A Daubechies DWT Based Image Steganography Using Smoothing Operation

Vijay Sharma, Devesh Srivastava, and Pratistha Mathur
Computer Science and Engineering Department, Manipal University Jaipur, India

Abstract: *Steganography is a capability which conceals the top-secret information into cover media (e.g., digital images, sound files etc.,). This Paper presents a secure, higher embedding capacity Discrete Wavelet Transformation (DWT) based technique. Before embedding correlation in between cover and the secret image is increased by multiplying some variable (i.e., 1/k) to the secret image. In embedding process, the Daubechies DWT of both Arnold transformed secret and cover images are taken followed by alpha blending operation. Arnold is a type of scrambling process which increases the confidentiality of secret image and alpha blending is a type of mixing operation of two images, the alpha value indicates the amount of secret image is embedded into the cover image. Daubechies Inverse Discrete Wavelet Transformation (IDWT) of the resulting image is performed to obtain the stego image. Smoothing operation inspired by the Genetic Algorithm (GA) is used to improve the quality of stego-image by minimizing Mean square error and morphological operation is used to extract the image component from the extracted secret image. Simulation results of the proposed steganography technique are also presented. The projected method is calculated on different parameters of image visual quality measurements.*

Keywords: *Steganography, Daubechies DWT, Arnold transform, smoothing operation, genetic algorithm, morphological operation.*

Received March 18, 2017; accepted January 28, 2018
https://doi.org/10.34028/iajit/17/2/2

1. Introduction

In the recent times the development of high speed communication system has helped exchange of information at a fast pace. However, it has also increased the threat of data being snooped while information is exchanged between sender and receiver. It is requisite that the data has to be secured that is privacy and authentication of the information has to be maintained. Hence, it can be said that information security is an integral part of communication in these days.

Information system security is a discipline that deals with protection of data, prevents the malicious attack to violate the privacy of data and keeps the data secure from intermediates. The name steganography is derived from two Greek words, these are stegos and graphica which means "enclosed writing" (stgos-enclosed and graphica-writing) [12].

As we know that information exchange through internet has become the most powerful medium of communication around the world therefore safe exchange of data is an inevitable part of information exchange stack. Hence, there is a pressing need to develop a good steganography algorithm that can aid in exchange of information in a secure manner.

Ongoing parts of manuscript are assimilating as follow: review, proposed method, simulation results and finally conclusion.

2. Review of Dwt, Steganalysis and Genetic Algorithm

Digital media is not secure in comparison to analog media. Security is essential while converting data from one form to another. Transfer domain is used for conversion of data into different forms. Discrete wavelet transform separates the data into different frequency components. The digital media improves media quality, reliability, compression and editing quality etc., However, there amplification and augmentation can be tracked by outside attack.

The use of Discrete Wavelet Transformation (DWT) is to analyze the signals. Hence, it can be expressed as decomposition of images [2, 3]. Wavelets are the special kind of functions which are used for denoting signals. Wavelet are commonly known as small or little wave that is use to perform the analysis when the frequency of a signal varies over the time. Transformation of wavelet means splits a signal into dissimilar components of frequency in which each component have the different resolution. Different kind of wavelets are available, we are using daubechies wavelet with 2-D DWT.

In Shrestha and Timalsina [11], explained daubechies wavelet as, it gives more Peak Signal to Noise Ratio (PSNR) as compared to the haar DWT. The family name of daubechies wavelet is written as dbN (i.e., 'db2', 'db3',…. 'db45'), where db is the surname of daubechies wavelet of order N. Here we

are using db8. The main application of the 2-D DWT is, divide a image into the four sub images as Low-Low frequency sub band (LL), Low-High frequency sub band (LH), High-Low frequency sub band (HL) and High-High frequency sub band (HH) these are Low- Low, Low- High, High-low, High-High respectively. Figure 1 infer the 2-D DWT image view. The low frequency sub band (LL) is commonly known as approximation band which contain main information of image. Whereas the higher frequency sub band (i.e., HH, HL and LH) hold the edge and texture information. Human eyes are imperceptible to minor change in frequency, here secret image or secret object can be embedded at the sub band of higher frequency.

