ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(6), 548–555, March 2015* DOI : 10.17485/ijst/2015/v8i6/70074

Image Tamper Detection based on Edge Image and Chaotic Arnold Map

D. Vaishnavi* and T. S. Subashini

Department of Computer science and Engineering, Faculty of Engineering and Technology, Annamalai University, Tamilnadu, India; vaishume11@gmail.com; rtramsuba@gmail.com

Abstract

Digital images are widely used and can be easily altered through the internet medium. Therefore, this article proposes a novel method of fragile watermarking to detect the image tampers. The proposed method is implemented by an edge image and chaotic Arnold map. The idea of edge detection is to make the image as a binary version and also significantly decrease the sum of information in an image and conserving the structural properties. The edge image is obtained from the watermark image using the Canny edge detection operator. The security and sensitivity of the proposed method is enhanced by employing the Arnold map before embedding the edge image. The accuracy of tamper detection depends upon the variations made in the image and it highlights a location where the tamper has been done. The quality of the watermarked image is evaluated using the metrics Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC). The experiments were carried out to assess the performance of the proposed method for several forms of fiddling with different images. The result shows that the proposed method efficiently localizes the tampered regions.

Keywords: Fragile Watermarking, Tamper Detection, Chaotic Map, Edge Image, PSNR, NC

1. Introduction

Today's digital media play an essential role in news coverage, intelligence information gathering and transmission, criminal exploration, security assessment and military applications etc. The advancements of web technology and internet medium provide access to the digital content quite effortlessly[1]. This leads to manipulating, tampering or altering the digital contents with the help of image processing softwares. Currently, it is hard to find whether the digital content is a true camera output or not by just visually examining it and this significantly damages their trustworthiness[2]. For this reason, an image tamper detection turn into a noteworthy research field to verify the honesty and to isolate the tampered patches. Image tamper detection has been carried out by employing the digital watermarking[3,4,5]. There are several schemes of digital watermarking and among them the fragile watermarking scheme is used for image tamper detection. Here, a mark is inserted into an image without degrading the perceptual quality; however, it will be distorted when the host image is tampered. The watermarking algorithms which are used for tamper detection has several essential properties such as[6]:

Invisibleness: The embedding method should not corrupt the quality of the image and should be perceptually undetectable to preserve its shielding concealment.

Sensitivity: The embedded watermark must be strong to combat the normal image processing operations while it is fragile to malicious tampering.

Security: The watermark must be embedded in a protected manner and it cannot be detached illicitly.

A plenty of fragile watermarking techniques have been proposed in literature[7,8,9]. Shan Suthaharan et al.,[10] proposed a pixel level tamper detection using the logistic map where, the five Most Significant Bit planes are

*Author for correspondence

used to generate the watermark and embedded into its three Least Significant Bit planes. The cryptographic techniques of hashing and confusion or diffusion were used to enhance the tamper detection. Shivendra Shivani et al.[11] embedded the shuffled extensive ten bit recovery data and two bit authentication data of the image block into its Least Significant Bits (LSB) of its corresponding mapping block. The integrity of a test block is decided by comparing 2 × 2 non- overlapping blocks of the test block with its corresponding mapping block. A technique of fuzzy C-means clustering is utilized to cluster all the image blocks to create an association among them. A method using a chaotic map is proposed in[12], the watermark is generated by taking the exclusive- or operation among the binary watermark image and chaotic pattern is obtained as a result of the logistic map. The watermark is embedded into the least significant bit stream of the scrambled image. The work in[13], authors used the K-mean clustering algorithm on the watermarked image to calculate the number of one's and number of zero's in each layer (red, green, blue) separately. Tampered region in an image is mapped by comparing the original clustering values along with tampered watermarked image.

