

# Data and Image Hiding Using SWT and Arnold Transform

Aravall Saiganesh<sup>1</sup>, P Ratna Kamala<sup>2</sup>

<sup>1</sup>P.G Student, Department of ECE(DECS), SIETK, Puttur, Andhra Pradesh, India

<sup>2</sup>Professor, Department of ECE, SIETK, Puttur, Andhra Pradesh, India

## ABSTRACT

The data is added with some extra protection an method called digital water marking is used. In addition to RDWT and SVD is been used in this paper where the character or a format of string is been hidden in a layer of image. The locations were the watermark images are been found out by using entropy of the original image. The string hidden locations are obtained by changed entropy. The string and image present in binary format is been merged with Arnold chaotic map in order to increase security of the data.

**Keywords:** RDWT and SVD, Watermarking, Encoding

## I. INTRODUCTION

For present business trends, digital media plays a significant part and also there comes the need of securing the data/information from unauthorized personals. For achieving this, the secured Personal information should be embedded in to digital content which is conjoined by nature. This concept of protecting the information is called as watermarking. The key property of watermarking is its robustness to any kind of attacks which in turn makes it impossible to separate the watermark without disturbing or degrading content.. Digital watermarking, steganography and Reversible Data Hiding are methods used.

Data hiding is performed by some assistant, when the owner doesn't trust the assistant or an admin completely. Then this watermarking technique comes in to picture. Where an secret image is added in order to protect the copyright value provided by the owner . Where owner can add a concept of encryption where bits are added and now images are added. Encryption can defined as let's consider a sentence "there code is 100052" this is very

confidential which should be known only to two persons which is sender and receiver. Here sender adds some information using some algorithms and the sentence becomes 'thereacodeaisa1a0a0a0a5a2' or a by using a circuit called encoder. The same when the receiver uses the same encoded algorithm to remove the extra bits added here is the original data is obtained by using decoder circuit which performs the inverse operation of that of encoder.

When the owner performs watermarking the data whose owner ship remains non conflicts because only the owner knows the key to remove the watermark so the owner can provoke the copyright permission whom the owner owns the full copy right protection of the data or the picture.

## II. METHODS AND MATERIAL

### 2. Review of Literature

**Keshav S Rawat, Dheerendra S Tomar [1]:** the common facts of image water marking with respective digital which has the variation of red, blue and green in short the images are RGB images a very

compactable and very safe with respect to the copy rights and which is non editable CDMA water marking of images. Watermarking techniques can be done is some separate 8 colour lab format which eliminates odd part which is not clearly visible to the eyes.

**R. Zhang, Y. Wang [5]:** With DCT and HVS, a recurrence area picture watermarking calculation dependent on mapping standard in Total Auto orphism. Right off the bat, we mixed the first watermark picture with Arnold change. Besides, we changed the first transporter picture by discrete cosine change and picked some legitimate transitional recurrence coefficients dependent on human visual framework. Thirdly, the prepared watermark was inserted into these coefficients with spread-range system. At last, the watermark was removed by the visually impaired discovery and recouped by intermittent Arnold change, which could validate computerized works and ensure the copyrights. The calculation has the upsides of power and security with scrambling change and spread-range strategies, intangibility with HVS highlights.

**J. Abraham, V. Paul [3] :** Compressing an image can reduce three storage space in this paper the whole method is been described by setting threshold and some ideas of audio coding and resource allotment is been done. It deals with image frequency coding and local block alignment it deals with eliminating the degraded part present in the images where the unwanted components are removed to make the visual appearance nice as possible.

