J Inf Process Syst, Vol.13, No.5, pp.1331~1344, October 2017
https://doi.org/10.3745/JIPS.03.0042

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Data Hiding Algorithm for Images Using Discrete Wavelet Transform and Arnold Transform

Geeta Kasana*, Kulbir Singh**, and Satvinder Singh Bhatia***

Abstract
In this paper, data hiding algorithm using Discrete Wavelet Transform (DWT) and Arnold Transform is proposed. The secret data is scrambled using Arnold Transform to make it secure. Wavelet subbands of a cover image are obtained using DWT. The scrambled secret data is embedded into significant wavelet coefficients of subbands of a cover image. The proposed algorithm is robust to a variety of attacks like JPEG and JPEG2000 compression, image cropping and median filtering. Experimental results show that the PSNR of the composite image is 1.05 dB higher than the PSNR of existing algorithms and capacity is 25% higher than the capacity of existing algorithms.

Keywords
Arnold Transform, DWT, JPEG, JPEG2000, PSNR, SIM

1. Introduction

Recent years have witnessed the rapid development of the Internet and multimedia techniques. Due to these developments, it has been possible to exchange large amount of digital data over a wide range of public networks. However, data transmitted through these networks may not be secure. So security of transmitted data is becoming more and more important. Data hiding is an important branch of information security. It is a technique that aims at hiding the existence of hidden data. Data is hidden in a host medium such as digital images, videos and audios, etc., and then transmitted to the receiver using public networks like Internet. The main characteristics required by the data hiding applications are transparency, capacity and robustness. Transparency is the ability to avoid suspicion about the existence of a secret hidden data, capacity is the amount of hidden secret data in the host medium and robustness measures the vulnerability against intentional and non-intentional attacks. Data hiding consists of two branches–digital watermarking and steganography. The watermarking process is to hide given secret data into an image. Steganography is data hiding technique used in covert communication which hides the existence of hidden data. In case of steganography, the most important feature is the transparency followed by the capacity while in watermarking, robustness plays more important role than transparency and capacity.

Manuscript received January 16, 2015; accepted July 28, 2015; onlinefirst December 17, 2015.
Corresponding Author: Geeta Kasana (gkasana@thapar.edu)
* Computer Science and Engineering Department, Thapar University, Patiala 147-004, India (gkasana@thapar.edu)
** Electronics and Communication Engineering Department, Thapar University, Patiala 147-004, India (ksingh@thapar.edu)
*** School of Mathematics, Thapar University, Patiala 147-004, India (ssbhatia@thapar.edu)

Data hiding techniques are generally designed for following special applications [1,2]:

a. Metadata or additional information: Embedding data to describe the information such as structure, indexing terms etc.
b. Copyright protecting: Embedding the ownership of the information for preventing copyright from duplication or abuse.
c. Multiple data embedding: Embedding smaller images in a larger host image or multiple audio data in a video.

Data hiding methods can be classified mainly into two categories- frequency domain methods and spatial domain methods. In frequency domain methods, the image is transformed using some transform like DWT. After transformation, secret data is hidden into the transformed coefficients of the image. DWT based methods are discussed into [3-10]. In these methods, wavelet coefficients produced by DWT are used to embed the secret data bits. In spatial domain methods, secret data is embedded directly into the pixels of the cover image. Some spatial domain methods are discussed into [11-14]. However, these methods have low capacity and are not robust enough to the image processing operations. So, there is a need to have data hiding algorithm having good capacity and robust to the image processing operations.

The rest of this paper is organized as follows. In Section 2, theory behind the DWT and Arnold Transform is presented. In Section 3, proposed data hiding algorithm and quality parameters used in comparison are discussed. In Section 4, experimental results are demonstrated to show the effectiveness of the proposed algorithm. Finally, the paper is concluded in Section 5.

2. DWT and Arnold Transform

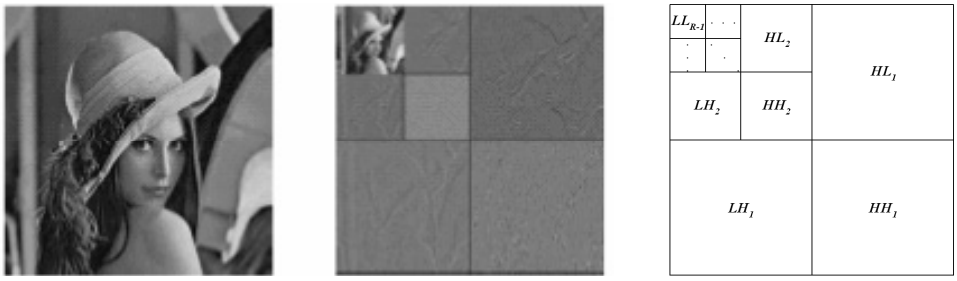
In this section, DWT, Arnold Transform and related terms used in this paper are defined.

