



# A robust information hiding algorithm based on lossless encryption and NSCT-HD-SVD

O. P. Singh<sup>1</sup> · A. K. Singh<sup>1</sup>

Received: 14 March 2021 / Revised: 24 May 2021 / Accepted: 10 June 2021 / Published online: 1 July 2021  
© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2021

## Abstract

Aiming at the problem of the security of secret information in various potential applications, we introduce a robust information hiding algorithm based on lossless encryption, non-subsampled contourlet transform (NSCT), Hessen-berg decomposition (HD) and singular value decomposition (SVD). Firstly, the carrier and secret mark information is transformed by NSCT-HD-SVD. Secondly, the singular score of secret media information is concealed in the carrier image. Thirdly, the text document is further concealed in the carrier marked image via pseudo magic cubes to achieve the final carrier marked image. Finally, the lossless encryption scheme is utilized to encrypt the final marked image. The simulation results of the proposed algorithm indicate good invisibility and robustness effect compared to existing schemes with high security and hiding efficiency. It indicates a considerable improvement in robustness of up to 96.36% over other schemes. Overall, the proposed algorithm for various images, achieved peak signal-to-noise ratio (PSNR), normalized correlation (NC), structural similarity index (SSIM), number of changing pixel rate (NPCR) and unified averaged changed intensity (UACI) of up to 67.36 dB, 0.9996, 1.0000, 0.9964 and 0.4005, respectively, indicating its effectiveness for secure media applications.

**Keywords** Data hiding · Encryption · Contourlet Transform · Hessen-berg · SVD

## 1 Introduction

With the advancement of internet technologies, an increasing amount of media data is easily distributed, stored and shared on different social media and other platforms such as LinkedIn, Facebook, Twitter and Flickr [1]. Using digital images is a most common way to share such data over these popular platforms. Sharing of such images might bring issues of privacy leakage, copyright protection, identity theft and the data tampered by any intruder [2, 3]. Therefore, protection of such images has attracted considerable attention for different research community. To overcome such issues, data hiding scheme is widely adopted in the past few years to protect the media content by invisibly concealing secret mark (s) into host media for copy-protection purpose [4]. Watermarking and steganography are the main branch of

data hiding scheme. Among the schemes, digital watermarking is widely and actively used method [5]. The research of watermarking scheme is mainly to improve performances in context to the invisibility, embedding capacity and robustness, which is difficult to balance the tradeoff among these performances [2]. According to the operations domains, the watermarking approaches include two significant domains, i.e., spatial and transform [6]. Compared with the spatial-domain scheme, the transform domain-based watermarking schemes are more robust in nature [7].

Considering the advantages and limitations of a single type of domain-based method, this paper introduces a hybrid of spatial and transform-based dual watermarking algorithm. The contributions of this work are as follows:

- Invisible and robust hiding scheme with high hiding efficiency: The proposed scheme uses fusion of NSCT-HD-SVD [8, 9], which is improving the robustness. The proposed scheme is further improving the embedding capacity by means of pseudo magic cubes [10], so as to avoid the increase in distortion caused by large-capacity embedding.

✉ A. K. Singh  
amit.singh@nitp.ac.in

O. P. Singh  
omprakash7667@gmail.com

<sup>1</sup> Deptt. of CSE, NIT Patna, Bihar, India

- Enhanced security via dual marking and encryption: Dual marks are concealed into the cover media to ensure the copy-protection and content security at the same time. Further, fusion of DNA computing, chaotic and hash function-based encryption scheme [11] provides the additional security of our scheme.
- Enhanced robustness: The simulation results of the proposed algorithm indicate good robustness effect compared to existing schemes with high security and hiding efficiency.

The remaining chapter is ordered as follows: Sect. 2 gives the relevant works. Section 3 gives the detailed design of the proposed scheme, followed by result analysis in Sect. 4. The work summary along with future directions is presented in Sect. 5.

## 2 Literature survey

Some related works are briefly described in this section.

Kazemi et.al developed a watermarking algorithm utilized neural network model in the NSCT-domain [12]. Firstly, cover image is transformed using NSCT, and appropriate coefficients are chosen by means of Kurtosis. The method uses genetic algorithm to get the optimum embedding strength, and perceptron neural network is performed at extraction procedure to obtain recovered logo image. Although the method is robust, it required more time to perform training data sets. Thakur et al. [13] designed an improved algorithm, which can invisibly embed dual marks in NSCT-RDWT-SVD domain. Further, chaotic encryption is applied on marked image to ensure confidentiality of the media data.

Ali et.al [14] introduced a PSO-based scheme in NSCT-SWT-SVD domain. In this approach, NSCT decomposed host image into lower frequency and directional coefficient. However, SWT and SVD performed on NSCT coefficient of host image. The embedding factor of this scheme is optimized through PSO scheme optimized by neural networks. In the blind watermarking scheme proposed by Li and Zhang [15], scrambled mark is embedded into carrier image using NSCT and Schur. Although method is invisible and robust, it doesn't provide better performance against few attacks such as scaling and low pass filtering. Su et.al [16] designed a blind watermarking using NSCT and HD and included a hash algorithm to randomly select the block for embedding binary mark purpose. A watermarking algorithm is introduced for offering the authenticity of digital data in [17]. In embedding part, multiple marks are embedded into cover image through NSCT, RDWT and SVD. After that, marked image is encrypted and compressed to increase the security

and reduce bandwidth utilization, respectively. In Ref [18], author discussed a watermarking algorithm using transformed schemes and included wavelet-based compression to reduce the bandwidth utilization. This method increased the security by using dual watermarking and scrambled the signature mark. A robust watermarking scheme has been developed for 3D images in ref [19]. In preprocessing part, cover image is transformed into YUV channel, and sub-block division is performed on Y-component. After that, 3rd level of NSCT is utilized on designated sub-block of cover image. The scrambled mark is placed in the appropriate NSCT cover. Vaidya et.al [20], have introduced a multi-decomposition-based watermarking approach is proposed for copy-protection of color media. Initially, DWT adopted on 'Y' part of host media. After that 'LL' band is transformed using CT, Schur and SVD. Thereafter, encrypted mark image is concealed in the transformed coefficient of host. To provide the solution of false positive problem, authors have introduced a multi-scale watermarking scheme through IWT and SVD [21]. Objective Evaluation Function (OEF) is applied to provide solution of false positive problem. An optimal factor is obtained by using optimal mapping scheme to balance the tradeoff among watermarking performances. The various NSCT-based watermarking schemes and their limitations are depicted in Table 1.

