VOL. 13, NO. 21, NOVEMBER 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

NEW STATISTICAL STEGANOGRAPHY METHOD TO HIDE INFORMATION IN IMAGE WITH HIGH ROBUSTNESS AGAINST JPEG ATTACK

Mohammed Kamal and Hameed M. Abduljabbar
College of Education for Pure Science Ibn Al-Haitham, University of Baghdad, Iraq
E-Mail: mohammed1985kamal@gmail.com

ABSTRACT

New statistical steganography method (NSSM) to override or reduce the effect of JEPG attack on a cover image is presented in this work. The new method based on an analysis of the JPEG algorithm, in which it uses the value of the mean and the standard deviation of each cover blocks to embed the secret message, where the cover image blocks calculated in the same manner of the JPEG algorithm. Two standard images that differ in their amount of texture (Lena and The Baboon images) are used to test the new method; an analysis and discussion are presented for the results of applying this method which proved the validity of this method to override the JEPG attack.

Keywords: steganography, stego-image, new statistical, JPEG attack. image quality.

INTRODUCTION

Securing the transpose of information with high security and protection to avoid exposing it to unwanted a terminal, is one of the great interest subjectsfor many centuries (Ibadi & Akif, 2010). The development and progress in the field of computer and internet, the security of information exchange become one of the most important issue (Cheddad, 2009)(Chanu, *et al.*, 2012), where there are two main techniques to achieve secure information exchange, which are encryption and steganography. In the first technique, the message is transformed to un-readable form to ensure the secure delivering of the message but it will be obvious that the message is important, while the other technique hide the message into another media in a way that it is very hard to predict that it contains a message in it (Al-Towayjri, 2003)(Al-Sudany, 2006).

Steganography is a preferable way to deliver a secure message between two partnerssince it uses another electronic media such as [image, text, audio and video] as a cover to embed the secret information (Sravanthi, et al., 2012)(Barán, *et al.,* 2001)(Abboud, *et al.*, 2010). Historically, Steganography word origin Greek and it means the conceal writing, where steganography composed from two-part, the first part ‘stegano’ it means the "covered or conceal" and the second part ‘graphein’ it means, "Write"(Cheddad, 2009)(Rana, *et al.*, 2012).There are many techniques of steganography such as spatial domain, transform domain, statistical, distortion(Cheddad, *et al.*, 2010), etc. In this work, we propose to use a new method to hide the secret data inside the grey image.

To prevent transmitting secret message using one of the steganography methods, usually there are many counter-managements are applied when the controller suspect that the media may contain a secret message, the standard protocol in case of using an image as a cover media is to attack it using a lossy compression method such as JPEG algorithm and transform it back its original image format before the attack where this procedure has a catastrophic effect on the hidden message(Currie III & Irvine, 1996) (Kamal & Abduljabbar, 2018).

The basic idea of the new statistical method is very similar to the JPEG algorithm where the cover is divided into blocks and maintain the mean of image intensity.

In general, there are three important objectives for steganography: robustness, undetectability and storage capacity (Sabnis & Awale, 2016)(Krutz, 2003)(Nadiya & Imran, 2013). By analyzing the JPEG algorithm, in this research a new steganography method is presented to reduce or override the effect of JPEG attack on the cover image, this new method is designed to have high robustness and undetectability but with low storage.

The are many researchers try to propose robust steganography method, as follow: In 2011, R. Yadav, *et al.*,(Yadav, *et al.*, 2011) proposed hiding the secret information within the grayscale image, where, the image is divided into blocks uniformly. The secret message is embedding into blocks by the cyclic combination of (6,7,8) bit. In 2012, D. Singla, *et al.*, (Singla & Syal, 2012) proposed a new steganography method based on LSB & DCT techniques for hiding the data. where the secret message's bits are embedding by change the least significant bit of low-frequency DCT coefficients of cover image blocks. In 2017, M. Kalita, *et al.*, (Kalita, *et al.,* 2017) suggested a new method of image steganography based on (LSB) &neighbouring pixel pair difference (PPD) value. the cover-image is divided into blocks (3×3) pixel, where embed one bit of message within the centre of the block.

The goal of this paper is calculated how strong and robust of the new steganography statistical method to survive from attack using JPEG algorithm.

