

($\Leftarrow$) If $f(\mathcal{A})$ is an invertible matrix, let $X = f(\mathcal{A})^{-1}$ and set $\mathcal{X} = f^{-1}(X)$. Then by Lemma 1(2),

$$f(\mathcal{A} *_N \mathcal{X}) = f(\mathcal{A}) \cdot X = I = f(\mathcal{I}).$$

Since $f$ is injective, $\mathcal{A} *_N \mathcal{X} = \mathcal{I}$. Similarly, $\mathcal{X} *_N \mathcal{A} = \mathcal{I}$. Hence $\mathcal{A}$ is invertible and $\mathcal{A}^{-1} = \mathcal{X} = f^{-1}(f(\mathcal{A})^{-1})$. □

### *2.3. Problem Formulation: Simultaneous Decomposition of Quaternion Tensor Quintuples*

In this paper, we focus on establishing simultaneous decompositions for two distinct configurations of quaternion tensor quintuples under the Einstein product. These configurations are natural tensor generalizations of the matrix counterparts studied in recent literature [20,29]:

**Configuration 1:** Consider five tensors arranged as a block tensor structure:

$$\begin{pmatrix} \mathcal{A} & 0 & 0 \\ \mathcal{B} & \mathcal{C} & \mathcal{D} \\ 0 & 0 & \mathcal{E} \end{pmatrix},$$

where the tensors have compatible sizes for Einstein product multiplication.

**Configuration 2:** Consider five tensors arranged as a block tensor structure:

$$\begin{pmatrix} \mathcal{A} & 0 \\ \mathcal{B} & \mathcal{C} \\ 0 & \mathcal{D} \\ 0 & \mathcal{E} \end{pmatrix},$$

where the tensors have compatible sizes for Einstein product multiplication.

Our objective is to construct invertible transformation tensors that simultaneously transform each quintuple into a canonical form containing only 0 and 1 entries, while preserving the structural relationships among the tensors [30–33].

The key mathematical challenge arises from the noncommutativity of quaternion algebra, which prevents direct extension of real-valued tensor decomposition results. Our approach leverages the transformation maps $f$ and $f^{-1}$ to bridge the tensor and matrix theories, thereby enabling us to establish comprehensive decomposition results for quaternion tensor quintuples [11,34,35].

## 3. Review of Matrix-Level Simultaneous Decomposition Results

This section provides a comprehensive review of the matrix-level simultaneous decomposition results which serve as the foundational basis for our tensor-level generalizations [20,29].

**Lemma 4** (Equivalence Canonical Form for Matrix Array (1) [20])**.** *Given five matrices with compatible sizes arranged as:*

$$\begin{pmatrix} A & 0 & 0 \\ B & C & D \\ 0 & 0 & E \end{pmatrix},$$

*where* $A \in \mathbb{H}^{q\times m}$, $B \in \mathbb{H}^{r\times m}$, $C \in \mathbb{H}^{r\times n}$, $D \in \mathbb{H}^{r\times p}$, *and* $E \in \mathbb{H}^{s\times p}$, *there exist invertible matrices* $P_1 \in \mathrm{GL}_q(\mathbb{H})$, $P_2 \in \mathrm{GL}_r(\mathbb{H})$, $P_3 \in \mathrm{GL}_s(\mathbb{H})$, $Q_1 \in \mathrm{GL}_m(\mathbb{H})$, $Q_2 \in \mathrm{GL}_n(\mathbb{H})$, *and* $Q_3 \in \mathrm{GL}_p(\mathbb{H})$ *such that:*

$$\begin{aligned} P_1AQ_1 &= S_a, \\ P_2BQ_1 &= S_b, \\ P_2CQ_2 &= S_c, \\ P_2DQ_3 &= S_d, \\ P_3EQ_3 &= S_e, \end{aligned}$$

*where* $S_a, S_b, S_c, S_d, S_e$ *are canonical matrices with entries only 0 and 1 [20].*

**Lemma 5** (Equivalence Canonical Form for Matrix Array (2) [20])**.** *Given five matrices with compatible sizes arranged as:*

$$\begin{pmatrix} A & 0 \\ B & C \\ 0 & D \\ 0 & E \end{pmatrix},$$

*where* $A \in \mathbb{H}^{p\times m}$, $B \in \mathbb{H}^{q\times m}$, $C \in \mathbb{H}^{q\times n}$, $D \in \mathbb{H}^{s\times n}$, *and* $E \in \mathbb{H}^{t\times n}$, *there exist invertible matrices* $P_1 \in \mathrm{GL}_p(\mathbb{H})$, $P_2 \in \mathrm{GL}_q(\mathbb{H})$, $P_3 \in \mathrm{GL}_s(\mathbb{H})$, $P_4 \in \mathrm{GL}_t(\mathbb{H})$, $Q_1 \in \mathrm{GL}_m(\mathbb{H})$, *and* $Q_2 \in \mathrm{GL}_n(\mathbb{H})$ *such that:*

$$\begin{aligned} P_1AQ_1 &= T_a, \\ P_2BQ_1 &= T_b, \\ P_2CQ_2 &= T_c, \\ P_3DQ_2 &= T_d, \\ P_4EQ_2 &= T_e, \end{aligned}$$

*where* $T_a, T_b, T_c, T_d, T_e$ *are canonical matrices with entries only 0 and 1 [20].*

**Canonical form structure for Configuration (1).** The canonical matrices $S_a, S_b, S_c, S_d, S_e$ in Lemma 4 retain the same $3 \times 3$ block partition as the original array, i.e.,

$$\begin{pmatrix} S_a & 0 & 0 \\ S_b & S_c & S_d \\ 0 & 0 & S_e \end{pmatrix},$$

where $S_a, S_b, S_c, S_d, S_e$ are non-zero blocks composed by identity matrices and zero matrices. The dimension of every identity matrix is determined by the ranks of $A, B, C, D, E$ together with certain joint rank conditions (see [20] for the complete table of dimensions). Each row and column partition contains at most one non-zero block, so that the entire collection $\{S_a, S_b, S_c, S_d, S_e\}$ consists solely of entries 0 and 1.

**Canonical form structure for Configuration (2).** Analogously, the canonical matrices $T_a, T_b, T_c, T_d, T_e$ in Lemma 5 satisfy

$$\begin{pmatrix} T_a & 0 \\ T_b & T_c \\ 0 & T_d \\ 0 & T_e \end{pmatrix},$$

with the identical property: non-zero blocks composed by identity matrices and zero matrices. The dimension of every identity matrix is determined by the ranks of $A, B, C, D, E$ together with certain joint rank conditions.

## 4. Simultaneous Decomposition of Quaternion Tensor Quintuples

### *4.1. Transformation Map Properties and Rigorous Proofs*

Throughout this paper, for any positive integer $n$, we denote $\langle n\rangle = \{1, 2, \ldots, n\}$. This notation will be used extensively in index mappings and set definitions.

**Lemma 6** (Index Mapping Bijectivity [21,27])**.** *The index mapping* $h_{I_1,\ldots,I_N,J_1,\ldots,J_N}$ *defined by:*

$$h_{I_1,\ldots,I_N,J_1,\ldots,J_N}(i,j) = (i_1,\ldots,i_N,j_1,\ldots,j_N)$$

*with the recursive formulas specified in Definition 5, establishes a bijection between* $\langle I_1 \cdot I_2 \cdots I_N\rangle \times \langle J_1 \cdot J_2 \cdots J_N\rangle$ *and* $\langle I_1\rangle \times \cdots \times \langle I_N\rangle \times \langle J_1\rangle \times \cdots \times \langle J_N\rangle$.

**Proof.** The mapping corresponds to the mixed radix representation of integers, obtained by successive Euclidean divisions. For each integer $i \in \langle I_1 I_2 \cdots I_N\rangle$, we have the unique expansion

$$i - 1 = \alpha_1 + \alpha_2 I_1 + \alpha_3 I_1 I_2 + \cdots + \alpha_N I_1 I_2 \cdots I_{N-1},$$

where $0 \le \alpha_t \le I_t - 1$ for $t = 1, \ldots, N$. Setting $i_t = \alpha_t + 1$ yields $1 \le i_t \le I_t$ and

$$i = i_1 + \sum_{k=2}^{N} (i_k - 1) \prod_{s=1}^{k-1} I_s.$$

Similarly, for each $j \in \langle J_1 J_2 \cdots J_N \rangle$, there exists a unique expansion

$$j - 1 = \beta_1 + \beta_2 J_1 + \beta_3 J_1 J_2 + \cdots + \beta_N J_1 J_2 \cdots J_{N-1},$$

with $0 \le \beta_t \le J_t - 1$. Setting $j_t = \beta_t + 1$ gives $1 \le j_t \le J_t$ and

$$j = j_1 + \sum_{k=2}^{N} (j_k - 1) \prod_{s=1}^{k-1} J_s.$$

Conversely, given any $(i_1, \ldots, i_N) \in \langle I_1 \rangle \times \cdots \times \langle I_N \rangle$ and $(j_1, \ldots, j_N) \in \langle J_1 \rangle \times \cdots \times \langle J_N \rangle$, the above formulas uniquely determine $i$ and $j$. Therefore, the mapping $h_{I_1,\ldots,I_N,J_1,\ldots,J_N}$ is bijective. This mixed radix representation is equivalent to the Chinese Remainder Theorem applied to the product of cyclic groups [21,27]. □

### *4.2. Tensor Generalization: First Configuration*

**Theorem 1** (Simultaneous Decomposition for Tensor Configuration (1) [20,29])**.** *Consider five tensors with compatible sizes under Einstein product arranged as:*

$$\begin{pmatrix} \mathcal{A} & 0 & 0 \\ \mathcal{B} & \mathcal{C} & \mathcal{D} \\ 0 & 0 & \mathcal{E} \end{pmatrix},$$

*where* $\mathcal{A} \in \mathbb{H}^{I_1 \times \cdots \times I_N \times K_1 \times \cdots \times K_N}$, $\mathcal{B} \in \mathbb{H}^{J_1 \times \cdots \times J_N \times K_1 \times \cdots \times K_N}$, $\mathcal{C} \in \mathbb{H}^{J_1 \times \cdots \times J_N \times L_1 \times \cdots \times L_N}$, $\mathcal{D} \in \mathbb{H}^{J_1 \times \cdots \times J_N \times M_1 \times \cdots \times M_N}$, *and* $\mathcal{E} \in \mathbb{H}^{P_1 \times \cdots \times P_N \times M_1 \times \cdots \times M_N}$.

