Original scientific paper

Informacije MIDEM
Journal of Microelectronics,
Electronic Components and Materials
Vol. 47, No. 2(2017), 91 – 99

Reversible Data Hiding Based on Radon and Integer Lifting Wavelet Transform

A.Amsaveni[1], P.T Vanathi[2]

[1]Kumaraguru College of Technology, Department of Electronics and Communication Engineering, Coimbatore, India
[2]PSG College of Technology, Department of Electronics and Communication Engineering, Coimbatore, India

Abstract: This paper presents a reversible data hiding technique based on radon and integer lifting wavelet transform to secure the data transmitted over communication network. The technique focuses on three optimality criteria, namely imperceptibility, robustness, and reversibility. The frequency domain strategy is applied due to its superior performance over the spatial domain techniques in certain important aspects like robustness and reversibility towards signal processing and image processing operations. The cover image is first transformed from spatial domain to radon domain and then, this radon image is applied with integer lifting wavelet transform. As the Radon transform performs rotation, scaling and translation operations on the cover image, it changes the locations of the secret bits. Hence, it is very difficult to detect the embedded data without taking the inverse Radon transform and subsequently, it increases the security of the embedded payload. The integer lifting wavelet transform guarantees complete reversibility as they produce integer wavelet coefficients. Then, the middle bit planes of high frequency lifting coefficients are compressed using arithmetic coding to provide space for embedding secret payload. As the proposed framework embeds data in red, green, and blue channels, it can work well for a variety of images with different distribution of colors.

Keywords: reversible data hiding; radon transform; integer lifting transform;bit plane coding;arithmetic coding

Reverzibilno skrivanje podatkov na osnovi Radonove in diskretne valčne transformacije

Izvleček: Članek opisuje tehnike reverznega skrivanaj podatkov na osnovi Radonove in diskretne valčne transformacije za varovanje podatkov preko omrežja. Tehnika sloni na trhe kriterijih: neopaznost, robustnost in reverzibilnost. Uporabljena je strategija na osnovi frekvence saj prednjači pred prostorsko tehniko v ključnih točkah robustnosti in reverzibilnosti obdelave signalov in slik. Slika je najprej pretvorjena v radon proctor in nato še z diskretno valčno transformacijo. Radonova transformacija opravi rotacijo, skaliranje in translacijo in spremeni lokacijo skrivnih bitov. Brez inverzne transformacije je skoraj nemogoče odkriti skrite podatke. Valčna transformacija zagotavlja popolno reverzibilnost in določi valčnbe koeficiente, ki so stisnjeni z aritmetičnim kodiranjem. Predlagan postopek vsebije morer, zelen in rdeč kanal, tako da je uporaben za številne slike.

Ključne besede: reverzibilno skrivanej podatkov; radonova transformacija; diskretna valčna transformacija; koditanje bitne ravnine; aritmetično kodiranje

** Corresponding Author's e-mail: amsaveni.a.ece@kct.ac.in*

1 Introduction

Securing data transmitted over the internet has become a challenging issue caused by the advancement in data digitization and communication networking over the past decade. Therefore, it is necessary to devise strategies to secure information during the process of information exchange. Reversible data hiding has emerged as a major research area due to the phenomenal growth in internet and multimedia technologies. It involves concealing confidential data within another seemingly innocuous cover media such as text, video, audio, images, and compression coding [1].

Basic terminologies used in data hiding are as follows: *Secret Payload* – Message to be embedded in the cover image; *Cover image* – Image that carries the secret message; *Stego image / Embedded image* – Cover image after embedding the secret payload (Cover image + Secret data); *Imperceptibility* – Measure of distortion which is caused by embedding the secret message in the original cover image. It is the inability of the human eye to differentiate between the cover image and the embedded image. Generally, embedded images with higher imperceptibility are preferred in data hiding; *Robustness* – Robustness is the ability of the secret payload to withstand various intentional attacks such as image processing operations and unintentional attacks such as addition of noise; *Embedding Capacity* – Data embedding rate or number of bits embedded per pixel, measured in terms of bits per pixel; *Security / Undetectability* – Any data hiding system may be considered as secure if the possibility of knowing the presence of a secret message in any cover medium is very difficult; *Attacks* – Process of revealing the hidden data from the embedded image by attacking with various signal processing and image processing techniques.