RESEARCH METHODOLOGY

The proposed algorithm designed and works as follow:

a) Divided the cover-image into blocks.

b) Each block consists of (8x8) pixel compatible with the JPEG algorithm.
c) One of the (8x8) block pixels is reserved, in this research is the centre pixel.
d) Calculating the mean value of each block without the contribution of the centre pixel.
e) Calculating the standard deviation (STD) value of each block without the contribution of the centre pixel.
f) Determine the threshold value for the STD to select the block as a valid location to embed the message's bit.
g) Replace the marked pixel by the modified mean value (V_n) depending on the value of the planted message's bit, as in equation (1).
h) In (DIF=1), If bit value equal one, add standard deviation value to mean value

Either, if bit value equal zero subtract standard deviation value from the mean value.

$$V_n = \begin{pmatrix} \mu+\omega\sigma if message bit=1 \\ \mu+\omega\sigma otherwise \end{pmatrix} \quad (1)$$

Where:

V_n The new value for the centre block pixel
ω The difference factor ($\omega > 0$)
μ The mean value of each block without the contribution of the centre pixel
σ the standard deviation (STD) value of each block without the contribution of the centre pixel

In order study the effect of JPEG attack on the embedded message in the stego-image, we suggest the following steps:

a) Select the cover-image (Grayscale)
b) Select the secret message (ASCII).
c) Embed one bit of the secret message within one block of the cover-image with different difference value (DIF=1-25)
d) Perform JPEG Attack on stego-image (using Irfan view graphics viewer) with compression quality ranging between [50-100].
e) Calculate the cover-image quality after applying the proposed algorithm and after the JPEG attack.
f) Calculate the retrieved message's quality after JPEG attack, by finding the error percent of the affected bytes.

RESULTS AND DISCUSSIONS

The texture factor of the cover image is an important factors that effects on the steganography methods, therefore, two standard images are considered as sample images, which are Lena and the Baboon images. The first image represents a moderate texture image and the other represents a high texture image, see Figure-1.

(a) (b)

Figure-1. The Sample 512×512 images for (a) Lena (b) The Baboon.

The NSSM applied to embed an ASCII code message. Figure-2, illustrates the cover quality after embedding the message by using two different values of STD as a threshold values which 0.5 and 1.

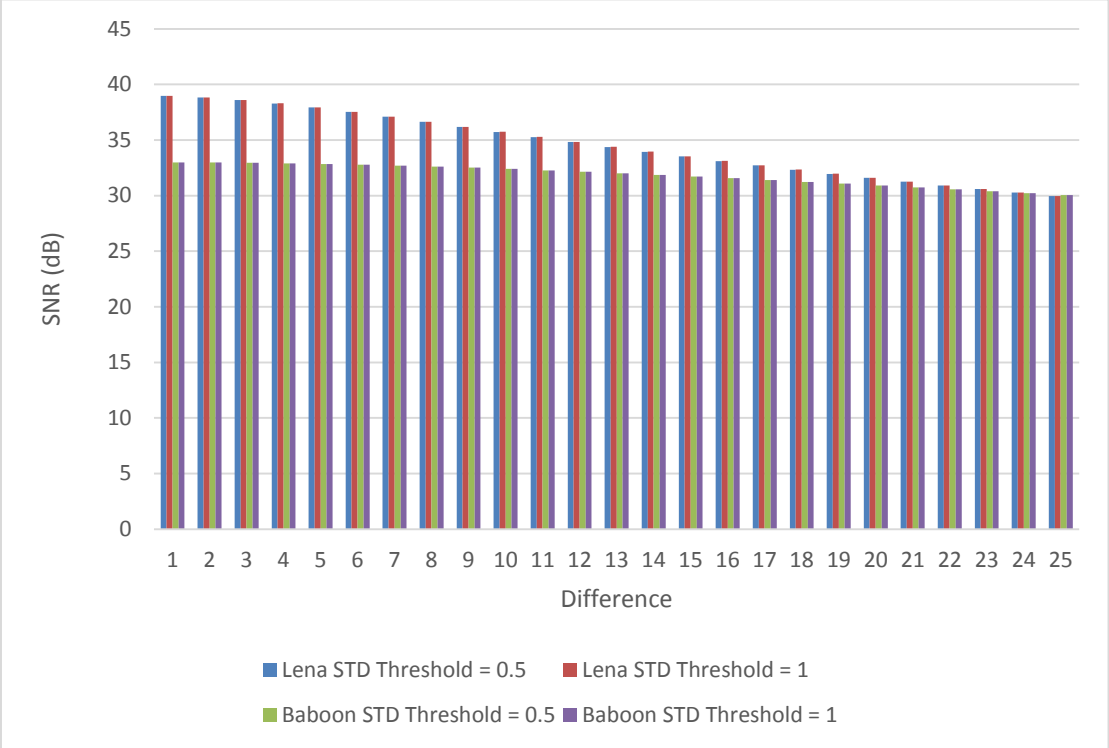

Figure-2. The cover quality after applying the NSSM for two threshold values 0.5 and 1.