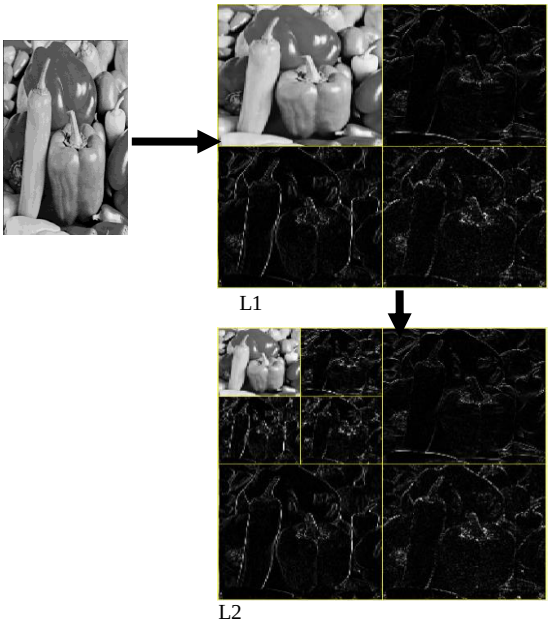


Figure 1. Two levels of discrete wavelet transform of bd8.

The comparative study of DWT based steganography with different types of image processing attacks is explained in [7]. In the process of steganography, an embedder can select any digital cover media that can generate least detectable stego file. Ataby and Naima [1], presents DWT based high capacity image steganography.

Hybrid curvelet transformed technique for image steganography is explained by [8], it handle the curve discontinuities problem in the carrier image. Subhedar and Mankar [15], stated about the cover selection and contourlet transformation steganography that results better stego image picture quality then other existing DWT techniques. In the paper DWT based technique gives the better results which depends on the pre-processing steps and smoothing operation as shown in result section.

Different performance evaluation parameters of image steganography are shown in [9].

Prabakaran and Bhavani [10], proposed elevated embedding capacity based data hiding technique, which hide large size of secret image inside relative small cover image. DWT based blind image steganography technique is proposed by [13], which eliminated the host or cover image requirement at receiver.

2.1. Steganalysis

Steganalysis is an attack that breaks this protection and fetches the hidden message. The central objective of steganalysis is to identify the image, whether it is stego or not a stego. Fridrich *et al.* [4], introduced a dominant steganalysis process (named as RS attack) which is based on statistical techniques, where the image is partitioned into groups of 8X8 pixels blocks, with the help of discrimination function "softness", was calculated for every group of 8X8 blocks. Magnitude of the function determines the strength of association. Small value of discrimination indicates stronger association. This discrimination of image block is calculated by performing zig-zag scan.

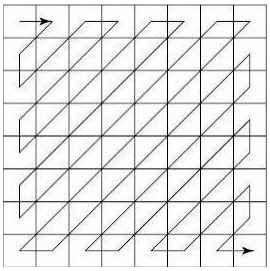


Figure 2. Zigzag scan operation for a block size of 8x8 pixels.

$$f(G) = f(X_1, X_2, ..., X_n) = \sum_{i=1}^{n-1} \left| X_{i+1} - X_i \right| \quad (1)$$

Here x_i represents pixel intensity and n represents number of pixels.

In [4], shown that RS steganalysis is divided into three categories of blocks based on flipping function (F). Firstly, positive flipping F_{+1} (i.e., $2i$ can be replaced with $2i+1$ or vice versa). Secondly, negative flipping F_{-1} (i.e., $2i-1$ can be replaced with $2i$ or vice versa) and lastly, zero flipped F_0.

F_1 and F_{-1} has the following relationship

$$F_{-1} = F_1(x + 1) - 1 \quad (2)$$

F_0, F_1 and F_{-1} are the flipping function.

If $f_{\text{New}} < f$ the block is called singular; if $f_{\text{new}} > f$ then the block is regular.

The relationship for a natural image block has been given by [4].

$$R_m \approx R_{-m}, S_m \approx S_{-m} \text{ and } R_m > S_m, R_{-m} > S_{-m} \quad (3)$$

Embedding increases the variation among R_m and R_{-m} or S_m and S_{-m}.

The discrimination function of an image or an image block is defined as the sum of the difference of adjacent pixels. Natural images have high degree of correlation, in other words, the value of it's discrimination function increases significantly. Hence, steganalysis attack can determine efficiently that the

image is stego image.

Therefore, it is imperative that the image visual quality needs to improve at every level of embedding.

2.2. Genetic Algorithm

In [6, 16] explained the genetic algorithm based image visual quality improvement. Performing genetic algorithm on stego image, results natural image.

3. Proposed Method

The proposed technique enables to embed large image inside a comparatively small image. The Figure 3 shows the development algorithm's process applied at sender's end.

Secret image is preprocessed by multiplying some variable (i.e., 1/K, here K=1, 1.2, 1.4, 1.6) to increase the correlation between cover and secret image, it can be observed on the basis of obtained intensity matrix and PSNR or other word we can say that better PSNR stego can be generated.

