



SecDH: Security of COVID-19 images based on data hiding with PCA

O.P. Singh^a, Amit Kumar Singh^{a,*}, Amrit Kumar Agrawal^b, Huiyu Zhou^c

^a Department of Computer Science and Engineering, National Institute of Technology Patna, Patna, Bihar, India

^b Department of Computer Science and Engineering, Galgotias College of Engineering and Technology, Greater Noida, Uttar Pradesh, India

^c School of Computing and Mathematical Sciences, University of Leicester, United Kingdom

ARTICLE INFO

Keywords:

Healthcare
Cyber physical system
Data hiding
Security
PCA

ABSTRACT

Nowadays, image security and copyright protection become challenging, especially after the COVID-19 pandemic. In the paper, we develop SecDH as a medical data hiding scheme, which can guarantee the security and copyright protection of the COVID-19 images. Firstly, the cover image is normalized, which offers high resistance against the geometric attacks. Secondly, the normalized principal component as embedding factor is computed, which are calculated based on principal component analysis (PCA) between cover and mark image. Thirdly, the medical image is invisibly marked with secret mark based on normalized component, redundant discrete wavelet transform (RDWT) and randomized singular value decomposition (RSVD) is introduced. Finally, Arnold cat map scheme employed to ensure the security of the watermarking system. Under the experimental evaluation, our SecDH tool is not only imperceptible, but also has a satisfactory advantage in robustness and security compared with the traditional watermarking schemes.

1. Introduction

Nowadays, the transmission of medical images has become exceedingly convenient with the advent of communication networks, mobile communications, internet of things (IoT), cyber physical systems, and many multimedia devices [1]. As a result, medical images, especially after the COVID-19 pandemic time, served as the information carrier for different purposes such as medical diagnosis, tele-surgery, defense, medical education, teleconsulting, research, and business analytics [1–3]. Researchers are directed towards a smart healthcare system that needs for transmitting the electronic medical records (EMR) through a secure network [4]. However, security of medical images and related records is a great concern since these images can be easily theft, altered, duplicated or modified via insecure networks [5]. Also, cloud-based healthcare has ensured uninterrupted clinical diagnosis with mobility support and low latency [6]. It is no doubt that advancement in healthcare industries has brought great confidence for communication, but has also caused serious infringement of EMRs. Watermarking is considered as a powerful tool to prevent copyright violation of digital records, which involves embedding an information mark into cover as a form of identification [7,8]. The primary aim of a watermarking is to enhance three features, namely invisibility, capacity, and robustness that should be maintained to ensure a robust system [9]. Over the past few years, researchers have adopted transformed-domain-based watermarking to provide stronger robustness of medical images [10–17].

In order to enhance the security for e-healthcare application Anand and Singh [10], suggested an optimization based data hiding scheme in transform domain. Multiple marks are concealed inside cover image using the optimal factor which is obtained by the fusion of PSO and FA. Further, marked image is encrypted using chaotic map to offer additional security of this scheme. However, computational cost is high. Authors [11] have proposed a novel dual watermarking algorithm for ensuring the security and privacy of medical information in E-healthcare application. The dual mark images are concealed inside different coefficient of medical host image, which ensures better security. Further, chaotic encryption is employed on marked image to offer the additional security. This scheme did not offer better resistance against geometric attacks.

In [12], author introduced a novel scheme, which aims to provide the better robustness along with better visual quality at very low cost. First, LWT transforms host image and then multiple decomposition are performed on selected coefficient of host image for embedding purpose. Further, security of this scheme is enhanced using chaotic encryption. The robustness performance is further increased by performing DCNN at extraction procedure. Anand and Singh [13] introduced a fuzzy based scheme, which aims to provide the security for smart healthcare applications. First, IWT transforms cover image and then selected sub-band is further decomposed using Schur and RSVD. Further, final mark image is concealed into transformed cover image with the help optimal embedding factor which is obtained using fuzzy logic. Lastly,

* Corresponding author.

E-mail addresses: omprakash7667@gmail.com (O.P. Singh), amit.singh@nitp.ac.in (A.K. Singh), agrawal.amrit4@gmail.com (A.K. Agrawal), hz143@leicester.ac.uk (H. Zhou).

<https://doi.org/10.1016/j.comcom.2022.05.010>

Received 18 March 2022; Received in revised form 23 April 2022; Accepted 10 May 2022

Available online 18 May 2022

0140-3664/© 2022 Elsevier B.V. All rights reserved.

chaotic encryption employed on marked image to ensure better security. Optimized watermarking approach is developed for providing the security of landslide images by Mohan et al. [14]. Prior to embedding process, the fusion of PSO and FA is employed to compute optimal embedding factor which maintains the trade-off between robustness and invisibility. Further, scrambled mark image embedded inside transformed cover image with the help of optimal embedding factor. After that, selective encryption employed on marked image to provide the additional security of this scheme.

To provide the security of multimedia data, authors [15] illustrated a robust data hiding scheme in transform domain. First, multiple decomposition performed on cover and mark image respectively and then mark image hidden into cover image. Further, text mark along hash value of cover is concealed inside marked image using magic cubes to enhance the capacity of this scheme. Furthermore, lossless encryption employed on marked image to ensure better security. Authors have introduced an image fusion based watermarking algorithm for securing the medical information [16]. Firstly, wavelet based image fusion is performed on mark images to obtain fused mark image, which offers better capacity. In order to enhance the security of proposed scheme, Arnold transform is utilized to scramble fused mark image and then it is concealed inside the cover image using the fusion DWT and SVD. To address the issue of false positive problem (FPP), Ansari et al. [17] proposed a watermarking framework in transform domain. This scheme utilizes the concept of digital signature which provides the solution of FPP. It shows better resistance against geometric attacks.