While embedding secret information in a cover image, the emphasis is on two key problems. The first one is to produce an embedded image with a tolerable level of quality so that the distortion produced due to data embedding is imperceptible. The second is to produce the embedded image that is distortion tolerant (robust), i.e., even if the embedded image is attacked during communication, the hidden data can be recoverable. Robustness of data hiding techniques can be enhanced if the properties of the cover image could be properly utilized. By considering these aspects, embedding data in frequency domain becomes more popular compared to spatial domain techniques [2]. The frequency domain techniques modify the frequency coefficients of the cover image by applying a specific transformation function on the cover image. They are designed to be imperceptible and robust against various geometrical transformations and external attacks.

Frequency domain schemes use transformation methods, such as integer cosine transform [3] or integer wavelet transform [4] to compute the transform coefficients of the cover image. Then, these coefficient values are modified to embed the secret data. In reversible data hiding technique based on DCT, one secret bit was embedded into two neighboring DCT coefficients in an image block [5].The secret payload is embedded in the high frequency coefficients of discrete wavelet transform (DWT) by exploiting the statistical properties of the cover image [6]. The DWT works well against various image processing attacks. As it produces floating coefficients, embedded data is potentially lost while reconstructing the cover image by inverse wavelet transform. This drawback is overcome by integer wavelet transform (IWT). The secret data is embedded into the middle frequency of the integer lifting wavelet domain by modifying the histogram of the cover image [7].

Data embedding is also performed in radon domain, which shows a considerable improvement in bit error rate. A radon-based approach was introduced to incorporate translation invariance properties to the payload [8]. RST invariant watermarking technique has been proposed by utilizing the Fourier transform and transforming them to log polar coordinates, which are quite flexible towards rotation, scaling and translation attacks [9].

Hybrid transform has been proposed based on the unique features of the transforms in the hybrid combination, so that it is able to address the robustness and reversibility criteria. Accordingly, the rotation, scaling and translation properties of the Radon transform and reversibility property of integer lifting transform have been joined together in a hybrid formation. The paper investigates a combinatorial data hiding approach using radon transform and integer lifting wavelet transform (ILWT). Radon transform ensures robustness and ILWT makes the algorithm reversible by using the lifting scheme on orthogonal and bi-orthogonal wavelets. The superiority of this combination is also tested and compared with the other existing works in literature. The proposed method improves the quality of embedded image as well as the robustness of embedded payload against various attacks compared to the existing methods.

This paper is organized as follows. Section 2 describes the Radon transform. Section 3 explains Integer Lifting Transform. Section 4 discusses the proposed algorithm. Section 5 presents the experimental results and, Section 6 concludes the paper.

2 Radon transform

Radon transform is a linear transform which is an effective method to analyze signal between the spatial domain and its projection space. It represents the image as a collection of projections along various directions [10]. It computes the projection of the image intensity along a radial line oriented at a specific angle. For each angle θ and at each distance ρ, the intensity of a ray perpendicular to the ρ axis is summed up at $R(\rho,\theta)$. Radon transform converts rectangular coordinates (x, y) into polar coordinates (ρ,θ). The simplest form of discrete Radon transform is to select finite number of the

angular variable of projection, then to take the summation on the discrete image along the projection line.

As shown in Fig.1, the radon transform of a two dimensional function f (x, y) is the integral of function f along a straight line parallel to the y-axis, which is given by,

$$R_\theta(x') = \int_{-} f(x'\cos\theta - y'\sin\theta, x'\sin\theta - y'\cos\theta)\,dy' \quad (1)$$

Where $$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad (2)$$

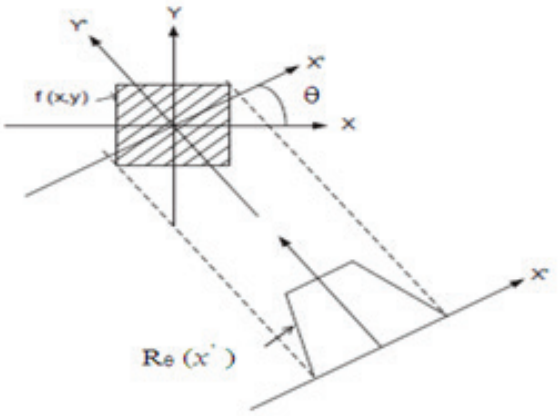

Figure 1: Geometry of the Radon transform

An efficient reversible data hiding method must be robust against a wide range of image processing operations such as image enhancement, cropping, rotation, scaling, compression, and signal processing operation such as addition of noise. However, conventional data hiding algorithms are more sensitive to geometric distortions. Hence, radon transform is introduced to perform rotation, scaling, and translation operations on the cover image. These operations change the positioning of the secret bits. Without taking inverse Radon Transform, it is very difficult to detect the embedded data and subsequently, this increases the security of embedded payload.