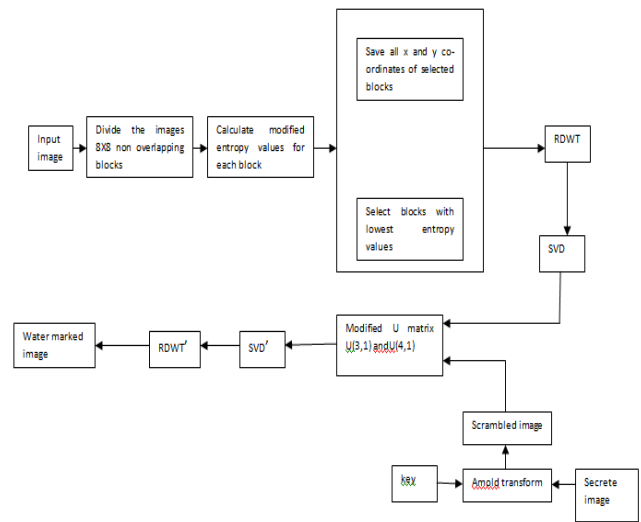
**III. Existing Method**

Comparing to domains it is classified in to spatial and frequency. LSB is purely referred to the spatial data. In that data, the pixel of values of the cover picture are processed by the watermarking bits. This method is easily implementable but very secure towards the

noise and unwanted information, in frequency domain inserted after the conversation, there are some of the frequency domain methods are like singular values decomposition ,lifting wavelet transformation(LWT) etc.

**3.1. Insertion Algorithm**

The technique of watermarking inserting is shown in below steps and figure water mark is placed in the U3,1 and U4,1 of the number 1st column of U. The relationship to deter mine the water marking place of bits is considered 0 or 1.



**Figure 1:** Block diagram for Watermark insertion

**3.1.1. Algorithm:**

**3.1.1.1. Pre-processing:**

- Step 1: A input image is sliced into 8 x8 blocks.
- Step 2: Calculate the modified entropy foe each and every block.
- Step 3: The blocks whose having lowest entropy values are selected and those coordinates were saved.
- Step 4: By using key and Arnold transform to provide more security for the secret image.

**3.1.1.2. Watermark Insertion:**

Step 5: LL sub band was selected by applying the RDWT to the selected lowest entropy values and apply SVD to that sub band.

Step 6: The below rules are used to add the watermark bits:

Rule 1: if the  $U_{3,1}$  or  $U_{4,1}$  are -ve values, then  $x = -1$ ,  $\alpha = -T$ , otherwise if the  $U_{3,1}$  or  $U_{4,1}$  are +ve, set  $x = 1$ ,  $\alpha = T$ . Then, calculate the average  $U_{3,1}$  and  $U_{4,1}$

$$m = \frac{|U_{3,1}| + |U_{4,1}|}{2}$$

Rule 2: if the watermark value =1,

$$U_{3,1} = x \cdot m + \alpha/2, U_{4,1} = x \cdot m - \alpha/2$$

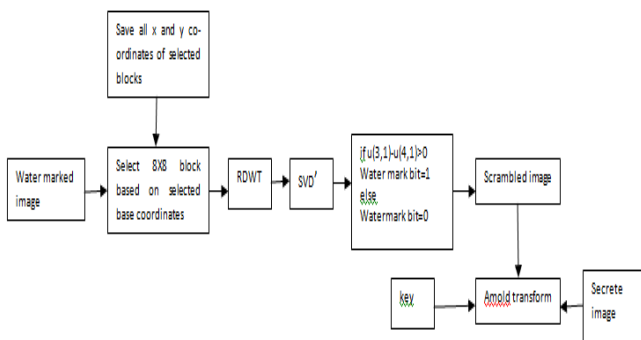
Rule 3: if the watermark value =0,

$$U_{3,1} = x \cdot m - \alpha/2, U_{4,1} = x \cdot m + \alpha/2$$

**3.1.1.3. Post-processing after embedding:**

Step 7: On each selected block, apply Inverse svd and inverse RDWT.

**3.2. Extraction Algorithm**



**Figure 2:** Block diagram for Watermark Extraction

**3.2.1. Algorithm:**

Step 1: The extracted watermark image is divided into 8 x 8 blocks.

Step 2: On each and every block apply first level RDWT.

