IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 38, No. 4, August, 2021, pp. 1113-1121
Journal homepage: http://iieta.org/journals/ts

Spectral Graph Wavelet Based Image Steganography Using SVD and Arnold Transform

Shikha Chaudhary[1*], Saroj Hiranwal[1], Chandra Prakash Gupta[2]

[1] Department of Computer Science & Engineering, Rajasthan Institute of Engineering & Technology, Jaipur 302026, India
[2] University College of Engineering, Rajasthan Technical University, Kota 324010, India

Corresponding Author Email: shikha.chaudhary18@gmail.com

https://doi.org/10.18280/ts.380422

Received: 22 January 2021
Accepted: 25 July 2021

Keywords:
graph signal processing, steganography, spectral graph wavelet, SVD, Arnold transform

ABSTRACT

Steganography is the process of concealing sensitive information within cover medium. This study offers an efficient and safe innovative image steganography approach based on graph signal processing (GSP). To scramble the secret image, Arnold cat map transform is used, then Spectral graph wavelet is used to change the cover and scrambled secret image, followed by singular vector decomposition (SVD) of the modified cover image. To create the stego image, an alpha blending process is used. To produce the stego image, GSP-based synthesis is used. By maintaining the inter-pixel correlation, GSP improves the visual quality of the produced stego image. The effects of image processing attacks on the suggested approach are examined. The investigational results and assessment indicate that the proposed steganography scheme is more efficient and robust in terms of quality measures. The quality of stego image is evaluated in respect of PSNR, NCC, SC and AD performance metrics.

1. INTRODUCTION

Nowadays, the utmost prevailing communication means amongst individuals across the globe is the internet. The usage of the internet removed the hindrance to interchange the data among individuals. To exchange confidential or private information; security and privacy are the most pressing matter. Steganography is a key solution to provide a higher level of security to exchange concealed information [1]. Steganography refers to 'covert communication or secretive composition', this is the primary feature of steganography which separates it from other related techniques like cryptography and watermarking [2]. While cryptography changes information so that it cannot be observed by an intruder, steganography conceals the existence of concealed information; this critical characteristic shields the hidden message from a spectator [3]. The exchange of encrypted information may be apparent since it may draw the attention of a spectator, whereas obscure practice will not. Watermarking is a strategy to ensure licensed or copyright protection. The prime target of watermarking is to identify the proprietor, not to hide secret data. Steganography creates a secret channel which is proficient in disguising the concealed data. Among different advanced media like picture or image, sound, video and so forth; anyone can be picked as cover or carrier media, yet more appropriate are image and sound as a result of their serious extent of excess [4]. Steganography is widely utilized in military, safeguard, and insight offices for secure correspondence of surreptitious information. Steganography methods are categorized into two primary domains: spatial and frequency domain [5]. In the spatial domain-based technique secret message is unswervingly inserted into carrier image pixels however, in the latter method, the carrier image is converted in frequency domain first then surreptitious information is inserted. Therefore frequency domain approach is more robust in nature [6]. The current frequency domain techniques depend on fast Fourier transform [7], discrete wavelet transform (DWT) [2, 3], discrete cosine transform [8], curvelet transform etc. [9]. In recent years, in the field of image processing, to analyze an image signal wavelet transform is originated as an alternate of Fourier transform and other related transforms [10-12]. Wavelets are numerical or mathematical procedures to analyze and synthesize a signal in the time domain. Nowadays, wavelet transform is accepted by many applications like printing, mobile applications, digital photography, digital library, medical imagery, e-commerce, color facsimile, scanning, and image compression, etc. Recently, researchers have shown interest in graph signal processing (GSP) to study multidimensional data and creating a graph from the specified data [13, 14]. The GSP is mainly used to depict the accurate information of the data. Several graphs can be framed from an image [13, 15], GSP tool delivers the adaptability of selecting a graph like grid, cube, spiral, ring etc. according to the effectiveness of a signal. In recent years, plenty of research has been done from typical wavelet transforms to graph wavelet transform [16]; various multi-scale transforms are proposed in [17-19]. The fundamental preferences of utilizing a graph wavelet-based methods are (i) it has more noteworthy numerical dependability in recreation as it provides more localize, frequency, and temporal information [13, 16] (ii) graph is more appropriate for multidimensional information investigation such as network, image etc. [15], (iii) graph wavelet repels the receiver to splinter the data itself [20]. The graph wavelet stores the inter-pixel information that can be further used to rebuild the original data.

This paper proposes secure image steganography depends on spectral graph wavelet. The main impact of applying the spectral graph wavelet on image, is to produce a stego image with high visual quality by leveraging inter-pixel correlation.

The embedding technique consists mainly of three processes: (i) Arnold transform [21] based scrambling of the secret image using a secret key (ii) SVD transformation of the cover image to find out singular values of cover for embedding (iii) blending operation to embed the secret image inside the singular value diagonal matrix of the cover image. The quality of the extracted image is attained by using graph signal processing. The performance of the proposed method is tested on the various cover and secret images of different sizes. The quality of the stego image and the decoded secret image is achieved by changing the value of the alpha (blending factor). Several image processing attacks are performed to check the robustness of the proposed scheme.

The rest of this work is organized as follows: Section 2 shows the related work carried out in the field of image steganography. The methodology of the proposed image steganography technique is introduced in depth in section 3. The investigational results, performance analysis, and robustness testing are presented in section 4. Finally, the conclusion is drawn in section 5.

