

Digital watermarking using Hall property image decomposition method

Nazeer Muhammad¹ · Nargis Bibi² · Iqbal Qasim³ · Adnan Jahangir¹ · Zahid Mahmood⁴

Received: 11 December 2015 / Accepted: 16 March 2017 / Published online: 31 March 2017
© Springer-Verlag London 2017

Abstract Most of the existing singular value decomposition-based digital watermarking methods are not robust to geometric rotation, which change the pixels' locations without maintaining the corresponding changes to the pixel's intensity values of entire image and yield high computational cost. To answer this, we propose a digital image watermarking algorithm using the Hall property. In the proposed method, a digital watermark image is factorized into lower-triangular, upper-triangular, and permutation matrices. The permutation matrix is used as the valid key matrix for authentication of the rightful ownership of the watermark image. The product of the lower and upper triangular matrices is processed with a few iterations of the Arnold transformation to obtain the scrambled data. The scrambled data are embedded into particular sub-bands of a cover image using Wavelet transform. Our experiments show that the proposed algorithm is highly reliable and computationally efficient

compared with state-of-the-art methods that are based on singular value decomposition.

Keywords Hall property · Watermarking · Wavelet transform · Arnold transform · Image encryption

1 Introduction

Advent of the Internet and technology has made easier to spread and share multimedia information in various forms of digital documents including images, videos, and audio contents. However, this growth has given rise to problems of security and authentication of digital documents. Therefore, it is important to employ algorithms that provide sufficient security for digital documents while providing protection against various forms of forgery in an efficient manner with respect to the speed of the verification process. Ultimately, these requirements have led to the development of efficient digital watermarking techniques that guarantee ownership and maintain the integrity of digital documents at a low computational cost.

Digital watermarking refers to the process of embedding a watermark into a digital document to prevent illegal counterfeiting [1]. The embedded watermark may be extracted from a watermarked document to authenticate its copyright status as per need. Robust security is a key objective of digital watermarking, as it ensures that a watermark cannot be fragile by unintentional attacks and affords sufficient protection for copyright enforcement. To overcome piracy of digital documents and support claims of rightful ownership, a number of watermarking techniques have been developed by many authors. The majority of existing watermarking schemes concentrate on robustness, which aims to achieve a high imperceptibility of the

✉ Zahid Mahmood
zahid0987@ciit.net.pk

Nazeer Muhammad
nazeermuhammad@ciitwah.edu.pk

Nargis Bibi
nargis@fjwu.edu.pk

¹ Department of Mathematics, COMSATS Institute of Information Technology, Wah Cantt, Pakistan
² Department of Computer Science, Fatima Jinnah Women University, Rawalpindi, Pakistan
³ Department of Computer Science, University of Science and Technology Bannu, Bannu 28100, KPK, Pakistan
⁴ Department of Electrical Engineering, COMSATS Institute of Information Technology, Abbottabad, Pakistan

watermarked image rather than focusing on issues of noteworthiness [1]. Among existing watermarking schemes, it is important to mention the method proposed by Craver et al. [2], which provided a noninvertible scheme that was further improved by Cox et al. [3]. In addition, Craver et al. simulated cases of existing watermarking techniques with different attacking strategies by providing counterfeit watermarking techniques that could be executed on a watermarked image. These techniques employ numerous claims of ownership in an attempt to discredit the authority of the watermark image by embedding one or more additional watermark images, such that it becomes uncertain which one is the genuine authoritative watermark. However, the noninvertibility of their scheme is based on an invalid assumption [1]. As a result, other transform representations have been investigated for watermarking based on singular value decomposition (SVD) methods [4] that are considered to be robust against a variety of image processing attacks and improved the level of imperceptibility for human visual systems. In [5], the DWT-SVD-based approach, the watermark is embedded into lowest frequencies and high frequencies sub-bands. Unfortunately, as recounted in the contemporary literature by Zhang et al. [6], Xiao et al. [7] showed that SVD-based watermarking algorithms exhibit a high-level probability of false positive detections. They demonstrated the intrinsic reasons of the high false-alarm probability are as follows: the basis space of singular value decomposition is image content dependent, and there is no one-to-one correspondence between singular value vector and image content, because singular value vectors have no information on the structure of image.

Ganic et al. [8] proposed a watermarking technique based on a hybrid DWT-SVD domain. They focused on the human visual system properties of watermarked images. In their work, they decomposed the cover image into four sub-bands and imposed the SVD on each sub-band. In doing so, they embedded singular values of the watermark into the respective sub-bands of the cover image, and thus, the embedding strength was determined by a human visual model. In another scheme, Chandra et al. [9] suggested embedding singular values of a watermark image to singular values of the entire cover image. Similar approaches and techniques involve embedding the watermark image, which can be a pseudorandom sequence [10], a binary image sequence (technique 2 in [11]), or a gray-scale image, directly into the largest singular values or by quantizing the largest singular values of each block of the cover image. As identified in [11] and [12], these techniques are subject to the false positive problem, which refers to the invalid detection of a watermark image in an image that does not in fact hold a watermark [13]. However, the ambiguous situation of a false positive may also

occur when a specific watermark image is detected from content in which a different watermark image was embedded. This fact creates an ambiguity and does not allow one to resolve the issue of rightful ownership [14]. Muhammad et al. [15] tried to resolve a false positive issue using weightage-based differential evolution algorithm which is used to achieve the possible scaling factor for getting the maximum possible robustness, but found computationally expensive one compared to our proposed method.

Chang et al. [16] proposed a technique based on singular vectors to embed bits of a watermark image into the left or right singular vectors of a corresponding cover image, with the cover image and watermark consisting of a gray-scale image and binary image, respectively. In this method, embedding strategy is modified to provide the extra information for later restoration with the usage of least important nonzero coefficients. While this algorithm is robust with respect to common attacks, it cannot be used to perform an exact watermark extraction [17], which is triggered by the values of the left matrix that belong to the interval $[-1, 1]$. An additional flaw of this algorithm is related to the selection of higher rank blocks. Specifically, it has been demonstrated that rank is not a reliable parameter [19]. Mohan et al. [18] proposed a watermarking technique based on hybrid block adjustments, where the cover image is divided into four blocks and the watermark image is embedded in two bins: firstly in the largest singular values of the upper-left block by means of quantization, and secondly in the bottom right, using the technique proposed by Chung et al. [19]. To enhance the security of this technique, the watermark image is permuted prior to the embedding process. Moreover, a quantization table with the largest singular value of each block of the cover image is used in the extraction process. While this algorithm is robust against geometric and common attacks, altering only the upper-left and bottom-right blocks of the cover image with the watermarked image may result in artifacts at the blocks' borders, resulting in strong differences in luminance between the upper-left corner and upper-right or bottom-left corners of the watermarked image. On applying SVD decomposition to image $I : [U, S, V] = \text{svd}(I)$, the magnitude of the singular values S of I will increase the luminance of an image, while lowering the magnitude will decrease the luminance of an image, respectively. Therefore, it is appropriate to state that I is in close relation with the image luminance, while the intrinsic "geometry" of the image depends upon orthogonal matrices; the vertical V and horizontal U details of an image I [20].

It is important to note that none of the above-mentioned watermarking techniques, which are based on singular vectors, are capable of preserving the orthogonal properties

of the left or right singular vectors of corresponding matrices, since the transformation used to embed the watermark image is nonlinear [20]. In this method, the spatial domain watermarking algorithm based on SVD with combination of differential evolution is used to obtain the optimal scaling factors for watermark embedding. Indeed, it is exceedingly difficult to embed a watermark image into the singular vectors of a cover image while preserving orthogonality, because it is simultaneously required for performing the orthogonal transformation of the watermark image embedding and preserving the quality of the watermarked image.

Fahmy et al. [21] proposed watermarking scheme that uses natural preserves transform (NPT) to encode a gray-scale watermarking logo image or text, into a host image at any location. NPT brings a unique feature which is uniformly distributing the logo across the host image in an imperceptible manner. The contribution of this paper lies in presenting two efficient nonblind and quasiblind watermark extraction techniques. In the quasiblind case, the extraction algorithm requires little information about the original image that is already conveyed by the watermarked image. In Lai et al. [22] method one column entries of SVD decomposed component could be preserved, while for other columns, the entries were changed when general image processing was performed. In Hu et al. [23], the decomposition of cover image had been performed using the discrete Fourier transform (DCT) and the middle-band DCT coefficients are chosen to obtain the good imperceptibility of watermarked image.

Ali et al. [24] used self-adaptive differential evolution (SDE) algorithm which is presented. SDE adjusts the mutation factor and the crossover rate dynamically in order to balance an individual’s exploration and exploitation capability for different evolving phases. Agarwal et al. [25] show that dividing an image into block gives more space to embed multiple watermarks which in turn gives a more secure watermarking technique. In the proposed approach, the host color image is divided into *R*, *G*, *B* channels. Each channel is further divided into four blocks, and then four watermark images are embedded in each of these channels. Muhammad et al. [26], using the Fresnelet transform with a family of wavelet transforms, make the scheme more

efficient in terms of extracted accuracy of hidden information. An improved SVD-based image watermarking method was considered using human visual characteristics. Xing et al. [27] method is based on SVD, where important information of the reference data is used to retrieve the hidden watermark, which will cause the false extraction. Tao et al. [28] reviews the theoretical analysis and performance investigation of representative watermarking systems in transform domains and geometric invariant regions.

