1. Ahmed Gamal Abdellatif Ibrahim [1], 2. Mohamed Saleh [2], 3. Adham Ahmed Elmahallawy [3]

[1]Department of Communications and Electronics Engineering, Air Defense College, Alexandria, Egypt,[2] Department of Electrical Engineering, Faculty of Engineering, Pharos University in Alexandria, [3] Higher institute of Engineering and Technology, king Mariout.
ORCID: 1. 0000-0002-3440-8448, 2. 0000-0001-7981-8187, 3. 0000-0002-0044-3675

doi:10.15199/48.2023.02.03

De-Noising of Secured Stego-Images using AES for Various Noise Types

Abstract*. Steganography plays a crucial part in secret communication systems because information security is a crucial duty in the process of transferring data. However, there are considerable challenges involved in preserving that information, including alteration, privacy, and origin validation. In this paper, the Advanced Encryption Standard (AES) approach and the stenographic method are combined into a reliable model in this study. Furthermore, as Stego-images are acquired or spread across the communication channel, several noise shapes, including additive and multiplicative forms, occur. Therefore, several classes of linear and nonlinear filtering methods are presented and used for noise sweep and stego-image extraction. The results of the experiments showed that the appropriate assessment metrics were Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Correlation (COR).*

Streszczenie. *Steganografia odgrywa kluczową rolę w systemach tajnej komunikacji, ponieważ bezpieczeństwo informacji jest kluczowym obowiązkiem w procesie przesyłania danych. Jednak z zachowaniem tych informacji wiążą się poważne wyzwania, w tym zmiany, prywatność i weryfikacja pochodzenia. W niniejszym artykule podejście Zaawansowany Standard Szyfrowania (ZSS) i metoda stenograficzna zostały połączone w wiarygodny model w tym badaniu. Ponadto, gdy obrazy Stego są pozyskiwane lub rozprzestrzeniane w kanale komunikacyjnym, pojawia się kilka kształtów szumu, w tym formy addytywne i multiplikatywne. W związku z tym przedstawiono kilka klas liniowych i nieliniowych metod filtrowania, które są wykorzystywane do przemiatania szumów i ekstrakcji obrazów stego. Wyniki eksperymentów wykazały, że odpowiednimi metrykami oceny były błąd średniokwadratowy (Śbk) stosunek sygnału szczytowego do szumu (SWSS) i korelacja (KOR). (**Odszumianie obrazu stego przy wtkorzystanmiu AES dla różnych rodzajów szumu**)*

Keywords: Discrete Wavelet Transform, Advanced Encryption Standard (AES), Stego-image, Noise Model, Average Filter, Median Filter and Wiener Filter.
Słowa kluczowe: Dyskretna transformacja falkowa, Zaawansowany Standard Szyfrowania (*ZSS*), obraz Stego, model szumu, filtr średni, filtr medianowy i filtr Wienera.

Introduction

The goal of steganography is to conceal information in a covered medium such that others cannot extract it or detect it, which is advantageous as it does not call attention to or cast doubt on the presence of the concealed message. Another technique for preserving data and providing communication with security is encryption, although in this scenario, outsiders would be able to learn and the cipher text may be viewed without being able to decipher or use it. Therefore, both strategies are used to achieve and provide more protection and safety. Recent Steganography algorithms support a variety of image Steganography types, including transform domains, statistical analysis, hybrid domains, and geographical domains. The hybrid domain, which combines the spatial and transforms domains, is used in this research to increase security and strength. The secret message is additionally encrypted and integrated into the cover picture using (AES). Assessment criteria including quality, visualization, correlation, and distribution were applied to statistical analysis. Different image de-noising techniques have been developed, each with its own advantages and drawbacks. Therefore, while selecting a technique, consider the kind and level of noise present in the image. Other elements such as image de-noising performance, computing time, and cost must also be estimated. De-noising is possible in many different contexts, including transform domain filtering and spatial domain filtering [1, 2].