2.1 DWT

DWT is identical to a hierarchical subband system, where the subbands are logarithmically spaced in frequency. DWT decomposes the image into L-level dyadic wavelet pyramid. For each level, DWT is applied twice, once row-wise and once column-wise and hence four subbands are produced which are:

(i) Horizontally and vertically low-pass (LL) subband
(ii) Horizontally low pass and vertically high-pass (LH) subband
(iii) Horizontally high-pass and vertically low-pass (HL) subband
(iv) Horizontally high-pass and vertically high-pass (HH) subband

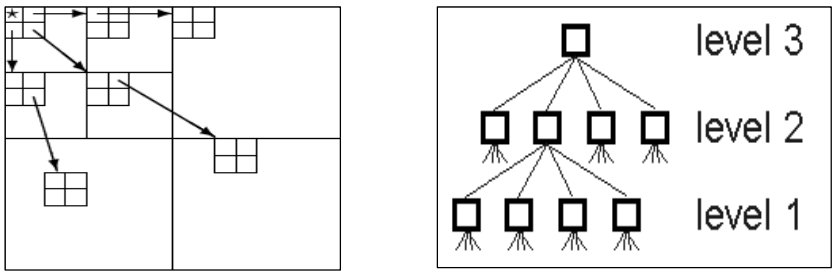
Let us consider the input image Lena shown in Fig. 1(a) as LL0 subband. LL0 subband is decomposed into LL1, LH1, HL1, and HH1 subbands. At next level, LL1 is further decomposed into LL2, LH2, HL2, and HH2 subbands. A two level wavelet decomposition of the image Lena is shown in Fig. 1(b). The decomposition process is repeated until the image is decomposed into required level as shown in Fig. 1(c).



(a) (b) (c)

Fig. 1. Discrete wavelet transform (DWT) pyramid decomposition.

After transforming an image using DWT, it is represented using tree structure because of the sub sampling that is performed in the transform. A wavelet coefficient in a subband has four descendants in the next higher level subband, as shown in Fig. 2(a). Each of the four descendants also has four descendants in the next higher level subband. Due to this property, there is the quad tree in which each root has four children, as shown in Fig. 2(b).



(a) (b)

Fig. 2. (a) Parent child relationship of wavelet coefficients of image subbands**.** (b) Relationship between the levels of the wavelet decomposed image.

Fig. 3. Original secret data.

2.2 Arnold Transform

Encryption is an effective way to protect the contents of digital media. Arnold transform is very popular and has been widely used as a method to shuffle the secret image. It was proposed by Arnold [6] and is defined by the following equation:

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix} (mod\ N) \tag{1}$$

where mod is modulo operator, (m, n) are the coordinates of the original image pixel, (m', n') are the coordinates of the scrambled image pixel, N is the image size. The transform changes the position of

image pixels, and if it is repeated several times, a disorder image is generated.

2.3 Related Terms

Cover image is an image in which secret data is hidden. Composite image is one in which data has been hide inside it after embedding process. Capacity is the amount of secret data which is to be concealed.

Bits Per Pixel (bpp): It is the number of bits used to indicate the color of a single pixel in a bitmapped image or video frame buffer. Suppose there is an image having 256 colors, then 8 bpp are required to represent a pixel of image. If this image is compressed 50%, then 4 bpp are required to represent each pixel in a compressed image.

Quality Factor (QF): It is a number used in JPEG compression and lies in the interval [0,100]. The small value of QF means higher compression ratio but it can decrease the visual quality of compressed image and large value of QF means less compression ratio which generally produce good visual quality images.

3. Proposed Algorithm

In this section, data embedding and extracting method using DWT and Arnold transform is proposed. The secret data is scrambled using Arnold transform and it is embedded into largest child coefficient of a wavelet coefficient in a subband which is greater than the threshold of the subband of cover image. Median value of respective subband is taken as threshold of the subband.

3.1. Embedding Method

Following are the steps to embed the secret data into cover image.

Step 1. The cover image is decomposed using DWT to get its wavelet subbands.
Step 2. Arnold transform is applied on the secret data to get the scrambled secret image.
Step 3. Take the median of all wavelet subbands.
Step 4. Compare the wavelet coefficients of subband with its median.
Step 5. If a wavelet coefficient is greater than median then find the largest child of this wavelet coefficient, and embed the scrambled secret data pixel using the following equation:

$$B(m,n) = A(m,n) + \alpha \times W(m,n)$$

where α is the scaling parameter [5]. $W(m,n)$ is the scrambled secret data, $A(m,n)$ is the value of largest child and $B(m,n)$ is the pixel of the composite image, m and n are the index of a pixel.

