Soft Computing (2018) 22:1555–1567
https://doi.org/10.1007/s00500-017-2944-5

FOCUS

An adaptive hybrid fuzzy-wavelet approach for image steganography using bit reduction and pixel adjustment

Imran Shafi[1] · Muhammad Noman[2] · Moneeb Gohar[3] · Awais Ahmad[4] · Murad Khan[5] · Sadia Din[6] · Syed Hassan Ahmad[7] · Jamil Ahmad[8]

Published online: 11 December 2017

Abstract
Transform-based techniques partially address challenges like robustness and the imperceptibility in image steganography. Such approaches, however, increase the memory requirement and reduce the quality of the cover image and hiding capacity. Moreover, the steganography is always coupled with cryptography to strengthen the confidentiality. This paper presents an adaptive hybrid method for image steganography procedure based on bit reduction and pixel adjustment using the fuzzy logic and integer wavelet transform technique. The fuzzy set theory provides powerful tools to represent and process human knowledge in the form of fuzzy if-then rules that can resolve difficulties in image processing arising due to the uncertainty of the data, tasks, and results. We apply a bit reduction algorithm to each byte of the data which are to hide in the cover image. This decreases the memory usage and increases the capacity. The embedding of the input text into the cover image distorts the cover image. Hence, to minimize the visual difference between the cover image and the text embedded image, an optimum pixel adjustment algorithm is applied to the text embedded image. Simulation results demonstrate the effectiveness of our proposed approach.

Keywords Steganography · Watermarking · Cryptography · Fuzzy logic · Integer wavelet transform · Optimum pixel adjustment algorithm

1 Introduction

Data have been of importance throughout all ages from ancient kingdoms to modern-day countries and from small-scale private institutions to large-scale commercial organizations; nobody can deny the threats faced due to unwanted preying eyes and hence the importance of hiding or concealing important data. On a smaller or personal scale, we just

Communicated by M. Anisetti.

✉ Awais Ahmad
aahmmad.marwat@gmail.com

Imran Shafi
imranshafi@ceme.nust.edu.pk

Muhammad Noman
noman049@gmail.com

Moneeb Gohar
moneebgohar@gmail.com

Murad Khan
murad.csit@suit.edu.pk

Sadia Din
saadia.deen@gmail.com

Syed Hassan Ahmad
s.h.ahmed@ieee.org

Jamil Ahmad
jamil@ieee.org

[1] National University of Sciences and Technology, Islamabad, Pakistan

[2] Abasyn University, Islamabad Campus, Islamabad, Pakistan

[3] Department of Computer Science, Bahria University, Islamabad, Pakistan

[4] Department of Information and Communication Engineering, Yeungnam University, Gyeongsan, Republic of Korea

[5] Department of Computer Science, Sarhad University of Science and Information Technology, Peshawar, KPK, Pakistan

[6] School of Computer Science and Engineering, Kyungpook National University, Daegu, Republic of Korea

[7] University of Central Florida, Florida, USA

[8] Kohat University of Science and Technology, Kohat, Pakistan

apply passwords to hide data, but on a larger and professional scale, this is just not enough, and we have to apply professional data hiding techniques such as watermarking, cryptography and steganography. Steganography is the field of science for hiding the secret information into text, image or video in such a way that no one can make a guess of hidden information. It is a form of security through obscurity (Simmons 1984; Wu and Hwang 2007).

The first recorded act of steganography is of Demaratus, a Greek citizen who initially used this idea. At a time when the Persians were planning an attack on Greece, Demaratus came to know and warned Greece of the attack. To keep the message out of the reach of prying eyes and unwary interceptors, he came up with the idea of hiding the message within a wax tablet. He scraped away all the wood from the tablet until the wood was exposed. On it, he scraped his message and covered it with wax again so that it looked like a normal wax tablet. His technique proved to be successful, and the message reached Greece without the Persians noticing it, and hence, the inevitable danger was combated, and the Greeks defeated the invading Persian army. This was first known the case of steganography, but since then, the complexity of steganography has increased, and this technology has advanced too quickly and is a topic of interest to a large scientific community (Wu and Hwang 2007).

There are two techniques to protect the information, i.e., steganography and cryptography. Steganography hides the information in the text, image or video and differs from encryption where the cryptography scrambles the information into the non-understandable information. Both the steganography and cryptography are not perfect alone to achieve the confidentiality, so the strength of steganography lies in combining it with cryptography. It is the cover object which determines which suitable steganographic techniques should be followed. Various digital mediums that can be used for steganography are described as under and are shown in Fig. 1.

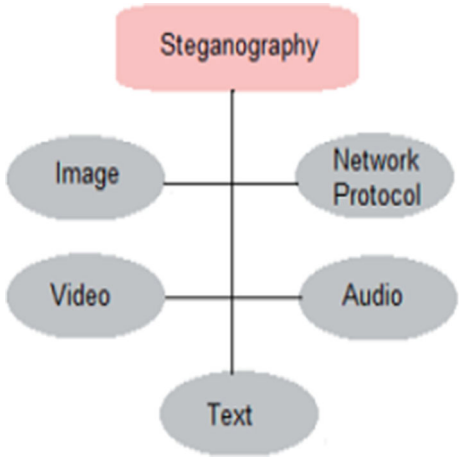


Fig. 1 Digital medium to achieve steganography

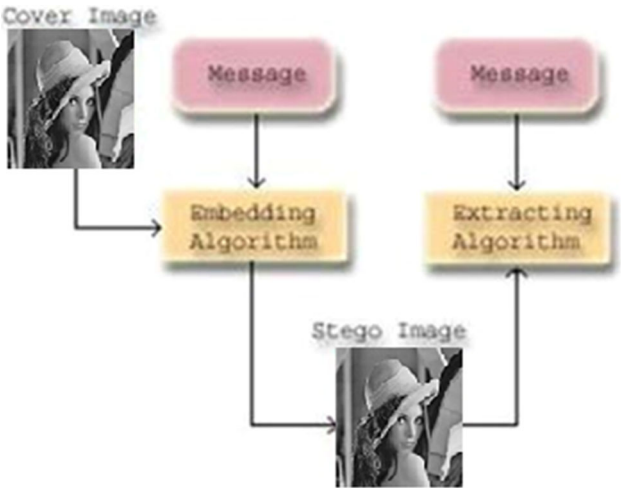


Fig. 2 Image steganography without stego-key

(a) *Image Steganography* Hiding the information in an image by taking the image called cover image and embedding into it is known as image steganography. It is achieved by embedding the bits into pixels.
(b) *Network Steganography* Taking the network protocols such as TCP, UDP, ICMP, IP as cover image is known as network protocol steganography.
(c) *Video Steganography* Hiding the information in the video is called video steganography. It is the most complex type of stangnograpghy, and intelligence can reveal from it quickly.
(d) *Audio Steganography* Hiding the information in audio files is called audio steganography. By the invent of VOIP services it gained popularity.
(e) *Text Steganography* Hiding the information in the text is called text steganography. It is the most common type of steganography in which some tabs, white spaces, capital letters, are used to achieve information hiding.