A) Spatial Domain Filtering

Resampling and noise reduction are two common jobs that use filtering algorithms. It is often used in all image operation techniques [3]. Based on the kind and amount of noise present in the image, a filter is chosen so that various filters may effectively eliminate various types of noise. The following are examples of spatial domain filters:

1) Linear Filters

It is used to distinguish one type of noise from another. And these filters result in blurring, which obliterates an image's key elements [4]. As a result, it performs poorly at separating noise from the signal. The two most popular types of linear filters are average filters and wiener filters: By replacing pixels with their mean value, an average filter may remove extraneous features from a picture. In order to minimize the (MSE), the Wiener filter was used. also capable of reducing noise and deteriorating features. One technique assumes knowledge of the spectral characteristics of the original signal and the noise. It is necessary to apply a linear time-invariant filter that, to the greatest extent feasible, produces output that is identical to the original signal.

2) Non-Linear Filters

Non-linear filters are used to overcome the limitations of linear filters. Therefore, the median filter is the most typical and often used nonlinear filter. Smoothing the photos brings out the noise. Reduces the intensity variation between a pixel's one and its neighbor pixels as well. Additionally, the median value and the image's pixel value are switched. In order to calculate the average value, all the pixel values are first arranged in ascending order. The computed pixel is then alternated with the middle pixel value. It alternates the pixel with an average of two middle pixel values if the surrounding pixel in the picture has to be counted as even with no pixels [5]. The median filter performs poorly at eliminating high-density salt and pepper noise; it performs best when the impulse noise percentage is less than 0.1.

B) Steganography

The goal is to conceal the secret data by incorporating it into a cover picture, making it impossible to find. The Stenographic system requires a cover media with plus bits

that can be modified without removing the medium's primary properties [6, 9].The process of doing this entails restoring the media's plus bits together with the secret data that will be implanted. Three different parameters are very important to execute a stenographic framework, namely. strength, security, and capacity. The quantity of data that can be securely stored in the media is indicated by capacity and fig. 1 illustrated the block diagram of steganographic system. The steganography techniques include:

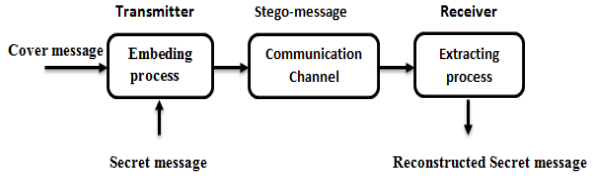


Fig. 1 The block diagram of steganographic system.

1) Spatial Domain Technique

Spatial domain steganographic techniques sometimes referred to as replacement techniques are a collection of very straightforward methods that provide a hidden channel in the areas of the cover picture where changes are likely to be a little scarce in comparison to the Human Visual System (HVS). Among the methods for doing this is to conceal data in the Least Significant Bit (LSB) of the picture data [10, 13].

2) Transform Domain Technique

Transform domain embedding is a class of embedding methods for which several algorithms have been proposed. This approach is more resistant to raid than others like compression and filtering since the secret data is added by modifying the transform coefficients of the picture. The alternative techniques included discrete wavelet transform (DWT) and discrete cosine transform (DCT) [14, 15].

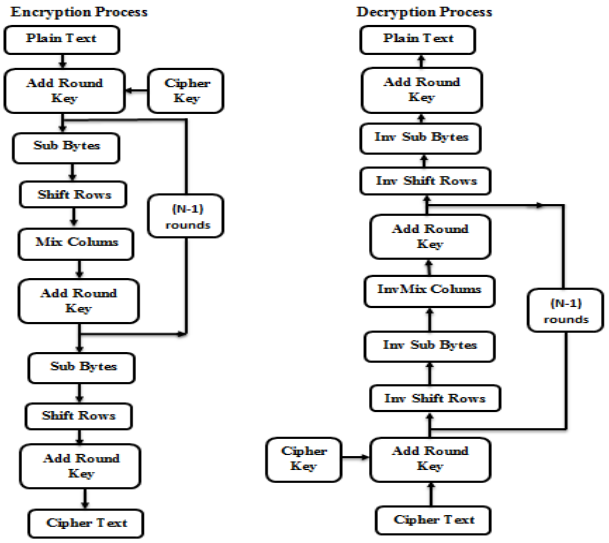


Fig. 2 The block diagram of The AES algorithm.

