مقایسه اثر پنهان‌نگاری بر محتوای دیتای ارسالی در استانداردهای کدگذار صوتی MELP، CELP و LPC

پوریا اعتضادی‌فر[1*]، سعید طلعتی[2]، محمدرضا حسنی آهنگر[3]، مهدی ملازاده[4]

۱- استادیار، دانشگاه جامع امام حسین(ع)، ۲- دانشجوی دکتری، دانشگاه جامع امام حسین(ع)، ۳- استاد، دانشگاه جامع امام حسین(ع)، ۴- استادیار، دانشگاه جامع امام حسین(ع)

چکیده:

پنهان‌نگاری یکی از مهم‌ترین روش‌های انتقال امن اطلاعات حساس در دنیای جنگ الکترونیک است، همچنین پنهان‌نگاری داده‌های صوتی با توجه ظرفیت و پیچیدگی بالاتر، نسبت به سایر روش‌های پنهان‌نگاری که آن را شبیه به آنتروپی می‌کند موردتوجه و علاقه پژوهشگران حوزه امنیت اطلاعات قرار می‌گیرد. در این پژوهش کدینگ کدگذارهای صوتی LPC ، CELP وMELP شکسته شده که به‌عنوان یک نوآوری مهم در حوزه امنیت ملی اطلاعات و جنگ الکترونیک مطرح می‌شود، چراکه این کدگذارها جزو قدرتمندترین روش‌های کدگذاری صوتی هستند که توسط نیروهای ناتو برای انتقال صوت مورداستفاده قرار می‌گردند. در روش پیشنهادی این مقاله از تبدیل ویولت برای پنهان کردن داده‌ها در بیت کم‌ارزش استفاده‌شده است. نتایج شبیه‌سازی و ارزیابی مطابق جدول۱ نشان می‌دهد این روش با توجه به مقاومت بالا نسبت به سایر روش‌ها امنیت زیادی دارد و مقایسه این سه کدگذار بیانگر آن است که روش MELP دارای امنیت بالاتری نسبت به یکدیگر هستند.

واژه‌های کلیدی: پنهان‌نگاری، SNR، LPC، CELP، MELP

Comparing the Effect of Steganography on the Content of Transmitted Data in LPC, CELP, and MELP Audio Encoder's Standards

Pourya Etezadifar*[1], Saeed Talati [2], Mohammad Reza Hassani Ahangar [3], Mahdi Molazade[4]

1- Assistant Professor, Faculty of Electrical Engineering Department, Imam Hossein University, Tehran,Iran
Email: petezadifar@ihu.ac.ir (Corresponding Author)
2- PhD Candidate, Faculty of Electrical Engineering Department, Imam Hossein University, Tehran,Iran
3- Professor, Faculty of Electrical Engineering Department, Imam Hossein University, Tehran,Iran
4- Assistant Professor, Faculty of Electrical Engineering Department, Imam Hossein University, Tehran,Iran

Abstract

Information security is one of the most important issues today, which always receives the attention of many researchers. The purpose of steganography is to hide secret messages in a non-secret file so that it appears that no information is hidden in the carrier medium. Generally, steganography is one of the secure communication methods whose purpose is to hide information in the context of data and content; although audio steganography is not so widespread compared to image encryption, audio data can provide high capacity and due to its high complexity, it behaves like entropy, which makes these types of signals unrecognizable. The simulation and evaluation results of this article show the high security of the proposed method; by checking the SNR of the proposed method compared to other methods in Tab 1, we can conclude that this method is very robust. Also, by comparing the three examined encoders, it can be seen that the MELP method has the highest level of security, followed by the LPC and CELP methods.

Keywords: Steganography, Audio Encoder, LPC, CELP, MELP.

۱- مقدمه

روش کدگذار صوتی پیش‌بینی خطی[1] یکی از متداول‌ترین روش‌های کدگذار صوت است که صدای آنالوگ به دیجیتال با ۲۴۰۰ بیت بر ثانیه تبدیل می‌کند. این کدگذار صوتی یکی از روش‌های قدرتمند تجزیه‌وتحلیل با کیفیت بالاست که تخمین‌های بسیار دقیقی از پارامترهای صوتی ارائه می‌دهد [۱].