3.2. Extraction Method

To extract the secret data, both cover and composite images are required.

Step 1. Decompose composite and cover images using DWT to get their subbands.
Step 2. Take the median of subbands of cover image.
Step 3. Compare the wavelet coefficients of subbands of cover image with its median value.
Step 4. If a coefficient is greater than median then find the largest child of this coefficient and use the following equation to extract the secret data.

$$W'(m,n) = \frac{((B(m,n) - A(m,n))}{\alpha}$$

where $A(m,n)$ is the wavelet coefficient of the cover image and $B(m,n)$ is the wavelet coefficient of the composite image and α is a scaling parameter.
Step 5. Process the scrambled secret data $W'(m,n)$ with Arnold transform to get the extracted secret data.

3.3. Quality Parameters

In this work peak signal to noise ratio ($PSNR$) is taken as a quality parameter to evaluate the quality of the composite image. The $PSNR$ is defined as

$$PSNR = 10log_{10}\frac{(2^b - 1)^2}{MSE}$$

where b is the bit depth of the image and MSE is the mean square error, which is defined as

$$MSE = \sum_{m=1}^{h}\sum_{n=1}^{w}\frac{\big(A(m,n) - B(m,n)\big)^2}{h \times w}$$

where $A(m,n)$ is the pixel of composite image and $B(m,n)$ is the pixel of cover image, h and w is the height and width of the images, respectively.

Similarity Index Modulation (SIM) is defined as

$$SIM = \frac{\sum_m \sum_n W(m,\ n)\ \times\ W'(m,n)}{\sum_m \sum_n [W(m,n)]^2}$$

is used evaluate the quality of the extracted secret data by measuring the similarity of the original secret data W and the extracted secret data W'. It is taken as an objective measure in this research work.

Correlation is given by the

$$correlation = \frac{\sum(x - \bar{x}) \times (y - \bar{y})}{\sqrt{\sum(x - \bar{x})^2 \times \sum(y - \bar{y})^2}}$$

where x is the pixel of cover image, $\bar{x}$ is the mean of the cover image and y is pixel of composite image and $\bar{y}$ is the mean of composite image.

The larger the PSNR, the image quality is better. In general, a composite image is acceptable by human perception if its PSNR is greater than 30 dB [15]. SIM is generally between 0 to 1. Ideally it should be 1 but upto 0.75 is acceptable. One can say SIM and correlation are used to evaluating the

robustness of data hiding technique and the PSNR is used for evaluating the imperceptibility of data hiding technique.

4. Experimental Results

The proposed algorithm is implemented in MATLAB software. The secret data is logo image of size 7200 bits, shown in Fig. 3. The cover images are decomposed into 5 level using wavelet transform. For this work, we considered different 512×512 gray scale cover images like Lena, Barbara, Baboon, Pepper, Clown, Boat, Crowd and Girl. Some of these cover images are shown in Fig. 4(a)-4(d). Table 1 shows capacity, PSNR, correlation and SIM of Lena image after embedding secret data into sub bands of 5^{th}, 4^{th} and 3^{rd} level. We can embed the secret data of 390728 bits into all sub bands of cover image of size 512×512. In this case, PSNR is 52.8008 and correlation and SIM between original and extracted secret data is 0.9011 and 0.9405, respectively.

Table 1. Payload, PSNR, correlation and SIM from Lena composite image

Capacity (bits)	PSNR (dB)	Correlation	SIM
7200	54.7329	0.9999	1.00
8192	53.9716	0.9998	1.00
8712	53.8467	0.9997	1.00
9800	53.5701	0.9990	1.00