At present, transform domain watermarking is more popular due to its high robustness nature against attacks. However, these transformations are sensitive to geometric changes in the images. Further, we noticed that most of the schemes apply manual embedding factor for embedding purpose, which does not offer better results. Furthermore, most of the SVD-based watermarking method showed good results but they do not offer the solution for false positive issue. Lastly, most of the schemes did not offer better embedding capacity and less resistance against geometric attacks. In this study, we develop a medical data hiding scheme, namely, SecDH, which can guarantee the security and copyright protection of the COVID-19 images. Major novelties of this work are:

1. Advantages of image normalization: Image normalization procedure [18] is utilized to transform the image into standard image, which offers high resistance against the geometric attacks.
2. High invisibility and robustness features: Combination of RDWT-RSVD transformed scheme is used to perform imperceptible marking of logo mark within the carrier media. This combination offers not only the high robustness and imperceptibility, but also increases the mark capacity with linear complexity. RDWT is shift invariant and holds all the desirable properties of DWT [19]. Additionally, RSVD [20] used to embed the mark data in the source image for reducing the amount of calculation, i.e., computational cost.
3. Solution for FPP issue: The principal component (PC) of mark image is hidden in the host image, which solves the FPP issue.
4. PCA [21] is utilized to determine the normalized principal component for embedding purpose, which maintains the balanced trade-off between robustness and imperceptibility of proposed scheme.
5. Additional Security: Arnold cat map [22] encryption scheme is used to ensure the security of the watermarking system. Arnold cat map has several properties in terms of simplicity and periodicity.
6. Better robustness performance: Compared with the traditional, our scheme, namely, SecDH, has better robustness, indicating its potential for secure healthcare.

The remaining part of this work is summarized as follows. Section 2, contains the background information which is used in proposed scheme, and proposed architecture is described in Section 3. Further, the experimental analysis is described in Section 4. Lastly, conclusion along with future trends are demonstrated in Section 5.

2. Background information

2.1. Image normalization

Image normalization is a procedure to transform the image into standard image such that it contains detailed information of input image [18]. It provides better resistance against the geometric attacks. The detailed steps of image normalization procedure are summarized below.

1. Translation: First, it transforms original image $Img(m, n)$ from initial position $p^1 = (m_1, n_1)$ to new position $p^2 = (m_2, n_2)$. Where, p^1 and p^2 are indicated as specific positions of original image $Img_1(m, n)$ and output image $Img_2(m, n)$ respectively. The translation operation is described below:

$$(m_2, n_2)^T = (m_1 - t_\alpha, n_1 - t_\beta)^T \quad (1)$$

2. Shearing: In this step, we transform $Img_2(m, n)$ in the x -direction to obtain desired image $Img_3(m, n)$ with the help of shearing operator, ' S_x '.

$$S_x = \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} \quad (2)$$

where, the value of β can be determined using the below equation.

$$\beta^3 \mu_{03} + 3\beta^2 \mu_{12} + 3\beta \mu_{21} + 0 \cdot \beta \mu_{30} = 0 \quad (3)$$

Further, transform the $Img_3(m, n)$ in the y -direction to obtain desired image $Img_4(m, n)$ with the help of shearing operator, ' S_y '.

$$S_y = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \quad (4)$$

Where, the value of λ can be determined using the below equation.

$$\lambda = \frac{\mu_{11}}{\mu_{20}} \quad (5)$$

3. Scaling: In this step, we transform the image $Img_4(m, n)$ in both x and y direction respectively to obtain normalized image $Img_5(m, n)$ with the help of scaling operator, ' S_s '. The scaling operator is computed using below equation:

$$S_s = \begin{bmatrix} \alpha & 0 \\ 0 & \delta \end{bmatrix} \quad (6)$$

2.2. Redundant discrete wavelet transform (RDWT)

Although DWT has major advantages of multi-scalability, multi-resolution and space frequency localization, it suffers from the issues of shift sensitivity and poor directionality [19]. RDWT solved these issues as suffered by DWT. RDWT is shift invariant and holds all the desirable properties of DWT for robust and imperceptible watermarking [19]. As presented in Fig. 1, the size of RDWT coefficients and original image are equal which improves the embedding capacity and helps in more precise extraction of local texture of RDWT domain [19].

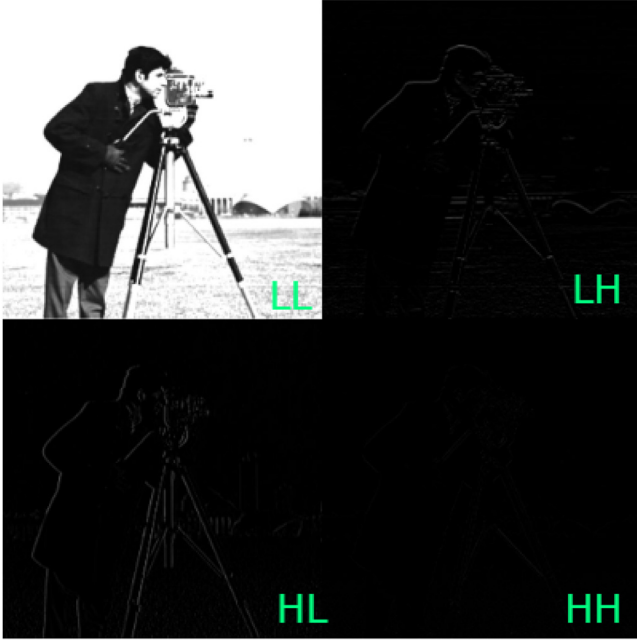


Fig. 1. RDWT decomposition of cameraman image.

2.3. Randomized singular value decomposition (RSVD)

RSVD plays an important role to perform matrix factorization in image processing [20]. The computational cost of RSVD is less than SVD. The time complexity of RSVD is $O(ijr)$, where size of input matrix is denoted as $i \times j$ and rank of this matrix is termed as r . The mathematical equation of RSVD of input matrix, 'A' is obtained as,

$$A = U_r S_r V_r^T \quad (7)$$

Where, ' U_r ' and ' V_r^T ' are termed as orthogonal matrix, and diagonal matrix is denoted as ' S_r '.

RSVD decomposed the input matrix, 'A' into two parts. In first part, random sampling is performed to obtain reduced matrix, 'W'. The rank of input and reduced matrix is same. However, randomization process is performed to obtain an optimal matrix. A new matrix, 'X' is obtained as,

$$X = W^T A \quad (8)$$

In second part, SVD operation is performed to decompose the matrix, 'X'.

$$X = U_X S_X V_X^T \quad (9)$$

Here, ' U_X ' is denoted as left singular matrix of the matrix, 'X'. RSVD decomposition can be justified using Eq. (10),

$$A = W W^T A = W X = W U_X S_X V_X^T = U_R S_R V_R^T \quad (10)$$

Here, ' U_R ' = ' $W U_X$ ' and ' V_R ' are orthogonal matrices. For illustration purpose, the pixel value of matrix, 'A' with size of 4×4 is obtained from input 'Cameraman' image is presented below.