All in all, any file format, i.e., image, video or audio, can be used to conceal data, but our main focus will remain in hiding data in a digital image, as it is the most favorable hiding mode for secret messages due to its high hiding capacity and good distortion tolerance (Wu and Hwang 2007; Chen 2003).

In the image, steganography information is hidden into a cover image which then makes a stego-image which is sent to the receiving party. The receiving party extracts the stego-image with or without key called stego-key. Image steganography is shown in Fig. 2 without stego-key, in which embedding algorithm requires a cover image with a message for embedding. A stego-image is simply sent to extracting algorithm as an output of embedding algorithm to reveal the stego-image. Figure 3 shows image steganography with

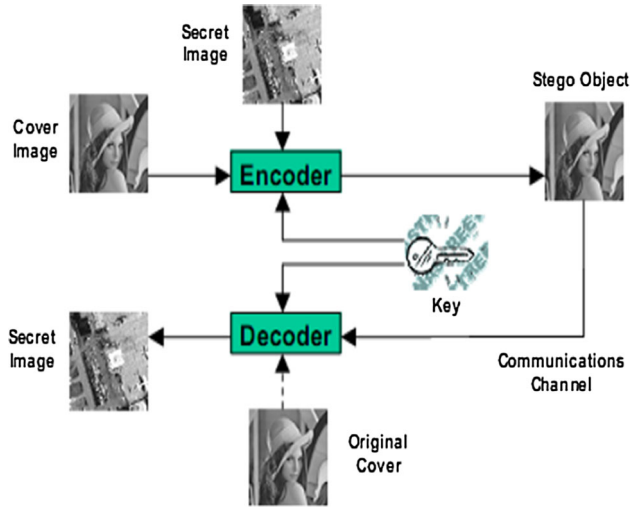


Fig. 3 Image steganography with stego-key

stego-key, where extraction algorithm required a security key generated by embedding algorithm for extraction procedure.

The stenographic techniques can be classified by either the cover image or the other data hiding schemes. Further data concealing or hiding can be achieved by the transforms two methods, i.e., by domain techniques and spatial domain techniques (Chan and Cheng 2004). Least-significant bit encoding (LSB) is an example of the spatial domain techniques, and it is the simplest steganographic technique that embeds the bits of the message directly into the least-significant bit plane of the cover image in a deterministic sequence (Chen 2003). Due to the simplicity LSB embedding is mostly used as it also allows high perceptual transparency. It is also worth to mention that when we consider robustness and tamper resistance, the detection becomes easy as it provides easy manipulation of stego image. Additionally, an attacker can easily remove the message (Chan and Cheng 2004). Spatial domain techniques are broadly classified into PVD, EBE, RPE, pixel intensity-based, text-based, histogram shifting-based, labeling or connectivity method, mapping pixel to hidden data techniques (Changa et al. 2008; Zayed 2005). Two issues such as robustness and the imperceptibility of the spatial domain techniques are resolved by the transformed techniques (Changa et al. 2008; Zayed 2005). Fourier transform (FT), discrete wavelet transform (DWT), and discrete cosine transform (DCT) are most commonly used transforms (Lai and Chang 2006). However, the spatial domain and the transform domain techniques have their disadvantages.

This paper proposes a hybrid technique which adaptively hides data in integer wavelet coefficients after image fuzzification and employs an optimum pixel adjustment algorithm to maintain visual quality of the stego-image along with a bit reduction algorithm to increase the hiding capacity of the stego-image. Bit reduction algorithm is applied to each byte of the secret data which needs for embedding in the image's cover; this decreases the memory usage and eventually increases the hiding capacity of the cover image. The embedding of the input text into the cover image may result in the distorted image cover image. To minimize the visual difference between the cover image and the text embedded image, an optimum pixel adjustment algorithm is applied to the text embedded image.

The rest of this paper is organized as follows. The review of approaches for integer wavelet transform is performed in Sect. 2. Section 3 describes the proposed approach. The proposed schemed is validated through experimental results and discussed in Sect. 4. The research work is concluded in Sect. 5.

2 Background and literature survey

A famous mathematician Alfred Haar proposed Haar wavelet in the year 1909 (Lai and Chang 2006; Lillo and Shih 2008). Later, the term wavelet in 1984 was used by the Morlet and the physicist Alex Grossman. Before 1985, only Yveseyer knew about the integer wavelet transform. Ingrid Daubechies devised the concept of multi-resolution analysis proposed by Stephane Mallat and Meyer in 1988 and the same year, a mechanism for the compaction of orthogonal wavelet systematical method. In 1989, Mallat proposed the fast wavelet transform. The major reason behind using the wavelet transform is that it allows for hiding data in areas to which the human visual system (HVS) is less prone. These include the HL, HH and LH bands. It can be shown in Figs. 4 and 5. This maintains good visual quality of the stego-image while maintaining a good level of robustness also.

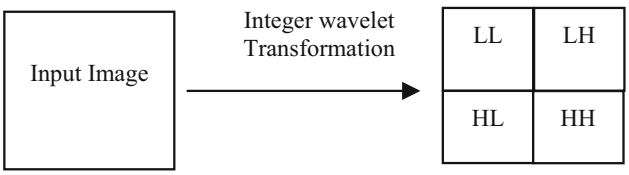


Fig. 4 Applying 2D integer wavelet transformation on 2D matrix

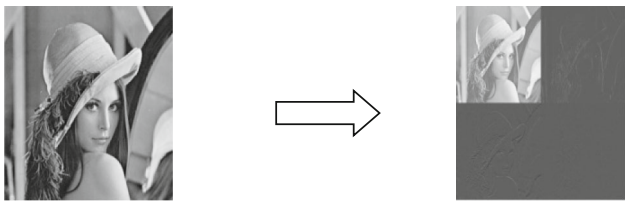


Fig. 5 Applying 2D integer wavelet transformation on image

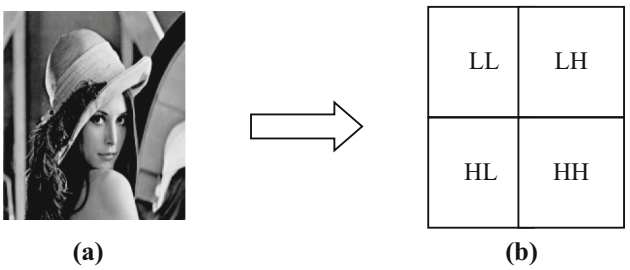


Fig. 6 Original Lena image and how it decomposes using one level integer wavelet transformation

