

Chapter 5

Steganographic Scheme based on DCT and DWT

So far, different steganographic schemes have been discussed in the spatial domain. Though the schemes exhibit very good embedding capacity and payload, they suffer from attacks like jpeg compression, rotation, and scaling, etc. Steganography in the transform domain may help to improve the performance against these attacks. In this chapter, two different schemes in transform domain have been designed, so that the stego image can sustain such attacks to some extent. The schemes have been proved to be suitable for highly compressed images also.

In the first approach, a secured stenographic scheme using the weighted matrix in the Discrete Cosine Transform (DCT) domain has been designed for the highly compressed images. The scheme is secured for employing a secret key of 512 through SHA-512. The PSNR is reasonable and higher than 40 dB when QF is around 80. Surprisingly, around 36 dB PSNR is achieved even when QF is approximately 40. In this connection, it can be claimed that the scheme is better than existing state-of-the-art methods when highly compressed images are used for data communication in real life. Another achievement of the proposed scheme is security because the coefficient value of DCT is increased or decreased instead of embedding actual secret data in the stego image. Again, in this scheme, it is possible to hide more secret bits by changing only one bit in a block of DCT coefficients using the weighted matrix. For this reason, the scheme is recommended for use with highly compressed images (QF 40) for secret data communication as the images have a fewer number of coefficients available for data embedding.

In the second approach, a DWT-based stenographic scheme has been developed. The main objective is to maintain a good trade-off between imperceptibility and payload. DWT and DCT coefficients are very sensitive. A small change in the coefficients introduces large distortion to the stego image. Use of weighted matrix permits to change the least number of coefficients to embed multiple secret bits. This increases the visual quality and imperceptibility along with good embedding capacity. The experimental results clearly show that the proposed scheme generates better stego image in terms of PSNR (55 dB) and SSIM (0.9950). The proposed scheme does not require the original cover image to extract the secret image. Moreover, the unknown weighted matrix acts as a secret key and hence it increases the security of the scheme. The results of the proposed scheme are compared with other relevant techniques, and it has been observed that the proposed scheme outperforms other existing techniques in many ways.

5.1 Steganographic Scheme Using DCT (SSDCT)

Due to rapid growth of the internet technology and the advent of various image processing tools, people started using digital media for hidden communication to protect valuable information on multimedia commercials, health-care, medical, and defense applications etc. On the other hand, image authentication and tamper detection are essential, especially when it is utilized for evidence of legal action. Here, a weighted matrix based steganographic scheme (SSDCT) through Discrete Cosine Transform (DCT) has been designed for highly compressed JPEG color image to maintain a good balance between payload and imperceptibility. Here, the AC components are collected from (8×8) quantized DCT coefficient matrices of YCbCr channel. Then, a series of (3×3) original matrices are formed to hide secret data. The collection of AC components are controlled by 128 bits shared secret key. A predetermined weighted matrix is employed to select the embedding position within a (3×3) coefficient matrix of a cover image through the sum of the entry-wise multiplication operation. The proposed SSDCT scheme provides good embedding capacity with the high visual quality compared to the existing state-of-the-art methods. Finally, different steganographic analysis and attacks are carried out to observe its imperceptibility and robustness.

5.1.1 Data Embedding Procedure

In this section, a novel steganographic technique has been developed based on DCT using a weighted matrix. The detail data embedding process is depicted through a schematic diagram shown in Fig. 5.1. The color cover image (C) is partitioned into three color channel (YCbCr). The DCT coefficient matrix is obtained from each (8×8) image blocks from each YCbCr channel separately. A quantized DCT coefficient is obtained from each block using a pre-determined quantization table. The AC coefficients, except 0, are collected from all (8×8) DCT coefficient matrices and stored into a coefficient array ($DATA[]$). The way of collecting the coefficients from each (8×8) block depends on the 512 shared secret key bits κ . A shared secret key of size 128-bit is used to generate 512 bits binary stream key (κ) using SHA-512. If the κ bit is 1, the coefficients are collected in the zigzag pattern (as shown in Fig. 5.1 (f1)) otherwise the coefficients are collected in reverse zigzag pattern (as shown in Fig. 5.1 (f2)). After the formation of the coefficient array ($DATA[]$), a series of (3×3) matrices ($DATA_MATRIX$) are

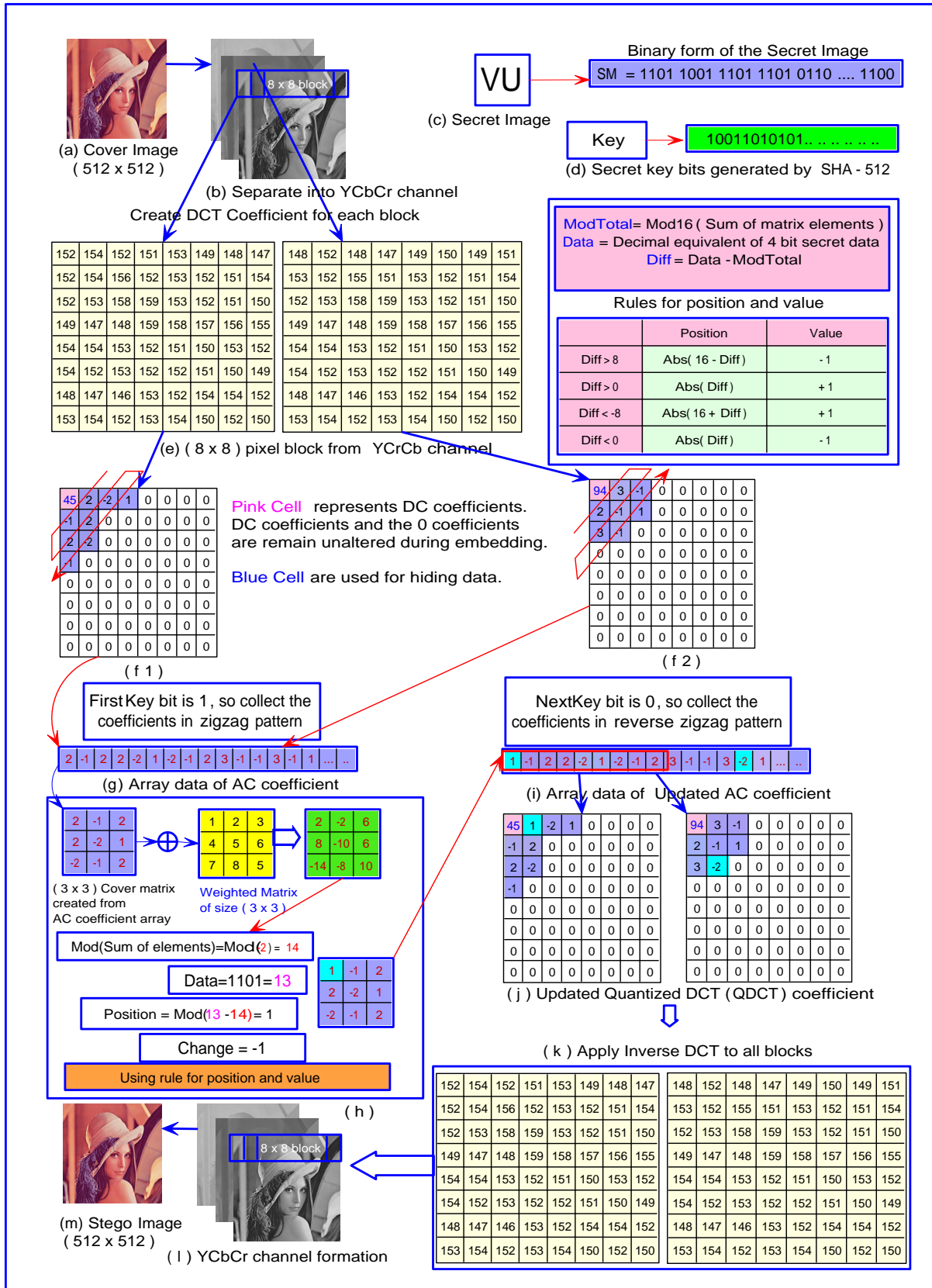


Figure 5.1: Schematic diagram of data embedding process in SSDCT

Algorithm 5.1: SSDCT: Embedding Algorithm

input : Cover image (C) ($m \times n$), Secret image(S), weighted matrix (WM) and a shared secret key (κ)
output: Stego image (SI)