استاندارد کدگذار صوتی پیش‌بینی خطی برانگیخته از کد[2] صدای آنالوگ را به صدای دیجیتال با ۴۸۰۰ بیت بر ثانیه تبدیل می‌کند. این روش دارای کیفیت بالایی است و از آن در کدگذار گفتار صوتی MPEG-4 استفاده می‌شود [۲].

روش کدگذار صوتی روش پیش‌بینی خطی تحریک مختلط یکی از متداول‌ترین روش‌های کدگذار صوت است که صدای آنالوگ به دیجیتال با ۲۴۰۰ بیت بر ثانیه تبدیل می‌کند. از این روش عمدتاً در برنامه‌های نظامی و ارتباطات ماهواره‌ای، انتقال صوت امن و امنیت ارتباطات دستگاه‌های رادیویی استفاده می‌شود [۶]. در ادامه روش پیشنهادی پنهان‌نگاری در این سه کدگذار تشریح خواهد شد [۳].

۲- پنهان‌نگاری

روش‌های پنهان‌نگاری برای پنهان کردن یک پیام به‌طور نامحسوس در داخل علائم دیگر به کار می‌روند. اصل و اساس پنهان‌سازی، استفاده از فضاهایی از حامل اطلاعات هست که به هویت حامل لطمه وارد نکند. اطلاعات پنهان‌شده بدون اینکه ضرری به علائم وارد کنند، درون آن پنهان می‌شوند. حامل پیام می‌تواند صوت، تصویر، فیلم یا متن باشد [۴]. به‌منظور ارزیابی منطقی عملکرد انواع روش‌های پنهان‌نگاری، سه نیازمندی متداول امنیت، ظرفیت و نامحسوس بودن که معیارهایی برای میزان عملکرد روش‌های پنهان‌نگاری است بررسی می‌شوند با توجه به اینکه این سه معیار کیفی هستند نیاز است تا با استفاده از معیار SNR به ارزیابی عملکرد روش پیشنهادی بپردازیم که در ادامه این معیار تشریح می‌شود.

کدگذارهای صوت عموماً در نرخ بیت‌های کمتر از ۴/۸ کیلوبیت بر ثانیه استفاده می‌شوند. هدف اصلی کدگذارهای صوت[3] (برخلاف کدگذارهای موجک[4] که هدفشان به‌دست آوردن سیگنال گفتار با شبیه‌ترین حالت ممکن به سیگنال اصلی با حداکثر میزان سیگنال به نویز است) ساخت گفتار مصنوعی است که دارای کیفیت مشابه سیگنال اصلی باشد.

۳- معیار سیگنال به نویز (SNR)[5]

یکی از ویژگی‌های پنهان‌نگاری غیرقابل مشاهده بودن (نامحسوس بودن) است. منظور از غیرقابل مشاهده بودن توسط انسان این است که یک فرد عادی با شنیدن به صوت اولیه و صوت حاوی پیام نتواند بین دو صوت تفاوتی قائل شود. ازآنجاکه این معیار دقیق نیست باید معیاری تعریف شود تا توسط آن بتوان کارایی الگوریتم‌ها را درزمینه حفظ امنیت بسنجیم که این معیار SNR است و این مقیاس نشان‌دهنده میزان نویز اضافه‌شده به صوت پنهان‌نگاری در اثر تعبیه اطلاعات در صوت اصلی است. واحد این معیار db بوده و هرچه مقدار SNR بیشتر باشد صوت حاوی پیام پنهان‌نگاری از کیفیت ظاهری بهتری برخوردار است. SNR از رابطه (۱) محاسبه می‌شود:

$$SNR = 10\log\frac{s^2}{(s-sw)} \qquad (۱)$$

در این رابطه، s سیگنال حامل و sw سیگنال نهان‌نگاری شده است. [۵]