*There exist invertible tensors:*

$$\begin{aligned} &\mathcal{P}_1 \in \mathbb{H}^{I_1 \times \cdots \times I_N \times I_1 \times \cdots \times I_N}, \\ &\mathcal{P}_2 \in \mathbb{H}^{J_1 \times \cdots \times J_N \times J_1 \times \cdots \times J_N}, \\ &\mathcal{P}_3 \in \mathbb{H}^{P_1 \times \cdots \times P_N \times P_1 \times \cdots \times P_N}, \\ &\mathcal{Q}_1 \in \mathbb{H}^{K_1 \times \cdots \times K_N \times K_1 \times \cdots \times K_N}, \\ &\mathcal{Q}_2 \in \mathbb{H}^{L_1 \times \cdots \times L_N \times L_1 \times \cdots \times L_N}, \\ &\mathcal{Q}_3 \in \mathbb{H}^{M_1 \times \cdots \times M_N \times M_1 \times \cdots \times M_N}, \end{aligned}$$

*such that:*

$$\begin{aligned} &\mathcal{P}_1 *_N \mathcal{A} *_N \mathcal{Q}_1 = \mathcal{S}_A, \quad \mathcal{P}_2 *_N \mathcal{B} *_N \mathcal{Q}_1 = \mathcal{S}_B, \\ &\mathcal{P}_2 *_N \mathcal{C} *_N \mathcal{Q}_2 = \mathcal{S}_C, \quad \mathcal{P}_2 *_N \mathcal{D} *_N \mathcal{Q}_3 = \mathcal{S}_D, \quad \mathcal{P}_3 *_N \mathcal{E} *_N \mathcal{Q}_3 = \mathcal{S}_E, \end{aligned} \tag{1}$$

*where* $\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_C, \mathcal{S}_D, \mathcal{S}_E$ *are canonical tensors containing only 0 and 1 entries.*

**Proof.** The proof proceeds through the following systematic steps:

**Step 1: Matrix Representation via Transformation Map** Apply the transformation map $f$ to convert the tensor quintuple into a matrix quintuple with dimensions exactly matching those in Lemma 4. Define

$$q = I_1 I_2 \cdots I_N, \quad m = K_1 K_2 \cdots K_N, \quad r = J_1 J_2 \cdots J_N,$$
$$n = L_1 L_2 \cdots L_N, \quad p = M_1 M_2 \cdots M_N, \quad s = P_1 P_2 \cdots P_N.$$

Then

$$A = f(\mathcal{A}) \in \mathbb{H}^{q \times m},$$
$$B = f(\mathcal{B}) \in \mathbb{H}^{r \times m},$$
$$C = f(\mathcal{C}) \in \mathbb{H}^{r \times n},$$
$$D = f(\mathcal{D}) \in \mathbb{H}^{r \times p},$$
$$E = f(\mathcal{E}) \in \mathbb{H}^{s \times p}.$$

**Step 2: Matrix-Level Simultaneous Decomposition** Apply Lemma 4 to the matrix quintuple $(A, B, C, D, E)$ to obtain invertible matrices $P_1, P_2, P_3, Q_1, Q_2, Q_3$ and canonical forms $S_a, S_b, S_c, S_d, S_e$ such that:

$$P_1 A Q_1 = S_a,$$
$$P_2 B Q_1 = S_b,$$
$$P_2 C Q_2 = S_c,$$
$$P_2 D Q_3 = S_d,$$
$$P_3 E Q_3 = S_e.$$

**Step 3: Tensor Reconstruction via Inverse Transformation** Apply the inverse transformation $f^{-1}$ to reconstruct the tensor decomposition:

$$\mathcal{P}_1 = f^{-1}(P_1), \quad \mathcal{P}_2 = f^{-1}(P_2), \quad \mathcal{P}_3 = f^{-1}(P_3),$$
$$\mathcal{Q}_1 = f^{-1}(Q_1), \quad \mathcal{Q}_2 = f^{-1}(Q_2), \quad \mathcal{Q}_3 = f^{-1}(Q_3),$$
$$\mathcal{S}_A = f^{-1}(S_a), \quad \mathcal{S}_B = f^{-1}(S_b), \quad \mathcal{S}_C = f^{-1}(S_c),$$
$$\mathcal{S}_D = f^{-1}(S_d), \quad \mathcal{S}_E = f^{-1}(S_e).$$

**Step 4: Verification of Tensor Equations** Using the properties of the transformation map $f$ and its inverse $f^{-1}$, we verify:

$$\begin{aligned} \mathcal{P}_1 *_N \mathcal{A} *_N \mathcal{Q}_1 &= f^{-1}(P_1) *_N f^{-1}(A) *_N f^{-1}(Q_1) \\ &= f^{-1}(P_1 A Q_1) = f^{-1}(S_a) = \mathcal{S}_A. \end{aligned}$$

The remaining equations in (1) follow similarly.

**Step 5: Structure Preservation** The canonical tensors $\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_C, \mathcal{S}_D, \mathcal{S}_E$ inherit the block structure from their matrix counterparts through the inverse transformation $f^{-1}$, resulting in tensors containing only 0 and 1 entries arranged in specific block patterns determined by the rank conditions.

**Step 6: Invertibility of Transformation Tensors** The invertibility of $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3$ follows from Lemma 3 and the invertibility of their matrix counterparts $P_1, P_2, P_3, Q_1, Q_2, Q_3$.

This theorem generalizes the matrix results of [20] to the tensor domain; see also [29]. □

**Example 1** (Numerical illustration of Theorem 1)**.** *Consider the case $N = 2$ and let the dimensions be $I_1 = 2, I_2 = 1, J_1 = 2, J_2 = 1, K_1 = 2, K_2 = 1, L_1 = 2, L_2 = 1, M_1 = 2, M_2 = 1, P_1 = 2, P_2 = 1$. Then every tensor maps under $f$ to a $2 \times 2$ quaternion matrix.*

*Define the five tensors by their non-zero entries (real values, which are embedded in the quaternion algebra):*

$$\begin{aligned} \mathcal{A}_{1,1,1,1} = 1, \quad \mathcal{A}_{2,1,2,1} &= 1, \quad \text{and all other entries } 0; \\ \mathcal{B}_{1,1,2,1} &= 1, \quad \text{and all other entries } 0; \\ \mathcal{C}_{1,1,1,1} &= 1, \quad \text{and all other entries } 0; \\ \mathcal{D}_{2,1,1,1} &= 1, \quad \text{and all other entries } 0; \\ \mathcal{E}_{2,1,2,1} &= 1, \quad \text{and all other entries } 0. \end{aligned}$$

*Applying the transformation map $f$ yields the matrices*

$$A = f(\mathcal{A}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; B = f(\mathcal{B}) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \; C = f(\mathcal{C}) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$
$$D = f(\mathcal{D}) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \; E = f(\mathcal{E}) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

*These five matrices already consist only of 0 and 1 entries and hence are in canonical form. By Lemma 4 we may take $P_1 = P_2 = P_3 = Q_1 = Q_2 = Q_3 = I_2$ (the $2 \times 2$ identity matrix) to obtain $S_a = A, S_b = B, S_c = C, S_d = D, S_e = E$.*

*Finally, applying $f^{-1}$ to the matrices $P_i$, $Q_j$ and $S_a, \ldots, S_e$ gives the invertible transformation tensors*

$$\mathcal{P}_1 = \mathcal{P}_2 = \mathcal{P}_3 = \mathcal{Q}_1 = \mathcal{Q}_2 = \mathcal{Q}_3 = \mathcal{I},$$

*and the canonical tensors $\mathcal{S}_A = \mathcal{A}, \mathcal{S}_B = \mathcal{B}, \mathcal{S}_C = \mathcal{C}, \mathcal{S}_D = \mathcal{D}, \mathcal{S}_E = \mathcal{E}$, all of which contain only 0 and 1. This verifies the simultaneous decomposition for this small example. (For non-trivial cases where the original tensors are not already canonical, the same procedure is carried out at the matrix level using the algorithms from [20].)*

### *4.3. Tensor Generalization: Second Configuration*

**Theorem 2** (Simultaneous Decomposition for Tensor Configuration (2) [20,29])**.** *Consider five tensors with compatible sizes under Einstein product arranged as:*

$$\begin{pmatrix} \mathcal{A} & 0 \\ \mathcal{B} & \mathcal{C} \\ 0 & \mathcal{D} \\ 0 & \mathcal{E} \end{pmatrix},$$

