A Secure and Robust DWT based Digital Image Watermarking Technique

Swati Saxena
M.Tech Scholar
Technocrats Institute of Technology – Advance, Bhopal (MP)

Pankaj Soni
Professor
Technocrats Institute of Technology – Advance, Bhopal (MP)

Manish Gurjar
Professor
Technocrats Institute of Technology – Advance, Bhopal (MP)

ABSTRACT
Due to the tremendous growth of internet, the web may produce huge information in digital form. The information may be in the form of numbers, strings, images, and video. If the data to be transmitted are confidential, it is suitable as well for some mischievous users to illegitimately destroy, copy, or change them on the Internet. As a consequence, information security becomes an essential issue. Security and robustness are two important requirements for digital image processing algorithms in applications involving authentication.

In this method, we proposed digital image watermarking technique to improve the PSNR value. Our experimental result showed that method is well suited for unauthorized tempering detection. We used watermarking for secure data transmission and to prevent unauthenticated image access. We applied Discrete Wavelet Transform technique to compress the image with better compression ratio and low processing power. Our method detected the image tempering and data can be transmitted securely over the channel.

Keywords
Digital image, Security, Watermarking, Discrete Wavelet Transform, PSNR, MSE.

1. INTRODUCTION
Watermarking is used to verify the identity and authenticity of the owner of digital image .watermarking procedures are extensively used in the prevention of image against tampering. The DWT represents an image as a sum of wavelet function, kwons as wavelet, with different location and scale .Discrete cosine transform (DCT) is extensively used in image processing, particularly for image and video compression procedure decoding and encoding. DWT gives better compression ratio without losing more information of image but it needs more processing power.

2. PROPOSED WORK

2.1 Proposed step
Step 1: Select image from database
Step 2: Apply DWT techniques
Step 3: Watermark embedding
Step 4: Image compression algorithms
Step 5: Image tempering detection
Step 6: Message decryption
Step 7: Image recovery
The first step in our algorithm is to select an image from image database. The next step is to apply DWT technique to the image.

2.2 Encoding system steps
Step 1: First original source image have to been passed through high pass filter and low pass filter by applying filter on each row.

Step 2: now output of the both image l_1 and h_1 are combining into $t_1 = [l_1\ h_1]$.

Step 3: T_1 is down sampled by 2.

Step 4: Now, again T_1 has been passed through high pass filter and low filter by applying on each column.

Step 5: Output of the step4 is supposed l_2 and h_2. Then l_2 and h_2 is combine into $t_3 = [l_2\ \ h_2]$

Step 6: Now down sampled t_3 by 2.This is our compressed image.

2.3 Decoding system steps
Step 1: Extract low pass filter image and high pass filter image from compressed image simply by taking upper half rectangle of matrix is low pass filter image and down half rectangle is high pass filter image

Step 2: Both images are up sampled by 2.

Step 3: Now we take the summation of both images into one image called r_1.

Step 4: Then again extract low pass filter image and high pass filter image by simply dividing vertically. First half is low pass filtered image. And second half is high pass filter image.

Step 5: Take summation of both images that is out reconstructed image. The next step is to embed watermark into the source image.

Now image compression algorithm is applied to compress the image. The next step is to detect any tempering in image. The next step is to decrypt the desired message. If any tempering is done in the original image then recovery operation is performed to recover original image.

3. IMPLEMENTATION OF PROPOSED METHOD
For implementation, we have used core i5 3.0 GHz processor speed, 8 GB RAM, 1 TB Hard disk. We have used MATLAB programming language for implementation of proposed work. MATLAB is widely used programming environment for image processing.

The parameters used in proposed system is PSNR, embedding capacity, MSE.

PSNR (Peak Signal to Noise Ratio) is defined as follows:

$$\mathbf{PSNR = 10log_{10}\ 255^2 / MSE}$$

Where MSE (Mean Square Error) stands for the mean-squared difference between the cover-image and the stego-image. The mathematical definition for MSE is:

$$MSE = (\frac{1}{M \times N})\sum_{i=1}^{M}\sum_{j=1}^{N}(a_{ij} - b_{ij})^2$$

Embedding capacity represent the size of the data can be embedded into original image.