At sender end, Arnold transform is applied to secret image that provides the confidentiality and later host image or cover image is added to the secret image for DWT coefficients, with the support of alpha blending.

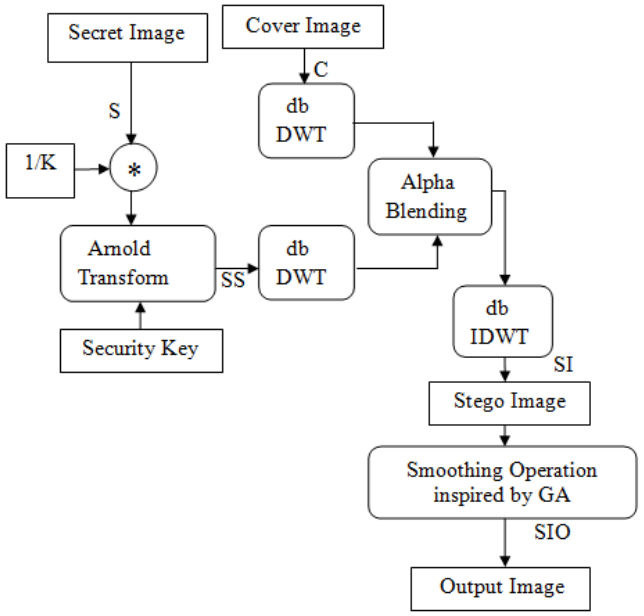


Figure 3. Steganography technique followed by smoothing operation inspired from Genetic Algorithm.

The function alpha blending generate the matrix, which is obtained by adding wavelet coefficients of respective sub-bands of the cover image and Arnold transferred secret image, as explained in next section. Alpha factor increase the embedding strength, here it is known as strength factor. After performing combination operation (alpha blending), the daubechies (db8) Inverse Discrete Wavelet Transform (IDWT) is applied and get the stego image. The algorithmic steps of encoding process are shown below:

- *Step* 1: take cover image (Let's say C) and secret image (Let's say S).
- *Step* 2: apply S = S*(1/K) operation step, for any K value, for K=1, 1.2, 1.4, 1.6, which can generate better PSNR stego image.
- *Step* 3: apply 2-D daubechies (db8) DWT on the C image.
- *Step* 4: apply Arnold transformation on secret image S that results scrambled secret Image (Let's say SS).
- *Step* 5: apply a 2-D daubechies (db8) DWT on SS image.
- *Step* 6: obtain matrices of approximation coefficient Approximation frequency sub band (LA) and detailed coefficient matrices as LH, Vertical frequency sub band (LV) and LD of C image.
- *Step* 7: extract the LA and LH, LV & LD of the SS image.
- *Step* 8: apply Alpha Blending on the C image and secret image SS which is obtained from above steps.
- *Step* 9: for generating the stego image (Let's say SI), 2-D daubechies (db8) IDWT is applied.
- *Step* 10: apply Smoothing operation at SI image and get output image (Let's say Stego Image Output (SIO)).

The main application of smoothing operation on stego image blocks is to provide resist against the RS attack.

3.1. Arnold Transformation

In Sehgal and Sharma [13] proposed an image based scrambling process. Image scrambling happens after the application of Arnold transformation, a new matrix is obtained as the result, which was explained by [5].

In the transformed image matrix, each pixel has some correlation with others. It comprises of a class of special matrices in which correlation between the elements exists. Arnold transform for setting the image pixel coordinates is as in Equation (4).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (Mod \quad N) \tag{4}$$

Here $x, y \in (0, 1, 2, ..., N-1)$ is the pixel position.

The transformation has increases security and robustness in proposed technique.

3.2. Alpha Blending

The operation combined two images and generate desired harvest image, it was introduced by Prabakaran and Bhavani [10] and Saha and Sharma [13]. The final image is given by following equation.

$$FImage = C + \alpha * SS \tag{5}$$

Here the value of α is $0 < \alpha < 1$, Alpha is the strength factor for embedding.

The value of alpha will affect the stego image picture quality (i.e., PSNR). As alpha value increases

the stego image picture quality decreases. It is a needed to improve the stego image visual quality. This is done by applying pixel value or gray level smoothing operation inspired from genetic algorithm [6, 16] as explained in section 3.3, by applying the 3.3, Genetic Algorithm (GA) based smoothing operation the discrimination function will be decreases and image moves towards the natural or original image which is also explained by [4].