2. RELATED WORK

To achieve a higher level of security during data transfer, various steganography techniques have been developed. A steganography method proposed by Chan and Chang [22] is least-significant bit substitution (LSB), where the LSB of the pixels is altered to insert the secret information. A method using DWT transform with LSB substitution proposed by Prabakaran and Bhavani [23]. DWT is applied on cover and secret image both, the secret image is embedded using two secret keys which makes the stego image indistinguishable from the cover [24]. The optimum hiding capability-based steganography for concealing the moderately huge size secret image inside a comparatively small size carrier image is developed by Archana et al. [25]. A DWT-based steganography is proposed by utilizing LSB substitution, where the adaptive hiding function is used in integer wavelet to optimize the hiding capacity [26]. The steganography technique where the embedding algorithm is allowed to choose any cover media to make the stego image least detectable is proposed by Kumar, V. and Kumar, D. [5]. The Mid position value-based image steganography method is presented where Arnold transform is applied to scramble the cover image and mid position value (MPV) over a scrambled cover image is applied to insert bits of a secret image [27]. Integer Wavelet Transform (IWT) is applied to the images and for scrambling of the secret image; the Arnold transform is applied in the study [28]. Information embedding is performed using LSB substitution and Arnold transformation is applied twice consecutively in the study [29]. Mathematical decomposition techniques [30] are applied on contourlet coefficients of the carrier thereafter secret data is implanted into factorized coefficients. Framelet transform is carried out in the study [31] on a cover image to get transform coefficients for embedding Secret information. A genetic algorithm is used to map information in DWT coefficients of 4 × 4 blocks of the carrier image. Then optimal pixel adjustment process (OPAP) is subsequently applied to insert the secret data [32]. A robust modified DWT-based steganography method is proposed by Kumar, V. and Kumar, D. [33], in which secret key computation and blocking methods are used. A graph wavelet-based steganography is proposed by Sharma et al. [34] where graph wavelet is applied on the cover and secret images to get a good quality of stego. SVD and DWT-based steganography method is presented by Lakshmi Sirisha [35] where secret image features are stored in the LL band.

3. BACKGROUND

3.1 Graph signal processing

A digital image can be denoted as a graph by showing each pixel as a vertex, joining every pixel to one another of an image. Pixel value in an image is treated as a graph signal T in the graphical representation of an image [15, 16, 29]. In this paper, we apply a weighted undirected graph which is represented as $G = (V, E, W)$, where V is a set of vertices or pixels and $|V| = N$. Nodes are connected using a set of weighted links called edges of a graph represented as a set $E = \{e_{ij} : v_i, v_j \in V\}$. W is a set of weights contains w_{ij} of an edge linking vertices v_i and v_j. The pixel value or intensity x_i is the i^{th} element of the graph signal T on vertex v_i. Everything about graph signal representation is described in the researches [13, 15]. The graph is generally represented using adjacency matrix M where each item is shown as $w_{ij,}$ which is the weight of an edge joining a vertex v_i and v_j. The Gaussian weight can be derived from the pixel values using Eq. (1) A degree matrix D is a graph where each d_i is the addition of all the edges linked to vertex v_i. The Laplacian is a difference operator carried out on graph signal T as shown in Eq. (2) and the Laplacian graph can be obtained by Eq. (3) [36-38].

$$W_{ij} = \begin{cases} \exp\left(\dfrac{-\left|x_i - x_j\right|^2}{b}\right), if \left|x_i - x_j\right| < \in \\ 0, \qquad elsewhere \end{cases} \tag{1}$$

Here, b is the empirically determined parameter.

$$Lx_i = \sum_{v_j : e_{ij} \in E} W_{ij}\left[x_i - x_j\right] \tag{2}$$

$$L = D - W \tag{3}$$

Here, L is a semi-definite symmetric matrix containing a discrete set of E non-negative eigenvalues λ_k.

3.2 Spectral graph wavelet

The spectral graph wavelet [38] is created using eigenvectors Z_k of the Laplacian graph. Therefore the spectral graph wavelet $\psi_{h,n}(m)$ is defined in Eq. (4) on scale h and vertex n.

$$\psi_{h,n}(m) = \sum_{k=0}^{N-1} p\left(h\lambda_k\right) Z_k(n) Z_k(m) \tag{4}$$

Here, kernel p is a wavelet generating function, in our approach we used Meyer wavelet to generate kernel p and scaling function s, which are defined in Fourier domain as Eq. (5) and Eq. (6). The low-frequency $\varphi_n(m)$ of the graph signal is defined as Eq. (7).

$$p(\lambda)=\begin{cases}\sin\left(\frac{\pi}{2}v\left(\frac{1}{\lambda 1}|\lambda|-1\right)\right) & if\ \ \lambda 1\le\lambda<\lambda 2\\ \cos\left(\frac{\pi}{2}v\left(\frac{1}{\lambda 2}|\lambda|-1\right)\right) & if\ \ \lambda 2\le\lambda<\lambda 3\\ 0 & otherwise\end{cases} \quad (5)$$

$$s(\lambda)=\begin{cases}1 & if\ \ \lambda<\lambda 1\\ \cos\left(\frac{\pi}{2}v\left(\frac{1}{\lambda 1}|\lambda|-1\right)\right) & if\ \ \lambda 1\le\lambda<\lambda 2\\ 0 & otherwise\end{cases} \quad (6)$$

$$\varphi_n(m)=\sum_{k=0}^{N-1}s(h\lambda_k)Z_k(n)Z_k(m) \quad (7)$$

where, $(y)=y^4*(35-84*y+70*y^2-20y^3)$; $\lambda 1=2/3$, $\lambda 2=2\lambda 1$ and $\lambda 3=4\ \lambda 1$.

4. PROPOSED STEGANOGRAPHY APPROACH

The proposed technique involves mainly two processes encoding or embedding process and decoding or extracting process. During the embedding phase firstly Arnold cat map transform is applied by means of a secret key to scramble the secret image [21, 37]. Scrambling is a procedure of rearranging the pixels of an image to make the image visually unreadable while keeping pixel values unchanged. The technique becomes more robust by applying Arnold cat map-based scrambling over on a secret image. It enhances the security of the hidden secret image. After applying Arnold Cat Map transforms operation to the secret image, a scrambled image is produced as shown in Figure 3(c).

Let $A=\begin{bmatrix}a\\b\end{bmatrix}$ is an image matrix of size *NXN*, the Arnold transform is performed using the following formula:

$$\begin{bmatrix}a\\b\end{bmatrix}=\begin{bmatrix}1 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix}\text{Mod N} \quad (8)$$

The Arnold Cat map transform shears the image in *x* and *y* direction by the factor 1, followed by evaluation of modulo. It provides security or confidentiality to our proposed technique. Formerly, apply GSP-based analysis on the cover image and scrambled secret image separately to generate spectral graph wavelets of both the images. Further, apply singular vector decomposition (SVD) transform on the graph wavelet of the cover image to compress the image without losing its quality.

