Presenting a New Steganography Method Based on Wavelet Transform in Gray Image

Vahid Reza Soltaninia[1], Saeed Talati[2], Seyed Mahdi Khatmi Tajani[3], Kazem Ghafari[4]

1- Shahid Sattari University of Aeronautical Engineering, Tehran, Iran.
Email: v.soltaninia@ssau.ac.ir

2- Shahid Sattari University of Aeronautical Engineering, Tehran, Iran.
Email: P9513621342@ihu.ac.ir (Corresponding Author)

3- Shahid Sattari University of Aeronautical Engineering, Tehran, Iran.
Email: Mahditajani@yahoo.com

4- PhD Candidate, Faculty of Electrical Engineering Department, Imam Hossein University, Tehran,Iran
Email: kazemghaffari1425@gmail.com

Received: 8 April 2023 Revised: 14 April 2023 Accepted: 18 May 2023

ABSTRACT:
The ever-increasing development of telecommunications has made secure transmission one of the most important issues today. Using steganography keeps information away from unauthorized people, and the information is hidden inside the original file without harming the marks. Since there is a high hiding capacity in the image, the use of image steganography is much more common than other steganography methods. In this article, the wavelet transform steganography technique is used, and the comparison results of the images before and after applying steganography, as well as the histogram output, show that this method benefits from high resistance, as well as the SNR of this method compared to other methods. The reviewed results show the superiority of this steganography method.

KEYWORDS: Telecommunications, Steganography, SNR, Wavelet Transform.

1. INTRODUCTION

steganography is the art and science of covert communication, the purpose of which is to hide the communication by placing the message in a mask (a medium that has the ability to hide information in it such as image, sound, or any possible data) in such a way that the least detectable change is made. Create in it and the existence of the hidden message in the media cannot be revealed even in a possible way [1].

In obfuscation, the aim is to hide any sign of the existence of the message [2]. Hiding information originates from the natural weakness of human vision and hearing systems in recognizing vision and hearing coverage. For example, next to a strong signal, there can be a weak signal that cannot be seen or heard, which depends on the spectrum of the signal and its time parameters in two strong and weak signals, which makes the strong signal able to cover the weak signal. Among other cases, we can mention insensitivity to the signal phase and also to the noises that exist in the time or frequency domain and humans are not able to recognize it [3].

The principle of concealment is the use of Information carrier spaces that do not harm the identity of the carrier. With a little precision, it can be seen that hiding in the image has the most possibilities for hiding because there is a lot of bandwidth for image transmission, giving us more space for hiding [4].

The basic algorithm of steganography according to Figure 1 is that in the system, the message data is inserted into the carrier signal with the help of the hiding key.

The signal work output contains secret information. After transmission and recording, recording, other communication processes, the signal containing information, the hidden message are recovered using the hiding key. Information concealment solutions go back to the nature of the message carrier and are highly dependent on the type of use the designer uses for concealment [5].

Paper type: Research paper
DOI: 10.30486/MJTD.2023.1983555.1031
How to cite this paper: V. R. Soltaninia, S. Talati, S. M. Khatmi Tajani, K. Ghafari, "**Presenting a New Steganography Method Based on Wavelet Transform in Gray Image**", *Majlesi Journal of Telecommunication Devices*, Vol. 12, No. 2, pp.105-111, 2023.

Fig. 1. Hiding information and returning information [5]

2. CHARACTERISTICS OF A STEGANOGRAPHY SYSTEM

A steganography system to have an acceptable and reliable performance should have the following characteristics:

2.1. Transparency of hiding information

One of the important issues in information concealment is the degree of influence of the information on the carrier signal. If the transparency of the carrier signal is lost, the signal will be easily suspected. The transparency of the system states that the host subject before and after embedding the message should not have a noticeable difference because the main goal in hiding information is to not feel the existence of the message. In fact, the security of an information hiding system lies in this issue of transparency, and the greater the degree of similarity of the subject of the message in both normal and message-containing situations, the higher the security of the system is, and if this degree of similarity is low and recognizable, then there is doubt The observer will be motivated to search for the secret message, which is contrary to the purpose of hiding the information. Also, choosing the appropriate message host topic is also very important in creating doubt. For example, the exchange of a huge amount of nature images between two organizations clearly indicates the existence of a secret message exchange in the form of these images.