The SVD-based method has been demonstrated to be noneffective and prone to a high probability of false detections of watermarks by many authors as described above and also in [21–28], among others. Moreover, the majorities of the aforementioned techniques exhibit a high computational cost and have a much smaller embedding capacity of watermark data compared with the size of the cover data.

We propose a novel method that is highly robust and achieves a large embedding capacity and improved security for image-based documents. The proposed method is focused on the digital image watermarking issues that have arisen from ownership claims and reducing computational cost. The algorithm is based upon partial pivoting lower and upper triangular (PPLU) decomposition, which is an algebraic method used in many applications, such as real-time signal processing where fast computation is required [29, 30]. In addition, a small number of iterations of the Arnold transform are used to uniformly distribute the scrambled data energy to attain a high imperceptible level of watermark data [31]. The integration of the PPLU algorithm with the Arnold transform (AT) in the wavelet domain makes promising in the improvement of pixel watermarking to content watermarking. Content-based watermarking has been used to effectively lessen the contradictions between perceptibility and robustness of conventional watermarking algorithms [32]. To authenticate the ownership of host data, the extraction process can be used to decrypt the scrambled watermark data with the inverse AT using the genuine key in the form of a permutation matrix.

The remainder of the paper is organized as follows: Sect. 2 discusses singular value decomposition-based

Table 1 Notations and their meanings

Notation	Description	Notation	Description
AT	Arnold transform	WT	Wavelet transform
CC	Coefficient correlation	PSNR	Peak signal-to-noise ratio
PPLU	Partial pivoting lower and upper triangular	RS	Rescaling
SVD	Singular value decomposition	BL	Blurring
HS	Histogram	GM	Gamma correction
NS	Noise	JP	JPEG compression

watermarking scheme. Section 3 explains the watermarking based on the partial pivoting lower and upper triangular (PPLU) decomposition. Detailed simulation results and evaluations are discussed in Sect. 4. Finally, conclusions and future research directions are listed in Sect. 5. For ease of understanding, Table 1 lists few notations and their meanings that are frequently used in the paper.

2 The SVD-based watermarking

This section illustrates the SVD-based watermarking technique. For ease of understanding, *Nomenclature* guides the reader to keep pace with the reading.

Nomenclature

Notation	Description	Notation	Description
C	Cover image for hiding purpose	C_w	Watermarked image (embedded output)
W	Watermark image	\tilde{C}_w	Distorted watermarked image (for extracting out)
α	Scaling factor	S_{sw}	Singular value with watermark
V^t	Transpose of left unitary matrix	\bar{S}_w	Reconstructed singular values in extraction stage
U	Right unitary matrix	\tilde{W}	Extracted watermark data matrix

Let C and W be matrices representing the cover image and watermark image, respectively. The SVD is applied to a cover image $C \in R^{N \times N}$ to embed a watermark W as follows:

$$\text{svd}(C) := USV^t, \tag{1}$$

On employing SVD decomposition on C , we obtain three matrices [U, S, and V], where $S \in R^{N \times N}$ is the diagonal matrix with eigenvalues of C , and $U, V \in R^{N \times N}$ are the corresponding unitary matrices. A watermark $W \in R^{N \times N}$ is embedded with a suitable strength factor into diagonal matrix S and produced embedded diagonal matrix with watermark W as follows

$$S_{sw} = S + \alpha W, \tag{2}$$

where $\alpha > 0$ controls the embedding strength of the watermark. From the SVD of S_{sw} :

$$\text{svd}(S_{sw}) = U_w S_w V_w^t. \tag{3}$$

The key matrices are reserved as U_w and V_w , and the diagonal matrix S_w is used along with the U and V of the C to obtain a watermarked image C_w given by:

$$C_w = US_w V^t. \tag{4}$$

In the extraction stage, a distorted watermarked image \tilde{C}_w may be obtained. A corrupted watermark W can be extracted with the help of the three matrices $U_w, S,$ and V_w by reversing the embedding process as follows:

$$\text{svd}(\tilde{C}_w) = \tilde{U} \tilde{S}_w \tilde{V}^t, \tag{5}$$

with setting $\tilde{S}_w = U_w \tilde{S}_w V_w^t$, the watermark W is estimated by:

$$\tilde{W} = \frac{(\tilde{S}_w - S)}{\alpha}. \tag{6}$$

Since the matrices $U_w, S,$ and V_w are assumed to be known for the watermark extraction process, anyone who uses an arbitrary diagonal matrix along with known data for U_w and V_w can extract the watermark image with only the diagonal elements being different from the original watermark image. Indeed, as logically pointed out by Zhang [6], this is a major flaw of the SVD-based watermarking algorithms. From Eqs. (2) and (3) it is observed that the diagonal matrix S with real nonnegative diagonal entries $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_n \geq 0$ can be modified by false positive detection of digital watermark [38, 40].

3 Watermarking based on the PPLU decomposition and Arnold transform

This section explains watermarking that is based on the PPLU decomposition and the Arnold transform.

3.1 The PPLU decomposition

To better understand the PPLU decomposition, *Nomenclature* explains the terms used in this section.

Nomenclature

Notation	Description	Notation	Description
$a_{jk}^{(i-1)}$	Row of lower-triangular matrix	P	Permutation matrix
$a_{rk}^{(i-1)}$	Row of upper-triangular matrix	L	Lower-triangular matrix
$a_{ik}^{(i-1)}$	Updated pivot row	U	Upper-triangular matrix

The PPLU decomposition is a factoring method for the low and upper triangular matrices of a matrix associated with the partial pivoting procedure for stable row operations implementing Gauss–Jordan elimination [29, 30]. At each step of row operation, the partial pivoting procedure tries to place the largest absolute value into the pivot position prior to division to obtain a leading 1. Starting from a given $n \times n$ matrix $A^{(0)} = A$, let $A^{(i)}, 1 \leq j \leq n$, be induced from $A^{(i-1)}$ by selecting the row $a_{jk}^{(i-1)} (1 \leq k \leq n)$ from the rows $a_{rk}^{(i-1)} (1 \leq k \leq n), i \leq r \leq n$, such that for $i \leq j \leq n$,

$$|a_{ji}^{(i-1)}| = \max_{r=i}^n |a_{ri}^{(i-1)}|, \tag{7}$$

which is followed by exchanging rows with $a_{ik}^{(i-1)} (1 \leq k \leq n)$ and $a_{jk}^{(i-1)} (1 \leq k \leq n)$. According to the partial pivoting process described above, we can define the PPLU decomposition as follows:

$$PA = LU. \tag{8}$$

This procedure provides three matrices of the given matrix A , namely a lower-triangular matrix L , an upper-triangular matrix U , and permutation matrix P , where L is the product of a sequence of elementary matrices induced from the partial pivoting process, U is a reduced echelon form of A , and P is induced from the row exchanges performed during the partial pivoting process.

3.1.1 Proposition

The following propositions are observed regarding the use of the PPLU decomposition for digital watermarking process:

- a. For general coefficient matrices, Gaussian elimination *PPLU* decomposition without pivoting is numerically unstable.
- b. The pivot element in stage k is the largest element a_{rk} in a column k . Everything revolves around it. It is farthest from 0, and division by a_{rk} is most stable. The pivot row r is thus determined by expression:

$$|a_{rk}| = \max(|a_{ik}| : k \leq i \leq n) \tag{9}$$

where r is the argument (or index) of the maximum.

- c. Full pivoting would take the largest pivot from the whole sub-matrix $A(k : n - 1, k : n - 1)$. This gives the best stability, but is more costly. In practice, partial pivoting suffices.
- d. Partial pivoting is considerably more efficient than complete pivoting; it compares $\frac{1}{2}n^2 + O(n)$ pairs of potential pivots, while complete pivoting compares $\frac{1}{3}n^3 + O(n^2)$ pairs [29].

- e. Partial pivoting is crucial to prevent breakdown and to improve the accuracy. Partial pivoting chooses largest element in a column (or row) and interchanges rows (columns). The partial pivoting for round-off reduction is shown as follows.

$$|A_{ii}| \max_{j>i} |A_{ji}|, \text{ swap row } i \text{ with } \arg \left(\max_{j>i} |A_{ij}| \right). \tag{10}$$

To illustrate further the effect of small pivots, example 3.1.2 is shown.

