

Robust Perceptual Color Image Hashing Using Quaternion Singular Value Decomposition

Lahouari Ghouti

Department of Information and Computer Science.

King Fahd University of Petroleum and Minerals.

Dhahran 31261. Saudi Arabia. Email: lahouari@kfupm.edu.sa.

Abstract—Perceptual hashing provides compact and efficient representations for image retrieval, authentication and tamper detection applications. However, most of existing perceptual hashing algorithms are designed for gray-level images and, therefore, color correlation and interaction are simply ignored. In this paper, we propose a novel perceptual hashing for color images using the quaternion singular value decomposition (Q-SVD). In this algorithm, color images are processed through randomized dimensionality reduction which results in secure and robust hashing codes. The motivation behind our work is twofold: 1) a compact representation of color images where the red, green and blue (RGB) components are handled as a single entity using hypercomplex representations and 2) the ability of Q-SVD decomposition to provide the best low-rank approximation of quaternion matrices in the sense of Frobenius norm. Possible geometric attacks are properly modeled as an independent and identically-distributed hypercomplex noise on the singular vectors. Such modeling simplifies the hash code detector design. Finally, the hashing robustness against geometric attacks is evaluated over a large set of standard test images using the receiver operating characteristics analysis. The proposed scheme outperforms SVD-based hashing algorithms in terms of lower miss and false alarm probabilities by orders of magnitude.

I. INTRODUCTION

Indexing, categorization and retrieval of multimedia content, especially images, are challenging problems that are constantly addressed in the literature [1]. Initially, image retrieval was concerned with assigning textual annotations to images for retrieval purposes. This approach is tedious and mostly subjective. Content-based image retrieval (CBIR) overcomes these limitations by extracting specific features from query images (such as color and shape). CBIR systems can, therefore, help massively improving image indexing and retrieval. Such performance improvement led naturally to many applications including medical imaging databases, crime and forensic detection and multimedia libraries [2]. Moreover, image hashing (non-perceptual and perceptual) concepts were adopted in CBIR systems. A traditional hash function, commonly known as a *cryptographic hash*, takes an arbitrary-size input string of data and produces a fixed-size string, known as the *hash value*. These hash functions, such as the SHA-1 and MD5 algorithms, have two important features [3]: 1) they are one-way functions, i.e., the input string cannot be deduced from the output string in a finite time; 2) any change in the input string, no matter how insignificant, will potentially result in a hash value significantly different from the original one [3].

Consequently, two images, with slightly different pixel values, will have very different hash values although perceived identical by a human observer. Cryptographic hashing, therefore, is not suited for representing images that will undergo several accidental and intentional alterations. On the other hand, perceptual hashes seem more appropriate for robust compact representations by assigning *identical* hash values to two different, but perceptually similar, images. This paper proposes a novel color image perceptual hashing algorithm using the Q-SVD algorithm that can withstand several unintentional and intentional image manipulations. The generation of the perceptual hash code is governed by a low-rank color image approximation using robust summarizations based on left and right quaternion singular vectors. The paper is subdivided into the following sections: Section II summarizes current perceptual hashing algorithms for gray and color images. A review of hypercomplex numbers and Quaternion algebra is given in Section III. The following section provides a detailed account of the proposed scheme. The performance and robustness analysis of this scheme against benchmark attacks follow in Section V. Finally, in Section VI we draw conclusions and propose some guidelines for future work with respect to the design of optimal detectors under quaternion noise assumptions.

II. RELATED WORK

Several approaches are available for the design of perceptual hashing algorithms. In their pioneering work, Monga and Evans [4] proposed to extract robust feature points to efficiently represent the images through hash values. Later, Monga et al. [5] described a perceptual image hashing that consists of feature extraction and clustering steps. The feature extraction step produces what is referred to as an *“intermediate”* hash by selecting a set of visually prominent features. A block-based hashing algorithm is suggested by Kozat et al. [6]. In this algorithm, fixed-size overlapping blocks are pseudo-randomly selected. Then, these blocks are processed using the SVD decomposition to generate feature vectors. Using non-negative matrix factorization (NMF), Monga and Mihçak [7] developed a robust hashing technique. In this technique, the generated hash codes withstand rotation attacks but exhibit high fragility to embedded watermarks. Two different hashing algorithms are attributed to [8], [9]. The first algorithm is based on a novel lexico-graphical framework to generate perceptual hash codes

