

A NOVEL DISCRETE WAVELET TRANSFORM BASED DIGITAL GRAY SCALE IMAGE STEGANOGRAPHY TECHNIQUE

Ajay Goel*

Ravina**

Abstract: The major target of digital image steganography are inconspicuous of the front image and there is no chance to recover the secret image from the stego image. To face these targets, a novel Discrete Wavelet Transform (DWT) based Digital Image Steganography Technique is proposed. In this given technique, two new ideas are introduced. Mainly, the focus point is minimizing the distortion in the cover image and make a good quality stego image. The first procedure which is related to the secret key computation concept is initiated to build it more rigorous and defiant concerning about steganalysis. The next procedure which is partitioning or blocking comes into play for ensuring the least blurring and variation in the stego image as well as cover image. The given technique or approach is applied on five different types of cover images and two secret images. The proposed technique results are very virtuous when compared with three most popular steganography techniques in terms of PSNR and CC. Data Hiding metrics are Peak Signal to Noise Ratio (PSNR) and Correlation Coefficient (CC) and in this the proposed technique performs much better than other techniques. There are several types of attacks in digital image steganography which can be applied on generated stego image for checking the quality and robustness of the image. Mainly, The proposed technique is tested over the six image processing attacks and the steadiness of the given approach is good. The results in the tables explain the steadiness of the given technique under six-image processing attacks. Both stego-image and extracted secret images possess a much better perceptible quality.

Keywords: Discrete Wavelet Transform, Digital Image Steganography, Image Processing attacks.

* **Department of BBA, Gateway School of Business, Sonapat, Haryana, India**

** **Department of Commerce, Hindu Girls College, Sonapat, Haryana, India**

INTRODUCTION

In today's world, Multimedia processing system and internet technologies, an enormous amount of digital data can be dispatched very easily and quickly at very low cost. Using multimedia technologies, The dispatched digital data can be quickly modified with very low amount of data loss with in few seconds.. However, these modifications may influence the violation of delicate data. Hence, the security of this sensitive data has become an necessary need. To solve the above problem, many techniques and procedures for the consolidation of delicate data have been initiated.

To hide the secret data into carrier data, the process is called Digital steganography and the secret data existence is concealed. There are a lot of carriers available in data hiding, the use of digital image is particular recognized as a carrier data. Digital images can be transferred over very lower bandwidth[3] that's why using it. Mainly, In spatial domain, the intensity value of the cover data or image directly modifies through embedding the secret data. Mostly, Spatial domain procedure is used by the least significant bit (LSB). The other very good and popular spatial domain techniques utilize the contrast, noise insertion etc. [4]. The main advantages of this technique are easy to handle, high speed, analyse and accurate. However, it is very delicate towards digital image processing attacks.

There are three other transformation techniques, namely, DFT, DCT and DWT using in data hiding. Out of these three, one can apply on the cover image. After that, blocking concept can be implemented on both types of images i.e, cover image and secret image. The secret image is then embedded into cover image. The main advantages of this technique is discord progressive and fixed[4]. The focus of this paper is on transform domain (especially DWT) based steganography technique. It is also worth mentioning that DWT break down the secret image into four sub-bands such as LH, LL, HH and HL bands. Data hiding in three bands (LH, HL and HH) maintains better image quality. There is no need to maintain extra information about embedded data due to self similarity and uniqueness of DWT coefficients [4, 5].

The main benefaction of this approach is to generate a novel DWT based digital image steganography technique. This technique takes advantage of the hide capabilities of DWT to

preserve quality of image after generating the stegao image. The blocking concept is to reduce the effect of embedded secret images into cover image. Firstly, Both cover image and secret image are decomposed into small, small blocks i.e. called blocking. The small blocks of secret image are embedded into small blocks of cover image by using best matching algorithms. And the best matching block address is stored for further computation. It will help in computation of the secret the key.

It includes a general overview on recently developed image steganography techniques followed by proposed digital image steganography technique. The result will be calculated on many cover images and many secret images. Finally, the concluding remarks are presented.

RELATED WORKS

In literature, There are a number of digital image steganography techniques given which shows the image feature extraction and embedding procedure of secret image into cover image. The first one steganography technique is least significant bit (LSB) substitution which is very popular and very well-known, in which embed the secret data into LSB of the pixels [3]. But this technique is not so good due to the performance of the LSB technique in terms of PSNR and the extracted secret digital image from stegao image is not good [10]. Abdelwahabb and Hassan [6] technique is different from others, which was applied DWT strategy on both the images. But The technique is not so useful because the extracted image is not the same as the embedded image. Kumar and Kumar [1] decomposed the cover image into different bands and embed the secret image into different bands and compare the results of all the bands. However, this technique doesn't increase the loading capacity of secret data. Kumar and Kumar [2] defined a new technique in which combined the DCT and DWT into single technique. This is not appropriate due to the loss of data by rounding in it.