## 3 Proposed method

This section provides the detailed description of the proposed algorithm (See Fig. 1). It is divided into different procedures: (a) the mark embedding, (b) marked encryption and (c) recovery. Initially, sub-sampling process is employed to obtain sub-component of cover image. Further, the multiple decomposition (NSCT-HD-SVD) is performed on maximum entropy component of cover image. Similarly, mark image is also transformed. After that, mark image is concealed into singular vector of cover image with the help of appropriate embedding factor to obtain marked image. However, text mark and hash value of cover image are also embedded into the marked image using pseudo magic cubes to obtain final marked image. The fusion of DNA computing, chaotic and hash function-based encryption scheme on marked data provides the additional security of our scheme. Finally, the inverse steps of embedding process are performed to obtain extracted mark image. The process of lossless encryption procedure of the marked data can be seen in Fig. 2. The detail description of embedding procedure, encryption scheme and recovery procedure are presented below in Algorithm 1–3, respectively. Notation and its description used in Algorithm 1 to 3 are depicted below in Table 2.

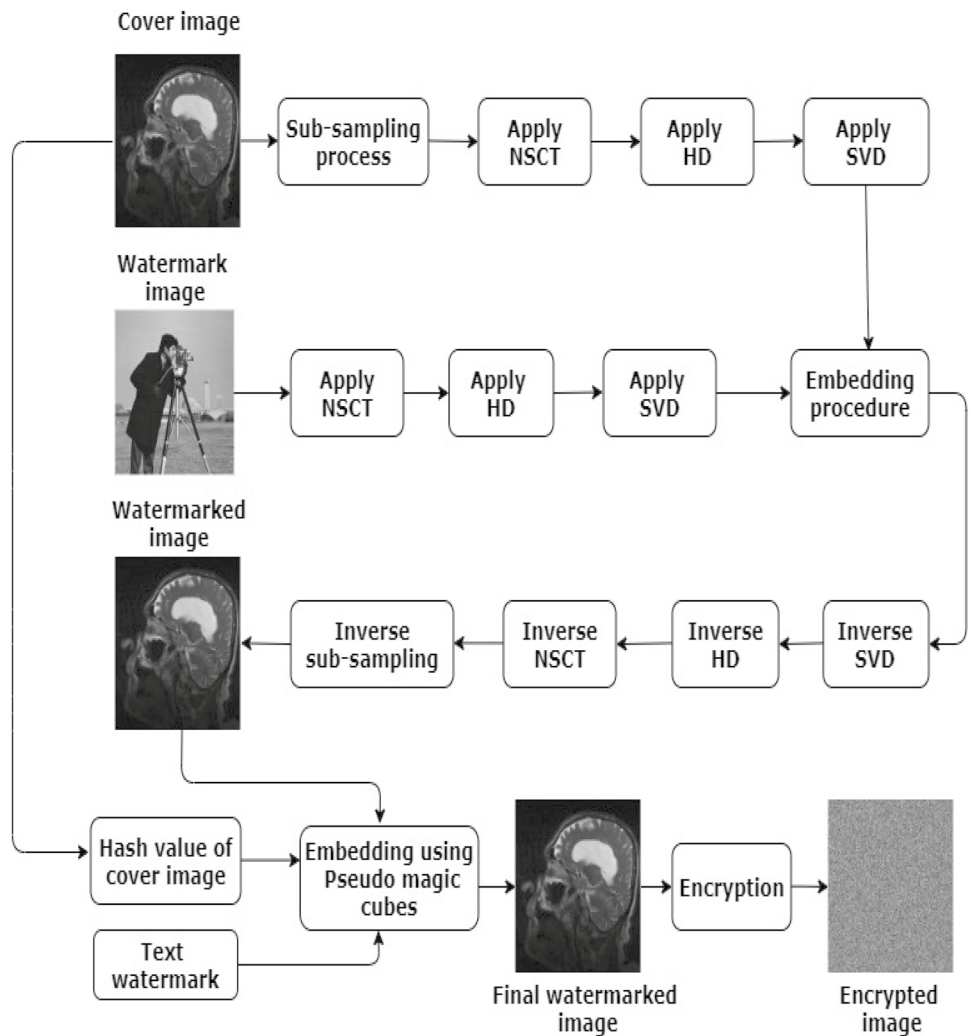
**Algorithm 1: Embedding Procedure ( $Cov_{img}, \delta, W_{img}, Text_{wat}, N, R_{seed}, [R_x, R_y, R_z]$ )****Begin**