3.1.2 Example

Let's consider

$$A = \begin{bmatrix} \epsilon & 1 \\ 1 & 1 \end{bmatrix}, \text{ where } |\epsilon| \ll 1 \tag{11}$$

where ϵ is positive number smaller than ϵ . If rows are not interchanged, then pivot is ϵ and multiplier is $1/\epsilon$, so

$$\begin{aligned} M &= \begin{bmatrix} 1 & 0 \\ -1/\epsilon & 1 \end{bmatrix}, \quad L = \begin{bmatrix} 1 & 0 \\ 1/\epsilon & 1 \end{bmatrix} \\ U &= \begin{bmatrix} \epsilon & 1 \\ 0 & 1 - 1/\epsilon \end{bmatrix} = \begin{bmatrix} \epsilon & 1 \\ 1 & -1/\epsilon \end{bmatrix}. \end{aligned} \tag{12}$$

In floating-point arithmetic, but then

$$LU = \begin{bmatrix} 1 & 0 \\ 1/\epsilon & 1 \end{bmatrix} \begin{bmatrix} \epsilon & 1 \\ 0 & 1 - 1/\epsilon \end{bmatrix} = \begin{bmatrix} \epsilon & 1 \\ 0 & 0 \end{bmatrix} \neq A. \tag{13}$$

In above example, the pivot was a very small number with respect to other numbers. According to Gaussian elimination general approach, to divide by the pivot in terms of small numbers is dangerous against certain watermark attacks. But this issue can be eliminated by a row exchange operation of partial pivoting trick. This shows that nonzero value will do as pivot, but in practice pivot should be chosen to minimize the error propagation [33]. Row pivoting strategy that swaps the diagonal element with that of largest magnitude from those in and below the diagonal in the current column guarantees that every element in L is equal or smaller than 1 in magnitude and handles properly the growth of the elements in U , limiting the impact of the round-off errors. This situation involves a growth in the magnitude of the elements of U , with the consequent rounding errors [34].

3.2 The PPLU authentication

We discuss the problems of structure prediction for right ownership of digital watermark image. The first problem considers the nonzero structure and tight bounds of L and

U prior to the Gaussian elimination process of the matrix A the Hall property [33]. This property is the combinatorial property that shows the nonzero values in A are algebraically independent from each other. This structure is called the row merge bipartite graph. Few definitions in this regard are following.

3.2.1 Definition

Hall property [33]: A is Hall if every $n \times k$ sub-matrix ($1 \leq k \leq n$) has at least k nonzero rows with following facts:

- a. Every nonsingular matrix is a Hall matrix.
- b. The columns (or rows) of a Hall matrix may be permuted to provide the zero-free diagonal.
- c. A bipartite graph has a column-complete matching if and only if it has the Hall property.
- d. Bipartite graphs provide the path structure and tight bounds in LU factorization for L and U [33].

Matching A matching of \mathcal{M} corresponding to A is a choice of nonzero diagonal elements [33].

Paths Paths in graphs are important in many sparse matrix settings; the notion of alternating paths links matching and connectivity [33].

Bipartite graph The bipartite graph of A , which we write $H(A)$, has m “row vertices” and n “column vertices.” The column and row vertices are drawn from two unlike data of the positive integers, which we distinguish by using primes on row vertex names.

3.2.2 Lemma

A matching \mathcal{M} with m row and n column vertices of bipartite graph H has set of edges that do not incident on the same vertex [33]. Moreover, when the edges of the \mathcal{M} fit to the diagonal elements, the net permuted matrix becomes diagonally dominant. We use this effect to show the authenticity of permutation matrices of our proposed method for proving the exact structure prediction as shown in Sect. 4.

3.2.3 Theorem

Hall’s theorem [33]: A bipartite graph is satisfying the Hall property, if and only if it shows a column-complete matching.

3.2.4 Corollary

The $H(A)$ is called the Hall of the full column rank of matrix A . If H is Hall, then all matrices of A have full column rank, i.e., $H = H(A)$.

3.2.5 Lemma

From Lemma 3.2.3 and Corollary 3.2.5, a matrix A from column vertex i to column vertex j can be expressed with $H(A) = H$, such that $A_{ij} > n$ for $i', j \in \mathcal{M}$ and $0 < A_{ij} < 1$ for $i', j \notin \mathcal{M}$. A column and row (c and r) alternating paths are the path that follows the matching edges from columns to rows and rows to columns, respectively. Suppose the last vertex of one c - alternating path is the first vertex of another c - alternating path. Same result holds for r - alternating path. Suppose ϑ is an alternating path from an unmatched vertex v to a different vertex w . If the last vertex w on ϑ is unmatched, or the last edge on \mathcal{P} belongs to \mathcal{M} , then the set of edges $\hat{\mathcal{M}} = \mathcal{M} \oplus \vartheta = (\mathcal{M} \cup \vartheta) - (\mathcal{M} \cap \vartheta)$ is another matching; We say that $\hat{\mathcal{M}}$ is obtained from \mathcal{M} by alternating along path ϑ . If w is matched in \mathcal{M} , then v is matched and w is unmatched in $\hat{\mathcal{M}}$, and $|\hat{\mathcal{M}}| = |\mathcal{M}| + 1$. In the latter case we also call ϑ an augmenting path (with respect to \mathcal{M}). A classical result of matching theory is that a maximum size matching can be constructed by greedily finding augmenting paths alternating along them.

A perfect matching in the bipartite graph $H = H(A)$ of a square matrix can be thought of as a way to find a row permutation P for A so that the permuted matrix PA has nonzero diagonal. Our main purpose is to prove the dissimilarity of two permutation matrix of two different matrix A and \hat{A} .

3.2.6 Theorem

Let A and \hat{A} ($A \neq \hat{A}$) are $n \times n$ nonsingular matrices that are factored by Gaussian elimination with row swapping as $PA = LU$ and $\hat{P}\hat{A} = \hat{L}\hat{U}$. If $P = \hat{P}$, then $\hat{P}^{-1}LU = A$, but $\hat{P}^{-1}LU \neq \hat{A}$.

Proof We denote the sub-matrix $LU(i : j, d : e)$ of A formed by elements of row indices from i to j and column indices from d to e . Similarly, the sub-matrix $\hat{L}\hat{U}(\hat{i} : \hat{j}, \hat{d} : \hat{e})$ of \hat{A} formed by elements of row indices from \hat{i} to \hat{j} and column indices from \hat{d} to \hat{e} , where any two different matrices $A \neq \hat{A}$ can have the similar permutation matrices as:

$$A = \begin{bmatrix} a_{ij} & 0 \\ 0 & a_{ij} \end{bmatrix}, \hat{A} = \begin{bmatrix} \hat{a}_{ij} & 0 \\ 0 & \hat{a}_{ij} \end{bmatrix}, LU(i : j, d : e) / \hat{L}\hat{U}(\hat{i} : \hat{j}, \hat{d} : \hat{e}) \rightarrow P = \hat{P}. \tag{14}$$

Moreover, the products LU and $\hat{L}\hat{U}$ are factored by Gaussian elimination with row swapping which produces the permutation matrices as an identity matrix.

3.2.7 Theorem

Let A and \hat{A} ($A \neq \hat{A}$) are $n \times n$ nonsingular matrices that are factored by Gaussian elimination with row swapping as $PA = LU$ and $\hat{P}\hat{A} = \hat{L}\hat{U}$ with $P \neq \hat{P}$. Then the permutation matrix P_{LU} of LU and the permutation matrix $\hat{P}_{\hat{L}\hat{U}}$ of $\hat{L}\hat{U}$ are equal to identity matrices; $P_{LU} = \hat{P}_{\hat{L}\hat{U}} = I$, but the $PA \neq \hat{P}\hat{A}$.

Proof We denote the sub-matrix $LU(i : j, d : e)$ formed by elements of row indices from i to j and column indices from d to e . Similarly, the sub-matrix $\hat{L}\hat{U}(\hat{i} : \hat{j}, \hat{d} : \hat{e})$ formed by elements of row indices from \hat{i} to \hat{j} and column indices from \hat{d} to \hat{e} .

$$A \neq \hat{A}, \rightarrow LU(i : j, d : e) \neq \hat{L}\hat{U}(\hat{i} : \hat{j}, \hat{d} : \hat{e}). \tag{18}$$

Suppose the permutation matrices P and \hat{P} of $A \neq \hat{A}$ do not keep the elements in same numerical order: $P \neq \hat{P}$ as follows:

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \hat{P} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{19}$$

The product LU and $\hat{L}\hat{U}$ is factored by Gaussian elimination with row swapping that produces the permutation matrices as an identity matrices.

$$P_{LU} =: \hat{P}_{\hat{L}\hat{U}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{20}$$

On the contrary, A and \hat{A} may not be simultaneously defined, and even if $P_{LU} = \hat{P}_{\hat{L}\hat{U}} = I$, however, false permutation matrix \hat{P} do not permute the rows of A exactly like the P and shows that $PA \neq \hat{P}\hat{A}$ as follows:

$$PA = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \rightarrow \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{31} & a_{32} & a_{33} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}. \tag{21}$$

$$\hat{P}\hat{A} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \rightarrow \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}. \tag{22}$$

Theorems 3.2.11 and 3.2.12 show that no fake information can be retrieved from embedding watermark with false permutation matrix \hat{P} , because the embedding structure can be retrieved only on using the permutation matrix same as

the original permutation matrix for obtaining the true watermark. Any different and false permutation matrix spoils the extracting information which can be observed from the resultant matrices as shown in Eqs. (21) and (22).