$$A = \begin{bmatrix} 169 & 157 & 167 & 160 \\ 130 & 33 & 131 & 160 \\ 80 & 44 & 126 & 133 \\ 83 & 87 & 126 & 115 \end{bmatrix} \quad (11)$$

$$U_r = \begin{bmatrix} -0.6514 & -0.6322 & -0.3321 & -0.2566 \\ -0.4849 & 0.6453 & -0.5088 & 0.2994 \\ -0.4065 & 0.4008 & 0.5233 & -0.6327 \\ -0.4189 & -0.1528 & 0.5975 & 0.6665 \end{bmatrix} \quad (12)$$

$$S_r = \begin{bmatrix} 494.5455 & 0 & 0 & 0 \\ 0 & 83.4700 & 0 & 0 \\ 0 & 0 & 36.9540 & 0 \\ 0 & 0 & 0 & 0.9779 \end{bmatrix} \quad (13)$$

$$V_r = \begin{bmatrix} -0.4861 & -0.0428 & -0.8366 & 0.2590 \\ -0.3490 & -0.8819 & 0.1646 & -0.2707 \\ -0.5587 & 0.1222 & 0.5173 & 0.6367 \\ -0.5743 & -0.4532 & 0.1022 & -0.6740 \end{bmatrix} \quad (14)$$

The diagonal matrix, ' S_r ' contains the singular values which arranged in descending order.

2.4. Arnold cat map

Arnold cat map is one of the most popular scrambling methods, which was first introduced by V. I. Arnold [22]. It contains several properties in terms of simplicity and periodicity. The scrambling operation is performed by altering the pixel values of mark image. Besides, the recovery of mark image is possible only if they used secret key. The specific formula of two-dimensional Arnold scrambling is provided below.

$$\begin{bmatrix} X^i \\ Y^i \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \mod N \quad (15)$$

Where, the height of image is indicated as 'N' and variables 'a' and 'b' are known as positive integer values. ' X^i ' and ' Y^i ' are scrambled image with respect to i th iteration of 'X' and 'Y' respectively. In Fig. 2, Arnold transform performed on original image with dimension of 256×256 and after 192 iterations original image is recovered.

2.5. Principal component analysis (PCA)

In order to evaluate the normalized PCA values, we have taken two images namely $Img_1(u, v)$ and $Img_2(u, v)$ along with similar dimensions of $N \times N$. The evaluation of PCA score is highlighted in Fig. 3, and detailed steps for obtaining the PCA score is described below.

$$[Eig, Diag] = \text{Eign} \{ \text{Cov} [Img_1(u, v), Img_2(u, v)] \} \quad (16)$$

$$Eig = \begin{bmatrix} Eig_{11} & Eig_{12} \\ Eig_{21} & Eig_{22} \end{bmatrix} \quad (17)$$

$$Diag = \begin{bmatrix} Diag_{11} & \cdot \\ \cdot & Diag_{22} \end{bmatrix} \quad (18)$$

Where, Eig is denoted as Eigen vectors and Diag is termed as diagonal matrix, which contains the Eigen values. Further, NPC values (PC_1, PC_2) are obtained using below mentioned equations.

If ($Diag_{11} > Diag_{22}$) then

$$PC_1 = \frac{Eig_{11}}{Eig_{11} + Eig_{21}} \quad (19)$$

$$PC_2 = \frac{Eig_{21}}{Eig_{11} + Eig_{21}} \quad (20)$$

Else-if ($Diag_{22} > Diag_{11}$) then

$$PC_1 = \frac{Eig_{12}}{Eig_{12} + Eig_{22}} \quad (21)$$

$$PC_2 = \frac{Eig_{22}}{Eig_{12} + Eig_{22}} \quad (22)$$

Therefore, PCA fusion approach is obtained by given equation

$$PCA(u, v) = PC_1 \times Img_1(u, v) + PC_2 \times Img_2(u, v) \quad (23)$$

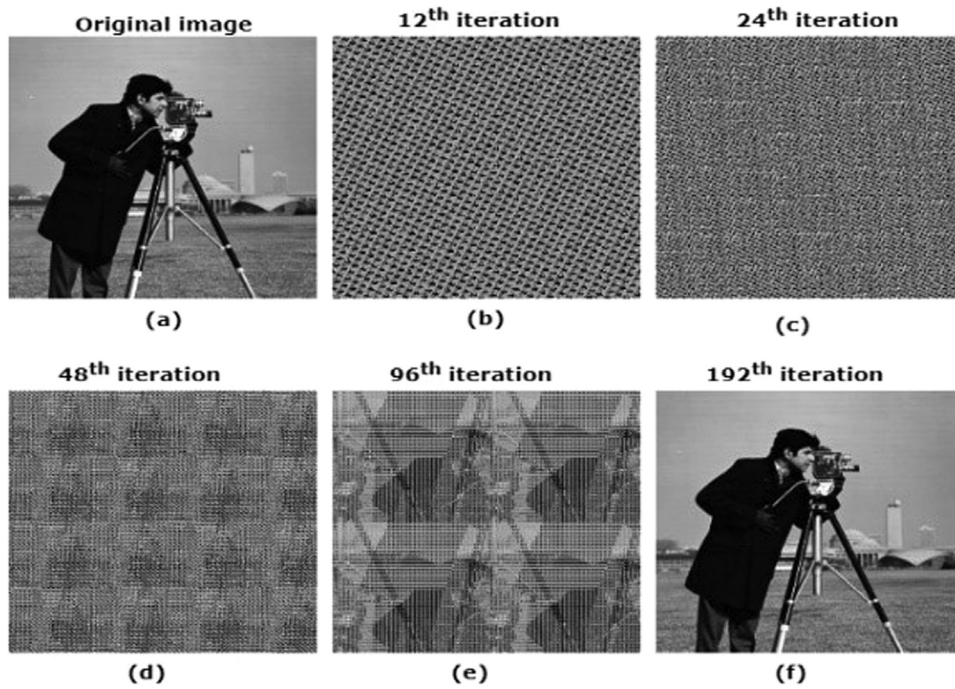


Fig. 2. Arnold transform.

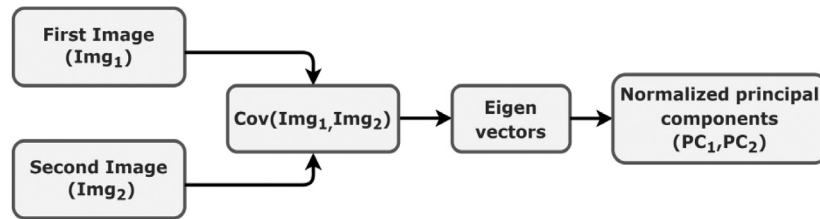


Fig. 3. PCA based fusion.