In[14], image protection and modification detection was achieved by combining a two-pass logistic map with Hamming code. Several researchers have used the image characteristics such as color, texture and edge etc., for the underlying principle of image authentication and tamper detection[15]. Bedi et al.,[16] embedded a watermark block vice by means of either the Discrete Hartley Transform (DHT) domain or in Discrete Cosine Transform (DCT) domain. The decision about which transforms domain is used to embed the watermark is depend upon the number of edges which exist in a given block in the image to be watermarked. Sumalatha et al.,[17] proposed a block based reversible watermarking system for image authentication based on histogram modification of the differences between adjacent coefficients using DWT. A content watermark is computed from the image Wavelet Edge Features (WEF) and is inserted into the vertical (LH) sub band in a reversible manner. In this article, a fragile watermarking method is proposed based on the edge features and chaotic map. The rest of an article is composed as follows: Section 2 explains the background concepts of algorithms employed, Section 3 furnishes the proposed method, Section 4 discusses the experimental results and Section 5 concludes the article.

2. Chaotic Arnold Map

The Chaotic map is useful for information hiding and it is very much sensitive to initial conditions[18]. Because of its characteristics, it is mostly used for watermarking and encryption. Arnold transform is used as a pretreatment stage for watermarking, which makes the meaning full image as meaningless one. It is an essential concern to have the spatial relationship decreased between the host image and the watermarked image[19,20]. The 2-dimensional Arnold scrambling transformation is defined as:

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \bmod N \; i, j \in \{0, 1, 2, ..., N-1\} \qquad (1)$$

Wherein, i, j are the pixel coordinates of the original space: i, j is the pixel coordinates after iterative computation scrambling; N is the size of image. By the equation (1), the corresponding inverse transform can be obtained as in equation (2):

$$\begin{bmatrix} i \\ j \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} i' \\ j' \end{bmatrix} \bmod N \; i', j' \in \{0, 1, 2, ..., N-1\} \qquad (2)$$

The original image is restored by inverse transforming as many numbers of iterations it was iterated to transform carried. This used as a secret key and it makes the watermark stronger.

3. Proposed Method

The proposed method consists of the following two phases. First phase illustrates the generation and embedding procedure of watermark. Second phase furnishes the recovery of a watermark and detection and localization of tampered region. Figure 1 illustrates the proposed tamper detection method of fragile watermarking scheme using the edge image.

3.1 Watermark Generation and Embedding

The image features like edges are recognized in an image where the intensity of an image varies abruptly and it has discontinuities. The attacks spawned by the noise, edge strips and acuity are controlled by way of these edge features. The idea of edge detection is to make the image as a binary version and also significantly decrease the sum of information in an image and conserving the structural properties. As a consequence, an edge detection process with Canny edge operator is employed on the watermark

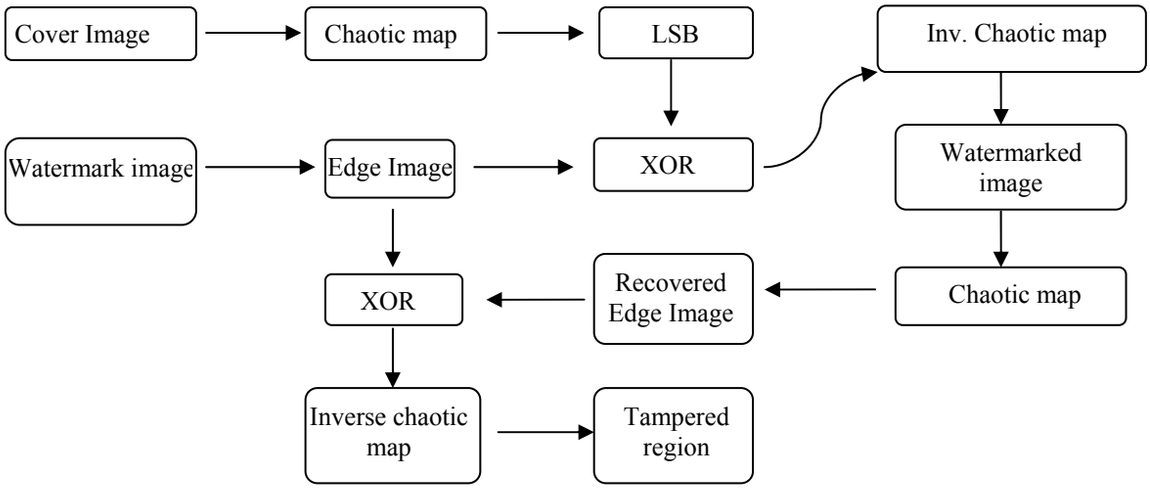


Figure 1. Proposed fragile watermarking scheme.

image to produce an edge image. The chaotic Arnold map is employed to jumble the cover image and it is sliced into 8 significant bit planes. The Most Significant Bit plane contains the majority of visually significant data and the quality of the entire image is degraded if it got any changes. But the Least Significant Bit plane contains the compromising pixels in the image and the quality of an image is not degraded considerably even if it gets changed. Hence, an edge image is embedded on every pixel of the LSB plane of the cover image. Finally, the watermarked image is built by making use of an inverse chaotic Arnold map.