1.  $C_1 \leftarrow \text{zeros}(256)$ ;  $C_2 \leftarrow \text{zeros}(256)$ ;  $C_3 \leftarrow \text{zeros}(256)$ ;  $C_4 \leftarrow \text{zeros}(256)$ ;
2. **for**  $a \leftarrow 1:256$  **do**
3.   **for**  $b \leftarrow 1:256$  **do**
4.      $C_1(a, b) \leftarrow Cov_{img}(2 \times a - 1, 2 \times b - 1)$ ;  $C_2(a, b) \leftarrow Cov_{img}(2 \times a - 1, 2 \times b)$ ;
5.      $C_3(a, b) \leftarrow Cov_{img}(2 \times a, 2 \times b - 1)$ ;  $C_4(a, b) \leftarrow Cov_{img}(2 \times a, 2 \times b)$ ;
6.   **end for**
7. **end for**
8.  $E_1 \leftarrow Entropy(C_1)$ ;  $E_2 \leftarrow Entropy(C_2)$ ;  $E_3 \leftarrow Entropy(C_3)$ ;  $E_4 \leftarrow Entropy(C_4)$ ;
9.  $comp \leftarrow Max^m(E_1, E_2, E_3, E_4)$ ;
10.  $[NS_1, NS_2, NS_{31}, NS_{32}, NS_{41}, NS_{42}] \leftarrow NSCT(comp)$ ;
11.  $[P, H] \leftarrow hess(NS_{42})$ ;
12.  $[U, S, V] \leftarrow SVD(H)$ ;
13.  $[NS_{w1}, NS_{w2}, NS_{w31}, NS_{w32}, NS_{w41}, NS_{w42}] \leftarrow NSCT(W_{img})$ ;
14.  $[P_w, H_w] \leftarrow hess(NS_{w42})$ ;
15.  $[U_w, S_w, V_w] \leftarrow SVD(H_w)$ ;
16.  $S_1 \leftarrow S + \delta \times S_w$ ;
17.  $W_1 \leftarrow U \times S_1 \times (V)^T$ ;
18.  $W_2 \leftarrow P \times W_1 \times (P)^T$ ;
19.  $W_{comp} \leftarrow INSC(T(NS_1, NS_2, NS_{31}, NS_{32}, NS_{41}, W_2))$ ;
20. **for**  $a \leftarrow 1:256$  **do**
21.   **for**  $b \leftarrow 1:256$  **do**
22.      $Wat_{ed}(2 \times a - 1, 2 \times b - 1) \leftarrow C_1(a, b)$ ;  $Wat_{ed}(2 \times a - 1, 2 \times b) \leftarrow C_1(a, b)$ ;
23.      $Wat_{ed}(2 \times a, 2 \times b - 1) \leftarrow C_1(a, b)$ ;  $Wat_{ed}(2 \times a, 2 \times b) \leftarrow W_{comp}(a, b)$ ;
24.   **end for**
25. **end for**
26.  $Wat_{img} \leftarrow Wat_{ed}$ ;
27.  $hash_{val} \leftarrow HashFunction(Cov_{img})$ ;
28.  $finalwat_{text} \leftarrow TextAppend(hash_{val}, Text_{wat}, Wat_{img})$ ;
29.  $dec_{wat} \leftarrow Char2Decimal(finalwat_{text})$ ;
30.  $MC \leftarrow MagicCube(N, [R_x, R_y, R_z])$ ;
31.  $Rand_{seq} \leftarrow RandomSequence(R_{seed})$ ;
32.  $b \leftarrow 1$ ;
33. **for**  $i \leftarrow 1:Length(dec_{wat})$  **do**
34.    $m \leftarrow dec_{wat}[i]$ ;
35.    $X \leftarrow Wat_{img}[Rand_{seq}[b]]$ ;
36.    $Y \leftarrow Wat_{img}[Rand_{seq}[b + 1]]$ ;
37.    $Z \leftarrow Wat_{img}[Rand_{seq}[b + 2]]$ ;
38.    $[X_1, X_2, X_3] \leftarrow EmbeddingMCF(X, Y, Z, m, MC)$ ;
39.    $Final_{img}[Rand_{seq}[b]] \leftarrow X_1$ ;
40.    $Final_{img}[Rand_{seq}[b + 1]] \leftarrow X_2$ ;
41.    $Final_{img}[Rand_{seq}[b + 2]] \leftarrow X_3$ ;
42.    $b \leftarrow b + 3$ ;
43. **endfor**
44. Return **Final<sub>img</sub>**

**Table 1** Various NSCT-based watermarking schemes and their limitations

Watermarking schemes	Limitations
Neural network-based watermarking method in NSCT-domain [12]	It required more time to perform training on data sets
Dual watermarking approach via NSCT-RDWT-SVD [13]	This scheme designed for medical images only
NSCT-RDWT-based watermarking scheme via PSO-GA-AI [14]	High cost
Blind watermarking scheme based on Schur and NSCT [15]	The performance of this scheme did not offer better result against scaling and low pass filtering
Blind watermarking in HD-Contourlet transform domain [16]	It does not resist against rotation attacks
Joint use of encryption-compression in watermarking domain [17]	This method can be examined result for color image also
A dual watermarking algorithm through NSCT-RDWT-SVD[18]	The computational cost of this scheme can be further reduced
NSCT-based watermarking scheme for 3D images [19]	This scheme can be further improved through selecting optimal embedding factor
Multi-decomposition-based watermarking approach [20]	Apply some metaheuristic approach to obtain the optimal scaling factor for embedding purpose
Optimization-based watermarking approach using IWT and SVD[21]	This scheme is tested on few gray scale image only

**Fig. 1** The proposed algorithm



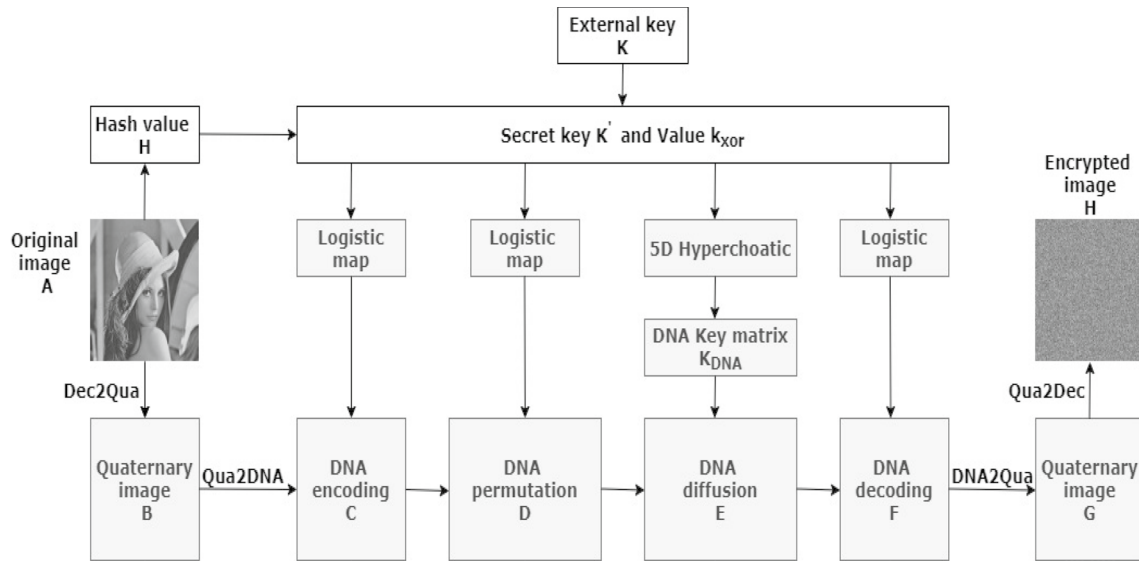


Fig. 2 Flowchart diagram of encryption scheme [11]