3 Integer lifting wavelet transform

There are many researches that have been explored using wavelets in the field of image processing and image steganography. The main advantage of wavelet is that they offer multi-resolution capability, which is similar to the operation of the human visual system. Wavelets provide an optimal representation of signals. Normally, wavelet-based data hiding gives better performance compared to other methods. As the conventional wavelet transform performs a convolution of the input image and the wavelet basis, it requires large memory space for the computation process. The time taken and the large memory required for the conventional wavelet transform is reduced in the lifting method. Lifting transform is a technique used in constructing second generation wavelets entirely in the frequency domain. It is fast compared to the first generation wavelets, as it requires only addition and subtraction.

Conventional wavelet transform is not suitable for reversible data hiding scheme as reversibility property is not guaranteed. Wavelet transform operates on a floating-point arithmetic basis. An image that has integer intensity values in the spatial domain is converted into decimal wavelet coefficients. The wavelet coefficients are modified appropriately during data hiding operation and inverse wavelet transform is carried out to reconstruct the image in the spatial domain. A serious note here is that practically wavelet coefficients are truncated or rounded as it is not viable to represent the coefficients to its full accuracy. Information is potentially lost while reconstructing the image by inverse wavelet transform. But reversible data hiding schemes have to recover the host image without distortion along with the secret payload. Eventually, this makes the discrete wavelet transform a poor choice for reversible data hiding [11]. To address this specific issue, an invertible integer lifting wavelet transform is used in the proposed scheme. The system operates on integer arithmetic and alleviates the loss of any information via forward and inverse transforms [12].

The lifting wavelet transform decomposes the image into frequency subbands, which contain approximation and detail coefficients. The system reserves the detail coefficients, which have texture, edges, and region boundary for data hiding. It is an insensible region for human visual system. An advantage of the Lifting Scheme is that it can be converted easily into a transform that maps integers to integers while retaining the perfect reconstruction property. Thus, embedding data in integer lifting wavelet domain satisfies the properties like security, imperceptibility, and robustness of the proposed technique.

4 Bit plane embedding using binary arithmetic coding

The Binary Arithmetic Coding can be exploited for compressing the bit planes of grayscale/colour images. As arithmetic coding is a lossless compression method, it guarantees the recovery of original payload. In bit plane embedding, the most significant bits for each

CLH Header (16 bits)	CHL Header (16 bits)	CHH Header (16 bits)	CLH Length (16bits)	CHL Length (16bits)	CHH Length (16 bits)	Length of embedding data (32 bits)	Secret Payload

Figure 2: Structure of the embedded bit plane

pixel are grouped into one bit plane, the next most significant bits into another bit plane and so on till the least significant bit plane. Mostly, the five highest order planes contain visually significant data. The other lower bit planes contain fine details in the image. Lesser the bit plane number, lesser is its contribution to the final stage.

Statistically, there is an equal distribution of zeroes and ones in the lower planes of the image than in the higher planes. This leads to lower compression ratio and lower embedding capacity in the lower bit planes than in the higher planes. This is because binary sequences of length L having higher probability may be encoded more compactly than another one of the same length with a lower probability. But the signal to noise ratio falls down as higher bit planes are altered for embedding [13].

The most significant bit plane contains the most critical approximation values of the image. Hence, modifications made in higher bit-plane may degrade the quality of the cover image. In order to have the embedded image visually as same as the cover image, data is hidden in one or more middle bit planes.

The bits in one or more bit-planes can be compressed to provide space to hide data like text or image due to the existence of redundant information. The approximate coefficients in the LL sub-band contribute to visual perception. Hence, the secret bits are embedded in LH, HL or HH subbands (Detail Coefficients). The original bits in the selected bit plane of LH, HL or HH subbands are compressed using arithmetic coding to provide space for embedding the payload bits.

The structure of the embedded bit plane is shown in Fig.2. CHH, CHL, and CLH headers represent the header information of the compressed HH, HL, and LH sub bands. They describe the bit distribution required for arithmetic encoder and decoder. CHH, CHL, and CLH lengths denote the length of the compressed bit stream in the chosen bit plane of the LH, HL, and HH subbands.

5 Proposed methodology

Majority of the methods discussed in the literature addressed only a few of the desired characteristics, namely lossless/reversible, imperceptible, high payload capacity and robustness, and not all. The proposed method of reversible data hiding is based on bit plane embedding in radon and integer lifting wavelet domain. It aims to meet all the desired characteristics to an optimal level. The block diagram of the proposed data embedding algorithm is shown in Fig.3.