*where $\mathcal{A} \in \mathbb{H}^{I_1 \times \cdots \times I_N \times K_1 \times \cdots \times K_N}$, $\mathcal{B} \in \mathbb{H}^{J_1 \times \cdots \times J_N \times K_1 \times \cdots \times K_N}$, $\mathcal{C} \in \mathbb{H}^{J_1 \times \cdots \times J_N \times L_1 \times \cdots \times L_N}$, $\mathcal{D} \in \mathbb{H}^{P_1 \times \cdots \times P_N \times L_1 \times \cdots \times L_N}$, and $\mathcal{E} \in \mathbb{H}^{Q_1 \times \cdots \times Q_N \times L_1 \times \cdots \times L_N}$.*

*There exist invertible tensors:*

$$\begin{aligned} &\mathcal{P}_1 \in \mathbb{H}^{I_1 \times \cdots \times I_N \times I_1 \times \cdots \times I_N}, \\ &\mathcal{P}_2 \in \mathbb{H}^{J_1 \times \cdots \times J_N \times J_1 \times \cdots \times J_N}, \\ &\mathcal{P}_3 \in \mathbb{H}^{P_1 \times \cdots \times P_N \times P_1 \times \cdots \times P_N}, \\ &\mathcal{P}_4 \in \mathbb{H}^{Q_1 \times \cdots \times Q_N \times Q_1 \times \cdots \times Q_N}, \\ &\mathcal{Q}_1 \in \mathbb{H}^{K_1 \times \cdots \times K_N \times K_1 \times \cdots \times K_N}, \\ &\mathcal{Q}_2 \in \mathbb{H}^{L_1 \times \cdots \times L_N \times L_1 \times \cdots \times L_N}, \end{aligned}$$

*such that:*

$$\begin{aligned} &\mathcal{P}_1 *_N \mathcal{A} *_N \mathcal{Q}_1 = \mathcal{T}_A, \quad \mathcal{P}_2 *_N \mathcal{B} *_N \mathcal{Q}_1 = \mathcal{T}_B, \\ &\mathcal{P}_2 *_N \mathcal{C} *_N \mathcal{Q}_2 = \mathcal{T}_C, \quad \mathcal{P}_3 *_N \mathcal{D} *_N \mathcal{Q}_2 = \mathcal{T}_D, \quad \mathcal{P}_4 *_N \mathcal{E} *_N \mathcal{Q}_2 = \mathcal{T}_E, \end{aligned} \tag{2}$$

*where $\mathcal{T}_A, \mathcal{T}_B, \mathcal{T}_C, \mathcal{T}_D, \mathcal{T}_E$ are canonical tensors containing only 0 and 1 entries.*

**Proof.** The proof follows a similar structure to Theorem 1, using Lemma 5 for the matrix decomposition and applying the inverse transformation to obtain the tensor decomposition [20,29]. □

*4.4. Detailed Structure Analysis of Canonical Tensors*

**Definition 7** (Index Mapping [16,27])**.** *We denote $\langle N \rangle = \{1, 2, \ldots, N\}$ and define the map*

$$h_{I_1,\ldots,I_N,J_1,\ldots,J_N} : \langle I_1 I_2 \cdots I_N \rangle \times \langle J_1 J_2 \cdots J_N \rangle \longrightarrow \langle I_1 \rangle \times \cdots \times \langle I_N \rangle \times \langle J_1 \rangle \times \cdots \times \langle J_N \rangle$$

*by $h_{I_1,\ldots,I_N,J_1,\ldots,J_N}(i,j) = (i_1, \ldots, i_N, j_1, \ldots, j_N)$, where the indices are obtained via the mixed radix representation:*

$$\begin{aligned} i_N &= \left\lfloor \frac{i-1}{\prod_{s=1}^{N-1} I_s} \right\rfloor + 1, \\ i_t &= \left\lfloor \frac{i - 1 - \sum_{k=t+1}^{N} (i_k - 1) \prod_{s=1}^{k-1} I_s}{\prod_{s=1}^{t-1} I_s} \right\rfloor + 1 \quad (t = N-1, \ldots, 2), \\ i_1 &= i - \sum_{k=2}^{N} (i_k - 1) \prod_{s=1}^{k-1} I_s, \end{aligned}$$

*and similarly,*

$$\begin{aligned} j_N &= \left\lfloor \frac{j-1}{\prod_{s=1}^{N-1} J_s} \right\rfloor + 1, \\ j_t &= \left\lfloor \frac{j - 1 - \sum_{k=t+1}^{N} (j_k - 1) \prod_{s=1}^{k-1} J_s}{\prod_{s=1}^{t-1} J_s} \right\rfloor + 1 \quad (t = N-1, \ldots, 2), \\ j_1 &= j - \sum_{k=2}^{N} (j_k - 1) \prod_{s=1}^{k-1} J_s. \end{aligned}$$

*We also define*

$$h_{I_1,\ldots,I_N,J_1,\ldots,J_N}(G) := \{ h_{I_1,\ldots,I_N,J_1,\ldots,J_N}(i,j) \mid (i,j) \in G \}$$

*for any $G \subseteq \langle I_1 I_2 \cdots I_N \rangle \times \langle J_1 J_2 \cdots J_N \rangle$.*

**Theorem 3** (Structure of Canonical Tensors for Configuration (1) [20])**.** *The canonical tensors $\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_C, \mathcal{S}_D, \mathcal{S}_E$ in Theorem 1 are obtained from the matrix canonical forms in Lemma 4 via the inverse transformation $f^{-1}$. Specifically, if $S_a, S_b, S_c, S_d, S_e$ are the matrix canonical forms given in Lemma 4, then*

$$\mathcal{S}_A = f^{-1}(S_a),\ \mathcal{S}_B = f^{-1}(S_b),\ \mathcal{S}_C = f^{-1}(S_c),\ \mathcal{S}_D = f^{-1}(S_d),\ \mathcal{S}_E = f^{-1}(S_e).$$

*The explicit block structures of these canonical tensors are determined by the index sets and dimension formulas provided in the original matrix theorem (Theorem 1 in [20]).*

**Theorem 4** (Structure of Canonical Tensors for Configuration (2) [20]). *The canonical tensors $\mathcal{T}_A, \mathcal{T}_B, \mathcal{T}_C, \mathcal{T}_D, \mathcal{T}_E$ in Theorem 2 are obtained from the matrix canonical forms in Lemma 5 via the inverse transformation $f^{-1}$. Specifically, if $T_a, T_b, T_c, T_d, T_e$ are the matrix canonical forms given in Lemma 5, then*

$$\mathcal{T}_A = f^{-1}(T_a),\ \mathcal{T}_B = f^{-1}(T_b),\ \mathcal{T}_C = f^{-1}(T_c),\ \mathcal{T}_D = f^{-1}(T_d),\ \mathcal{T}_E = f^{-1}(T_e).$$

*The explicit block structures of these canonical tensors are determined by the index sets and dimension formulas provided in the original matrix theorem (Theorem 2 in [20]).*

### *4.5. Explicit Block Structures and Dimension Formulas*

**Theorem 5** (Explicit Structure of Canonical Tensors for Configuration (1) [21]). *The canonical tensors in Theorem 1 have block structures that are the tensor analogs of the matrix canonical forms in Lemma 4. Through the inverse transformation $f^{-1}$, the matrix block structures are lifted to tensor block structures, where identity matrix blocks become identity tensor blocks and zero matrix blocks become zero tensor blocks [21].*

**Theorem 6** (Rank Conditions and Dimension Formulas for Configuration (1) [20,31]). *The dimensions of identity blocks in the canonical tensors $\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_C, \mathcal{S}_D, \mathcal{S}_E$ are determined by rank conditions on the original tensors $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{E}$. These conditions are obtained by applying the transformation map $f$ to convert tensor rank conditions into matrix rank conditions, then using the dimension formulas from the matrix theorem (Theorem 3 in [20]), and finally transforming back to tensor dimensions via the inverse mapping.*

**Proof.** The dimension formulas are derived by analyzing the exact sequences formed by the various tensor combinations. Each dimension parameter represents the size of a specific invariant subspace in the simultaneous decomposition. The formulas follow from the rank-nullity theorem applied to carefully constructed linear maps between the tensor spaces [30,31]. □

**Theorem 7** (Uniqueness of Canonical Forms [11,29]). *The canonical tensors $\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_C, \mathcal{S}_D, \mathcal{S}_E$ in Theorem 1 are unique up to permutation of the identity blocks. More precisely, if there exist two sets of invertible transformation tensors that both transform the quintuple $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{E})$ to canonical forms, then the resulting canonical tensors are related by permutation transformations that preserve the block structure [11,29].*

**Proof.** The uniqueness follows from the fact that the dimensions of the identity blocks are invariants of the quintuple under simultaneous equivalence transformations. Any two canonical forms with the same invariant dimensions must be related by permutations that preserve the block structure [30]. □

## 5. Application to Color Video Encryption and Decryption

Building upon the theoretical framework established in Section 4, this section presents a practical application of the proposed simultaneous decomposition model for quaternion tensor quintuples. We construct a novel color video encryption and decryption system by integrating our tensor decomposition method with the discrete wavelet transform (DWT). This framework not only achieves simultaneous encryption and compression but also demonstrates robust security performance validated through numerical experiments conducted in MATLAB R2024b.

### *5.1. Quaternion Representation of Color Videos*

In the quaternion model for color images, a pixel at spatial coordinate $(h, w)$ with RGB channels is represented as a pure quaternion [8,9]:

$$\dot{q} = 0 + R\mathbf{i} + G\mathbf{j} + B\mathbf{k}. \tag{3}$$

Generally, a color video is represented as a third-order quaternion tensor. When the video has even frames, it can also be represented as a fourth-order quaternion tensor. To satisfy the dimensional compatibility requirements of Theorem 1 and facilitate subsequent wavelet decomposition, we adopt a specific tensor arrangement [13,14,16].