Table 1
Notations and their description.

Notations	Description	Notations	Description
Org_{img}, Wat_{img}	Cover and mark image	U_2, V_2	Orthogonal value of mark image
A_1, B_1, C_1, D_1	RDWT coefficients of cover image	S_2	Singular value of mark image
A_2, B_2, C_2, D_2	RDWT coefficients of mark image	S_{emb}	Modified singular value
U_h, V_h	Orthogonal value of cover image	D_{new}	Modified RDWT coefficient
U_w, V_w	Orthogonal value of mark image	$Mark_{img}$	Marked image
S_h, S_w	Singular value of cover and mark image	Enc_Mark_{img}	Encrypted marked image
Cov	Covariance value	Dec_Mark_{img}	Decrypted marked image
Eig, Diag	Eigen and diagonal value	A_3, B_3, C_3, D_3	RDWT coefficients of marked image
PC_1, PC_2	Principal coefficients of mark image	U_3, V_3	Orthogonal value of marked image
$Norm_{img}$	Normalized image	S_3	Singular value of marked image
U_1, V_1	Orthogonal value of normalized image	Ext_{pc}	Extracted principal component
S_1	Singular value of normalized image	Rec_Wat_{img}	Recover watermark

3. The SecDH scheme

The proposed SecDH scheme is consist of three main phases: (a) PCA fusion, (b) the embedding procedure, and (c) the decryption procedure. The proposed watermarking framework is shown in Fig. 4. The stepwise procedure of each phase is illustrated in algorithm 1 to algorithm 3, respectively. Some commonly used notations in algorithms are listed in Table 1.

3.1. Determination of normalized principal component

The simplified concept of PCA based fusion is shown in Fig. 3. It is utilized to compute the normalized principal component as a

factor for embedding the mark information into the host media. From Fig. 3, covariance is calculated between host and mark image and then normalized principal coefficients are obtained with the help of Eigen value. The detailed step for finding the normalized principal coefficients is described in Algorithm 1.

3.2. Embedding of the mark

In this section, image normalization procedure is utilized to transform the original image, ' Org_{img} ' into normalized image, ' $Norm_{img}$ '. Further, ' $Norm_{img}$ ' and mark image, ' Wat_{img} ' are transformed using RDWT and RSVD respectively. Furthermore, PCA fusion is employed to compute the optimal embedding factor for embedding purpose. The

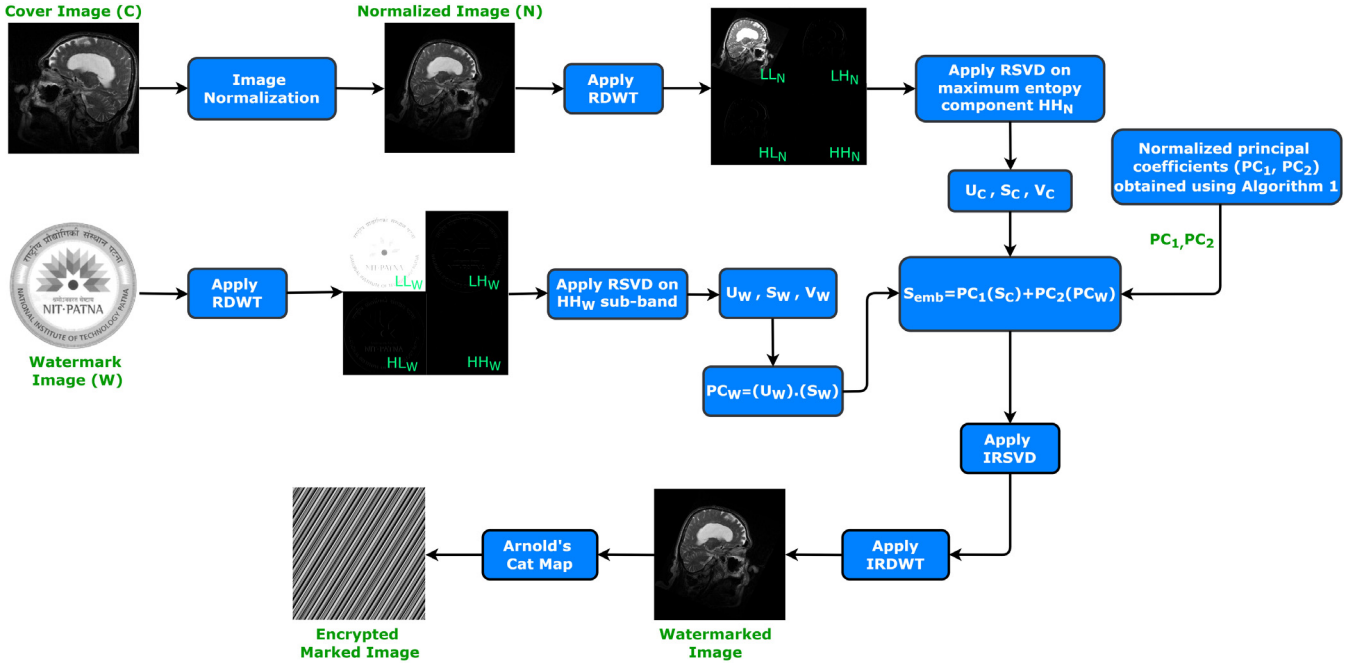


Fig. 4. The proposed watermarking framework.

Algorithm 1: Determination of principal coefficients (Org_{img} , Wat_{img})

```

Begin
1  $Org_{img} \leftarrow \text{imread}(\text{'original image'})$ ;
2  $Wat_{img} \leftarrow \text{imread}(\text{'mark image'})$ ;
3  $[A_1, B_1, C_1, D_1] \leftarrow \text{RDWT}(Org_{img}, 1, \text{'haar'})$ ;
4  $[A_2, B_2, C_2, D_2] \leftarrow \text{RDWT}(Wat_{img}, 1, \text{'haar'})$ ;
5  $[U_h, S_h, V_h] \leftarrow \text{RSVD}(D_1)$ ;
6  $[U_w, S_w, V_w] \leftarrow \text{RSVD}(D_2)$ ;
7  $\text{Cov} \leftarrow \text{covariance}(S_h, S_w)$ ;
8  $[\text{Eig}, \text{Diag}] \leftarrow \text{Eign}(\text{Cov})$ ;
9  $Z_1 \leftarrow \text{Eig}(1, 1)$ ;
10  $Z_2 \leftarrow \text{Eig}(2, 1)$ ;
11  $Z_3 \leftarrow \text{Eig}(1, 2)$ ;
12  $Z_4 \leftarrow \text{Eig}(2, 2)$ ;
13 if ( $\text{Diag}_{11} > \text{Diag}_{22}$ ) then
14    $\text{PC}_1 \leftarrow Z_1 / (Z_1 + Z_2)$ ;
15    $\text{PC}_2 \leftarrow Z_2 / (Z_1 + Z_2)$ ;
16   if ( $\text{Diag}_{22} > \text{Diag}_{11}$ ) then
17      $\text{PC}_1 \leftarrow Z_3 / (Z_3 + Z_4)$ ;
18      $\text{PC}_2 \leftarrow Z_4 / (Z_3 + Z_4)$ ;
19   end
20 end
Return  $\text{PC}_1, \text{PC}_2$ 