In [8], a new steganography approach was proposed which is based on side matching. It totally reserve the quality of a image, which increases the capacity of the embedding data. This technique is not prosperous against the image processing attacks and no transfer is used. Narasimmalou et al. [7] gave an most favourable discrete wavelet transform based steganography technique. They have divide the cover image into bands by applying DWT procedure and some modification had done in the transform coefficients of the divided

images. Here also the same problem exists i.e, the extracted secret image from the stego image is not appropriate and good quality. In [5] invented a technique that combines the discrete cosine transform and integer wavelet transform. Munkres' assignment algorithm used in the given technique for embedding the data in frequency domain. However, there is possibility of further optimizing the matching and distribution of secret key bits.

El-Emam and Al-Zubidy [9] developed a novel algorithm which is using four layers for security to hide an enormous amount of secret image into a cover image. Moreover, it includes adaptive neural network technique i.e, image segmentation. However, the major drawback of this algorithm takes more time to produce the results. Ghebleh and Kanso [3] proposed a turbulent technique for digital image steganography which is based on lifted discrete wavelet transform with three dimensional chaotic cat map. This approach is very potent, agile and extensible. However, it cannot increase the payload capacity. Baby et al. [10] introduced a new type of data hiding in which multiple color images hide into a single color image by using DWT. N-level decomposition is used for above procedure on cover and secret images. By the help of data compression, we can increase the payload capacity.

In this paper, a novel discrete wavelet transform based digital image steganography has been developed. There are some reasons for adopting DWT as an underlying technique; mainly its simplicity, easy to implement, and maintenance of better image quality.

PROPOSED TECHNIQUE

The proposed technique is a novel discrete wavelet transform. In this paper, three different secret keys are proposed. This enables the proposed approach to be more potent and protected steganalysis. The cover image and secret image are decomposed by the blocking technique. The reason behind this is that it results in negligible change in the cover image. The proposed approach is based on the DWT technique, which is used to decompose the cover image. The detail coefficient concept of DWT is used to utilize the small variation or change in the cover image during embedding of secret image in these coefficients.

The proposed technique having two phases: embedding phase (secret image into cover image) and extraction phase (secret image from stegao image). The details of these phases are depicted as follows.

Embedding Phase

The process of embedding phase shows in the *Figure 1*. In the embedding phase, take the two images i.e, the cover image (I) and the secret image (S), decomposed into four sub-images such as coefficients of approximation (ICA), coefficients of horizontal (ICH), coefficients of vertical (ICV), and coefficients of diagona (ICD), SCA , SCH , SCV and SCD using DWT . These sub-images are divided into non-overlapping blocks. The blocks of SCA are attached with blocks of ICA using root mean square method. Then, compute the difference blocks to each block of ICA with the each block of SCA . After that replace the difference block with best matched block coefficients of ICH , ICV or ICD . The inverse DWT ($IDWT$) is applied on ICA and modified detail coefficients (ICH , ICV , and ICD) to get Stegano Image (I'). The process is as follows:

1. The cover image (I) and the secret image (S) decomposed into four sub-images (ICA , ICH , ICV , ICD) and (SCA , SCH , SCV , SCD) respectively using DWT .
2. Each of ICA , SCA , SCH , SCV , and SCD are divided into blocks of 4×4 pixels and can be represented as:

$$SCA = \{BSA_i, 1 \leq i \leq SA_n\}$$

$$ICA = \{BIA_j, 1 \leq j \leq IA_n\}$$

$$ICH = \{BIH_k, 1 \leq k \leq IH_n\}$$

$$ICV = \{BIV_l, 1 \leq l \leq IV_n\}$$

$$ICD = \{BID_p, 1 \leq p \leq ID_n\}$$

where BSA_i represents i^{th} block in SCA . BIA_j designates j^{th} block in ICA . BIH_k , BIV_l , and BID_p represent k^{th} block in ICH , l^{th} block in ICV and p^{th} block in ICD

3. For each block BSA_i in SCA , the best matched block BIA_j using ($RMSE$). The first secret key $K1$ introduced.

4. Find the difference block DB_i as follows

$$DB_i = BSA_i - \left(\min_{1 \leq j \leq IA_n} BIA_j \right)$$

5. $Bt_{CH} = \min_{1 \leq k \leq IH_n} (RMSE(DB_i, BIH_k))$

$$Bt_{CV} = \min_{1 \leq l \leq IV_n} (RMSE(DB_i, BIV_l))$$

$$Bt_{CD} = \min_{1 \leq p \leq ID_n} (RMSE(DB_i, BID_p))$$

6. Replace DB_i with either Bt_{CH} , Bt_{CV} , or Bt_{CD} which is best matched. The secret keys $K2$, $K3$ and $K4$ introduced.

$$DB_i \leftarrow \min \{ Bt_{CH}, Bt_{CV}, Bt_{CD} \}$$

7. Steps 3 to 6 will repeat until all secret image difference blocks are embedded into cover image ICH , ICV , and ICD blocks.