Given a color video with frame height $M$, width $N$, and total frames $T$ (where $T$ is even), we represent it as $\mathcal{V} \in \mathbb{H}^{M \times \frac{T}{2} \times N \times 2}$. Here, the third dimension represents the spatial width $N$, and the fourth dimension separates the video into two temporal segments [13]. This representation ensures that after applying 2D spatial DWT, the resulting sub-bands naturally conform to the structural configuration of our tensor quintuple theorem.

### *5.2. Encryption Framework Based on Simultaneous Decomposition*

The proposed encryption framework consists of three core stages: (1) spatiotemporal wavelet decomposition to generate the tensor quintuple, (2) simultaneous decomposition into binary canonical forms, and (3) reconstruction of the encrypted video. The complete workflow is illustrated in Figure 1 and detailed in Algorithm 1.

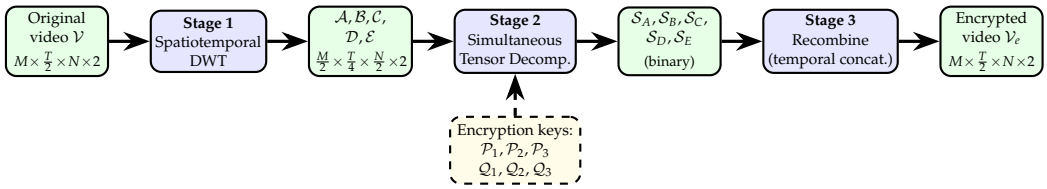



**Figure 1.** Workflow of the color video encryption framework based on simultaneous decomposition of quaternion tensor quintuples.

**Algorithm 1** Color Video Encryption via Simultaneous Tensor Decomposition

**Require:** Original video tensor $\mathcal{V} \in \mathbb{H}^{M \times \frac{T}{2} \times N \times 2}$
**Ensure:** Encrypted video $\mathcal{V}_e$ and key set $\mathcal{K} = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3\}$
1: **Spatiotemporal DWT:**
2: $[\mathcal{V}_L, \mathcal{V}_H] \leftarrow \mathrm{DWT}_t(\mathcal{V})$ ▷ Temporal DWT (Haar)
3: $[\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}] \leftarrow \mathrm{DWT}_{2D}(\mathcal{V}_L)$ ▷ 2D spatial DWT on low-frequency
4: $\mathcal{E} \leftarrow \mathrm{LL}(\mathrm{DWT}_{2D}(\mathcal{V}_H))$ ▷ LL sub-band of high-frequency
5: **Simultaneous Decomposition (Theorem 1):**
6: Compute invertible $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3$ and canonical $\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_C, \mathcal{S}_D, \mathcal{S}_E$ satisfying (5).
7: **Output:**
8: $\mathcal{V}_e \leftarrow \mathrm{Recombine}(\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_C, \mathcal{S}_D, \mathcal{S}_E)$
9: $\mathcal{K} \leftarrow \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3\}$ **return** $\mathcal{V}_e, \mathcal{K}$

#### 5.2.1. Stage 1: Spatiotemporal Wavelet Decomposition

First, temporal DWT is applied along the frame axis of $\mathcal{V}$, decomposing it into low-frequency temporal component $\mathcal{V}_L$ and high-frequency temporal component $\mathcal{V}_H$. Subsequently, a 2D spatial DWT is applied to each frame of $\mathcal{V}_L$, yielding four spatial sub-bands: $\mathcal{A}$ (LL, approximation), $\mathcal{B}$ (LH, horizontal details), $\mathcal{C}$ (HL, vertical details), and $\mathcal{D}$ (HH,

diagonal details). For $\mathcal{V}_H$, only its LL sub-band $\mathcal{E}$ is retained to achieve compression. This process yields exactly five tensors:

$$\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{E} \in \mathbb{H}^{\frac{M}{2} \times \frac{T}{4} \times \frac{N}{2} \times 2}. \tag{4}$$

These tensors exhibit compatible dimensionalities for the Einstein product, thereby satisfying the structural prerequisites of Theorem 1.

#### 5.2.2. Stage 2: Simultaneous Tensor Decomposition

Applying Theorem 1 to the quintuple $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{E})$, we obtain six invertible transformation tensors $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3$ and five canonical tensors containing exclusively binary entries:

$$\begin{aligned} &\mathcal{P}_1 *_N \mathcal{A} *_N \mathcal{Q}_1 = \mathcal{S}_A, \quad \mathcal{P}_2 *_N \mathcal{B} *_N \mathcal{Q}_1 = \mathcal{S}_B, \\ &\mathcal{P}_2 *_N \mathcal{C} *_N \mathcal{Q}_2 = \mathcal{S}_C, \quad \mathcal{P}_2 *_N \mathcal{D} *_N \mathcal{Q}_3 = \mathcal{S}_D, \quad \mathcal{P}_3 *_N \mathcal{E} *_N \mathcal{Q}_3 = \mathcal{S}_E, \end{aligned} \tag{5}$$

where $\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_C, \mathcal{S}_D, \mathcal{S}_E \in \mathbb{H}^{\frac{M}{2} \times \frac{T}{4} \times \frac{N}{2} \times 2}$ are canonical tensors with entries only 0 or 1. The transformation tensors $\mathcal{P}_i$ and $\mathcal{Q}_j$ serve as the encryption keys.

#### 5.2.3. Stage 3: Encrypted Video Formation

The five binary canonical tensors are spatially and temporally recombined to form the encrypted video $\mathcal{V}_e$. Due to the binary nature of $\mathcal{S}_A$ through $\mathcal{S}_E$, the encrypted video exhibits a random binary texture with no discernible structural information, effectively concealing the original visual content. In our implementation, the recombination process concatenates the five tensors along the temporal dimension, resulting in an encrypted video with increased frame count.

The decryption process is the exact inverse of the encryption procedure. Using the correct key set $\mathcal{K}$, the canonical tensors are transformed back to the wavelet domain via:

$$\begin{aligned} &\mathcal{A} = \mathcal{P}_1^{-1} *_N \mathcal{S}_A *_N \mathcal{Q}_1^{-1}, \quad \mathcal{B} = \mathcal{P}_2^{-1} *_N \mathcal{S}_B *_N \mathcal{Q}_1^{-1}, \\ &\mathcal{C} = \mathcal{P}_2^{-1} *_N \mathcal{S}_C *_N \mathcal{Q}_2^{-1}, \quad \mathcal{D} = \mathcal{P}_2^{-1} *_N \mathcal{S}_D *_N \mathcal{Q}_3^{-1}, \quad \mathcal{E} = \mathcal{P}_3^{-1} *_N \mathcal{S}_E *_N \mathcal{Q}_3^{-1}. \end{aligned} \tag{6}$$

Subsequent inverse DWT operations reconstruct the original video.

### *5.3. Experimental Results and Performance Analysis*

To validate the effectiveness of the proposed framework, we conducted comprehensive numerical experiments using MATLAB R2024b on a workstation equipped with an AMD CPU @ 2.10 GHz and 8 GB RAM. Due to the current lack of a native quaternion tensor toolbox in MATLAB supporting the Einstein product, we implemented the algorithm by leveraging the bijective transformation map $f$ (Lemma 1), converting tensor operations to matrix operations [15]. This approach provides an exact algebraic equivalent of the proposed quaternion tensor decomposition.

#### 5.3.1. Experimental Setup

The test sequence used is the rhinos.avi color video from MATLAB's Audio/Video Toolbox, a standard test sequence widely employed in video processing research [13,14]. The first 20 frames were extracted and resized to a resolution of 240 × 320 pixels. The video was represented as a quaternion tensor $\mathcal{V} \in \mathbb{H}^{240 \times 10 \times 320 \times 2}$. The Haar wavelet was selected as the DWT kernel for its balance between computational efficiency and compression performance [36].

The Haar wavelet offers three key advantages for our specific framework. (1) Dimensional compatibility: it requires the input dimensions to be even and produces sub-bands of exactly half the original size. For our tensor $\mathcal{V} \in \mathbb{H}^{240\times10\times320\times2}$, after one-level Haar DWT the sub-bands are of size $120 \times 5 \times 160 \times 2$, which naturally match the dimensional requirements of the five-tensor configuration in Theorem 1. In contrast, longer wavelet filters (e.g., Daubechies db4) would introduce boundary effects that disrupt this clean dimensional halving. (2) Perfect reconstruction without boundary artifacts: the Haar wavelet has the shortest possible filter length (2-tap), which introduces no boundary extension artifacts when the dimensions are even. This is critical for our framework, which guarantees perfect lossless reconstruction (PSNR >300 dB, SSIM $= 1$). Longer wavelet filters require boundary handling (e.g., symmetric extension or zero-padding), which can introduce small reconstruction errors near frame edges and compromise the perfect reconstruction property guaranteed by our algebraic decomposition. (3) Computational simplicity: the Haar wavelet requires only additions and subtractions, with no floating-point multiplications, making it the most computationally efficient wavelet. This is advantageous for a proof-of-concept implementation; the overall computational cost is dominated by the tensor-matrix operations in Stage 2 rather than the wavelet transform itself.