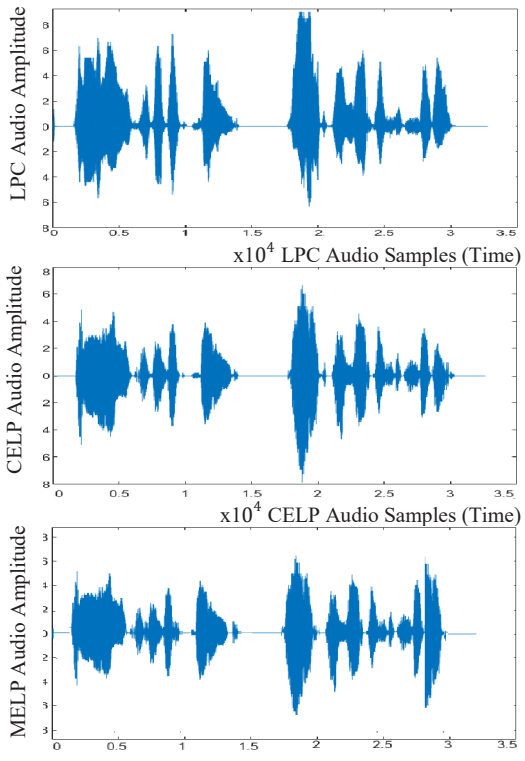
۴- روش پیشنهادی[6]

اکثر روش‌های پنهان‌نگاری به روش دامنه زمانی از تکنیک کدگذاری بیت کم‌ارزش استفاده می‌کنند[۵]. این روش یکی از اولین و ساده‌ترین روش‌هاست که برای پنهان‌کردن اطلاعات به دلیل ظرفیت و شفافیت بالا به‌طور گسترده استفاده مورداستفاده قرار می‌گیرد[۶]. هرچند استفاده از صدا به‌عنوان یک رسانه میزبان برای پنهان‌نگاری در مقایسه با پنهان‌نگاری تصویری آن‌چنان محبوب نیست[۷]؛ اما داده‌های صوتی می‌توانند ظرفیت بالاتری را برای پنهان کردن داده‌ها فراهم کنند. از دیگر مزایای LSB ترکیب آن با سایر تکنیک‌های پنهان‌نگاری است [۸]. در این مقاله و با استفاده از نرم‌افزار متلب به شبیه‌سازی

1 Linear Predictive Coding
2 FEDERAL STANDARD 1016
3 Voice Coders
4 Wavelet Coders

5 Bit Error Rate
6 LSB: least significant bit

سیگنال صوتی در سه کدگذارصوتی LPC، CELP و MELP پرداختیم که شکل۱ هیستوگرام خروجی طیف گفتار در سه استاندارد کدگذارصوتی LPC، CELP و MELP نشان می‌دهد.



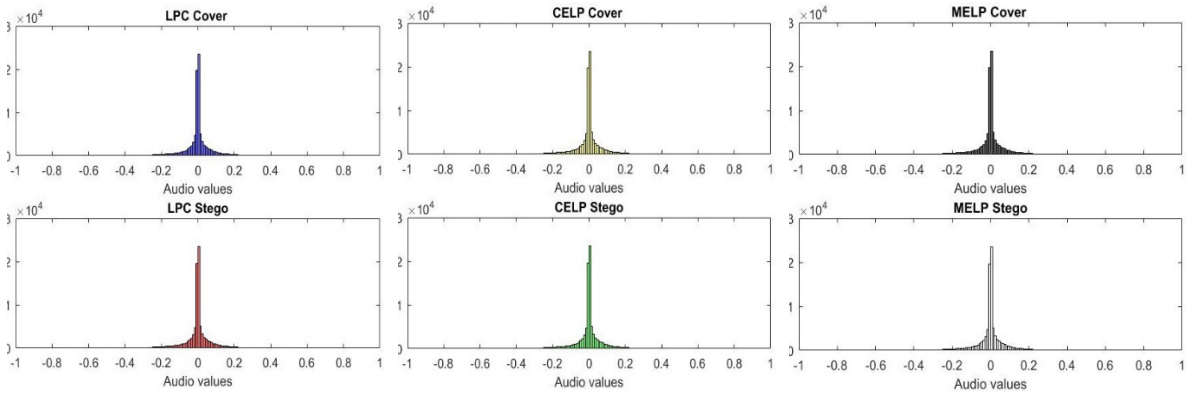
شکل۱- خروجی‌های هیستوگرام طیف گفتارهای (LPC، CELP و MELP)

در این مقاله از یک تصویر با ۲۵۶*۲۵۶ برای پنهان کردن در سه صدای موردنظر استفاده شد.