using the NMF tool in association with the discrete cosine transform (DCT) [8]. Image hash codes are generated using structural features in their second algorithm [9]. Moreover, image tampering is detected using a new similarity metric described in [9]. With respect to robustness, both hashing algorithms are vulnerable to rotation attacks. Despite their robustness and discriminative capabilities, most of the above algorithms are *specifically* designed for gray-level images. Extending these algorithms to color images by extracting hash codes from their luminance components or merging hashes from different components does not fully exploit the discriminative power of color information. However, few color-based image hashing algorithms are reported in the literature. For instance, a color hashing technique is attributed to Tang et al. [10]. This algorithm, strongly resilient to rotation attacks, extracts invariant moments from color components in the YCbCr and HSI color spaces after color conversion from the RGB space. Another color-based scheme is suggested by Tang et al. [11] where the histogram of color vector angles forms the basis for the generation of hash codes. In [12], a color-based technique is attributed to Tang et al. where the input image is first scaled to a fixed size prior to color conversion to YCbCr and HSI spaces. Then, local features, consisting of mean and variance, are extracted from each block in both color representations. Finally, Laradji et al. [13] proposed a block-based perceptual hashing scheme for color images using quaternion fast Fourier transform (Q-FFT) representations. Zero-crossings of the difference vectors of the mean Q-FFT energies of the image blocks represent the generated perceptual hash codes. It is noteworthy that three different implementations are possible for this scheme depending on the Q-FFT type [14].

III. HYPERCOMPLEX NUMBERS AND CLIFFORD ALGEBRA

A. Hypercomplex Numbers

Hypercomplex (quaternion) numbers consist of a real and three imaginary numbers (i , j , and k). Moreover, a four-dimensional vector, \mathbf{z} , can be used to define a quaternion number:

$$\mathbf{z} = a + b \cdot i + c \cdot j + d \cdot k \quad (1)$$

where a , b , c , and d are real numbers. Using a 4-tuple or 2-tuple notation, Eq. 1 is written as:

$$\mathbf{z} = (a, b, c, d) = (a, \vec{\mathbf{z}}) \quad (2)$$

where $\vec{\mathbf{z}} = (b, c, d)$. In Eq. 2, a and $\vec{\mathbf{z}}$ represent the scalar and vector parts of \mathbf{z} , respectively. The quaternion conjugate of \mathbf{z} , \mathbf{z}^* , is defined as:

$$\mathbf{z}^* = (a, -\vec{\mathbf{z}}) = a - b \cdot i - c \cdot j - d \cdot k \quad (3)$$

Hamilton rule for quaternions is defined as follows:

$$\begin{aligned} i^2 = j^2 = k^2 = -1 \\ ij = -ji = k, jk = -kj = i, ki = ik = j \end{aligned} \quad (4)$$

It is obvious that the multiplication of quaternions is not commutative. This property sets any quaternion-based solution apart from its real and complex-based counterparts.

B. Quaternion Algebra

Quaternions represent extensions of the 2D complex domain space to the 3D and 4D spaces leading to one of the four existing division algebra (real \mathbb{R} , complex \mathbb{C} , quaternions \mathbb{H} and octonions \mathbb{O}). It is obvious that the non-commutativity property leads to two types of vector spaces over \mathbb{H} (left and right). In order to study data with values in \mathbb{H} , some details on the definition of Hilbert spaces over the quaternion field are given below.

1) *Hilbert Space in the Quaternion Domain*: Following the presentation of [15], only right vector spaces over \mathbb{H} are considered in this paper¹. \mathbb{H}^N defines an N -dimensional vector space over \mathbb{H} . Unlike scalars, matrices operate on the opposite side of \mathbb{H}^N . Using classical matrix calculus rules, it is possible to let matrices operate on the left side and scalars operate on the right side as suggested in [15].

Definition 1: A N -dimensional vector space, namely \mathbb{H}^N , over the field of quaternions \mathbb{H} is a right vector space if [15]:

$$\forall \nu \in \mathbb{H}^N \text{ and } \forall \zeta, \mu \in \mathbb{H}: (\nu \zeta) \mu = \nu (\zeta \mu) \quad (5)$$

Eq. 5 is not equivalent to the property that holds in the case of left vector spaces over \mathbb{H} . The latter property is given by: $\mu (\lambda \nu) = (\mu \lambda) \nu$. It is very important to preserve the order of factors in matrix manipulation (multiplication mainly) in right vector spaces as adopted in this paper.