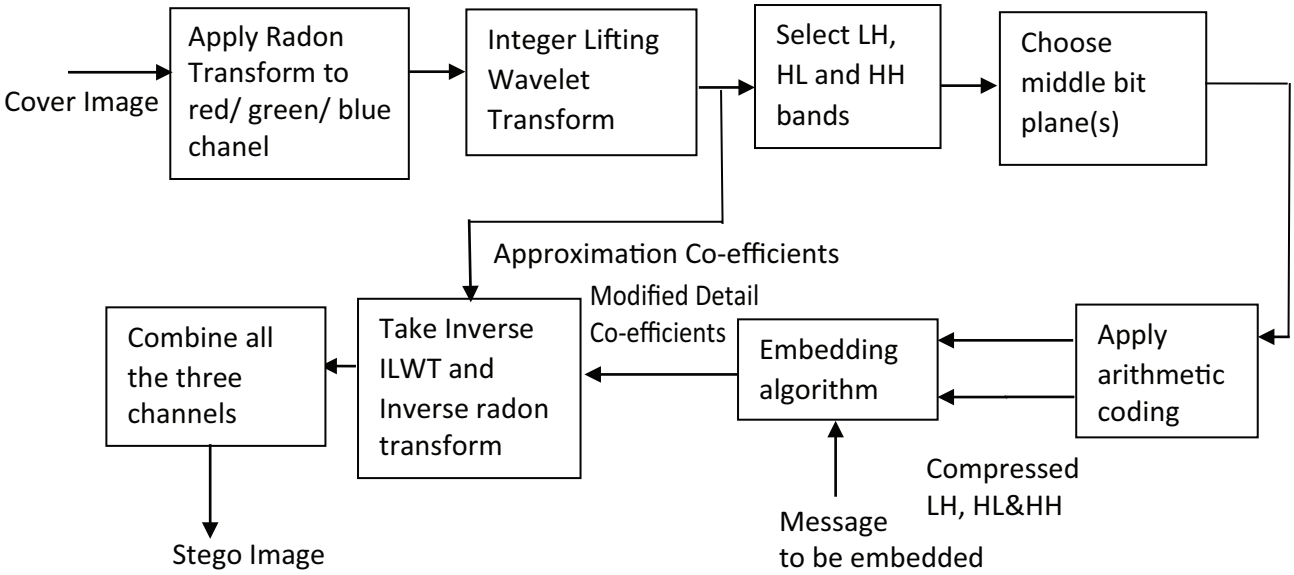

Figure 3: Block diagram of embedding process

5.1 Data Embedding Algorithm

Input: Cover image with M-rows and N-columns, Secret payload bits.
Output: Stego Image
Step 1: Read the cover image of size M x N.
Step 2: Separate color channels (Red, Green, and Blue) of the cover image.
Step 3: Apply radon transform on any one of the channels.
Step 4: Notice that Radon image undergoes a single level integer lifting wavelet transform which results in 4 subbands (LL, LH, HL, HH) of size M/2 x N/2, each.
Step 5: Construct binary images from the chosen bit planes of LH, HL, and HH bands.
Step 6: Compress the original bits in the chosen bit plane of these bands using arithmetic coding and obtain the header information required for the arithmetic encoder and decoder.
Step 7: Read the secret payload and convert it into a bit string.
Step 8: Concatenate the header length, header information, and compressed bit streams of CLH, CHL, and CHH and the secret payload to get a single bit stream.
Step 9: Embed bit stream into chosen bit plane of LH band. If not enough, embed in HL band and then in HH band and observe that it results in embedded LH, HL, and HH components.
Step 10: Apply inverse integer lifting transform on LL coefficients and the modified LH, HL, and HH coefficients.
Step 11: Compute inverse radon transform of the image obtained from Step 10.
Step 12: Combine all the three color channels to get stego image.

5.2 Data Extraction Algorithm

Step 1: Read the stego image of size M x N.
Step 2: Separate color channels (Red, Green, and Blue) of stego image.
Step 3: Apply radon transform to the channel in which the data is embedded.
Step 4: Notice that Radon image undergoes single level integer lifting wavelet transform which results in 4 subbands (LL, LH, HL, HH) of size M/2 x N/2, each**.**
Step 5: Construct binary images from chosen bit planes of LH, HL, and HH bands.
Step 6: Derive the header information and header length needed for arithmetic decoding.
Step 7: Extract the compressed bits from the chosen bit plane of these bands using arithmetic decoder and decompress the subbands to get the reconstructed subbands.
Step 8: Apply inverse integer lifting transform on the reconstructed subbands LH, HL, and HH along with LL subband.
Step 9: Compute inverse radon transform of the image obtained from Step 8.
Step 10: Combine all the three channels to get the original cover image.