The criterion for measuring the similarity between two normal images and the image with steganography to determine transparency is the signal-to-noise ratio, which is calculated from equation 1 [6].

$$SNR = 10\,log\frac{\sum_{m,n} x^2(m,n)}{\sum_{m,n}(y(m,n) - x(m,n)^2} \qquad (1)$$

In this regard, x(m,n) represents the pixel values of the original image and y(m,n) represents the pixel values of the steganography image. Often, if the SNR is greater than or equal to 40, the difference between the original and reconstructed image is undetectable by the human eye.

2.2. Stability of information hiding

Stability means the ability of a signal containing information to maintain hidden information against intentional and unintentional attacks that occur on the signal. It is possible that in this situation, the signal containing information has complete transparency and the information hiding operation has been done with high quality, and this will make the analyzer less sensitive and the signal will pass safely through the communication channel. Also, it is possible that more attacks on the signal will occur with the decrease of transparency [7].

2.3. Information hiding rate

In an information hiding system, the more messages that can be hidden in a carrier or host, the more suitable this system is.

In fact, the amount of information that each method can hide in the carrier signal is one of the important issues in information hiding. The amount of data that can be stored in a host depends exactly on the host signal, and it is the nature of the host signal that determines to what extent the message can be hidden in it without seriously affecting its transparency [8].

2.4. Retrievability of information

Retrievability of information means that the authorized person can extract the hidden message from inside the host with the key and recovery algorithm. If the information is not reversible, the problem of hiding information leads to the loss of information [9].

2.5. The probability of detection error is low

An information hiding system should have a low probability of detection error so that when the message is retrieved, it can be corrected with error correction codes, because otherwise the information was not transmitted correctly. The higher the information hiding

rate, the greater the transparency and strength of the signal. Maintaining transparency means reducing the difference between the main signal and the signal containing information and reducing the hidden information.

Due to the importance of maintaining the important parameters of the signal to establish transparency, the less important parts of the signal are assigned to the hidden data and the stability of the message is reduced. To increase the stability of message storage, information should be hidden in more resistant places and at a lower rate, which means reducing the transparency and rate of information hiding [10].

3. WAVELET TRANSFORM

The Wavelet transform was introduced in the early 1980s. Since then, different types of Wavelet transform have been developed and many other applications have been found [4].

The continuous-time wavelet transform, also called the integral wavelet transform (IWT), is most widely used in data analysis, representing an invariant time-frequency representation. The most famous version of these transforms is the discrete wavelet transform (DWT). This transform has excellent signal compression properties for many classes of real-world signals along with very efficient computational aspects.

In the Wavelet transformation, the image is divided into frequency bands almost equal to the logarithmic scale, and therefore the changes made in the field of Wavelet transformation are less recognizable to the human eye. This transform is also better than DCT for higher-order compressions.

Fourier Transform consists of decomposing the signal into sine waves with different frequencies. Similarly, the wavelet transform is based on decomposing the signal into transposed and scaled versions of a parent wavelet function. Transposed and scaled versions of a parent Wavelet function are of the form Equation 2.

$$\psi_{\omega,n}(t) = \frac{1}{\sqrt{2^{\omega}}}\psi\left(\frac{t-2^{\omega}n}{2^{\omega}}\right), \quad \omega, n \in Z \qquad (2)$$

In that case, the Wavelet coefficients are obtained by multiplying the initial signal x(t) in the form of equation 3.

$$W(\omega, n) = \left\langle x(t) \quad , \quad \psi_{\omega,n}(t) \right\rangle \qquad (3)$$

What makes this transformation so efficient is its ability to perform local analysis and provide local features with fewer units of information than the samples themselves.

Wavelet transform creates variable frequency accuracies by creating variable lengths in the analysis, in such a way that when accurate information is desired at low frequencies, it uses long time intervals and conversely, it uses short intervals during accurate frequency analysis at high frequencies.

Calculating the Wavelet coefficients at any transition and scale is very difficult. A quick way to obtain the Wavelet coefficients is to use filter banks as shown in Figure 2. In that case, the Wavelet analysis includes filtering and reducing the sampling rate and reconstructing the original signal, including increasing the sampling rate and filtering.