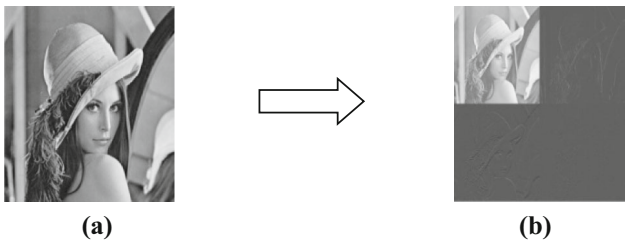


Fig. 7 **a** Original Lena image and **b** one level of 2D integer wavelet transformation decomposition

The integer wavelet transform maps an integer data set into another integer data set (Westfeld 2001; Tseng and Chnag 2004). Now the question that arises is why the IWT is preferred over other transforms such as DCT and DWT. The answer lies in the coefficients which form the matrix as a result of the operations of average and difference. The coefficients which are formed as a consequence of these operations are floating point numbers. This is good for precision, but the issue arises when data are hidden and transforms like the inverse wavelet transforms are applied to the cover image. Truncations of the floating point numbers result in important information loss which is unwanted. Hence, we use the integer wavelet transformation so that all operations are performed in integers, and hence, no such loss occurs.

The integer wavelet transform can be mentioned regarding averages and differences are given by the equations:

$$D_{(1,n)} = S_{(0,2n+1)} - S_{(0,2n)} \tag{1}$$

$$S_{(1,n)} = S_{(0,2n)} + \text{floor}\left[\left(D_{(1,n)}/2\right)\right]. \tag{2}$$

The first equation is used to calculate the differences, and second equation is used for the calculations of the averages. The averages are the low-frequency components of the image, whereas the differences are showing the high-frequency components of the cover image. The above equations can compute an only 1D average or cover image's differences. To fix this issue and obtain the full transformation, we have to apply these equations twice.

The inverse integer wavelet transform can be calculated by the following equations:

$$S_{(0,2n)} = S_{(1,n)} - \text{floor}\left[\left(D_{(1,n)}/2\right)\right]. \tag{3}$$

$$S_{(0,2n+1)} = D_{(1,n)} + S_{(0,2n)} \tag{4}$$

Similarly like the integer wavelet transformation, the above equations can compute only 1D inverse integer wavelet transformation of the transformed image; to obtain the full inverse transformation, we have to apply these equations twice (Figs. 6, 7).

3 The proposed adaptive steganographic approach

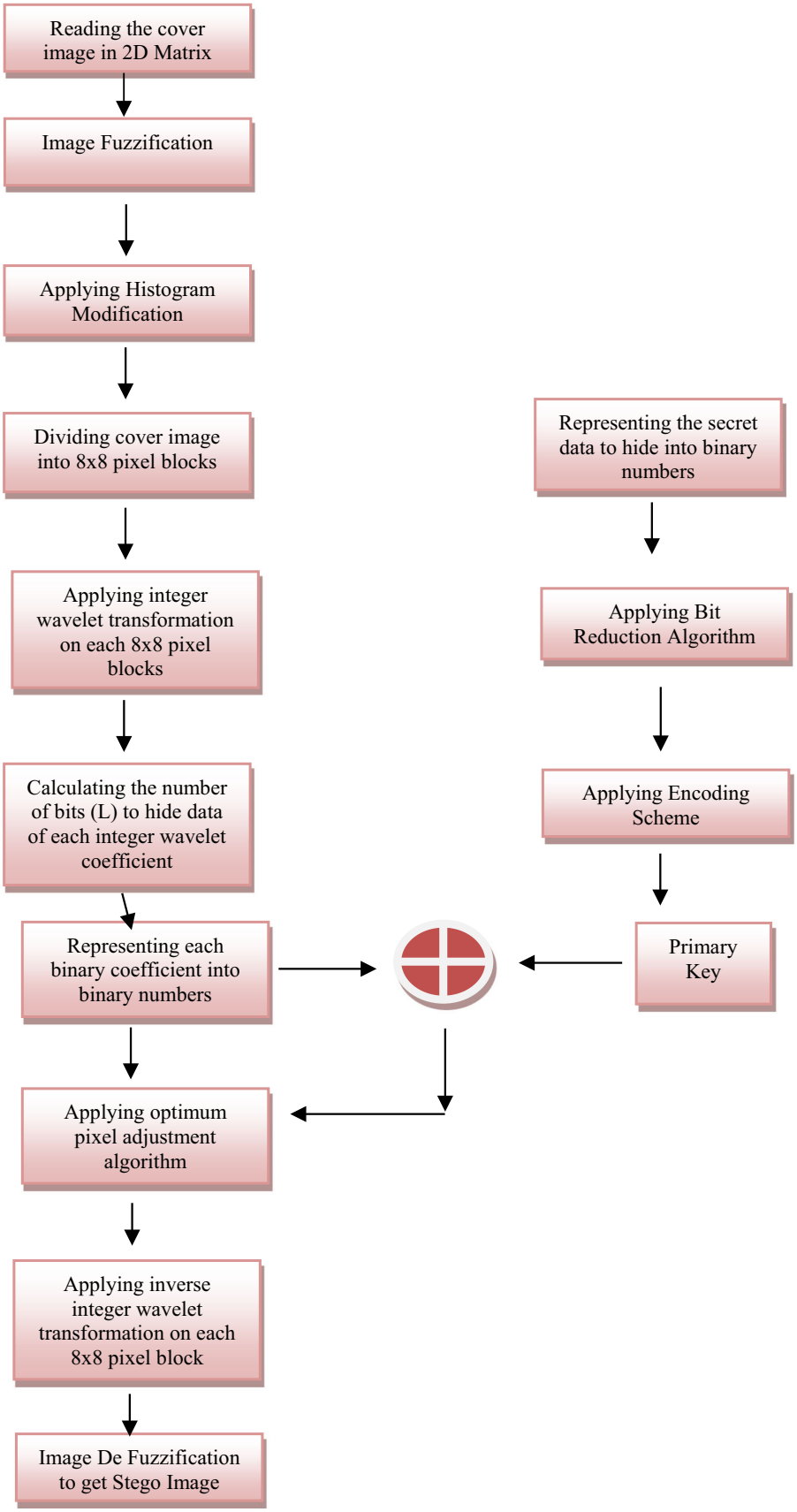
The implemented system is an improved adaptive data hiding scheme, by selecting the coefficient of the original image of the wavelet of the original image by modifying the message bits. The data which are going to be inserted in the original cover image are first reduced by using the bit reduction algorithm so that more data can be expressed in fewer bits which increase the hiding capacity of our system than the previously implemented system. Before inserting data in the cover image, an encoding technique is used to scramble the text so that it is of no use for the intruder if he receives it. After applying the encoding scheme, the secret text is inserted in the coefficients of integer wavelet transformed which are randomly selected. The hiding capacity of each of these coefficients varies for hiding the message bits. In our research work, we have modified the hiding capacity functions used in earlier functions. Once we have inserted the data, then we apply optimum pixel algorithm for the sake of error reduction. There are four types of implementations:

(1) Good visualization and low hiding capacity
(2) Medium visualization and medium hiding capacity
(3) Ordinary hiding capacity and image visualization
(4) Low visualization and high bits hiding capacity.

The procedure which we adopt for steganography consists of two phases

1. Embedding phase
2. Extraction phase.

3.1 Embedding phase



The embedding phase is divided into two portions 'Text portion' and 'Image portion.' In the above figure, the portion of figure is 'Text portion, ' and that part to the left is 'Image portion.'

(1) *Text Portion*

(a) *Step 1* The input data are converted to 8-bit binary number Highlight all author and affiliation lines.
(b) *Step 2* Bit reduction algorithm is applied to the input data to reduce the number of bits which are to be inserted into the cover image. By doing this, we are reducing the number of bits which we are going to insert in the image.
(c) *Step 3* This step involves enhancing date security, and for this, an encoding scheme is applied to the input data

(2) *Image Portion*

(a) *Step 1* First step is the fuzzification of the cover image. Before we can apply a fuzzy processing to an image, it is necessary to map the original image into the fuzzy domain. Since in some cases we are trying to represent a concept or characteristic of the image related to the perception, we may call the new domain the perception domain (Gupta et al. 1987).
(b) *Step 2* Reading the cover image pixel value information in the 2D array to know the whole content of the cover image.
(c) *Step 3* Checking the histogram of the cover image and applying the histogram modification to avoid overflow and underflow in the cover image. The histogram modification is the process of limiting the coefficient value between 15 and 240. All the values of the coefficient which are less than 15 are changed to 15, and all those values which are greater than 240 are set to 240. This is done to avoid the coefficient values to exceed greater than 255 or to decrease less than 0 when data are inserted into the cover image.
(d) *Step 4* Dividing the cover image into 8×8 non-overlapping blocks.
(e) *Step 5* Select Applying the Integer Wavelet Transformation on each 8×8 block.
(f) *Step 6* Calculating the hiding capacity of the cover image (L). The "L" is the maximum number of bits of the cover image which we can change.

$$L = \begin{cases} k+3, & \text{if } C_0 \geq 2^{k+3} \\ k+2, & \text{if } 2^{k+2} \leq C_0 < 2^{k+3} \\ k+1, & \text{if } 2^{k+1} \leq C_0 < 2^{k+2} \\ k+1, & \text{if } C_0 < 2^{k+1} \end{cases}$$

where C_0 is the value of each pixel. The 'k' is the minimum number of bits that we can use in each coefficient. The steganography system can be divided into four different cases depending on the values of L.

The cases are discussed as follows:

Case 1: $k = 1$ for LH, HL HH and 2 bits for the LL-sub band. The hiding capacity is low, and visual quality is high for stego-image.
Case 2: $k = 2$ for LH, HL, HH and 2 bits for the LL-sub band. It is suitable for applications requiring average hiding capacity and average visual quality. As compared with Case 1, using $k = 2$ increases the hiding capacity of the image but deteriorates the visual quality
Case 3: $k = 3$ for LL, HL, HH and 2 bits for the LL-sub band. It is suitable for applications which require good hiding capacity and average visual quality.
Case 4: $k = 4$ for LH, HL, HH and 0-bit for LL-sub band. Regarding hiding capacity, Case 4 is considered the best among all the cases of data embedding, but regarding visual quality, it is considered the worst. This case is suitable for low-quality stego-image but more hiding capacity.

(g) *Step 7* Each coefficient of the cover image is represented as binary numbers, and some of the bits according to our secret key are replaced with the text which is already in binary numbers.
(h) *Step 8* In this step, the optimum pixel adjustment algorithm is applied. The objective of the optimum pixel adjustment (OPA) algorithm is to reduce the difference of error between original coefficient value and the altered coefficient value by checking the right next bit to the modified LSBs so that the resulted change will be minimal (Ramaiya et al. 2013a, b).

The OPA (optimum pixel adjustment) algorithm is dependent on the difference (ζ_i) between the original value $P_i(x, y)$ and the modified value $P_i'(x, y)$ of selected cover and the stego-image or modified image in which text is inserted.
The difference (ζ_i) can be calculated by

$$\zeta_i = P_i'(x, y) - P_i(x, y) \tag{5}$$

After calculating the difference (ζ_i), the algorithm modifies the changed value (i.e., minimizing the error between the original value and modified value) in the following manner:

Case 1: $-2^k < \zeta_i < -2^{k-1}$
If $P_i'(x, y) < 256 - 2^k$
Then $P_i(x, y)^* = P_i'(x, y) + 2^k$
Else $P_i(x, y)^* = P_i'(x, y)$

Case 2: $-2^{k-1} \leq \zeta_i \leq 2^{k-1}$
$P_i(x, y)^* = \mathrm{P}_i'(x, y)$

Case 3: $2^{k-1} \leq \zeta_i \leq 2^k$
If $P_i'(x, y) \geq 2^k$
Then $P_i(x, y)^* = P_i'(x, y) - 2^k$
Else $P_i(x, y)^* = P_i'(\mathrm{x,y})$

(i) *Step 9* In this step, the inverse 2D-inverse integer wavelet transformation is applied on each of the (8 × 8 pixels) blocks.
(j) *Step 10* In the last step, image defuzzification is applied on the image obtained in the above step to get the stego-image.