6 Expermental results

In order to investigate the performance of the proposed data hiding algorithm, several experiments are carried out in a computer system equipped with Intel core 2 duo processor with 2 GB memory and a clock speed of 2 GHz. Matlab 8 (R2013a) platform is used for the digital simulation of the algorithm. Five standard 512 x 512 color images such as (a) *Airplane*,(b) *Baboon*, (c) *Boat*, (e) *Lena* and (e) *Pepper*, obtained from USC-SIPI (Image database), have been used as cover images. The performance of the algorithm is investigated in terms of imperceptibility, robustness, and reversibility.

6.1 Imperceptibility

The metrics used to test the imperceptibility property of the proposed algorithm are PSNR (Peak Signal to Noise Ratio) and SSIM (Structural Similarity Index Measure).

The PSNR for an image of size M x N is calculated by,

$$PSNR = 10 \log_{10} (255^2 / MSE) \text{ dB} \quad (3)$$

where,

$$MSE = \sum_{x=1}^{M}\sum_{y=1}^{N} \left(p(x,y) - p'(x,y)\right)^2 \quad (4)$$

where *p(x, y)* stands for the pixel value in the cover image and *p'(x, y)* is the pixel value at position *(x, y)* in the stego image after embedding the secret message. M and N denote the number of rows and columns of the image and (*x, y*) denotes the pixel coordinates.

The quality of the stego image is also calculated using SSIM as follows:

$$SSIM = \frac{(2\mu_x\mu_y + c1)(2\sigma_{xy} + c2)}{(\mu 2x + \mu 2y + c1)(\sigma 2x + \sigma 2y + c2)} \quad (5)$$

where x and y are same size windows of the cover and stego images and μ_x and μ_y are corresponding x and y averages. σ^2_x and σ^2_y are the variances of x and y and

σ_{xy} is the covariance of x and y. The positive constants c_1 and c_2 are included to avoid a null denominator. Typically $c_1 = (k_1L)^2$; $c_2 = (k_2L)^2$; L= $(2^{\text{no.of bits/pixel}})$ -1; [k_1, k_2]=[0.01,0.03] by default.

Table 1 shows the PSNR and SSIM of cover images after embedding a payload of 10,000 bits using the wavelet *cdf2.4* (Cohen-Daubechies-Feauveau 2.4) in the fourth bit plane of Red, Green and Blue channels. As the PSNR obtained from the stego images is greater than 42 dB, the embedded payload is highly imperceptible to the human eye, i.e., the perceptual quality of the resultant stego images is good. The red channel offers better PSNR and SSIM compared to green and blue channels. The red channel gives an improvement in PSNR of about 2.0 to 7.0 dB over green and blue channels. Among all cover images, the *Airplane* image yields better PSNR for the same payload.

Table 1: Quality metrics

Cover image	PSNR (dB) and SSIM					
	Red Channel		Green Channel		Blue Channel	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Airplane	47.70	0.9771	47.65	0.9867	46.70	0.9519
Baboon	43.29	0.9900	42.91	0.9704	42.49	0.9894
Boats	46.96	0.9921	43.23	0.9740	43.69	0.9693
Lena	45.87	0.9820	42.46	0.9780	43.46	0.9409
Pepper	46.86	0.9784	44.34	0.9840	42.39	0.9656

The Fig.4. shows the embedded images of size 512 x 512, after embedding a payload of 10,000 bits using *cdf2.4* in the fourth bitplane of red channel of standard images.

Table 2 summarizes the quality of the Lena image under varying payload, after embedding in the bit plane 4, 5, and 6 of red channel using wavelet *cdf2.4*.

Table 2: Embedding capacity Vs. PSNR (dB)

Secret payload (bits)	Embedding Rate (bpp)	PSNR (dB)		
		Bit Plane 4	Bit Plane 5	Bit Plane 6
1000	0.004	45.27	43.08	41.42
3000	0.011	45.26	43.07	41.40
6000	0.023	45.14	43.04	41.20
10,000	0.038	45.10	43.02	41.06
20,000	0.076	44.68	42.54	40.83
40,000	0.153	42.21	40.41	38.33
50,000	0.191	42.20	39.80	38.33
70,000	0.267	41.49	39.52	37.44
80,000	0.305	41.28	38.79	37.17