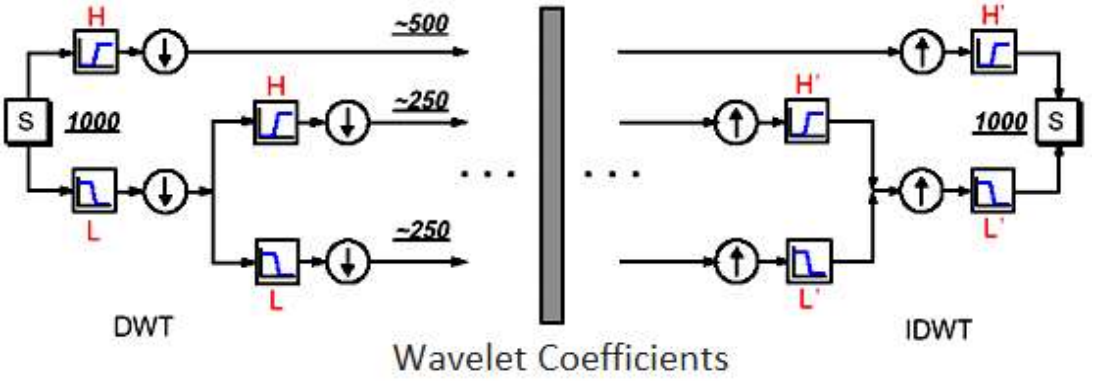

Fig. 2. Wavelet-based analysis and synthesis system [4]

In the Wavelet transformation, the analysis low-pass and high-pass filters (L and H) along with their complementary reconstruction filters (L' and H') form a system called square mirror filters (QMF). The corresponding QMF filters of the transform tree depend on the original Wavelet function.

3.1. Reasons for Replacing Discrete Wavelet Transform with Discrete Cosine Transform

After its introduction, this transformation found its place in the field of encryption and image compression and replaced the discrete cosine transformation.

The reason for this replacement was the existence of weak points in the discrete cosine transformation, which are mentioned below:

3.2 Weaknesses of DCT

In this transformation, only the spatial (temporal) correlation of pixels inside a two-dimensional block is considered, and the correlation between neighboring blocks is ignored.

It is impossible to completely disconnect the blocks at their border points using DCT.

Unwanted artificial blocking affects image reconstruction or video frames. (high compression ratio or very low bit rate)

The DCT transform is fixed so it cannot adapt to the data source.

It does not perform effectively on binary images (fax or fingerprint images) drawn by large intervals with constant amplitude.

(low spatial frequencies) are represented by short periods of light transitions.

3.3 Advantages of DWT over DCT

• No need to divide the input data into non-overlapping two-dimensional blocks.

• Using a hierarchical and multi-precision structure.

• Placing information in all bands and all places

4. STEGANOGRAPHY USING WAVELET TRANSFORM

The steganography algorithm using wavelet transformation in the image is as shown in Figure 3 and as follows:

• Wavelet transform is taken from the carrier image.

• The secret message is converted into an ascii code.

• The bit string is hidden next to the rows of one of the four wavelet transform components.

The steps of this method are given in Figure 3.