```

principal component of mark image is concealed inside cover image to solve the issue of FPP. Furthermore, inverse operation of RSVD and RDWT is performed to compute the marked image, ' $Mark_{img}$ '. Lastly, Arnold cat map is performed on $Mark_{img}$ to enhance the additional security of proposed scheme.

3.3. Recovery procedure of the mark

It is the just inverse procedure of embedding scheme. First, inverse Arnold cat map is performed to obtain decrypted marked image,

Algorithm 2: Watermarking Embedding (Org_{img} , Wat_{img})

```

Begin
1  $Org_{img} \leftarrow \text{imread}(\text{'original image'})$ ;
2  $Wat_{img} \leftarrow \text{imread}(\text{'mark image'})$ ;
3  $\text{Norm}_{img} \leftarrow \text{Normalization}(Org_{img})$ ;
4  $[A_1, B_1, C_1, D_1] \leftarrow \text{RDWT}(\text{Norm}_{img}, 1, \text{'haar'})$ ;
5  $[U_1, S_1, V_1] \leftarrow \text{RSVD}(D_1)$ ;
6  $[A_2, B_2, C_2, D_2] \leftarrow \text{RDWT}(Wat_{img}, 1, \text{'haar'})$ ;
7  $[U_2, S_2, V_2] \leftarrow \text{RSVD}(D_2)$ ;
8  $[\text{PC}_1, \text{PC}_2] \leftarrow \text{PCA}(S_1, S_2)$ ;
9  $S_{PC} \leftarrow U_2 \times S_2$ ;
10  $S_{emb} \leftarrow \text{Modi\_Singular}(\text{PC}_1 \times S_1 + \text{PC}_2 \times S_{PC})$ ;
11  $D_{new} \leftarrow \text{IRSVD}(U_1 \times S_{emb} \times (V_1)^T)$ ;
12  $\text{Mark}_{img} \leftarrow \text{IRDWT}(A_1, B_1, C_1, D_{new}, 1, \text{'haar'})$ ;
13  $\text{Enc\_Mark}_{img} \leftarrow \text{Arnold cat map}(\text{Mark}_{img})$ ;
Return  $\text{Enc\_Mark}_{img}$ 

```

Algorithm 3: Watermarking Extraction (Enc_Mark_{img} , PC_1, PC_2)

```

Begin
1  $\text{Enc\_Mark\_Eng} \leftarrow \text{imread}(\text{'enc\_marked image'})$ ;
2  $\text{Dec\_Mark}_{img} \leftarrow \text{Inverse\_Arnold}(\text{Enc\_Mark}_{img})$ ;
3  $[A_3, B_3, C_3, D_3] \leftarrow \text{RDWT}(\text{Dec\_Mark}_{img}, 1, \text{'haar'})$ ;
4  $[U_3, S_3, V_3] \leftarrow \text{RSVD}(D_3)$ ;
5  $\text{Ext}_{pc} \leftarrow \text{Ext\_Singular}(1/\text{PC}_2 \times (S_3 - \text{PC}_1 \times S_2))$ ;
6  $D_{mod} \leftarrow \text{IRSVD}(\text{Ext}_{pc} \times (V_2)^T)$ ;
7  $\text{Rec\_Wat}_{img} \leftarrow \text{IRDWT}(A_2, B_2, C_2, D_{mod}, \text{'haar'})$ ;
Return  $\text{Rec\_Wat}_{img}$ 

```

' Dec_Mark_{img} ' and then it is transformed using RDWT and RSVD. Further, singular value is extracted using PCA fusion. Lastly, the mark image is recovered by applying the inverse of RSVD and IDWT respectively.

Table 2

Computation of NPC score for embedding purpose.

NPC	Covid-1	Covid-2	Covid-3	Covid-4	Covid-5
PC_1	0.6193	0.5682	0.7189	0.8186	0.7170
PC_2	0.3807	0.4318	0.2811	0.1814	0.2830

Table 3

Performance analysis of proposed scheme on two different datasets.

Database	Cover image	Mark image	PSNR	SSIM	NC
COVID_19 Dataset	Covid-1	WM1	59.0432	0.9995	1.0000
	Covid-2	WM1	57.6656	0.9992	1.0000
	Covid-3	WM1	63.9822	0.9998	1.0000
	Covid-4	WM1	57.0695	0.9994	1.0000
	Covid-5	WM1	57.4242	0.9992	0.9998
	Covid-6	WM1	53.9216	0.9979	1.0000
	Covid-7	WM1	59.3445	0.9996	1.0000
	Covid-8	WM1	58.3692	0.9994	1.0000
	Covid-9	WM1	59.5596	0.9996	1.0000
	Covid-10	WM1	61.0891	0.9997	1.0000
Mean (COVID_19 Dataset)			58.8718	0.9993	0.9999
SIPI-USC Dataset	Sailboat	WM2	55.2356	0.9997	0.9996
	Barbara	WM2	53.2807	0.9995	0.9995
	Airplane	WM2	57.6960	0.9996	0.9999
	Boat	WM2	54.4618	0.9995	0.9999
	Peppers	WM2	56.8292	0.9996	0.9999
	Crowd	WM2	58.3993	0.9997	1.0000
	Gold-hill	WM2	55.9361	0.9995	0.9998
	Brain	WM2	57.1768	0.9993	1.0000
	Couple	WM2	56.0686	0.9994	0.9999
	Elaine	WM2	56.9093	0.9994	0.9999
Mean (SIPI-USC Dataset)			56.2034	0.9992	0.9998

4. Experimental analysis

To verify the effectiveness of the proposed SecDH scheme, this section puts forward the results obtained from a series of different tests challenging the robustness, and imperceptibility. It also includes the comparative discussion on the basis of resistance ability against different geometric and non-geometric attacks. The SecDH scheme is implemented MATLAB 2019b in a system with windows 11 operating system, 8 GB of RAM, and core i7 processor. The standard medical images are considered from the different standard datasets, namely COVID-19 [23], and SIPI-USC [24], of size 512×512 as

Table 4

Robustness comparison against various attacks.