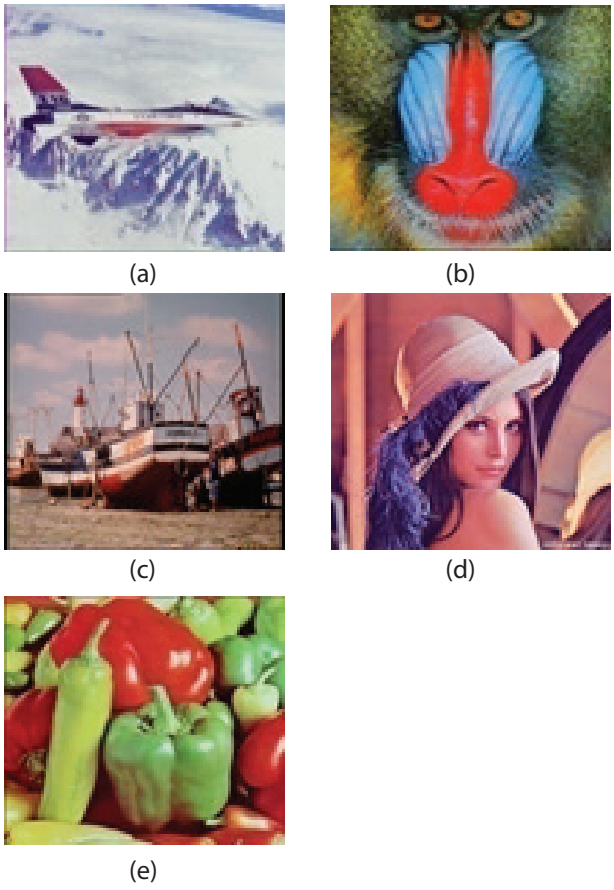

Figure 4: Standard color images of size 512 x 512 after embedding a payload of 10,000 bits (a) Airplane; (b) Baboon; (c) Boat; (d) Lena; (e)Pepper

86,000	0.328	41.16	38.72	37.13
90,000	0.343	Insufficient	38.64	37.11
95,000	0.362	Insufficient	Insufficient	37.04
96,000	0.366	Insufficient	Insufficient	Insufficient

The perceptual quality of cover image will get reduced if the data is embedded in higher bit planes and also PSNR drops down as more number of bits embedded in that plane. The bit plane 4 can accommodate only 90,000 bits as the bit plane 4 provides less space for data embedding compared to other bit planes. The maximum embedding capacity of bit planes 5 and 6 is 95,000 bits and 96,000 bits respectively. Beyond 95,000 bits, there is no space to accommodate the secret payload in both the bit planes. The embedding capacity completely depends upon cover image and is also based on the bit distribution of the chosen bit plane. The PSNR varies from 41.12 dB at the embedding rate of 0.004 bits per pixel to 37.04 dB at 0.362 bits per pixel for bit plane 6.

The experimental results of the proposed scheme are compared with the various schemes discussed in Tsai &

Sun [14], Fu & Shen [15], and Niu et al [16] and summarized in Table 3. The PSNR of the cover images is measured after embedding a payload of 10,000 bits in Red channel using the wavelet *cdf2.4*.The PSNR offered by the proposed scheme is about 15% greater than Niu et al scheme. The proposed scheme gives better PSNR for *Lena* image compared to *Baboon* and *Boat* images.

Table 3: Comparison of the proposed scheme with the schemes in the literature

Host image	PSNR (dB)			
	Tsai and Sun Scheme	Fu and Shen Scheme	Niu et al Scheme	Proposed Scheme
Lena	39.43	38.10	40.57	45.87
Baboon	41.76	38.90	41.67	43.29
Boat	42.49	39.72	40.71	44.03

6.2 Robustness

Robustness is measured using Bit Error Rate (BER) and is defined as:

$$\mathrm{BER} = \sum_{k=0}^{n} b_k \oplus b_k' / N \quad (6)$$

where b and b' are embedded and extracted bits respectively, N is the total number of secret bits embedded and represents $\oplus$ the XOR operation. The value of BER ranges between 0 and 1. If BER is closer to 1 then, it means that the error value of extracted data is higher. The value of BER is calculated after retrieving the secret data from the embedded block. Lower the BER%, higher is the accuracy of the extracted secret data.

The stego images are added with Gaussian noise with a variance of 0.2 and 0.4, Poisson Noise, Impulse Noise with a variance of 0.05 and 0.1 and Speckle Noise with a variance of 0.05 and 0.1. Generally, addition of noise is responsible for the degradation of the image. The image processing operations such as Rotation (5 and 10 degrees), Scaling (200% and 400%), Blurring and Cropping (10% and 25%) are performed on embedded images.