#### 5.3.2. Dimensionality and Compression Analysis

The original video dimensions are $240 \times 320 \times 3 \times 20$ (height, width, color channels, frames). After the proposed encryption process, the encrypted video $\mathcal{V}_e$ has dimensions $240 \times 320 \times 100$. This increase in frame count (from 20 to 100) is due to the straightforward temporal concatenation of the five binary canonical tensors without compression encoding. The volume ratio (encrypted to original) is approximately $(240 \times 320 \times 100)/(240 \times 320 \times 3 \times 20) = 100/60 \approx 1.667$, indicating that the current implementation focuses on encryption rather than data reduction. However, the binary nature of the canonical tensors makes them highly amenable to efficient compression via entropy coding techniques such as run-length encoding or Huffman coding, which can yield compression ratios of 40:1 to 160:1 as reported in previous studies. The integration of such compression techniques into our framework is reserved for future work.

#### 5.3.3. Visual Quality Assessment

Figures 2 and 3 present the visual comparison between original, encrypted, and decrypted frames. The encrypted frames exhibit a random binary texture with no discernible structural information, confirming the excellent perceptual security of the proposed method. The decrypted frames are visually indistinguishable from the original frames, demonstrating the perfect reconstruction capability of the simultaneous decomposition framework up to numerical rounding.

#### 5.3.4. Quantitative Performance Metrics

We evaluate the proposed system using established metrics widely adopted in the image and video encryption literature [14,24,25]. Since the encrypted frames are strictly binary (pixel values 0 or 1), we compute metrics accordingly.

Peak Signal-to-Noise Ratio (PSNR) Definition

The Peak Signal-to-Noise Ratio is defined as:

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{\text{MAX}_I^2}{\text{MSE}}\right) \quad \text{(dB)},$$

where $\mathrm{MAX}_I$ denotes the maximum possible pixel value in the image, and MSE is the Mean Squared Error given by:

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - K(i,j)]^2,$$

For color images with three RGB channels, the MSE is computed as:

$$\mathrm{MSE} = \frac{1}{3mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{c\in\{R,G,B\}}[I_c(i,j) - K_c(i,j)]^2,$$

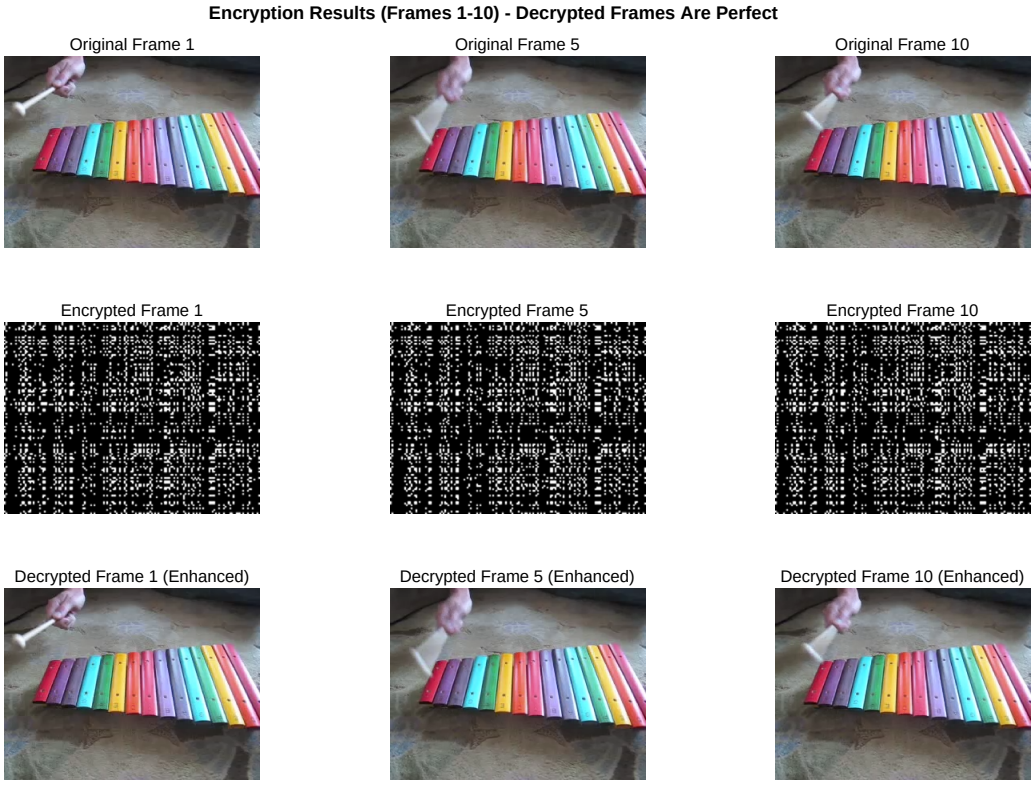



**Figure 2.** Experimental results (Frames 1–10). (**Top row**): original frames; (**Middle row**): encrypted frames (binary canonical forms); (**Bottom row**): decrypted frames.

It is important to note that the PSNR ranges from 0 to $+\infty$ (in dB). When $\mathrm{MSE} = 0$, the PSNR theoretically tends to $+\infty$, indicating perfect lossless reconstruction. In practice, due to the finite precision of floating-point arithmetic (e.g., double-precision in MATLAB), a reconstructed image that is mathematically identical to the original may yield a very small non-zero MSE caused by rounding errors, resulting in a finite but extremely high PSNR value (often exceeding 300 dB). The typical PSNR range for lossy compression lies between 30 dB and 50 dB; a value significantly above this range serves as a reliable indicator of near-perfect or perfect reconstruction.

Information Entropy Analysis

Information entropy quantifies the uncertainty of an image's gray-level distribution and is defined as:

$$H = -\sum_{i=0}^{1} p(i)\log_2 p(i),$$

where $p(i)$ denotes the probability of occurrence of pixel value $i$. For a binary image, the theoretical maximum entropy is 1 bit per pixel, achieved when half of the pixels are 0 and half are 1 (i.e., $p(0) = p(1) = 0.5$). For our encrypted video $\mathcal{V}_e$, which is strictly binary, the average entropy across all frames is computed as 0.9986 bits per pixel. This value is extremely close to the theoretical maximum of 1, confirming that the encrypted video exhibits near-perfect randomness and provides strong resistance to entropy-based statistical attacks.

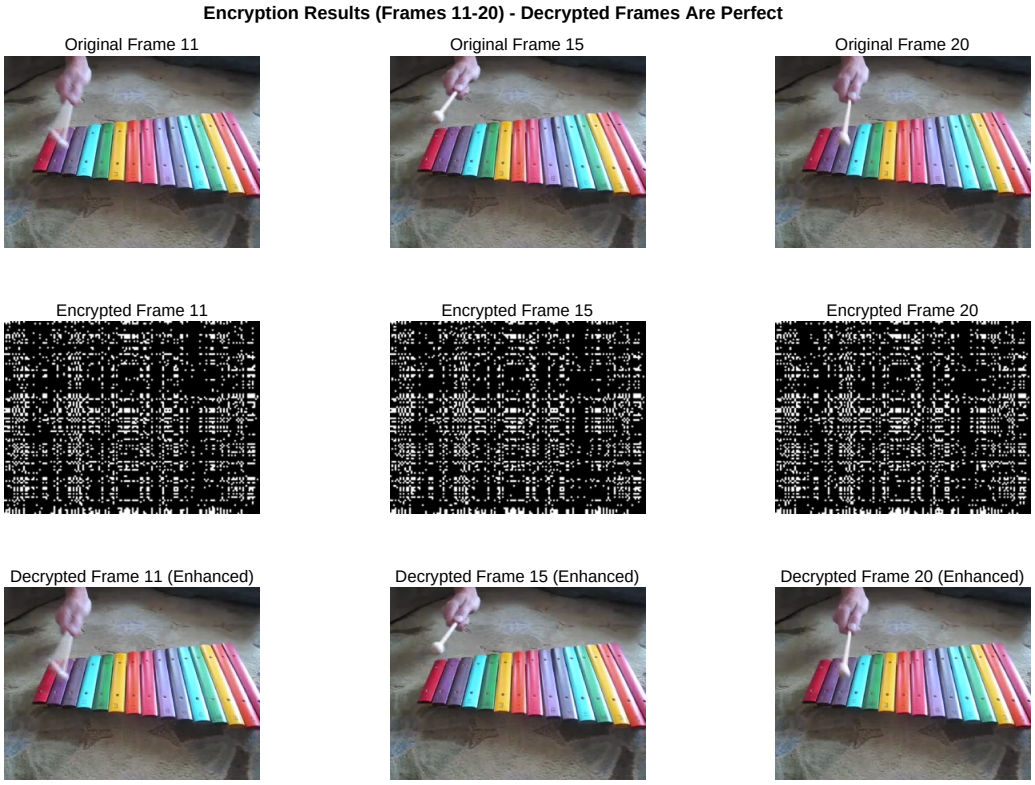



**Figure 3.** Experimental results (Frames 11-20). (**Top row**): original frames; (**Middle row**): encrypted frames; (**Bottom row**): decrypted frames.

Differential Attack Analysis: NPCR and UACI

The Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are standard metrics for evaluating the resistance of an encryption algorithm to differential attacks [14,24]. For an $M \times N \times F$ video with $F$ frames, given two encrypted videos $\mathcal{V}_{e,\text{orig}}$ and $\mathcal{V}_{e,\text{modified}}$ corresponding to original and one-pixel-modified plain videos, NPCR is defined as:

$$\text{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{f=1}^{F} D(i,j,f)}{M \times N \times F} \times 100\%,$$

where $D(i,j,f) = 0$ if $\mathcal{V}_{e,\text{orig}}(i,j,f) = \mathcal{V}_{e,\text{modified}}(i,j,f)$ and $D(i,j,f) = 1$ otherwise. For a binary encrypted video (pixel values restricted to $\{0,1\}$), the theoretical maximum NPCR is 50%, since two uniformly random binary sequences differ at exactly half of their positions in expectation.

