

Robust Reversible Data Hiding Using Integer Wavelet Transform

¹A. Kalaiselvi and ²V.R. Vijaykumar

¹Department of ECE, Sri Ramakrishna Engineering College, 641022 Coimbatore, India

²Department of ECE, Anna University Regional Campus, 641046 Coimbatore, Tamil Nadu, India

Abstract: This study proposes the rotation, scaling and shift invariant reversible data hiding technique using scale invariant feature transform with embedding in wavelet domain. Also, the content is made secure by encryption using rotation invariant hash key. Rotation, scaling and shift invariant reversible data hiding is implemented using SIFT and embedding is done in wavelet domain and the results are analyzed. The experimental results show that, this scheme provides high embedding capacity with low distortion. Also, it is robust against rotation. The computational complexity of the proposed technique is low and the execution time is short compared to the existing methods like expansion embedding based reversible data hiding, histogram shifting based reversible data hiding and prediction based reversible data hiding.

Key words: Data hiding, integer wavelet transform, hash function, Scale Invariant Feature Transform (SIFT)

INTRODUCTION

Data hiding is the process of hiding secret information in an image. If the recovery of cover image is lossless then the data hiding is said to be reversible. Reversible data hiding is used in applications where the cover image is of greater importance. The proposed methodology is used to hide the secret data in an image using a modern stegano-graphic technique which is robust against rotation along with securing the hidden data using rotational invariant hash. The hidden image is sub sampled during embedding and interpolated in the extraction process. Most of the existing data hiding techniques are not reversible (Celik *et al.*, 2002). For instance, the widely used spread spectrum based data hiding method are not invertible owing to truncation (Fallahpour and Sedaaghi, 2007). Data hiding using discrete wavelet transform are not lossless as the scaling factor for embedding data varies for every pixel. The well-known Least Significant Bit (LSB) plane based schemes are not lossless owing to bit replacement without memory. Zhicheng has proposed reversible data hiding using histogram modification which retrieve the original image without any distortion from the water marked image. In Thodi and Rodriguez have been proposed a histogram-manipulation based lossless data hiding scheme which is reversible. A normal reversible data hiding technique to embed patient private information into the post ECG signal by adapting reversible multilevel Haar-DWT and histogram shifting was discussed. A secure reversible data hiding (Ni *et al.*, 2006) peak points in the histogram of an image are utilized to embed data by

modifying gray scale values in the image. Yi and Zhou proposed an improved version of reversible data hiding using histogram shifting and image encryption method reversible data embedding using a difference expansion proposed a high-capacity, high visual quality, reversible data-embedding method for digital images. Wang proposed an efficient integer transform based reversible watermarking. Li *et al.* (2013) presented a general framework to construct histogram shifting based reversible data hiding. In this study, a novel reversible data hiding method for digital images using integer wavelet transform and threshold embedding technique is proposed. Hu *et al.* (2009) have been proposed a reversible data hiding which increase the embedding capacity and to improve the compressibility of the over flow location map using difference expansion embedding and predicted error expansion. Lee *et al.* (2015) was proposed an dual image data hiding method which uses a magic matrix and histogram modification to embedded the secret data. The proposed reversible data hiding technique is rather simple and yet, outperforms the prior arts. Both theoretical analysis and experimental results demonstrate the superiority of the proposed technique.

MATERIALS AND METHODS

Security using rotational invariant hash: Security of the hidden image is of greater importance during transmission. The basic securing operation is encryption and decryption of the hidden message using a common key. A simple XOR cipher is, therefore, sometimes used for hiding information in cases where no particular

security is required. In this study, the image undergoes rotation, scaling and shifting. Hence, the conventional repeated XOR keys will not be suitable. In order to overcome this problem, the key is generated from a rotational invariant hash. So, even if the image is rotated, scaled or shifted in the receiver end the key remains same.