Single value Decomposition (SVD) [39, 40] is a factorization of an *m* x *n* matrix *A* into the product of three matrices $A=USV'$. The two matrices *U* of size *m* x *m* and *V* of *n* x *n* are orthogonal unitary matrices, whereas *S* is a singular value diagonal matrix with nonnegative items. It is a mathematical illustration of an image and decomposes the features of an image into matrices. Applying SVD on the cover image in image steganography has two major advantages, first: a slight difference in singular values of image does not disturb the visual quality of an image and second, it offers more robustness against attacks. Further, an alpha blending operation is implemented on the *S* matrix generated using SVD transformation of spectral graph wavelet based cover image and spectral graph wavelet of scrambled secret image using Arnold transform. This operation generates a blended image matrix. Alpha blending operation is the process of combining or overlaying two images to produce a new-fangled image. The alpha blending operation is done using the following equation:

$$CA=S_S+\alpha S_{GA} \quad (9)$$

where, *CA* is the blended image, S_S is the diagonal matrix obtained after SVD transformation on the cover image and S_{GA} is the spectral graph wavelet of Arnold scrambled secret image. Here α signifies a blending factor to control the noticeability of the secret image. The value of α should be $0<\alpha<1$ as the value 0 means the fully transparent color and 1 signifies the opaque that means the value of α influences the visual quality of generated stego image. After performing the alpha blending operation, Inverse SVD transformation is applied to the blended image. Now, apply the graph synthesis process (inverse of graph wavelet) to generate the stego image.

The extracting framework or decoding process involves the same strategy in a reverse manner.

4.1 Encoding phase

The process or flowchart of the encoding or embedding phase of the proposed steganography technique is shown in Figure 1 and algorithmic steps of the technique are as shown in algorithm 1.

In algorithm 1, step one is about taking the input as the cover image *C* and the secret image *S* followed by resizing of the secret image as per the size of the cover image in step 2. In step 3, Arnold transforms on secret image *S* is applied using a secret key *K* to generate scrambled image S_A in procedure *Arnold(S,K)*, here the function calculates the new pixel positions of the secret image by using Eq. (8). In step 4, the procedure *GSP_2dgrid(N)* designs a two-dimensional grid graph with *NxN* nodes and returns a graph structure *G*. The procedure *GSP_design_meyer(G,Nf)* in step 5 returns Meyer wavelet with two filters for designing the graph. In step 6, the procedure *gsp_filter_analysis(G,p,C)* applies SGWT or GSP-based analysis on cover image *C* and generates an image C_{GA}. The procedures used in steps 4,5 and 6 are predefined functions of the Graph Signal Processing Toolbox in MATLAB or Python. Further, SGWT is applied on Arnold scrambled secret image S_A and gets an SGWT image S_{GA} in step 7. The *S*ingular vector decomposition (SVD) on C_{GA} is applied in step 8 to get 2-D matrices U_S, S_S and V_S. in step 9, Alpha blending operation is performed on the scrambled image S_{GA} and the diagonal matrix S_S to get the image *CS* followed by Inverse SVD on *CS* image to get image *IS* using formula U_S*CS*V_S' in step 10. Finally, inverse graph wavelet or GSP-based synthesis process is applied on *IS* to get stego image *I* in step 11. The function to compute Arnold transform is defined in the algorithm 1.

Algorithm 1: SGWT Embedding Algorithm

Input: Cover Image *C*, Secret Image *S*
Output: Stego Image *I*.
Require: Key *K=10*, Number of Nodes *N=16*, Number of Filters *Nf=2*

(1) *Read image C, S*
(2) *S = resize(S,size(C))*
(3) S_A*= Arnold(S,K)* *// function to compute Arnold transform*
(4) *G= GSP_2dgrid(N)* *// 2-D grid graph design*
(5) *p=GSP_design_meyer(G,Nf)* *// Meyer kernel wavelet*
(6) C_{GA} *= gsp_filter_analysis(G,p,C)* *// to compute SGWT of cover*
(7) $S_{GA=}$ *gsp_filter_analysis(G,p,*S_A*)* *// to compute SGWT of scrambled*
(8) $[U_S,S_S,V_S]$ *=SVD(*C_{GA}*)* *// SVD computation of cover graph*
(9) *CS=1.*Ss+alpha.**S_{GA} *// alpha blending*
(10) *IS=US*CS*VS'* *// Inverse SVD transform*
(11) *I= gsp_filter_synthesis(G,p,IS);* *// Inverse of SGWT to generate stego*

Procedure: Arnold(S,K)
(1) *Read the secret image S and get its Size NxN*
(2) *For k=1 to K*
(3) *for each row x and column y do*
(4) *X=(x+y)ModN*
(5) *Y =(x+2y) ModN*
(6) *O(X,Y)=S(x,y)*
(7) *Return O*

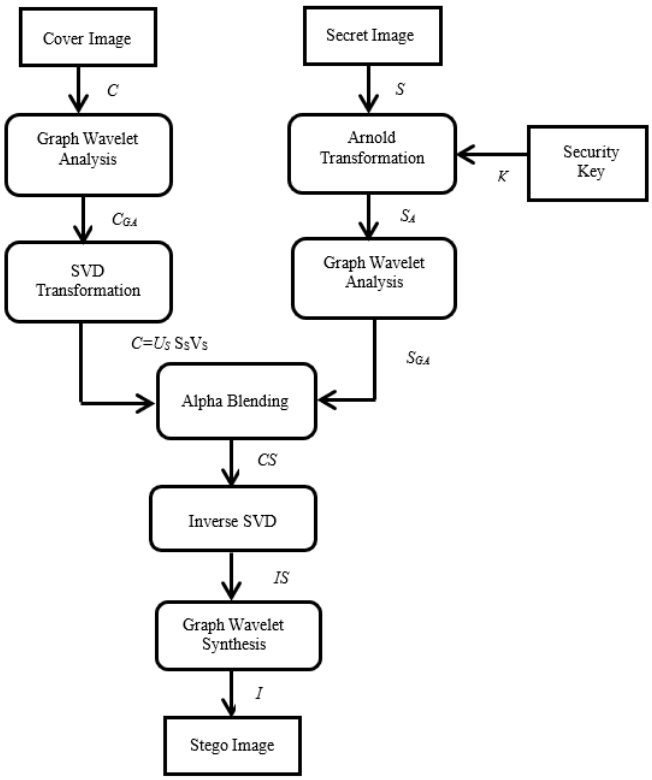


Figure 1. Block diagram of the encoding process of proposed steganography technique

4.2 Decoding phase

The decoding procedure is the opposite of the encoding procedure. First, perform graph wavelet analysis on the stego image. Take the SVD transform of the stego image, then apply the alpha blending function between the diagonal matrices of the cover image and the stego image. The image should next be generated using inverse SVD, followed by graph synthesis. Finally, use the inverse Arnold transform to descramble the scrambled image. The flowchart or block diagram of the decoding or extracting phase of the proposed technique is presented in Figure 2 and algorithmic steps are shown in algorithm 2.