3.2 Extraction phase

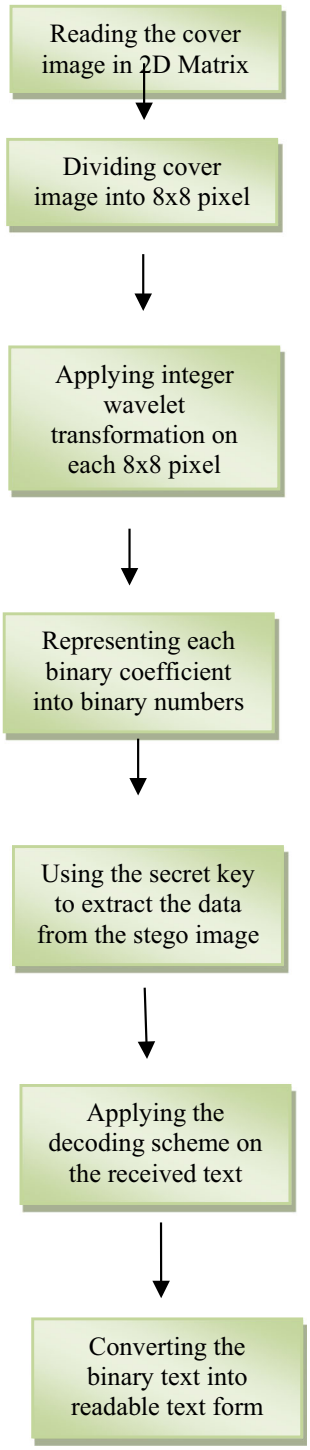


Fig. 8 Fuzzification of the cover image

50	52	50	49	53
49	125	240	243	49
50	240	242	120	50
51	243	242	242	120
49	243	243	243	49
50	120	240	243	50
50	52	50	49	53

Fuzzification

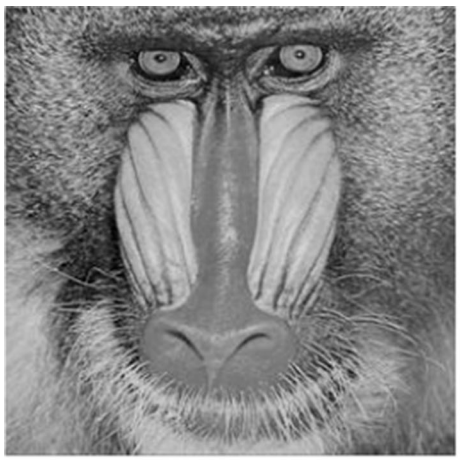
0.2	0.2	0.2	0.19	0.2
0.19	0.49	0.94	0.95	0.19
0.2	0.94	0.95	0.47	0.2
0.2	0.95	0.95	0.95	0.47
0.19	0.95	0.95	0.95	0.19
0.2	0.47	0.94	0.95	0.2
0.2	0.2	0.2	0.19	0.2

Fuzzy operator

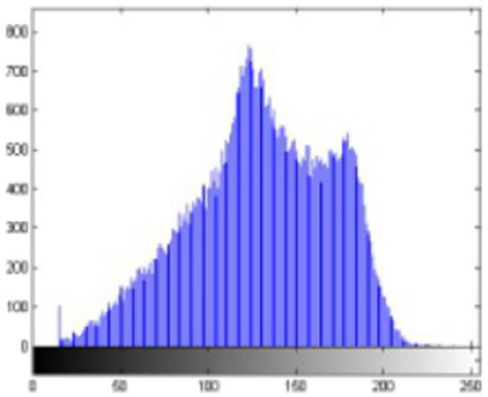
0.1	0.1	0.1	0.1	0.1
0.1	0.2	1	1	0.1
0.2	1	1	.2	0.1
0.2	1	1	1	0.2
0.2	1	1	1	0.1
0.2	02	1	1	0.1
0.2	0.2	0.2	0.1	0.1

defuzzification

0	0	0	0	0
0	255	255	255	0
0	255	255	0	0
0	255	255	255	0
0	255	255	255	0
0	0	255	255	0
0	0	0	0	0

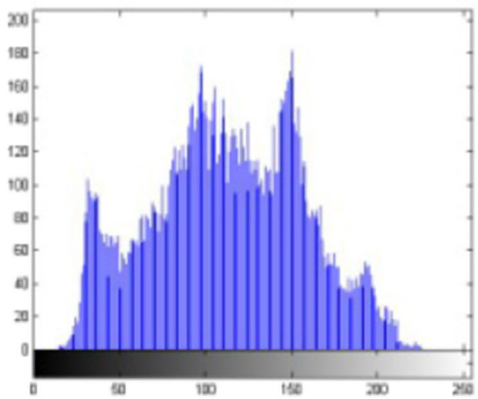


(a)



(b)

(c)



(d)

Fig. 9 Cover images and their corresponding histograms. **a** Cover image, **b** histogram, **c** cover image, **d** histogram