Step 3: Select the LL sub band and apply the SVD .It decomposes into S,V,D.

**3.2.2. Watermark extraction:**

Step 4:  $U_{3,1}$  and  $U_{4,1}$  are used to calculate the watermark data values using a rule as follows:

If  $|U_{3,1}| - |U_{4,1}| > 0$ , then set the watermark bit =1, else the watermark bit = 0.

**3.2.3. Post-processing:**

Step 5: Then Applying the inversed Arnold method of transformation and key whatever given in the insertion process for extracting the watermark.

**IV. Proposed Method**

In spatial domain, LSB correlation based methods are preferred. The input image where the pixel values are placed by watermark data's in spatial domain. The implementation is easy but not robust towards attacks; frequency domain techniques embed the watermark to image after transformation. Generally used frequency domain techniques are discrete cosine transformation (DCT), Discrete Wavelet Transformation (DWT), Lifting Wavelet Transformation (LWT), Discrete Fourier Transformation (DFT) and Singular Values Decomposition(SVD).

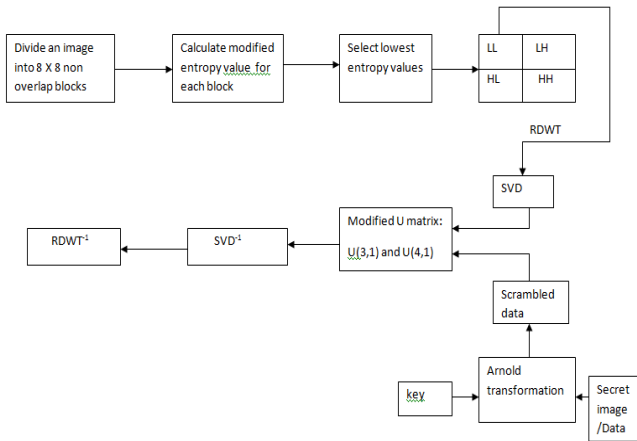


Figure 3: Block diagram for insertion Process

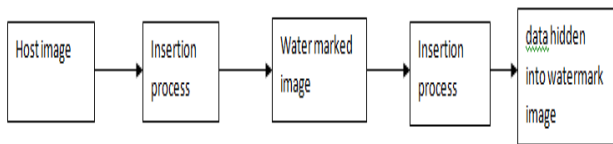


Figure 4: Data is hidden into watermark image

4.1. Watermark Insertion process:

The following are the details of the algorithm

4.1.1. Algorithm: Procedure for inserting Watermark

4.1.1.1. Pre-processing:

- Step 1: An input image is sliced into 8 x8 blocks.
- Step 2: Calculate the modified entropy for each and every block.
- Step 3: The blocks that's having lowest entropy values are selected and those coordinates were saved.
- Step 4: By using key and Arnold transform to provide more security for the secret image.

4.1.1.2. Watermark Insertion:

Step 5:LL sub band was selected by applying the RDWT to the selected lowest entropy values and apply SVD to that sub band.

Step 6: The following rules are used to embed the watermark bits:

Rule 1: if the  $U_{3,1}$  or  $U_{4,1}$  coefficients are negative values, then  $x = -1$ ,  $\alpha = -T$ , otherwise if the  $U_{3,1}$  or  $U_{4,1}$  coefficients are positive, we set  $x = 1$ ,  $\alpha = T$ . Then, calculate the average  $U_{3,1}$  and  $U_{4,1}$  Coefficients

$$m = \frac{|U_{3,1}| + |U_{4,1}|}{2}$$

Rule 2: if the binary watermark bit =1,

$$U_{3,1} = x \cdot m + \alpha/2, U_{4,1} = x \cdot m - \alpha/2$$

Rule 3: if the binary watermark bit =0,

$$U_{3,1} = x \cdot m - \alpha/2, U_{4,1} = x \cdot m + \alpha/2$$

Step 7: On each selected block, apply Inverse svd and inverse RDWT.