The efficiency of the PPLU decomposition is viewed in terms of computational cost and storage of the algorithm. Since one application of the Gauss–Jordan elimination phase gives the factorization $PA = LU$, the PPLU decomposition asymptotically requires only $1/3 n^3$ long operations (multiplication and division), which is lower than for SVD decomposition [35, 37]. Moreover, from a storage point of view, the PPLU decomposition is very compact, because it can overwrite entries of L and U . For a given watermark image matrix A , the PPLU processed matrix \tilde{A} gives a scrambled image where the permutation matrix P is the key matrix for recovering the watermark. To reconstruct A from the scrambled data, A is simply permuted inversely using P . The PPLU decomposition of an image $l(m,n)$ with $m = 1, 2, \dots, M$ and $n = 1, 2, \dots, N$ is shown in Fig. 1.

The product LU is embedded into the transformed domains of a host image, and the permutation matrix P is reserved for authenticating the watermark during the reconstruction process. For robust watermarking, the Arnold transformed data of LU must be embedded into particular bands of the wavelet domain of the host.

3.3 The Arnold transform (AT)

The AT method was recently proposed as a method for blending information data [32]. We employ the AT as a pretreatment for encrypting the product data LU of a watermark image. For $M \times M$ image data $I(x,y)$, the AT encryption is given as:

$$\begin{bmatrix} a \\ b \end{bmatrix} = D(a,b) := \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{M}, \tag{23}$$

where $(x,y) \in [0, M-1] \times [0, M-1]$ and $(a,b) \in [0, M-1] \times [0, M-1]$ are the pixel coordinates of the original and transformed data, respectively. With the periodic boundary treatment, after m iterations of the Arnold transform, the image data can be encrypted as follows:

$$I((x,y)^{(k)}) = I(D(x,y)^{(k-1)}), \quad k = 1, 2, \dots, m, \tag{24}$$

where $(x,y)^{(0)} = (x,y)$. An example of four iterations of the AT applied to the product data LU of a watermark image is shown in Fig. 2b, which results in scrambled data. The original data may be recovered from the scrambled data by applying m iterations of the inverse D^{-1} as follows:

$$I((a,b)^{(k)}) = I(D^{-1}(a,b)^{(k-1)}), \quad k = 1, 2, \dots, m, \tag{25}$$

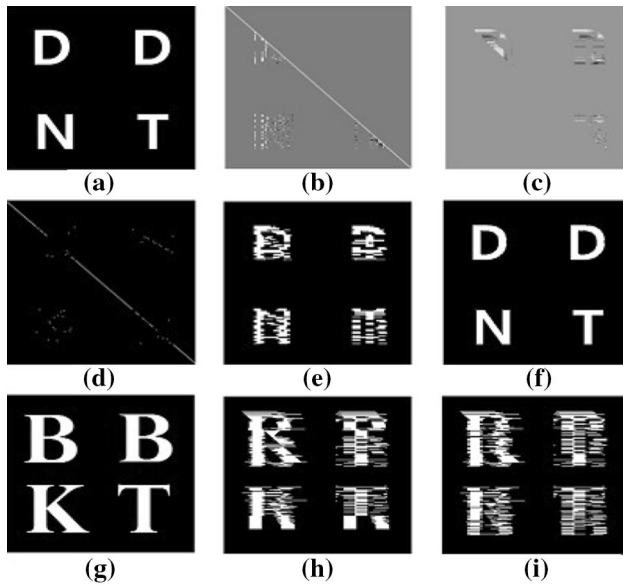


Fig. 1 PPLU decomposition of a watermark image. **a** Original watermark image, **b** lower-triangular data, **c** upper-triangular data, **d** key permutation data of the original watermark image, **e** product of the lower and upper triangular data of original watermark image, and **f** reconstruction of the watermark image from the true product data of the original watermark image using the true key permutation data in **d**. **g** Supposed fake watermark image and **h** product image of the lower and upper triangular data of the supposed fake watermark image. **i** Reconstruction of the watermark image from the fake product data **h** of the supposed fake watermark image **g** using the genuine key permutation data of original watermark image **a**

where $(a, b)^{(0)}$ is a pixel of the scrambled data. It should be noted that due to the periodic characteristics of the Arnold transform, the original data can also be obtained after T iterations, depending on the size of the given data. The periodicity T of the AT is shown in Table 2.

Thus, the proposed method applies the AT to the PPLU decomposition. Importantly, the integration of these two techniques provides high-end security for embedding a watermark into respective bands of the wavelet transform of a cover image.

3.4 Embedding process

The proposed watermark embedding process comprises two starting components (see Fig. 3). For a given cover image, a wavelet transform is applied to obtain sub-band images in which the coded watermark data are embedded. Transform domain methods [32] are robust compared to spatial domain methods because when an image is inverse transformed, the watermark is irregularly distributed over the image, making it difficult for an attacker to read or modify. As a result of the localization of both the spatial and frequency domain, the wavelet transform is the preferred method among current transforms. For the

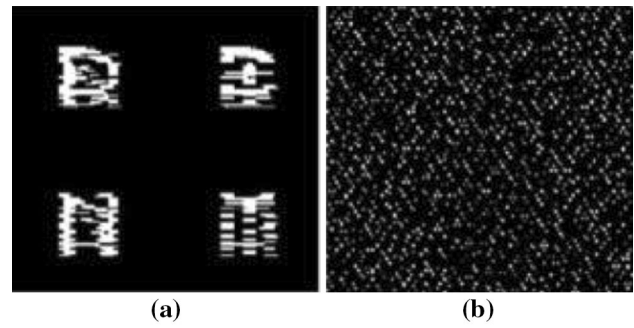


Fig. 2 An example of four iterations of the Arnold transform for **a** product data of the lower and upper triangular matrices shown in Fig. 1c. **b** Scrambled data after employing the Arnold transforms to the product data of the lower and upper triangular given in **a**

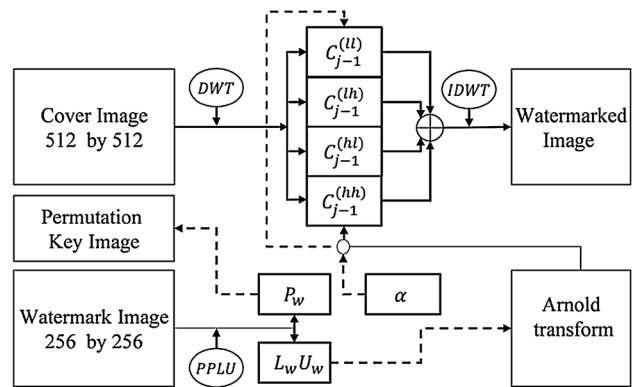


Fig. 3 Block diagram of the embedding process

watermark process, PPLU decomposition of a watermark image W as described in Eq. (8) can be expressed as:

$$P_w W = L_w U_w, \tag{26}$$

where P_w is the permutation matrix associated with W containing the row swapping information and L_w, U_w are the lower and upper triangular matrices of W , respectively. In order to attain a highly imperceptible level of watermark data with scrambled coded watermark data Δ_w , a few of iterations of the AT are applied to $L_w U_w$. Furthermore, the permutation matrix P_w is reserved as a security key to validate the original watermark at the extraction stage. The scrambled coded watermark data Δ_w are embedded accordingly into a chosen sub-band image set of the cover image C .

We let j be the finest resolution level given by the exponent of the dyadic representation of the image size of C . From a one level decomposition of C by a discrete

Table 2 Periodicity of Arnold transforms

M	128	256	480	512
T	96	192	240	384

wavelet transform, four sub-band images with resolution level $j - 1$ are attained as follows:

$$C_{j-1}^{(ll)}, C_{j-1}^{(lh)}, C_{j-1}^{(hl)}, C_{j-1}^{(hh)} \tag{27}$$

By applying a low-pass wavelet filter along the rows and columns of C , approximated data for $C_{j-1}^{(ll)}$ are obtained.

Also, $C_{j-1}^{(lh)}$ is the horizontally oriented detail image data obtained by applying a low-pass wavelet filter along the rows and a high-pass wavelet filter along the columns of C .

Similarly, $C_{j-1}^{(hl)}$ is a vertically oriented detail image data. By applying a high-pass wavelet filter along the rows and columns of C , the detailed image data $C_{j-1}^{(hh)}$ are obtained.

Specifically, $C_{j-1}^{(ll)}$, the lower resolution level, contains a larger perceptual capacity and provides high imperceptibility by preserving the scrambled data of the watermark [32]. The remaining three parts $C_{j-1}^{(lh)}$, $C_{j-1}^{(hl)}$, and $C_{j-1}^{(hh)}$ consist of detailed information from the high-resolution level.