Attacks	Noise density	SecDH	[10]	[11]	[12]	[13]	[14]	[15]
Salt and pepper noise	0.001	1.0000	0.9981	0.9251	0.9986	0.9722	–	0.9362
	0.005	0.9997	0.9846	–	–	–	0.9007	0.9364
	0.01	0.9993	0.9599	–	0.9274	0.9144	0.9929	0.9366
Speckle noise	0.001	1.0000	0.9995	0.9800	0.9984	0.9847	0.9953	0.9360
	0.005	0.9997	0.9985	0.9014	–	–	–	0.9360
	0.01	0.9994	0.9868	–	0.9362	–	0.9738	–
Gaussian noise	0.001	0.9999	0.9920	–	0.9934	–	0.8122	–
	0.01	0.9982	0.9655	–	–	–	0.8163	0.9621
Median filter	[1 1]	1.0000	–	0.9819	1.0000	0.9997	–	0.9995
	[2 2]	1.0000	0.7549	0.9457	0.9859	0.9880	0.7361	0.9950
	[3 3]	1.0000	0.7341	–	–	–	0.6985	0.9948
JPEG	10	1.0000	0.9391	0.8952	0.9961	0.9111	0.7972	0.9950
	50	1.0000	0.9825	0.9510	0.9993	0.9947	0.8411	0.9978
	90	1.0000	0.9955	0.9809	0.9996	0.9963	0.9811	0.9989
Rotation	5	1.0000	0.7849	–	–	–	–	–
	1	1.0000	–	0.8817	–	0.9997	–	–
Image scaling	0.5	1.0000	0.7185	–	–	–	–	–
	2	1.0000	0.9245	0.7157	–	0.5216	–	–
Cropping	[20 20 400 480]	1.0000	0.7842	0.5082	–	0.7941	0.8237	–
Sharpening	0.1	1.0000	0.8716	0.6763	1.0000	0.9599	0.9776	–
Histogram equalization		1.0000	0.5650	0.8716	0.6383	0.6797	0.9113	0.9832

cover image. NITP logo and cameraman image are considered as mark image with the size of 512×512 for embedding purpose. The visual quality of the suggested method is measured in terms of PSNR and SSIM [11]. Also, NC scores verify the robustness [12]. The computation of embedding factor plays significant role in embedding and extraction procedure in watermarking scheme. Hence, proposed method computes normalized principal component (NPC) for embedding and extraction purpose which maintains the good relationship between the robustness and invisibility performance. In our experiments, normalized principal components are computed between singular value of host and mark image, which produces the embedding factors as ' PC_1 ' and ' PC_2 '. The computation of NPC score for different host images are listed in Table 2.

The performance analysis of proposed method is computed in terms of PSNR, SSIM, and NC score for two different datasets, which is listed in Table 3. According to this table, it can be noticed that average value of PSNR and SSIM obtained as 58.7818 dB and 0.9993 respectively for COVID-19 dataset [23]. The average value of PSNR and SSIM obtained as 56.2034 dB and 0.9992, respectively for SIPI-USC dataset [24]. Hence, it shows better visual quality for different marked image. The average NC score are approaching one for both datasets, which indicates high robustness. From this table, it can be observed that our scheme provides the good trade-off among robustness and visual quality.

Table 4 shows the comparison outcomes of NC values of the proposed approach and the tradition schemes [10–15] in the cases of various attacks. In case of JPEG compression, NC score is approaching '1' for different quality factor, which indicates the compression strength. In salt and pepper and speckle noise, NCs score are greater than 0.9993 and 0.9994, respectively. The NC score is greater than 0.9982 against the Gaussian noise. In median filter, NC score is approaching '1' for different window size. The robustness performance of our scheme is ideal, i.e. 1, against the considered geometric attacks such as rotation, scaling, and cropping. Hence, our scheme is more robust against wide range of attacks.

Robustness analysis of the proposed work is tested using two different mark images and their results are summarized in Fig. 5. From this Figure, it can be remarked that quality of recover mark images are acceptable against the mentioned attacks. Further, we have compared the various parameters of our proposed SecDH scheme and the other schemes models [10–14] in Table 5. According this table, it can be noticed that our scheme delivers better payload capacity as compared to mentioned scheme. From the Table it can be summarized that the

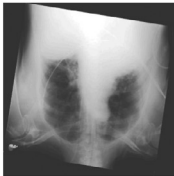


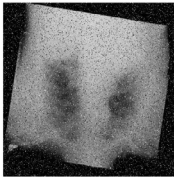





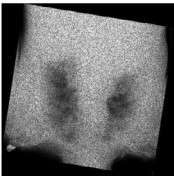


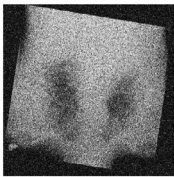


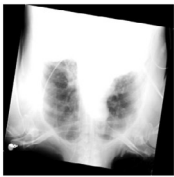


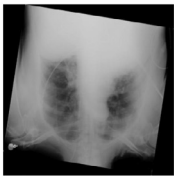


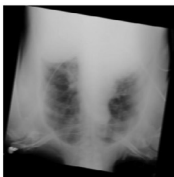


Attacks	Distorted Marked Image	Recovered Watermark (WM1)	Recovered Watermark (WM2)
Histogram Equalization			
Salt and Pepper noise (0.1)			
Sharpening Mask attack (0.1)			
Speckle noise (0.1)			
Gaussian noise (0.1)			
Scaling (1.5)			
Gaussian low pass filter (0.1)			
Motion Blur attack			

Fig. 5. Robustness analysis against various attacks.

execution time is very less as compared to the most of the scheme. Due to the use of NPC, it is very clear the robustness and visual quality of the proposed technique is quite balanced which is better than some traditional schemes [11–13]. Lastly, our technique provides a solution

for FPP. However, the schemes proposed in [10–14] did not address this major issue with SVD based watermarking. The robustness analysis of proposed work against various density of salt and pepper, speckle, Gaussian noise is shown in Figs. 6 to 8. After

Attacks	Distorted Marked Image	Recovered Watermark (WM1)	Recovered Watermark (WM2)
Median filter [3 3]			
Average filter [3 3]			
Poisson noise			
JPEG (QF=90)			
Rotation (5°)			
Cropping (1/16)			
Cropping (1/4)			
Cropping (1/2)			

Fig. 5. (continued).