3.3. Genetic Algorithm based Smoothing Operation

1. *Initialization*: chose two adjacent pixels from a row. These are called initial chromosomes in the genetic terminology. We are forming new pixel pair (gray level) by choosing adjacent pixel value or gray level as explained in next step.
2. *Imitation and Transmutation*: in a pixel pair first Least Significant Bit (LSB) is swapped to produce the possible next generation chromosome, Table 1 shows the next generation Pixel pair.

Table 1. Possible next generation pixel pair (i.e., chromosomes).

First Pixel Value	Second Pixel Value	First LSB Operation		Next Generation Pixel pair		
		First Pixel	Second Pixel			
62	91	NoSwap	NoSwap	C1=	62	91
		Swap	Swap	C2=	63	90

3. *Pixel pair Selection*: out of two chromosomes (original and next generation), the one that minimize the difference intensity value is selected.
4. *Intersection*: Shift the pixel pair as one pixel right. If same intersection is repeated up to two instant, stop the selection.
5. Followed by adjustment of the image block, analyze R, R–, S and S– block in a image. Check If the blocks meets the criteria for natural images [4, 16] the image is successfully modified, else, adjust the next block.

3.4. Decoding Process

The decoding process at receiver's end shown in Figure 4. Since there is only minor change in stego image picture quality when smoothing operation is performed. Hence, there is no need to apply reverse of such operation at receiver's end.

The decoding process at receiver is just the opposite of the former sender process. Apply 2-D daubechies (db8) DWT, at the cover image and the stego image. The alpha blending is applied on both images. Finally, the secret image is obtained by applying the daubechies (db8) IDWT followed by Inverse Arnold transform process as exposed in Figure 4. The decoding process use following subsequent algorithm steps.

- *Step* 1: apply 2-D daubechies (db8) DWT on the output stego image SIO and cover image C.
- *Step* 2: apply Alpha blending on both image SIO and image C.
- *Step* 3: apply daubechies (db8) IDWT to generate SS image.
- *Step* 4: apply Inverse Arnold transform with secret key to reform an original secret image S.

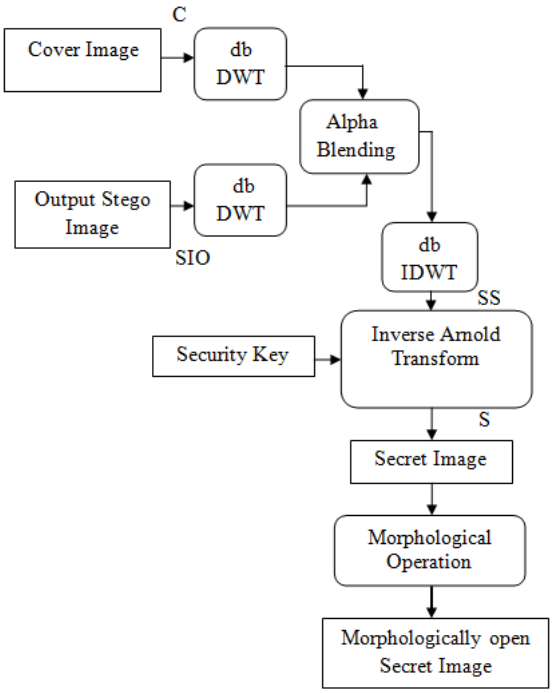


Figure 4. Flow chart for generating secret image at receiver's end.