In the proposed algorithm, the same scrambled data obtained from Fig. 2b are embedded into $C_{j-1}^{(ll)}$ and $C_{j-1}^{(hh)}$, respectively [35]. Likewise, an additional scale parameter alpha with values between 0 and 1 is introduced as a strength factor that influences the trade-off between perceptual transparencies of the watermarked cover image and reliability of watermark detection [32, 36]. Large alpha values may lead to increased perceptual transparency but are less robust against several attacks [38]. In the proposed method, we use a combination mentioned in Eq. (30) for embedding the scrambled coded of watermark data Δ_w into the DWT decomposed parts $C_{j-1}^{(ll)}$ and $C_{j-1}^{(hh)}$, so that watermark embedded data are obtained as follows:

$$\widetilde{C}_{j-1}^{(ll)} = C_{j-1}^{(ll)} + \alpha\Delta_w, \tag{28}$$

$$\widetilde{C}_{j-1}^{(hh)} = C_{j-1}^{(hh)} + \alpha\Delta_w, \tag{29}$$

where α is a scaling factor and derived from approximation sub-band of cover image as follows:

$$\alpha = \frac{|C_{j-1}^{(ll)}|}{\max |C_{j-1}^{(ll)}|} \times \Gamma. \tag{30}$$

We considered Γ with values between 0 and 1 is introduced as a strength factor that influences the trade-off between perceptual transparencies of the watermarked image. In the proposed method, we use empirical value of scaling factor $\Gamma = 0.075$ for embedding the watermark image into cover image [37]. Importantly, embedding the same watermark in the approximated data and detailed data at the lower

resolution level enhances robustness against certain attacks [38]. Furthermore, the watermarked image \widetilde{C}_j is obtained by using inverse wavelet transform from the following modified sub-band data:

$$\widetilde{C}_{j-1}^{(ll)}, C_{j-1}^{(lh)}, C_{j-1}^{(hl)}, \widetilde{C}_{j-1}^{(hh)}.$$

3.5 Extracting process

A wavelet transform is applied to decompose a possibly distorted watermarked image as well as the original cover images into the four sub-band data as shown in Fig. 4. The distorted watermarked image is decomposed into the approximated sub-band, the horizontal sub-band, vertical sub-band, and diagonal sub-band data, $\widetilde{C}_{j-1}^{(ll)}$, $\widetilde{C}_{j-1}^{(lh)}$, $\widetilde{C}_{j-1}^{(hl)}$, and $\widetilde{C}_{j-1}^{*(hh)}$, respectively. Extraction of the scrambled watermark data is performed as follows:

$$\widetilde{\Delta}_{w1} = \frac{\widetilde{C}_{j-1}^{*(ll)} - C_{j-1}^{(ll)}}{\alpha}, \tag{31}$$

$$\widetilde{\Delta}_{w2} = \frac{\widetilde{C}_{j-1}^{*(hh)} - C_{j-1}^{(hh)}}{\alpha}, \tag{32}$$

where the first scrambled watermark data $\widetilde{\Delta}_{w1}$ are obtained using Eq. (31) and the second scrambled watermark data $\widetilde{\Delta}_{w2}$ are obtained from Eq. (32), respectively. The extracted scrambled data are the estimated product data of the lower and upper triangular matrices, which are further processed by an inverse Arnold transform using the same number of iterations performed during the embedding process through Eq. (11). To authenticate the watermark, the information data obtained after an inverse Arnold transform are multiplied with the permutation matrix P_w that is the owner’s security key. As a result, we obtain two watermark images: W_1 (watermark image 1) from $\widetilde{C}_{j-1}^{*(ll)}$

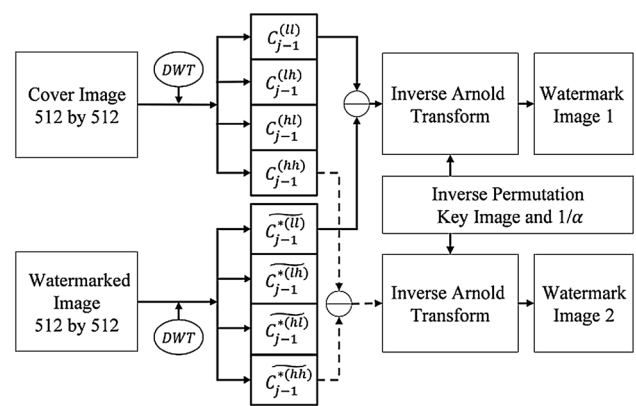


Fig. 4 Block diagram of the extraction process

and W_2 (watermark image 2) from $\widetilde{C}_{j-1}^{*(hh)}$, respectively, as shown in Fig. 4. Experimentally, the retrieving the watermark with W_1 is robust against various attacks such as JPEG compression, rotation, adding Gaussian noise, and resizing. The retrieving the watermark with W_2 is also robust against the contrast adjustment and cropping attacks.

4 Simulations and evaluations

The proposed scheme is examined with respect to its ability to provide security for certain digital documents and is found to be more convenient than existing methods. In addition, the proposed method performs without delay and huge computational requirement and verifies the identity of the true ownership. Specifically, we examine the visual quality of watermarked images by the PSNR [39] as follows:

$$PSNR = 10 \log \left(\frac{MAX_{m,n}^2(I_{m,n})}{\frac{1}{MN} \sum_{m,n} (I_{m,n} - \tilde{I}_{m,n})^2} \right), \quad (33)$$

where I is the cover image, \tilde{I} is the watermarked image, and M and N are the number of pixels for the rows and columns of the host image matrix, respectively. To evaluate the correlation between the original watermark image and the extracted watermark image, the coefficient correlation CC [39] is defined in Eq. (34) and is a number between 0 and 1 used to specify the confidence level between the two images.

$$CC = \frac{\sum_{m,n} (U_{m,n} - \bar{U})(V_{m,n} - \bar{V})}{\sum_{m,n} (U_{m,n} - \bar{U})^2 \sum_{m,n} (V_{m,n} - \bar{V})^2}, \quad (34)$$

where $\bar{U} = \text{mean}^2(U)$ and $\bar{V} = \text{mean}^2(V)$ are the averages of the embedded and extracted images, respectively. A value of 1 shows that two images are having the same quality, and value of 0 shows no correlation between the two images.

As shown in Figs. 5 and 6, our experiments indicate that the proposed watermarking scheme exhibits high imperceptibility and good robustness. Specifically, the method verifies only the true ownership of the watermark image, as determined by perfect reconstruction of the watermark image. Likewise, due to the nature of certain attacks, the product of the lower and upper triangular matrices of the watermark image does not allow for false extraction of the watermark image. We perform experiments on different images, ranging from the relatively less complicated image (Lena) to the more complicated images (Man and Scene) shown in Fig. 5. In all experiments, the sizes of the test images are cropped to 512×512 pixels. Likewise, the size

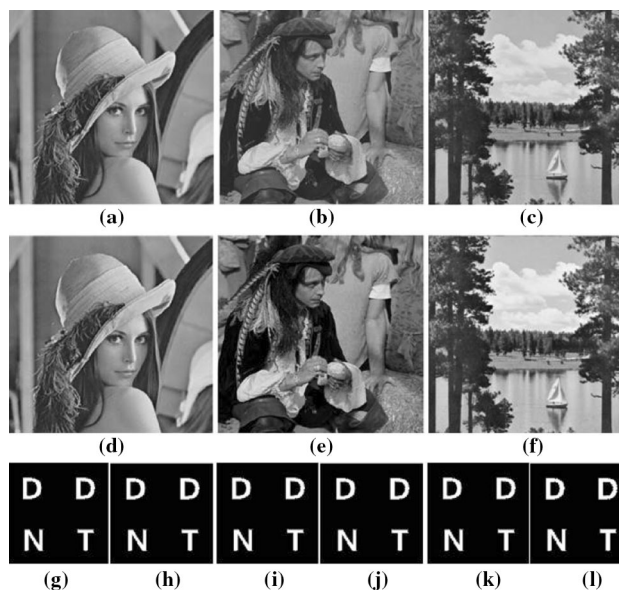


Fig. 5 Visual quality of watermarked and extracted watermark images: **a** original cover image Lena, **b** original cover image Man, **c** original cover image Scene, **d** cover image Lena embedded with watermark data Δ_w (Lena watermarked image), **e** cover image Man embedded with watermark data Δ_w (Man watermarked image), **f** cover image Scene embedded with watermark data Δ_w (Scene watermarked image), **g** watermark image extracted from the $\widetilde{C}_{j-1}^{*(ll)}$ band of **d**, **h** watermark image extracted from the $\widetilde{C}_{j-1}^{*(hh)}$ band of **d**, **k** watermark image extracted from the $\widetilde{C}_{j-1}^{*(ll)}$ band of **e**, **l** watermark image extracted from the $\widetilde{C}_{j-1}^{*(hh)}$ band of **e**, **m** watermark image extracted from the $\widetilde{C}_{j-1}^{*(ll)}$ band of **f**, **n** watermark image extracted from the $\widetilde{C}_{j-1}^{*(hh)}$ band of **f**

of the DDNT watermark image is 256×256 pixels. For general analysis of the proposed method, simple and unique watermark-based perceptual observations of watermarked images are performed as demonstrated in the following figures.