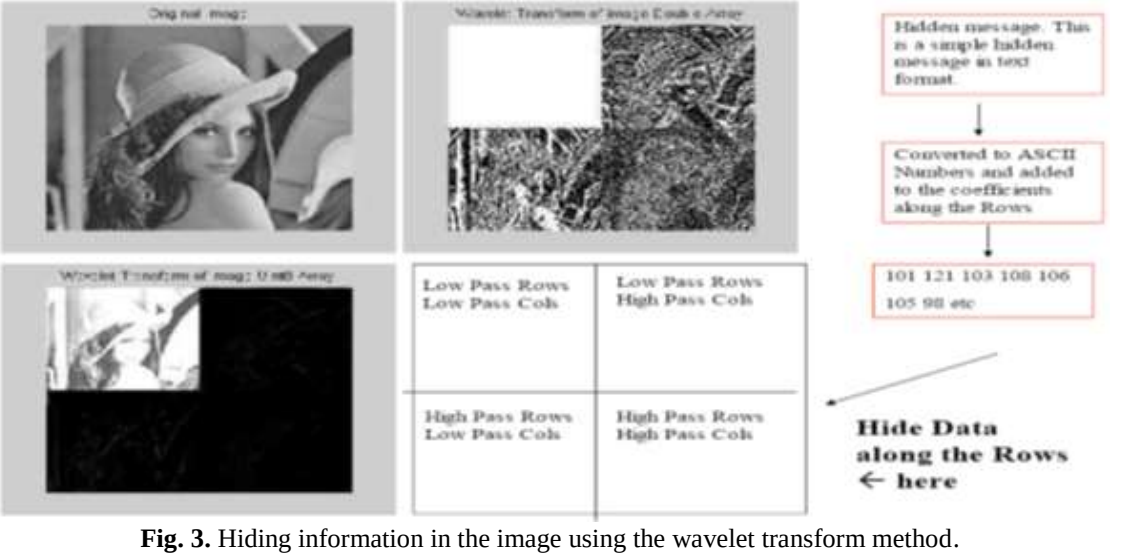

Fig. 3. Hiding information in the image using the wavelet transform method.

4.1 Analyzing the results of steganography using discrete wavelet transform

Figure 4 shows the original and steganography image of the man, which is implemented by the wavelet transform method**.**

Fig. 4. (a): Original image, (b): Image with steganography.

Discrete wavelet transformation has many advantages that have made this transformation a superior and up-to-date method of steganography.

The bandwidth of each of these channels is approximately one octave, and the signals of each of these channels are processed separately in the brain. In wavelet transformation, the image is divided into frequency bands almost equal to the logarithmic scale, and therefore the changes made in the field of wavelet transformation are less recognizable to the human eye. DWT transformation is a separable transformation, a two-dimensional DWT can be implemented by applying two consecutive one-dimensional DWT, which is applied first on the rows and then on the columns of the image. A well-known filter bank implementation can be used to calculate the 2D DWT, which results in a pyramidal structure. One of the reasons for using wavelet transform in steganography is that the new research of the human retina divides the images into several frequency channels.

Figure 5 shows the histograms of the original image and the steganographic image. By carefully comparing these histograms, the following results are obtained

.

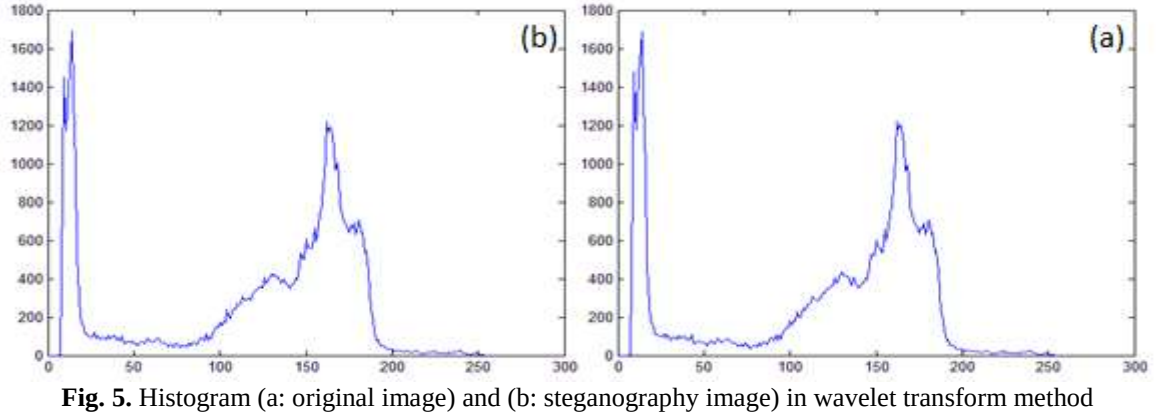

Fig. 5. Histogram (a: original image) and (b: steganography image) in wavelet transform method

The histogram of the steganographic image has very little difference from the histogram of the original image. Therefore, steganography with this method has a very high resistance to histogram analysis.

Figure 6 shows the comparison of the SNR in the images of Lena and the male photographer in the modes with steganography and without steganography. Table 1 compares the SNR of the proposed method and compares it with other methods.