Step-1: Separate color blocks (YCbCr) and partition cover image C into (8×8) pixel blocks
Step-2: Apply DCT to all (8×8) pixel blocks to get DCT coefficient matrix
Step-3: Get quantized DCT matrix from the DCT matrix
Step-4: Create 512 bits binary stream key κ from shared secret key using SHA-512
Step-5: Generate binary *secretData* from secret image (logo)
Step-6: Create an arrays **DATA[]** from the DCT coefficients.

for *detBlock*=1 to $(M \times N)/64$ **do**

- (a) Skip DC coefficient and 0 AC coefficient;
- (b)
 - if** κ bit is 0 **then**
 - Add dct values to **DATA[]** in **clockwise** pattern;
 - else if** κ bit is 1 **then**
 - Add dct values to **DATA[]** in **anticlockwise** pattern;

Step-7: Form a series of (3×3) matrix **DATA_MATRIX** from **DATA[]** array

Step-8:

- (a) Consider a **DATA_MATRIX**;
- (b) **MATRIX** = **DATA_MATRIX** elementary multiplication with Weight Matrix (WM);
- (c) total = SUM of elements in **MATRIX**;
- (d) modTotal=Mod(total,16);
- (e) Get 4 bits secret data from *secretData* and convert it to its decimal equivalent;
 data4Bit=Bin2Dec(4 bits data from *secretData*);
- (f) Get the difference;;
 diff=data4Bit - modTotal;
- (g) Apply following rules to get the position in the matrix where the data will be embedded. As (3×3) weighted matrix is used which can only hide 3 bits secret data in (3×3) DCT block. To embed 4bits secret data in the (3×3) DCT block, the following rules are used [99]. ;

if (*diff*>8) **then**

- diff=16-diff;
- pos = Abs(diff);
- sign=-1;

else if (*diff*>0) **then**

- pos = Abs(diff);
- sign=+1;

else if (*diff*<-8) **then**

- diff=16+diff;
- pos = Abs(diff);
- sign=+1;

else if (*diff*<0) **then**

- pos = Abs(diff);
- sign=-1;

h If *diff* is 0, then no change is done in the **DATA_MATRIX**, otherwise change the value in the position *pos* using *sign* value;

if (*diff* = 0) **then**

- No Change in **DATA_MATRIX**;

else

- DATA_MATRIX**[*pos*] = **DATA_MATRIX**[*pos*] + *sign*;

Step-9: Repeat Step-8 for the rest of the **DATA_MATRIX** to embed the *secretData*;

Step-10:From all modified **DATA_MATRIX**, form a new **DATA[]** array

Step-11:Using this new **DATA[]** array, reconstruct the quantized DCT matrices

Step-12:Apply Inverse DCT and generate the Stego image SI

considered. Then, an entry-wise multiplication operation is performed between the predefined weighted matrix and the *DATA_MATRIX*. Secret data bits, collected from a secret logo image, are embedded by increasing or decreasing the coefficient value at a particular position *POS* of the *DATA_MATRIX*. The *POS* is calculated by the modulo-16 operation on the difference between secret data and the sum of entry-wise multiplication value, depicted in Fig. 5.1

(h). The rules for position and value in Fig. 5.1 describes the position change and value change in the *DATA_MATRIX*. The process is continued for the rest of the *DATA_MATRIX* to embed maximum secret data bits. Then, coefficient array (*DATA*[]) is reconstructed by collecting all modified *DATA_MATRIX* (Fig. 5.1 (i)). After that, a new (8×8) quantized DCT matrices are formed using the (*DATA*[]) array (Fig. 5.1 (j)). Applying inverse quantization and inverse DCT, all (8×8) stego pixel blocks are acquired. Then, the pixel blocks are converted into YCbCr channel and, finally, the stego image is generated (Fig. 5.1 (m)). A step by step embedding procedure is presented in Algorithm 5.1.

5.1.2 Data Extraction Procedure

The detail extraction process of SSDCT scheme is depicted in Fig. 5.2 and corresponding step by step extraction procedure is presented in Algorithm 5.2. The stego image (SI) is partitioned into three color channel (YCbCr). Then, the DCT coefficient matrix is obtained from each (8×8) image blocks of each YCbCr channel separately. A quantized DCT coefficient is obtained from each block using a pre-determined quantization table. The AC coefficients, except 0, are collected from all (8×8) DCT coefficient matrices and stored into a coefficient array (*DATA*[]). The way of coefficient collection from each (8×8) block depends on the 512-bit shared secret key κ through SHA-512. The AC coefficients, except 0, are collected from all quantized DCT blocks and stored into a *DATA*[] array. The way of collecting the coefficients from each DCT block depends on the κ bits. If the κ bit is 1, the coefficients are collected in a zigzag pattern (As shown in Fig. 5.2 (d1)) and when the κ bit is 0, the coefficients are collected in reverse zigzag pattern (as shown in Fig. 5.2 (d2)). A series of (3×3) matrices (*DATA_MATRIX*) are formed from *DATA* array. Now, a (3×3) *DATA_MATRIX* is considered and entry-wise multiplication operation is performed with the weighted matrix. The modulo-16 of the sum of elements of the resultant matrix, *modTotal*, is then obtained (as shown in Fig. 5.2 (g)). This *modTotal* is actually the extracted secret data. It is then converted to 4 bits binary string. In this way, 4 bits binary secret data are collected from each (3×3) *DATA_MATRIX* matrices and appended to form the final stream of secret data. Finally, the secret image is formed from the secret data bits.