Image hash: Image hashing maps an input image to a short string called image hash and has been widely used in image retrieval, image authentication, digital watermarking, image copy detection, tamper detection, image indexing, multimedia forensics and reduced reference image quality assessment. There are some classical cryptographic hash functions, for example, SHA-1 and MD5 which can convert input message (document, image, graphic, text, video, etc.) into a fixed-size string. However, they are sensitive to bit-level changes and cannot be suitable for image hashing. This is because digital images often undergo normal digital processing such as JPEG compression and image enhancement in real applications without changing visual contents of images. This is the first one of the two basic properties of the image hash function, known as perceptual robustness, i.e., a hash function should be robust against content preserving operations such as geometric transform, format conversion and JPEG compression. In other words, hashes of an image and its processed versions are expected to be the same or very similar. Hash will be expected to be significantly changed only when visual content is altered by malicious operations such as object deletion and object insertion. Another basic property is the discriminative capability, i.e., images with different contents should have different hashes. This means that hash distance between different images should be large enough.

Image sub sampling and interpolation: The image to be hidden should satisfy the size constraint because reversibility and security is achieved by adding redundant information. Hence, the hidden image is sub sampled during embedding and interpolated during extraction. A nonlinear interpolation is used in this study. The algorithm uses the switching of existing Soft-decision Adaptive Interpolation (SAI) algorithm and Single Pass Interpolation Algorithm (SPIA) Methods. The error pattern is learnt in the interpolation process of SAI Method and SPIA Method after interpolating down sampled version of LR image. Then a mechanism to correct the error pattern is devised. SAI Methods works well on smooth images (variation among the pixels is less) while SPIA Method works better on detailed images (more variation among the pixels) because of the type of pixels

used in the interpolation. So, a hybrid scheme of combining SAI and SPIA Method is used for best prediction of High Resolution (HR) image. This algorithm has produced the best results in different varieties of images in terms of both PSNR measurement and subjective visual quality.

Scale invariant feature transform: SIFT is used for extracting distinctive invariant features from images that can be invariant to image scale and rotation. It was widely used in image mosaic, recognition, retrieval, etc. SIFT mainly includes four major stages, scale-space extrema detection, key point localization, orientation assignment and key point descriptor. The first stage used Difference-Of-Gaussian function (DOG) to identify the potential interest points which were invariant to scale and orientation. DOG was used instead of Gaussian to improve the computation speed. The scale space of an image is defined as a function, $L(x,y,s)$, produced from the convolution of a variable-scale Gaussian and an image as given in Eq. 1 and 2:

$$L(x, y, s) = G(x, y, s) \times I(x, y) \quad (1)$$

$$G(x, y, s) = \frac{1}{2s^2} e^{-(x^2+y^2)/2s^2} \quad (2)$$

In the scale-space, all local maximums and minimums are retrieved by checking the eight closest neighborhoods in the same scale and nine neighborhoods in the scale above and below. Finally, the locations and descriptors of feature points are determined, against to the scale and orientation change of images. In the key point localization step, the low contrast points are rejected and the edge response is eliminated. Hessian matrix was used to compute the principal curvatures and eliminate the key points that have a ratio between the principal curvatures that are greater than the ratio. An orientation histogram was formed from the gradient orientations of sample points within a region around the key point in order to get an orientation assignment. The key point descriptors are calculated from the local gradient orientation and magnitudes in a certain neighborhood around the identified key point. The gradient orientations and magnitudes are combined in a histogram representation from which the descriptor is formed.

Integer wavelet transform: Wavelet domain allows us to hide data in regions that the Human Visual System (HVS) is less sensitive to such as the high resolution bands (HL, LH and HH), hiding data in these regions allow us to maximize the robustness while managing good

visual quality. Integer wavelet transform make an integer data set into another integer data set. Lifting schemes can be used to perform integer wavelet transform. A distortion less image data hiding algorithm based on integer wavelet transform that can invert the embedded image into the original image without any distortion after the hidden data are extracted is used in the implementation. Integer wavelet transform provides the decomposition of the original signal into a set of integer coefficients from which inverse wavelet transform of the original image can be recovered without any loss. Since, it is required to reconstruct the original image with no distortion, integer lifting scheme wavelet transform is used in this research.