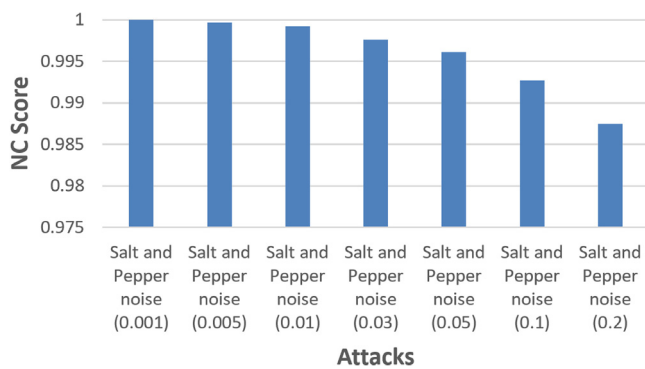
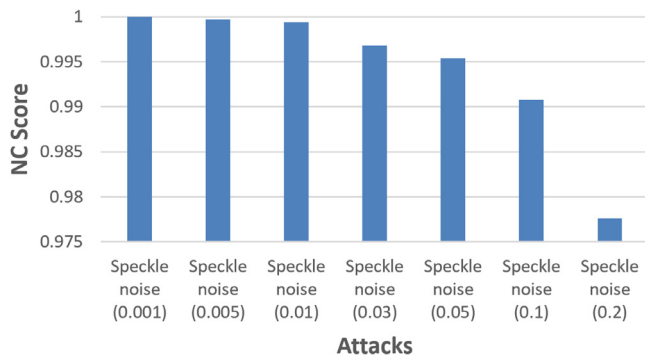
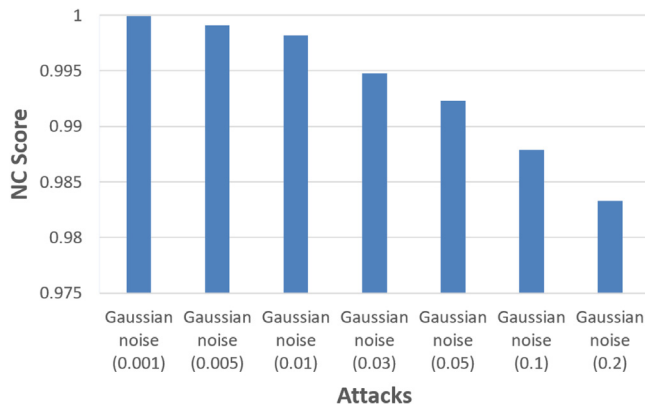
that, Fig. 9 contains the robustness score against median filter with different window size. Hence, proposed work shows better resistance against various attacks. Further, robustness score of our scheme is tested against hybrid attacks and it is recorded in Table 6. From

this table, it can be noticed that our scheme offered better results in terms of robustness against mentioned attacks. The overall results and discussion indicate that the proposed SecDH scheme is suitable for secure and smart healthcare applications.

Table 5

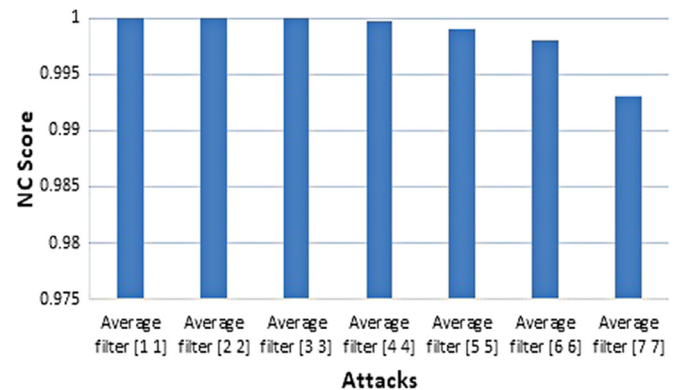
Comparative analysis of proposed SecDH with recent state of art techniques.

Parameters		SecDH	[10]	[11]	[12]	[13]	[14]
PSNR		63.9822	45.5891	44.1944	37.6912	49.8855	55.1471
SSIM		0.9998	0.9961	0.9913	0.9994	0.9959	–
NC (without attack)		1.0000	0.9985	0.9911	1.0000	0.9997	0.9956
Size	cover	512×512	512×512	512×512	512×512	512×512	512×512
	mark	512×512	256×256	256×256	256×256	256×256	256×256
Payload (bit/pixel)		1.0000	0.2504	0.2500	0.2500	0.2500	0.2500
Time complexity	Embedding	0.3244	0.2576	–	–	0.4462	–
	Extraction	0.1176	0.1588	–	–	0.3035	–
	Encryption	0.3222	1.3122	–	–	0.2444	–
	Decryption	0.2859	0.3397	–	–	0.0032	–
Techniques		RDWT, RSVD	RDWT, RSVD	DWT, SVD	LWT, HD, and RSVD	IWT, Schur, RSVD	DWT, HD, SVD
Soft computing approach		PCA	PSO, FA	–	–	Fuzzy Logic	HPSO
Scaling factor		Optimal	Optimal	Manual	Manual	Optimal	Optimal
False positive problem		No	Yes	Yes	Yes	Yes	Yes
Security		Arnold cat map	Linear chaotic map	Hyper chaotic map	Chaotic map	Chaotic map	Selective encryption
Application		E-healthcare	E-healthcare	Tele-health	Multimedia	E-healthcare	Landslide Images

**Fig. 6.** Robustness analysis against salt and pepper noise.**Fig. 7.** Robustness analysis against speckle noise.**Fig. 8.** Robustness analysis against Gaussian noise.**Table 6**

Robustness score against hybrid attacks.