Cameraman image of size 512 × 512 8-bit gray scale is watermarked using our proposed method explained as shown in fig (1)

Fig 1: Image to be hidden

Fig 2: Original Image

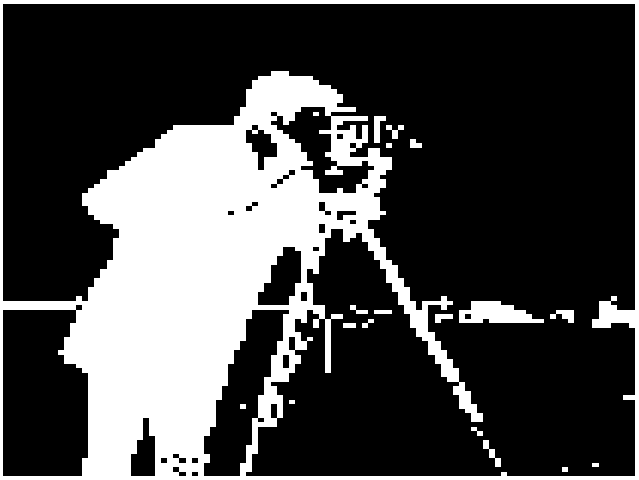

Fig 3: Hidden Image Threshold at 70

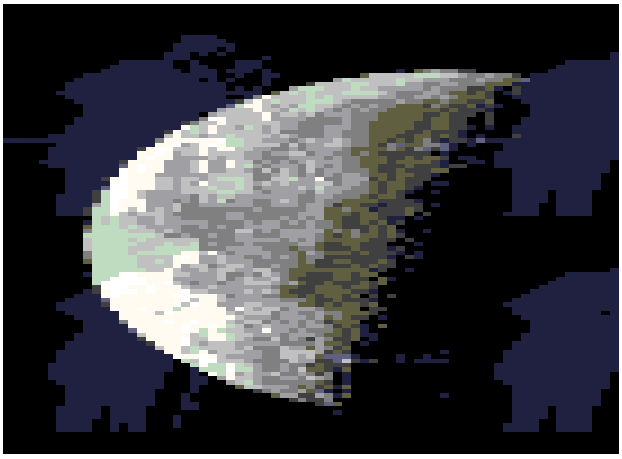

Fig 4: Final watermarked image

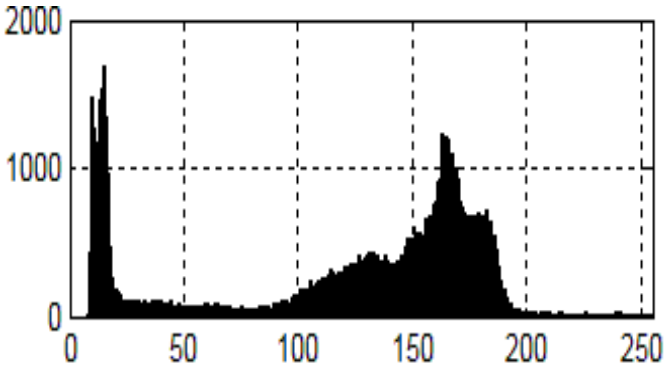

Fig 5: Histogram of image to be hidden

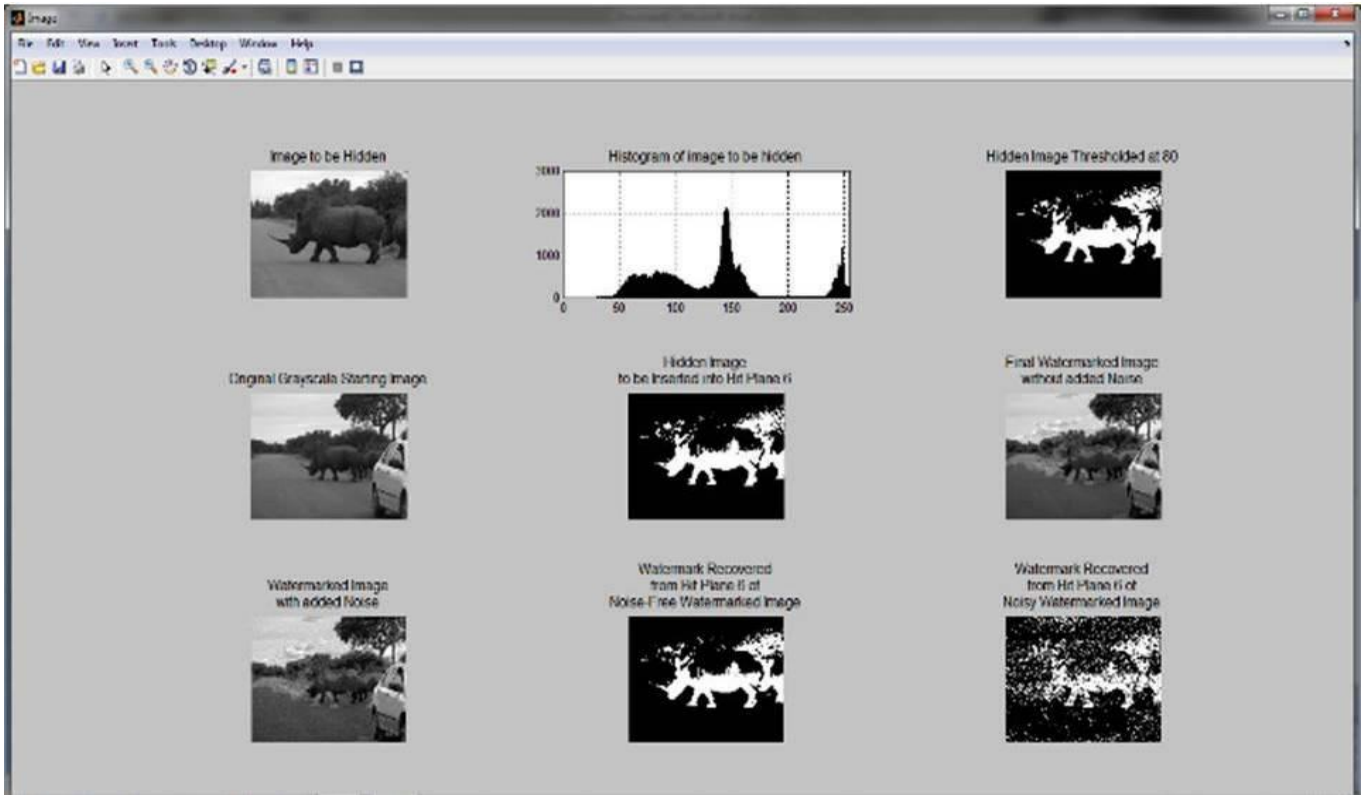

Fig 6: The result for threshold 80 and Rhino Image data set.

After executing program using our proposed method we get the PSNR value 45.5dB and MSE value 6.31. Rhino image of size 512 × 512 8-bit gray scale is watermarked using our proposed method explained.

RESULTS / IMAGES	MSE	PSNR
FIGURE 1	11.7807	65.9482
FIGURE 2	15.7041	41.9752
FIGURE 3	13.8529	51.9481

Fig 7: MSE and PSNR values for different data set.