2) *Quaternion Vectors*: N quaternionic numbers, $x_l, l = 1, 2, \dots, N$, can be represented (for processing purposes) by an N -dimensional quaternion vector in \mathbb{H} . Then, the quaternion vector, \mathbf{x} , is defined as $\mathbf{x} = [x_1, x_2, \dots, x_N]^T \in \mathbb{H}^N$. Over this vector space, the scalar product between two quaternion vectors, $\mathbf{x}_1 = [x_1^{(1)}, x_2^{(1)}, \dots, x_N^{(1)}]^T$, $\mathbf{x}_2 = [x_1^{(2)}, x_2^{(2)}, \dots, x_N^{(2)}]^T \in \mathbb{H}^N$, is given below:

$$\langle \mathbf{x}_1, \mathbf{x}_2 \rangle = \mathbf{x}_1^\Delta \mathbf{x}_2 = \sum_{l=1}^N \bar{x}_l^{(1)} x_l^{(2)} \quad (6)$$

where Δ and $\bar{\cdot}$ represent the vector quaternion transposition-conjugate and scalar quaternion conjugate operators, respectively. Similarly to the norm of complex-valued vectors, the norm of quaternion vectors is defined by:

$$\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} \quad (7)$$

To compare quaternion vectors, \mathbf{x}_1 and \mathbf{x}_2 , a distance metric is defined as follows:

$$DM(\mathbf{x}_1, \mathbf{x}_2) = \|\mathbf{x}_1 - \mathbf{x}_2\| = \sqrt{(\mathbf{x}_1 - \mathbf{x}_2)^\Delta (\mathbf{x}_1 - \mathbf{x}_2)} \quad (8)$$

3) *Quaternion Matrices*: Quaternion matrices have been the focus of an active research since 1936 [16]. Zhang [17] provides an extensive investigation of quaternion matrices and their underlying algebra which is considered as an extension of classical matrix algebra concepts to the quaternion field.

¹Right vector spaces over \mathbb{H} represent a division algebra.

Quaternion algebra is the foundation behind the Q-SVD representation of a quaternion matrix. In the proposed hashing algorithm, Q-SVD, is applied on pseudo-randomly selected overlapping blocks of a color image to generate singular vectors. An image, \mathbf{I} , consists of a set of N quaternion vectors, $\mathbf{x}^{(i)} \in \mathbb{H}^M$, as follows:

$$\mathbf{I} = \begin{bmatrix} (\mathbf{x}^{(1)})^T \\ (\mathbf{x}^{(2)})^T \\ \dots \\ (\mathbf{x}^{(M)})^T \end{bmatrix} \quad (9)$$

Therefore, the image, \mathbf{I} , defines a vector space in $\mathbb{H}^{N \times M}$.

4) Quaternion Singular Value Decomposition (Q-SVD):

The importance of Q-SVD in domains related to one- and multi-dimensional signal processing applications has been first recognized by Le Bihan and Sangwine [15]. According to Zhang [17], any image, $\mathbf{I} \in \mathbb{H}^{N \times M}$, of rank r , can be decomposed into:

$$\mathbf{I} = \mathbf{U} \begin{pmatrix} \Sigma_r & 0 \\ 0 & 0 \end{pmatrix} \mathbf{V}^\Delta \quad (10)$$

where $\mathbf{U} \in \mathbb{H}^{N \times N}$ and $\mathbf{V} \in \mathbb{H}^{M \times M}$ are quaternion unitary matrices containing the left and right singular vectors of \mathbf{I} , respectively. Σ is a real diagonal matrix whose non-zero entries are r singular values of \mathbf{I} . Various algorithms are proposed for the numerical computation of the Q-SVD decomposition [18], [19].

IV. PROPOSED COLOR IMAGE PERCEPTUAL HASHING

In the proposed perceptual hashing algorithm, the input color image, of size $M \times N$, is first resized to 256×256 prior to encoding using quaternions where the color components are combined into a single hypercomplex number. Afterwards, the input image, viewed as a quaternion matrix, is decomposed using the Q-SVD algorithm block-wise using the following double Q-SVD hashing algorithm²:

- 1) Given a color image, p $m \times m$ blocks, \mathbf{A}_i , are pseudo-randomly selected using a secret selection key \mathbf{K} :

$$\mathbf{A}_i \in \mathbb{H}^{m \times m}, \quad i = 1, 2, \dots, p$$

- 2) Decompose each block, \mathbf{A}_i , using the Q-SVD algorithm as follows:

$$\mathbf{A}_i = \mathbf{U}_i \Sigma_i \mathbf{V}_i^\Delta, \quad i = 1, 2, \dots, p$$

where \mathbf{U}_i and \mathbf{V}_i are the left and right singular vectors of \mathbf{A}_i and Σ_i is the real diagonal matrix consisting of the singular values.