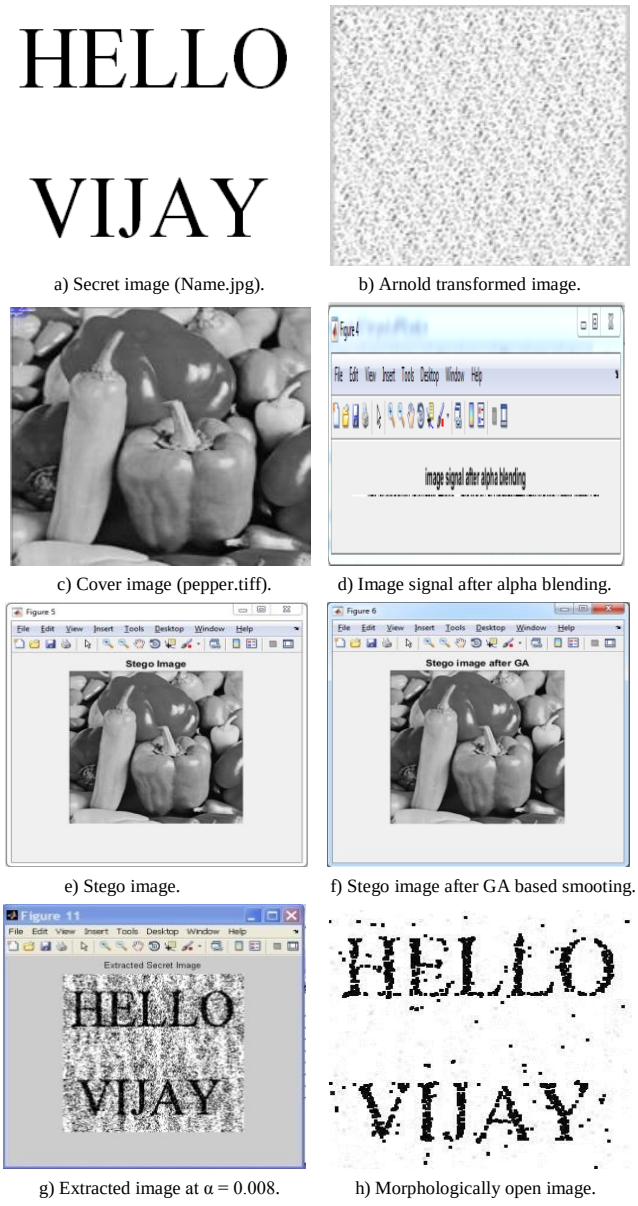
The secret image obtained as in result is not similar to the original one. Here is requirement to increase the visual quality of noisy image message. Extracted image visual quality can be increases by applying the morphological operation [2, 3]. This operations accomplished using dilation, erosion, opening and closing algorithms to remove any spurious noise within a image frame.

4. Simulation Results

The projected method's performance is measured by executing it in MATLAB. Experimental results are shown in Figure 5 below. Here, pepper.tiff (cover image) and Name.jpeg (secret image) are used to evaluate the performance. All the experiments are based on grayscale images for different value of alpha and K.

The presentation of the proposed technique is scrutinized by comparing with following factors of cover Image and stego image.

1. Peak Signal to Noise Ratio (PSNR).
2. Mean Square Error (MSE).
3. Normalized Cross Correlation (NCC).



a) Secret image (Name.jpg). b) Arnold transformed image.

c) Cover image (pepper.tiff). d) Image signal after alpha blending.

e) Stego image. f) Stego image after GA based smooting.

g) Extracted image at α = 0.008. h) Morphologically open image.

Figure 5. Results obtained after executing proposed algorithmic steps.

PSNR evaluate the bend between these images. It is measured by Equation (6).

$$PSNR = 10\frac{\log_{10}(255)^2}{MSE}dB \quad (6)$$

Where MSE is the unit for measuring the difference among these two images, of size M x N. It is measured by Equation (7).

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})^2 \quad (7)$$

Here $x_{j,k}$ is pixel value at j^{th} row and k^{th} column of cover image and $x'_{j,k}$ is pixel value at j^{th} row and k^{th} column of Stego image. *NCC* is measure by Equation (8).

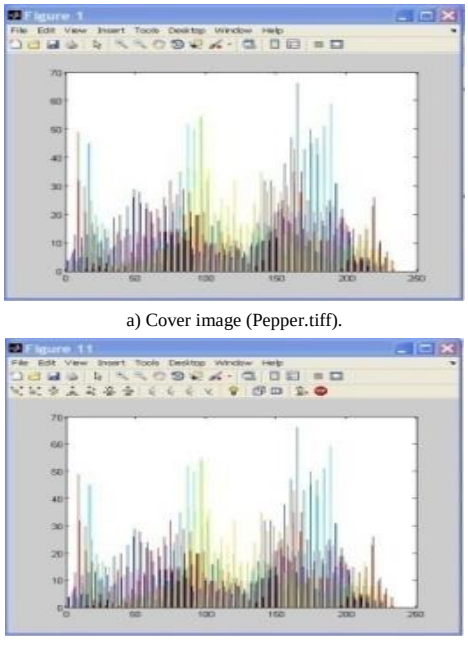
$$NCC = \sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} * x'_{j,k})\frac{1}{\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k})^2} \quad (8)$$

The performance of projected method is measured on the basis of results. Table 2 shows the effect of alpha (α) at PSNR, MSE, and NCC.

Table 2. Measurement of stego image's PSNR, MSE and NCC for both cover image-Pepper.tiff (430 X 425) and secret image-Name.jpg (430 X 425) without multiplying 1/k.