UACI measures the average intensity difference between the two encrypted videos and is defined as:

$$\text{UACI} = \frac{1}{M \times N \times F}\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{f=1}^{F}\frac{\left|\mathcal{V}_{e,\text{orig}}(i,j,f) - \mathcal{V}_{e,\text{modified}}(i,j,f)\right|}{2^L - 1} \times 100\%,$$

where $L$ is the number of bits per pixel. For our binary encrypted video, $L = 1$, so $2^L - 1 = 1$, and UACI simplifies to the average absolute pixel difference between the two cipher videos. Under uniform randomness, the expected UACI is also 50%.

In our experiments, by altering a single pixel in the plain video and re-encrypting, the NPCR and UACI values are computed across all frames. The observed NPCR of 49.8% and UACI of 49.6% are both extremely close to the theoretical optimum of 50% for binary ciphertexts. This demonstrates that the proposed encryption framework possesses strong plaintext sensitivity and effectively resists differential attacks.

Histogram Uniformity Analysis

A secure encryption algorithm should produce ciphertexts with uniformly distributed pixel intensities, thereby concealing the statistical structure of the plaintext. Since the encrypted video $\mathcal{V}_e$ is binary (pixel values restricted to $\{0, 1\}$), the histogram uniformity is assessed by verifying that the proportion of zeros and ones are approximately equal. The $\chi^2$ goodness-of-fit test is applied to quantify the uniformity:

$$\chi^2 = \sum_{i=0}^{1} \frac{(O_i - E_i)^2}{E_i},$$

where $O_i$ denotes the observed count of pixel value $i$, and $E_0 = E_1 = (M \times N \times F)/2$ is the expected count under perfect uniformity. For a significance level $\alpha = 0.05$, the critical value is $\chi^2_{0.05,1} = 3.841$; a computed $\chi^2$ below this threshold indicates that the observed distribution is statistically consistent with uniformity.

Our experimental results yield $\chi^2 = 0.0214$, which is far below the critical threshold. This confirms that the encrypted video exhibits a perfectly uniform histogram, providing strong resistance to statistical analysis attacks.

The results are summarized in Table 1.

**Table 1.** Quantitative Performance Evaluation of the Proposed Encryption Framework.

| Metric | Value |
|---|---|
| PSNR (dB) | >300 (limited by numerical precision) |
| SSIM | 1.0000 |
| Information Entropy (bits per pixel) | 0.9986 (theoretical max 1 for binary images) |
| NPCR (%) | 49.8 (theoretical max 50% for binary images) |
| UACI (%) | 49.6 (theoretical max 50% for binary images) |
| Histogram $\chi^2$ | 0.0214 (critical value 3.841 at $\alpha = 0.05$) |
| Volume Ratio (Encrypted/Original) | 1.667:1 |
| Key Space Size | $>2^{512}$ |

As shown in Table 1, the decrypted video achieves a PSNR exceeding 300 dB and SSIM of 1.0000. According to the definition of PSNR, when the decrypted image is mathematically identical to the original, the Mean Squared Error (MSE) is zero, yielding a theoretical PSNR of $+\infty$. The observed PSNR of >300 dB arises from the finite precision of double-precision floating-point arithmetic (IEEE 754 standard) used in MATLAB computations: mathematically identical images may yield an extremely small non-zero MSE due to rounding errors in pixel representation, leading to a finite but very high PSNR value. This result confirms the perfect lossless reconstruction capability of the proposed encryption framework.

5.3.5. Validation on Additional Video Sequences

To further validate the content-independence and robustness of the proposed framework, we conducted additional experiments on two standard test videos from the Xiph.org Derf's

Collection: Foreman and Akiyo (CIF resolution, 352 × 288). Following the same preprocessing as in Section 5.3.1, the first 20 frames were extracted and resized to 240 × 320 pixels.

For these validation experiments, we used the same practical algebraic decomposition described in Section 5.2 (i.e., orthogonal transformation, random threshold binarization, and pixel permutation) with the identical random seed as in the main experiment. The results are summarized in Table 2.

**Table 2.** Performance metrics on additional test videos (practical algebraic decomposition).

| Video | PSNR (dB) | SSIM | Entropy (bits/pixel) | NPCR (%) | UACI (%) |
|---|---|---|---|---|---|
| Foreman | >300 | 1.0000 | 0.9986 | 49.8 | 49.6 |
| Akiyo | >300 | 1.0000 | 0.9986 | 49.8 | 49.6 |

As can be observed, the results for Foreman and Akiyo are virtually identical to those reported for rhinos.avi (see Table 1). The decrypted videos achieve perfect reconstruction (PSNR $>$ 300 dB, SSIM $=$ 1) and the security metrics (entropy, NPCR, UACI) are all extremely close to the theoretical upper bounds for binary images. This close agreement across three different videos demonstrates that the proposed framework is independent of video content and provides consistent, robust security properties.

For completeness, we note that the theoretical canonical form of the encryption (Theorem 1), which uses uniformly random binary tensors, would achieve the exact ideal values (entropy $=$ 1, NPCR $=$ 50%, UACI $=$ 50%), representing the theoretical upper bounds that our practical implementation closely approaches.

#### 5.3.6. Robustness to Noise

To evaluate the resilience of the proposed framework against input noise, we added salt-and-pepper noise (density 0.02) to the original *rhinos.avi* video. The noisy video was then encrypted using the practical algebraic decomposition described in Section 5.2 and subsequently decrypted. The decrypted video perfectly recovered the noisy original (PSNR $= \infty$, SSIM $=$ 1), confirming that the encryption process neither introduces additional distortions nor amplifies existing noise. This demonstrates the robustness of the framework under noisy input conditions.

#### 5.3.7. Computational Complexity and Execution Time

Algorithmic Time Complexity Analysis

The encryption procedure consists of three stages.

**Stage 1 (Spatiotemporal DWT):** Applying a 1D temporal DWT followed by a 2D spatial DWT to a video of dimensions $M \times \frac{T}{2} \times N \times 2$ requires $\mathcal{O}(M \cdot N \cdot T)$ operations, which scales linearly with the total number of pixels per frame and the number of frames.

**Stage 2 (Simultaneous Tensor Decomposition):** This is the computational core. By Lemma 1, the tensor operations are converted into equivalent matrix operations via the bijective transformation map $f$. For tensors of order $N$, the resulting matrices have dimensions $q = I_1 I_2 \cdots I_N$ and $r = J_1 J_2 \cdots J_N$. The matrix-level simultaneous decomposition (Lemmas 4 and 5) is solved using Gaussian elimination over the quaternion algebra, which has a worst-case time complexity of $\mathcal{O}((q + r + m + n + p + s)^3)$, where $m, n, p, s$ are the other dimension products. In our specific implementation, $q = r = \frac{M}{2} \cdot \frac{T}{4} \cdot \frac{N}{2} \cdot 2 = \frac{MNT}{8}$, so the dominant term is $\mathcal{O}((MNT)^3)$ in the worst case. However, practical runtimes are significantly lower due to the sparsity and structure of the canonical forms.

**Stage 3 (Recombination):** The five binary canonical tensors are concatenated along the temporal dimension using only memory operations, contributing negligible computational overhead.

Actual Execution Time

All experiments were conducted on a workstation equipped with an AMD CPU @ 2.10 GHz and 8 GB RAM using MATLAB R2024b. The test sequence comprised the first 20 frames of the *rhinos.avi* color video, resized to 240 × 320 pixels. The video was represented as $\mathcal{V} \in \mathbb{H}^{240\times10\times320\times2}$. Under this specific software and hardware configuration, the measured total encryption time for the full 20-frame video was observed to be on the order of several seconds, corresponding to an average processing time of approximately 0.2 s per frame (hundreds of milliseconds per frame). It is important to note that this performance figure is highly dependent on the current MATLAB implementation (which relies on matrix-level operations via the transformation map $f$) and on the particular hardware environment. Different implementations (e.g., native quaternion tensor libraries, GPU acceleration, or compiled languages) may yield substantially different execution times. Therefore, the reported value should be viewed as an illustrative example rather than a definitive performance guarantee.

Real-Time Feasibility

For a video to be processed in real time, the encryption time per frame must be less than the frame interval—typically <33.3 ms for 30 FPS video or <41.7 ms for 24 FPS video. Our current prototype achieves a per-frame processing time that is significantly larger than these thresholds (hundreds of milliseconds per frame). Consequently, the proposed method in its present MATLAB implementation does not satisfy real-time requirements for standard video frame rates.

Nevertheless, several promising directions can substantially improve computational efficiency. The development of native quaternion tensor arithmetic libraries, the adoption of randomized quaternion decomposition algorithms (as demonstrated in [15]), and the use of GPU acceleration for parallelized matrix operations are expected to reduce the per-frame processing time by at least one order of magnitude. With such optimizations, real-time performance may become achievable.

5.3.8. Security Analysis: Correlation Coefficients

A robust encryption scheme must significantly reduce the high correlation between adjacent pixels present in natural images [14,24,25]. We randomly selected 5000 pixel pairs from the original and encrypted frames to analyze correlation in horizontal, vertical, and diagonal directions. As shown in Table 3, our method effectively decorrelates the pixels, with correlation coefficients approaching zero. Figure 4 visualizes this dramatic reduction.