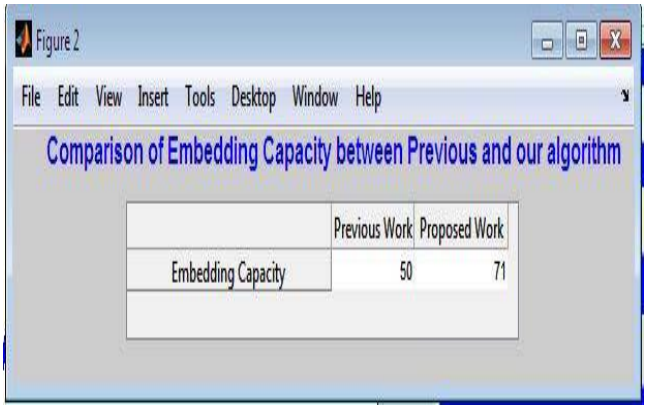

Fig 8: Embedding capacity

The PSNR and MSE values for different dataset are given in above figure. PSNR values of our method are improved as shown in figure above. The figure above showed that embedding capacity is increased in our method.

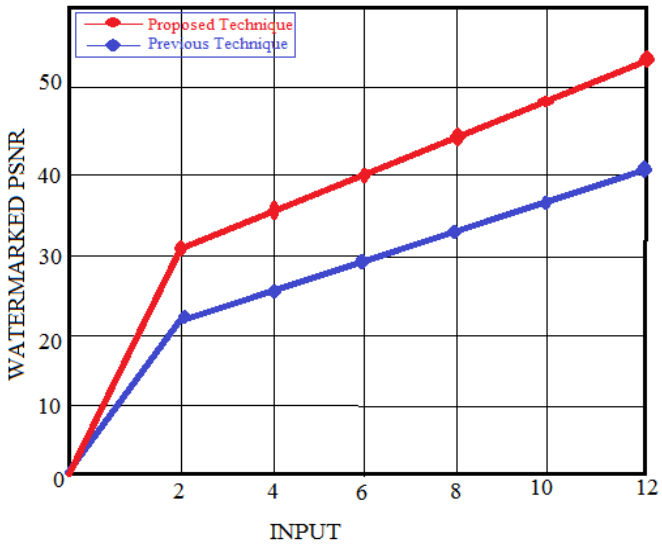

Fig 9: The PSNR values of proposed and previous technique

We have applied our implementation at different databases. The PSNR value generated by first database is 44.94, second database is 42.9752 and from third database is 43.94 respectively. Similarly the MSE values we got from different databases are 11.7808, 15.70, and 13.8529 respectively. From experimental results our embedding capacity is also improved

to 71. The graph represented the PSNR comparisons of our technique and previous technique are shown in Table 1 below:

Table1: Comparison PSNR

Parameters	Proposed method PSNR	Base paper Method PSNR
For k=3	44.30	42.51
For k=5	43.10	40.32

4. RESULT & CONCLUSION

Watermarking procedures have been extensively used in the image and video forensics. Security and robustness and are two important requirements for digital image processing algorithms in applications involving authentication, watermarking, and image databases.

Our method detected the image tempering and data can be transmitted securely over the channel. Our experimental result shows that method is well suited for unauthorized tempering detection. We used watermarking for secure data transmission and to prevent unauthenticated image access.

We applied Discrete Wavelet Transform technique to compress the image with better compression ratio and low processing power. Our proposed work will apply discrete wavelength transform technique to compress the image with better compression ratio and low processing power. We proposed a novel method using watermarking and steganography to improve the PSNR value. Our method improved the message hiding capacity, peak to signal ratio and mean square error.

5. REFERENCES

[1] Tianrui Zong1, Yong Xiang1, Song Guo2 and Yue Rong "Rank- Based image watermarking method with high embedding capacity and robustness" IEEE Trans. Image process, vol.4, pp.2169-3536, May 2016.

[2] A.Swaminathan, M. Wu ana, K.J.R Liu, "Digital image forensics via intrinsic Fingerprint" IEEE Trans.inf. Forensics Security, vol.3, no.1, pp.101-117, March 2008.

[3] X. B. Kang and S. M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Proc. Int. Conf. Comput. Sci. Softw. Eng., vol. 3. Dec. 2008, pp. 926–930.

[4] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[5] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE Trans. Image Process., vol. 10, no. 10, pp. 1593–1601.

[6] J. Lee and C. S. Won, "Authentication and correction of digital watermarking images," Electron. Lett., vol. 35, no. 11, pp. 886–887, 1999.

[7] D. Kumar and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," Proc. IEEE, vol. 87, no. 7, pp. 1167–1180, Jul. 1999.

[8] J. Fridrich, "Image watermarking for tamper detection," in Proc. Int. Conf. Image Process. (ICIP), vol. 2. Oct. 1998, pp. 404–408.

[9] P. W. Wong, "A public key watermark for image verification and authentication," presented at the IEEE Int. Conf. Image Processing, Chicago, IL, 1998.

[10] S. D. Servetto, C. I. Podilchuk, and K. Ramchandran, "Capacity issues in digital image watermarking," presented at the 5th IEEE Conf. Image Processing, 1998.

[11] D.Kunder and D. Hatzinakos, "Digital watermarking using multi resolution wavelet decomposition" Proc. IEEE int conf, Acostics, Speech, and signal processing, vol.5 pp.2969-2975, 1998.

[12] A.B Watson, G.Y Yang, J.A.Solomon and J.Villasenor "Visibility of wavelet quantization noise," IEEE Tran image processing, vol.6, pp.1164-1175, 1997.

6. AUTHOR PROFILE

Ms. Swati Saxena has received her Engineering degree in Electronics & Communication in June 2012 from Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, (M.P.) India and currently pursuing Master of Technology degree in Digital Communication from Technocrats Institute of Technology- Advance under Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, (M.P.) India.

Prof. Pankaj Soni has received his Engineering degree in June 2008 and Master of Technology degree in Dec 2012 from Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, (M.P.) India. He is currently working as Professor in department of Electronics & Communication in Technocrats Institute of Technology- Advance, Bhopal, (M.P.) India. He has five years teaching experience. He has published 8 international research papers. His research interest is in Digital Communication, Wireless Communication and VLSI Design.

Prof. Manish Gurjar has received his Engineering degree in June 2003 and Master of Technology degree in Dec 2012 from Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, (M.P.) India. He is currently working as Professor & Head in department of Electronics & Communication in Technocrats Institute of Technology- Advance, Bhopal, (M.P.) India. He has five years teaching experience. His research interest is in Digital Communication, Wireless Communication.