To provide a general comparison of computational time (s) of the extraction process and the imperceptibility of watermarked images on the basis of PSNR (dB) using Eq. (27), the experimental results of the proposed method are compared with the method described in [15] and [24]: using test images of Lena, Man, and Scene and displayed graphically as shown in Fig. 6. The imperceptibility of watermarked images, CC values of the extracted watermark images W_1 and W_2 from the particular sub-band data $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$, and the corresponding computational time of the extraction process are analyzed numerically and reported in Table 3. Experiments are performed on an Intel[®]Core (TM) 2 QUAD CPU Q6700 @ 2.66 GHz with 4 GB of RAM running a 32-bit Windows 7 system.

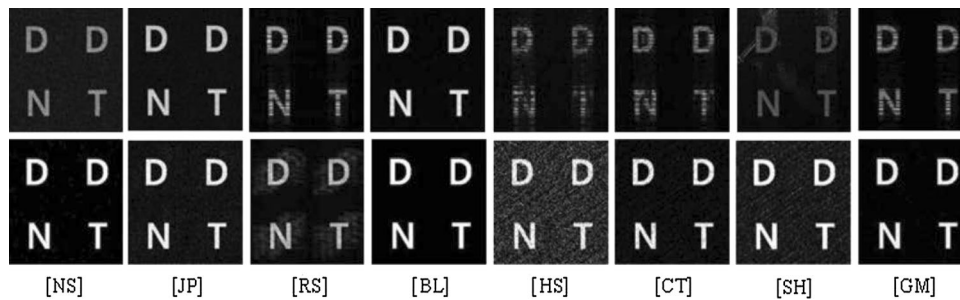


Fig. 6 Extraction of watermark images from the watermarked Lena against corresponding to certain watermark attacks including: noise attack *NS*, JPEG Compression *JP*, rescaling *RS*, blurring *BL*, histogram *HS*, contrast *CT*, sharpening *SH*, and gamma correction *GM*. *First row* shows the extracted watermark using recent existed

method [24]. *Second row* shows the extraction of watermark image using proposed method with high value *CC* from $\widetilde{C}_{j-1}^{*(ll)}$ or $\widetilde{C}_{j-1}^{*(hh)}$, respectively

Table 3 Comparison of the proposed method, [15] and [24] by evaluations of different test images

Test images/method	PSNR (dB)			CC (Index)			Extraction time (s)		
	Proposed	[15]	[24]	$\widetilde{C}_{j-1}^{*(ll)}$	[15]	[24]	Proposed	[15]	[24]
Lena	40.69	40.7832	38.37	0.9999	0.9988	0.9969	1.9058	111.59	344.34
Man	41.45	40.783	38.46	0.9998	0.9986	0.9968	1.9909	112.99	342.49
Scene	41.41	40.7834	38.40	0.9998	0.9987	0.9968	1.8862	114.28	345.31

Bold represents results of the proposed method

Table 4 Robustness against fragile watermarking attacks

Test images	Methods	JP	RS	BL	HS	CT	GM
Lena	CCLL	<u>0.9272</u>	0.9474	0.9995	0.0203	0.1641	0.3969
	CCHH	0.3134	0.1816	0.9997	<u>0.8051</u>	<u>0.9405</u>	<u>0.9902</u>
	[15]	0.9849	0.8505	0.9971	0.8953	0.9765	0.9928
	[24]	0.9708	0.8829	0.9968	0.6642	0.7782	0.8407
Man	CCLL	<u>0.9077</u>	0.9474	0.9994	0.0424	0.1533	0.4624
	CCHH	0.2647	0.1816	0.9970	0.7506	0.9322	<u>0.9826</u>
	[15]	0.9838	0.7806	0.9970	0.8501	0.9619	0.9897
	[24]	0.9690	0.8429	0.9966	0.6726	0.8994	0.8448
Scene	CCLL	<u>0.8987</u>	0.9474	0.9993	0.0675	0.1159	<u>0.2893</u>
	CCHH	0.3411	0.1817	0.9994	<u>0.5924</u>	<u>0.8621</u>	<u>0.9781</u>
	[15]	0.9818	0.7484	0.9967	0.7093	0.8828	0.9829
	[24]	0.9754	0.8696	0.9904	0.5795	0.7431	0.8144

Bold represents result of the proposed method

Underline represents highest result of the given method

The proposed method is examined by measuring the quality of watermarked test images as shown in Table 3. The high PSNRs as shown in Table 3 are maintained the good level of imperceptibility of watermarked images, and the corresponding correlation coefficient *CC* values for the extracted watermark images are highly reliable for high-end security. In addition the less computational time (s) of the extraction process shows the efficiency of the PPLU

decomposition process. The noise addition test is conducted by adding salt and pepper noise to the watermarked image. To analyze the effects of a JPEG compression attack, we use the Stir Mark test [40]. With respect to the sharpening attack, test images are analyzed using a contrast enhancement filter based upon a negative Laplacian matrix. Blurring attacks are conducted using low-pass Gaussian filter with a standard deviation of 0.05. The most of the

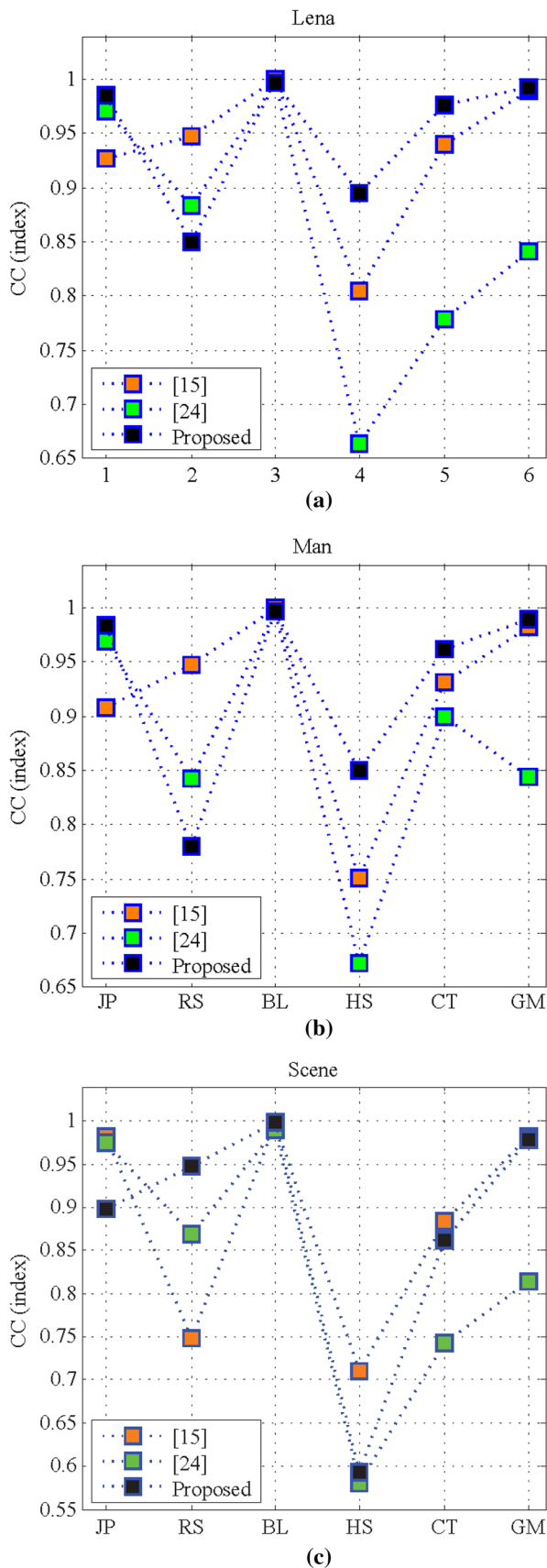


Fig. 7 The CC values are used to compare our proposed method with [15] and [24]. *Brown square* represents [15], *green square* represents [24], and *black square* represents our proposed method, respectively. The CC values of extracted watermark from three different standard images: **a** Lena, **b** Man, and **c** Scene, are demonstrated corresponding to the different nature of attacks: JPEG compression JP , rescaling RS , blurring BL , histogram HS , contrast CT , and gamma correction GM , respectively

watermark tests are performed using the standard MATLAB tools, respectively. The corresponding numerical results for the described experiments are shown in Table 3 and visually represented in Fig. 5.

For a watermark embedding procedure to be efficient, it has robustness against various pirating attacks, including compression, noise attack (NS), JPEG compression (JP), rescaling (RS), blurring (BL), histogram (HS), contrast (CT), sharpening (SH), gamma correction (GM), cropping including row and column removal, and rotation with cropping as well as cryptographic modification [41]. The certain robustness attacks in existing methods [15] and [24] are compared with our proposed method in Table 4 and graphically demonstrated in Fig. 7.

In Table 3 the CCLL and CCHH are the CC values for watermark images extracted from $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$ of corresponding watermarked images, respectively. These $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$ have different levels of resistance against certain attacks. Specifically, the $\widetilde{C}_{j-1}^{*(ll)}$ is robust to common attacks including, noise, JPEG compression as shown in Table 4 and Figs. 6 and 7, respectively. Furthermore, the $\widetilde{C}_{j-1}^{*(hh)}$ enhances the quality of the watermark extracting from $\widetilde{C}_{j-1}^{*(ll)}$ since the same watermark embedded in both $C_{j-1}^{(ll)}$ and $C_{j-1}^{(hh)}$. Moreover, it provides robustness against rescaling, blurring, histogram, contrast, sharpening, and gamma correction, etc. However, in the case of blurring tests, the $\widetilde{C}_{j-1}^{*(ll)}$ shows sufficient robustness compared to the $\widetilde{C}_{j-1}^{*(hh)}$.