As expected, the high texture image (the Baboon) quality is less affected by the NSSM method for the small difference values, while with the increasing of the difference factor, the two image quality joins at the difference value equal to 20 STD. The threshold value doesnot affect the result of the cover image after applying the NSSM when all the blocks are selected.

The essential idea that the NSSM is based on is the fact that the JPEG algorithm after the attack, in fact, it maintains the mean value of the brightness of the cover image, sees Figure-3.

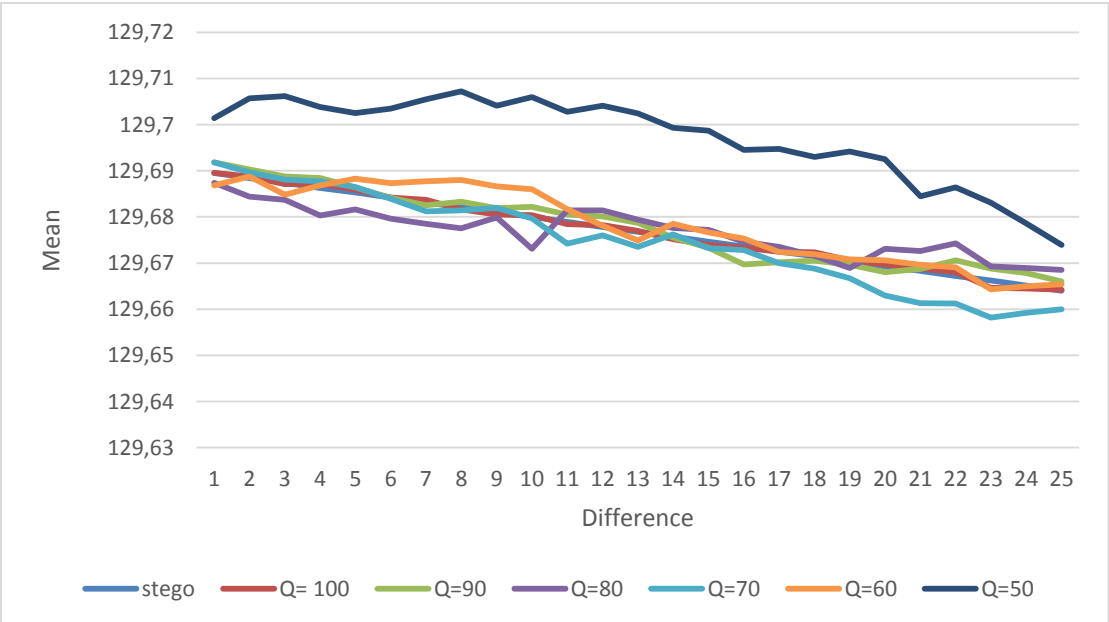

Figure-3. The mean value of the Baboon cover image for different threshold values after JPEG attack for different compression quality

The distortion in the cover image after the JPEG attack is illustrated in Figure (4) and (5), in which, the cover image quality is very good (i.e. higher than 25 dB).