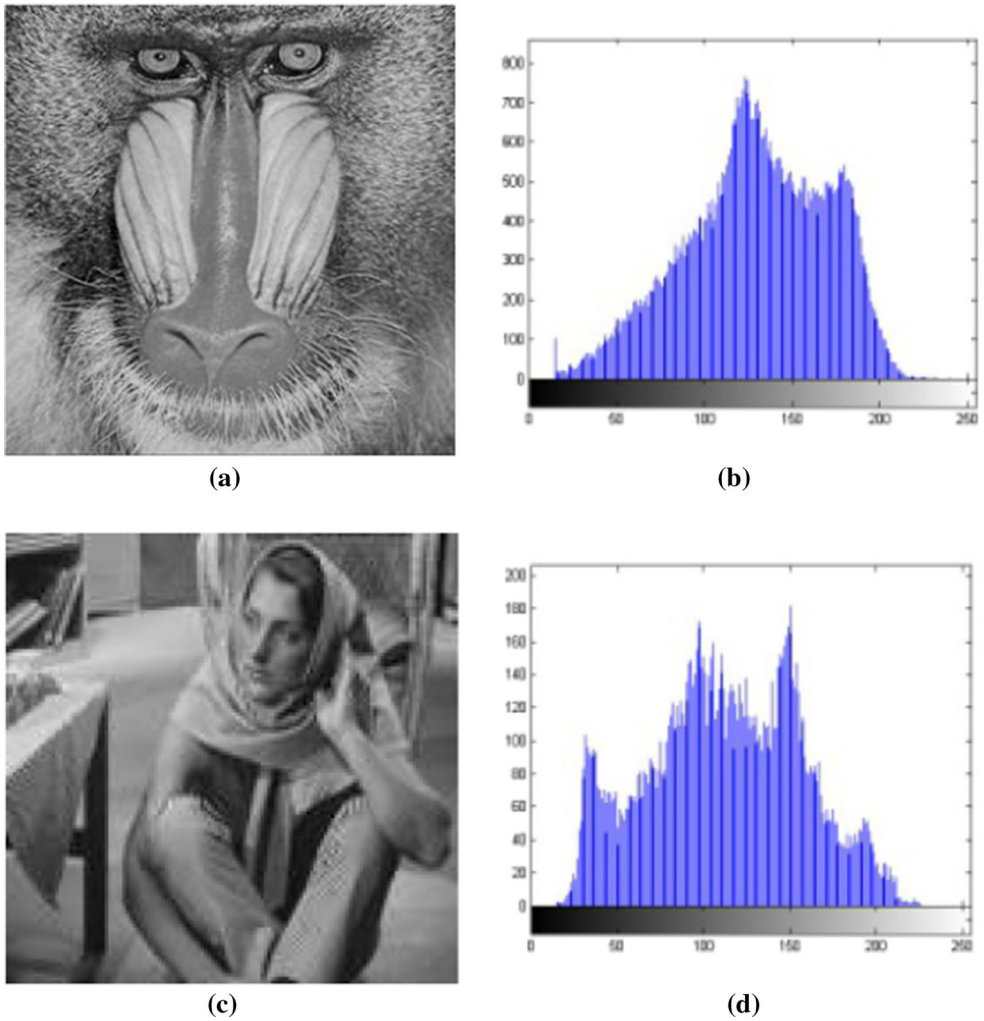


Fig. 10 Output stego-images of Case I for embedding data and their corresponding histograms. **a** H.C. = 30%, **b** PNR = 45 db, **c** H.C. = 32%, **d** PNR = 44 db

(a) *Step 1* Reading the cover image pixel value information in the 2D array to know the whole content of the cover image.
(b) *Step 2* Dividing the cover image into 8 × 8 non-overlapping blocks.
(c) *Step 3* Applying the integer wavelet transformation on each 8 × 8 blocks.
(d) *Step 4* Each coefficient of the stage image is represented as binary numbers.
(e) *Step 5* Using the same secret key as it was used in embedding phase the text is extracted from the stage image.
(f) *Step 6* In this step, the decoding algorithm is applied to the received text to decode the original embedded text.
(g) *Step 7* In the final step, the received text which is in binary format is converted into readable text format.

4 Experimental results and discussion

To check the performance of proposed technique, the implemented system is applied on two 512 × 512, 8-bit grayscale images shown in the figure. Figure 8 shows the original cover images and their histogram analysis

Two widely used concepts are mainly used for evaluation of the proposed technique.

Imperceptibility/Stego-image quality

Imperceptibility determines the difference that exists in the original cover. It can be noted that if we achieve the high-quality stego-image, the visibility of the image is compromised. PSNR is used to determine the stage-image quality.

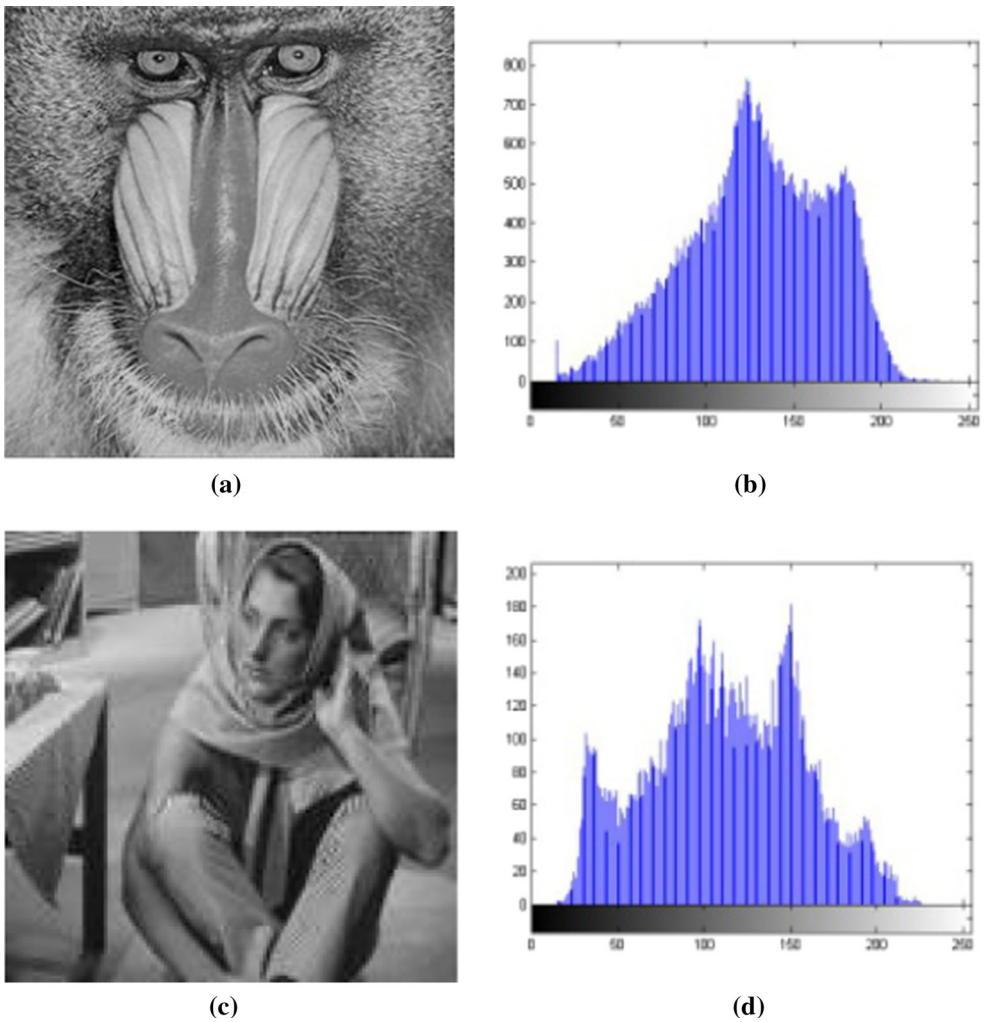


Fig. 11 Stego-images are showing the output of Case II for insertion of data and their histograms accordingly. **a** H.C. = 35%, **b** PNR = 45 db, **c** H.C. = 37%, **d** PNR = 44 db

The PSNR, an image of size $M \times N$, is calculated by

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right) \tag{6}$$

And

$$\text{MSE} = \left(\frac{1}{M \times N}\right)\sum_{x=1}^{M}\sum_{y=1}^{N}\left(P\left(x, y\right) - P'\left(x, y\right)\right) \tag{7}$$

The mean square error (MSE), $P(x, y)$ used for value in the cover image of the pixel value. $P'(x, y)$ is used to specify pixel value at position (x, y) in the stego-image. A high PSNR shows the better image, and lower the PSNR, the bad the image. Additionally, it has also been observed that grayscale human visual system (HVS) is not able to detect distortions in stego-images of more than 36 dB PSNR (Grover and Mohapatra 2013; Wang et al. 2014)

4.1 Hiding capacity/payload

It shows the amount of data to hide in the cover image without compromising the cover image quality. The hiding capacity of the algorithm is not a mandatory feature of an algorithm because it does not matter how much data an algorithm can hide.