الگوریتم اولیه برای پنهان‌نگاری با استفاده از تبدیل ویولت در بیت کم‌ارزش به‌صورت زیر است:

- از تصویر حامل تبدیل ویولت گرفته می‌شود.
- ضرایب تبدیل ویولت تصویر میزبان به باینری تبدیل می‌گردند.
- تصویر لنا به کد اسکی[1] تبدیل می‌گردد.
- رشته بیتی باینری تصویر لنا در لابه‌لای ردیف‌های یکی از چهار جزء تبدیل ویولت پنهان می‌گردد.
- از ضرایب حاصل تبدیل ویولت معکوس گرفته می‌شود و صوت حامل پیام به‌دست می‌آید.

مقایسه خروجی هیستوگرام سه کدگذار صوتی LPC، CELP و MELP پس از پنهان‌نگاری به روش بیت کم‌ارزش پیشنهادی در این سه کدگذار صوتی در شکل ۲ آورده شده است.



شکل۲- مقایسه خروجی هیستوگرام سه کدگذار صوتی LPC، CELP و MELP پس از پنهان‌نگاری به روش پیشنهادی

با توجه به شباهت هیستوگرام خروجی صدای با پنهان‌نگاری و بدون پنهان‌نگاری می‌توان نتیجه گرفت که با مقایسه هیستوگرام خروجی نمی‌توان به تشخیص پنهان‌نگاری رسید. لذا این روش از مقاومت بالایی برخوردار

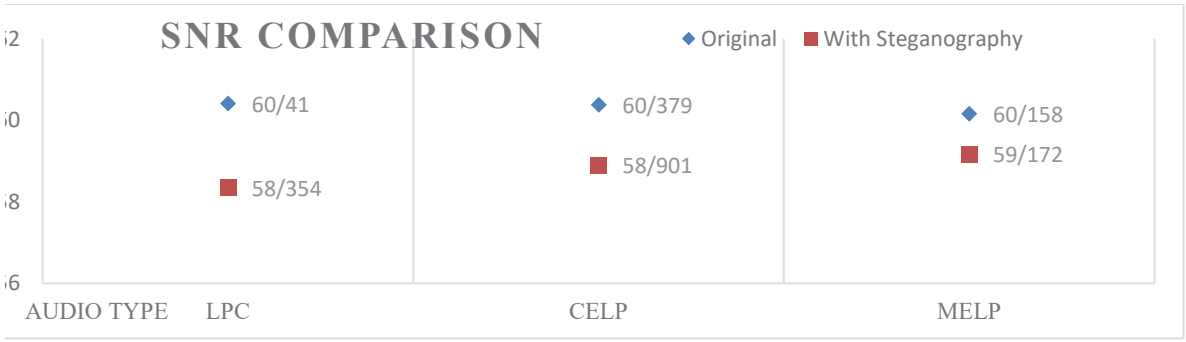
1 ASCII

است ولی با توجه به اینکه این بررسی کیفی است نیاز است تا با استفاده از معیار SNR به ارزیابی عملکرد این استانداردها و مقایسه آن‌ها بپردازیم. جدول ۱ نتایج مقایسه میزان SNR روش‌های مختلف پنهان‌نگاری با روش پیشنهادی پس از اعمال پنهان‌نگاری را نشان می‌دهد.