After subjecting to the attacks, the original cover image is extracted and the bit error rate of extracted payload over secret payload is measured. Table 4 summarizes the experimental results for the proposed data hiding scheme against various attacks. As the BER is about 0.15 to 0.35 % of embedded payload, the algorithm is robust against various intentional and unintentional attacks.

6.3 Reversibility

In order to ensure the reversibility, the extracted cover image and the original cover image must be similar.The metric used to measure the similarity between the two images is Normalized Correlation Coefficient (NCC). The value of 0 represents no correlation. NCC will approach to one if the extracted cover image resembles the original cover image. The Normalized Correlation Coefficient between cover image and extracted cover image is defined as,

$$\mathrm{NCC} = \frac{\sum_{x,y}\left(f(x,y)-f_{mean}\right)\left(g(x,y)-g_{mean}\right)}{\sqrt{\sum_{x,y}\left(f(x,y)-f_{mean}\right)^2 \sum_{x,y}\left(g(x,y)-g_{mean}\right)^2}} \quad (7)$$

Table 4: Effect of various attacks on BER

Attacks	Bit Error Rate				
	Airplane	Baboon	Boats	Lena	Pepper
Gaussian Noise (σ^2 =0.2)	0.0032	0.0034	0.0035	0.0032	0.0034
Gaussian Noise (σ^2 =0.4)	0.0036	0.0036	0.0037	0.0037	0.0038
Poisson Noise	0.0028	0.0030	0.0029	0.0030	0.0031
Impulse Noise (σ^2=0.05)	0.0017	0.0020	0.0021	0.0018	0.0022
Impulse Noise (σ^2=0.10)	0.0019	0.0022	0.0024	0.0020	0.0024
Speckle Noise (σ^2=0.05)	0.0018	0.0021	0.0025	0.0026	0.0024
Speckle Noise (σ^2=0.10)	0.0019	0.0024	0.0027	0.0027	0.0026
Rotation (5°)	0.0018	0.0021	0.0020	0.0022	0.0024
Rotation (10°)	0.0020	0.0023	0.0023	0.0024	0.0026
Scaling (200%)	0.0016	0.0017	0.0018	0.0019	0.0022
Scaling (400%)	0.0018	0.0019	0.0020	0.0020	0.0024
Blurring (5)	0.0024	0.0023	0.0020	0.0019	0.0023
Blurring (10)	0.0027	0.0026	0.0022	0.0021	0.0025
Cropping (10%)	0.0026	0.0028	0.0030	0.0029	0.0031
Cropping (25%)	0.0031	0.0034	0.0033	0.0031	0.0033

where f (x, y) is the original cover image, g (x, y) is the extracted cover image.

Table 5 summarizes the experimental results for the proposed data hiding scheme against various attacks. As the NCC values are greater than 0.98, it is concluded that the algorithm restores the original cover image exactly at the destination.

7 Conclusion

In this paper, a reversible data hiding technique based on radon and integer lifting wavelet transform is presented. Hybrid transform has been proposed based on the unique features of the transforms, so that it is able to address the robustness and reversibility criteria. As the Radon transform performs rotation, scaling and translation operations on the cover image, it changes the positioning of the secret bits. The integer lifting wavelet transform guarantees complete reversibility. The original bits in the selected bit planes of LH, HL or HH subbands are compressed using arithmetic coding to provide space for embedding the payload bits. Generally, middle bit planes are used for embedding as they provide a balanced trade-off between embedding capacity and visual quality of that stego image. Data is embedded in red, green, and blue channels of the color image independently. As the PSNR obtained for the stego images is greater than 42 dB, the embedded payload is imperceptible to the human eye. The results have been compared with the existing works in the literature and the proposed method gives 10 to 15% improvement in PSNR. As the BER is about 0.15 – 0.35 % of embedded payload, the algorithm is robust to attacks. From the simulation results, it is inferred that the proposed algorithm exhibits reversibility due to high NCC values.

8 References

1. Amsaveni, A. and Vanathi, P.T. (2015) 'A comprehensive study on image steganography and steganalysis techniques', *Int. J. Information and Communication Technology*, Vol. 7, Nos. 4/5, pp.406–424.
2. Amsaveni, A. and Vanathi, P.T. (2015) 'An efficient reversible data hiding approach for colour images based on Gaussian weighted prediction error expansion and genetic algorithm', *Int. J. Advanced Intelligence Paradigms*, Vol. 7, No. 2,pp.156–171.
3. Yang, B., Schmucker, M., Funk, W., Busch, C & Sun, S (2004), 'Integer DCT-based reversible watermarking for images using companding technique', Proceedings of Electronic Imaging, Science and Technology, vol. 5306, pp. 405-415.
4. Xuan, G., Zhu, J., Chen, J., Shi, Y.Q., Ni, Z., & Su, W (2002), 'Distortion less data hiding based on integer wavelet transform', IEEE Electronics Letters., vol. 38, no. 25, pp. 1646-1648.
5. Lin, S.D., Shie, S.C., & Guo, J.Y., (2010), 'Improving the robustness of DCT based image watermarking against JPEG compression', International Journal of Computer Standards and Interfaces, vol. 32, no. 1, pp. 54-60.