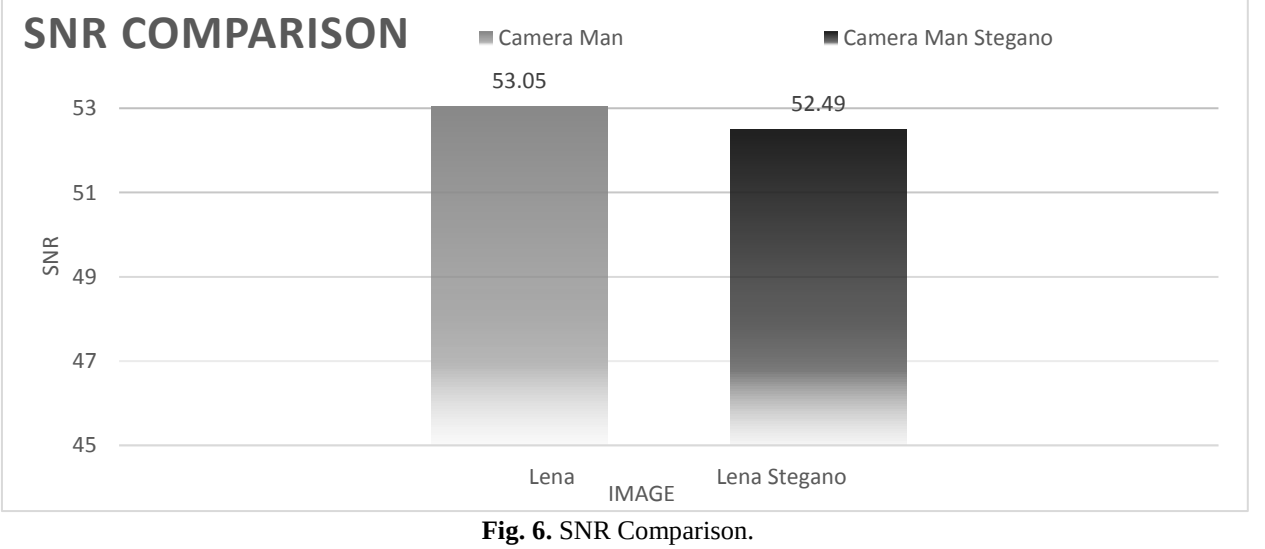

Fig. 6. SNR Comparison.

Table 1. Comparison of the SNR of the proposed method with other methods

Steganography method	SNR
Improved wavelet-based image watermarking through SPIHT.[11]	43.8 dB
Guided Dynamic Particle Swarm Optimization for Optimizing Digital Image Watermarking in Industry Applications.[12]	50 dB
An adaptive hybrid fuzzy-wavelet approach for image steganography using bit reduction and pixel adjustment.[13]	36.2 dB
A Secure Spatial Domain Image Steganography u sing Genetic Algorithm and Linear Congenital Generator.[14]	36.26 dB
proposed method (Lena)	53.40 dB
proposed method (Man)	52.49 dB

5. CONCLUSION

The science of steganography is developing rapidly and new methods are emerging every day. The main purpose of these methods is to create a secure connection for information transfer. In this article, steganography was performed on the images of Lena, Camera Man according to the proposed algorithm of Figure 3 and using MATLAB software, and Figure 4 shows the images before and after steganography. The results of this project show that the proposed method, using the output histogram in Figure 5 and the SNR criterion in Figure 6, compared to other methods reviewed in Table 1, it shows that this method has high security and it can be highly resistant to attacks.

REFERENCES

[1] De Rosal Ignatius Moses Setiadi, et al, **"Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)"** *Signal Processing*, Volume 206, May 2023.

[2] Pratap Chandra Mandal, Imon Mukherjee, Goutam Paul, B. N. Chatter "**Digital image steganography: A literature survey**" *Information Sciences Volume 609*, September 2022, Pages 1451-1488.

[3] B. F. Alatiyyat and N. C, "**Survey on Image Steganography Techniques"** *2nd International Conference on Computing and Information Technology (ICCIT)*, Tabuk, Saudi Arabia, 2022, pp. 57-64, doi: 10.1109/ICCIT52419.2022.9711651.