C) Advanced Encryption Standard Algorithm

A state with a key length of 128, 192, or 256 bits is used by the symmetric encryption method (AES) to work on a 44 array of bytes (128 bits). Depending on the key length, the state is encrypted or decrypted using four transformations for 10, 12, or 14 cycles (128, 192, or 256 bits). The AES method reduces the administrative burden of managing keys by using the same key for both data encryption and decryption. It is advantageous if both plain text and encrypted text be the same size. The most effective technique to encrypt any data is with the AES algorithm. High security, versatility, simplicity, and most importantly, a fair price, are all features it offers. Both linear and differential cryptanalysis cannot break it. Because the method has been through numerous rounds, the attack is almost impossible. It works well across a variety of platforms for both hardware and software. And fig. 2 illustrated the block diagram of The AES algorithm [15].

Problem Formulation and Modeling

The proposed method combines the weighted (DWT) coefficient of the relevant sub-bands of the cover picture and encrypted secret message using the (AES) technique, a modified embedding weighting function is introduced. And it is presented by the following equations:

$$S(j,k) = \beta C(j,k) + \alpha M(j,k) \quad (1)$$

Where

$$\beta + \alpha = 1 \quad (2)$$

Since α and β are two weighting intensity factors for the DWT of the encrypted Secret message (M), cover image (C) respectively, and (S) is the modified DWT coefficients of the stego-image. When the Stego-image is passed into the communication channel, Its distortion is caused by the presence of dissimilar types of noise, and the best way to reduce the impact of these different types of noise without sacrificing or damaging the important aspects of the Stego-edges image's is to use a variety of filters, whether linear or nonlinear. And the noisy Stego-block system's diagram is shown in fig. 3. The secret message is compressed using fuzzification, and the DWT is then applied and embedded in the cover picture in accordance with the weighted embedding function. The DWT is first conducted on the cover image to create the LH, HL, HH, and LL bands. After that, a Stego-image is performed using the IDWT. Therefore, the following equation presents the weighted embedding function that takes noise into account:

$$S(j,k) = \beta C(j,k) + \alpha M(j,k) + N(j,k) \quad (3)$$

where (N) is noise model.

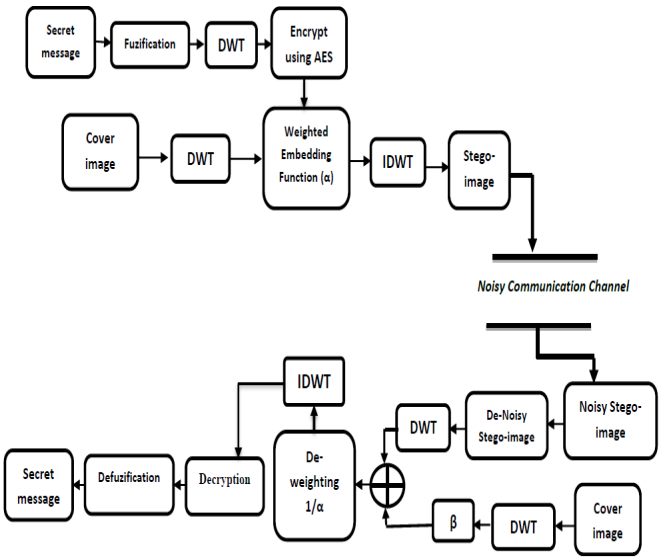


Fig.3. the block diagram of the noisy stego-system.

Results and Discussion

The experiment was conducted using a variety of common grayscale cover images and encrypted secret images using the Advanced Encryption Standard (AES)

with a size of (256 x 256). The secured Stego-images were then corrupted using simulated Gaussian white noise (mean=0, variance=0.01), Salt & Pepper noise (noise density=0.05), and Speckle noise (mean=0, variance=0.04). Different spatial linear filters (such as the average filter (3x3), Wiener filter (3x3), and spatial nonlinear filter (such as the median filter (3x3)) are employed for the de-noising process. So, fig. 4 shows the original images (Locomotive and House), fig 4 (a) shows the secret message without encryption, and fig 4 (b) shows the secret message with encryption using the (AES) algorithm.

Fig.4 (a).The secret messages before encryption process.

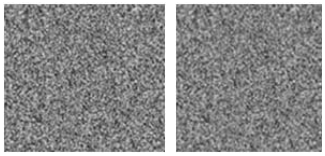


Fig.4 (b). The encrypted Messages secret

Fig. 5 presents stego-image before entering into the noisy communication channel, Lena is utilized as a cover and (House or Locomotive) as a secret message (α=0.1-α=0.8).