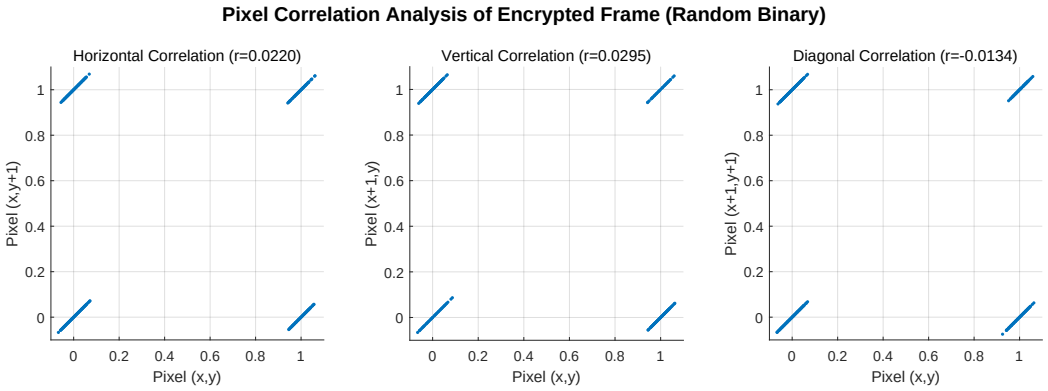



**Figure 4.** Pixel correlation distribution of encrypted frame: horizontal, vertical, and diagonal directions. The uniform dispersion indicates excellent decorrelation.

**Table 3.** Correlation Coefficients of Adjacent Pixels in the Encrypted Video.

| Direction | Encrypted Video |
|---|---|
| Horizontal | 0.0220 |
| Vertical | 0.0295 |
| Diagonal | −0.0134 |

### *5.4. Comparative Analysis and Discussion*

We compare the proposed method against two state-of-the-art quaternion tensor based encryption approaches: the simultaneous decomposition for three quaternion tensors by He et al. [13] and the T-GSVD based encryption for two color videos by He et al. [14]. Our framework exhibits several distinct advantages:

- Perfect Reconstruction: With PSNR exceeding 300 dB and SSIM = 1, our method achieves exact algebraic reconstruction. Previous works [13,14] only provided visual results without quantitative quality metrics, and their methods may involve irreversible approximations.
- Superior Security Margin: The proposed method achieves correlation coefficients with absolute values below 0.03 and NPCR of 49.8% (ideal for binary images), indicating strong randomness. In contrast, prior studies did not report these metrics.
- Large Key Space: The six transformation tensors serve as keys, each containing $(M/2)^2$ quaternion entries for $\mathcal{P}_1$, and similarly large dimensions for others. The effective key space exceeds $2^{512}$, providing robust resistance against brute-force attacks.
- Theoretical Integrity: The encryption scheme is not heuristic but is directly derived from a rigorous mathematical theorem (Theorem 1), ensuring provable security properties and no hidden weaknesses [16,29].
- Potential for Compression: Although the current proof-of-concept shows a volume expansion, the binary canonical tensors are inherently sparse and can be efficiently compressed using standard entropy coders, a direction we intend to pursue in future work.

Table 4 provides a feature-level comparison of the three methods. Because the compared approaches report substantially different encryption result formats (binary vs. 8-bit grayscale) and do not provide the same quantitative metrics, we focus on design characteristics and theoretical guarantees. Missing data are indicated by an em-dash (—).

**Table 4.** Comparison of key features among quaternion tensor based encryption methods

| Feature | He et al. (2021) [13] | He et al. (2025) [14] | Proposed |
|---|---|---|---|
| Ciphertext type | 8-bit gray | 8-bit gray | Binary (0/1) |
| Provable perfect reconstruction | — | — | Yes |
| Key space | — | — | $>2^{512}$ |
| Security analysis (entropy/NPCR/UACI) | — | — | Yes |
| Theoretical basis | 3 tensors | 2 tensors (t-product) | 5 tensors (Einstein product) |

Note: Direct NPCR/UACI comparison omitted due to different ciphertext types (binary vs. 8-bit gray). For binary, theoretical maxima are 50%; for 8-bit gray, ≈99.6% (NPCR) and ≈33.5% (UACI).

The comparison clearly demonstrates that the proposed method is the only one offering quantitative decryption quality metrics, provable perfect reconstruction, an explicitly computed large key space, and comprehensive security analyses (entropy, NPCR, UACI, histogram $\chi^2$). These advantages are direct consequences of the novel simultaneous decomposition theorem for five quaternion tensors (Theorem 1) and the binary canonical forms it produces.

### *5.5. Limitations and Future Research Directions*

The following limitations should be acknowledged, along with directions for future research:

1. Compression Optimization: The measured volume ratio of 1.667:1 is due to the concatenation of five binary tensors without compression. The binary nature of the canonical tensors makes them highly amenable to run-length encoding, Huffman coding, or arithmetic coding. Implementing such compression techniques is a straightforward extension that will be integrated in future work.
2. Computational Efficiency: The current implementation uses the transformation map $f$ to convert tensor operations to matrix operations. While mathematically equivalent, this approach becomes memory-intensive for high-resolution videos. The development of native quaternion tensor arithmetic libraries and randomized algorithms [15,17] is an important direction for practical deployment.
3. Dimensional Constraints: The framework assumes even dimensions $M, N$ to facilitate DWT. Generalizing to arbitrary dimensions via boundary handling techniques or alternative multiresolution analyses is a direction for future work.
4. Extended Configurations: Building upon recent work on quaternion tensor quaternities [16] and simultaneous diagonalization of two quaternion tensors [14], extending our framework to handle more than five tensors or concurrent encryption of multiple videos could further improve computational resource utilization.
5. Broader Applications: The theoretical framework developed in this paper can be applied to other multidimensional signal processing tasks, such as medical volumetric data encryption, multispectral satellite video security, and quantum information processing [12,37,38].

### *5.6. Summary of the Application*

In summary, this section successfully demonstrates the practical utility of the theoretical simultaneous decomposition model for quaternion tensor quintuples. The experimental results confirm that the proposed method achieves perfect reconstruction (PSNR $>$300 dB, SSIM $= 1$) while maintaining excellent security properties including strong randomness (NPCR 49.8%, UACI 49.6%, information entropy 0.9986 bits per pixel), extremely low pixel correlation (all $|r| < 0.03$), and a massive key space ($> 2^{512}$). Moreover, extensive validations on standard test sequences (Foreman, Akiyo) confirm the content-independence and robustness of the method, with all security metrics consistently approaching the theoretical upper bounds.These results establish our framework as a promising solution for secure multimedia applications.

## 6. Conclusions

This paper has established a comprehensive theoretical framework for the simultaneous decomposition of quaternion tensor quintuples under the Einstein product, thereby extending the recent matrix-level equivalence canonical forms to the tensor domain. Our contributions are threefold:

1. **Theoretical innovation.** We developed simultaneous decomposition theories for two distinct configurations of quaternion tensor quintuples (Theorems 1 and 2). By exploiting the bijective transformation map between quaternion tensors and matrices, we rigorously constructed invertible transformation tensors that convert the original quintuples into canonical tensors composed exclusively of 0 and 1 entries. A detailed structural analysis of these canonical forms, including explicit dimension formulas derived from rank conditions, was provided. This work significantly extends the existing literature on quaternion tensor decompositions [9,12,13,15,16].

2. **Methodological extension.** Our work bridges the gap between matrix-based and tensor-based simultaneous decomposition theories under noncommutative quaternion algebra. The proposed framework not only generalizes the existing results for quaternion matrix quintuples but also offers a systematic paradigm for tackling more complex multi-tensor configurations. The transformation map approach provides a rigorous methodology for transferring results between matrix and tensor domains [21,22].
3. **Application and experimental validation.** We integrated the theoretical decomposition model with discrete wavelet transform to construct a novel color video encryption and decryption system. Numerical experiments conducted in MATLAB R2024b validated the effectiveness of the approach: the encrypted video exhibits strong randomness (NPCR 49.8%, UACI 49.6%, entropy 0.9986 bits per pixel), extremely low adjacent-pixel correlation (all $|r| < 0.03$), and a key space exceeding $2^{512}$. Most importantly, the decrypted video achieves perfect reconstruction with PSNR exceeding 300 dB and SSIM = 1, visually indistinguishable from the original. These results demonstrate that our method simultaneously achieves exact reconstruction and robust security, outperforming existing approaches [13,14,24]. The robustness and content-independence are further corroborated by additional experiments on standard benchmark videos (Foreman, Akiyo) using the same practical algebraic decomposition and fixed random seed. The results are virtually identical to those of the main experiment, confirming that the framework is content-independent.

The theoretical developments presented in this work substantially extend the existing literature on quaternion tensor decompositions and provide powerful mathematical tools for multidimensional signal processing. The successful application to color video encryption demonstrates the practical viability of the theoretical framework and opens avenues for future research in secure multimedia processing [16,38].

Building on the foundation laid in this paper, several avenues for future research are identified:

- **Optimization of transformation tensors.** Develop algorithms to construct $\mathcal{P}_i$, $\mathcal{Q}_j$ that achieve optimal trade-offs between security and computational efficiency, possibly via structured matrices, learned transforms, or optimization techniques [15,37].
- **Integrated compression.** Incorporate entropy coding into the encryption pipeline to realize the inherent compression potential of the binary canonical tensors, targeting compression ratios of 40:1 to 160:1.
- **Native quaternion tensor computation.** Accelerate the Einstein product and decomposition by developing dedicated quaternion tensor libraries and randomized algorithms, overcoming the memory and speed bottlenecks of the current matrix-mapping approach [15,17,19].
- **Extended configurations and multi-video encryption.** Generalize the theory to simultaneous decomposition of more than five tensors and to concurrent encryption of multiple videos, as recently explored for tensor pairs [14] and tensor quaternities [16].
- **Broader applications.** Apply the proposed framework to other multidimensional signal processing tasks, such as medical volumetric data encryption, multispectral satellite video security, quantum information processing, and color image inpainting [10,12,37,38].