- 3) Select the left and right singular vectors associated with the largest r_1 singular values in each image block \mathbf{A}_i .
- 4) Form a feature vector for each block, \mathbf{A}_i , using the selected left and right singular vectors according to:

$$\gamma_i = \{\mathbf{u}_1^i, \mathbf{u}_2^i, \dots, \mathbf{u}_{r_1}^i, \mathbf{v}_1^i, \mathbf{v}_2^i, \dots, \mathbf{v}_{r_1}^i\}$$

²The selection of Q-SVD for low-rank approximation is motivated by the fact that the rank- α truncation of the Q-SVD of a matrix, \mathbf{I} , is the best rank- α approximation of matrix \mathbf{I} in the mean square sense [15].



Fig. 1. Original Lena image (a). JPEG-compressed with $QF = 20$ (b). JPEG-compressed with $QF = 10$ (c). JPEG-compressed with $QF = 5$ (d).

- 5) Pseudo-randomly select vectors from the set, $\Gamma = \{\gamma_1, \gamma_2, \dots, \gamma_p\}$, to form a smooth image $\mathbf{J} \in \mathbb{H}^{m \times 2pr_1}$. Smoothing is achieved by selecting and replacing subsequent vectors from Γ that are close according to a norm sense³.

- 6) Using the smooth image, \mathbf{J} , q image blocks, \mathbf{B}_i , are pseudo-randomly selected using \mathbf{K} :

$$\mathbf{B}_i \in \mathbb{H}^{m \times m}, \quad i = 1, 2, \dots, q$$

- 7) Decompose each block, \mathbf{B}_i , using the Q-SVD algorithm as in step 2 above.
- 8) Select the left and right singular vectors associated with the largest r_2 singular values in each image block \mathbf{B}_i .
- 9) Form a feature vector for each block, \mathbf{B}_i , using the selected left and right singular vectors according to:

$$f_i = \{\mathbf{u}_{b1}^i, \mathbf{u}_{b2}^i, \dots, \mathbf{u}_{br_2}^i, \mathbf{v}_{b1}^i, \mathbf{v}_{b2}^i, \dots, \mathbf{v}_{br_2}^i\}$$

- 10) The perceptual hash code is generated according to:

$$h = \{f_1, f_2, \dots, f_q\}$$

To motivate for using Q-SVD in robust perceptual hashing, we first illustrate the robustness of the image features, extracted using Q-SVD decomposition, in the presence of malicious image attacks such as JPEG compression. Fig. 1 shows the original 512×512 Lena image and its JPEG-compressed versions using various quality factors (QF). Using 25 Q-SVD vectors, the images, shown in Fig. 1, are reconstructed using SVD and Q-SVD algorithms, respectively. Fig. 2 provides a plot of the L_2 -norm of the difference between the corresponding left singular vectors produced using SVD (Fig. 2-left) and Q-SVD (Fig. 2-right). Unlike the SVD decomposition, Q-SVD yields more robust singular vectors that can withstand compression noise and discriminate between samples pertaining to distinct images.

V. EXPERIMENTAL RESULTS

A database consisting of 6000 standard test images is used to assess the performance of the QSVD-based hashing algorithm. Four different attacks are applied on four different database subsets where each subset contains 100 distinct and pseudo-randomly selected images from the main database. These attacks, defined in [7], are: (i) rotation by 15° ; 15% cropping, resizing, and JPEG compression with $QF = 10$; (ii) randomized affine warping using Stirmark benchmarking tool [20]; (iii) gamma correction (i.e., nonlinear intensity

³Therefore, all elements of Γ are pseudo-randomly reordered after $2p$ iterations.

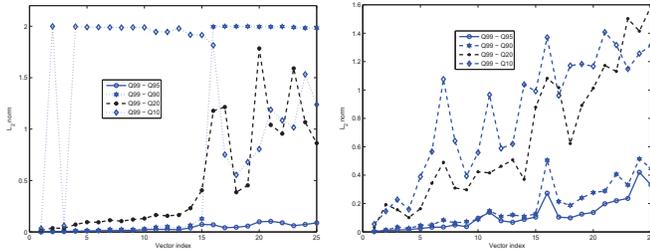


Fig. 2. L_2 norm of the difference between SVD (left) and Q-SVD vectors (right).