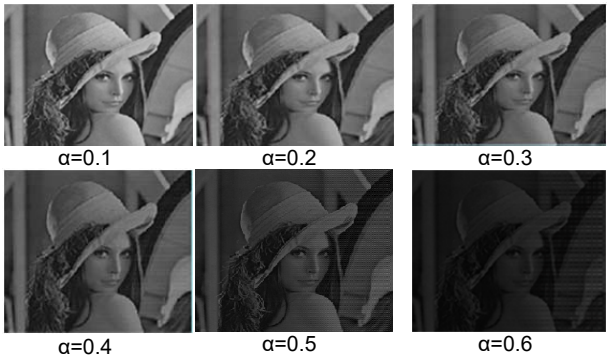
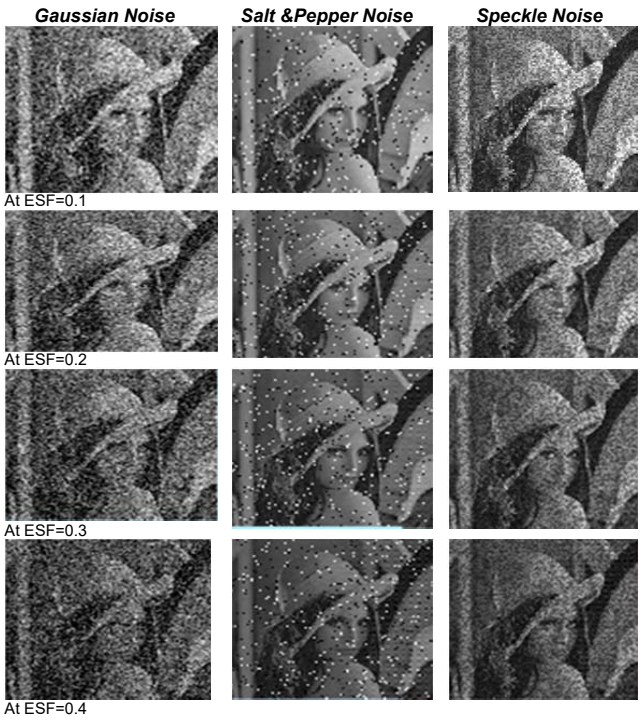


Fig.5. The stego-image for different amounts of ESF.

Fig.6 displays the stego-image after transmission into the noisy communication channel with unlike types of noise, like Gaussian, Salt and pepper, and Speckle noise with unlike amounts of embedding strength factor.



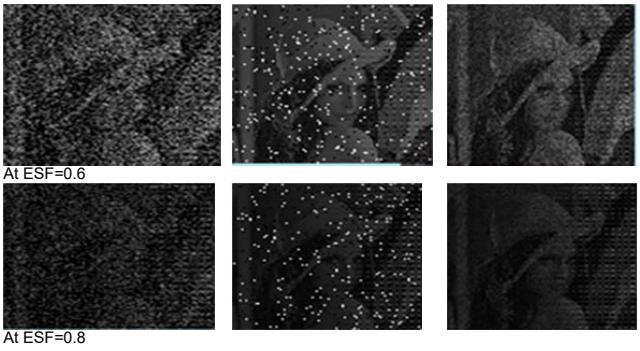


Fig.6. Noisy stego-images with different kinds of noise.

Fig. 7 presents the denoisy Stego-images utilizing the average, Median, and Wiener filter at Gaussian Noise for unlike amounts of ESF. From the examination, the de-noised stego-images that utilized the median filter are perfectible than other used filters.