3.2 Watermark Recovery and Tamper Localization

The Arnold map is applied for two iterations on the watermarked image to obtain the scrambled image. The scrambled image is sliced into 8 bit planes and an embedded edge image is recovered from the least significant bit plane of each pixel. In addition to detect the tampers, the original and recovered watermark edge images are subject to exclusive-or (XOR) operation and the result of the XOR operation visually shows the approximate amount of pixels which are modified or tampered. Finally, the inverse Arnold map is applied to locate the tampered region.

4. Experimental Results

The experimental setup was done using Math works MATLAB 12. The test images are taken as gray scale of resolution 256×256. The experiments were carried out on four MATLAB standard images, namely, cameraman, Lena, Mandi and lifting body as cover images. The 2-dimensional Arnold chaotic map is applied for two iterations on all the cover images. The Annamalai University AU logo is used as a watermark image and which is shown in the Figure 2 a). Figure 2 b) shows the watermark edge image which is embedded on the cover image. To experimentally ascertain the invisibleness of the proposed method, the metrics Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) were used which is given in the equations (3) & (4).

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\text{dB where}$$
$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]}{M \times N} \quad (3)$$

$$NC = \frac{\sum_{i=0}^{M}\sum_{j=0}^{N} I_1(i,j)^* I_2(i,j)}{\sum_{i,j}^{M,N} I_1(i,j)^2 \sum_{i,j}^{M,N} I_2(i,j)^2} \quad (4)$$

Table 1 provides the invisibleness of the proposed watermarking scheme with the metrics PSNR and NC for various images. The PSNR and NC value of all the images indicates that the invisibleness of the proposed fragile watermarking method is pretty good.

Now to evaluate the performance of the proposed system, the watermarked images are subjected to various

a) b)

Figure 2. a) Watermark image AU, b) Watermark edge image.

Table 1. Invisibleness of proposed method

Image	PSNR in dB	NC
Cameraman	51.0789	0.9974
Lena	50.6246	0.9972
Mandi	51.1086	0.9961
Lifting body	51.1483	0.9973

attacks, namely Copy Move, Text addition, Image splicing and Object Removal and the results are demonstrated in the following subsections.

4.1 Copy Move Attack

In this experiment, copy move attack was applied to the watermarked cameraman image. The PSNR value of watermarked image is 51.0789 dB. In Figure 3 a), a tall building (a portion which is marked in red color) from the background was copied and pasted twice in two different places. The tampered image is shown in Figure 3 b) and tampered region is marked with pink color. The extracted watermark edge image is shown in Figure 3 c), which shows some noise is presented here and this indicates that the tamper has been done on the watermarked image. Figure 3 d) displays the localized tampered region.

4.2 Text Addition

Figure 4 a) shows the watermarked lena image and whose PSNR value is 50.6246 dB. The text 'i am Lena' is inserted at the top of the watermarked lena image which is indicated by the red color rectangle and is shown in Figure 4 b). Figure 4 c) displays the recovered watermark edge image which shows some noise is presented here and it indicates that the tamper has been done on the watermarked image. The result of the localized tampered region is shown in Figure 4 d).

4.3 Image Splicing

The watermarked Mandi image shown in Figure 5 a) was used to apply the image composite attack and it has the PSNR value of 51.1086 dB. Some portions/object of an image was combined with another image and defined as college attack or splicing attack. A dog (object) was combined with Figure 5 a) and the tampered image is shown in Figure 5 b). Figure 5 c) displays the recovered watermark edge image and which shows some noise is presented here and it indicates that the tamper has been done on the watermarked image. The result of the localized tampered region is shown in Figure 5 d).