←Alpha(α)	Before Smoothing operation			After GA based Smoothing operation			Secret Image Recognition?
	PSNR	MSE	NCC	PSNR	MSE	NCC	
.002	53.6687	1.5287e+04	0.9968	54.5839	1.2382e+04	0.9972	No
.007	42.6179	1.9472e+05	0.9888	42.7874	1.8726e+05	0.9890	No
.008	41.6275	2.4459e+05	0.9874	42.7344	1.8956e+05	0.9894	Yes
.009	40.6045	3.0956e+05	0.9859	41.5860	2.4694e+05	0.9878	Yes
.010	39.6893	3.8217e+05	0.9843	40.5714	3.1192e+05	0.9863	Yes
.02	33.6687	1.5287e+06	0.9690	34.1115	1.3805e+06	0.9709	Yes
.03	30.1469	3.4396e+06	0.9540	30.4464	3.2104e+06	0.9559	Yes
.04	27.6481	6.1148e+06	0.9393	27.8765	5.8015e+06	0.9412	Yes
.05	25.7099	9.5543e+06	0.9250	25.8958	9.1540e+06	0.9268	Yes
.06	24.1263	1.3758e+07	0.9110	24.2839	1.3268e+07	0.9128	Yes
.07	22.7874	1.8726e+07	0.8973	22.9249	1.8143e+07	0.8991	Yes
.08	21.6275	2.4459e+07	0.8840	21.7500	2.3779e+07	0.8857	Yes
.09	20.6045	3.0956e+07	0.8709	20.7152	3.0177e+07	0.8726	Yes
.10	19.6893	3.8217e+07	0.8581	19.7907	3.7336e+07	0.8599	Yes

Figure 6 shows the histogram of cover image and output stego image. Here, the both histograms are equal to each other, means both images have strong correlation.



a) Cover image (Pepper.tiff).

b) Output stego image.

Figure 6. Image histogram.

From the above table it is concluded that the picture quality of secret image is recognized at the minimum α value=0.008.

As the alpha factor increases, the stego image visual quality degrades and secret image picture quality also increases. Thus on the basis of above result value of alpha should not be more than 0.03.

On the basis of results it can be concluded that the value of α is in between 0.008< α <0.03, Hence here is a need to increase the PSNR, it can be achieved by applying k value at secret image.

Table 3 shows the change in results with variable secret image intensity for Stego Image (SI) and SIO image.

Table 3. Measurement of PSNR, MSE and NCC for Pepper.tiff (as cover image) and Name.jpg (as secret image) at variable K.

←Alpha(α)	Stego image(i.e.SI) before Smoothing operation						Stego image(i.e. SIO) after Smoothing operation inspired by GA					
	K= 1.2			K= 1.4			K= 1.2			K=1.4		
	PSNR	MSE	NCC	PSNR	MSE	NCC	PSNR	MSE	NCC	PSNR	MSE	NCC
.008	43.20	1.7060e+05	0.9877	44.56	1.2462e+05	0.9910	43.27	167735	0.9903	49.37	41202	0.9962
.009	42.17	2.1591e+05	0.9882	43.54	1.5772e+05	0.9899	43.21	170127	0.9902	43.31	166153	0.9904
.010	41.26	2.6656e+05	0.9876	42.62	1.9472e+05	0.9888	43.18	171385	0.9901	43.23	169239	0.9902
.02	35.24	1.0662e+06	0.9740	36.60	7.7887e+05	0.9777	36.59	781643	0.9779	36.68	764891	0.9783
.03	31.72	2.3990e+06	0.9613	33.08	1.7524e+06	0.9668	32.79	1871660	0.9658	34.41	1287697	0.9783

5. Comparison with the Previous Work

Tables 4 and 6 show the improvement in image quality (i.e., PSNR, NCC etc.,) as compared to the existing techniques [7, 13, 14].

Table 4. Comparison of PSNR and NCC with existing technique [13, 14], at alpha = 0.008 and variable secret image intensity (Here IWT stands for Integer wavelet Transform).