Proposed robust reversible data hiding algorithm

Data hiding: Host image block is divided into four sub-bands (LL, LH, HL, HH) using IWT. The LH, HL and HH sub-bands are chosen for embedding. The high frequency coefficients are divided into 8x8 blocks. IWT is applied to the entire image blocks. Two sequences are generated k1 and k2 each of size 3x3. The IWT coefficient blocks are denoted as f(u,v), u = 0,1, ... 7, v = 0,1, ... 7. The IWT coefficients in the lines 2~4 are modified and the modified blocks f'(u,v) are obtained by the formula given in Eq. 3:

$$f'(u,v) = \begin{cases} D(u,v) + a \times k1(u,v) & \text{if } w(i,j) = 0 \\ D(u,v) + a \times k2(u,v) & \text{if } w(i,j) = 1 \end{cases} \quad (3)$$

Where D(u,v) indicates the mean value of each IWT coefficient block in the lines 2~4 and the columns 2~4 and a is the embedding depth factor, the value of a is a positive real constant.

Hidden data extraction and original image restoration: In the data extraction stage. The high frequency wavelet coefficients (LH, HL, HH) are obtained by applying IWT on each block. The IWT coefficient blocks in the lines 2~4 and the columns 2~4 is denoted as D(u,v). We calculate the correlation coefficient of D(u,v) and k1 and k2 which is denoted as pk1 and pk2. If pk1 > pk2 then w(i,j) = 0 if pk1 < pk2 then w(i,j) = 1. The w(i,j) is the detected water mark. The image is rotated back to get the cover image.

Block diagram reversible data hiding: The Block diagram for embedding and extracting the data using rotational invariant reversible data hiding with nonlinear interpolation are given in Fig. 1 and 2, respectively.

Generally, the file used to hide data is referred to as cover image, the term stego image is used for the file

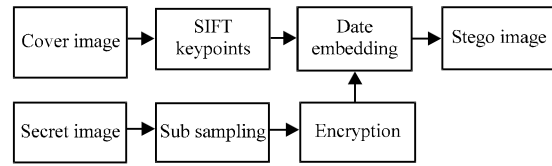


Fig. 1: Block diagram for data embedding

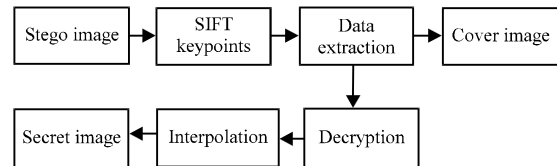


Fig. 2: Data extraction

containing secret message. Prior to hiding the secret image is sub sampled and then encrypted using a key generated using rotational invariant hash. The data is embedded using IWT coefficients. Data extraction is the reverse process. After extraction the data is decrypted and interpolated.

Data embedding

Step 1: Sub sampling; The secret image of size 128x128 is which has to hidden is sub sampled to the size of 32x32.

Step 2: Encryption is done using XOR operation. The key generation involves the rotation invariant hash generation. The image is resized to a fixed size of 64x64.

Ring partition: The resized image is ring partitioned to obtain the secondary image. To make image has resilient to rotation, we can divide an image into different rings and use them to form a secondary image invariant to rotation. Figure 3 is a schematic diagram of secondary image construction where is a square image divided into seven rings and the secondary image formed by these rings.