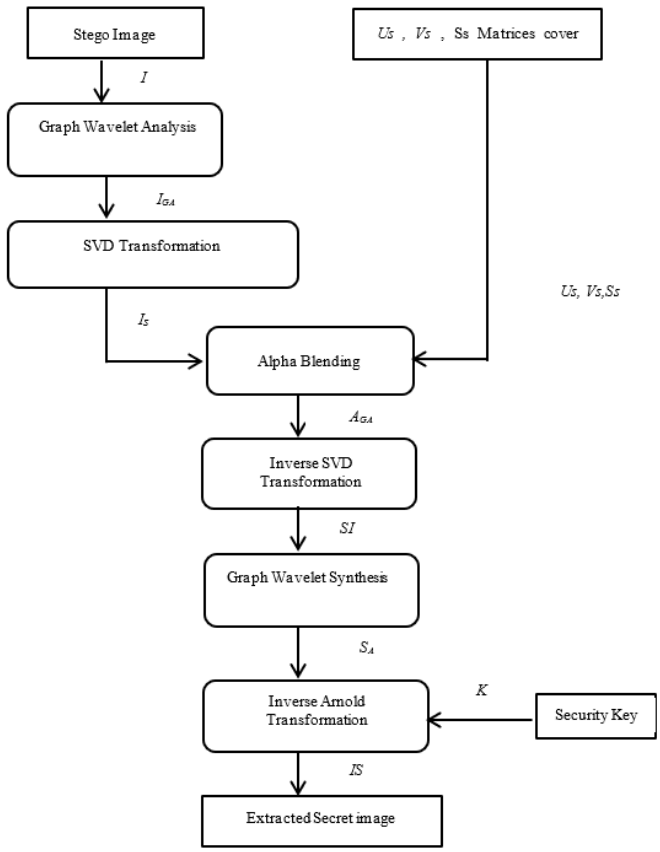


Figure 2. Block diagram of the decoding process of proposed steganography technique

Algorithm 2: SGWT Decoding Algorithm

Input: U_S, V_S *and* Stego Image *I.*
Output: Extracted Secret Image *IS.*
Require: Key *K=10,* Number of Filters *Nf=2*

(1) I_{GA} = *gsp_filter_analysis(G,p,I)*
(2) $[U, I_S, V]$ =*SVD*(I_{GA})
(3) A_{GA} =*(Is-1.*Ss)*
(4) $SI = U_S * A_{GA} * V_S'$
(5) *S= gsp_filter_synthesis(G,p,SI)*
(6) *IS= inverseArnold(S,K)*

5. EXPERIMENTAL RESULTS AND DISCUSSIONS

To analyze the performance of the proposed steganography method through experimental simulation, MATLAB software is used. The grayscale image Lenna.jpg having size *256 X 256* shown in Figure 3a is taken as the carrier or cover image and Peppers.jpg of size 256 × 256 shown in Figure 3b is taken as the secret image. Different values of blending factor α in the range of 0 and 1 are applied during the performance evaluation of the proposed method. A higher value of blending factor signifies that good quality of the secret image is mingled within the cover image which gives good quality of extracted secret image whereas a lower value of alpha generates poor extracted secret image.

The scrambled secret image after carrying out Arnold cat map transformation is shown in Figure 3c. The results after performing spectral graph analysis i.e. SGWT on the cover image and scrambled image are displayed in Figures 4a and 4b; after carrying out SVD and alpha blending operations is shown in Figure 4c. The stego image *I* after applying the graph-based synthesis (Inverse SGWT) process looks like Figure 5a and extracted secret image *IS* extracted using decoding algorithm is shown in Figure 5b. It can be concluded from Figure 5 that the proposed approach offers improved visual quality of generated stego image as compared to existing wavelet-based approaches. The experiment is carried out on the different cover and stego images to check the performance based on different sizes and types of images as shown in Figures 6 and 7.

5.1 Performance analysis

The great visual quality of the stego image is the utmost indispensable feature of the steganography systems so that it makes it tough to notice or detect the presence of any secret data inside the cover media by the finders.

The performance of the proposed approach is investigated with one of the quality metrics known as Peak Signal to Noise Ratio (PSNR) [22]. It is measured by the alteration between the cover image and the generated stego image. PSNR is determined using Mean Square Error (MSE) as in Refs. [21, 23], *C* is an $m \times n$ size noise-free image and its noisy approximation is *I*, and then MSE is defined as:

$$MSE = \frac{1}{mn}\sum_{k=1}^{m}\sum_{l=1}^{n}[C(k,l) - I(k,l)]^2 \tag{10}$$

Here, *C(k,l)* and *I(k,l)* are the pixel value of cover image *C* and stego image *I* at k^{th} row and l^{th} column.

Now, PSNR in dB can be defined as:

$$PSNR = 10\ log_{10}\left(\frac{Max_C^{\ 2}}{MSE}\right) \tag{11}$$

Here, Max_C is the maximum possible pixel value of the image, in our approach Max_C is 255 as the image is a grayscale image, 8 bit representation is used to represent the image. The range of pixel values in our simulation is between 0 to 255. Lesser value of *MSE* and greater value of *PSNR* represent better quality of stego image which is hard to distinguish by the human eye. For the 8 bit image, the PSNR value between 30 to 50 dB is appreciable, where a higher value is better.