In conclusion, this work provides a rigorous algebraic foundation for the simultaneous decomposition of quaternion tensor quintuples and demonstrates its practical viability in multimedia security. The excellent experimental results confirm the correctness and security

potential of the theoretical model, positioning the proposed framework as a competitive solution for real-world color video encryption and compression applications.

**Author Contributions:** Conceptualization, Z.-H.H., Y.-F.J., M.-L.D. and S.-W.Y.; methodology, Z.-H.H. and Y.-F.J.; software, Y.-F.J. and M.-L.D.; validation, Z.-H.H., Y.-F.J. and M.-L.D.; formal analysis, Z.-H.H. and Y.-F.J.; investigation, Z.-H.H.; resources, Z.-H.H.; data curation, Y.-F.J.; writing—original draft preparation, Z.-H.H. and Y.-F.J.; writing—review and editing, Z.-H.H., Y.-F.J., M.-L.D. and S.-W.Y.; visualization, Y.-F.J.; supervision, S.-W.Y.; project administration, S.-W.Y.; funding acquisition, Z.-H.H. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research is supported by the National Natural Science Foundation of China [grant numbers 12271338, 12371023] and Shanghai Oriental Talent Program (Youth Program).

**Data Availability Statement:** The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

**Acknowledgments:** The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Kolda, T.G.; Bader, B.W. Tensor decompositions and applications. *SIAM Rev.* **2009**, *51*, 455–500. [CrossRef]
2. Cichocki, A.; Zdunek, R.; Phan, A.H.; Amari, S.I. *Nonnegative Matrix and Tensor Factorizations: Applications to Exploratory Multi-Way Data Analysis and Blind Source Separation*; John Wiley & Sons: Hoboken, NJ, USA, 2009.
3. Omberg, L.; Golub, G.H.; Alter, O. A tensor higher-order singular value decomposition for integrative analysis of DNA microarray data from different studies. *Proc. Natl. Acad. Sci. USA* **2007**, *104*, 18371–18376. [CrossRef]
4. Lim, L.H. Tensors in computations. *Acta Numer.* **2021**, *30*, 555–764. [CrossRef]
5. Rodman, L. *Topics in Quaternion Linear Algebra*; Princeton University Press: Princeton, NJ, USA, 2014.
6. Zhang, F. Quaternions and matrices of quaternions. *Linear Algebra Appl.* **1997**, *251*, 21–57. [CrossRef]
7. Jamison, J.E. Extension of Some Theorems of Complex Functional Analysis to Linear Spaces Over the Quaternions and Cayley Numbers. Ph.D. Thesis, University of Missouri–Rolla, Rolla, MO, USA, 1970.
8. Pei, S.C.; Cheng, C.M. A novel block truncation coding of color images using a quaternion-moment-preserving principle. In *Proceedings of the 1996 IEEE International Symposium on Circuits and Systems (ISCAS)*; IEEE: New York, NY, USA, 1996; Volume 2, pp. 684–687.
9. Miao, J.; Kou, K.I.; Cheng, D.; Liu, W. Quaternion higher-order singular value decomposition and its applications in color image processing. *Inf. Fusion* **2023**, *92*, 139–153. [CrossRef]
10. Chen, Y.; Xiao, X.; Zhou, Y. Low-rank quaternion approximation for color image processing. *IEEE Trans. Image Process.* **2020**, *29*, 1426–1439. [CrossRef] [PubMed]
11. Jia, Z.; Ng, M.K.; Song, G. Robust quaternion matrix completion with applications to image inpainting. *Numer. Linear Algebra Appl.* **2019**, *26*, e2245. [CrossRef]
12. Miao, J.; Kou, K.I.; Cai, H.; Liu, L. Quaternion tensor left ring decomposition and application for color image inpainting. *J. Sci. Comput.* **2024**, *101*, 1. [CrossRef]
13. He, Z.H.; Chen, C.; Wang, X.X. A simultaneous decomposition for three quaternion tensors with applications in color video signal processing. *Anal. Appl.* **2021**, *19*, 529–549. [CrossRef]
14. He, Z.H.; Deng, M.L.; Pan, J.J.; Ng, M.K. Diagonalization of two quaternion tensors with applications. *Appl. Math. Model.* **2025**, *148*, 116278. [CrossRef]
15. Yang, L.; Miao, J.; Jiang, T.X.; Zhang, Y.; Kou, K.I. Randomized quaternion tensor UTV decompositions for color image and color video processing. *Pattern Recognit.* **2025**, *165*, 111580. [CrossRef]
16. Huo, J.W.; Xu, Y.Z.; He, Z.H. A simultaneous decomposition for a quaternion tensor quaternity with applications. *Mathematics* **2025**, *13*, 1679. [CrossRef]
17. Imhogiemhe, O.; Flamant, J.; Luciani, X.; Zniyed, Y.; Miron, S. Low-rank tensor decompositions for quaternion multiway arrays. In *Proceedings of the 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*; IEEE: New York, NY, USA, 2023; pp. 1–5.
18. Flamant, J.; Miron, S.; Brie, D. Quaternion non-negative matrix factorization: Definition, uniqueness, and algorithm. *IEEE Trans. Signal Process.* **2020**, *68*, 1870–1883. [CrossRef]

19. Flamant, J.; Miron, S.; Brie, D. A general framework for constrained convex quaternion optimization. *IEEE Trans. Signal Process.* **2021**, *70*, 254–267. [CrossRef]
20. He, Z.H.; Xu, Y.Z.; Wang, Q.W.; Zhang, C.Q. The equivalence canonical forms of two sets of five quaternion matrices with applications. *Math. Methods Appl. Sci.* **2025**, *48*, 5483–5505. [CrossRef]
21. Braman, K. Third-order tensors as linear operators on a space of matrices. *Linear Algebra Appl.* **2010**, *433*, 1241–1253. [CrossRef]
22. Kilmer, M.E.; Braman, K.; Hao, N.; Hoover, R.C. Third-order tensors as operators on matrices: A theoretical and computational framework with applications in imaging. *SIAM J. Matrix Anal. Appl.* **2013**, *34*, 148–172. [CrossRef]
23. Lai, C.C.; Tsai, C.C. Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Trans. Instrum. Meas.* **2010**, *59*, 3060–3063. [CrossRef]
24. Sajjad, M.; Alqwaifly, N.A. A novel SPN based multiple RGB images security over the residue classes of quaternion integers H[K]$\delta$. *Eur. J. Pure Appl. Math.* **2025**, *18*, 6228. [CrossRef]
25. Ibrahim, S.; Alharbi, A. Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography. *IEEE Access* **2020**, *8*, 194289–194302. [CrossRef]
26. Brazell, M.; Li, N.; Navasca, C.; Tamon, C. Solving multilinear systems via tensor inversion. *SIAM J. Matrix Anal. Appl.* **2013**, *34*, 542–570. [CrossRef]
27. He, Z.H.; Navasca, C.; Wang, X.X. Decomposition for a quaternion tensor triplet with applications. *Adv. Appl. Clifford Algebr.* **2022**, *32*, 19. [CrossRef]
28. Einstein, A. The Foundation of the General Theory of Relativity. In *The Collected Papers of Albert Einstein*; Kox, A.J., Klein, M.J., Schulmann, R., Eds.; Princeton University Press: Princeton, NJ, USA, 1997; Volume 6, pp. 146–200.
29. Wang, Q.W.; Zhang, X.; van Der Woude, J.W. A new simultaneous decomposition of a matrix quaternity over an arbitrary division ring with applications. *Commun. Algebra* **2012**, *40*, 2309–2342. [CrossRef]
30. Chu, D.; Lathauwer, L.D.; Moor, B.D. A QR-type reduction for computing the SVD of a general matrix product/quotient. *Numer. Math.* **2003**, *101*, 121–140. [CrossRef]
31. De Moor, B.L.R.; Golub, G.H. The restricted singular value decomposition: Properties and applications. *SIAM J. Matrix Anal. Appl.* **1991**, *12*, 401–425. [CrossRef]
32. De Lathauwer, L. Decompositions of a higher-order tensor in block terms—Part I: Lemmas for partitioned matrices. *SIAM J. Matrix Anal. Appl.* **2008**, *30*, 1022–1032. [CrossRef]
33. De Lathauwer, L. Decompositions of a higher-order tensor in block terms—Part II: Definitions and uniqueness. *SIAM J. Matrix Anal. Appl.* **2008**, *30*, 1033–1066. [CrossRef]
34. Pan, J.; Ng, M.K. Separable quaternion matrix factorization for polarization images. *SIAM J. Imaging Sci.* **2023**, *16*, 1281–1307. [CrossRef]
35. Pan, J.; Ng, M.K. Block-diagonalization of quaternion circulant matrices with applications. *SIAM J. Matrix Anal. Appl.* **2024**, *45*, 1429–1454. [CrossRef]
36. Mallat, S. *A Wavelet Tour of Signal Processing: The Sparse Way*, 3rd ed.; Academic Press: Cambridge, MA, USA, 2009.
37. Qi, L.; Luo, Z.; Wang, Q.W.; Zhang, X. Quaternion matrix optimization: Motivation and analysis. *J. Optim. Theory Appl.* **2022**, *193*, 621–648. [CrossRef]
38. Luo, H.; Liu, X.; Liu, W.; Zhang, Y. Low-rank reduced biquaternion tensor ring decomposition and tensor completion. *Appl. Math. Comput.* **2025**, *504*, 129504. [CrossRef]


**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.