The ring partition can be done by calculating the circle radii and the distance between each pixel and the image center. Suppose that r_k is the kth radius (k = 1; 2; ... n) which is labeled from small value to big value. Thus, r₁ and r_n are the radii of the innermost and outermost circles, respectively. For the m x m image, the outermost radius is given in Eq. 4:

$$r_n = \frac{m}{2} \quad (4)$$

To determine other radii, the area of the inscribed circle A and the average area of each ring μ_A are first calculated using Eq. 5:

$$\mu_A = \frac{A}{n} \quad (5)$$

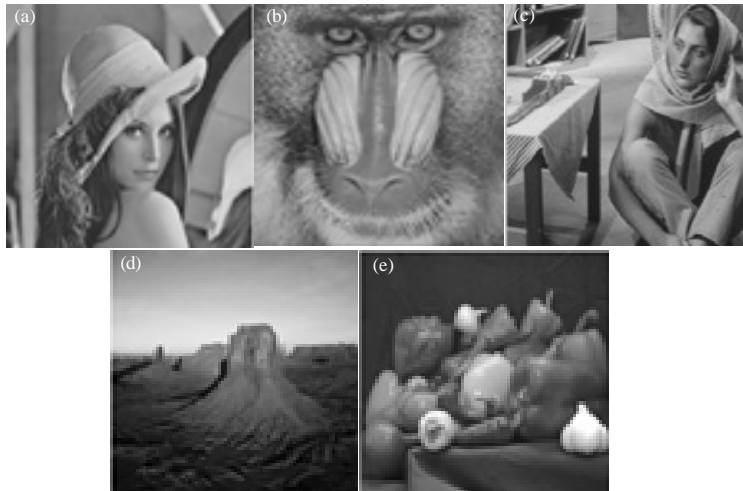


Fig. 3: Cover images of rotational invariant reversible data hiding; a) Lena; b) Baboon; c) Barbara; d) Desert; e) Peppers

Here, A is the area of the outer circle which can be calculated by Eq. 6. n be the number of rings:

$$A = \pi r_n^2 \tag{6}$$

So, r_1 can be computed by using the Eq. 7:

$$r_k = \sqrt{\frac{\mu_A}{p}} \tag{7}$$

Thus, other radii r_k ($k = 2; 3, \dots, n-1$) can be obtained by Eq. 8:

$$r_k = \sqrt{\frac{\mu_A + \pi r_{k-1}^2}{p}} \tag{8}$$

Let, $p(x, y)$ be the value of the pixel in the y th row and the x th column of the image ($1 \leq x, y \leq m$). Suppose that (x_c, y_c) are the coordinates of the image center. The x_c and y_c are determined using Eq. 9 and 10:

$$X_c = (m / 2) + 0.5 \tag{9}$$

$$Y_c = (n / 2) + 0.5 \tag{10}$$

The distance between $p(x, y)$ and the image center (x_c, y_c) can be measured by the Euclidean distance as given in Eq. 11:

$$d_{x,y} = \sqrt{(x - x_c)^2 + (y - y_c)^2} \tag{11}$$

Having obtained the circle radii and pixel distances, we can classify these pixel values into n sets using Eq. 12 and 13:

$$r_1 = \{P_{x,y} \mid d_{x,y} \leq R_1\} \tag{12}$$

$$r_k = \sqrt{\frac{\mu_A + \pi r_{k-1}^2}{\pi}} \tag{13}$$

Elements in are rearranged to form sorted vector is then mapped then mapped to form a new vector of size $a \times 1$. Secondary image V is formed as $[V_1 V_2 \dots V_k]$. The vector V is reshaped to the size of the hidden image and encoded. This forms the key for encryption. The key is XORed with the message to get the encrypted data.

Step 3: Sift keypoints; the image is resized to 512×512 and SIFT key points are determined these points will give the stable points which are robust against rotation.

Step 4: Block selection; the image is divided into blocks of size 8×8 . Blocks having more key-points are chosen for embedding.