Table 2 Notations and its descriptions

Notation	Description	Notation	Description
$Cov_{img}$	Host image	$Rand_{seq}$	Random sequence
$W_{img}$	Mark image	N	Order of magic cube
$\Delta$	Scaling factor	$Final_{img}$	Final marked image
$Wat_{img}$	Watermarked image	$Key_{hex}$	External key
$C_1, C_2, C_3, C_4$	Sub-part of cover image	$Enc_{img}$	Encrypted image
$T_1, T_2, T_3, T_4$	Entropy of sub-part of host image	A, B	Size of row and column of final marked image
comp	Maximum entropy of sub-part image	$H_{value}, K_{xor}$	Hash and key value of final marked image
$NS_{1}, NS_{2}$	Lower NSCT sub-band of host image	$Key'$	Secret key
$NS_{3\_1}, NS_{3\_2}, NS_{4\_1}, NS_{4\_2}$	Higher frequency NSCT sub-band of host image	$Key_{dec}$	Decimal key
P, H	Orthogonal and Hessen-berg matrix of host image	$Key_{fea}$	Key feature
U, S	Orthogonal matrix of host image	$Qua_{img}$	Quaternary image
V	Diagonal matrix of host image	$PerDNA_{img}$	Permutated DNA image
$NS_{w1}, NS_{w2}$	Lower frequency NSCT sub-band of mark image	$KeyDNA_{img}$	Key DNA image
$NS_{w3\_1}, NS_{w3\_2}, NS_{w4\_1}, NS_{w4\_2}$	Higher frequency NSCT sub-band of mark image	$DifDNA_{img}$	Diffused DNA image
$P_w, H_w$	Orthogonal and Hessen-berg matrix of mark image	$EncDNA_{img}$	Encrypted DNA image
$U_w, S_w$	Orthogonal matrix of mark image	$EncQua_{img}$	Encrypted Quaternary image
$V_w$	Diagonal matrix of mark image	$D_1, D_2, D_3, D_4$	Sub-part of decrypted image
$S_1$	Modified singular value of marked image	$A_1, A_2, A_3, A_4$	Entropy of sub-part decrypted image
$Text_{wat}$	Text watermark	G	Maximum entropy of sub-part of decrypted image
$Final_{img}$	Final marked image	$G_1, G_2$	Lower frequency NSCT sub-band of decrypted image
$R_{seed}$	Random seed	$G_{11}, G_{12}, G_{21}, G_{22}$	Higher frequency NSCT sub-band of decrypted image
$R_x, R_y, R_z$	Rolling axes	$H_{w1}, P_{w1}$	Orthogonal and Hessen-berg matrix of decrypted image
$hash_{val}$	Hash value of marked image	$U_{w1}, S_{w1}$	Orthogonal matrix of decrypted image
$finalwat_{text}$	Final watermarked text	$V_{w1}$	Diagonal matrix of decrypted image
$dec_{wat}$	Decimal value of text watermark	$Rec_{wat}$	Recovered watermark
MC	Magic cube	$Rec_{text}$	Recovered text

**Algorithm 2: Encryption procedure**(Final<sub>img</sub>, Key<sub>hex</sub>)**Begin**

1. [A, B] ← size(Final<sub>img</sub>);
  2. [H<sub>value</sub>, K<sub>xor</sub>] ← HashFunction(Final<sub>img</sub>, MD5);
  3. Key' ← bitxor(H<sub>value</sub>, Key<sub>hex</sub>);
  4. Key<sub>dec</sub> ← HashtoDecimal(H<sub>value</sub>, Key<sub>hex</sub>);
  5. Key<sub>fea</sub> ← ExtractKeyFeatures(Key<sub>dec</sub>);
  6. Qua<sub>img</sub> ← Dec2Qua(Final<sub>img</sub>);
  7. DNA<sub>img</sub> ← Qun2DNA(Qua<sub>img</sub>, Key');
  8. PerDNA<sub>img</sub> ← PermutationDNA(DNA<sub>img</sub>, Key<sub>dec</sub>, Key<sub>fea</sub>, A, B);
  9. KeyDNA<sub>img</sub> ← HyperchaoticSystem(Key<sub>dec</sub>, Key<sub>fea</sub>, A, B);
  10. DifDNA<sub>img</sub> ← DiffusionDNA(PerDNA<sub>img</sub>, KeyDNA<sub>img</sub>, Key<sub>dec</sub>, Key<sub>fea</sub>, A, B);
  11. EncDNA<sub>img</sub> ← DecodingDNARule(DifDNA<sub>img</sub>, Key<sub>dec</sub>, Key<sub>fea</sub>, A, B);
  12. EncQua<sub>img</sub> ← DNA2Quq(EncDNA<sub>img</sub>);
  13. Enc<sub>img</sub> ← Qua2Dec(EncQua<sub>img</sub>);
- Return **Enc<sub>img</sub>**