8. Apply the inverse DWT to the ICA and the modified sub-images ICH , ICV , and ICD to obtain the stegano-image I' .

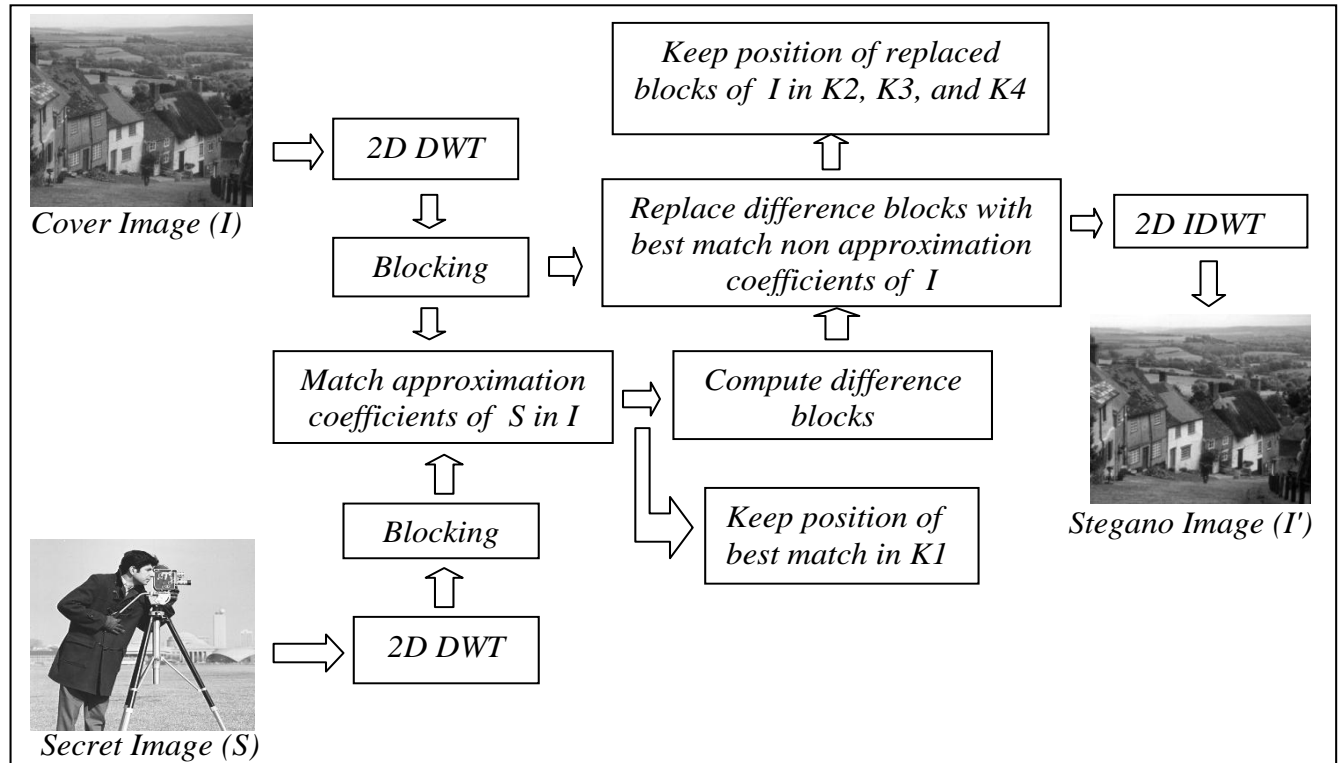


Figure 1. Proposed Embedding Procedure

Extraction Phase

The process of extraction phase shows in *Figure 2*. The difference and best matched blocks generates the secret image of ICA' . The extracting procedure is as follows:

1. Decompose Stegano-image I' into four sub-images (ICA' , ICH' , ICV' , ICD') using *DWT*.
2. Each of ICA' , ICH' , ICV' , and ICD' represented as:

$$ICA' = \{BIA'_j, 1 \leq j \leq IA'_n\}$$

$$ICH' = \{BIH'_k, 1 \leq k \leq IH'_n\}$$

$$ICV' = \{BIV'_l, 1 \leq l \leq IV'_n\}$$

$$ICD' = \{BID'_p, 1 \leq p \leq ID'_n\}$$

3. Extract the best matched block BIA'_j from sub-image ICA' using the first secret key $K1$. The secret keys $K2$, $K3$, and $K4$ are used to extract difference blocks DB'_i from sub-images ICH' , ICV' , and ICD' . The secret block BSA_i is computed as:

$$BSA_i = BIA'_j - DB'_i$$

4. Repeat *Step 2* until all the secret blocks are extracted.
5. Allocate each of sub-images SCH , SCV , and SCD as zeros and apply $IDWT$ to obtain the embedded secret image.