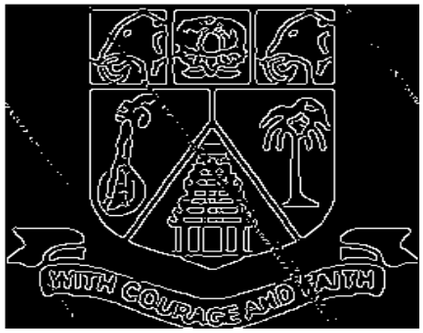
4.4 Object Removal

The watermarked lifting body image has 51.1483 dB of PSNR value and which shown in Figure 6 a). From the Figure 6 a), the closest lift (marked in red color) was removed with the intention to degrade the image and the tampered image is shown in Figure 6 b). Figure 6 c) shows recovered edge features which display some noise is presented and it indicates that the tamper has been done on the watermarked image. The result of tampered region where the content is removed is shown in the Figure 6 d).

Figure 7 shows the tampered image, recovered watermark edge image and output of XOR operation

a) Watermarked camerama

b)Tampered cameraman



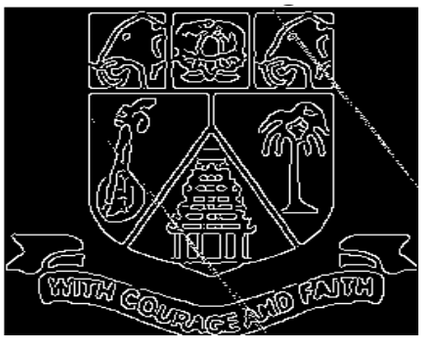
c) Recovered watermark edge image

d) Detected tampered region

Figure 3. Tamper detection result for copy move attack.

a) Original lena image

b) Watermarked lena



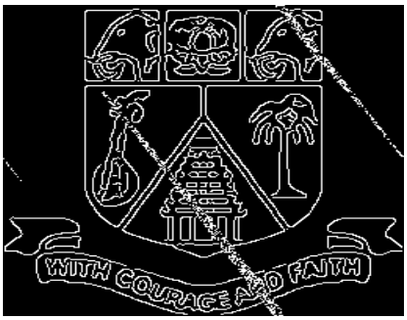
c) Recovered watermark edge image

d) Detection of tampered region

Figure 4. Tamper detection result for text addtion attack.

a) Watermarked mandi image

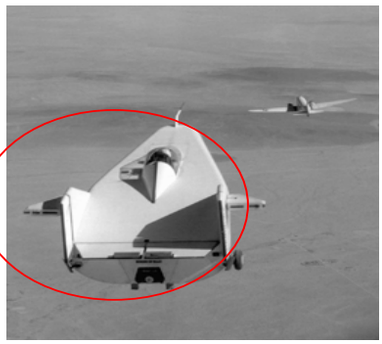
b)Tampered image



c) Recovered watermark edge image

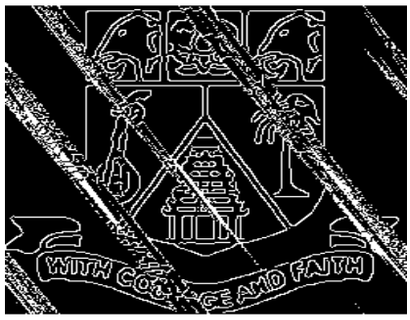
d) Tampered region detection

Figure 5. Tamper detection result for splicing attack.

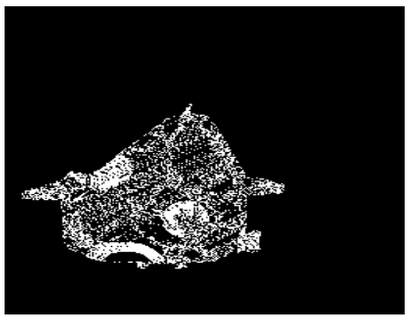


a) Watermarked lifting body image

b)Tampered image



c) Recovered watermark edge image



d) Detected tampered region

Figure 6. Tamper detection result for object removal attack.

for tampering attacks of Copy and Move, Test addition, image splicing and object removal. The XO Red output in the last column of Figure 7 c) is used as an indication of the content of tampering was done on the watermarked cover images shown in Figure 7 a). It reveals that more the noise more the tampering done and vice versa.