Figure 9 shows the resulting stego-images (by applying case $k = 1$ for all subbands) in which a binary stream is embedded in random order. The percentage of the cover image size is measuring the hiding capacity (H.C.). The val-

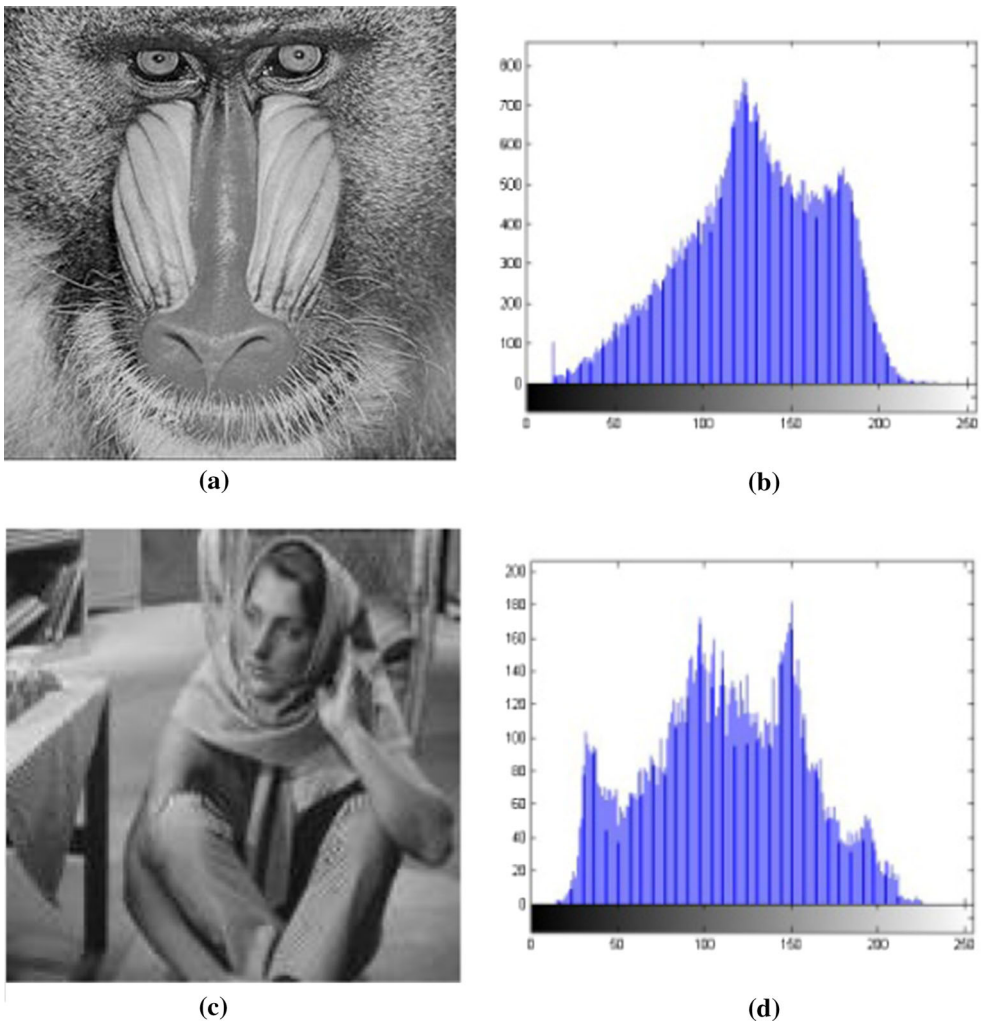


Fig. 12 Output of the stego-images of Case III after inserting data along with histograms. **a** H.C. = 40%, **b** PNR = 45 db, **c** H.C. = 42%, **d** PNR = 44 db

ues of hiding capacity vary from 20 to 60%. The PSNR ranges from 37 to 50 dB for the stage images.

Histograms in Fig. 9 show the comparison of stego-image with the Barb image. However, for the case of Baboon image, there is significant change seen, but the visual quality is not compromised.

Figures 10, 11 and 12 show the image results for Case 2 ($k = 2$ for all sub bands), Case 3 ($k = 3$ for all sub bands) and Case 4 ($k = 4$ for all sub bands), respectively (Fig. 13).

5 Conclusion

There exist many techniques for hiding and detecting the information, but no one is ideal in all situations. No scheme guarantees the error detection for finding the secret information (Wang et al. 2014). One of the reasons for this failure to detect the information is that cover image has no information about the stego information (Valenzise et al. 2013; Hou et al. 2012; Cao and Han 2012) (whereas, interested readers are referred to Ahmad et al. (2016a, b) and Paul et al. (2016) for more details.)