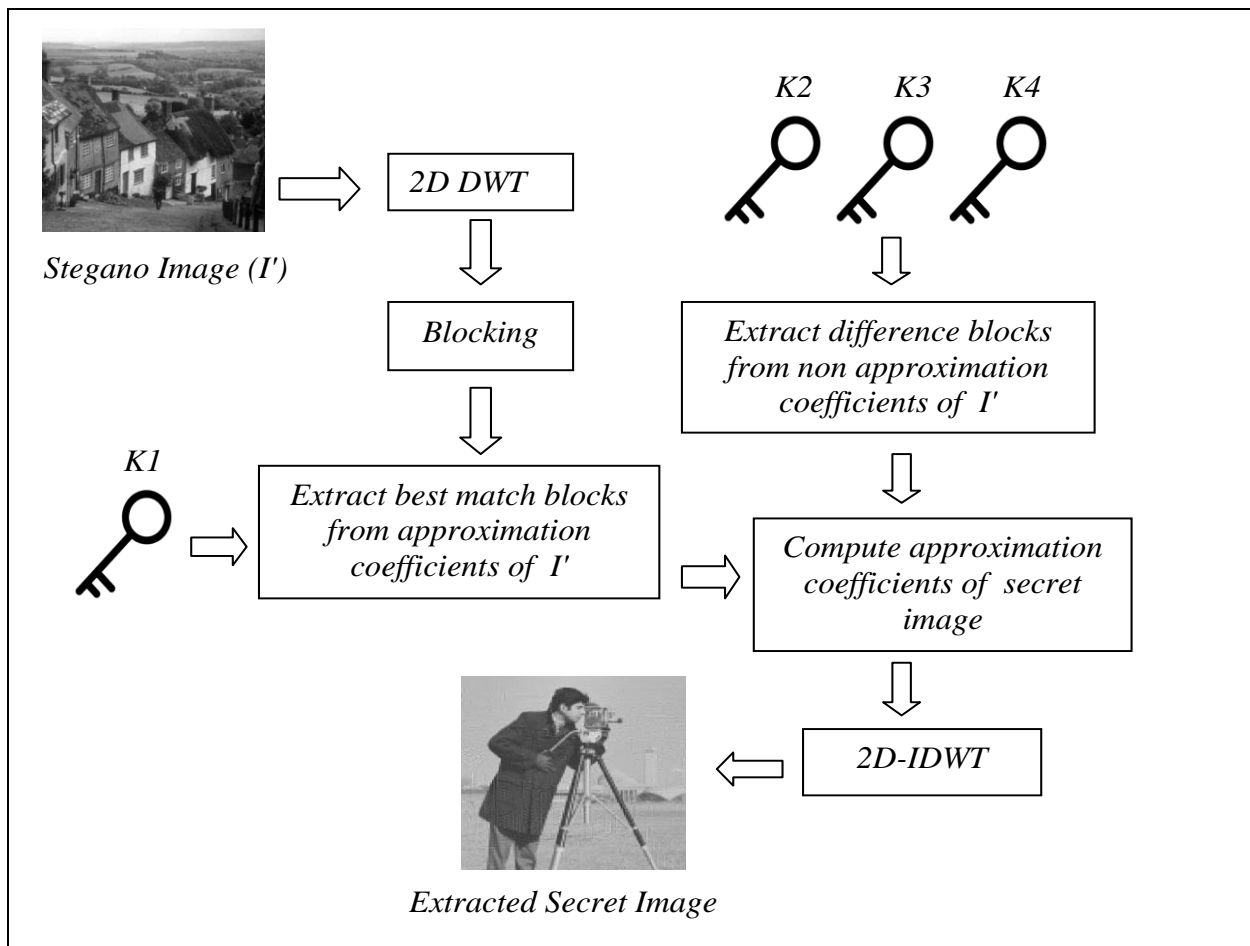


Figure 2. Proposed Extraction Procedure**PERFORMANCE EVALUATION**

In this section, Performance will be evaluated on the basis of many experiments whatever done on different images. The results will be compared with the other popular techniques and find the best results of proposed technique.

Performance Metrics and Digital Images

Take the four different images as cover image, namely, *Goldhill*, *Bird*, *Lena*, and *Raman* and two secret images: *Camerman* and *Baboon*. The different sizes of images include for evaluation. The sizes are 256×256 , 128×128 , 64×64 . Figure 3 shows the all cover images with same size. Figure 4 shows the all secret images with same size. The results in terms of PSNR or CC of new proposed technique is compared with other popular steganography techniques such as Least Significant Bit (LSB) [6], Discrete Wavelet Transform based steganography technique (DWS) [9], and DCT_DWT based steganography technique (DCWS) [4]. In terms of performance metrics, PSNR and CC used for comparison.