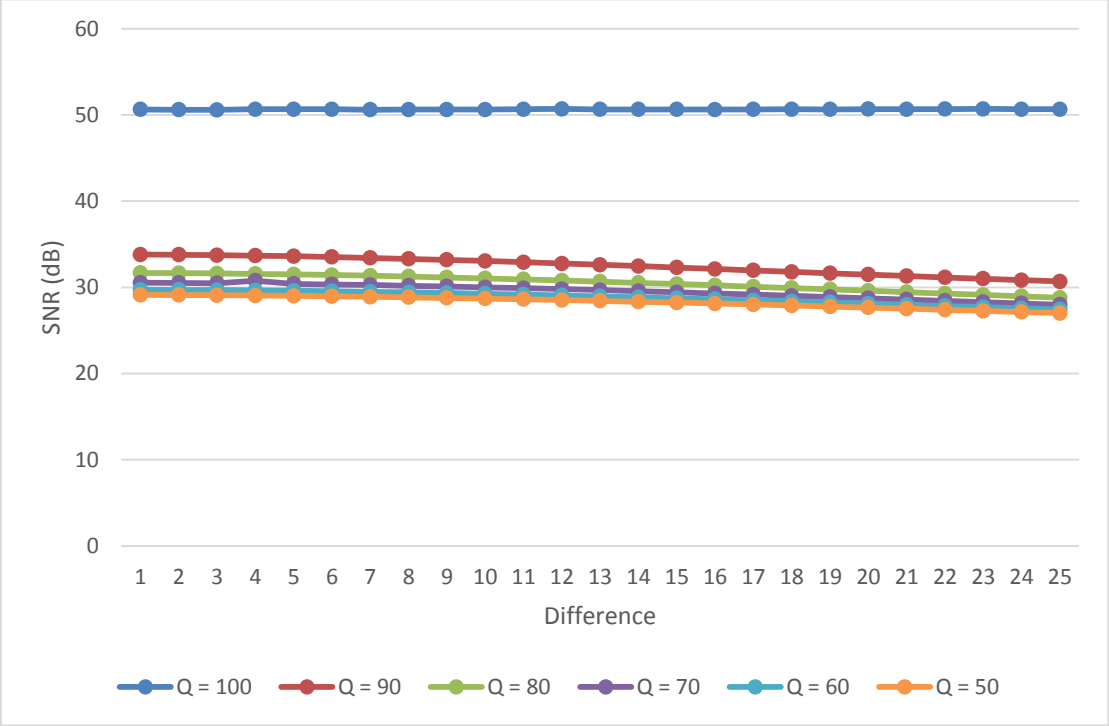

Figure-4. Cover quality for lena image after JPEG attack for STD threshold = 0.5 & 1.

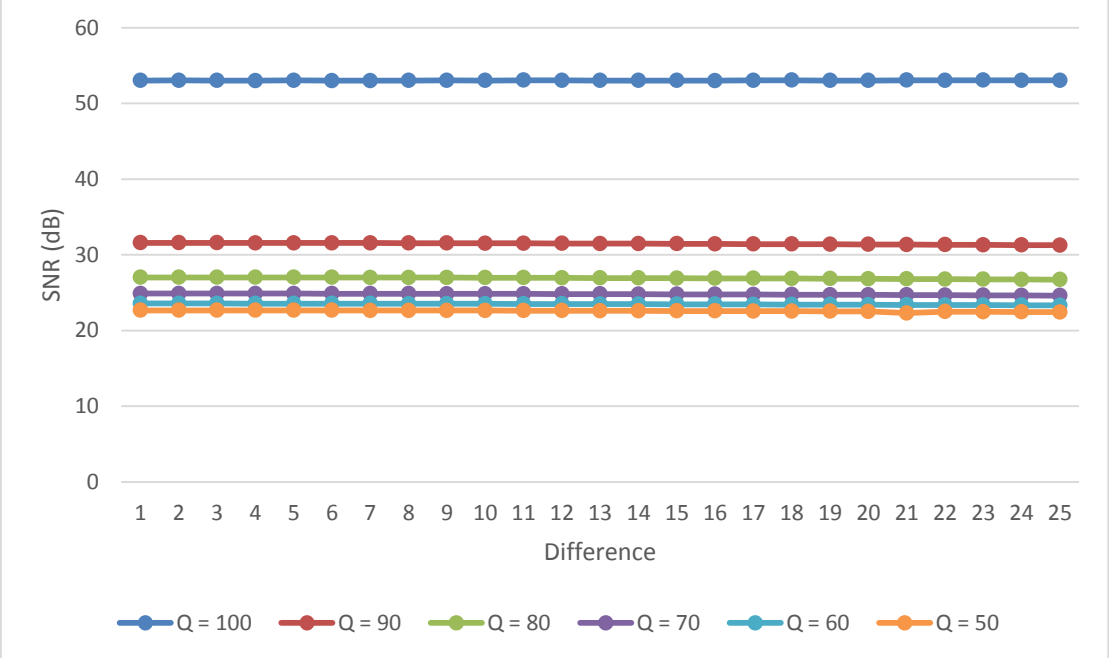

Figure-5. Cover quality for the Baboon image after JPEG attack for STD threshold = 0.5 & 1.