جدول۱- مقایسه میزان SNR روش‌های مختلف پس از پنهان‌نگاری

میزان SNR	الگوریتم موردبررسی	
۳۶	Steganographic Techniques and their use in an Open Systems Environment[9]	
۳۹	Increasing robustness of LSB audio steganography using a novel embedding method.[10]	
۴۲	Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding.[11]	
۳۹	Adaptive Digital Audio Steganography Based on Integer Wavelet Transform.[12]	
۴۹	High-Quality Audio steganography by Floating Substitution of LSBs in Wavelet Domain.[13]	
۵۵	Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography.[14]	
۳۶	Wavelet-Based Steganographic Method for Text Hiding in an Audio Signal. Sensors.[15]	
۵۸	A Robust Data Embedding Method for MPEG Layer III Audio Steganography.[16]	
۵۰	An audio steganography by a low-bit coding method with wave files.[17]	
۶۰.۴۱۰	LPC	روش پیشنهادی برای الگوریتم
۶۰.۱۵۸	CELP	
۶۰.۳۷۹	MELP	

همان‌طور که در مقایسه SNR در جدول شماره ۱ دیده می‌شود روش پیشنهادی در برابر سایر روش‌های بررسی‌شده دارای مقاومت بالاتری است. در ادامه و در شکل۳ به مقایسه مقادیر SNR در حالت‌های باوجود پنهان‌نگاری و بدون وجود پنهان‌نگاری در این سه استاندارد پرداخته‌شده است تا متوجه شویم کدام‌یک از این سه استاندارد پس از پنهان‌نگاری عملکرد بهتری خواهند داشت.



شکل۳- مقایسه تغییرات مقادیر SNR استانداردهای کدگذار صوتی LPC, CELP, MELP بعد از اعمال پنهان‌نگاری

۵- نتیجه‌گیری

در این مقاله استانداردهای کدگذار صوتی LPC، CELP و MELP کاملاً تشریح و با استفاده از نرم‌افزار متلب یک‌صدا انتخاب شد و با استفاده از این سه کدگذار شبیه‌سازی گردید؛ در ادامه برای افزایش امنیت انتقال پیام یک روش پنهان‌نگاری بر مبنای بیت کم‌ارزش با استفاده از تبدیل ویولت انتخاب و بر روی این سه استاندارد استفاده

شد که نتایج مقایسه روش پیشنهادی با سایر روش‌ها و بررسی معیار SNR به‌دست‌آمده مستخرج از جدول ۱ نشان می‌دهد روش پیشنهادی دارای میزان سیگنال به نویزی بالاتری نسبت به سایر روش‌هاست و البته با مقایسه این سه کدگذار در شکل ۳ متوجه می‌شویم کدگذار MELP دارای مقاومت بالاتری نسبت به کدگذارهای LPC و CELP است و همین‌طور استاندارد LPC دارای امنیت بالاتری نسبت به CELP است.