Another performance metric used to evaluate the performance of our approach is Normalized Cross-Correlation (NCC) [23]. NCC is accustomed to evaluate the degree of resemblance between two images. The value of NCC lies down in the range from -1 to 1. The value of NCC near 1 denotes a higher correlation or similarity between two images. Normalized Cross-Correlation is calculated using the following equation shown in Eq. (12).

$$\mathrm{NCC} = \frac{\sum_{k=1}^{m}\sum_{l=1}^{n} C(k,l) * I(k,l)}{\sum_{k=1}^{m}\sum_{l=1}^{n} C(k,l)^2} \tag{12}$$

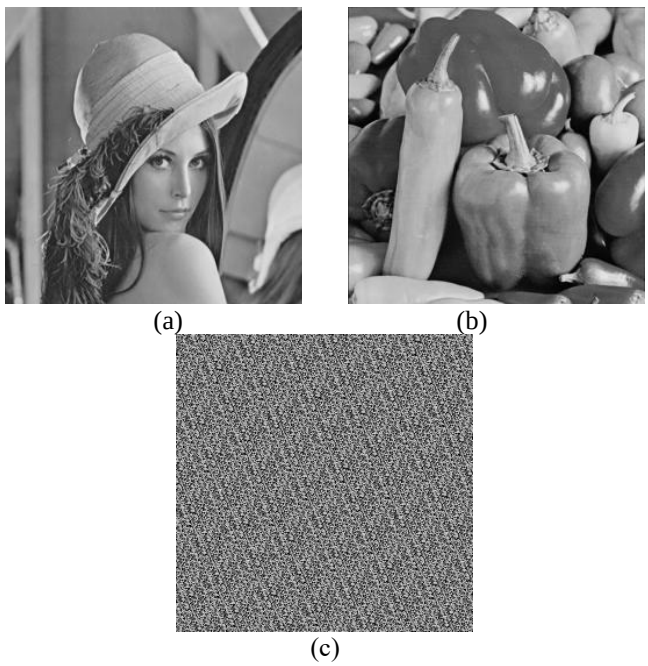
The other performance metric structural content (SC) as in Ref. [23] is defined as follows:

$$\mathrm{SC} = \frac{\sum_{k=1}^{m}\sum_{l=1}^{n} C(k,l)^2}{\sum_{k=1}^{m}\sum_{l=1}^{n} I(k,l)^2} \tag{13}$$

The average difference (AD) as in Ref. [23] is well-defined as follows:

$$AD = \frac{1}{mn}\sum_{k=1}^{m}\sum_{l=1}^{n}\left(C(k,l) - I(k,l)\right) \tag{14}$$

The lower value of structural content (SC) defines in Eq. (13) signifies that the image is of good quality. The average difference (AD) evaluated using Eq. (14) having a value of zero or less shows the good quality of the image.

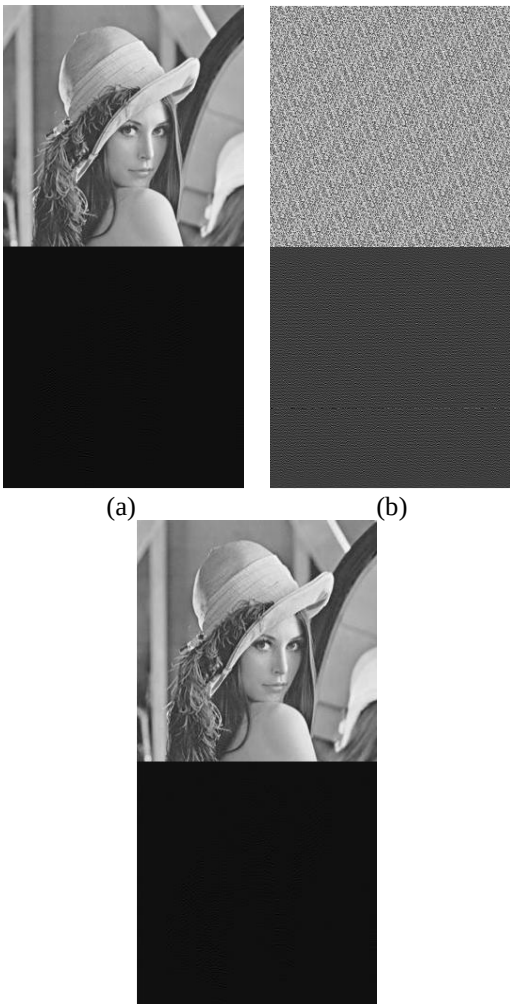


(a) (b) (c)

Figure 3. Original cover image Lenna (a), secret image Pepper (b), Arnold transformed scrambled secret image (c)

Table 1. Performance evaluation of proposed technique for estimation of PSNR and NCC at different values of α for cover image: Lenna.jpg and secret image: Pepper.jpg

α	PSNR-1	PSNR-2	NCC-1	NCC-2
0.01	63.156	5.1483	0.9999	0.4029
0.02	54.881	6.9391	0.9996	0.5357
0.025	52.2192	6.9476	0.9994	0.5844
0.030	50.0642	6.9976	0.9993	0.6228
0.035	48.2212	7.0122	0.9990	0.6598
0.04	46.5641	7.0018	0.9988	0.7032
0.45	45.0201	6.9465	0.9985	0.7583
0.05	43.7156	6.936	0.9982	0.7973
0.06	41.4749	6.9266	0.9975	0.8662
0.07	39.7876	7.004	0.9967	0.8843
0.08	38.3801	7.0940	0.9958	0.8863
0.09	37.1476	7.1661	0.9948	0.8849
0.10	36.0750	7.2634	0.9937	0.8767
0.20	27.2963	7.5120	0.9764	0.9011



(a) (b) (c)

Figure 4. GSP or spectral graph wavelet analysis of cover image C_{GA} (a), scrambled secret image S_{GA} (b), stego image I_{GA} (c) on α =0.25 and number of filters=2

The proposed technique is analyzed on the various values of α as shown in Table 1. It is analyzed, when the value of α is low, the value of PSNR-1(between the cover image and stego image) and NCC-1 (between cover and stego) is better but the NCC-2 (NCC between stego and cover) is low which means the features extracted from the stego image have poor visibility or less similarity index. The value of PSNR-1, PSNR-2, NCC-1 and NCC-2 is good when the value of α = 0.25, 0.30, 0.35. It is noted that when the value of α increases the PSNR-1 decreases and NCC-2 increases i.e. poor stego image and better-extracted image quality respectively. The experiment is performed on 2 channels, 3 channels, and 4 channels Meyer filters from the filter bank and analyzed the investigation results. The number of filters used in our approach is 2.