The JPEG algorithm has a smoothing effect on the image, therefore, the Baboon image suffer from this smoothing process more than Lena image since it has a texture more than Lena.

The error percent in the retrieved message from the cover images after the JPEG attack is illustrated in the Figures 6-8.

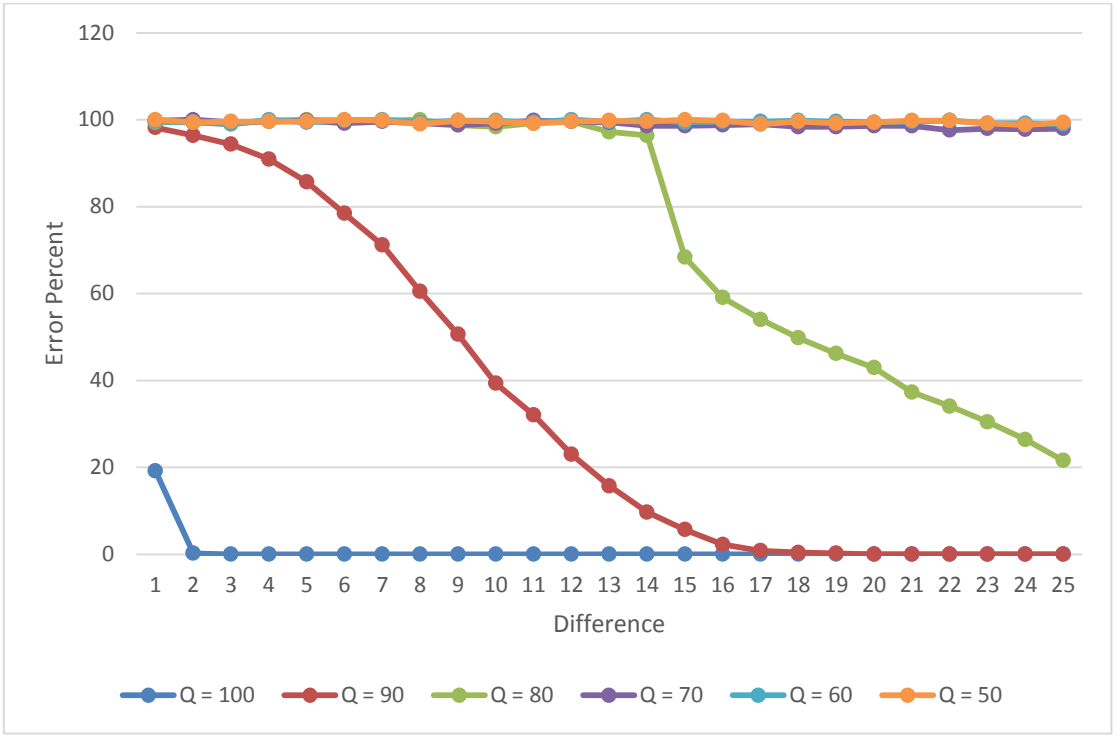

Figure-6. The error percent in the retrieved message from Lena cover image using threshold value equal to 0.5 and after different compression quality for the JPEG attack.