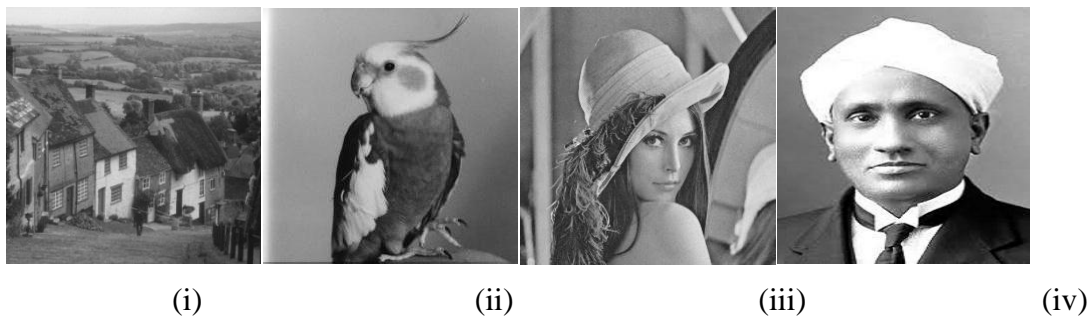


Figure 3. Original Cover Images (i) Goldhill (ii) Bird (iii) Lena (iv) Raman.

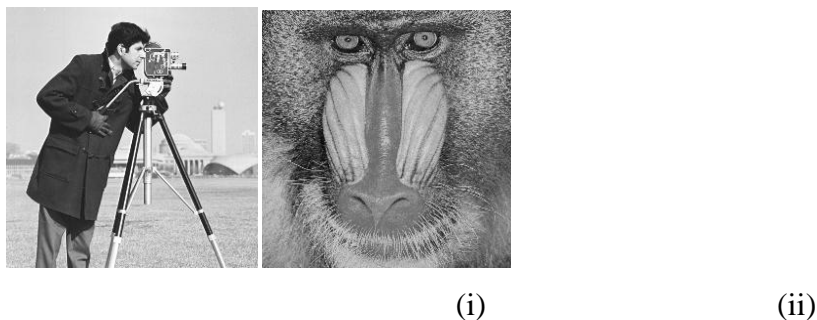


Figure 4. Original Secret Images (i) *Cameraman* (ii) *Baboon*.

The PSNR is used to measure imperceptibility. It is an important parameter for evaluation of steganographic techniques. Mathematical notation is :

$$\text{PSNR} = 10 \times \log_{10} \left(\frac{255 \times 255}{\text{MSE}} \right) \quad (1)$$

Here,

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (I_{i,j} - I'_{i,j})^2 \quad (2)$$

where $I_{i,j}$ shows the value of intensity of original cover image (or secret image), $I'_{i,j}$ shows the value of intensity of stegano image (or extracted secret image). The size of image is $M \times N$. The PSNR value is directly proportional to the quality of the image i.e, imperceptibility.

The other well-known similarity measure is Correlation Coefficient (CC). The mathematical representation of CC is given below [19]:

$$\text{CC} = \frac{\sum_{i=1}^M \sum_{j=1}^N (I_{i,j} - \bar{I})(I'_{i,j} - \bar{I}')}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N (I_{i,j} - \bar{I})^2} \sqrt{\sum_{i=1}^M \sum_{j=1}^N (I'_{i,j} - \bar{I}')^2}} \quad (3)$$

where \bar{I} and \bar{I}' are mean of original and stegano/extracted secret image. If the original and stegano/extracted secret image are highly correlated, this results in higher value of CC.

Results and Discussion

The *Cameraman* image was embedded into four cover images namely, *Lena*, *Goldhill*, *Bird*, and *Raman*. Similarly, we embedded *Baboon* image into *Goldhill*, *Bird*, *Lena*, and *Raman* images. Figure 3 represents the process of embedding of *Cameraman* as a secret image. The stegano images are much better image quality than other techniques stegano images. Figure 4 represents the process of embedding of *Baboon* as a secret image. The quality of stegano images are much better and negligible change shown in the used cover images.

Tables 1 and Table 3 characterize the PSNR value of stegano images after embedding. Table 2 and Table 4 represents the PSNR value of extracted secret images.