(a) (b)

Figure 5. Stego Image *I* (a) and extracted secret image *IS i.e.* Pepper (b)

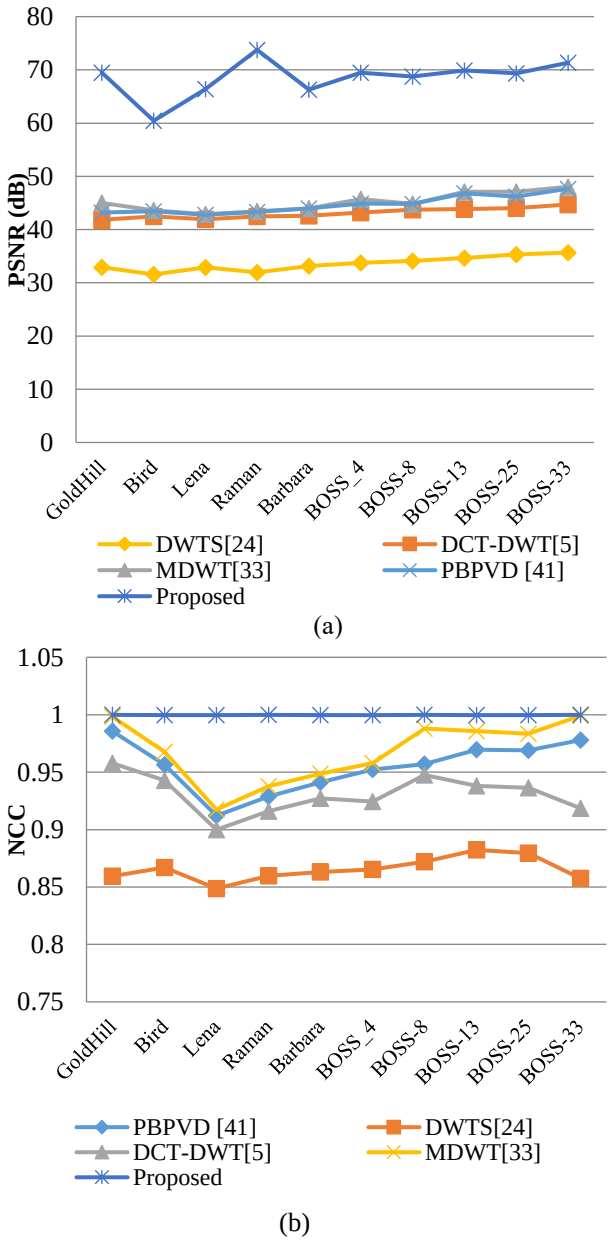


Figure 6. PSNR (a) and NCC (b) of different existing images on different techniques and proposed technique

Table 2. PSNR, NCC of different stego images and Baboon as secret image

Cover Image	Metric	Steganography Techniques				
		DWTS [24]	DCT-DWT [5]	MDWT [33]	PBPVD [41]	Proposed
GoldHill	**PSNR**	32.89	41.84	44.98	43.19	69.4828
Bird		31.57	42.45	43.60	43.45	60.4444
Lena		32.89	41.93	42.87	42.78	66.4022
Raman		31.92	42.45	43.46	43.31	73.7622
Barbara		33.15	42.57	43.97	43.97	66.2687
BOSS-4		33.74	43.19	45.69	44.86	69.4948
BOSS-8		34.12	43.74	44.82	44.79	68.7654
BOSS-13		34.68	43.86	47.09	46.80	69.8673
BOSS-25		35.30	44.02	47.11	46.21	69.3678
BOSS-33		35.69	44.71	48.03	47.67	71.3475
GoldHill	**NCC**	0.8595	0.9578	0.9983	0.9856	0.9999
Bird		0.8669	0.9429	0.9677	0.9564	0.9997
Lena		0.8487	0.8999	0.9174	0.9121	0.9998
Raman		0.8599	0.9162	0.9378	0.9289	0.9999
Barbara		0.8631	0.9273	0.9488	0.9412	0.9997
BOSS_4		0.8654	0.9244	0.9578	0.9523	0.9998
BOSS-8		0.8719	0.9475	0.9879	0.9569	0.9999
BOSS-13		0.8823	0.9382	0.9857	0.9695	0.9998
BOSS-25		0.8796	0.9365	0.9834	0.9691	0.9997
BOSS-33		0.8576	0.9185	0.9991	0.9778	0.9999

Table 3. PSNR, NCC and SC for stego images with different cover and secret images

Cover Image	Secret Image	DWT [23]			Proposed Technique		
		PSNR	NCC	SC	PSNR	NCC	SC
Deer	Baby	49.320	0.9943	1.0115	51.6336	0.9984	0.9968
Deer	Flower	47.943	0.9925	1.0152	58.2853	0.9994	0.9989
Coconut	Flower	52.391	1.008	0.9983	65.3415	0.9968	0.9936
Coconut	Baby	50.531	1.005	0.9898	55.4909	0.9902	0.9814
Leena	Pangram	34.0257	0.9691	-	48.6029	0.9989	0.9979

Table 4. AD for stego images with different cover and secret images

Cover Image	Secret Image	DWT [23]	Proposed Technique
		AD	AD
Deer.Jpg 316 X 380	Baby.jpg 458 X 500	0.5071	-0.0138
Deer.Jpg 316 X 380	Flower.jpg 300 X 450	0.7435	-0.0041
Coconut.jpg 768 X 1024	Flower.jpg 300 X 450	-0.3275	-0.0067
Coconut.jpg 768 1024	Baby.jpg 458 X 500	-0.5639	-0.0026

The proposed method is compared with existing recognized steganography techniques such as DWT based steganography (DWTS) [24], DCT and DWT based steganography (DCT-DWTS) [5], Modified DWT based image steganography (MDWT) [33], and Parity bit pixel value and differencing based data hiding technique (PBPVD) [41]. The performance of the algorithm is evaluated on well-known benchmark images like *Lenna*, *GoldHill*, *Barbara*, *Bird*, *Raman*, *Baboon*, *Deer Flower*, *baby*, and other images are taken from BOSSBase 1.01 Dataset [42]. Table 2 shows the comparison between the proposed technique and aforementioned techniques on different cover images and a common secret image. It is observed that our technique gives better PSNR and NCC of stego images when contrasted with other existing wavelet methods. The investigated results are plotted and shown in Figure 6. Table 3 and 4 show the comparison between proposed technique and DWT based technique [23] on different cover and different secret images. It is observed, proposed approach gives better PSNR and NCC with lower value of SC which signifies the good quality of stego image.

5.2 Robustness

Different image processing attacks are performed on proposed technique to check the robustness of the stego image. We performed sharpening, Gaussian noise, rotation, gamma correction and transform on image. In Gaussian noise attack the mean value is taken as zero and the variance is 0.5, in the rotation attack the angle is 30 degree.