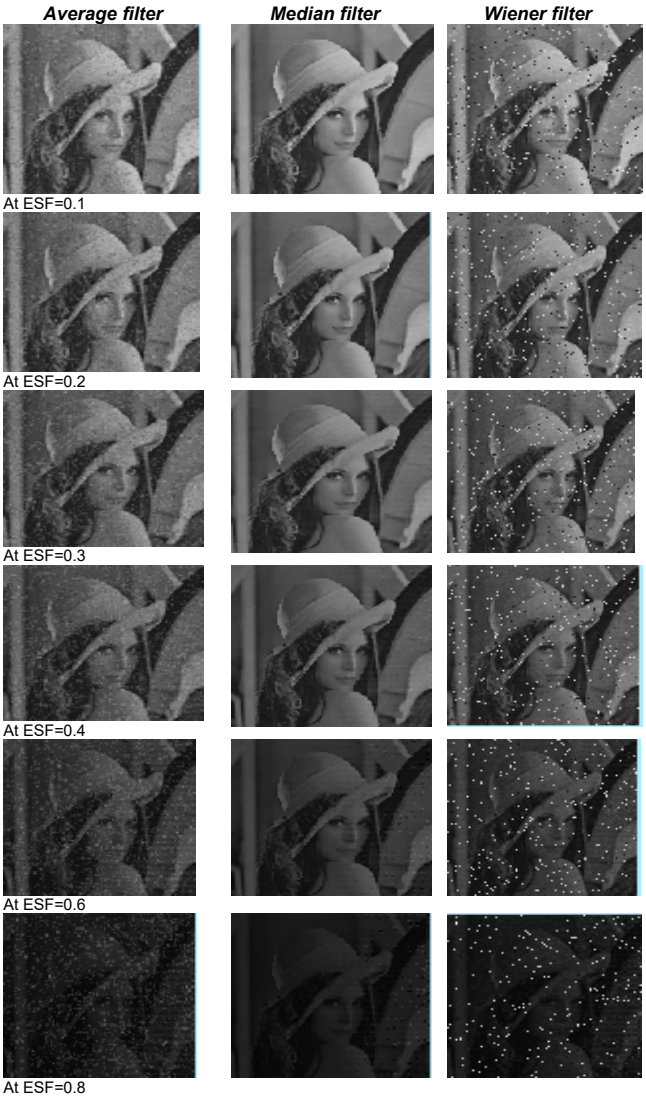


Fig.7. De-noised stego-images with Gaussian noise.

Fig. 8 presents the de-noised stego-images utilizing the average, Median, and Wiener filter with Salt and pepper Noise for unlike amounts of ESF. From the examination, the de-noised stego-images that utilized the average filter is perfectible than other used filters.

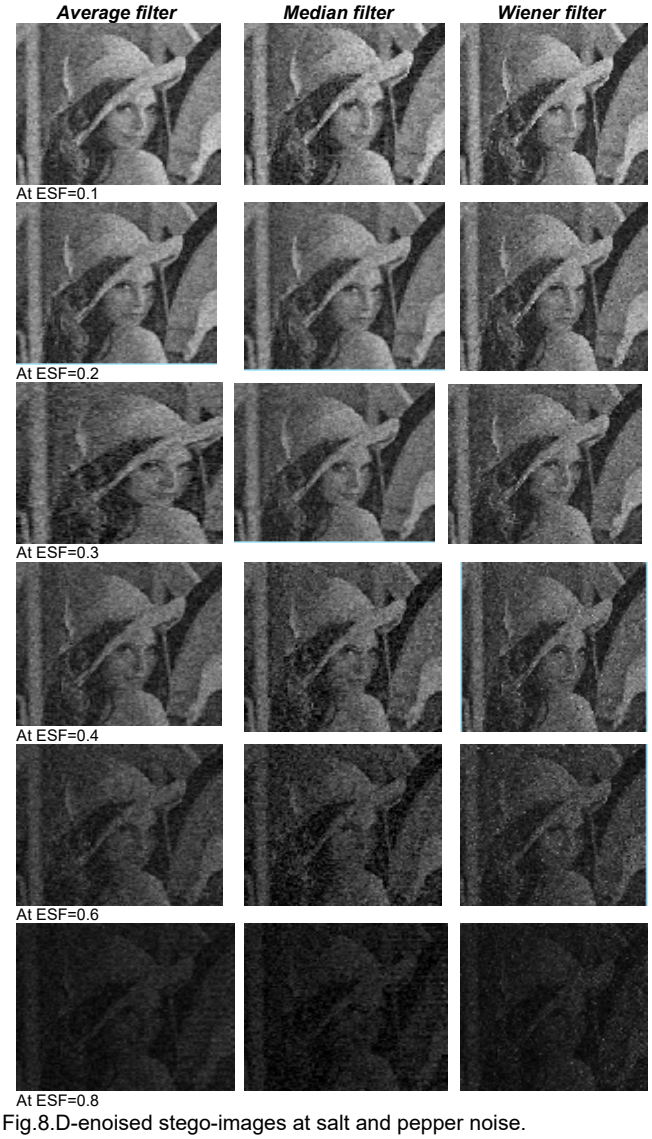


Fig.8.D-enoised stego-images at salt and pepper noise.