Step 8: Consider watermarked image as input for string hiding.

Step 9: Repeat Step 1,2,3,4 for the watermark image. Convert the string into ASCII values and length of the string.

Step10: Repeat the steps 5,6,7 for data hiding.

4.2. Watermark extraction process:

The block diagram for watermark extraction is as follows:

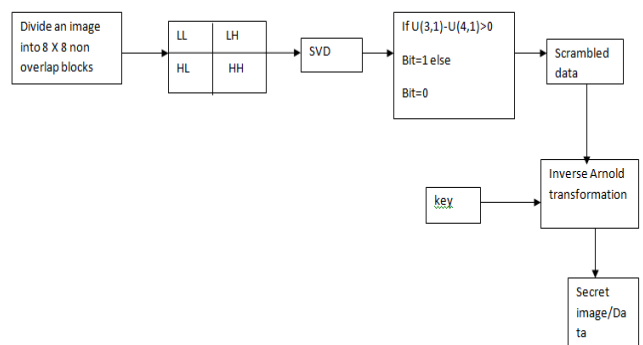


Figure 5: Extraction process

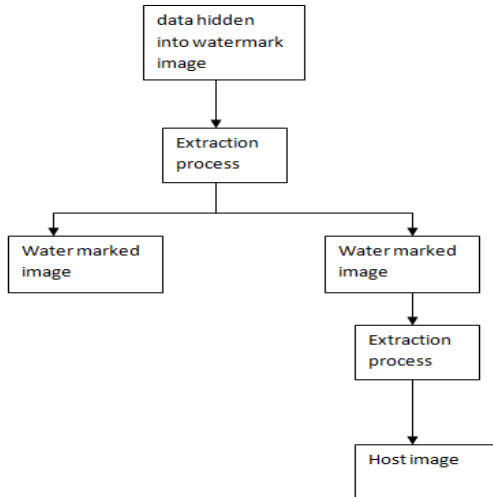


Figure 6: Data and image extraction

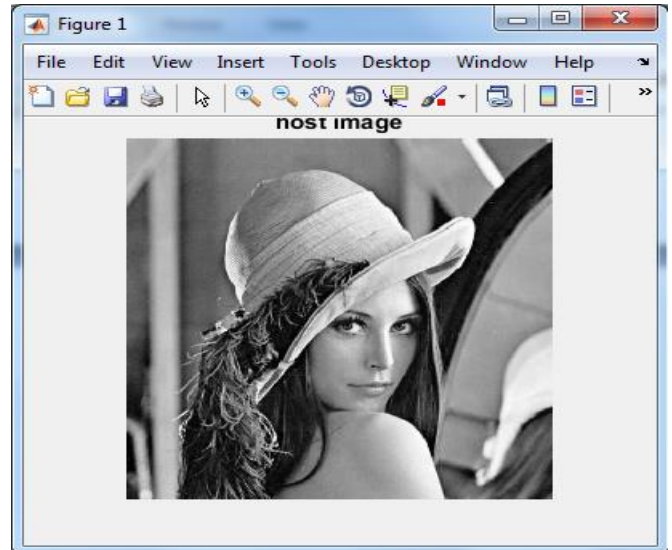


Figure 7: Host image

4.2.1. Algorithm:

Step 1: The extracted image were watermark is added is sliced into 8 x 8 blocks.

Step 2: On each and every block apply first level RDWT.

Step 3: select the LL sub band and apply the SVD .It decomposes into S,V,D.

Step 4:  $U_{3,1}$  and  $U_{4,1}$  coefficients are used to determine the watermark bits using a rule as follows: If  $|U_{3,1}| - |U_{4,1}| > 0$ , then set the watermark bit =1, else the watermark bit = 0.

Step 5: After that apply inverse Arnold transform and key whatever given in the insertion process for extracting the watermark.

Step 6: repeat the step 1 to step 5 to recover the secret image.