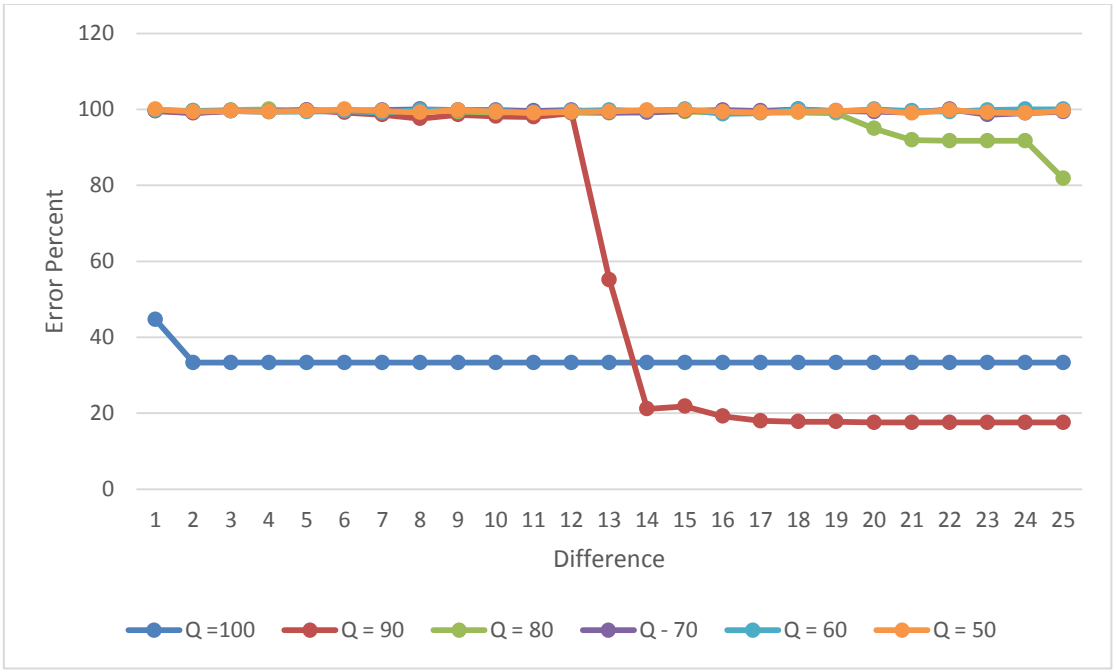

Figure-7. The error percent in the retrieved message from Lena cover image using threshold value equal to 1 and after different compression quality for the JPEG attack.

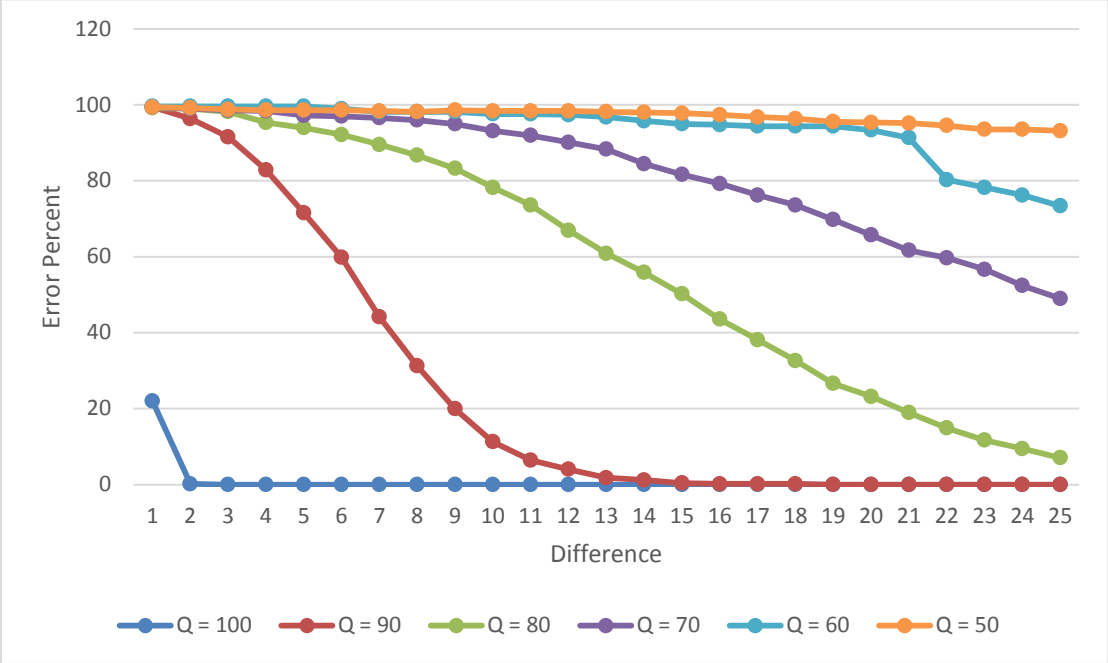

Figure-8. The error percent in the retrieved message from the Baboon cover image using threshold value equal to 0.5 or1 and after different compression quality for the JPEG attack

From the Figures 6-8 we can drive the following notes:

a) The NSSM able to override the JPEG attack starting from difference equal to 2 in the compression quality equal to 100 and difference parameter equal to 14 in case compression quality equal to 90.
b) In case Lena cover for STD threshold value equal 1, failed to retrieve the message even for compression quality 90 and 100. This failure is due to one of the cover blocks failed in the STD threshold test, since the threshold value is high, therefore, the sequence of the retrieved bits is miss-arranged which caused to corrupt the message starting from that bit. By decreasing the threshold value to 0.5 (figure 6), all blocks passed the test.
c) The Baboon cover image did not affect with the changing in the threshold value because it has high texture details, therefore, the JPEG attack couldn't reduce the texture to significant value due to the smoothing effect that companies with it.