Table 5. Comparison of proposed technique with others after performing image processing attacks (quality metric PSNR) for cover image GoldHill.tif and secret image Baboon.jpg

Attacks	Steganography Techniques			
	LSB	DWS	DCT-DWTS	Proposed
Sharpening	10.71	11.23	11.95	29.2300
Gamma Correction	10.05	21.91	25.54	56.8309
Gaussian Noise	10.06	16.27	18.69	27.6828
Transform	10.52	12.30	12.61	33.4972
Rotation	10.93	21.31	24.87	56.8301

The cover image GoldHill.jpg is taken as the cover image and Cameraman as a Secret image. It is observed from Table 5, the proposed technique is more robust than present techniques as compared to Refs. [5, 22, 24]. The proposed scheme offers better PSNR value as compared to other schemes under investigated image processing attacks as shown in Figure 7. The PSNR value of the attacked stego image is still good which shows that the stego image is not much disturbed with performed attacks by which quality of extracted image will not be not affected.

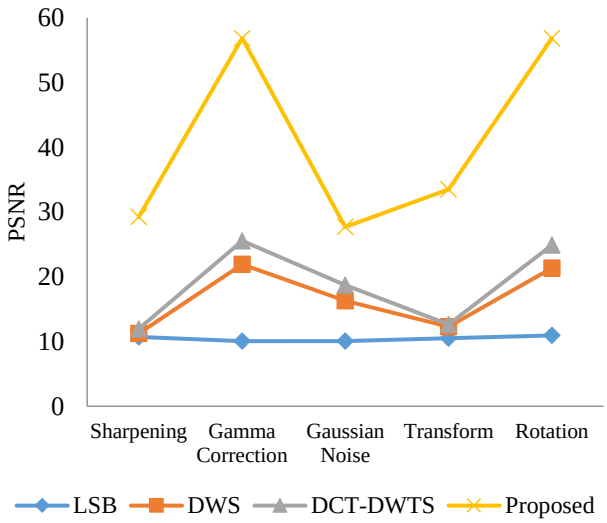


Figure 7. PSNR of stego image after performing attacks

6. CONCLUSION

For grayscale images, a graph wavelet-based safe and efficient steganography technique is suggested. Experiment results show that the suggested method improves the visual quality of stego and secret images in terms of PSNR, NCC, SC, and AD. The cover image is not required for this method to retrieve the hidden image. The suggested method is more resistant to different image processing attacks. The Arnold transform, SVD, and spectral graph wavelet improve the approach's robustness and security. It has been determined by comparing the findings that the suggested approach outperforms the other current methods.

REFERENCES

[1] Feng, B., Lu, W., Sun, W. (2015). Secure binary image steganography based on minimizing the distortion on the texture. IEEE Transactions on Information Forensics and Security, 10(2): 243-255. https://doi.org/10.1109/TIFS.2014.2368364

[2] Mahajan, P., Gupta, H. (2016). Improvisation of security in image steganography using DWT, Huffman encoding & RC4 based LSB embedding. 016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 523-529.

[3] Sehgal, P., Sharma, V.K. (2013). Eliminating cover image requirement in discrete wavelet transform based digital image steganography. International Journal of Computer Applications, 68(3): 37-42.

[4] Morkel, T., Eloff, J.H.P., Olivier, M.S. (2015). An overview of image steganography. Proceedings of the ISSA 2005 New Knowledge Today Conference, 29 June - 1 July 2005, Balalaika Hotel, Sandton, South Africa.

[5] Kumar, V., Kumar, D. (2010). Performance evaluation of DWT based image steganography. 2010 IEEE 2nd International Advance Computing Conference (IACC), pp. 223-228. https://doi.org/10.1109/IADCC.2010.5423005

[6] Shejul, A.A., Kulkarni, U.L. (2010). A DWT based approach for steganography using biometrics. 2010 International Conference on Data Storage and Data Engineering, pp. 39-43. https://doi.org/10.1109/DSDE.2010.10

[7] Rabie, T. (2012). Digital image steganograph: An FFT approach. In: Benlamri R. (eds) Networked Digital Technologies. NDT 2012. Communications in Computer and Information Science, vol 294. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-30567-2_18

[8] Patel, H., Dave, P. (2012). Steganography technique based on DCT coefficients. International Journal of Engineering Research and Applications, 2(1): 713-717. http://www.ijera.com/papers/Vol2_issue1/DK21713717.pdf.

[9] Mostafa, R., Ali, A.F., EI Taweal, G. (2015). Hybrid curvelet transform and least significant bit for image steganography. 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS), pp. 300-305. https://doi.org/10.1109/IntelCIS.2015.7397238

[10] Sifuzzaman, M., Islam, M.R., Ali, M.Z. (2009). Application of wavelet transform and its advantages compared to Fourier transform. Journal of Physical Science, 13: 121-134. http://inet.vidyasagar.ac.in:8080/jspui/handle/123456789/779.

[11] Rloul, O., Vetterli, M. (1991). Wavelets and signal processing. IEEE Signal Processing Magazine, 8(4): 14-38. https://doi.org/10.1109/79.91217

[12] Cheung, G., Magli, E., Tanaka, Y., Ng, M.K. (2018). Graph spectral image processing. Proceedings of the IEEE, 106(5): 907-930. https://doi.org/10.1109/JPROC.2018.2799702

[13] Shuman, D.I., Narang, S.K., Frossard, P., Ortega, A., Vandergheynst, P. (2013). The emerging field of signal processing on graphs: Extending high-dimensional data analysis to networks and other irregular domains. I EEE Signal Processing Magazine, 30(3): 83-98. https://doi.org/10.1109/MSP.2012.2235192

[14] Zhang, X. (2016). Design of orthogonal graph wavelet filter banks. IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society, pp. 889-894. https://doi.org/10.1109/IECON.2016.7793133

[15] Narang, S.K., Ortega, A. (2012). Perfect reconstruction two-channel wavelet filter banks for graph structured data. IEEE Transactions on Signal Processing, 60(6): 2786-2799. https://doi.org/10.1109/TSP.2012.2188718

[16] Hammond, D.K., Vandergheynst, P., Gribonval, R. (2011). Wavelets on graphs via spectral graph theory. Applied and Computational Harmonic Analysis, 30(2): 129-150. https://doi.org/10.1016/j.acha.2010.04.005