Fig.9 presents the de-noisy stego-images utilizing the average, median, and wiener filter for unlike amounts of ESF. From examination, the de-noised Stego-images utilized average filter is perfectible than other used filters.

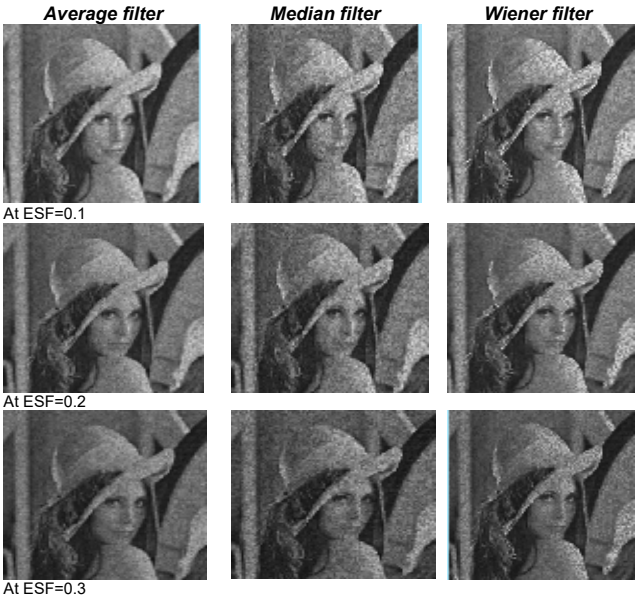


Fig.9. De-noised Stego-images for speckle noise.

Finally, the precision, effectiveness, and robustness of the proposed system have been evaluated using a variety of scales and parameters, including mean square error, peak signal to noise ratio, cross-correlation coefficient and entropy using the following equations:

A) Mean Square Error (MSE):

$$MSE = \sum_{j=1}^{M} \sum_{K=1}^{N} \frac{(C(j,k)-S(j,k))^2}{M*N} \quad (4)$$

where: C (j, k), is the cover image, S (j, k) is the stego-image and M, N is the Size of the image.

B) Mean Square Error (MSE):

$$PSNR = 10\, log_{10} \frac{(255)^2}{MSE} \quad (5)$$

C) Cross Correlation coefficient (COR):

$$COR = \frac{\sum_{0}^{N-1}(C(j,k)-m1)(S(j,k)-m2)}{\sqrt{\left(\sum_{0}^{N-1}(C(j,k)-m1)\right)^2\left(\sum_{0}^{N-1}(S(j,k)-m2)\right)^2}} \quad (6)$$

where: C (j, k), is the cover image, S (j, k) is the Stego-image, m1 is the average amounts of pixels of the cover image and m2 is average amounts of pixels of the Stego-image.

D) Entropy

$$Entropy = -\sum_{j} Pj\, Log(Pj) \quad (7)$$

where: Pj the probability between two adjacent pixels

Fig.10 displays the Entropy of the stego-image with various amounts of ESF while using the image of Lena as a cover and Locomotive as a secret message after passing into the noisy communication channel.

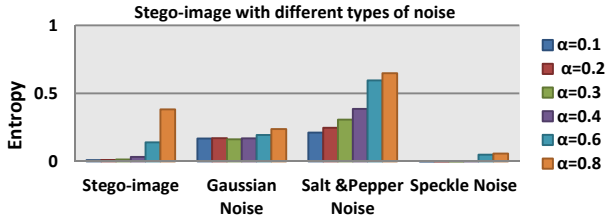


Fig.10.The entropy of the stego-image and noisy stego-image with various amounts of ESF.

Fig.11 displays the Correlation of the stego-image with various amounts of ESF when using the image of Lena as a cover and the Locomotive as a secret message, after passing into the noisy communication channel.

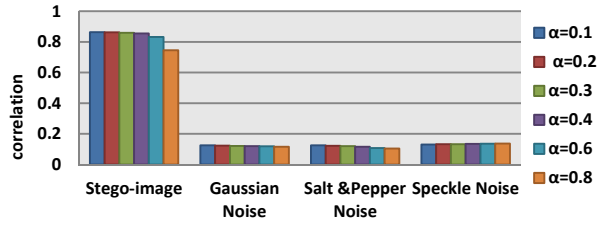


Fig.11. The correlation of the stego-image and noisy stego-image for various values of ESF.