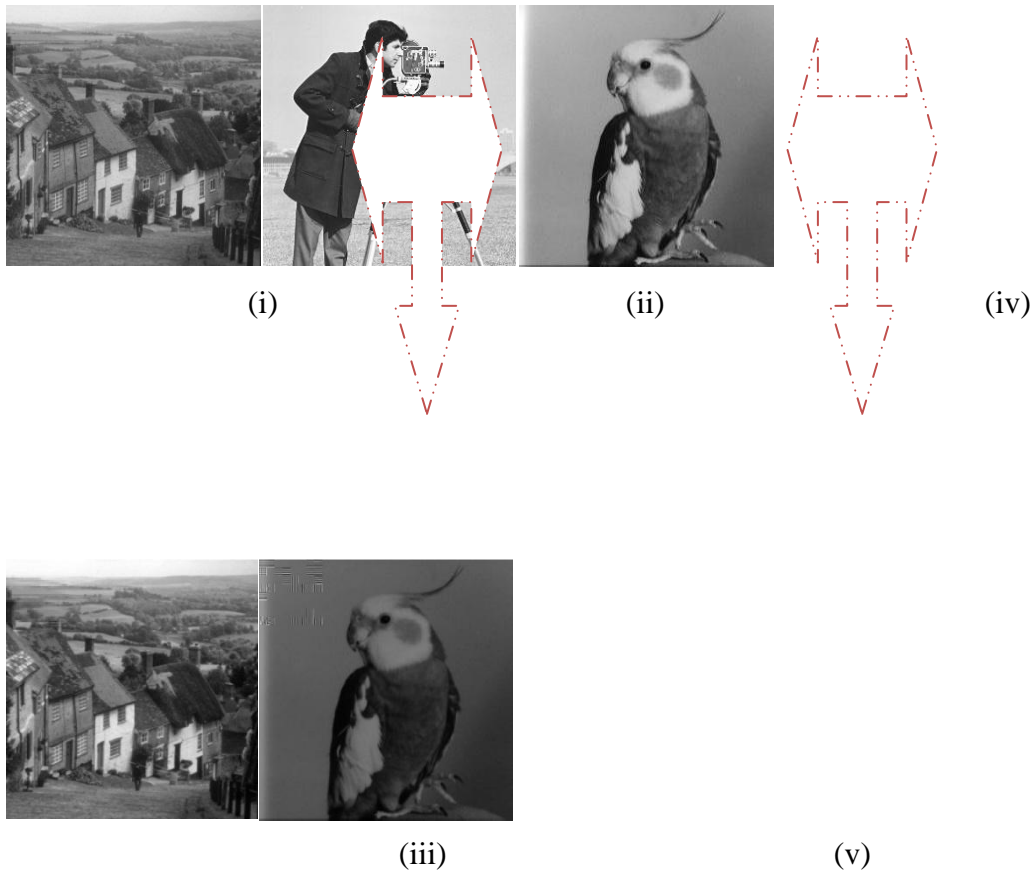
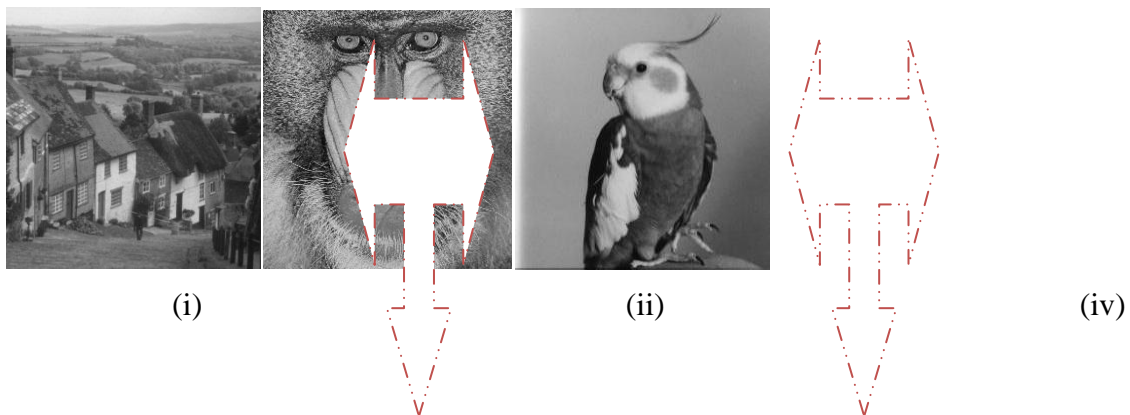


Figure 5.(i) Cover Goldhill Image (ii) Secret Cameraman Image (iii) Stegano Goldhill Image after embedding Cameraman (iv) Cover Bird Image (v) Stegano Bird Image after embedding Cameraman.





(iii)

(v)

Figure 6.(i) Cover Goldhill Image (ii) Secret Baboon Image (iii) Stegano Goldhill Image after embedding Baboon (iv) Cover Bird Image (v) Stegano Bird Image after embedding Baboon.