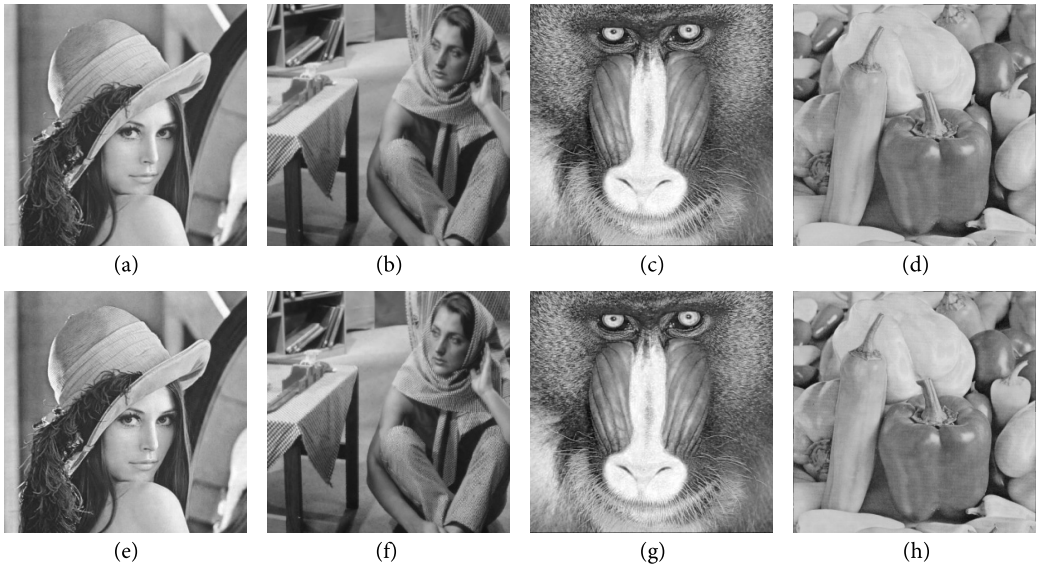


Fig. 4. (a-d) Cover image of Lena, Barbara, Baboon and Pepper. (e-h) Composite images of Lena, Barbara, Baboon and Pepper.

Table 2 shows PSNR, correlation and SIM of the different images after embedding the secret data having capacity 7200 bits into sub bands of 5^{th}, 4^{th} level. Fig. 4(e)-(h) are composite images with PSNR 46.8131, 46.7585, 46.8151, and 46.0376 dB after embedding the secret data image. If the cover images

shown in Fig. 4(a)-(d) and the composite images shown in Fig. 4(e)-(h) are observed, one cannot find any perceptual degradation. PSNR, correlation, SIM and extracted secret data from different composite images are shown in Table 2.

To study the robustness of the proposed algorithm, we carried out the attacks on the composite images and find out the correlation and SIM between original and extracted secret data. The results after different attacks performed on composite images are given in Table 3. One can observe that visual quality of composite images is good. From Tables 2 and 3, one can observe that SIM and correlation between original and extracted secret data is very close to one which means there is very less degradation in secret data. Visual quality of the extracted image is also very good.

Table 2. PSNR, correlation and SIM, extracted secret data without any attack

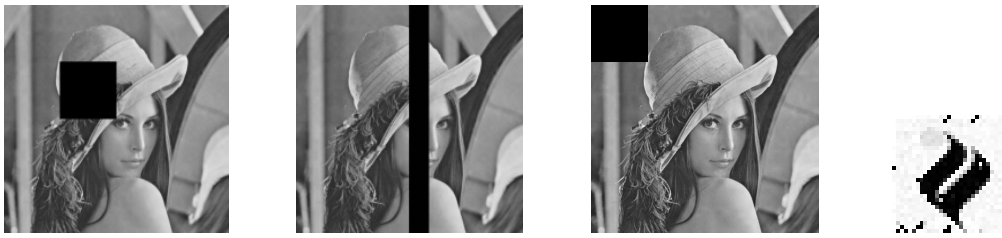
Image	PSNR(dB)	Correlation	SIM	Extracted Secret data
Barbara	46.7585	0.9998	0.9950	
Lena	46.8131	0.9998	0.9978	
Baboon	46.8151	0.9997	0.9972	
Pepper	46.0376	0.9998	0.9995	
Clown	46.8398	0.9998	0.9985	
Boat	46.7427	0.9998	0.9990	
Crowd	46.7432	0.9994	0.9933	
Girl	45.2078	0.9988	0.9774	

Table 3. Correlation and SIM values of extracted secret data under various attacks

Images		Gaussian noise	Salt and Pepper	Blur	Crop (64×64)	Rotation (90˚)	JPEG QF= (70/20)
Lena	Correlation	0.9990	0.9564	0.997	0.9211	0.9999	0.9983/0.9564
	SIM	0.9990	0.8901	0.903	0.8715	0.9990	1.000/0.8909
Barbara	Correlation	0.9990	0.9534	0.989	0.9401	0.9990	0.998/0.9961
	SIM	0.9890	0.9512	0.895	0.7755	0.9990	1.00/0.9593
Baboon	Correlation	0.9998	0.8989	0.997	0.9689	0.9998	0.9644/1.00
	SIM	0.8314	0.9308	0.877	0.9219	0.9950	0.9979/0.9879
Pepper	Correlation	0.9901	0.8600	0.996	0.9577	0.9990	0.9975/0.9580
	SIM	0.8895	0.9454	0.920	0.9240	0.9996	0.9606/0.9879
Clown	Correlation	0.9945	0.8328	0.996	0.9503	0.9990	0.9974/0.9566
	SIM	0.8457	0.9235	0.889	0.9804	0.9975	0.9925/0.8459
Boat	Correlation	0.9958	0.8902	0.997	0.9253	0.9999	0.9976/0.9690
	SIM	0.8433	0.9388	0.888	0.9321	0.9997	1.0000/0.8980
Crowd	Correlation	0.9995	0.8977	0.996	0.9561	0.9995	0.9961/0.9557
	SIM	0.7918	0.8734	0.848	0.8631	0.9927	0.9898/0.9539
Girl	Correlation	0.9963	0.8571	0.997	0.9865	0.9987	0.9965/0.9516
	SIM	0.8509	0.9105	0.886	0.9530	0.9743	0.9890/0.9539