Cover image	Secret image	PSNR						NCC					
		Existing Techniques [13, 14]		Proposed Technique				Existing Techniques [13, 14]		Proposed Technique			
				Before Smoothing		After GA based smoothing				Before Smoothing		After GA based Smoothing	
		IWT Based	DWT Based	K=1	K=1.2	K=1	K=1.2	IWT Based	DWT Based	K=1	K=1.2	K=1	K=1.2
Flower.jpg 250 X 250	Pangram.jpg 864 X 540	40.29	34.18	42.17	43.72	44.04	44.15	0.9896	0.9698	0.9878	0.9898	0.9910	0.9913
Peppers.tiff 256 X 256	Pangram.jpg 864 X 540	___	33.77	41.77	43.32	43.39	43.50	___	0.9699	0.9878	0.9898	0.9905	0.9908
Lenna.tiff 256 X 256	Pangram.jpg 864 X 540	40.04	34.03	42.03	43.58	43.72	43.82	0.9889	0.9691	0.9875	0.9895	0.9903	0.9906
Pirate.tiff 512 X 512	Pangram.jpg 864 X 540	___	34.06	42.03	43.59	43.53	43.65	___	0.9667	0.9865	0.9887	0.9901	0.9904

Comparison of PSNR for IWT, DWT and daubechies (db8) DWT based technique is shown in Table 4. Here, it is observed that daubechies (db8) DWT gives better results as compared to other exiting techniques. The comparative study of PSNR under the different kind of attacks is shown in Table 5.

Table 5. PSNR of output stego Image for same secret image (i.e., Pangram.jpg) under different attacks.

Output Stego Image after attack	Image processing Attacks			
	Median filtering	Histogram Equalization	Gamma Correction	Gaussian attack
Pirate.tiff	27.34	25.42	29.35	21.69
Flower.jpg	29.65	25.25	30.46	22.77
Peppers.tiff	27.34	20.36	28.75	22.56
Lenna.tiff	27.01	22.38	28.96	22.69

Comparison of proposed techniques PSNR at different value of K (before smoothing and after GA based smoothing) with the existing technique [7], for different cover image and secret image is shown in Table 6.

Table 6. Comparison of proposed technique's PSNR with the existing technique [7].

Secret images (128X128) \ Cover image (256 X 256)				Peppers. tiff	Goldhill. jpg	Cameraman. jpg	Barbara. jpg
Homi Bhaba.jpg	Existing Tech.[7]			25.11	25.58	26.65	24.54
	Proposed Tech.	Before Smoothing	K=1	44.36	37.84	45.15	44.76
			K=1.2	45.94	39.42	46.73	46.34
		After GA based smoothing	K=1	45.00	45.80	45.86	45.63
			K=1.2	46.78	47.49	47.62	47.35
Airplane.png	Existing Tech.[7]			27.72	28.43	27.40	27.92
	Proposed Tech.	Before Smoothing	K=1	47.23	40.71	48.02	47.63
			K=1.2	48.81	42.29	49.59	49.21
		After GA based smoothing	K=1	48.53	49.46	49.33	49.23
			K=1.2	49.51	50.40	50.33	50.19
Redfort.jpg	Existing Tech.[7]			30.79	30.91	29.76	30.34
	Proposed Tech.	Before Smoothing	K=1	45.24	38.72	46.02	45.64
			K=1.2	46.81	40.29	47.60	47.21
		After GA based smoothing	K=1	46.51	47.53	47.24	47.26
			K=1.2	48.98	50.10	49.68	49.80
Bird.png	Existing Tech.[7]			30.36	30.20	28.61	30.13
	Proposed Tech.	Before Smoothing	K=1	46.46	39.94	47.24	46.86
			K=1.2	48.03	41.51	48.82	48.43
		After GA based smoothing	K=1	48.27	49.24	49.06	47.26
			K=1.2	49.30	50.22	50.09	49.80

After comparing the results of proposed technique with the results given in [7, 13, 14], our PSNR is much better than the technique given in [7, 13, 14] and our technique provides better NCC than the existing techniques [13, 14].

6. Conclusions

The proposed technique achieves the research objective better than existing techniques, such as, [7, 13, 14]. The proposed technique introduces:

a) Good embedding capacity.
b) Three levels of data protection (Arnold transform, daubechies (db8) DWT, Smoothing).
c) Better visual quality output stego image.

Therefore there is negligible chance to detect the secret image. Experimental result shows the resistance of proposed techniques.

References

[1] Ataby A. and Naima F., "Modified High Capacity Image Steganography Technique Based on Wavelet Transform," *The International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 358-364, 2010.

[2] Daisy M., Selvi S., and Prinza L., "Gray Scale Morphological Enhancement of Concealing Capacity and Operations for Image Retrieval," *in Proceedings of International Conference on Computing, Electronics and Electrical Technologie*, Kumaracoil, pp. 571-575, 2012.

[3] Das P., Dasgupta T., and Bhattacharya S., "A Novel Scheme for Bengali Handwriting Recognition Based on Morphological Operations with Adaptive Auto-Generated Structuring Elements," *in Proceedings of 2nd International Conference on Control, Instrumentation, Energy and Communication*, Kolkata, pp. 211-215, 2016.