The numerical results shown in Table 4 and in Fig. 7 confirm the robustness of the proposed method against certain fragile nature of attacks in comparison to recent SVD-based method [15] and [24]. Although our method shows little less robustness against JPEG attack as compared to method described in [15] and [24], which is shown clearly in Fig. 7, in terms of watermarked imperceptibility and extraction time of watermark with unique confirmation of legitimate ownership, our method shows nearly equal or the superior performance than the recent existed methods of [15] and [24]. The rapidly developing field of digitized

Table 5 PSNR (dB) of the information embedded image

Embedded images (512 × 512)	DDNT (256 × 256)				
	Strength factor (Γ)				
	0.055	0.065	0.075	0.085	0.095
Lena	38.29	40.10	40.69	40.01	38.20
Man	39.33	40.92	41.45	40.75	39.15
Scene	39.68	40.90	41.41	40.88	39.29

Bold represents result of the proposed method

Table 6 CC index of the extracted information image

Embedded images (512 × 512)	DDNT (256 × 256)				
	Strength factor (Γ)				
	0.055	0.065	0.075	0.085	0.095
Lena	0.9777	0.9850	0.9999	0.9799	0.9701
Man	0.9760	0.9841	0.9998	0.9798	0.9698
Scene	0.9759	0.9844	0.9998	0.9790	0.9688

Bold represents result of the proposed method

Table 7 Robustness against cropping attacks

Cropping ratio	CC from $\widetilde{C}_{j-1}^{*(ll)}$	CC from $\widetilde{C}_{j-1}^{*(hh)}$
Corner, 25%	0.8502	0.8502
Column, 50%	0.6821	0.6821
Diagonal, 50%	0.6962	0.6962
Inner circle, 75 rad	0.7940	0.7940
Outer circle, 75 rad	0.5792	0.5792
One-fourth, 75%	0.6504	0.6504

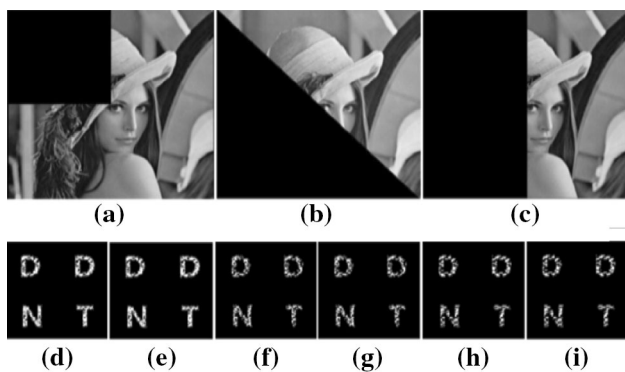


Fig. 8 Experimental results of cropping attacks using the Lena image. **a** Corner attack, **b** diagonal attack, and **c** column attack. **d, e** Watermark extractions from the $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$ of the attacked image (**a**), respectively. **f, g** Watermark extractions from the $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$ of the attacked image (**b**), respectively. **h, i** Watermark extractions from the $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$ bands of the attacked image (**c**), respectively

image documents enables authors to create documents bearing their own distinctive identity a pressing security issue in many organizations. Therefore, there is an urgent need for a screening system that can easily verify authentication and process large numbers of image documents rapidly. Our propose method allows large embedding capacity based on experimental value of Γ as shown in Tables 5 and 6. Note that there needs to be a trade-off

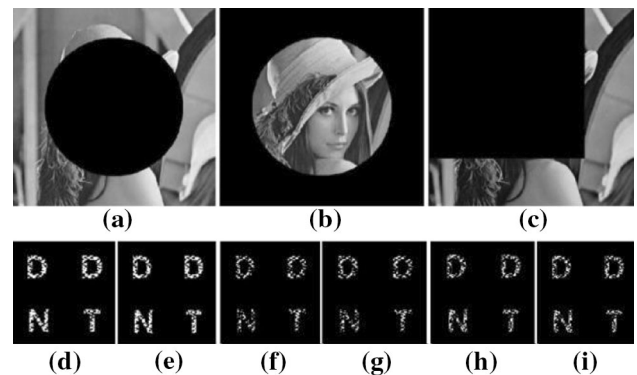


Fig. 9 Experimental results of intentional cropping attacks using the Lena image. **a** Crop to the inner circle, **b** crop to the area surrounding the center circle, and **c** anonymous huge area attack. **d, e** Watermark extraction from the $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$ of the attacked image (**a**), respectively. **f, g** Watermark extraction from the $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$ of the attacked image (**b**), respectively. **h, i** Watermark extraction from the $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$ of the attacked image (**c**), respectively

between the capacity of an embedded information data and the quality of the information embedded image [30]. For our proposed method, the capacity of an embedded information data is approximately twice as big as that of the information embedded data. For our proposed method, the capacity of an embedded information data is approximately twice as big as that of the information embedded data. Thanks to the diffusion process of the Arnold transform and partial pivoting to the information data, we can

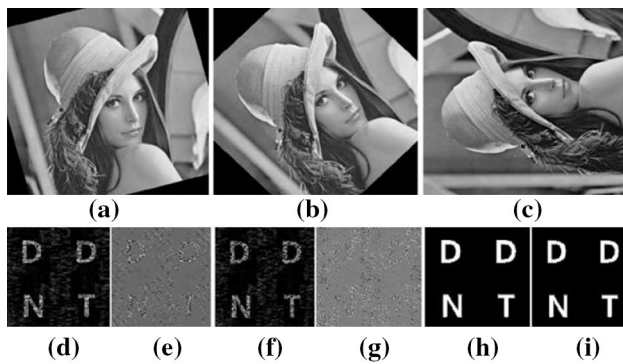


Fig. 10 Experimental results of rotation attacks of the Lena image. Rotation of **a** 3°, **b** 45°, **c** and 90°. **d**, **e** Watermark extraction from the $\widetilde{C}_{j-1}^{*(ll)}$, $\widetilde{C}_{j-1}^{*(hh)}$ of the attacked image (**a**), respectively. **f**, **g** Watermark extraction from the $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$ of the attacked image (**b**), respectively. **h**, **i** Watermark extraction from the $\widetilde{C}_{j-1}^{*(ll)}$ and $\widetilde{C}_{j-1}^{*(hh)}$ of the attacked image (**c**), respectively

Table 8 Robustness against rotation attacks

Rotation angle	CC from $\widetilde{C}_{j-1}^{*(ll)}$	CC from $\widetilde{C}_{j-1}^{*(hh)}$
3°	0.8290	0.5577
45°	0.7320	0.2750
90°	0.9999	0.9999

generate a coded data with almost uniformly scattered structure [15, 19] as shown in Figs. 2 and 5, which would be embedded to a cover image with keeping good quality of the information embedded data. While for most of the recent existing techniques [4, 7, 27–32]. Moreover, the fast computational time of the proposed method makes it more efficient and highly reliable for valid documents even for fast-track checking (e.g., airport entry gates or other security clearance gates).

Figure 6 shows the robustness of the proposed method for the Lena, Man, and Scene test images against certain watermark attacks, respectively. Using propose method, it is possible to uncover an appropriate latent data representation of the extracted watermark in terms of local, global, and the intrinsic structural consistencies which are exploited simultaneously, in reconstruction phase robustly [42]. Indeed, many existing algorithms are susceptible to common image manipulation and geometric attacks [11, 12]. The method developed in [15] and [24] does not show its performance in cropping and rotation attacks. However, our proposed method also performs well in rotation and cropping attacks. We examine the *CC* values of the extracted watermark images with only the Lena test image. To verify the high-end security capabilities of extracted watermark image, cropping tests are performed

on the watermarked Lena image as shown in Figs. 7 and 8. The corresponding numerical results of the cropping attack tests are shown in Table 7.

Table 7 shows the robustness of the proposed method against cropping attacks demonstrated by cropping different areas of the watermarked Lena image. Based on our experimental results, a reliable watermark could be extracted with up to 75% cropping as shown in Fig. 9h and i. In rotation attacks, the watermarked image is rotated by keeping the same size of the original image with the help of a cropping process. Various degrees of rotation are applied to the watermarked image, followed by extraction of the watermark image as shown in Fig. 10. The corresponding numerical results of the rotation attack tests are shown in Table 8.

5 Conclusions

In this work, a hybrid watermarking scheme with the partial pivoting lower and upper (PPLU) triangular decomposition and Arnold transform (AT) image decomposition is proposed in the wavelet domain. Therefore, the proposed framework benefits from wavelet multi-resolution and PPLU advantages. It provides the robustness of proposed method against various geometric attacks using only a genuine permutation key matrix of the original watermark image. The effectiveness of the proposed algorithm is numerically analyzed and validated by simulation results. The experimental results substantiate the reliability of the proposed method for protection of digital images and attain efficient computational time as shown in table. Toward this end, a fast machine learning-based robust digital watermarking with desired improvements will be the subject of a future study.