Table 1. PSNR of Stegano Images after embedding Cameraman as Secret Image

Cover Images	Algorithms			
	<i>LSB</i>	<i>DWS</i>	<i>DCWS</i>	<i>Proposed Approach</i>
<i>Goldhill</i>	11.16	31.86	41.84	43.22
<i>Bird</i>	12.91	32.37	42.45	45.12
<i>Lena</i>	09.66	31.86	41.93	44.84
<i>Raman</i>	12.91	32.37	42.45	45.23

Table 2. PSNR of Extracted Cameraman as Secret Image

Cover Images	Algorithms			
	<i>LSB</i>	<i>DWS</i>	<i>DCWS</i>	<i>Proposed Approach</i>
<i>Goldhill</i>	12.14	30.89	40.23	45.12
<i>Bird</i>	10.67	31.24	41.56	44.20
<i>Lena</i>	10.76	32.56	41.67	42.73
<i>Raman</i>	13.47	33.45	40.34	42.49

Table 3. PSNR of Stegano Images after embedding Baboon as Secret Image

Cover Images	<i>Algorithms</i>			
	<i>LSB</i>	<i>DWS</i>	<i>DCWS</i>	<i>Proposed Approach</i>
<i>Goldhill</i>	11.16	31.86	41.84	44.98
<i>Bird</i>	12.91	32.37	42.45	43.60
<i>Lena</i>	09.66	31.86	41.93	42.87
<i>Raman</i>	12.91	32.37	42.45	43.36

Table 4. PSNR of Extracted Baboon as Secret Image

Cover Images	<i>Algorithms</i>			
	<i>LSB</i>	<i>DWS</i>	<i>DCWS</i>	<i>Proposed Approach</i>
<i>Goldhill</i>	11.16	31.86	41.84	42.98
<i>Bird</i>	12.91	32.37	42.45	42.49
<i>Lena</i>	09.66	31.86	41.93	42.46
<i>Raman</i>	12.91	32.37	42.15	42.38

The another performance metrics correlation coefficient (*CC*) calculated for stegano images after applying the embedding process shown in Tables 5 and 7. Tables 6 and Table 8 illustrates the values of *CC* for extracted secret images.

Table 5. Correlation Coefficient of Stegano Images after embedding Cameraman as Secret Image

Cover Images	<i>Algorithms</i>			
	<i>LSB</i>	<i>DWS</i>	<i>DCWS</i>	<i>Proposed Approach</i>
<i>Goldhill</i>	0.7069	0.8595	0.9578	0.9993
<i>Bird</i>	0.7913	0.8669	0.9429	0.9677
<i>Lena</i>	0.6868	0.8487	0.8999	0.9174
<i>Raman</i>	0.6753	0.8599	0.9162	0.9378

Table 6. Correlation Coefficient of Extracted Cameraman as Secret Image

Cover Images	Algorithms			
	<i>LSB</i>	<i>DWS</i>	<i>DCWS</i>	<i>Proposed Approach</i>
<i>Goldhill</i>	0.9594	0.9523	0.9500	0.9718
<i>Bird</i>	0.9422	0.9479	0.9495	0.9527
<i>Lena</i>	0.9287	0.9388	0.9489	0.9624
<i>Raman</i>	0.9298	0.9458	0.9512	0.9576

Table 7. Correlation Coefficient of Stegano Images after embedding Baboon as Secret Image

Cover Images	Algorithms			
	<i>LSB</i>	<i>DWS</i>	<i>DCWS</i>	<i>Proposed Approach</i>
<i>Goldhill</i>	0.7527	0.8259	0.9345	0.9981
<i>Bird</i>	0.7908	0.8476	0.9352	0.9917
<i>Lena</i>	0.7596	0.8263	0.8965	0.9174
<i>Raman</i>	0.7668	0.8369	0.9159	0.9652

Table 8. Correlation Coefficient of Extracted Baboon as Secret Image

Cover Images	Algorithms			
	<i>LSB</i>	<i>DWS</i>	<i>DCWS</i>	<i>Proposed Approach</i>
<i>Goldhill</i>	0.7845	0.7900	0.8178	0.8268
<i>Bird</i>	0.7988	0.8008	0.8199	0.8270
<i>Lena</i>	0.8078	0.8211	0.8207	0.8476
<i>Raman</i>	0.7988	0.8175	0.8234	0.8364

Performance Evaluation Under Different Image Processing Attacks

The performance of proposed technique is also tested over some digital image processing attacks such as *Gamma Correction*, *Sharpening*, *Histogram Equalization*, *Gaussian Noise*, *Rotation* and *Transform*. Table 9 and Table 10 shows the results.