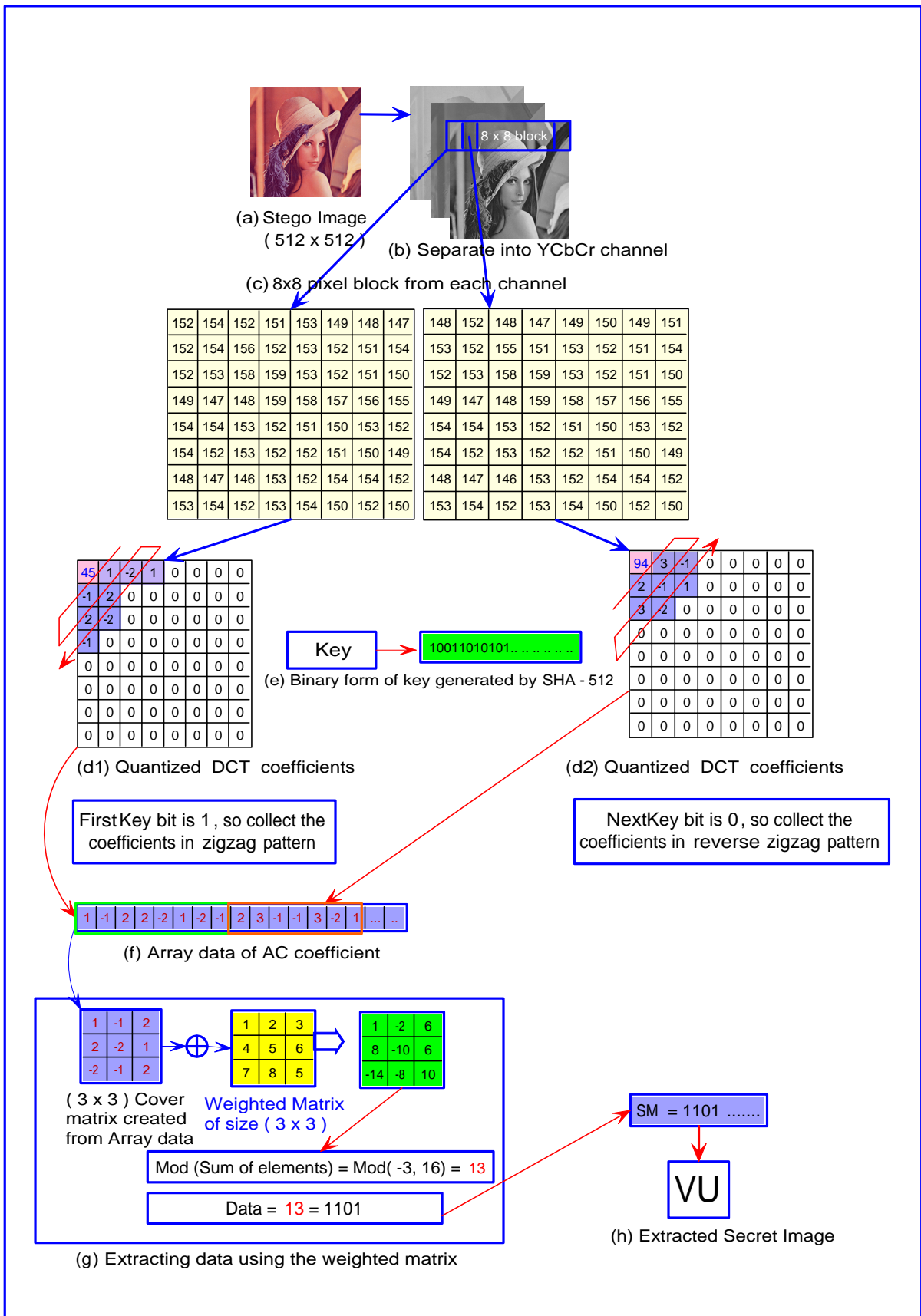


Figure 5.2: Schematic diagram of data extraction process in SSDCT

Algorithm 5.2: SSDCT: Extraction Algorithm

input : Stego image SI ($m \times n$), Weighted Matrix WM and Shared Secret Key κ
output: Secret image S

Step-1: Separate color blocks (YCbCr) and partition stego image SI into (8×8) pixel blocks
Step-2: Apply DCT to all (8×8) pixel blocks to get DCT coefficient matrix
Step-3: Get quantized DCT matrix from the DCT matrix
Step-4: Create 512 bits binary stream **keyData** from secret key κ using SHA-512
Step-5: Create an arrays **DATA**[] from the DCT coefficients.

for $dctBlock=1$ to $(m \times n)/64$ **do**

- (a) Skip DC coefficient and 0 AC coefficient;
- (b)
 - if** *keyData* bit is 0 **then**
 - Add dct values to **DATA**[] in **clockwise** pattern;
 - else if** *keyData* bit is 1 **then**
 - Add dct values to **DATA**[] in **anticlockwise** pattern;

Step-6: Form a series of (3×3) matrix **DATA_MATRIX** from **DATA**[] array
Step-7:

- (a) Take a **DATA_MATRIX**;
- (b) **MATRIX** = **DATA_MATRIX** elementary multiplication with Weight Matrix (WM);
- (c) total = SUM of elements in **MATRIX**;
- (d) modTotal=Mod(total,16);
- (e) Convert the modTotal decimal value to 4 bits binary number **binary4Bit**;
- (f) Add this **binary4Bit** to *secretBits* binary string;

Step-8: Repeat **Step-7** for rest of the **DATA_MATRIX**, extract 4 bits data from them, and add it to *secretBits* binary string;
Step-9: Construct Secret Image (S) from *secretBits* binary string;

5.1.3 Experimental Results and Comparisons

The proposed SSDCT scheme has been tested using some standard benchmark images shown in Fig. 1.1 and evaluated using various evaluation metrics. The experimental results and comparisons are given below:

5.1.3.1 Quality Measurement Analysis

The stego images of SSDCT scheme have been evaluated through some standard steganographic analysis like MSE, PSNR, SSIM, and Q-Index. High PSNR indicates better quality of the stego image. In SSDCT scheme, PSNR around 40 dB is achieved after hiding 1,43,996 bits secret data in a compress JPEG image of QF 80 shown in Table 5.1. The PSNR is around 39 dB and 36 dB when QF are 60, and 40 respectively. The corresponding selected coefficient available for data embedding, number of embedded secret data bits, SSIM and Q-Index are mentioned in Table 5.1 for the compressed image with different QF 90, 80, 60, 40, and 10. It can be observed that the results are very promising even with highly compressed images with QF 40. But when QF is as low as 10 or below, the PSNR is very low i.e. below 30 dB which is not acceptable for steganographic scheme. In the proposed SSDCT scheme, the SSIM is presented in Table 5.1, which is near 0.98 and it indicates good concealment of secret data in the stego image.

The visual distortion in an image is measured by the Q-Index. The range of values for the

Table 5.1: Available coefficient for data embedding, Number of bits embedded, PSNR (dB), SSIM and Q-Index of images at different QF level in SSDCT

Quality Factor (QF)	Images	Available Coefficient	Embedded bits	PSNR	SSIM	Q-Index
90	Lena	86,140	1,80,942	42.1241	0.9814	0.9965
	Airplane	89,456	1,76,541	41.1243	0.9887	0.9965
	Boat	88,653	1,77,546	40.9562	0.9857	0.9657
	Baboon	90,452	1,79,457	41.2354	0.9872	0.9897
	Peppers	89,499	1,79,657	40.1245	0.9879	0.9898
80	Lena	50,997	1,43,996	41.3335	0.9918	0.9979
	Airplane	48,133	1,42,821	40.4062	0.9890	0.9958
	Boat	52,524	1,45,620	40.6683	0.9991	0.9989
	Baboon	51,623	1,44,175	40.9030	0.9890	0.9992
	Peppers	52,503	1,46,758	40.2083	0.9927	0.9898
60	Lena	28,485	88,620	40.1345	0.9827	0.9948
	Airplane	29,688	89,562	38.2136	0.9892	0.9987
	Boat	29,568	88,563	39.7387	0.9887	0.9978
	Baboon	30,857	90,542	40.0230	0.9908	0.9992
	Peppers	29,670	89,224	39.1278	0.9992	0.9867
40	Lena	18,715	58,212	39.6634	0.9884	0.9817
	Airplane	21,140	59,863	38.1423	0.9978	0.9789
	Boat	20,647	58,461	36.2764	0.9885	0.9778
	Baboon	23,287	60,476	36.1532	0.9937	0.9892
	Peppers	19,250	57,632	36.0078	0.9898	0.9827
10	Lena	4,263	5,676	26.7506	0.7785	0.9783
	Airplane	6,045	6,415	27.3460	0.7874	0.9689
	Boat	5,417	6,745	27.3654	0.7642	0.9745
	Baboon	7,621	6,476	25.3641	0.7845	0.9756
	Peppers	4,557	5,632	26.3419	0.7745	0.9745

Q-Index is $[-1, 1]$. The best value 1 is achieved if and only if the images are identical. The Q-Index in SSDCT scheme is nearer to 0.9994, which indicates high imperceptibility of the stego image shown in Table 5.1. SSIM is a parameter for measuring the similarity between original and stego images. Its value lies between -1 to +1 and approaches +1 when two images are identical. The SSIM value for different images at different QF is given in Table 5.1, which shows the better imperceptibility of the stego images.

The SSDCT scheme has been compared with Lin et al. [110], Saidi et al. [52], Wei et al. [111], Rahman et al. [36] and Singh et al. [51] schemes. The comparison results are given in Table 5.2 and in Fig. 5.3. It is observed that SSDCT scheme achieves higher PSNR (40 dB) with highly compressed images carrying more than 50,000 bits. The other existing schemes ([110], [52], [111], [36], [51]) mostly used good quality images which can hide more data because of many non-zero DCT coefficients which depend on the percentage of compression. SSDCT scheme can hide more data than the existing schemes when high-quality images are used. Also,

in the compressed image, SSDCT scheme performs better than those existing schemes. SSDCT scheme has been tested with respect to embedding capacity and PSNR with different QF i.e. 80, 60, and 40 is shown in Fig. 5.4. It is also observed that the PSNR is 41 dB when QF is 80 and 36 dB when QF is 40. So, it can be concluded that for highly compressed image SSDCT scheme performs better due to the use of weighted matrix which can hide 4 bits secret data within the cover image by modifying only 1 bit in the DCT coefficient.