References

1. Qiao L, Nahrstedt K (1998) Watermarking schemes and protocols for protecting rightful ownership and customer's rights. *J Vis Commun Image Represent* 9(3):194–210
2. Craver S (1996) Can invisible watermarks resolve rightful ownership. IBM T.J. Watson Research Center, New York
3. Cox JJ, Kilian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. *IEEE Trans Image Process* 6(12):1673–1687
4. Liu R, Tan T (2002) An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans Multimed* 4(1):121–128
5. Ganic E, Eskicioglu AM (2004) Robust DWT-SVD domain image watermarking: embedding data in all frequencies. In: *Proceedings of the 2004 workshop on multimedia and security*. Magdeburg, Germany, 2004, pp 166–174

6. Zhang T-X, Zheng W-M, Lu Z-M, Liu B-B (2008) Comments on a semi-blind digital watermarking scheme based on singular value decomposition. pp 123–126
7. Xiao L, Wei Z, Ye J (2008) Comments on “Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition” and theoretical analysis”. *J Electron Imaging* 17(4):040501-040501-3
8. Ganic E, Eskicioglu AM (2005) Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *J Electron Imaging* 14(4):043004-043004-9
9. Chandra D (2002) Digital image watermarking using singular value decomposition. *Circuits Syst MWSCAS* 263(3):264–267
10. Rezazadeh S, Yazdi M (2006) A nonoblivious image watermarking system based on singular value decomposition and texture segmentation. In: *Proceedings of world academy of science, engineering and technology*, 2006
11. Mohammad AA, Alhaj A, Shaltaf S (2008) An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Process* 88(9):2158–2180
12. Yavuz E, Telatar Z (2006) SVD adapted DCT domain DC sub-band image watermarking against watermark ambiguity. *Multimedia content representation, classification and security*. Springer, Berlin, pp 66–73
13. Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2008) *Digital watermarking and steganography*. Morgan Kaufmann Publishers Inc., Burlington
14. Division IBMCR, Craver S, Memon N, Yeo BL, Yeung MM (1997) Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications. IBM T.J. Watson Research Center, New York
15. Muhammad N, Bibi N (2015) Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain. *IET Image Proc* 9(9):795–803
16. Chang CC, Lin C-C, Hu Y-S (2007) An SVD oriented watermark embedding scheme with high qualities for the restored images. *Int J Innov Comput Inf Control* 3(3):609–620
17. Patra JC, Soh W, Ang EL, Meher PK (2006) An improved SVD-based watermarking technique for image and document authentication. In: *APCCAS 2006–2006 IEEE Asia Pacific Conference on Circuits and Systems*, Singapore, pp 1984–1987. doi:[10.1109/APCCAS.2006.342276](https://doi.org/10.1109/APCCAS.2006.342276)
18. Mohan BC, Kumar SS (2008) A robust image watermarking scheme using singular value decomposition. *J Multimed* 3(1):7–15
19. Chung KL, Shen C-H, Chang L-C (2001) A novel SVD-and VQ-based image hiding scheme. *Pattern Recogn Lett* 22(9):1051–1058
20. Loukhaoukha K, Chouinard J-Y (2010) Security of ownership watermarking of digital images based on singular value decomposition. *J Electron Imaging* 19(1):013007-013007-9
21. Fahmy G, Fahmy M, Mohammed U (2010) Nonblind and quasi blind natural preserve transform watermarking. *EURASIP J Adv Signal Process* 10(1):1–13
22. Lai CC (2011) An improved SVD-based watermarking scheme using human visual characteristics. *Opt Commun* 284(4):938–944
23. Hu WC, Chen W-H, Yang C-Y (2012) Robust image watermarking based on discrete wavelet transform-discrete cosine transform-singular value decomposition. *J Electron Imaging* 21(3):33005
24. Ali M, Ahn CW (2014) An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. *Signal Process* 94:545–556
25. Agarwal R (2015) Block based digital watermarking using singular value decomposition on color images. In: *International conference on computing, communication automation (ICCCA)*, pp 1176–1181
26. Muhammad N, Bibi N, Mahmood Z, Kim D-G (2015) Blind data hiding technique using the Fresnelet transform. *SpringerPlus* 4(1):1–15
27. Xing Y, Tan J (2010) Mistakes in the paper entitled “A singular-value decomposition-based image watermarking using genetic algorithm”. *AEU-Int J Electron Commun* 64(1):80–81
28. Tao H, Chongmin L, Zain J, Abdallah N (2014) Robust image watermarking theories and techniques: a review. *J Appl Res Technol* 12(1):122–138
29. Zhang XP, Li K (2005) Comments on “An SVD-based watermarking scheme for protecting rightful Ownership. *IEEE Trans Multimed* 7(3):593–594
30. Gotsman C, Toledo S (2008) On the computation of null spaces of sparse rectangular matrices. *SIAM J Matrix Anal Appl* 30(2):445–463
31. Poole D (2006) *Linear algebra: a modern introduction*. Thomson Brooks/Cole, Stamford
32. Jie Y (2010) Algorithm of image information hiding based on new anti-Arnold transform and Blending in DCT domain. In: *2010 IEEE 12th International Conference on Communication Technology*, Nanjing, pp 312–315. doi:[10.1109/ICCT.2010.5689227](https://doi.org/10.1109/ICCT.2010.5689227)
33. Grigori L, Gilbert JR, Cosnard M (2008) Symbolic and exact structure prediction for sparse Gaussian elimination with partial pivoting. *SIAM J Matrix Anal Appl* 30(4):1520–1545
34. Guo J-M, Prasetyo H (2014) False-positive-free SVD-based image watermarking. *J Vis Commun Image Represent* 25(5):1149–1163
35. Watkins D (2004) *Fundamentals of matrix computations*. Wiley, New York
36. Kundur D, Hatzinakos D (2004) Toward robust logo watermarking using multiresolution image fusion principles. *IEEE Trans Multimed* 6(1):185–198
37. Wu HC, Wu N-I, Tsai C-S, Hwang M-S (2005) Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IEEE Proc Vis Image Signal Process* 152(5):611–615
38. Yassin NI, Salem NM, El Adawy MI (2012) Block based video watermarking scheme using wavelet transform and principle component analysis. *Int J Comput Sci Iss* 9(1):296–301
39. Junfeng L, Wenzhan D (2009) Image quality assessment based on the correlation coefficient and the 2-D discrete wavelet transform. pp 789–793
40. Peticolas FA, Steinebach M, Raynal F, Dittmann J, Fontaine C, Fatès N (2001) A public automated web-based evaluation service for watermarking schemes: StirMark benchmark. pp 575–584
41. Aslantas V (2009) An optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Opt Commun* 282(5):769–777
42. Li Z, Liu J, Tang J, Lu H (2015) Robust structured subspace learning for data representation. *IEEE Trans Pattern Anal Mach Intell* 37(10):2085–2098. doi:[10.1109/TPAMI.2015.2400461](https://doi.org/10.1109/TPAMI.2015.2400461)



Nazeer Muhammad received a Ph.D. degree in Applied Mathematics from Hanyang University, South Korea in 2015. Currently, he is Assistant Professor at the Department of Mathematics, COMSATS Institute of Information Technology, Wah Cantt, Pakistan. In 2010, he received the prestigious Pakistan Government higher education commission (HEC) scholarship award for MS and Ph.D. His interests are digital

signal processing, digital image denoising, digital holography, OFDM, and information theory.



Nargis Bibi received a Ph.D. degree in Computer Science, the School of Computer Science, University of Manchester, UK, in 2014. Currently, she is Assistant Professor at the Department of Computer Science, Fatima Jinnah Women University (FJWU), Rawalpindi, Pakistan. She received her M.Sc from Fatima FJWU, Rawalpindi, Pakistan. She is currently employed in FJWU as Assistant Professor. Her interests are digital signal process-

ing, OFDM, coding theory, and information theory.



Iqbal Qasim received a Ph.D. degree from South Korea in 2013. Iqbal Qasim's research expertise encompasses topics such as digital image processing and pattern recognition. He is the recipient of Government of Pakistan scholarship award for Ph.D. in Computer Engineering. Currently, he is serving as the Senior Research Assistant in Hanyang University, South Korea.



Adnan Jahangir is Assistant Professor at the Department of Mathematics, COMSATS Institute of Information Technology, Wah Cantt, Pakistan. He is the recipient of Pakistan Government higher education commission (HEC) scholarship award for MS and Ph.D. in Mathematics. His research expertise encompasses topics such as wave propagation, solid mechanics, digital image processing, and pattern recognition.



Zahid Mahmood received a B.S. degree in Electrical and Computer Engineering from COMSATS Institute of Information Technology, Pakistan, in 2007, MS degree in Electrical Engineering from South Korea in 2011, and a Ph.D. degree from USA in 2015. Zahid Mahmood's research expertise encompasses topics, such as digital image processing and signal processing. He is the recipient of Government of Pakistan scholarship award for

MS and Ph.D. in Electrical Engineering.