[4] I. R. Farah, I. B. Ismail, and M. B. Ahmed, **"A Watermarking System Using the Wavelet Technique for Satellite Images",** *WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY VOLUME 17 DECEMBER* 2006 ISSN 1307-6884.

[5] Lachlan McGill**, "Steganography: The Right Way",** *SANS Institute* 2005.

[6] Talati, S., Etezadifar, P **"Providing an Optimal Way to Increase the Security of Data Transfer using Watermarking in Digital Audio Signals"** *Majlesi Journal of Telecommunication Devices*, 9(1), pp. 35-46, 2020.

[7] Talati, S., EtezadiFar, P., Hassani Ahangar, M. R., Molazade, M **"Investigation of Steganography Methods in Audio Standard Coders: LPC, CELP, MELP"** *Majlesi Journal of Telecommunication Devices*, 12(1), pp. 7-15, 2023, doi: 10.30486/mjtd.2022.695928.

[8] I. R. Farah, I. B. Ismail, and M. B. Ahmed, **"A Watermarking System Using the Wavelet Technique for Satellite Images",** *WORLD ACADEMY OF SCIENCE, ENGINEERING VOLUME 17 DECEMBER 2006 ISSN* 1307-6884.

[9] Rafael C. Gonzalez, **"Digital Image Processing using Matlab",** *Pearson Prentice Hall*, 2004.

[10] Bo Yang and Beixing Deng, **"Steganography in Gray Images Using Wavelet",** *Department of Electronic Engineering, Tsinghua*, 2005.

[11] Kumar C, Singh AK, Kumar Pu, **"Improved wavelet-based image watermarking through SPIHT",** *Multimedia Tools and Applications*, vol. 79, no.15, pp.11069-11082.

[12] Zheng Z, Saxena N, Mishra KK, Sangaiah AK, **," Guided Dynamic Particle Swarm Optimization for Optimizing Digital Image Watermarking in Industry Applications"**, vol.88, pp.92–106, 2018.

[13] I. Shafi, M. Noman, M. Gohar, A. Ahmad, M. Khan, S. Din, S.H. Ahmad, J. Ahmad, **"An adaptive hybrid fuzzy-wavelet approach for image steganography using bit reduction and pixel adjustment",** *Soft Computing*, vol.u22, no.5, pp.1555–1567, 2018.

[14] P.D. Shah, R.S. Bichkar, "**A Secure Spatial Domain Image Steganography u using Genetic Algorithm and Linear Congr ential Generator",** *conference on intelligent computing*, pp.119-129, 2018.

[15] Talati, S., Hassani Ahangar, M, **"Analysis, Simulation and Optimization of LVQ Neural Network Algorithm and Comparison with SOM",** *Majlesi Journal of Telecommunication Devices*, 9(1), pp. 17-22, 2020.

[16] Talati, S., and M. R. Hasani Ahangar. **"Radar data processing using a combination of principal component analysis methods and self-organizing and digitized neural networks of the learning vector."** *Electronic and Cyber Defense* 9.2 (2021): 1-7.

[17] S. Talati, A. Rahmati, and H. Heidari. (2019) **"Investigating the Effect of Voltage Controlled Oscillator Delay on the Stability of Phase Lock Loops"**, *MJTD*, vol. 8, no. 2, pp. 57-61.

[18] Talati, S., & Hassani Ahangar. M. R. (2020) "**Combining Principal Component Analysis Methods and Self-Organized and Vector Learning Neural Networks for Radar Data",** *Majlesi Journal of Telecommunication Devices*, 9(2), 65-69.

[19] Hassani Ahangar, M. R., Talati, S., Rahmati, A., & Heidari, H. (2020). **"The Use of Electronic Warfare and Information Signaling in Network-based Warfare".** *Majlesi Journal of Telecommunication Devices*, 9(2), 93-97.

[20] Aslinezhad, M., Mahmoudi, O., & Talati, S. (2020). **"Blind Detection of Channel Parameters Using Combination of the Gaussian Elimination and Interleaving".** *Majlesi Journal of Mechatronic Systems*, 9(4), 59-67.

[21] Talati, S., & Amjadi, A. (2020). "**Design and Simulation of a Novel Photonic Crystal Fiber with a Low Dispersion Coefficient in the Terahertz Band".** *Majlesi Journal of Mechatronic Systems*, 9(2), 23-28.