5. Conclusion

A proposed scheme of fragile watermarking based on the edge image and chaotic Arnold map for tamper detection is implemented. The canny edge detector is used to obtain the edge from the watermark. The chaotic Arnold map is employed on the cover image to make the watermarking as strong. The invisibleness of the proposed watermarking technique is calculated using the metrics Peak-Signal to Noise-Ratio (PSNR) and Normalized correlation (NC) and it achieves the PSNR value about 50 dB and NC value about 0.99. The proposed scheme of tamper detection is tested with various content altering malicious manipulations and different images. And also, the proposed system was successful in efficiently localizing the tampered region.

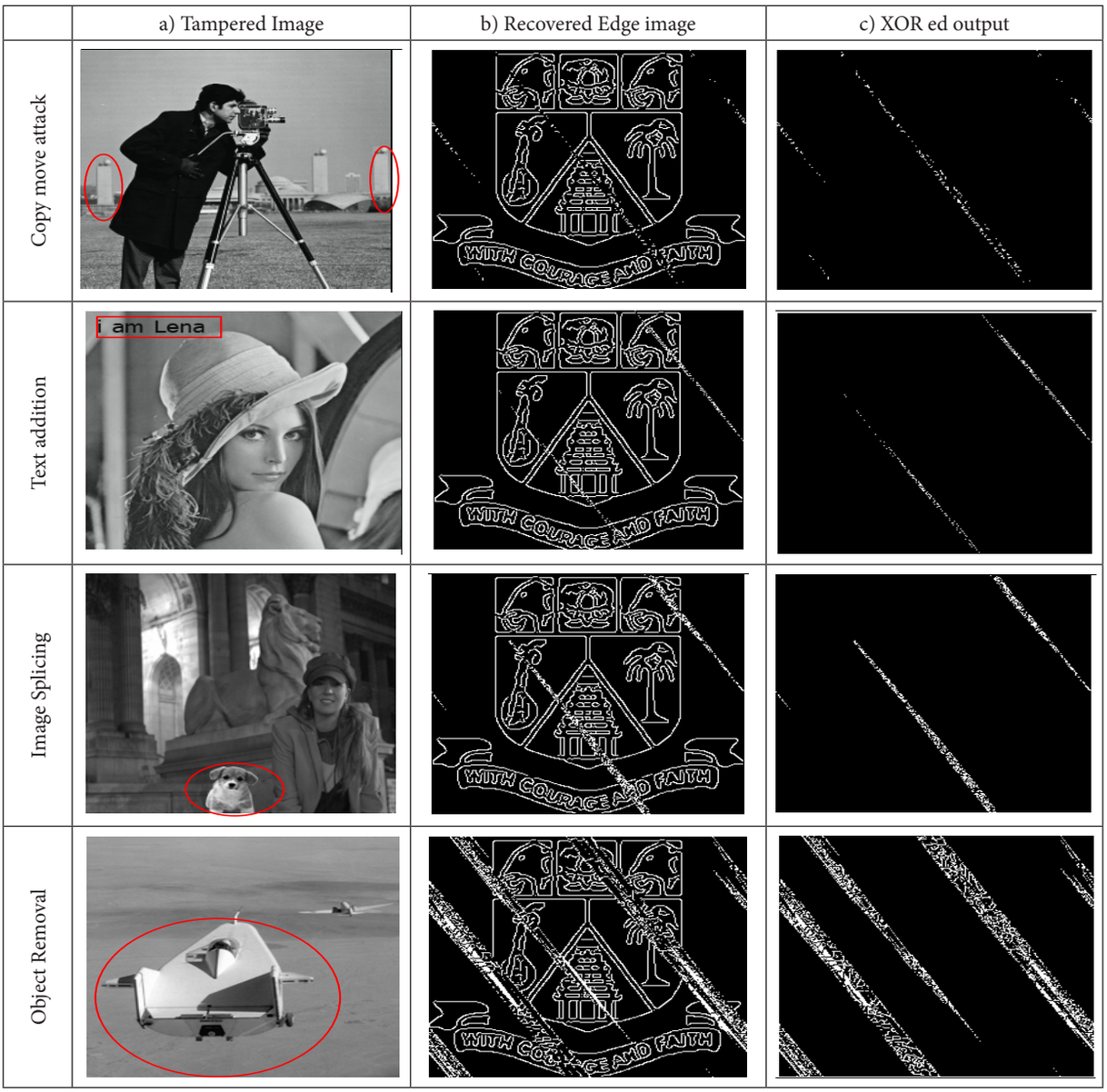


Figure 7. Comparison of resultant images of XOR operation with various kinds of tampers.

6. References

1. Alirezanejad M, Amirgholipour S, Safari V, Aslani S, Arab M. improving the performance of spatial domain image watermarking with high boost filter. Indjst. 2014; 7(12):2133–39.
2. Mishra M, Adhikary F. Digital image tamper detection techniques - a comprehensive study. 2013; 2(1): arXiv preprint arXiv:1306.6737.
3. Tiwari A, Sharma M. Comparative evaluation of semi-fragile watermarking algorithms for image authentication. J Inform Secur. 2012; 2(2).
4. Qi X, Xin X. A Quantization-based Semi-fragile watermarking scheme for image content authentication. J Vis Comun Image Represent. 2011; 22(2):187–200.
5. Chang C, Hu Y, Lu T. A watermarking-based image ownership and tampering authentication scheme. Pattern Recogn Lett. 2006; 27(5):439–46.
6. Zhang D, Pan Z, Li H. A Contour-Based Semi-fragile Image Watermarking Algorithm in DWT Domain. In: Education Technology and Computer Science (ETCS), Second International Workshop on; 2010; IEEE; p. 228–31.
7. Di Martino F, Sessa S. Fragile watermarking tamper detection with images compressed by fuzzy transform. Inform Sci. 2012; 195:62–90.