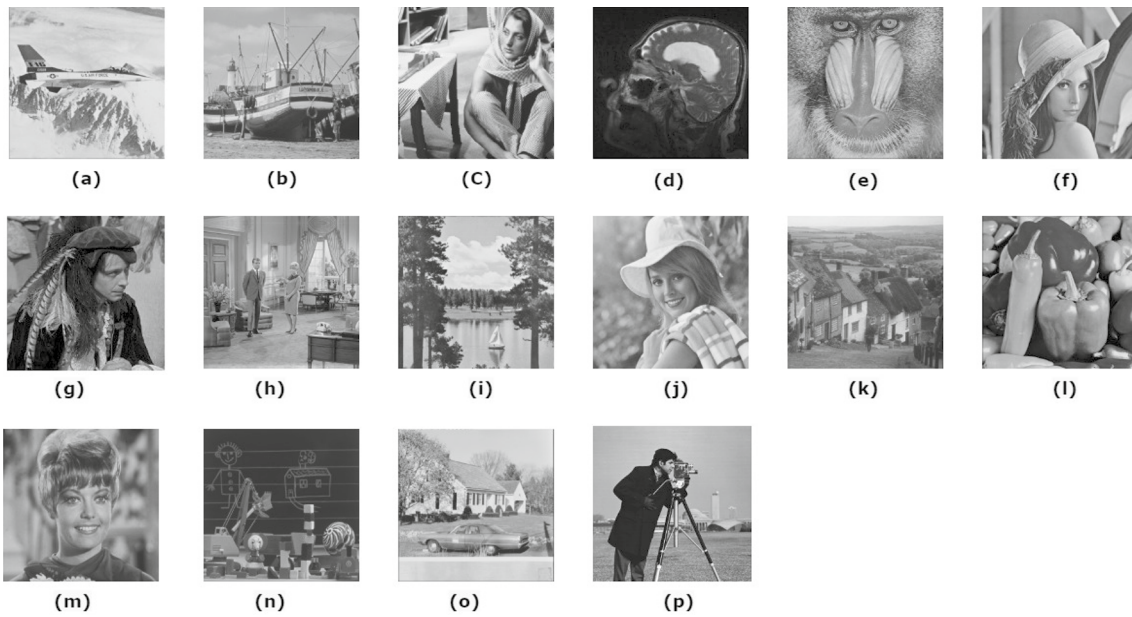
**Algorithm 3: Recovery procedure**(Enc<sub>img</sub>, δ, Key<sub>hex</sub>)**Begin**

1. Dec<sub>img</sub> ← Decryption(Enc<sub>img</sub>);
  2. Rec<sub>text</sub> ← ExtractMC(Dec<sub>img</sub>);
  3. D<sub>1</sub> ← zeros(256); D<sub>2</sub> ← zeros(256); D<sub>3</sub> ← zeros(256); D<sub>4</sub> ← zeros(256);
  4. **for** i ← 1: 256 **do**
  5.     **for** j ← 1: 256 **do**
  6.         D<sub>1</sub>(i, j) ← Dec<sub>img</sub>(2 × i − 1, 2 × j − 1);
  7.         D<sub>2</sub>(i, j) ← Dec<sub>img</sub>(2 × i − 1, 2 × j);
  8.         D<sub>3</sub>(i, j) ← Dec<sub>img</sub>(2 × i, 2 × j − 1);
  9.         D<sub>4</sub>(i, j) ← Dec<sub>img</sub>(2 × i, 2 × j);
  10.     **end for**
  11. **end for**
  12. A<sub>1</sub> ← Entropy(D<sub>1</sub>); A<sub>2</sub> ← Entropy(D<sub>2</sub>); A<sub>3</sub> ← Entropy(D<sub>3</sub>); A<sub>4</sub> ← Entropy(D<sub>4</sub>);
  13. G ← Max<sup>m</sup>(A<sub>1</sub>, A<sub>2</sub>, A<sub>3</sub>, A<sub>4</sub>);
  14. [G<sub>1</sub>, G<sub>2</sub>, G<sub>11</sub>, G<sub>12</sub>, G<sub>21</sub>, G<sub>22</sub>] ← NSCT(G);
  15. [H<sub>w1</sub>, P<sub>w1</sub>] ← hess(G<sub>22</sub>);
  16. [U<sub>w1</sub>, S<sub>w1</sub>, V<sub>w1</sub>] ← SVD(H<sub>w1</sub>);
  17. SV ←  $\frac{[S_{w1}-s]}{\delta}$ ;
  18. Y ← U<sub>w</sub> × SV × V<sub>w</sub><sup>T</sup>;
  19. W' ← P<sub>w</sub> × Y × P<sub>w</sub><sup>T</sup>;
  20. Rec<sub>wat</sub> ← INSCT(NS<sub>w1</sub>, NS<sub>w2</sub>, NS<sub>w31</sub>, NS<sub>w32</sub>, NS<sub>w41</sub>, W');
- Return **Rec<sub>wat</sub>** and **Rec<sub>text</sub>**

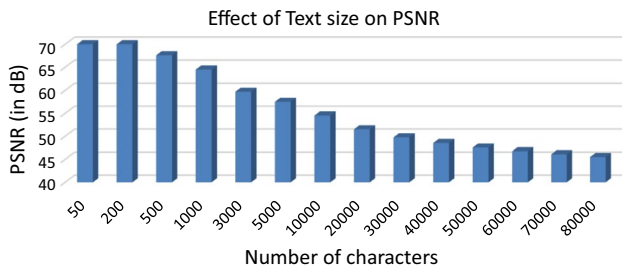
## 4 Experimental results

The experimental analysis of our implemented algorithm has been simulated on MATLAB 2019a. In the experiment, sixteen gray-images (See Fig. 3) of dimensions 512 × 512 × 8 are used for testing [22]. The size of mark image is chosen as 256 × 256 × 8 for embedding purpose. The

text document of the size 564 characters (500 characters of text information and hash value of cover image of 64 characters) is also chosen for embedding purpose into marked image. In our experiments, PSNR and SSIM [23] between original cover and marked image are used to measure invisibility, NC [23] between original mark and recovered mark are adopted to determine robustness. Further, NPCR and



**Fig. 3** Used images as cover **a** Airplane, **b** Boat, **c** Barbara, **d** Brain, **e** Baboon, **f** Lena, **g** Man, **h** Couple, **i** Sailboat, **j** Elaine, **k** Goldhill, **l** Peppers, **m** Zelda, **n** Toys, **o** House, and mark **p** Cameraman