Fig.12 illustrates the (PSNR) of stego-image for various amounts of ESF when utilizing the images of Lena as a cover and the Locomotive as a secret and in fig.12a the (PSNR) of the stego-image before passing over the noisy communication channel, while the stego-image passing over the noisy communication channel and fig.12. (b-g) illustrate the de-noisy process on the noisy stego-images using various kinds of filters with various values of ESF.

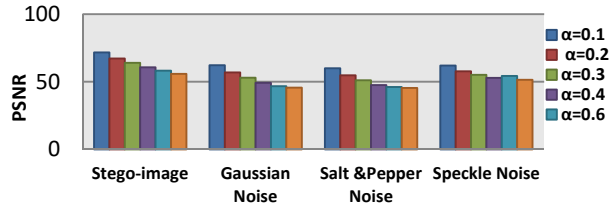
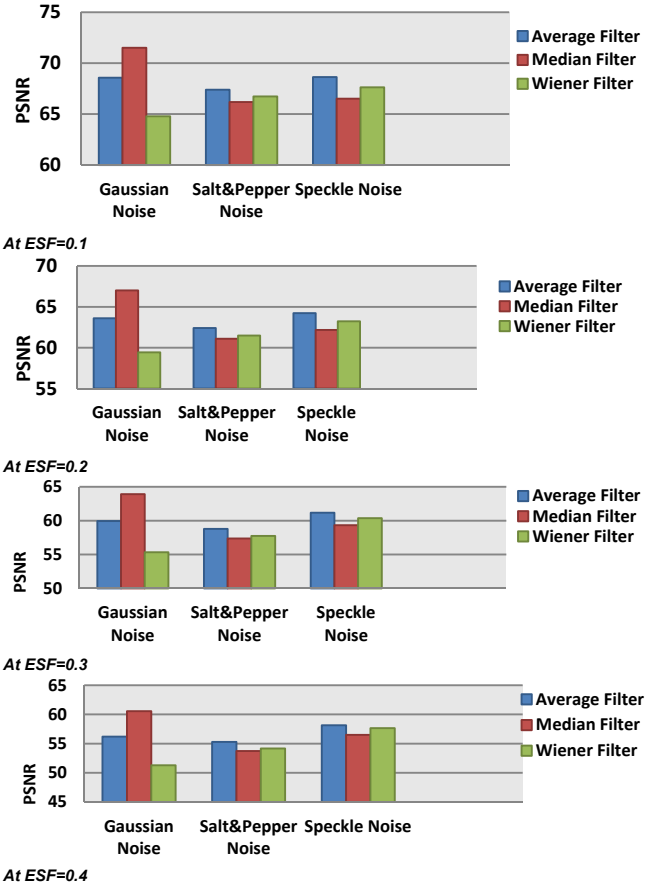


Fig. 12(a). The PSNR of stego-images and noisy stego-images for various amount of alpha.



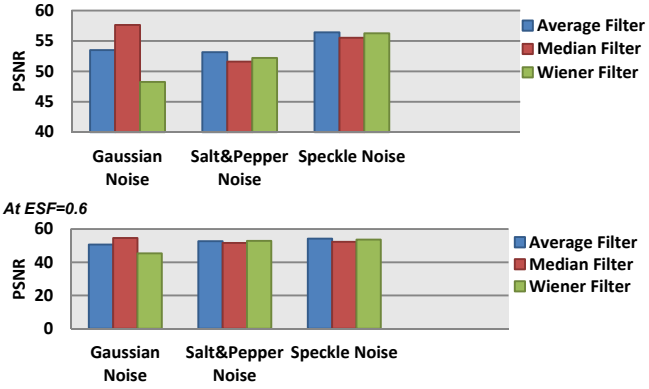


Fig.12 (b-g). PSNR of de-noisy stego-images for various kinds of filters at amount of ESF= 0.1-0.8.