4.1 Cropping Attack

To perform this attack, the composite image was cropped in different proportions. Cropped composite images of Lena are shown in Fig. 5(a)-5(c). In the extraction process, the cropped part of an image pixel values were replaced by zero values. Fig. 5(d) is the extracted secret data. If we cropped the image from center as shown in Fig. 5(b), the secret data can still be extracted in visual condition with correlation 0.8102 and SIM 0.7352.

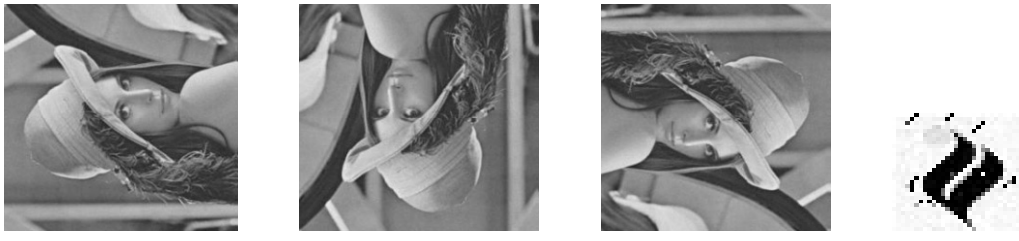


(a) (b) (c) (d)

Fig. 5. (a-c) Cropped composite images. (d) Extracted secret data after cropping.

4.2 Rotation Attack

It is among the most popular kinds of geometrical attack on digital multimedia images. The composite image is rotated and then rotated back to their original position using bilinear interpolation. Different levels of rotations have been implemented. First the composite image is being rotated by 90˚, 180˚ and 270˚ in counter clock wise direction. The composite image after rotation attack has been shown in Fig. 6(a)-(c) and extracted secret data is shown in Fig. 6(d), which is visually good. The proposed algorithm is also robust against rotation with the rotation angle between 0˚-10˚ and between 85˚-100˚. The extracted secret data is highly similar and correlated with original secret data underperforming rotation attacks.



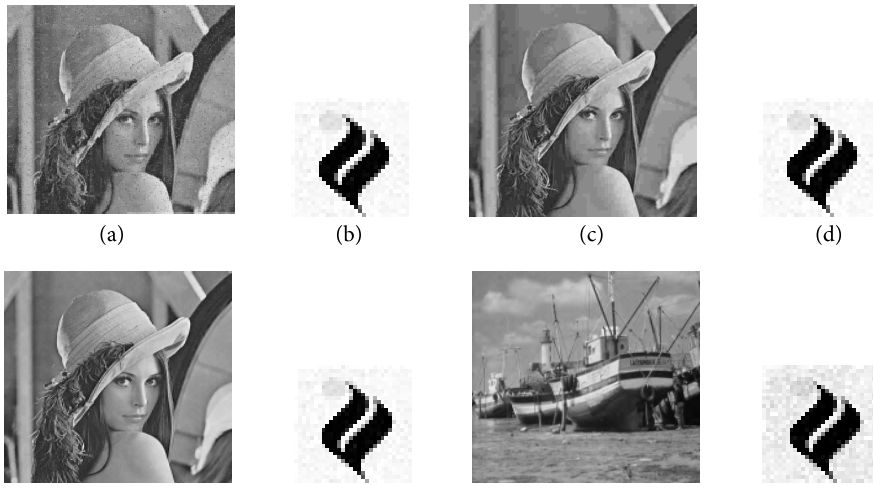
(a) (b) (c) (d)

Fig. 6. Rotation attack. (a) Composite image after 90˚ rotation. (b) Composite image after 180˚ rotation. (c) Composite image after 270˚ rotation. (d) Extracted secret data after rotation attack.

4.3 Gaussian Filter Attack

In this attack, Gaussian filter is added in the composite image. Maximum correlation between extracted and original secret data is 0.9990 and minimum is 0.9945. Maximum SIM between extracted and original secret data is 0.9990 and minimum is 0.7918. This indicates that proposed algorithm is

robust to filter attack. Composite image after filter attack is shown in Fig. 7(a) and extracted secret data from this is shown in Fig. 7(b), which is visually good.