[22] Talati, S., Alavi, S. M., & Akbarzade, H. (2021). **"Investigating the Ambiguity of Ghosts in Radar and Examining the Diagnosis and Ways to Deal with it".** *Majlesi Journal of Mechatronic Systems*, 10(2).

[23] Etezadifar, P., & Talati, S. (2021). **"Analysis and Investigation of Disturbance in Radar Systems Using New Techniques of Electronic Attack".** *Majlesi Journal of Telecommunication Devices*, 10(2), 55-59.

[24] Saeed. Talati, Behzad. Ebadi, Houman. Akbarzade **"Determining of the fault location in distribution systems in presence of distributed generation resources using the original post phasors"**. *QUID* 2017, pp. 1806-1812, Special Issue No.1- ISSN: 1692-343X, Medellin-Colombia. April 2017.

[25] Talati, S., & Alavi, S. M. (2020). **"Radar Systems Deception using Cross-eye Technique".** *Majlesi Journal of Mechatronic Systems*, 9(3), 19-21.

[26] Talati, Saeed, Akbari Thani, Milad, Hassani Ahangar, Mohammad Reza. 2020. **"Detection of Radar Targets Using GMDH Deep Neural Network",** *Radar Journal*, 8 (1), pp. 65-74.

[27] Talati, S., Abdollahi, R., Soltaninia, V., & Ayat, M. (2021). **"A New Emitter Localization Technique Using Airborne Direction Finder Sensor".** *Majlesi Journal of Mechatronic Systems*, 10(4), 5-16.

[28] Akbarzade, Houman, Seyed Mohammad Alavi, and Saeed Talati. **"Investigating the Ambiguity of Ghosts in Radar and Examining the Diagnosis and Ways to Deal with it."** *Majlesi Journal of Mechatronic Systems* 10.2 (2021): 17-20.

[29] Hashemi SM, Barati S, Talati S, Noori H**. "A genetic algorithm approach to optimal placement of switching and protective equipment on a distribution network."** *J Eng Appl Sci* 2016; 11: 1395-1400.

[30] O. Sharifi-Tehrani and S. Talati**, "PPU Adaptive LMS Algorithm, a Hardware-Efficient Approach; a Review on",** *Majlesi Journal of Mechatronic Systems*, vol. 6, no. 1, Jun. 2017.

[31] Hashemi, Seyed & Abyari, M. & Barati, Shahrokh & Tahmasebi, Sanaz & Talati, S. (2016). **"A proposed method to controller parameter soft tuning as accommodation FTC after unknown input observer FDI".** *Journal of Engineering and Applied Sciences.* 11. 2818-2829.

[32] Talati, Saeed, et al. **"Analysis and Evaluation of Increasing the Throughput of Processors by Eliminating the Lobe's Disorder."** *Majlesi Journal of Telecommunication Devices* 10.3, 2021, 119-123.

[33] S. Talati, A. Rahmati, and H. Heidari**, "Investigating the Effect of Voltage Controlled Oscillator Delay on the Stability of Phase Lock Loops"**, *MJTD*, vol. 8, no. 2, pp. 57-61, May 2019.

[34] Talati, Saeed, and Pouria EtezadiFar. **"Electronic attack on radar systems using noise interference."** *Majlesi Journal of Mechatronic Systems* 10.3, 2021, 7-11.

[35] Seyed Morteza Ghazali, Jalil Mazloum, Yasser Baleghid. "**Modified binary salp swarm algorithm in EEG signal classification for epilepsy seizure detection"** *Biomedical Signal Processing and Control*. Volume 78, September 2022.

[36] Talati, Saeed, Ghazali, Seyed Morteza, SoltaniNia, VahidReza, **"Design and construct full invisible band metamaterial-based coating with layer-by-layer structure in the microwave range from 8 to 10 GHz"** *Journal of Physics D: Applied Physics*. Volume 56, Number 17. 2023. DOI 10.1088/1361-6463/acb8c7.

[37] Seyed M. Ghazali; Y. Baleghi. **"Pedestrian Detection in Infrared Outdoor Images Based on Atmospheric Situation Estimation".** Journal of AI and Data Mining, 7, 1, 2019, 1-16.