Table 5.2: Comparison of proposed scheme with some state-of-the-art schemes in terms of PSNR (dB) in SSDCT

Cover Image	Lena		Airplane		Boat		Baboon		Pepper	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lin et al. [110]	90,112	35.28	90,112	34.53	90,112	33.05	90,112	28.22	90,112	35.09
Saidi et al. [52]	163,840	36.3762	163,840	36.7870	163,840	34.4317	163,840	26.4209	163,840	35.6165
Wei et al. [111]	64,008	33.971	64,008	31.949	64,008	31.147	64,008	25.995	64,008	33.400
Rahman et al. [36]	...	31.4550	30.0704	...	30.4195	...	30.5127
Singh et al. [51]	...	39.7928	39.9285	...	39.5467	...	40.1907
Chang et al. [42]	53,248	34.84	53,248	39.14	53,248	33.29	53,248	27.63	53,248	31.37
Chang et al. [44]	20,473	32.13	20,472	32.09	20,339	31.76	20,437	29.59	20,479	32.74
SSDCT	52664	41.335	51392	40.4062	52028	40.6683	50008	40.9030	53332	40.2083

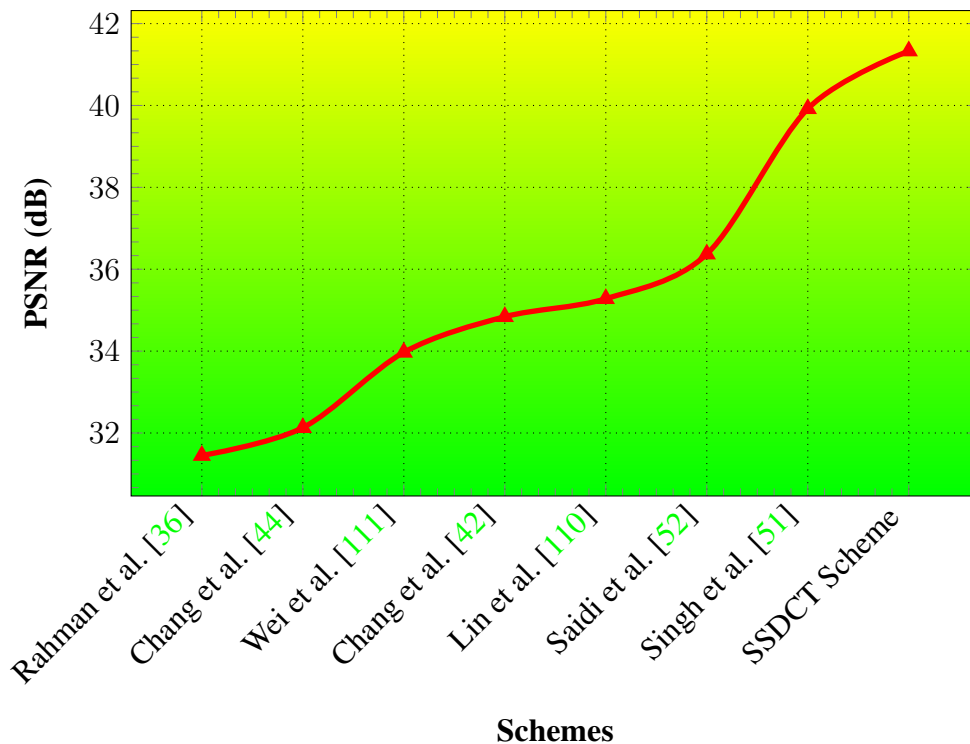


Figure 5.3: Comparison graph with existing DCT based schemes in terms of average PSNR (dB) in SSDCT

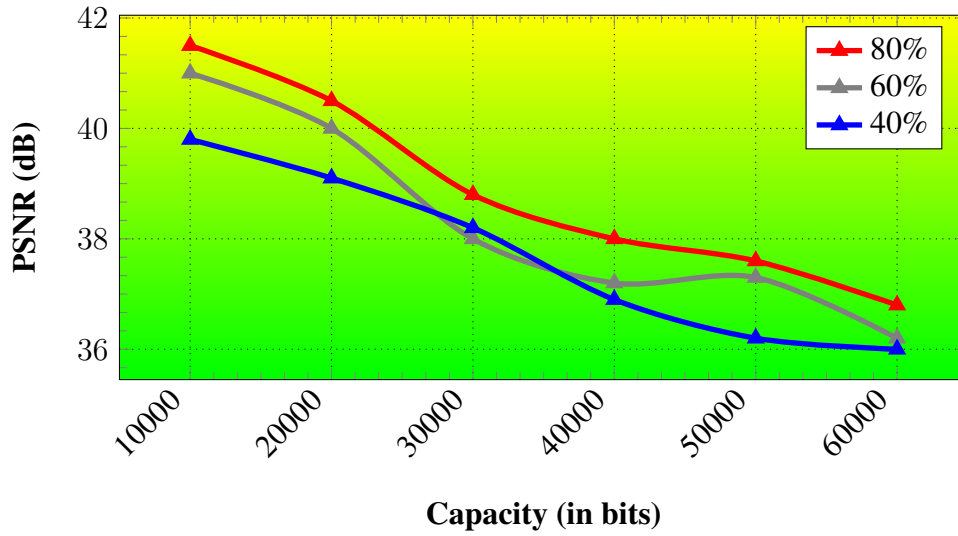


Figure 5.4: Comparison of PSNR (dB) with respect to capacity and different quality factor in SSDCT

5.1.3.2 Robustness Analysis

Table 5.3: Comparison of different evaluation metrics with different benchmark image datasets in SSDCT

Image Dataset	Images	NCC	BER
SIPI [90]	Lena	0.999927	0.019952
	Airplane	0.999475	0.021233
	Boat	0.999871	0.019880
	Baboon	0.999646	0.021256
	Peppers	0.999120	0.018331
UCID [91]	ucid00011	0.999771	0.019966
	ucid00015	0.999786	0.021991
	ucid00062	0.999938	0.031210
	ucid00407	0.999171	0.028161
	ucid00617	0.999234	0.024765



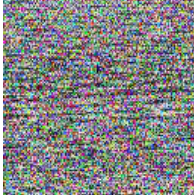
Table 5.4: Results of RS analysis in SSDCT

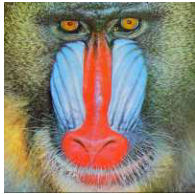

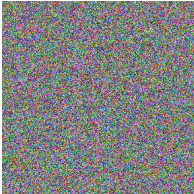
Image Database	No. of images	Stego image				RS value
		R_M	R_{-M}	S_M	S_{-M}	
SIPI	10	24824	25072	12381	12169	0.0123
	25	24832	25108	12401	12112	0.0109
	50	24742	25008	13004	12096	0.0127
UCID	10	42905	42919	3575	3583	0.0105
	25	43004	42017	3648	3698	0.0113
	50	42778	41728	3604	3694	0.0108

The robustness of a steganographic scheme can be analyzed by evaluating the quality metric NCC, BER, and RS-analysis. The NCC of the proposed SSDCT scheme is shown in Table 5.3. It is $0.9999 \approx 1$, which indicates high imperceptibility of the stego image. The BER is defined

as the rate at which errors occur in a transmission system, which can be directly translated into the number of errors that occur in a string of a stated number of bits. BER, as shown in Table 5.3, is 0.019952, which proves very less modification is done in the stego image while embedding secret data. The stego image has been analysed using RS Analysis proposed by Fridrich et al. [41]. Two different sets of images from two image databases are used to perform RS value which is shown in Table 5.4. The scheme has shown a good result when RS Analysis is performed. The average RS value is 0.0160, which is near 0. It indicates that SSDCT scheme has less distortion in the stego image after embedding secret data.