Fig. 3. Original (left) and attacked image (right) using attack (iii).

adjustment) and JPEG compression with $QF = 5$; and (iv) attack (i) combined with shearing by five pixels. Fig. 3 shows original and manipulated samples using attack (iii). Using the four subsets, Q-SVD and SVD-based perceptual hashes were generated using the following parameters [7]: 25 randomly-selected 100×100 blocks are decomposed and only the first left and right singular vectors were extracted from the secondary image, \mathbf{J} , to generate 150-length hash vectors. It should be noted that the SVD-based algorithm, defined in [6], is used for comparison purposes where two approaches are adopted to represent color images. In the first one, the average of the three color hash vectors is considered yielding a 150-length hash code for each image. These vectors are concatenated into a single 450-length hash vector in the second approach. Genuine and impostor distributions of the L_2 -norm differences between the hash vectors pertaining to similar and different images under attack (i) are shown in Fig. 3 for SVD- (left) and QSVD-based (right) hashing algorithms, respectively. The good distribution separation of the QSVD-based scheme confirms the fact that the inherent use of color information by Q-SVD enables significant performance improvement in terms of lower misclassification rates. Similar rates are achieved under attack (iii) as reported in Fig. 5. Finally, Fig. 6 shows the receiver operating characteristic (ROC) curves corresponding to attack (ii). In this case, the ROC curves were obtained by generating hash vectors for 100 images in subset 2 corresponding to attack (ii) using different values for \mathbf{K} . Once again, the QSVD-based technique achieves both miss and false alarm probabilities that are orders of magnitude lower than those yielded by the SVD-based algorithm. More specifically, setting the detection threshold to 0.02, enables our algorithm not making a single misclassification error (miss or false alarm) as clearly indicated in Fig. 6.

VI. CONCLUSIONS

In this paper, we have presented a robust perceptual hashing algorithm for color images based on the quaternion singular

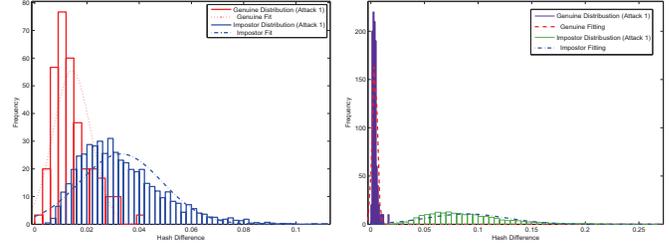


Fig. 4. Genuine and impostor distributions for attack (i) using SVD-based (left) and QSVD-based hashing algorithms (right).

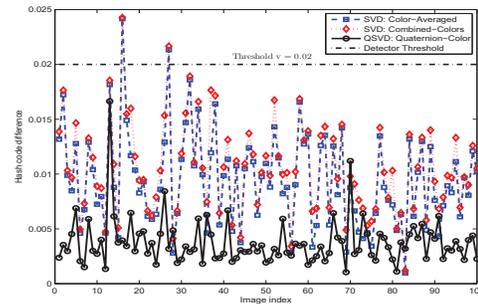


Fig. 5. L_2 norm of differences between generated hash vectors under attack (iii).

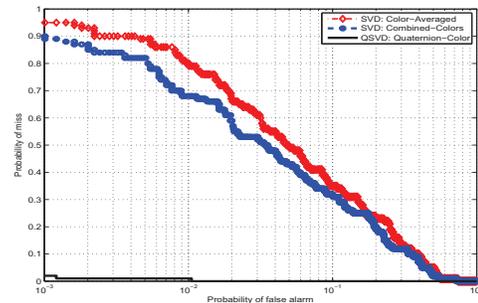


Fig. 6. ROC curves for attack (ii) using SVD- and QSVD-based hashing algorithms.

value decomposition (Q-SVD). Unlike existing color-based schemes, the proposed scheme treats the image color components in a holistic manner and, therefore, takes full advantage of the intrinsic color correlation/interaction between the image components. In addition, Q-SVD provides the best low-rank approximation of color images that can be efficiently used to generate robust hash codes consisting of Q-SVD singular vectors. In particular, the proposed hashing algorithm yields the lowest misclassification rate compared to SVD-based hashing scheme, while enjoying improved security and robustness to intentional standard attacks. Future work includes the design of optimal detectors under the assumption of proper quaternion noise which can be astutely used to derive optimal detection thresholds for the proposed hashing algorithm.