Conclusion

In this research, a novel steganographic methodology is provided that improves the secrecy and accuracy of the invisible data without sacrificing picture quality or giving up any image data by combining stenographic technique with (AES) method to create a stego-image that is highly secure. Additionally, stego-images were used to imitate various noise types and filtering techniques. Then, on contrasted noisy stego-images, several classes of spatial filters, such as the Average, Median, and Wiener filters, were used. Moreover, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Cross Correlation coefficient (COR), and Entropy are used to measure the resilience of the stego-system and the recovery efficiency of filters. Additionally, the results of the differentiation showed that the average filter is capable of collecting speckle noise and salt and pepper noise with efficiency. Finally, the several forms of noise that were used in this work may be effectively removed using median filter.

Authors:
Dr. Ahmed GAMAL ABDEL LATIF IBRAHIM ,is a Lecturer in the Department of Communications and Electronics, Air Defense College, Armed Forces, Egypt.
Email: ag.abdellatef@zu.edu.eg.
Dr. Mohamed SALEH ,is an Assistant Professor in the Department of the Electrical Engineering at the Faculty of Engineering ,Pharos University in Alexandria, Egypt.
Email: mawsaleh@gmail.com.
Dr. Adham AHMED ELMAHALLAWY, is a Lecturer in the Department of the Electrical Engineering, Higher institute of Engineering and Technology, king Mariout, in Alexandria.
Email: adhamegypt0@gemail.com.

REFERENCES

1. K. Ali, A. N. Quershi, A. Alauddin, M. S. Bhatti, A. Sohail et al., “Deep image restoration model: A defense method against adversarial attacks,” Computers, Materials & Continua, vol. 71, no. 2, pp. 2209–2224, 2022.
2. Douglas, M., Bailey, K., Leeney, M. and Curran, K. “An overview of steganography techniques applied to the protection of biometric data” Multimed Tools Appl., 2017.
3. M. Juneja, P. S. Sandhu, “An improved LSB based Steganography with enhanced Security and Embedding/Extraction,”3rd International Conference on Intelligent Computational Systems, 2013.
4. Yang, J., et al., “Spatial Image Steganography Based on Generative Adversarial Network”. ArXiv e-prints: 1804.07939v1, 2018.
5. Baluja, S. “Hiding Images in Plain Sight: Deep Steganography”. in Advances in Neural Information Processing Systems , 2017.
6. W. Tang, B. Li, S. Tan, M. Barni and J. Huang, "CNN-Based Adversarial Embedding for Image Steganography," in IEEE

Transactions on Information Forensics and Security, vol. 14, no. 8, pp. 2074-2087, Aug. 2019.
7. Ke, Y., et al., “Steganography Security: Principle and Practice”. IEEE Access, vol. 6, pp. 73009- 73022, 2018.
8. Chaumont, M., “Deep Learning in steganography and steganalysis from 2015 to 2018”, ArXiv e-prints, 2019.
9. Ma, S., et al., “Adaptive Spatial Steganography Based on Probability-Controlled Adversarial Examples”. ArXiv e-prints: 1804.02691, 2018.
10. A. Gamal, M. Mostafa, A. Masiero, A. Zaghloul ,M. Naser et al.,"Indoor positioning system based on magnetic fingerprinting image," Bulletin of Electrical Engineering and Informatics, vol. 10,no.3 pp. 1325–1336, 2021.
11. H.Fiyad ,A. Gamal, M. Mostafa,A. Zaghloul ,M. Naser et al.," An improved real visual tracking system using particle filter," Przeglad Electrotechniczny, vol. 11,no.1 pp. 164–169, 2021.
12. Zhang, Y., Qin, C., Zhang, W., Liu, F. and Luo, X "On the fault-tolerant performance for a class of robust image steganography" Signal Process. 146, 99–111, 2018.
13. Muaad M. Abu-Faraj and Prof. Ziad Alqadi, “Using Highly Secure Data Encryption Method for Text File Cryptography”, International Journal of Computer Science and Network Security, vol. 20, issue 11, pp.53-60, 2021.
14. Ziad A. Alqadi Muaad M. Abu -Faraj, "Improving the Efficiency and Scalability of Standard Methods for Data Cryptography”International Journal of Computer Science and Network Security, vol. 21, pp.451-458, 2021.
15. Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, and Jamil Al-Azzeh; "Comparative Analysis of ColorImage Encryption-Decryption Methods Based on Matrix Manipulation" International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, 2019.