Fig. 5.5 shows separate examples where a wrong weighted matrix and a wrong secret key is

(A) Attack with unknown weighted matrix												
Original Image	Secret Image	Brute force attack	Extracted Secret Image									
		<table border="1"> <tr><td>1</td><td>2</td><td>3</td></tr> <tr><td>4</td><td>5</td><td>6</td></tr> <tr><td>8</td><td>7</td><td>5</td></tr> </table>	1	2	3	4	5	6	8	7	5	
1	2	3										
4	5	6										
8	7	5										
512x512	40x40	Matrix	PSNR= 6.6347(dB)									

(B) Attack with unknown shared secret key			
Original Image	Secret Image	Brute force attack	Extracted Secret Image
		Key = 11010011..	
512x512	40x40	Key	PSNR= 6.2918(dB)




(C) Attack with unknown weighted matrix and unknown shared secret key												
Original Image	Secret Image	Brute Force Attack	Extracted Secret Image									
		<table border="1"> <tr><td>1</td><td>2</td><td>3</td></tr> <tr><td>4</td><td>5</td><td>6</td></tr> <tr><td>8</td><td>7</td><td>5</td></tr> </table> Key = 11010011..	1	2	3	4	5	6	8	7	5	
1	2	3										
4	5	6										
8	7	5										
512x512	40x40	Matrix and Key	PSNR= 5.5143(dB)									

Figure 5.5: Results of brute force attacks with unknown weighted matrix and secret key in SSDCT

used to extract the secret image. According to the result, it is clear that the attacker can only extract a noise-like image after using an invalid weighted matrix or secret key. In this context,

it is clear that the SSDCT steganographic scheme is highly robust. Only a valid shared secret key and valid weighted matrix can extract the secret message from the stego image without encountering any loss of data.

5.2 Steganographic Scheme Combining DWT with DCT (SSDWT)

The main challenge of any image steganographic scheme is to preserve the imperceptibility of the cover image along with undetectability and high embedding capacity. Here, a robust, secure, and imperceptible image steganographic scheme (SSDWT) combining Discrete Wavelet Transform (DWT) with DCT has been proposed. In the proposed approach, a cover image is decomposed into 4 subbands, LL, LH, HL and, HH using DWT. The sub-bands LH, HL, and HH are partitioned into non-overlapping blocks, and DCT is applied to each block. The secret bits from the secret image are embedded into the DCT coefficients with the help of a weight matrix. The purpose of the proposed scheme is to provide less distortion and better undetectability in the final stego image. The SSDWT scheme is tested using various images from some standard image databases. The effects of rotation, compression, and noise have also been investigated on the proposed scheme. Experimental results show better effectiveness of the proposed steganographic scheme with good visual quality and high embedding capacity. The results also demonstrate better robustness of the proposed SSDWT scheme under different image processing attacks compared to some other related existing schemes.

5.2.1 Data Embedding Procedure

In this section, a novel DWT based steganographic technique in combination with DCT has been proposed. The embedding process is illustrated in Fig. 5.6. In the embedding phase, the color cover image (C) is separated into RGB layers. At each layer, DWT is applied and decomposed into four subbands LL, HL, LH, and HH. The secret image (S) is also converted to a secret bitstream. Each subband is partitioned into (4×4) non-overlapping sub-blocks. Then, DCT is applied to each sub-block of HL, LH, and HH subbands separately to get (4×4) non-overlapping DCT coefficient blocks. A weighted matrix of size (4×4) is multiplied with each DCT block to embed 5 bit secret data from secret bitstream of secret image (S). Accordingly, all the DCT blocks of HL, LH, and HH subbands are processed to embed secret data bits. The inverse DCT is then applied to all the blocks of the subbands. Then, inverse DWT is applied to all the subbands. This process is continued for all three layers (R, G, and B) of the color

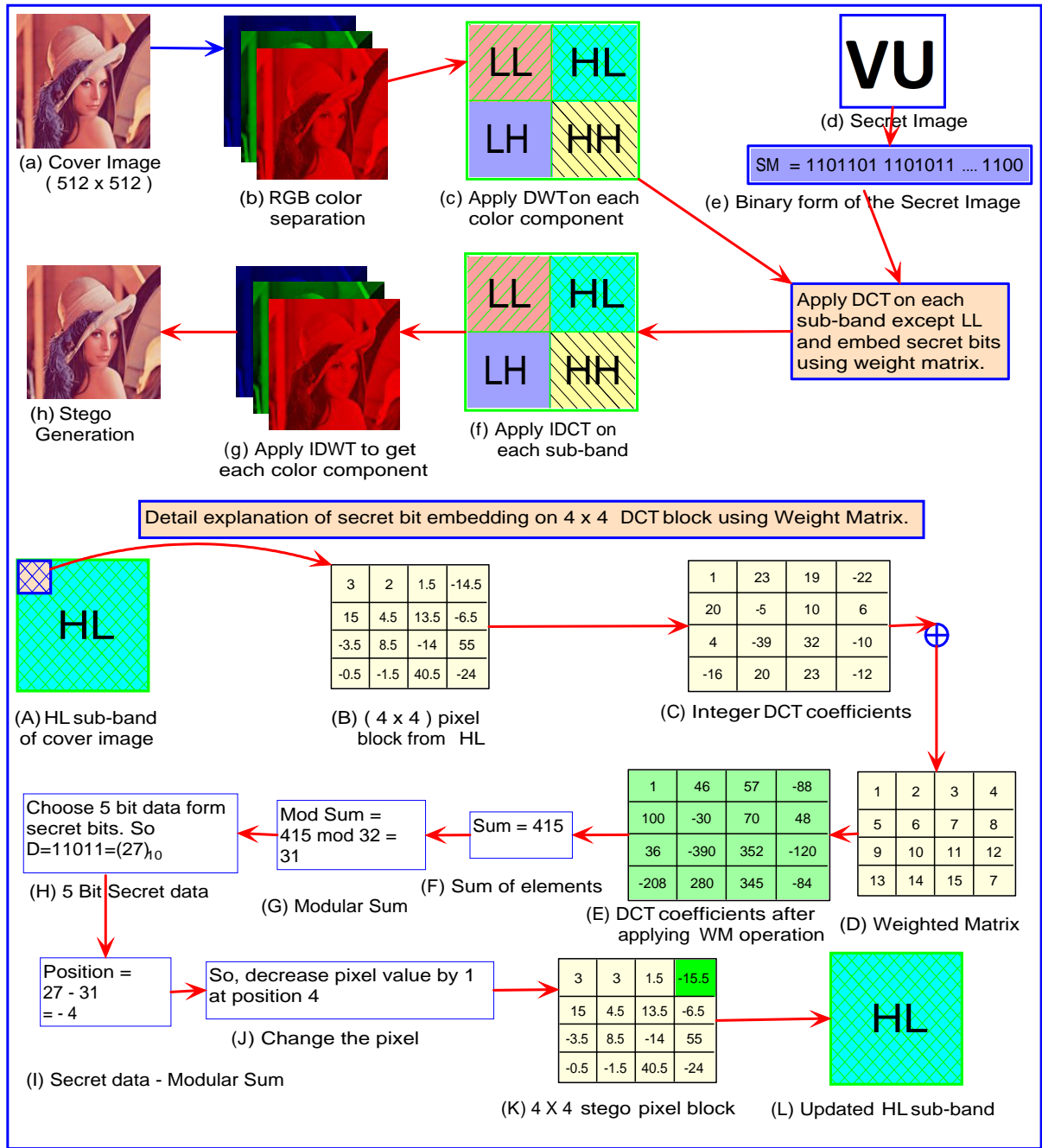


Figure 5.6: Schematic diagram of data embedding process in SSDWT

cover image (C). The stego image (SI) is formed with the three layers. The steps of embedding procedure are described in detail as follows:

Step 1: Decompose the color cover image (C) into RGB layers and then apply DWT to each layer to get four subbands ($C_{LL}, C_{HL}, C_{LH}, C_{HH}$).

Step 2: Generate secret bitstream from the secret image (S).

Step 3: Partition the subbands C_{HL}, C_{LH} , and C_{HH} into (4×4) subblocks and apply DCT to

each subblock to get (4×4) DCT coefficient block.

Step 4: For each (4×4) DCT block $B_{C_{HL}}$ in C_{HL} , an weighted matrix (WM) of size (4×4) is multiplied using entry-wise multiplication.

Step 5: Secret bits are embedded into a (4×4) DCT block by changing the value of the coefficient at a particular position.