[4] Fridrich J., Goljan M., and Du R., "Reliable Detection of LSB Steganography in Grayscale and Color Images," *in Proceedings of workshop on Multimedia and Security: New Challenges*, Canada, pp. 27-30, 2001.

[5] Hamdnaalla K., Wahaballa A., and Wahballa O., "Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithms," *International Journal of Video and Image Processing and Network Security*, vol. 13, no. 4, pp. 6-17, 2013.

[6] Jyoti and Sabir, "Genetic Algorithm Based Image Steganography for Enhancement of Concealing Capacity and Security," *International Journal Image, Graphics and Signal Processing*, vol. 5, no. 7, pp. 18-25, 2013.

[7] Kumar V. and Kumar D., "Performance Evaluation of DWT Based Image Steganography," *in Proceedings of IEEE 2nd International Advance Computing Conference*, Patiala, pp. 223-228, 2010.

[8] Mostafa H., Fouad A., and Taweal G., "Hybrid Curvelet Transform and Least Significant Bit for Image Steganography," *in Proceedings of IEEE 7th International Conference on Intelligent Computing and Information Systems*, Cairo, pp. 300-305, 2015.

[9] Pradhan A., Sahu A., Swain G., and Sekhar K., "Performance Evaluation Parameters of Image Steganography Techniques," *in Proceedings of International Conference on Research Advances in Integrated Navigation Systems*, Bangalore, pp. 1-8, 2016.

[10] Prabakaran G. and Bhavani R., "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform," *in Proceedings of International Conference on Computing, Electronics and Electrical Technologies*, Kumaracoil, pp. 1096-1100, 2012.

[11] Shrestha A. and Timalsina A., "Color Image Steganography Technique Using Daubechies Discrete Wavelet Transform," *in Proceedings of 9th International Conference on Software, Knowledge, Information Management and Applications*, Kathmandu, pp. 1-7, 2015.

[12] Saha B. and Sharma S., "Steganographic Techniques of Data Hiding using Digital Images," *Defence Science Journal*, vol. 62, no. 1, pp. 11-18, 2012.

[13] Sehgal P. and Sharma V., "Eliminating Cover Image Requirement in Discrete Wavelet Transform based Digital Image Steganography," *International Journal of Computer Applications*, vol. 68, no. 3, pp. 37-42, 2013.

[14] Sehgal P. and Sharma V., "Performance Improvement in Discrete Wavelet Transform Based Digital Image Steganography by the Use of Integer Wavelet Transform," *International Journal of Engineering Research and Technology*, vol. 2, no. 6, pp. 972-977, 2013.

[15] Subhedar S. and Mankar V., "Performance Evaluation of Image Steganography based on Cover Selection and Contourlet Transform," *in Proceedings of International Conference on Cloud and Ubiquitous Computing and Emerging Technologies*, Pune, pp. 172-177, 2013.

[16] Wang S., Yang B., and Niu X., "A Secure Steganography Method based on Genetic Algorithm," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 1, pp. 28-35, 2010.

Vijay Sharma completed M.Tech from RTU kota, India and B.Tech from Rajasthan Institute of Engineering and Technology, jaipur, India. Area of Research Biometrics, Computer Vision, Image Processing, Pattern Recognition, Information system security and Embedded system. Working with Rajasthan Institute of Engineering & Technology, Jaipur, India as a Assistant Professor, in CSE Department Honours and Awards:Published may papers in International Journals, International conferences, National journal and National conferences as; (SCI indexed), Springer conferences, IEEE conferences, and many other conferences etc. Reviewer: Journal of circuits, systems and computers, International Journal of Applied science and Engineering (Scopus indexed) Total teaching experience: more than 10 years to UG/PG (B. Tech., M. Tech. and MCA).

Devesh Srivastava completed Ph.D. from UTU Dehradun, India and M.Tech from AAI Allahabad, India. Current positions Professor in the Department of Deptt. of IT, Area of Research Software Engineering, Image Processing, Big data Published many papers in reputed journals and guided many Research scholars. Honours and Awards: Session chair in many international conferences. Total teaching experience: more than 15 Years, Classes taught: B.Tech. M.Tech and MCA.

Pratistha Mathur Completed Ph.D. from Banasthali Vidyapith in Digital image processing, and M.Tech in Computer science. Current positions Associate Professor, in the Department of Deptt. of IT, Area of Research Image Processing, Published many papers in reputed journals and guided many Research scholars. Total teaching experience: 18 Years, Classes taught: B.Tech. M.Tech.