Table 5: Effect of various attacks on NCC

Attacks	Normalized Correlation Co-efficient				
	Airplane	Baboon	Boats	Lena	Pepper
Gaussian Noise (σ^2 =0.2)	0.9817	0.9843	0.9825	0.9819	0.9824
Gaussian Noise (σ^2 =0.4)	0.9850	0.9842	0.9860	0.9805	0.9814
Poisson Noise	0.9829	0.9844	0.9832	0.9822	0.9814
Impulse Noise (σ^2=0.05)	0.9839	0.9843	0.9816	0.9811	0.9813
Impulse Noise (σ^2=0.10)	0.9810	0.9816	0.9804	0.9802	0.9807
Speckle Noise (σ^2=0.05)	0.9833	0.9822	0.9871	0.9864	0.9846
Speckle Noise (σ^2=0.10)	0.9811	0.9804	0.9810	0.9820	0.9825
Rotation (5°)	0.9880	0.9806	0.9802	0.9824	0.9816
Rotation (10°)	0.9863	0.9794	0.9788	0.9804	0.9810
Scaling (200%)	0.9835	0.9820	0.9869	0.9846	0.9863
Scaling (400%)	0.9825	0.9806	0.9832	0.9828	0.9822
Blurring (5)	0.9854	0.9810	0.9809	0.9817	0.9826
Blurring (10)	0.9825	0.9806	0.9789	0.9738	0.9805
Cropping (10%)	0.9732	0.9726	0.9727	0.9728	0.9716
Cropping (25%)	0.9702	0.9706	0.9701	0.9706	0.9678

6. Xiang, S., Kim, H.J., & Huang, J (2008), 'Invariant Image watermarking based on statistical features in the low frequency domain', IEEE Transactions on Image Processing, vol. 14, no. 12, pp. 2140-2150.
7. Xuan, G., Zhu, J., Chen, J., Shi, Y.Q., Ni, Z., & Su, W., (2002), 'Distortion less data hiding based on integer wavelet transform', IEEE Electronics Letters., vol. 38, no. 25, pp. 1646-1648.
8. Stankovic, S, Djurovic, I & Pitas, I 2001, 'Watermarking In The Space/Spatial-Frequency Domain Using Two-Dimensional Radon-Wigner Distribution', IEEE Transactions on Image Processing, vol. 10, no. 4, pp. 650-658.
9. Lin, C, Wu, M, Bloom, J, Cox, I, Miller, M & Lui, Y 2001, 'Rotation, scale, and translation resilient watermarking for images', IEEE Transactions on Image Processing, vol. 10, no. 5, pp. 767-782.
10. Kim, H, Baek, Y, Lee, H & Suh, Y 2003, 'Robust image watermark using Radon transform and bispectrum invariants', Lecture Notes in Computer Science, pp. 145-159.
11. Lee, S, Yoo, CD & Kalker, T 2007, 'Reversible image watermarking based on integer-to-integer wavelet transform', IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 321-330.
12. Calderbank, AR, Daubechies, I, Sweldens, W & Yeo, B 1998, 'Wavelet transforms that map integers to integers', Applied and Computational Harmonic Analysis, vol. 5, no. 3, pp. 332-369.
13. Xuan, G, Zhu, J, Chen, J, Shi, YQ, Ni, Z & Su, W 2002, 'Distortion less data hiding based on integer wavelet transform', IEEE Electronics Letters., vol. 38, no. 25, pp. 1646-1648.
14. Tsai, HH & Sun, DW 2007, 'Color image watermark extraction based on support vector machines' Journal of Information Sciences, vol. 177, no. 2, pp. 550-569.
15. Fu, YG & Shen, RM 2008, 'Color image watermarking scheme based on linear discriminant analysis. Computer Standard & Interfaces',vol. 30, no. 3, pp. 115-120.
16. Niu, PP, Wang, XY, Yang, YP & Ming, Y 2011, 'A novel color image watermarking scheme in non-sampled contourlet-domain', Journal of Expert Systems with Applications, vol. 38, no. 3, pp. 2081-2098 .

Arrived: 31. 03. 2017
Accepted: 12. 06. 2017