8. Xiao D, Shih FY. An improved hierarchical fragile watermarking scheme using chaotic sequence sorting and subblock post processing. Optic Comm. 2012; 285(10):2596–606.
9. Phan, RC. Tampering with a watermarking-based image authentication scheme. Pattern Recogn. 2008; 41(11):3493–96.
10. Shan S. Logistic map-based fragile watermarking for pixel level tamper detection and resistance. EURASIP J Informat Secur. 2010.
11. Shivani S, Singh D, Agarwal S. DCT based approach for tampered image detection and recovery using block wise fragile watermarking scheme. Springer Berlin; Heidelberg: 2013. p. 640–47.
12. Rawat S, Raman B. A chaotic system based fragile watermarking scheme for image tamper detection. AEU-International J Electron Communicat. 2011; 65(10):840–7.
13. Manickam L, Jilani SAK, Giri Prasad MN. A novel fragile watermarking scheme for image tamper detection using K mean clustering. 2013; Internat J Computer Trends Technol (IJCTT). 4(10):3380–85.
14. Chang C, Chen K, Lee C, Liu L. A secure fragile watermarking scheme based on chaos-and-hamming code. J Syst Software. 2011; 84(9):1462–70.
15. Ellinas JN. A robust wavelet-based watermarking algorithm using edge detection. World Acade Sci, Engin Technol. 2007; 1(10):234–39.
16. Bedi SS, Tomar GS, Verma S. Robust watermarking of image in the transform domain using edge detection. 11th International Conference on Computer Modelling and Simulation, UKSIM'09; 2009; IEEE; p. 233–38.
17. Sumalatha L, Krishna VV, Babu VA. Image content authentication based on wavelet edge features. Int J Comput Appl. 2012; 50:24–9.
18. Vaishnavi D, Subashini TS. An image watermarking scheme resilient to geometric distortions. Power Electron Renew Ener Syst. Springer India; 2015. p. 1225–33.
19. Thamizhchelvy K, Geetha G. Data hiding technique with fractal image generation method using chaos theory and watermarking. Indjst. 2014.
20. Vaishnavi D, Subashini TS. A robust image watermarking for geometric distortion using DC coefficients. Int J Appl Eng Res. 2014; 9(21):4895–4900.