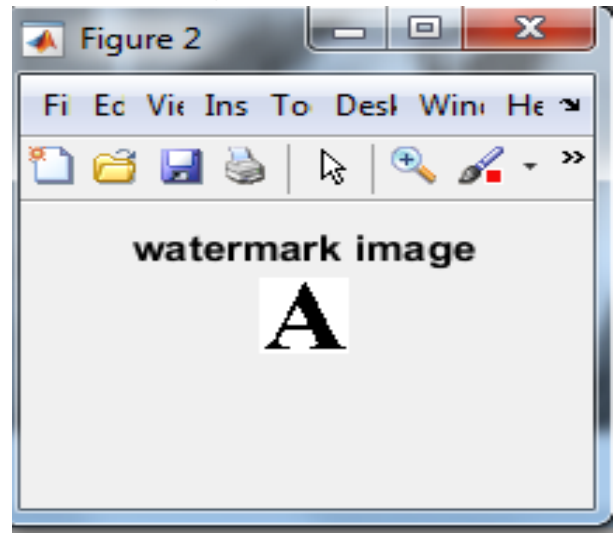


Figure 8: Watermark image

V. RESULTS AND DISCUSSION

The MATLAB simulated results are shown in below figures.

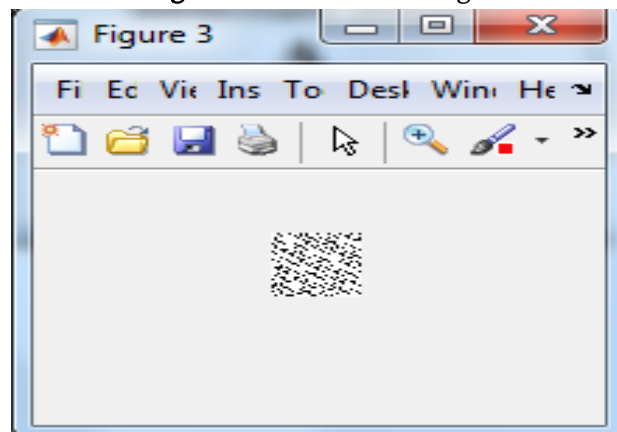


Figure 9: Scrambled image

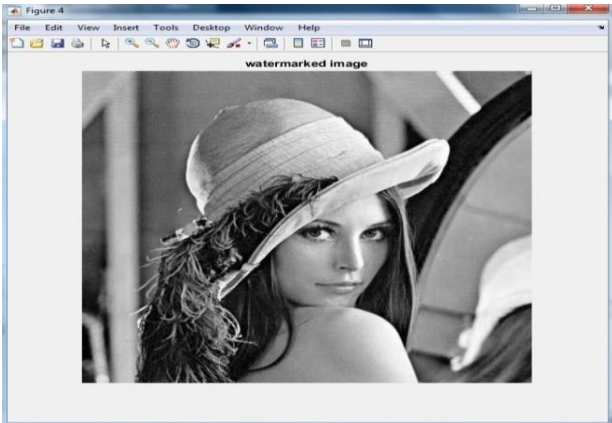


Figure 10: Watermarked image

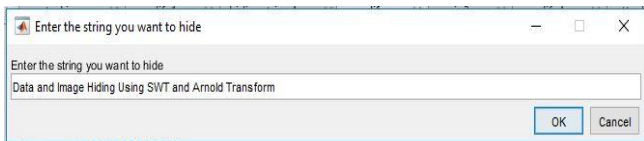


Figure 11: String insertion

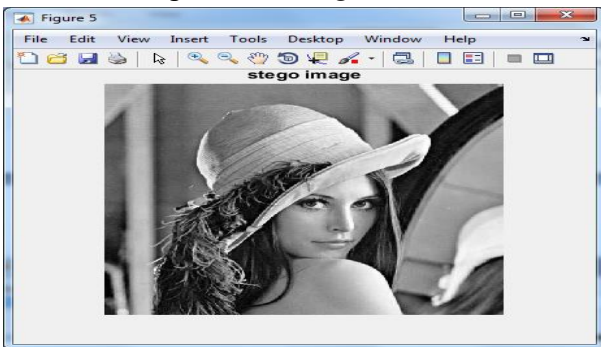


Figure 12: Stego image

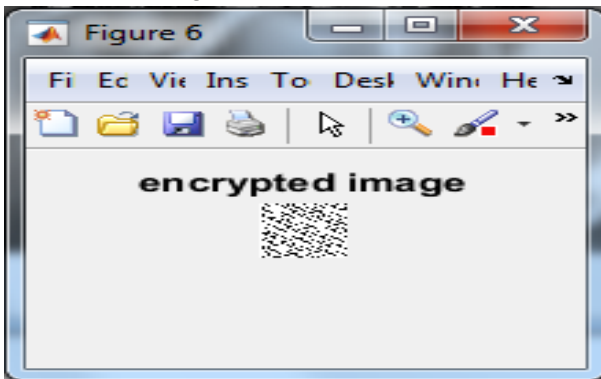


Figure 13: Descrambled image

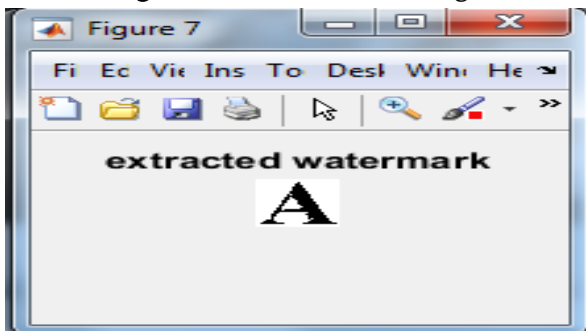


Figure 14: Extracted watermark image

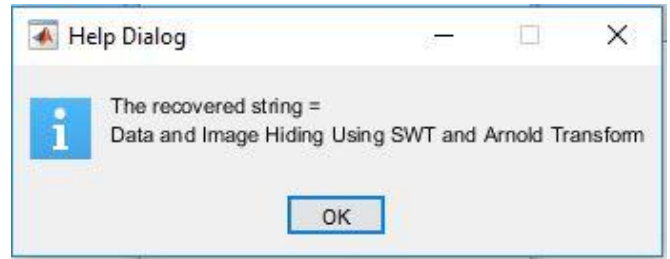












Figure 15: Recovered string

COMPARISION TABLES:

PSNR and visual perception of test image1Stego images for different threshold values. PSNR values are used to find the quality of the image. PSNR represents a measure of the peak error. The typical psnr values[8] are 38dB to 50dB.

Table 1: PSNR values for original image and stego image for different threshold values

Threshold	Original image	Stego image	PSNR
T=0.055			46.1194
T=0.04			48.2907
T=0.02			51.7529
T=0.01			53.4894
T=0.001			54.0990

**SSIM:**

SSIM values of Watermarked image and Stego image for different threshold values are shown below[9]. The structural similarity (*SSIM*) index is a method for predicting the perceived quality of digital television and cinematic *pictures*, as well as other kinds of digital *images* and videos. The resultant *SSIM* index is a decimal *value* between -1 and 1, and *value* 1.

**Table 2:** SSIM values for watermarked image and stego image for threshold values

Threshold values	SSIM of Watermarked image		SSIM of Stego Image	
	Test image1	Test image2	Test image1	Test image2
T=0.055	0.9885	0.9747	0.9885	0.9747
T=0.04	0.9935	0.9848	0.9935	0.9848
T=0.02	0.9980	0.9959	0.9980	0.9959
T=0.01	0.9992	0.9986	0.9992	0.9986
T=0.001	0.9997	0.9998	0.9997	0.9998

**Entropy**

Entropy is the average (expected) amount of information in a certain event. The range of entropy for normal image is 0 to 1.