Step 5: Embedding; host image block is divided into four sub-bands (LL, LH, HL, HH) using IWT. The LH, HL and HH sub-bands are chosen for embedding. The high frequency coefficients are divided into 8×8 blocks. IWT is applied to the entire image blocks. Two sequences are generated k_1 and k_2 each of size 3×3 . The IWT coefficient blocks are denoted as $f(u, v)$, $u = 0, 1, \dots, 7, v = 0, 1, \dots, 7$. The IWT coefficients in the lines 2-4 are modified and the modified blocks $f'(u, v)$ are obtained by the formula given in Eq. 14:

$$f'(u, v) = \begin{cases} D(u, v) + a \times k1(u, v) & \text{if } w(i, j) = 0 \\ D(u, v) + a \times k2(u, v) & \text{if } w(i, j) = 1 \end{cases} \quad (14)$$

Where, $D(u, v)$ indicates the mean value of each IWT coefficient block in the lines 2~4 and the columns 2~4 and a is the embedding depth factor, the value of a is a positive real constant.

Data extraction and original image restoration: Data extraction is the reverse process. The following are the step involved.

Step 1: SIFT keypoints; SIFT key points are determined from the stego these points will give the stable points which are robust against rotation.

Step 2: Block selection; the image is divided into blocks of size 8×8 . Blocks having more keypoints are chosen for extraction.

Step 3: Extraction; the high frequency wavelet coefficients (LH, HL, HH) are obtained by applying IWT on each block. The IWT coefficient blocks in the lines 2~4 and the columns 2~4 is denoted as $D(u, v)$. We calculate the correlation coefficient of $D(u, v)$ and $k1$ and 2 which is denoted as $pk1$ and 2 . If $pk1 > 2$ then $w(i, j) = 0$; if $pk1 < 2$, then $w(i, j) = 1$. The $w(i, j)$ is the detected water mark. Restoration is the reverse process. The image is rotated back to get the cover image.

RESULTS AND DISCUSSION

Performance metrics: The quality assessment of image after data hiding is done to measure the amount of distortion due to the data hiding. The Mean Square Error (MSE) gives the indication of how much degradation was introduced in the embedded image. Peak Signal to Noise Ratio (PSNR) is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. The PSNR and MSE can be measured as per Eq. 15 and 16:

$$PSNR = 10 \log_{10}(255^2 / MSE) \quad (15)$$

$$MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} c(i, j) - c'(i, j) \quad (16)$$

The host images of different modalities are chosen for embedding. The images of different size are chosen and resized to 512×512 . The cover images such as Lena, Baboon, Barbara, Desert and Peppers are used for testing and are shown in Fig. 3.

The secret image is of size 128×128 . This image is sub sampled to the size 32×32 . The image is encoded into stream of bits. Each pixel value is encoded into a bit stream of length 8 bits. The length of the encoded bits is 8192. Then, the image is encrypted using a rotation invariant key of same length. The encoded and encrypted image is shown in Fig. 4.

The SIFT key points are obtained for the cover image and the blocks are chosen for data embedding. The embedded images obtained are shown in Fig. 5. The secret decrypted bit streams are retrieved and decoded if the same size length of 8192 as shown in Fig. 6. The recovered cover image of proposed work with size 512×512 is shown in Fig. 7.

Performance measure: The PSNR, MSE and the SSIM value between cover and stego image are given in Table 1 and 2. The rotated scaled and shifted image results are shown in Table 3 and 4.

Table 1: Performance measure when hiding image using robust reversible data hiding

Images	SSIM	MSE	PSNR (dB)
Lena	0.9878	4.1914	41.9072
Pepper	0.9899	3.4506	42.7519
Barbara	0.9878	6.4631	40.0264
Desert	0.9818	5.5831	40.6621
Baboon	0.9797	13.1044	36.9566

Table 2: Performance measure of interpolated image

Images	SSIM	MSE	PSNR (dB)
Lena	0.060	5.7314	42.4174
Pepper	0.075	7.0435	39.8153
Barbara	0.040	10.0057	22.4196
Desert	0.190	8.2110	30.8560
Baboon	0.020	12.0145	20.3487