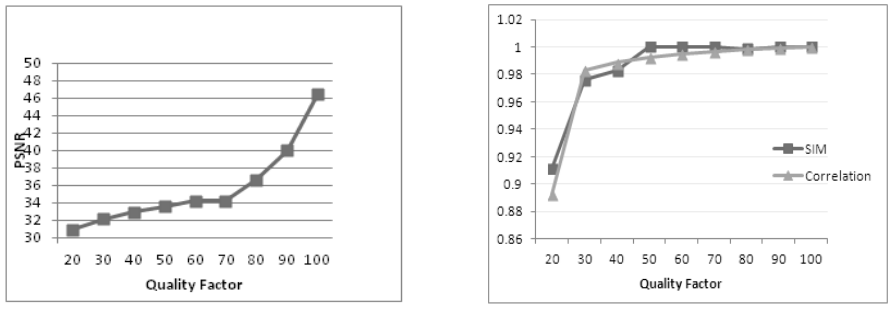
(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 7. (a) Composite image after Gaussian filter attack. (b) Extracted secret data after Gaussian filter attack. (c) Composite image after JPEG compression at QF=20. (d) Extracted secret data after JPEG compression. (e) Composite image after blurring. (f) Extracted secret data after blurring attack. (g) Compressed composite image using JPEG2000. (h) Extracted secret data after JPEG2000 compression.

4.4 JPEG Compression Attack

In this attack, corresponding composite images are compressed with various QF values. Fig. 8(a) shows the PSNR of Lena composite image against different QF of JPEG compression and that depicts that the composite image is imperceptible at all QF as PSNR is above 30 dB [15]. Fig. 8(b) shows the correlation, SIM against different QF of JPEG compression, that shows the robustness of proposed algorithm as SIM and correlation is greater than 0.9. From the result, one can analyze that the proposed algorithm is robust against JPEG compression. The extracted secret data is highly similar and correlated with original secret data under different QF. Composite image after JPEG compression attack is shown in Fig. 7(c) and extracted secret data from this is shown in Fig. 7(d), which is visually good.



(a) (b)

Fig. 8. (a) PSNR vs. quality factor of composite Lena image. (b) SIM, correlation of extracted secret data from Lena image vs. quality factor of JPEG compression.

4.5 Salt and Pepper Noise Attack

The salt and pepper noise attack is also performed on the composite images. Maximum correlation between extracted and original secret data is 0.9564 and minimum is 0.8328. Maximum SIM between extracted and original secret data is 0.9512 and minimum is 0.8901. This shows that the proposed algorithm can also tolerate the salt and pepper noise attack.

4.6 Blurring Attack

The blurring attack is performed on the composite images. Maximum correlation between extracted and original secret data is 0.9972 and minimum is 0.9890. Maximum SIM between extracted and original secret data is 0.9206 and minimum is 0.8486. This indicates that the proposed algorithm can also tolerate the blur attack. Composite image after blur attack is shown in Fig. 7(e) and extracted secret data from this is shown in Fig. 7(f), which is visually good. SIM of the extracted secret data from blurred Lena composite image using proposed algorithm is 0.9036 which is higher than 0.615 SIM of Lee et al. [7] algorithm.

4.7 JPEG2000 Compression Attack

All composite images have been compressed at different bit rates using Jasper tool [16] and then secret data is extracted from these images. The extracted secret data is shown in Fig. 7(h) and compressed composite image using JPEG2000 is shown in Fig. 7(g). PSNR, SIM and correlation are shown in Table 4. The PSNR comparison between cover image and compressed cover image; cover image and compressed composite image at different bit rates is shown in this table. From this comparison, one can conclude that maximum degrade in PSNR is 4.1757 dB and minimum degrade in PSNR is 2.7002 at 4 bpp; and maximum degrade in PSNR is 4.0277 dB and minimum degrade in PSNR is 1.0208 at 2 bpp; and maximum degrade in PSNR is 4.81 dB and minimum degrade in PSNR is 0.1164 at 1 bpp. PSNR is higher than 30 dB which shows that composite image still has good visual quality after JPEG2000 attack and hence imperceptibility is maintained [15]. The correlation and SIM found at different bit rates are highly correlated and similar, which confirms the robustness of the proposed algorithm.

Table 5 shows the comparison of PSNR, correlation and SIM of proposed algorithm with existing algorithms when secret data is extracted without any attack from composite Lena image. One can observe that correlation and SIM of proposed algorithm is equivalent to the existing algorithms and PSNR of proposed algorithm is more than existing algorithms.

Table 6 shows the performance comparison of proposed algorithm with the existing methods in terms of correlation coefficient. For these comparisons, Lena composite image is considered and different types of attacks are performed. After attacks, correlation is calculated. This comparison shows that performance of the proposed algorithm in terms of correlation is better than the existing algorithms [10].

