Table 3: Repaired image quality parameters Grayscale Image for text attack

| Image Quality Parameter Grayscale Image | Values |
|---|---|
| PSNR in dB | 55.5631 |
| MSE | 0.159996 |
| NCC | 1.00017 |
| SC | 0.999651 |
| AD | 0.03228 |

## 5. Conclusion

The algorithms developed for authentication of grayscale image embeds authentication data in the host file rather than in a separate data file. If authentication data embeds in a separate data file and if it is lost due to manual mistakes then it's a huge loss. In this case no one can check whether given image is authentic or not. This embedding approach increase complexity at the authentication checking. The developed algorithms embeds authentication data in alpha channel not in the grayscale image pixel. This embedding approach in an alpha channel keeps grayscale image or color image pixels unchanged. The results shows the quality of the stego image after embedding authentication data is high. The developed algorithms embeds authentication data in an alpha channel. Alpha channel produces transparency effect to the image. Authentication data is embedded into the alpha by using bitplane slicing in the highest bitplanes to reduce the opaque effect visible in the stego-image. The opaque effect visible in the stego-image when authentication data embedded into the lower bitplanes of an alpha channel. There are only few techniques in the research which works for authentication and data recovery of grayscale image. Most of the techniques in the literature embeds binary like data to check authenticity and for recovery. The proposed techniques embed five bitplanes of grayscale image in an alpha channel. These five bitplanes has highest information of the grayscale image. At the time of authenticity checking and recovery, maximum grayscale data is repaired. The result shows the quality of repaired image is 90%.

## *References*

[1] Rafeal Gonzalez et al., "Digital image processing", *3rd edition, published by Pearson India Education services Pvt Ltd, 2016.*

[2] Anand, A., Raj, A., Kohli, R., & Bibhu, V., "Proposed symmetric key cryptography algorithm for data security", *International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), pp. 159-162, 2016.*

[3] Omar Farook Mohammad et al., "A Survey and Analysis of the Image Encryption Methods", *International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, pp. 13265-13280, Number 23, 2017.*

[4] H. B BasanthKumar, "Digital Image Watermarking: An Overview", *Oriental Journal of Computer Science & Technology, Vol. 9, No. (1): pp. 07-11, April 2016.*

[5] Naina Choubey and Mahendra Kumar Pandey, "Transform based Digital Image Watermarking: An Overview", *International journal of Computer Trends and Technology (IJCTT), 24(2); pp. 80-83, 2015.*

[6] R. English, "Comparison of High Capacity Steganography Techniques *", IEEE, International Conference of Soft Computing and Pattern Recognition, pp.448-453, December 2010.*

[7] H. Sajedi, and M. Jamzad, " Secure steganography based on embedding capacity *", Springer Verlag, International Journal of Information Security, Vol.8, Issue 6, pp.433-445, August 2009.*

[8] T. Morkel, " Image Steganography Applications for Secure Communication ", *M.Sc. thesis, Faculty of Engineering, Built Environment and Information Technology University of Pretoria, Pretoria, pp.126-132, May 2012.*

[9] Y. Lee, H. Kim, and Y. Park, "A new data hiding scheme for binary image authentication with small image distortion", *Inf. Sci., vol. 179, no. 22, pp. 3866–3884, Nov. 2009.*

[10] H. Yang and A. C. Kot, "Pattern-based data hiding for binary images authentication by connectivity-preserving", *IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475–486, Apr. 2007.*