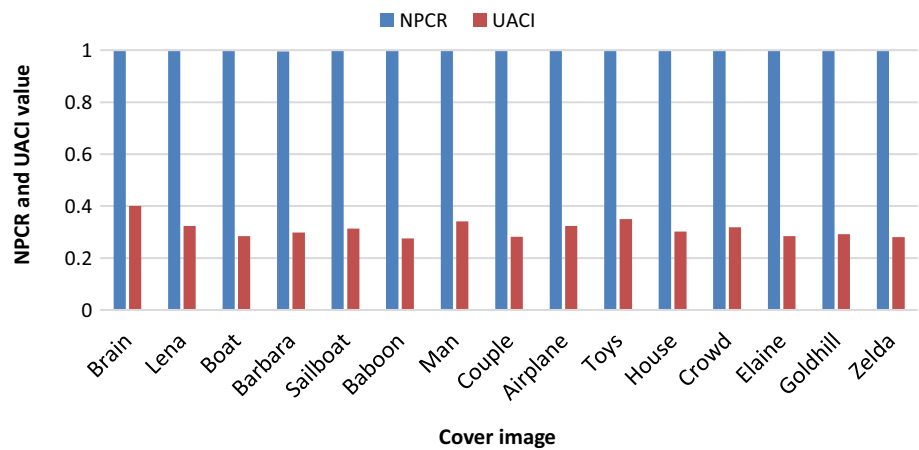


**Fig. 4** Effect on distortion with different payload

**Table 3** The invisibility and robustness at nine different gain values

Gain	PSNR	SSIM	NC
0.015	85.41	1.0000	0.9975
0.02	78.11	1.0000	0.9980
0.05	66.26	1.0000	0.9994
0.07	63.35	1.0000	0.9995
0.09	61.36	0.9999	0.9995
0.10	60.47	0.9999	0.9996
0.30	51.05	0.9992	0.9996
0.50	46.65	0.9979	0.9996
0.9	41.57	0.9934	0.9996

**Fig. 5** NPCR and UACI values of our proposed scheme for different digital image

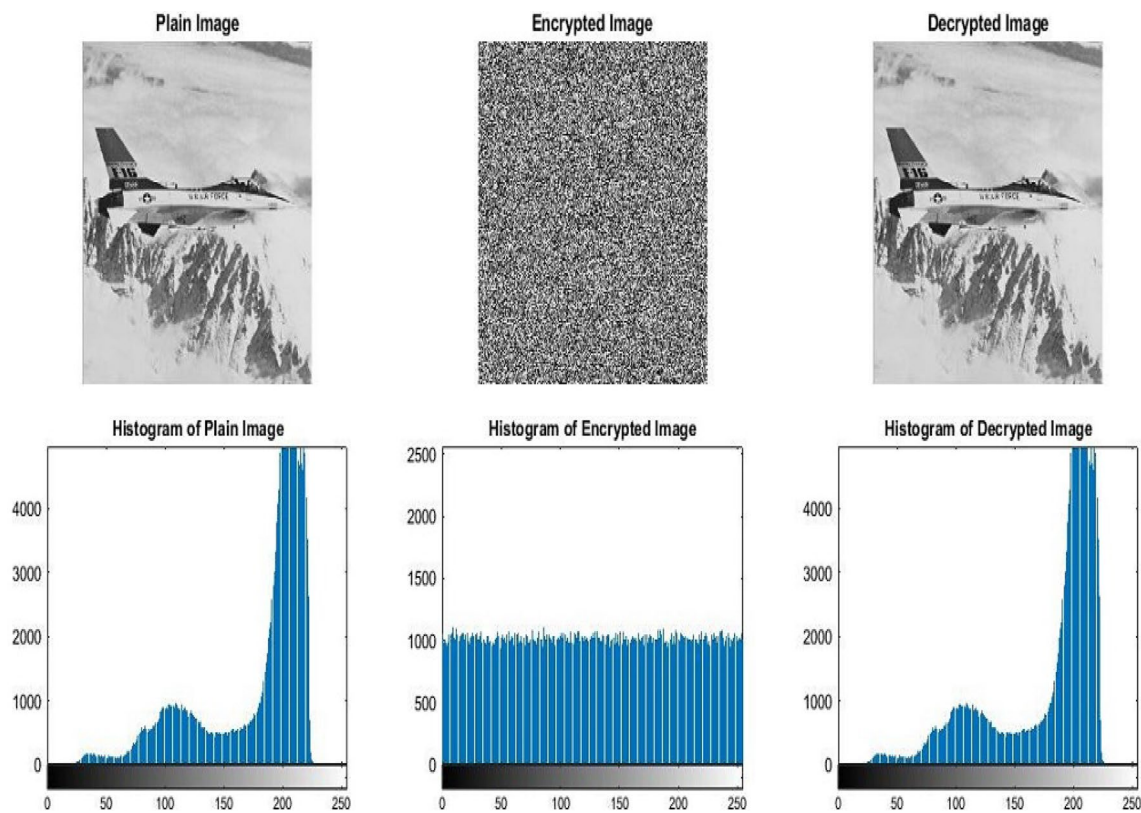


**Table 4** The comparative investigation in terms of invisibility

Host image	Ref [15]		Ref [16]		Ref [18]		Ref [19]		Proposed scheme	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Couple	47.54	0.9974	46.84	0.9959	48.49	0.9949	–	–	66.47	1.0000
Barbara	29.00	0.8567	–	–	48.22	0.9947	–	–	65.56	1.0000
Peppers	39.50	0.8387	46.84	0.9928	48.30	0.9952	33.33	0.9985	66.80	1.0000
Lena	29.00	0.8535	–	–	48.40	0.9955	33.21	0.9989	67.21	1.0000
Baboon	28.50	0.8877	46.68	0.9962	48.27	0.9984	31.34	0.9979	65.99	1.0000

**Table 5** Embedding capacity comparison between proposed method and mentioned techniques

Methods	Watermark image	Cover image	Payload (Bit/pixel)
[13]	$(256 \times 256) + (128 \times 128)$	$512 \times 512$	0.3125
[16]	$64 \times 64$	$512 \times 512$	0.0150
[17]	$32 \times 32$	$512 \times 512$	0.0039
[18]	$(256 \times 256) + (128 \times 128)$	$512 \times 512$	0.3125
[23]	$256 \times 256$	$512 \times 512$	0.2500
Proposed method	$256 \times 256 \times 8$	$512 \times 512 \times 8$	0.2500



**Fig. 6** Histogram analysis of plain, encrypted and decrypted image of our proposed scheme

UACI [23] are used to examine the performance of lossless encryption scheme. The performance analysis of our scheme is evaluated at a different gain are depicted in Table 3. It is noticed that the best PSNR and SSIM scores are obtained as 85.41 dB and 1.000, respectively, at gain = 0.015. The

best NC score = 0.9996 at gain = 0.1. In order to improve the mark capacity, magic cube-based algorithm is used to embed text data up to 80,000 characters. From Fig. 4, it indicates that the distortion increases at high payload. The NPCR and UACI scores as obtained for encryption scheme are depicted



in Fig. 5. In this figure, it is observed that best NPCR and UACI score is found as 0.9964 and 0.4005, respectively.