The proposed data hiding technique implemented in this paper inserts the secret data into the image using the hybrid fuzzy logic, and integer wavelet transformation is efficient as it provides with lossless decomposition and perfect reconstruction of the original image. Even when hidden data are inserted into the cover image, yet the stego-image is visibly very difficult to differentiate than the cover image. The implemented system inserts the data in the random order by using a private key known only to the sending and receiving

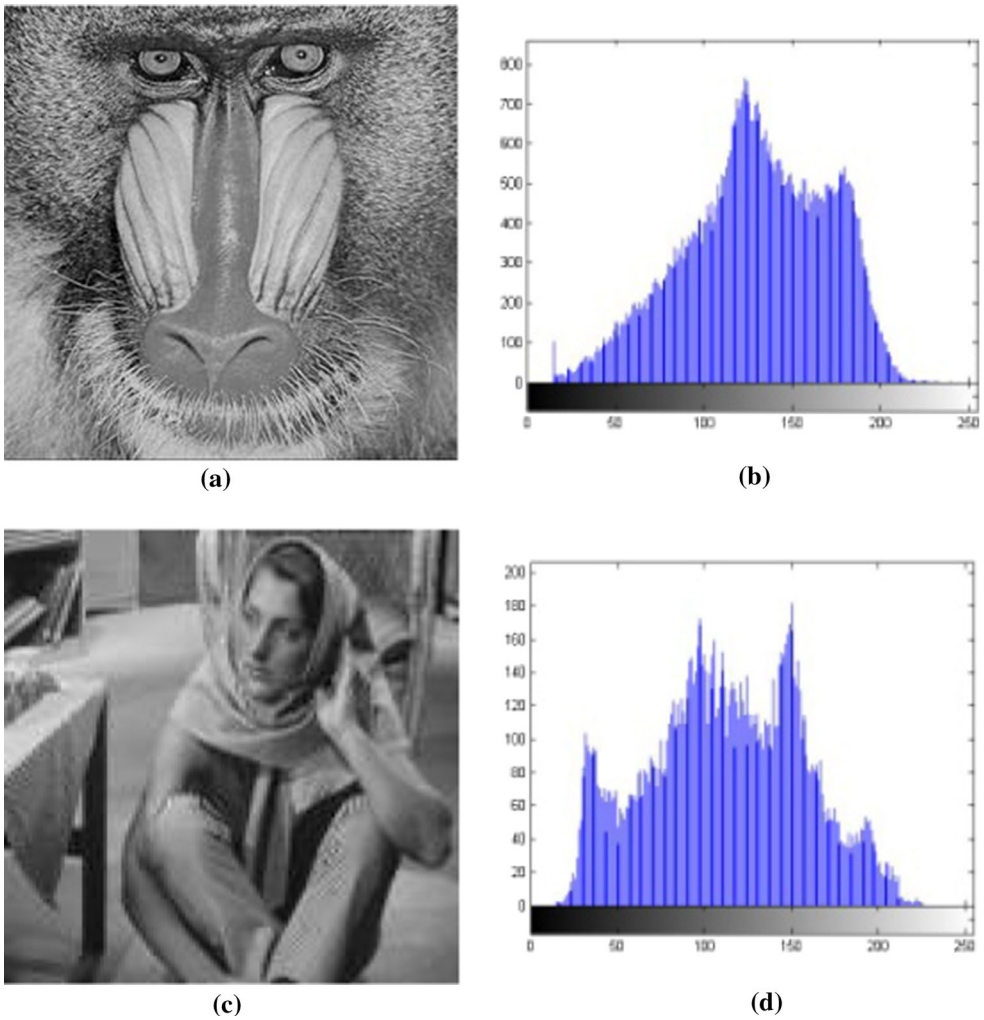


Fig. 13 Output of stego-images of Case IV after inserting data along with histograms. **a** H.C. = 45%, **b** PNR = 45 db, **c** H.C. = 47%, **d** PNR = 44 db

parties. The implemented scheme may be a preferred choice for most applications due to its effectiveness.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Ahmad A, Paul A, Rathore MM (2016a) An efficient divide-and-conquer approach for big data analytics in machine-to-machine communication. Neurocomputing 174:439–453

Ahmad A, Paul A, Rathore MM, Chang H (2016b) Smart cyber society: integration of capillary devices with high usability based on cyber-physical system. Future Gener Comput Syst 56:493–503

Cao W, Han J (2012) Steganalysis on JPEG decompressed bitmaps revisited. In: 2012 Fourth International Conference on Multimedia Information Networking and Security (MINES), pp 878–881

Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recognit 37:469–474

Changa K, Changa C, Huangb PS, Tua T (2008) A novel image steganographic method using tri-way pixel-value differencing. J Multimed 3(2):37–44

Chen W (2003) A comparative study of information hiding schemes using amplitude, frequency and phase embedding. PhD thesis, National Cheng Kung University, Tainan, Taiwan

Grover N, Mohapatra AK (2013) Digital image authentication model based on edge adaptive steganography. In: 2013 2nd International Conference on Advanced Computing, Networking and Security (ADCONS), pp 238–242

Gupta MM, Knopf GK, Nikiforuk PN (1987) Computer vision with fuzzy edge perception. In: International Symposium on Intelligent Control, Philadelphia, USA, pp 271–278

Hou X, Zhang T, Xiong G, Wan B (2012) Forensics aided steganalysis of heterogeneous bitmap images with different compression history. In: 2012 Fourth International Conference on Multimedia Information Networking and Security (MINES), pp 874–877

Lai B, Chang L (2006) Adaptive Data hiding for images based on Harr discrete wavelet transform. Lecture notes in computer science, vol 319

Lillo J, Shih M (2008) Generalizations of pixel-value differencing steganography for data hiding in images. Fundam Inform 83(3):319–335

Paul A, Ahmad A, Rathore MM, Jabbar S (2016) Smartbuddy: defining human behaviors using big data analytics in social internet of things. IEEE Wirel Commun 23(5):68–74

Ramaiya MK, Hemrajani N, Saxena AK (2013a) Improvisation of security aspect in steganography applying DES. In: 2013 International Conference on Communication Systems and Network Technologies (CSNT), pp 431–436

Ramaiya MK, Hemrajani N, Saxena AK (2013b) Security improvisation in image steganography using DES. In: 2013 IEEE 3rd International on Advance Computing Conference (IACC), pp 1094–1099

Simmons GJ (1984) The prisoners' problem and the subliminal channel. In: Proceedings of Crypto'83, pp 51–67

Tseng HW, Chang CC (2004) High capacity data hiding in JPEG-compressed images. Informatica 15(I):127–142

Valenzise G, Tagliasacchi M, Tubaro S (2013) Revealing the traces of JPEG compression anti-forensics. IEEE Trans Inf Forensics Secur 8(2):335–349

Wang K, Zhao H, Wang H (2014) Video steganalysis against motion vector-based steganography by adding or subtracting one motion vector value. IEEE Trans Inf Forensics Secur 9(5):741–751

Westfeld A (2001) F5a steganographic algorithm: high capacity despite better steganalysis. In: 4th International Workshop on Information Hiding, 25–27 April, pp 289–302

Wu N, Hwang M (2007) Data hiding: current status and key issues. Int J Netw Secur 4(1):1–9

Zayed HH (2005) A high-hiding capacity technique for hiding data in images based on K-Bit LSB substitution. In: The 30th International Conference on Artificial Intelligence Applications (ICAIA—2005), Cairo