Table 9. PSNR of Stegano Images and Extracted Cameraman as Secret Image Under Different Attacks

Image After Attack	Algorithms	Image Processing Attacks					
		Sharpening	Histogram Equalization	Gamma Correction	Gaussian Noise	Transformation	Rotation
Stegano-Goldhill	Proposed	27.65	41.68	32.31	41.69	41.46	37.37
	DCWS	11.95	16.51	25.54	18.69	12.61	24.87
Stegano-Bird	Proposed	34.34	42.72	31.63	42.73	40.66	37.01
	DCWS	29.78	18.94	18.37	31.76	26.63	29.87
Stegano-Lena	Proposed	37.62	44.12	31.92	45.23	41.42	37.26
	DCWS	13.65	16.25	19.89	40.48	11.78	25.37
Stegano-Raman	Proposed	35.82	42.56	34.87	44.76	40.67	38.23
	DCWS	31.64	30.06	20.19	18.66	38.66	32.38
Extracted-Cameraman	Proposed	27.66	41.68	32.31	41.68	41.45	37.38
	DCWS	17.10	13.26	12.44	19.50	38.92	37.27

Table 10. PSNR of Stegano Images and Extracted Baboon as Secret Image Under Different Attacks

Image After Attack	Algorithms	Image Processing Attacks					
		Sharpening	Histogram Equalization	Gamma Correction	Gaussian Noise	Transformation	Rotation
Stegano-Goldhill	Proposed	28.33	41.68	32.31	41.69	41.46	37.39
	DCWS	11.90	16.56	25.59	18.76	12.63	24.78
Stegano-Bird	Proposed	28.69	42.69	31.61	42.69	40.61	36.79

	<i>DCWS</i>	24.78	23.94	19.39	32.79	28.63	29.73
<i>Stegano-Lena</i>	<i>Proposed</i>	30.13	43.26	31.59	42.94	40.84	36.58
	<i>DCWS</i>	15.62	17.52	19.78	38.43	13.76	23.32
<i>Stegano-Raman</i>	<i>Proposed</i>	36.21	42.61	30.51	44.27	41.82	40.53
	<i>DCWS</i>	29.66	28.08	22.16	26.64	38.27	33.47
<i>Extracted-Baboon</i>	<i>Proposed</i>	37.40	42.43	35.92	42.44	42.34	35.59
	<i>DCWS</i>	26.48	32.76	32.67	37.89	36.56	28.78

CONCLUSIONS

A novel Discrete Wavelet Transform based digital image steganography approach has been proposed. Mainly, two novel concepts, computation of secret key and blocking phase applied on the proposed technique. The blocking uses the minimum deviation concept. Detail coefficient and minimum error matching criteria helps to compute the secret key. The performance of the proposed technique is much better than other techniques in terms of *PSNR* and correlation coefficient. Stegano image and the extracted secret image quality is very good and extracted secret image looks like the original secret image. Good visual quality provides by the newly secret key criterion.

REFERENCES

1. V. Kumar, and D. Kumar, "Performance evaluation of dwt based image steganography", Proceedings of 2nd International Conference on Advance Computing, **2010**, Patiala, India, pp.223-228.
2. V. Kumar, and D. Kumar, "Digital image steganography based on combination of DCT and DWT" (Ed. V. V. Das and R.Vijaykumar), Information and Communication Technologies, Kochi, Kerala, **2010**.
3. M. Ghebleh and A. Kanso, "A robust chaotic algorithm for digital image steganography", *Commun. Nonlinear Sci. Numer. Simulat.*, **2014**, *19*, 1898-1907.

4. C.K. Chan and L.M. Chang, "Hiding data in image by simple LSB substitution", *Pattern Recognition*, **2003**, 37, 469-474.
5. S. Mythreyi and V. Vaidehi, "Gabor transform based image steganography", *IETE Journal of Research*, **2007**, 53(2), 103-112.
6. A.A. Abdelwahab and L.A. Hassan, "A discrete wavelet transform based technique for image hiding", Proceedings of 25th National Radio Science Conference, **2008**, Tanta Univ., Egypt, pp.1-9.
7. T. Narasimmalou and A. R. Joseph, "Optimized discrete wavelet transform based steganography", Proceedings of IEEE International Conference on Advanced Communication Control and Computing Technologies, **2012**, Ramanathapuram, pp.88-91.
8. N. Raftari and A.M.E. Moghadam, "Digital image steganography based on assignment algorithm and combination of DCT-IWT", Proceedings of International Conference on Computational Intelligence, Communication Systems and Networks, **2012**, Phuket, pp.295-300.
9. N. El-Emam and R. Al-Zubidy, "New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm", *Journal of Systems and Software*, **2013**, 86, 1465-1481.
10. D. Baby, J. Thomas, G. Augustine, E. George and N. R. Michael, "A novel DWT based image securing method using steganography", *Procedia Computer Science*, **2015**, 46, 612-618.
11. A. Goel, V. Deswal, S. Chhabra, "A Novel Digital Color Image Steganography using Discrete Wavelet Transform", *International Journal of Computer Science and Engineering*, 2019, 2347-2693.
12. A. Goel, S.Chhabra, "PVO-Based Multiple Message Segments Reversible Data Hiding ", *Research Analysis and Evaluation*, 2019, 2320-5482.