Step 6: After applying weighted matrix (WM), this position in a DCT block $B_{C_{HL}}$ is calculated as follows:

$$\left. \begin{aligned} Sum &= \sum_1^{m \times n} B_{C_{HL}} \oplus WM \\ ModularSum &= MOD(Sum, 2^r), \text{ where } r \text{ is the number of bits embedded} \\ P &= r \text{ BitSecretData} - ModularSum \end{aligned} \right\} (5.1)$$

Step 7: The position P in $B_{C_{HL}}$ is changed according to the following rule:

$$\left. \begin{aligned} B_{C_{HL}}[P] &\text{ increased by } 1 \text{ if } P > 0 \\ B_{C_{HL}}[P] &\text{ decreased by } 1 \text{ if } P < 0 \\ B_{C_{HL}}[P] &\text{ is unchanged if } P = 0 \end{aligned} \right\} (5.2)$$

Step 8: This way by changing the coefficient value in the positions P , r bit secret data is embedded in every DCT subblock $B_{C_{HL}}$.

Step 9: After embedding secret bits in the subbands C_{HL} , C_{LH} , and C_{HH} , inverse DCT is applied to the subbands.

Step 10: Then, inverse DWT is applied to the C_{LL} , C_{HL} , C_{LH} , and C_{HH} subbands to get a stego image layer.

Step 11: Step 4: to Step 10: is repeated to embed secret information into all the RGB layers.

Step 12: The stego image (SI) is generated by combining all the RGB layers.

The embedding procedure is presented in the Algorithm 5.3.

Algorithm 5.3: SSDWT: Embedding Algorithm

```

input : Cover image ( $C$ ) ( $m \times n$ ), Secret image( $S$ ), weighted matrix ( $WM$ )
output: Stego image ( $SI$ )

Decompose the cover image ( $C$ ) into RGB layers
Apply DWT to each of the RGB layer separately
Get four sub-bands ( $C_{LL}, C_{HL}, C_{LH}, C_{HH}$ ) from each layer
Generate secret bit stream ( $secretData$ ) from the secret image ( $S$ )
// Process the following operations for each layer
foreach colorLayer in ( $RED, GREEN, BLUE$ ) do
    // Process  $C_{HL}, C_{LH}, C_{HH}$  subbands for each color
    foreach subBand in ( $C_{HL}, C_{LH}, C_{HH}$ ) do
        (a) Partition subBand into ( $4 \times 4$ ) blocks
        (b) Apply DCT to each ( $4 \times 4$ ) block to get the DCT coefficient blocks
        // Each ( $4 \times 4$ ) DCT block is then processed with the following operations
        for dctBlock=1 to  $(m \times n)/4$  do
            (i)  $dctBlock$  is multiplied with an weighted matrix ( $WM$ ) of size ( $4 \times 4$ ) using entry-wise multiplication
            (ii) Extract  $r$  secret bits from the secret bit stream ( $secretData$ )
            (iii) The value of the DCT coefficient at a particular position in the  $dctBlock$  is changed to embed  $r$  secret bits
            (iv) Inverse DCT is applied to the  $dctBlock$ 

Inverse DWT is applied to the  $C_{LL}, C_{HL}, C_{LH}$ , and  $C_{HH}$  subbands to get a stego image layer
The stego image ( $SI$ ) is generated by combining all the RGB layers

```

5.2.2 Data Extraction Procedure

The extraction process of SSDWT scheme is illustrated in Fig. 5.7. In the extraction phase, the stego image (SI) is separated into RGB layers. At each layer, DWT is applied and decomposed into four subbands LL, HL, LH, and HH. After that, the subbands are partitioned into (4×4) non-overlapping blocks. Then, DCT is applied to the blocks to get (4×4) DCT coefficient blocks. The same weighted matrix, used during embedding, is applied to each DCT block. In this way, all the DCT block of HL, LH, and HH subbands are processed to extract the secret data bits. After extracting secret bits from HL, LH, and HH of all RGB layers, the secret image (S) is generated. The steps of extraction procedure are described in detail as follows:

- Step 1: Decompose the stego image (SI) into RGB layers. Apply DWT to each layer to get four subbands ($SI_{LL}, SI_{HL}, SI_{LH}, SI_{HH}$).
- Step 2: Partition each subband SI_{HL}, SI_{LH} , and SI_{HH} into (4×4) non-overlapping blocks.
- Step 3: Apply DCT to each (4×4) block to get (4×4) DCT coefficient block.
- Step 4: The same weighted matrix (WM), used during embedding, is applied to each (4×4) DCT coefficient block $B_{SI_{HL}}$ in SI_{HL} .
- Step 5: After applying weighted matrix, r bit secret data is extracted from each block $B_{SI_{HL}}$ as

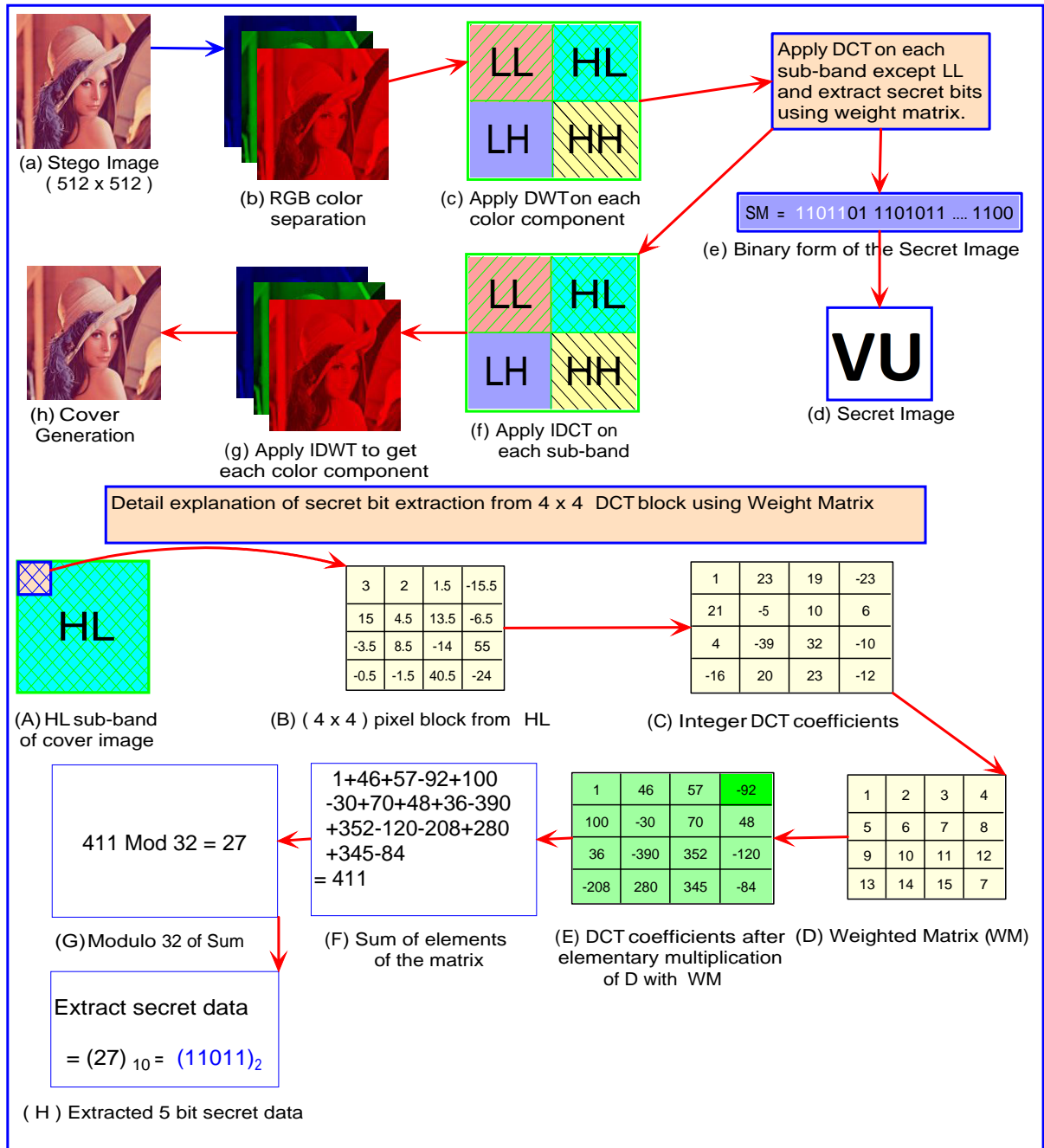


Figure 5.7: Schematic diagram of data extraction process in SSDWT

follows:

$$\left. \begin{aligned} Sum &= \sum_1^{m \times n} B_{SI_{HL}} \oplus WM \\ Data &= MOD(Sum, 2^r), \text{ where } r \text{ is the number of bits extracted} \end{aligned} \right\} (5.3)$$

Step 6: The *Data* is converted to *r* bit binary number. This is actually the extracted bits from the DCT coefficient block.