ACKNOWLEDGMENT

The author would like to thank King Fahd University of Petroleum and Minerals for supporting this work.

REFERENCES

- [1] A. K. Jain and A. Vailaya, "Image retrieval using color and shape," *Pattern Recognition*, vol. 29, no. 8, pp. 1233-1244, Aug. 1996.
- [2] [2] A. B. Gonde, R. P. Maheshwari, and R. Balasubramanian, "Modified curvelet transform with vocabulary tree for content based image retrieval," *Digital Signal Processing*, vol. 23, no. 1, pp. 142-150, Jan. 2013.
- [3] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, 2010.
- [4] V. Monga and B. L. Evans, "Perceptual hashing via image feature points: Performance evaluation and trade-offs," *IEEE Trans. Image Processing*, vol. 15, no. 11, pp. 3452-3465, Nov. 2006.
- [5] V. Monga, A. Banerjee and B. L. Evans, "A Clustering based approach to perceptual image hashing," *IEEE Trans. Infor. Forensics and Security*, vol. 1, no. 1, pp. 68-79, Mar. 2006.
- [6] S. S. Kozat, M. K. Mihçak and R. Venkatesan, "Robust perceptual image hashing via matrix invariants," in *IEEE Conf. on Image Processing*, vol. 5, pp. 3443-3446, Oct. 2004.
- [7] V. Monga and M. K. Mihçak, "Robust and secure image hashing via non-negative matrix approximations," *IEEE Trans. Infor. Forensics and Security*, vol. 2, no. 3, pp. 376-390, Sep. 2007.
- [8] Z. Tang, S. Wang, X. Zhang, W. Wei and Y. Zhao, "Lexicographical framework for image hashing with implementation based on DCT and NMF," *Multimedia Tools and Applications*, vol. 52, no. 23, pp. 325-345, 2011.
- [9] Z. Tang, S. Wang, X. Zhang and W. Wei, "Structural feature-based image hashing and similarity metric for tampering detection," *Fundamenta Informaticae*, vol. 106, no. 1, pp. 75-91, 2011.
- [10] Z. Tang, X. Dai and X. Zhang, "Perceptual hashing for color images using invariant moments," *Applied Mathematics & Information Sciences*, vol. 6, no. 2S, pp. 643-650, 2012.
- [11] Z. Tang, X. Dai, X. Zhang and S. Zhang, "Perceptual image hashing with histogram of color vector angles," in *the 8th International Conference on Active Media Technology (AMT' 2012)*, Lecture Notes in Computer Science, vol. 7669, pp. 237-246, 2012.
- [12] Z. Tang, X. Zhang, X. Dai and T. Wu, "Robust image hash function using local color features," *Int. J. Electron. Comm.*, vol. 67, pp. 717-722, 2013.
- [13] I. H. Laradji, L. Ghouti and E-H Khiari, "Perceptual hashing of color images using hypercomplex representations," in *IEEE Conf. on Image Processing*, vol. 4, pp. 4402-4406, Sep. 2013.
- [14] E. Todd and S. J. Sangwine, "Hypercomplex Fourier transforms of color images," *IEEE Trans. Image Processing*, vol. 16, no. 1, pp. 22-35, 2007.
- [15] N. Le Bihan and J. Mars, "Singular value decomposition of quaternion matrices: A New tool for vector-sensor signal processing," *Signal Processing*, vol. 84, pp. 1177-1199, 2004.
- [16] L. A. Wolf, "Similarity of matrices in which elements are real quaternions," *Bull. Amer. Math. Soc.*, vol. 42, pp. 737-743, 1936.
- [17] F. Zhang, "Quaternions and matrices of quaternions," *Linear Algebra Applications*, vol. 21, pp. 21-57, 1987.
- [18] S. J. Sangwine and N. Le Bihans, "Quaternion singular value decomposition based on bidiagonalization to a real matrix using quaternion Householder transformations," *Applied Mathematics and Computation*, vol. 182, no. 1, pp. 727-738, Nov. 2006.
- [19] N. Le Bihans and S. J. Sangwine, "Jacobi method for quaternion matrix singular value decomposition," *Applied Mathematics and Computation*, vol. 187, no. 2, pp. 1265-1271, Apr. 2007.
- [20] F. A. P. Petitcolas, "Watermarking schemes evaluation," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 5864, Sep. 2000.