Table 4 provides the comparative investigation in terms of invisibility of the proposed model with the existing techniques [15, 16, 18, 19]. As shown in Table 4, PSNR and SSIM score of our algorithm is superior than existing related techniques. The embedding capacity of our method is  $(256 \times 256 \times 8) / (512 \times 512 \times 8) = 0.25$ . We also embed text document of the size 564 characters in marked image to improve mark capacity of our algorithm. Table 5 provides the comparative investigation in terms of capacity of the proposed model with the existing techniques [13, 16–18, 23]. As the result indicated, the capacity of our algorithm is superior than existing related techniques [16, 17] except [13] and [18]. However, the capacity of our algorithm is similar to related techniques [23].

The histogram of plain, encrypted and decrypted image of our proposed scheme is illustrated in Fig. 6. According to Fig. 6, we can notice that encrypted image is similar to noise like image, and it could not be extract original information about plain image. Histogram of encrypted image indicates that it shows in uniform manner which makes very difficult to extract information.

Figure 7 shows the invisibility and robustness performance of our proposed algorithm for fifteen images. It can be seen that when gain = 0.05, the best PSNR, SSIM and NC scores are obtained as 67.36 dB, 1.000 and 0.9996, respectively. The performance our proposed scheme is evaluated in terms of robustness under various image processing attacks are shown in Fig. 8. According to Fig. 8, robustness is evaluated against JPEG attacks with different quality factor. If quality factor of JPEG is improved, then NC score of proposed scheme is also increased. The NC value is obtained more than 0.9875 against average filtering. In median filtering, NC value is obtained more than 0.9948. In Fig. 8, NC score is evaluated as 0.9832 against Histogram Equalization. In salt and pepper noise, NC score is obtained more than 0.9362. In Speckle and Gaussian noise, NCs value obtained more than 0.9360 and 0.9368, respectively. In rotation attack, NC value obtained as 0.9962. The NC score obtained as 0.9969 against scaling attack. In sharpening attack, NC value is evaluated as 0.9968. According to this table, we have observed that NC value of our scheme is more than 0.9360 against mention attacks.

Table 6 provides the comparative robustness investigation of the proposed model with the existing techniques [23–25] under well-known attacks. From this table, we have noticed that robustness of the model is higher than that of other traditional algorithms except salt & pepper and speckle noise. It indicates a considerable improvement in robustness of up to 96.36% against histogram equalization attack over other schemes.



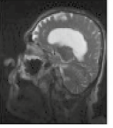



























**Table 6** The comparative analysis of NC values with other three techniques

Attacks	Ref [23]	Ref [24]	Ref [25]	Proposed method	Best improvement of NC (in %)
JPEG with varying QF					
10	0.7924	0.9814	0.8994	0.9950	25.56
50	0.9388	0.9988	0.9626	0.9978	06.28
90	0.9796	0.9995	NA	0.9989	01.97
Median filtering					
[1 1]	0.9860	0.9995	0.9973	0.9995	01.36
[2 2]	0.9457	0.9759	0.9099	0.9950	09.35
Salt & Pepper					
0.01	NA	0.8451	NA	0.9366	10.82
0.001	0.9251	0.9975	0.8761	0.9362	06.85
Gaussian noise					
0.005	NA	0.7676	0.8311	0.9368	22.04
Speckle noise					
0.005	0.9014	0.9774	NA	0.9360	03.83
Histogram Equalization	0.8716	0.7223	0.5007	0.9832	96.36

## 5 Conclusions

This paper has described an interesting information hiding algorithm that utilizes NSCT-HD-SVD for concealing of mark data. Further, the algorithm uses magic cube algorithm for higher payload and lossless encryption for additional authentication. The results show that compared with the traditional schemes, robustness of our algorithm is significantly improved. The proposed algorithm not only provides the additional level of information security, but also offers the good hiding efficiency. Further, performance of this scheme can be further improved by selecting optimal embedding factor using metaheuristic approaches.

**Fig. 7** Objective measure of our proposed scheme

Host image	Lena	Airplane	Brain	Barbara	Couple
Watermarked image					
PSNR (dB)	67.2175	66.2621	67.3428	65.5676	66.4470
SSIM	1.0000	1.0000	1.0000	1.0000	1.0000
Extracted watermark					
NC	0.9993	0.9994	0.9991	0.9996	0.9994
Host image	Toys	Boat	Baboon	Sailboat	Man
Watermarked image					
PSNR (dB)	66.3032	66.2320	65.9963	66.5747	66.1672
SSIM	1.0000	1.0000	1.0000	1.0000	1.0000
Extracted watermark					
NC	0.9995	0.9995	0.9995	0.9993	0.9995
Host image	Zelda	Goldhill	Elaine	Peppers	House
Watermarked image					
PSNR (dB)	66.4842	66.2320	67.3677	66.8066	66.0460
SSIM	1.0000	1.0000	1.0000	1.0000	1.0000
Extracted watermark					
NC	0.9994	0.9992	0.9992	0.9994	0.9994

**Fig. 8** Obtained watermarked and extracted mark image under various attacks





































Type of attack	Attacked Watermarked image	Recovered watermark	
JPEG (QF=10)			0.9950
JPEG (QF=30)			0.9966
JPEG (QF=50)			0.9978
JPEG (QF=90)			0.9989
Average Filtering [1 1]			0.9995
Average Filtering [2 2]			0.9875
Average Filtering [3 3]			0.9764
Median Filtering [1 1]			0.9995
Median Filtering [3 3]			0.9948