Attacks	SecDH	[25]
Salt and Pepper noise (0.02) + rotation (1)	0.9994	0.9715
Gaussian noise (0.02) + rotation (5)	0.9980	–
JPEG (QF=30) + rotation (1)	1.0000	0.9245
Speckle noise (0.02) + Scaling (0.25)	0.9994	–
JPEG (QF=90) + Scaling (1.5)	1.0000	–
Gaussian noise(0.01) + Cropping (0.25)	0.9967	0.9088
Salt and Pepper noise (0.1) + Scaling (0.25)	0.9992	0.9588
JPEG (QF=90) + Scaling (400)	0.9985	0.9855
Histogram Equalization + rotation (90)	0.9999	–
Sharpening (0.01) + Cropping (0.25)	1.0000	–
Salt and Pepper noise (0.02) + Cropping (0.25)	0.9973	0.9715
Gaussian noise(0.1) + rotation (45)	0.9975	–
Poisson Noise+ Cropping (0.25)	0.9999	–

**Fig. 9.** Robustness analysis against Average filter.

5. Conclusion

In this paper, we developed SecDH as PCA-based medical data hiding scheme to solve the problem of copyright violation of COVID-19 images for healthcare applications. In preprocessing stage, image normalization procedure is employed on host image to enhance the robustness of proposed scheme against the geometric attacks. Further, proposed scheme utilizes the integration of RDWT and RSVD, which offers better visual quality with improved embedding capacity at low cost. Furthermore, PCA is utilized to determine the normalized principal component for embedding purpose, which maintains the balanced trade-off between robustness and imperceptibility of proposed scheme. Additionally, the principal component of mark image is hidden in the

host image, which solves the FPP issue. Finally, Arnold cat map encryption is then employed in the marked image to generate encrypted form of image for additional security before transmission and outsourced to the cloud for convenient use. According to the experimental results, the proposed solution achieves better performance of perceptual robustness than six state-of-the-art methods on different parameters and attacks. Our future work is to study the medical data security solution for video applications.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is supported by research project order no. IES\R2\212111 - International Exchanges 2021 Round 2, dt. 28 February, 2022, under Royal Society, UK. All authors approved the version of the manuscript to be published.

References

- [1] A. Singh, A. Anand, Z. Lv, H. Ko, A. Mohan, A survey on healthcare data: a security perspective, *ACM Trans. Multimedia Comput. Commun. Appl.* 17 (2s) (2021) 1–26.
- [2] K. Amine, K. Fares, K.M. Redouane, E. Salah, Medical image watermarking for telemedicine application security, *J. Circuits Syst. Comput.* 31 (05) (2022) 2250097.
- [3] N. Sharma, O.P. Singh, A. Anand, A.K. Singh, Improved method of optimization-based ECG signal watermarking, *J. Electron. Imaging* 31 (4) (2021) 041207.
- [4] K. Swaraja, K. Meenakshi, P. Kora, Hierarchical multilevel framework using RDWT-QR optimized watermarking in telemedicine, *Biomed. Signal Process. Control* 68 (2021) 102688.
- [5] K. Swaraja, K. Meenakshi, P. Kora, An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine, *Biomed. Signal Process. Control* 55 (2020) 101665.
- [6] M.S. Rahman, I. Khalil, X. Yi, A lossless DNA data hiding approach for data authenticity in mobile cloud based healthcare systems, *Int. J. Inf. Manage.* 45 (2019) 276–288.
- [7] X.-L. Liu, C.-C. Lin, S.-M. Yuan, Blind dual watermarking for color images' authentication and copyright protection, *IEEE Trans. Circuits Syst. Video Technol.* 28 (5) (2016) 1047–1055.
- [8] O.P. Singh, A. Singh, G. Srivastava, N. Kumar, Image watermarking using soft computing techniques: A comprehensive survey, *Multimedia Tools Appl.* 80 (20) (2021) 30367–30398.
- [9] B.B. Haghighi, A.H. Taherinia, A. Harati, M. Rouhani, WSMN: An optimized multipurpose blind watermarking in Shearlet domain using MLP and NSGA-II, *Appl. Soft Comput.* 101 (2021) 107029.
- [10] A. Anand, A.K. Singh, Hybrid nature-inspired optimization and encryption-based watermarking for E-healthcare, *IEEE Trans. Comput. Soc. Syst.* (2022).
- [11] A. Anand, A.K. Singh, An improved DWT-SVD domain watermarking for medical information security, *Comput. Commun.* 152 (2020) 72–80.
- [12] O. Singh, A. Singh, Data hiding in encryption–compression domain, *Complex Intell. Syst.* (2021) 1–14.
- [13] A. Anand, A.K. Singh, Cloud based secure watermarking using IWT-schur-RSVD with fuzzy inference system for smart healthcare applications, *Sustainable Cities Soc.* 75 (2021) 103398.
- [14] A. Mohan, A. Anand, A. Singh, R. Dwivedi, B. Kumar, Selective encryption and optimization based watermarking for robust transmission of landslide images, *Comput. Electr. Eng.* 95 (2021) 107385.
- [15] O. Singh, A. Singh, A robust information hiding algorithm based on lossless encryption and NSCT-HD-SVD, *Mach. Vis. Appl.* 32 (4) (2021) 1–13.
- [16] E.E.-D. Hemdan, An efficient and robust watermarking approach based on single value decomposition, multi-level DWT, and wavelet fusion with scrambled medical images, *Multimedia Tools Appl.* 80 (2) (2021) 1749–1777.
- [17] I.A. Ansari, M. Pant, C.W. Ahn, Robust and false positive free watermarking in IWT domain using SVD and ABC, *Eng. Appl. Artif. Intell.* 49 (2016) 114–125.
- [18] S.P. Singh, G. Bhatnagar, A robust image hashing based on discrete wavelet transform, in: 2017 IEEE International Conference on Signal and Image Processing Applications, ICSIPA, IEEE, 2017, pp. 440–444.
- [19] O.P. Singh, C. Kumar, A.K. Singh, M.P. Singh, H. Ko, Fuzzy-based secure exchange of digital data using watermarking in NSCT-RDWT-SVD domain, *Concurr. Comput.: Pract. Exper.* (2021) e6251.
- [20] A. Anand, A.K. Singh, RDWT-SVD-firefly based dual watermarking technique for medical images (workshop paper), in: 2020 IEEE Sixth International Conference on Multimedia Big Data, BigMM, IEEE, 2020, pp. 366–372.
- [21] H. Khalilian, I.V. Bajic, Video watermarking with empirical PCA-based decoding, *IEEE Trans. Image Process.* 22 (12) (2013) 4825–4840.
- [22] M. Li, T. Liang, Y.-j. He, Arnold transform based image scrambling method, in: 3rd International Conference on Multimedia Technology, 2013, pp. 1309–1316.
- [23] T. Rahman, Covid-19 radiography database, 2021, Kaggle, URL <https://www.kaggle.com/tawsifurrahman/covid19-radiography-database>.
- [24] Sipi Image Database, URL <https://sipi.usc.edu/database/database.php?volume=misc>,
- [25] A.M. Cheema, S.M. Adnan, Z. Mehmood, A novel optimized semi-blind scheme for color image watermarking, *IEEE Access* 8 (2020) 169525–169547.