Fig. 4: Encoded and encrypted image

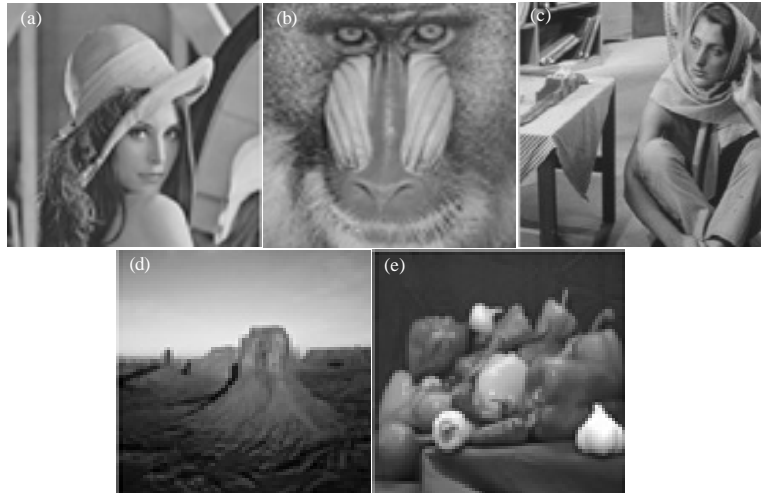


Fig. 5: Stego images of rotational invariant reversible data hiding: a) Lena; b) Baboon; c) Barbara; d) Desert; e) Peppers

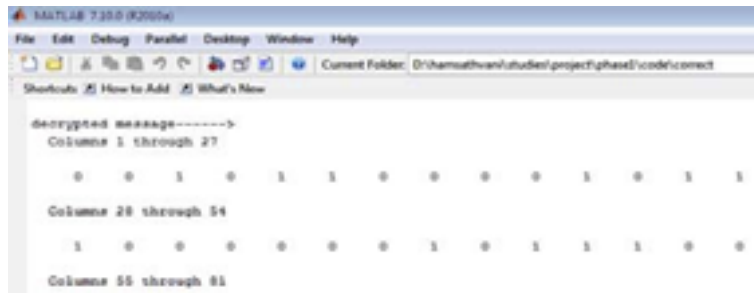


Fig. 6: Decrypted image

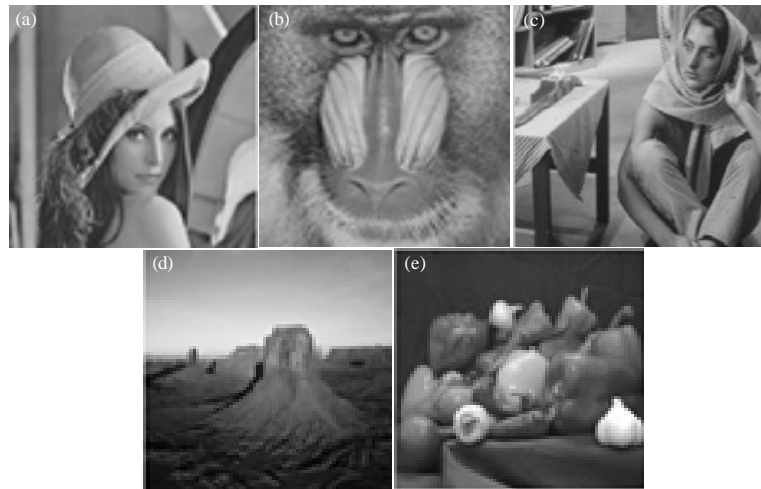


Fig. 7: Recovered images; a) Lena; b) Baboon; c) Barbara; d) Desert; e) Peppers

The results show that the images with more high frequency coefficients are with low capacity and more distorted. Hence, the PSNR value is reduced for Baboon image.