Fig. 8 (continued)

Type of attack	Attacked Watermarked image	Recovered watermark	
Histogram Equalization			0.9832
Salt and pepper noise (0.001)			0.9362
Salt and pepper noise (0.005)			0.9364
Salt and pepper noise (0.01)			0.9366
Speckle noise (0.001)			0.9360
Gaussian noise (0.005)			0.9368
Sharpening (0.001)			0.9968
Rotation 90			0.9962
Scaling			0.9969

## References

- Mahato, S., Yadav, D., Khan, D.: A novel information hiding scheme based on social networking site viewers' public comments. *J. Inf. Secur. Appl.* **47**, 275–283 (2019)
- Singh, A.K., Kumar, B., Singh, G., Mohan, A.: Digital Image Watermarking: Concepts and Applications. In: Singh, A., Kumar, B., Singh, G., Mohan, A. (eds) *Medical Image Watermarking. Multimedia Systems and Applications*. Springer, Cham (2017). [https://doi.org/10.1007/978-3-319-57699-2\\_1](https://doi.org/10.1007/978-3-319-57699-2_1)
- Xia, Z., Wang, X., Zhang, L., Qin, Z., Sun, X., Ren, K.: A Privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. *IEEE Trans. Inf. Forensics Secur.* **11**(11), 2594–2608 (2016)
- Singh, A.K.: Data Hiding: Current Trends, Innovation and Potential Challenges. *ACM Trans. Multimed. Comput. Commun. Appl.* **16**(3s), 1–16 (2021)

5. Singh, O.P., Singh, A. K., Srivastava, G., Kumar, N.: Image watermarking using soft computing techniques: A comprehensive survey. *Multimed. Tools Appl.*, pp. 1–32, 2020.
6. Mohanty, S., Sengupta, A., Guturu, P., Kougianos, E.: Everything you want to know about watermarking: from paper marks to hardware protection: from paper marks to hardware protection. *IEEE Consum. Electr. Mag.* **6**(3), 83–91 (2017)
7. Yuan, Z., Su, Q., Liu, D., Zhang, X.: A blind image watermarking scheme combining spatial domain and frequency domain. *Vis. Comput.* **37**, 1867–1881 (2021)
8. Nam, S., Mun, S., Ahn, W., Kim, D., In, Yu., Kim, W., Lee, H.: NSCT-based robust and perceptual watermarking for DIBR 3D images. *IEEE Access* **8**, 93760–93781 (2020)
9. Liu, J., Huang, J., Luo, Y., Cao, L., Yang, S., Wei, D., Zhou, R.: An optimized image watermarking method based on HD and SVD in DWT domain. *IEEE Access* **7**, 80849–80860 (2019)
10. Ranjani, J., Zaid, F.: Pseudo magic cubes: a multidimensional data hiding scheme exploiting modification directions for large payloads. *Comput. Electr. Eng.* **89**, 1–10 (2021)
11. Zefreh, E.: An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions. *Multimed. Tools Appl.* **79**(33–34), 24993–25022 (2020)
12. M. Kazemi, M. Pourmina and A. Mazinan, "Novel Neural Network Based CT-NSCT Watermarking Framework Based upon Kurtosis Coefficients", *Sensing and Imaging*, vol. 21, no. 1, 2019.
13. Thakur, S., Singh, A., Ghrera, S., Mohan, A.: Chaotic based secure watermarking approach for medical images. *Multimed. Tools Appl.* **79**(7–8), 4263–4276 (2018)
14. A. Amiri and S. Mirzakuchaki, "A digital watermarking method based on NSCT transform and hybrid evolutionary algorithms with neural networks", *SN Applied Sciences*, vol. 2, no. 10, 2020.
15. Li, J., Zhang, C.: Blind watermarking scheme based on Schur decomposition and non-subsampled contourlet transform. *Multimed. Tools Appl.* **79**(39–40), 30007–30021 (2020)
16. Su, Q., Wang, G., Lv, G., Zhang, X., Deng, G., Chen, B.: A novel blind color image watermarking based on Contourlet transform and Hessenberg decomposition. *Multimed. Tools Appl.* **76**(6), 8781–8801 (2016)
17. Singh, A.K., Thakur, S., Jolfaei, A., Srivastava, G., Elhoseny, M., Mohan, A.: Joint encryption and compression-based watermarking technique for security of digital documents. *ACM Trans. Internet Technol.* **21**(1), 1–20 (2021)
18. Kumar, C., Singh, A.K., Kumar, P., Singh, R., Singh, S.: SPIHT - based multiple image watermarking in NSCT domain. *Concurrency and Computation: Practice and Experience* **32**(1) (2018)
19. Nam, S., Mun, S., Kim, D., Ahn, W., Yu, I., Kim, W., Lee, H., et al.: NSCT-based robust and perceptual watermarking for DIBR 3D images. *IEEE Access* **8**, 93760–93781 (2020)
20. P. S. and C. P. V. S. S. R., "A robust semi-blind watermarking for color images based on multiple decompositions", *Multimedia Tools and Applications*, vol. 76, no. 24, pp. 25623–25656, 2017.
21. Luo, Y., Li, L., Liu, J., Tang, S., Zhang, S., Qiu, S., Cao, Y.: A multi-scale image watermarking based on integer wavelet transform and singular value decomposition. *Expert Systems with Applications* **168**, 114272 (2021)
22. <http://sipi.usc.edu/database/database.php?volume=misc>
23. Anand, A., Singh, A. K.: An improved DWT-SVD domain watermarking for medical information security. *Comput. Commun.* **152**, 72–80 (2020)
24. Anand, A., Singh, A.K., Lv, Z., Bhatnagar, G.: Compression-then-encryption-based secure watermarking technique for smart healthcare system. *IEEE Multimed.* **27**(4), 133–143 (2020)
25. Thakur, S., Singh, A. K., Kumar, B., Ghrera, S.P.: Improved DWTSVD-Based Medical Image Watermarking Through Hamming Code and Chaotic Encryption. *Lecture Notes in Electrical Engineering*, pp. 897–905 (2019)

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.