The comparison of PSNR and embedding capacity between existing algorithms and proposed algorithm is shown in Table 7. For this comparison, secret data is embedded into 5^{th} and 4^{th} level wavelet subbands of

cover image. The embedding capacity of proposed algorithm is about seven times higher than Honsinger, Macq, Fridrich, Vleeschouwer algorithms, 1.5 times higher than Zeng and nine times higher than that of Ni et al. [13]. PSNR of proposed algorithm is 6.61 dB and 9.96 dB higher than that of Ni et al. [13] and Hwang et al. [11], respectively and the visual quality of the composite image produced using proposed algorithm is also good. From the comparisons with the existing algorithms, one can observe that proposed algorithm has achieved highest PSNR with large data embedding capacity.

Table 4. Comparison of $PSNR^1$, $PSNR^2$, Correlation and SIM of different images after JPEG2000 attack

Images	Bit rate (bpp)	$PSNR^1$	$PSNR^2$	Correlation	SIM
Lena	4	46.9320	44.2235	0.9995	0.9490
	2	45.5492	41.5215	0.9980	0.9920
	1	41.5237	36.7137	0.9963	0.9797
Barbara	4	47.2971	43.2318	0.9997	0.9528
	2	43.0483	41.9890	0.9980	0.9947
	1	36.1403	35.6219	0.9938	1.0000
Baboon	4	46.8460	43.0117	0.9996	0.9606
	2	37.7235	37.2237	0.9942	0.9907
	1	30.8259	30.7095	0.9816	1.0000
Pepper	4	46.0999	42.2974	0.9996	0.9606
	2	40.6025	39.1102	0.9980	0.9919
	1	35.3282	34.7798	0.9930	1.0000
Clown	4	47.4269	43.3002	0.9996	0.9517
	2	41.9438	40.9230	0.9993	0.9875
	1	38.7655	36.7098	0.9974	0.9884
Crowd	4	47.4680	43.2923	0.9992	0.9456
	2	45.5953	42.3079	0.9988	0.9843
	1	38.7494	37.8622	0.9919	0.9676
Girl	4	45.5409	41.7606	0.9987	0.9256
	2	44.7313	41.1646	0.9983	0.9670
	1	40.5289	38.9573	0.9973	0.9591

$PSNR^1$ between cover image and compressed cover image without embedding using JPEG2000 compression
$PSNR^2$ between cover image and compressed composite image using JPEG2000 compression.

Table 5. Comparison of PSNR, correlation and SIM, extracted secret data (32×32 bytes) without any attack on Lena image

Method	PSNR (dB)	Correlation	SIM
Ramanjaneyulu and Rajarajeswari [10]	40.182	1.00	1.00
Hsieh et al. [5]	44.200	1.00	0.982
Huang and Yang [6]	52.630	1.00	-
Proposed	53.972	0.999	1.00

Table 6. Comparison of correlation of proposed algorithm with existing algorithms

Attack type	Li[a]	Lien[a]	Lin[a]	Algorithm [10]	Proposed algorithm
Blur	-	-	-	-	0.99
Gaussian filter (3×3) variance=0.5	0.7	0.84	0.96	0.98	0.99
Median filter (3×3)	0.35	0.79	0.92	0.91	0.99
Median filter (4×4)	0.26	0.51	0.75	0.64	0.74
Average filter (3×3)	-	-	-	0.80	0.98
Salt and pepper noise (0.001)	-	-	-	0.94	0.94
Rotation (0.25°)	0.46	0.53	0.61	0.88	0.91
Rotation (0.75°)	0.36	0.16	0.34	0.87	0.92
Rotation (1°)	0.33	0.07	0.27	0.86	0.90
Rotation (5°)	-	-	-	0.80	0.90
Rotation (30°)	-	-	-	0.57	0.58
JPEG (QF=30)	0.35	0.79	0.81	0.92	0.94
JPEG (QF=50)	0.52	0.89	1	1	0.99
JPEG (QF=70)	0.63	0.97	1	1	1

[a] Data from Ramanjaneyulu and Rajarajeswari [10].

Table 7. Comparison of PSNR and embedding capacity of proposed algorithm with existing algorithms

Method	Lena (512×512)		Baboon (512×512)	
	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)
Honsinger[a]	<1024	Not Mentioned	<1024	Not Mentioned
Macq and Deweyand[a]	<1024	Not Mentioned	<1024	Not Mentioned
Fridrich[a]	1024	Not Mentioned	1024	Not Mentioned
Vleeschouwer[a]	1024	30	1024	29
Ni et al. [12]	5460	48.2	5421	48.2
Ni et al. [13]	792	40.2	585	38.7
Zeng et al. [14]	4096	37.16	2000	37.21
Hwang et al. [11]	5336	44.53	5328	48.22
Proposed	7200 5460	46.81 49.25	7200 5421	46.86 49.24

[a] Data from Ni et al. [12].