Comparison: The proposed reversible data hiding system is compared with existing techniques like expansion embedding based reversible data hiding, Histogram shifting based reversible data hiding and prediction based

Table 3: Rotated image results


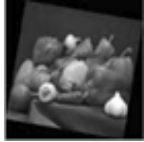



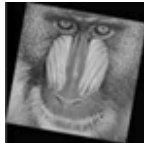




Original images	Rotated images	MSE	PSNR	SSIM
		3.4484	42.7546	0.9900
		4.1868	41.9120	0.9880
		13.1170	36.9523	0.9796
		5.5766	40.6671	0.9820
		6.4442	40.0391	0.9879

Table 4: Scaled image results











Original images	Rotated images	MSE	PSNR	SSIM
		3.5263	41.9843	0.98
		4.4319	41.1997	0.9892
		13.2660	36.2105	0.933
		5.1159	40.1254	0.972
		6.9921	40.0115	0.9711

Table 5: PSNR comparison with existing techniques

Images	EE based	HS based	Prediction	Rotation
	RDH	RDH	based RDH	invariant
Lena	38.9126	40.1876	41.2806	43.2082
Barbara	38.0176	42.5166	42.9157	39.8956
Desert	37.1659	38.2618	38.1608	40.5627
Baboon	37.1282	42.5291	42.6211	46.4196
Peppers	32.1783	32.4238	32.8212	32.1588

Table 6: MSE comparison with existing techniques

Images	EE based	HS based	Prediction	Rotation
	RDH	RDH	based RDH	invariant
Lena	11.5102	4.6175	3.2413	4.1914
Barbara	11.9211	3.2536	3.1021	3.4506
Desert	11.8636	11.9490	3.4125	6.4631
Baboon	13.0081	4.5091	3.1332	5.5831
Peppers	15.9872	16.7481	4.1264	13.1044

Table 7: SSIM comparison with existing techniques

Images	EE based	HS based	Prediction	Rotation
	RDH	RDH	based RDH	invariant
Lena	0.9876	0.9826	0.9878	0.9883
Barbara	0.9799	0.9976	0.9899	0.9987
Desert	0.9812	0.9801	0.9878	0.9876
Baboon	0.9698	0.9897	0.9818	0.9907
Peppers	0.9343	0.9214	0.9797	0.9274

reversible data hiding. The results show that the proposed data hiding system provides less distorted stego image and also rotation invariant. The comparison results are shown in Table 5-7.

CONCLUSION

In this study, a rotation scale and shift invariant reversible data hiding using scale invariant feature transform and integer wavelet transform along with nonlinear interpolation of the hidden image was implemented. Also, the message is secured by encrypting using rotation invariant image hash for key generation. From the performance analysis the PSNR value for hiding around 10000 bits is found to be in the range of 38-43. Also, the data are extracted and decoded along with the loss less recovery of the cover image.

REFERENCES

Celik, M.U., G. Sharma, A.M. Tekalp and E. Saber, 2002. Reversible data hiding. Proceedings of the International Conference on Image Processing, Volume 2, October 2002, New York, pp: II-157-II-160.

Fallahpour, M. and M.H. Sedaaghi, 2007. High capacity lossless data hiding based on histogram modification. IEICE Electr. Express, 4: 205-210.

- Hu, Y., H.K. Lee and J. Li, 2009. DE-based reversible data hiding with improved overflow location map. *IEEE Trans. Circuits Syst. Video Technol.*, 19: 250-260.
- Li, X., B. Li, B. Yang and T. Zeng, 2013. General framework to histogram-shifting-based reversible data hiding. *IEEE Trans. Image Process.*, 22: 2181-2191.
- Lee, C.F., S.T. Chen and J.J. Shen, 2015. Reversible dual-image data embedding on pixel differences using histogram modification shifting and cross magic matrix. *Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, September 23-25, 2015, Adelaide, SA., pp: 113-116.
- Ni, Z., Y.Q. Shi, N. Ansari and W. Su, 2006. Reversible data hiding. *IEEE Trans. Circuits Syst. Video Technol.*, 16: 354-362.