Step 7: The secret bits are extracted from all the DCT blocks of the subbands SI_{HL} , SI_{LH} , and

SI_{HH} .

Step 8: [Step 3:](#) to [Step 7:](#) is repeated for Red, Green, and Blue layers to collect all the secret bits.

Step 9: The secret image is then formed from the collected secret data.

The extraction procedure is presented in the Algorithm 5.4.

Algorithm 5.4: SSDWT: Extraction Algorithm

```

input : Stego image (SI), Weighted Matrix (WM)
output: Secret image (S)

Decompose the stego image (SI) into RGB layers
Apply DWT to each of the RGB layer separately
Get four sub-bands ( $C_{LL}, C_{HL}, C_{LH}, C_{HH}$ ) from each layer
// Process the following operations for each layer
foreach colorLayer in (RED, GREEN, BLUE) do
    // Process  $C_{HL}, C_{LH}, C_{HH}$  subbands for each color
    foreach subBand in ( $C_{HL}, C_{LH}, C_{HH}$ ) do
        (a) Partition subBand into  $(4 \times 4)$  blocks
        (b) Apply DCT to each  $(4 \times 4)$  block to get the DCT coefficient blocks
        // Each  $(4 \times 4)$  DCT block is then processed with the following operations
        for dctBlock=1 to  $(m \times n)/4$  do
            (i)  $dctBlock$  is multiplied with the same weighted matrix (WM) of size  $(4 \times 4)$  using entry-wise multiplication
            (ii) Sum of the elements (SUM) of the resultant matrix is calculated
            (iii) Using modulo operation on the SUM,  $r$  bit secret data is extracted
    
```

Secret image (S) is then formed from all the collected secret data from all layers

5.2.3 Experimental Results and Comparisons

The SSDWT scheme is tested using standard benchmark images shown in Fig. 1.1 and evaluated using various evaluation metrics. The experimental results and comparisons are given below:

5.2.3.1 Quality Measurement Analysis

The stego image of SSDWT scheme has been evaluated through some standard analysis like MSE, PSNR, SSIM, and Q-Index. High PSNR represents better quality of the stego image. In SSDWT scheme, PSNR around 55 dB is achieved after hiding around 60,440 bits in a cover image of size (512×512) . SSDWT scheme has been compared with Abdelwahab et al. [57], Kumar et al. [58], Acharya et al. [59], Baby et al. [60], Kumar et al. [62], and Atawneh et al. [61] schemes. The comparison results are given in Table 5.5. It is observed that the proposed SSDWT scheme achieves higher PSNR (55 dB) with high embedding capacity and good visual quality compared to the other existing schemes. The PSNR comparison graph is shown in Fig. 5.8 and the SSIM comparison graph is shown in Fig. 5.9.

The proposed SSDWT scheme has been compared with some DCT based schemes like Lin et

al. [110], Saidi et al. [52], Wei et al. [111], Rahman et al. [36], Chang et al. [42], Singh et al. [51], Chang et al. [44] schemes to show that the proposed scheme has higher PSNR than these schemes. The comparison result is shown in Table 5.6. Q-Index is used to measure

Table 5.5: Comparison of proposed scheme with some existing schemes in terms of PSNR (dB) and SSIM in SSDWT

Image	Lenna		Barbara		Goldhill		Bird		Raman	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Abdelwahab et al. [57]	19.66	0.8683	17.67	0.8754	11.16	0.8745	12.91	0.8798	12.91	0.8719
Kumar et al. [58]	41.93	0.9327	41.03	0.9421	42.84	0.9317	42.71	0.9389	42.54	0.9434
Acharya et al. [59]	42.00	0.9364	41.97	0.9443	41.78	0.9490	42.63	0.9482	43.06	0.9451
Baby et al. [60]	42.09	0.9483	42.74	0.9568	41.95	0.9585	42.76	0.9521	43.21	0.9529
Kumar et al. [62]	44.84	0.9572	44.25	0.9845	43.22	0.9826	45.12	0.987	45.23	0.9839
Atawneh et al. [61]	49.13	0.9861	49.09	0.9859	49.10	0.9856	49.13	0.9862	49.11	0.9845
SSDWT	55.32	0.9947	55.53	0.9983	55.46	0.9963	55.82	0.9987	54.98	0.9937

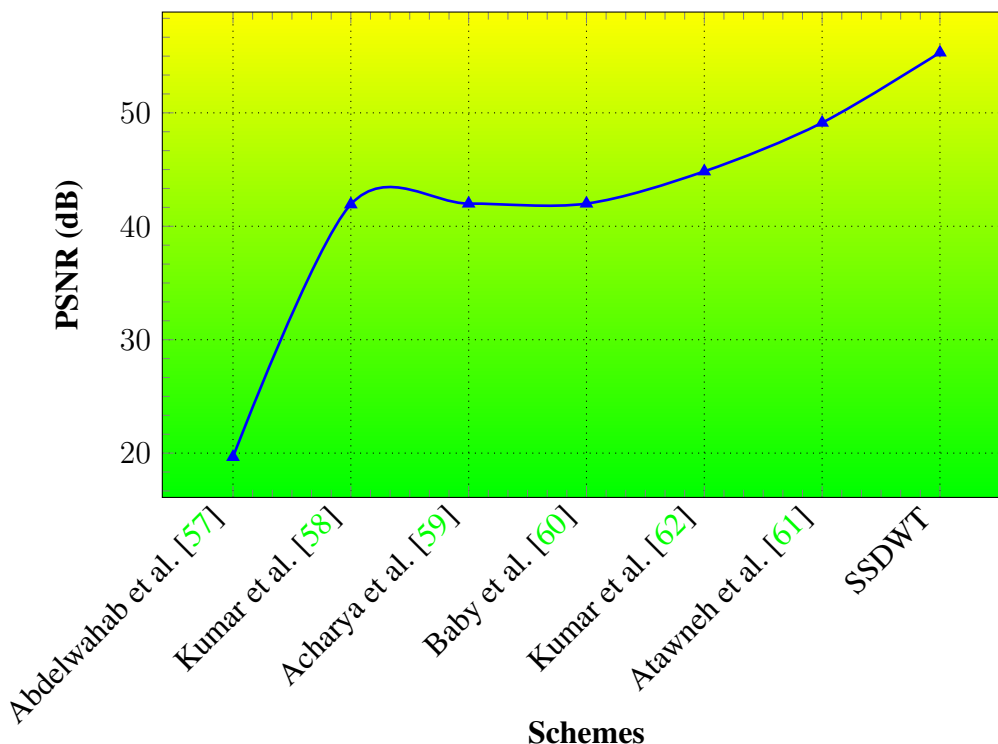


Figure 5.8: Comparison graph of SSDWT with existing DWT based schemes in terms of average PSNR (dB)

the distortion in an image. The Q-Index in SSDWT scheme is near 0.9999. It indicates that the imperceptibility of the stego images generated by the proposed scheme is high, as shown in Table 5.7. The similarity between the two images is measured by SSIM. Its value ranges between -1 and +1. When the images are identical, SSIM value approaches to +1. In the