[17] Hamidi, H., Amirani, M.C., Arashloo, S.R. (2015). Local selected features of dual tree complex wavelet transform

for single sample face recognition. IET Image Processing, 9(8): 716-723. https://doi.org/10.1049/iet-ipr.2013.0663
[18] Lim, W.Q. (2010). The discrete shearlet transform: A new directional transform and compactly supported shearlet frames. I EEE Transactions on Image Processing, 19(5): 1166-1180. https://doi.org/10.1109/TIP.2010.2041410
[19] Da Cunha, A.L., Zhou, J., Do, M.N. (2006). The nonsubsampled contourlet transform: Theory, design, and applications. IEEE Transactions on Image Processing, 15(10): 3089-3101. https://doi.org/10.1109/TIP.2006.877507
[20] Perraudin, N., Paratte, J., Shuman, D., Martin, L.., Kalofolias, V., Vandergheynst, P., Hammond, D.K. (2016). GSPBOX: A toolbox for signal processing on graphs. arXiv:1408.5781.
[21] Khalili, M., Asatryan, D. (2013). Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map. IET Signal Processing, 7(3): 177-187. https://doi.org/10.1049/iet-spr.2012.0380
[22] Chan, C.K., Chang, L.M. (2003). Hiding data in image by simple LSB substitution. Pattern Recognition, 37(3): 469-474. https://doi.org/10.1016/j.patcog.2003.08.007
[23] Prabakaran, G., Bhavani, R. (2012). A modified secure digital image steganography based on discrete wavelet transform. 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1096-1100. https://doi.org/10.1109/ICCEET.2012.6203811
[24] Abdelwahab, A.A., Hassan, L.A. (2008). A discrete wavelet transform based technique for image hiding. 2008 National Radio Science Conference, pp. 1-9. https://doi.org/10.1109/NRSC.2008.4542319
[25] Archana, S., Antony Judice, A., Kaliyamurthie, K.P. (2013). A novel approach on image steganographic methods for optimum hiding capacity. International Journal of Engineering and Computer Science, 2(2): 378-385. https://www.ijecs.in/index.php/ijecs/article/view/166.
[26] Ganesan, P., Bhavani, P. (2013). A high secure and robust image steganography using dual wavelet and blending model. Journal of Computer Science, 9(3): 277-284. https://doi.org/10.3844/jcssp.2013.277.284
[27] Mukherjee, S., Roy, S., Sanyal, G. (2018). Image steganography using mid position value technique. Procedia Computer Science, 132: 461-468. https://doi.org/10.1016/j.procs.2018.05.160
[28] Rima, V.G., Lakshmi, V.S. (2019). Integer wavelet transform and Arnold transform based image steganography with cryptanalysis. 2019 International Conference on Communication and Electronics Systems (ICCES), pp. 673-678. https://doi.org/10.1109/ICCES45898.2019.9002412
[29] Wyld, D.C., Zizka, J., Nagamalai D. (eds). (2012). Advances in Computer Science, Engineering & Applications. Advances in Intelligent Systems and Computing (Springer, Berlin, Heidelberg, vol. 167).
[30] Subhedar, M.S., Mankar, V.H. (2019). Image steganography using contourlet transform and matrix decomposition techniques. Multimedia Tools and Applications, 78: 22155-22181. https://doi.org/10.1007/s11042-019-7512-9
[31] Subhedar, M.S., Mankar, V.H. (2020). Secure image steganography using framelet transform and bidiagonal SVD. Multimedia Tools and Applications, 79: 1865-1886. https://doi.org/10.1007/s11042-019-08221-9
[32] Ghasemi, E., Shanbehzadeh, J., Fassihi, N. (2012). High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform. In: Ao S., Castillo O., Huang X. (eds) Intelligent Control and Innovative Computing. Lecture Notes in Electrical Engineering, vol 110. Springer, New York, NY. https://doi.org/10.1007/978-1-4614-1695-1_30
[33] Kumar, V., Kumar, D. (2018). A modified DWT-based image steganography technique. Multimedia Tools Appl., 77: 13279-13308. https://doi.org/10.1007/s11042-017-4947-8
[34] Sharma, V.K., Srivastava, D.K., Mathur, P. (2018). Efficient image steganography using graph signal processing. IET Image Processing, 12(6): 1065-1071. https://doi.org/10.1049/iet-ipr.2017.0965
[35] Lakshmi Sirisha, B. (2020). Image steganography based on SVD and DWT techniques. Journal of Discrete Mathematical Sciences and Cryptography, 23(3): 779-786. https://doi.org/10.1080/09720529.2019.1698801
[36] Narang, S.K., Ortega, A. (2013). Compact support biorthogonal wavelet filter banks for arbitrary undirected graphs. IEEE Transactions on Signal Processing, 61(19): 4673-4685. https://doi.org/10.1109/TSP.2013.2273197
[37] Hammond, D.K., Vandergheynst, P., Gribonval, R. (2019). The spectral graph wavelet transform: Fundamental theory and fast computation. In: Stanković L., Sejdić E. (eds) Vertex-Frequency Analysis of Graph Signals. Signals and Communication Technology. Springer, Cham. https://doi.org/10.1007/978-3-030-03574-7_3
[38] Leonardi, N., Van De Ville, D. (2011). Wavelet frames on graphs defined by fMRI functional connectivity. IEEE International Symposium on Biomedical Imaging: From Nano to Macro, Chicago, IL, pp: 2136-2139. https://doi.org/10.1109/ISBI.2011.5872835
[39] Wu, L., Zhang, J., Deng, W., He, D. (2009). Arnold transformation algorithm and anti-Arnold transformation algorithm. 2009 First International Conference on Information Science and Engineering, pp. 1164-1167. https://doi.org/10.1109/ICISE.2009.347
[40] William, F. (2014). Numerical Linear Algebra with Applications. Academic Press.
[41] Hussain, M., Wahab, A.W.A., Ho, A.T.S., Javed, N., Jung, K.H. (2017). A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. Signal Processing: Image Communication, 50: 44-57. https://doi.org/10.1016/j.image.2016.10.005
[42] Bas, P., Filler, T., Pevný, T. (2011). Break our steganographic system: The ins and outs of organizing BOSS. In: Filler T., Pevný T., Craver S., Ker A. (eds) Information Hiding. IH 2011. Lecture Notes in Computer Science, vol. 6958.