5. Conclusion

A robust data hiding technique for digital images has been proposed in this work. To secure the secret data, it is scrambled using Arnold transform before embedded into the cover image. The secret data is embedded into significant wavelet coefficients of the subbands of a cover image. Robustness of algorithm is tested against different type of attacks, like cropping, blur, Gaussian filter, JPEG2000 and JPEG compression. PSNR of the proposed algorithm for Lena image with embedding capacity of 5460 bits is 1.05 dB higher than the PSNR of Ni et al. [12]. algorithm. Comparison with the existing algorithms demonstrates that proposed algorithm provides equivalent SIM and correlation between the original and extracted secret data and more PSNR than the existing algorithms.

References

[1] W. R. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," in *Proceedings of SPIE 2420: Storage and Retrieval of Image and Video Database III*. Bellingham, WA: International Society for Optics and Photonics, 1995.

[2] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data embedding and watermarking technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064-1087, 1998.

[3] Z. H. Wei, P. Qin, and Y. Q. Fu, "Perceptual digital watermark of images using wavelet transform," *IEEE Transactions on Consumer Electronics*, vol. 44, no. 4, pp. 1267-1272, 1998.

[4] N. Kaewkamnerd and K. R. Rao, "Wavelet based image adaptive watermarking scheme," *Electronics Letters*, vol. 36, no. 4, pp. 312-313, 2000.

[5] M. S. Hsieh, D. C. Tseng, and Y. H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Transactions on Industrial Electronics*, vol. 48, no. 5, pp. 875-882, 2001.

[6] J. Huang and C. Yang, "Image digital watermarking algorithm using multiresolution wavelet transform," in *Proceedings of 2004 IEEE International Conference on Systems, Man and Cybernetics*, Hague, Netherlands, 2004, pp. 2977-2982.

[7] K. H. Lee, Y. H. Kim, and T. H. Yi, "A robust pattern digital watermarking method using wavelet transform," *Journal of Korea Multimedia Society*, vol. 7, no. 1, pp. 98-105, 2004.

[8] H. Wang and N. Li, "An algorithm of digital image watermark based on multiresolution wavelet analysis," in *Proceedings of 2005 IEEE International Workshop on VLSI Design and Video Technology,* Suxhou, China, 2005, pp. 272-275.

[9] M. Shinohara, F. Motoyoshi, O. Uchida, and S. Nakanishi, "Wavelet-based robust digital watermarking considering human visual system," in *Proceedings of the 2007 WSEAS International Conference on Computer Engineering and Applications*, Gold Coast, Australia, 2007, pp. 177-180.

[10] K. Ramanjaneyulu and K. Rajarajeswari, "Wavelet-based oblivious image watermarking scheme using genetic algorithm," *IET Image Processing*, vol. 6, no. 4, pp. 364-373, 2012.

[11] J. Hwang, J. Kim, and J. Choi, "A reversible watermarking based on histogram shifting," in *Digital Watermarking*. Heidelberg: Springer, 2006, pp. 348-361.

[12] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, 2006.

[13] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, "Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18, no. 4, pp. 497-509, 2008.

[14] X. T. Zeng, X. Z. Pan, and Z. Li, "Robust lossless data hiding scheme," *Journal of Zhejiang University Science C*, vol. 11, no. 2, pp. 101-110, 2010.

[15] M. S. Hsieh, "A robust image authentication method based on wavelet transform and Teager energy operator," *International Journal of Multimedia and Its Applications*, vol. 2, no. 3, pp. 1-17, 2010.

[16] M. D. Adams, "JasPer software reference manual," 2001; http://iie.fing.edu.uy/ense/asign/codif/material/laboratorio/jpeg_2000/doc/jasper.pdf.

Geeta Kasana

She received M.C.A. degree from Department of Computer Science, Mysore University, Karnataka in 2000. She has more than 14 years of teaching and research experience. Since May 2008, she is working with Thapar University, Patiala, as a faculty member. Currently, she is pursuing Ph.D. from Computer Science and Engineering Department, Thapar University. Her research interest includes watermarking, cryptography and steganography.

Kulbir Singh

He received his B.Tech. degree in 1997 from PTU, Jalandhar. He received his M.E. and Ph.D. degrees from Thapar University, Patiala, in 2000 and 2006, respectively. He has published more than 72 research papers in national and international journals/conference proceedings. He is a recipient of the Best Paper Award of the IETE Journal of Education for the year 2008. His research interests include signal processing, image processing, DSP processors based design and fractional transforms.

Satvinder Singh Bhatia

He received M.Sc. and Ph.D. degrees from MDU Rohtak. He has more than 28 years of teaching and research experience and has guided 10 Ph.D. theses. He has published more than 60 papers in in national and international journals/conference proceedings. His current research interests include Fourier Series and Transforms.