CONCLUSIONS

The NSSM method success to override the JPEG attack for low compression quality (Q = 90 & 100), since uses the idea of maintaining the mean value of the image brightness after the attack to embed the secret message.

Using high texture image will enhance the NSSM results to reduce the effect of the smoothing process the combine the JPEG attack on the cover image. The NSSM has a high robustness against the compression attacks with low capacity comparing with the traditional LSB methods.

REFERENCES

Barán B., Gómez S. & Bogarín V. 2001. Steganographic Watermarking for Documents. IEEE Proceedings of the 34th Hawaii International Conference on System Sciences.

Kalita M., Majumder S. & Tuithung T., 2017. A Spatial Domain Steganographic Approach Using Pixel Pair Differencing and LSB Substitution. s.l., s.n.

Katharotiya, A., Patel, S. & Goyani, M., 2011. Comparative Analysis between DCT & DWT Techniques of Image Compression. Journal of Information Engineering and Applications, 1(2).

Singh M., Kumar S., Singh S. & Manish. 2016. Various Image Compression Techniques: Lossy and Lossless. International Journal of Computer Applications. 142(6): 23-26.

Singla D. & Syal R. 2012. Data Security Using LSB & DCT Steganography in Images. International Journal of Computational Engineering Research IJCER. 2(2): 359-364.

Abboud G., Marean J. & Yampolskiy R., 2010. Steganography and Visual cryptography in computer forensics. Fifth International Workshop on Systematic Approaches to Digital Forensic engineering.

Al-Sudany, I. F. 2006. Analysis and detection of Information Hiding in Digital Images. M.SC. in Computer Science, University of Technology.

Al-Towayjri J. M. A. 2003. Overcoming the Effect of JPEG Compression on Steganography. M.Sc. in computer Science,Universtiy of Technology.

Chanu Y. J., Singh K. M. & Tuithung, T., 2012. Image steganography and Steganalysis: A Survey. International Journal of Computer Application. 52(2).

Cheddad A. 2009. Steganoflage: A new image Steganography Algorithm. PH.D School of computing & Intelligent systems Faculty of Computing & Engineering,University of Ulster.

Cheddad A., Condell, J., Curran, K. & Kevitt, P. M., 2010. Digital image steganography: Survey and analysis of current methods. Signal processing. 90(3), pp. 727-752.

Currie III, D. & Irvine, C. C., 1996. Surmounting the Effects of Lossy Compression on Steganography. Proceedings of th19 National Information System security Conference, pp. 194-201.

Ibadi, A.O. & Akif, O. Z., 2010. A Proposed Algorithm for Steganography. Ibn Al-Haitham Journal for Pure and Applied Science. 23(3).

Kamal, M. & Abduljabbar, H. M., 2018. The Effect of JPEG Compression Algorithm Attack on the LSB Steganography Method. Information. 21(5):1615-1624.

Krutz R. D. 2003. Hiding Plain sight: Steganography and the Art of covert Communication. s.l.:Wiley.

Nadiya P. V. & Imran B. M. 2013. Image Steganography in DWT Domain usingDouble-stegging with RSA Encryption. International Conference on Signal Processing, Image Processing and Pattern Recognition [ICSIPRj.

Rana M., Sangwan B. & Jangir J. 2012. ART of Hiding: An Introduction to Steganography. International Journal of Engineering and Computer Science (IJECS). 1(1): 11-22.

Sabnis S. K. & Awale R. N. 2016. Statistical Steganalysis of High Capacity Image Steganography with Cryptography. 7thInternational Conference on Communication, Computing and Virtualization, ScienceDirect. 79: 321-327.

Sravanthi G. S., Devi B. S., Riyazoddim S. M. & Reddy M. J. 2012. A spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method. Global Journal of Computer Science and Technology Graphics& Vision. 12(15).

Yadav R., Saini R. & Kamaldeep 2011. Cyclic Combination Method for Digital Image Steganography with Uniform Image Steganography with Uniform. Advanced Computing: An International Journal (ACIJ). 2(6): 29-43.