**Mean and Variance**

'Mean' value gives the contribution of individual pixel intensity for the entire image & 'Variance' is normally used to find how each pixel varies from the neighbouring pixel (or centre pixel) and is used in classify into different regions.

**Table 3:** Mean and variance values for the original image for different threshold value

Threshold Value	Original image		
	Entropy	Mean	Variance
T=0.055	7.7608	111.7894	3.7344e+03
T=0.04	7.7608	111.7894	3.7344e+03
T=0.02	7.7608	111.7894	3.7344e+03
T=0.01	7.7608	111.7894	3.7344e+03
T=0.001	7.7608	111.7894	3.7344e+03

**Table 4:** Mean and variance values for the watermarked image for different threshold value

Threshold Value	Watermarked image		
	Entropy	Mean	Variance
T=0.055	7.7652	111.7885	3.7342e+03
T=0.04	7.7640	111.7890	3.7336e+03
T=0.02	7.7621	111.7892	3.7330e+03
T=0.01	7.7614	111.7894	3.7328e+03
T=0.001	7.7608	111.7895	3.7327e+03

**Table 5:** Mean and variance values for the Stego image for different threshold value

Threshold Value	Stego image		
	Entropy	Mean	Variance
T=0.055	7.7652	111.7885	3.7342e+03
T=0.04	7.7640	111.7890	3.7336e+03
T=0.02	7.7621	111.7892	3.7330e+03
T=0.01	7.7614	111.7894	3.7328e+03
T=0.001	7.7608	111.7895	3.7327e+03

**VI. CONCLUSION**

Finally a watermarking method which is added with RDWT and SVD for protecting copy of images which is called copyright. We use the modified entropy to calculate the watermarked region with low noise and to secure the data which is confidential where this method provides very high data security.

## VII. REFERENCES

- [1] Keshav S Rawat, Dheerendra S Tomar “Digital Watermarking Schemes of Color Images” in Indian Journal of Computer Science and Engineering.
- [2] Vidyasagar M. Potdar, Song Han, Elizabeth Chang “A Survey of Digital Image Watermarking Techniques” in 3rd IEEE International Conference on Industrial Informatics (INDIN) in 2005.
- [3] J. Abraham, V. Paul, "Image watermarking using DCT in selected pixel regions", IEEE International Conference on Control Instrumentation Communication and Computational Technologies (ICCICCT), pp. 398- 402, 2014.
- [4] S. Rawat, B. Raman, "A New Robust Watermarking Scheme For Color Images", IEEE 2nd International Advance Computing Conference, pp. 206-209, 2010.
- [5] R. Zhang, Y. Wang, “Scrambling image watermark algorithm based on DCT and HVS,” International Conference on Information Technology and Applications, Nov. 2013, pp. 54-57.
- [6] Claypoole, R. L., Baraniuk, R. G., Nowak, R. D.: Adaptive wavelet transforms via lifting. In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Seattle, WA, pp. 1513-1516 (1998).
- [7] Radhika G. Kabra and Sushma S. Agrawal, “Robust embedding of image watermark using LWT and SVD” in IEEE International Conference on Trends in Electronics and Informatics ICEI 2017 978-1Conference on Communication and Signal Processing, pp 1968 1972, 2016.
- [8] Chia-Sung Chang, Jau-Ji Shen, ‘Features Classification Forest: A Novel Development that is Adaptable to Robust Blind Watermarking Techniques’ Published in IEEE Transactions on Image Processing 2017, Volume: 26 , 3921-3935, Aug. 2017.
- [9] C. Yim, A.C. Bovik, “Quality assessment of deblocked images,” IEEE Transactions on Image Processing, vol. 20, no. 1, pp. 088-098, 2011.

### Cite this article as :

Aravall Saiganesh, P Ratna Kamala, "Data and Image Hiding Using SWT and Arnold Transform", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 281-288, May-June 2019. Journal URL : <http://ijsrcseit.com/CSEIT195353>