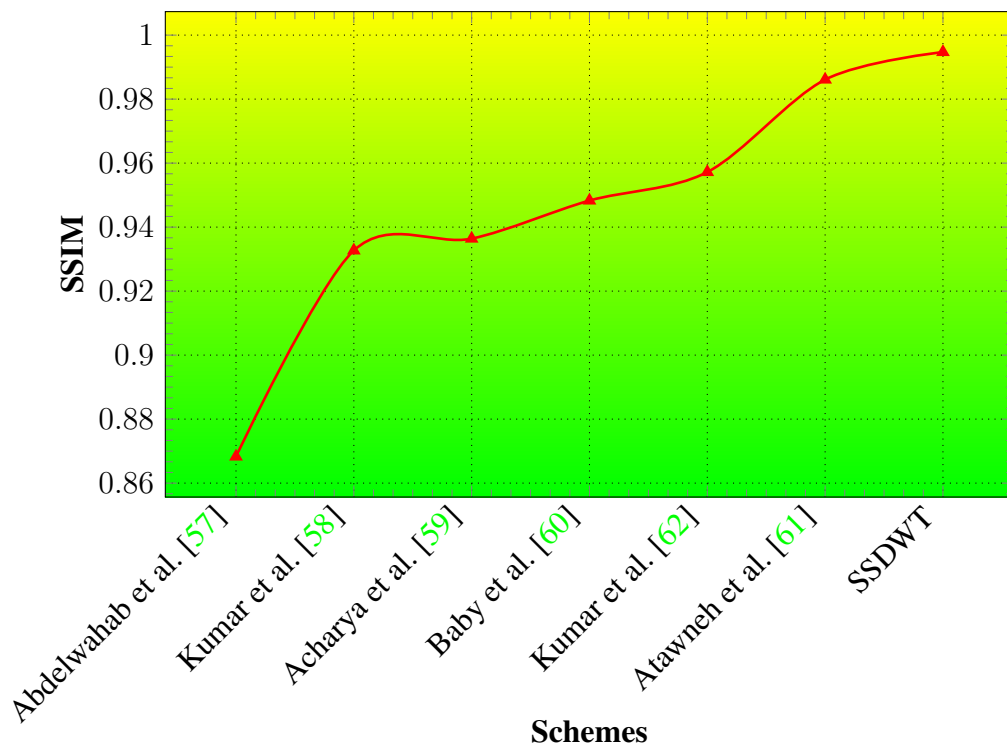


Figure 5.9: Comparison graph of SSDWT with existing DWT based schemes in terms of average SSIM

Table 5.6: Comparison of proposed scheme with some state-of-the-art DCT based schemes in terms of PSNR(dB) in SSDWT

Cover Image	Lena		Airplane		Boat		Baboon		Pepper	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lin et al. [110]	90,112	35.28	90,112	34.53	90,112	33.05	90,112	28.22	90,112	35.09
Saidi et al. [52]	163,840	36.3762	163,840	36.7870	163,840	34.4317	163,840	26.4209	163,840	35.6165
Wei et al. [111]	64,008	33.971	64,008	31.949	64,008	31.147	64,008	25.995	64,008	33.400
Rahman et al. [36]	...	31.4550	30.0704	...	30.4195	...	30.5127
Singh et al. [51]	...	39.7928	39.9285	...	39.5467	...	40.1907
Chang et al. [42]	53,248	34.84	53,248	39.14	53,248	33.29	53,248	27.63	53,248	31.37
Chang et al. [44]	20,473	32.13	20,472	32.09	20,339	31.76	20,437	29.59	20,479	32.74
SSDWT	60440	55.32	60440	55.46	60440	55.15	60440	55.37	60440	54.87

proposed SSDWT scheme, the SSIM is presented in Table 5.7. The average SSIM value is around 0.9960. It indicates good concealment of secret data in the stego image.

5.2.3.2 Robustness Analysis

To analyze the robustness of the proposed SSDWT scheme, NCC, BER, and RS-analysis are carried out :

The NCC is shown in Table 5.7 for the proposed scheme. It is around 0.9998, which is nearer to

Table 5.7: Results of different evaluation matrices for different images in SSDWT

Images	Capacity (bits)	PSNR	SSIM	NCC	BER	Q-Index
Lenna	60440	55.32	0.9947	0.9996	0.0216	0.9997
Barbara	60440	55.53	0.9983	0.9998	0.0208	0.9998
Goldhill	60440	55.46	0.9963	0.9997	0.0206	0.9998
Bird	60440	55.82	0.9987	0.9998	0.0219	0.9998
Raman	60440	54.98	0.9937	0.9996	0.0221	0.9997

1. It indicates high imperceptibility of the stego image. The BER is defined as the rate at which errors occur in a transmission system which can be directly translated into the number of errors that occur in a string of a stated number of bits. BER of the proposed scheme is shown in Table 5.7. It is around 0.0206 when a huge amount of secret data is embedded and around 0.0006 when a moderate amount of secret information is embedded. The value of BER indicates that a very less amount of modification is done in the stego image while embedding secret data. RS Analysis method proposed by Fridrich et al. [41] is used to analyze the stego image after secret data embedding. Two standard image databases are used to perform RS value, which is shown in Table 5.8. The scheme has shown a very good result against RS Analysis. The average RS value of the scheme is around 0.0181 for test images in SIPI image database [90] and 0.0196 for test images in the UCID image database [91]. The value is nearer to zero, and it indicates that SSDWT scheme has less distortion in stego images after embedding secret data.

Table 5.8: Results of RS analysis in SSDWT

Image Database	No. of images	Stego image				RS value
		R_M	R_{-M}	S_M	S_{-M}	
SIPI	05	23861	23572	20259	20467	0.0113
	20	22978	23120	17330	17173	0.0174
	50	33113	30676	06517	06778	0.0181
UCID	05	22354	22334	18137	18221	0.0026
	20	39959	43867	09524	08091	0.0079
	50	21411	21064	11942	12249	0.0196

5.3 Analysis and Discussion

Here, two steganographic schemes, SSDCT and SSDWT, have been designed in the transform domain and analysed. The first scheme, SSDCT uses DCT and the second scheme, SSDWT uses DWT to embed secret data in the stego image. The comparison of the two proposed transform domain based steganographic schemes in terms of PSNR (dB), capacity and payload are described below in Table 5.9. The table establishes that the payload is better in SSDCT scheme, whereas the visual quality of the stego image, in terms of PSNR, is better in the SSDWT scheme. The stego images of these schemes are analysed through RS analysis. The relative entropy and the correlation coefficient (ρ) are calculated and tabulated in Table 5.10. DCT coefficients are very sensitive, and a slight change in the coefficients degrades the quality of the image. In SSDCT scheme, multiple secret bits are embedded by changing a single bit of the DCT coefficient. Moreover, the least number of coefficients are changed to embed the same amount of secret bits compared to other similar schemes. This increases the visual quality of the stego image without compromising with the payload of the scheme. In the second scheme, SSDWT, DWT is used in combination with DCT and employed a weighted matrix to improve the visual quality of the image by changing the least number of coefficients. Though the embedding capacity is less in SSDWT scheme compared to SSDCT scheme, the visual quality of the stego image is more in SSDWT scheme. Moreover, this scheme can be used for the new JPEG 2000 type of images.

Table 5.9: Comparison of SSDCT and SSDWT in terms of PSNR (dB) and payload (bpp)

Schemes	Capacity (bits)	PSNR (dB)	Payload (bpp)
SSDCT	180942	42.12	0.67
SSDWT	60440	55.32	0.23

Table 5.10: Comparison of steganalysis values of SSDCT and SSDWT

Schemes	RS Value	Relative Entropy	CC
SSDCT	0.0325	0.0098	0.9932
SSDWT	0.0453	0.0087	0.9899

Key features of the schemes discussed in this chapter:

- i) Till date, few researchers have considered highly compressed color image for data hiding with acceptable quality measured by PSNR(dB). Here, a novel steganographic scheme for the highly compressed color image has been designed.
- ii) A novel scheme has been used to hide more secret data in DCT domain modifying the

least number of coefficients through weighted matrix. It helps to preserve the quality of the image.

- iii) A shared secret key with SHA-512 encryption and an unknown weighted matrix are suggested to improve the security of the steganography scheme.
- iv) Instead of a gray scale image, a color image is used in the transform domain steganographic scheme because a color image is less sensitive to distortion by our human visual system.
- v) Discrete Wavelet Transform (DWT) in combination with the Discrete Cosine Transform (DCT) is used to increase the robustness and security of the scheme.
- vi) Weighted matrix is predominantly used in the spatial domain. Using the weighted matrix in both these transform domain schemes makes it possible to hide the secret message without hiding the actual secret bits in the stego image. This procedure increases the security and robustness of the schemes two-fold.