مراجع

1. J. J. D. van Schalkwyk, D. J. Joubert and J. G. van der Linde, "Linear predictive speech coding at 2400 b/s," in Transactions of the South African Institute of Electrical Engineers, vol. 84, no. 3, pp. 146-152, June 1993.
2. M. Schroeder and B. Atal, "Code-excited linear prediction (CELP): High-quality speech at very low bit rates," ICASSP '85. IEEE International Conference on Acoustics, Speech, and Signal Processing, 1985, pp. 937-940, doi: 10.1109/ICASSP.1985.1168147.
3. A. V. McCree and T. P. Barnwell, "A mixed excitation LPC vocoder model for low bit rate speech coding," in IEEE Transactions on Speech and Audio Processing, vol. 3, no. 4, pp. 242-250, July 1995.
4. Talati, S., Etezadifar, P. (2020). '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.
5. Etezadifar, P., Talati, S., Hassani Ahangar, M. R., Molazade, M. (2023). 'Investigation of Steganography Methods in Audio Standard Coders: LPC, CELP, MELP', Majlesi Journal of Telecommunication Devices, doi: 10.30486/mjtd.2022.695928.
6. Muhammad Asad; Junaid Gilani; Adnan Khalid, An enhanced least significant bit modification technique for audio steganography, International Conference on Computer Networks and Information Technology, July 2011.
7. H. Liu, J. Liu, R. Hu, X. Yan and S. Wan, "Adaptive audio steganography scheme based on wavelet packet energy," in IEEE International Conference on High Performance and Smart Computing (HPSC), 2017.
8. Samir Kumar, Bandyopadhyay Barnali, Gupta Banik, LSB Modification and Phase Encoding Technique of Audio Steganography Revisited, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2012.
9. Bao, Ma, "Steganographic Techniques and their use in an Open Systems Environment", Bret Dunbar, The information Security reading Room, SANS Institute 2002.
10. N. Cvejic and T. Seppanen, "Increasing robustness of LSB audio steganography using a novel embedding method," International Conference on Information Technology: Coding and Computing. Proceedings. ITCC 2004, Las Vegas, NV, USA, 2004, pp. 533-537 Vol.2, doi: 10.1109/ITCC.2004.1286709.
11. Cvejic, N. and Seppänen, T., 2005. Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding. J. Univers. Comput. Sci, 11(1).
12. Delforouzi, A., Pooyan, M. "Adaptive Digital Audio Steganography Based on Integer Wavelet Transform". Circuits Syst Signal Process 27, 247–259 (2008). https://doi.org/10.1007/ s00034-008-9019-x.
13. Mansour Sheikhan et al, High-Quality Audio steganography by Floating Substitution of LSBs in Wavelet Domain, world applied science Journal IDOSI publications, 2010.
14. S. S. Divya and M. R. M. Reddy,

“Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography,” Int. J. Sci. Technol. Res., vol. 1, no. 6, pp. 68–70, 2012.

15. Veselska, O.; Lavrynenko, O.; Odarchenko, R.; Zaliskyi, M.; Bakhtiiarov, D.; Karpinski, M.; Rajba, S. A “Wavelet-Based Steganographic Method for Text Hiding in an Audio Signal”. Sensors 2022.
16. Mohsen Bazyar and Rubita Sudirma, “A Robust Data Embedding Method for MPEG Layer III Audio Steganography”, International Journal of Security and Its ApplicationsVol.9, No.12 (2015).
17. M. Wakiyama, Y. Hidaka, and K. Nozaki, “An audio steganography by a low-bit coding method with wave files,” Proc. - 2010 6th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIHMSP 2010, pp. 530–533, 2010, doi: 10.1109/IIHMSP.2010.135.
18. Hashemi, Seyed & Barati, Shahrokh & Talati, S. & Noori, H. (2016). “A genetic algorithm approach to optimal placement of switching and protective equipment on a distribution network”. Journal of Engineering and Applied Sciences. 11. 1395-1400.
19. 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.
20. 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.
21. Talati, S., & Alavi, S. M. (2020). “Radar Systems Deception using Cross-eye Technique”. Majlesi Journal of Mechatronic Systems, 9(3), 19-21.
22. Saeed Talati, mohamadreza Hasani Ahangar (2020) “Analysis, Simulation and Optimization of LVQ Neural Network Algorithm and Comparison with SOM”, MJTD, vol. 10, no. 1.
23. 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.
24. 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.
25. 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.
26. Talati, Saeed, Hassani Ahangar, Mohammad Reza. (2021). “Radar Data Processing Using a Combination of Principal Component Analysis Methods and Self-Organized and Digitizing Learning Vector Neural Networks”, Electronic and Cyber Defense, 9 (2), pp. 1-7.
27. 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).
28. 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.
29. 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

Eavesdroppشing UAV', Electronic and Cyber Defense, 11(2), pp. 45-56.

Issue No.1- ISSN: 1692-343X, Medellín-Colombia. April 2017.

30. 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.
31. 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.
32. Ghazali, S. M., Baleghi, Y. “Pedestrian Detection in Infrared Outdoor Images Based on Atmospheric Situation Estimation” Journal of AI and Data Mining, 2019; 7(1): 1-16. doi: 10.22044/jadm.2018.5742.1696
33. Talati, S., Ghazali, S. M., Hassani Ahangar, M., & Alavi, S. M. (2021). “Analysis and Evaluation of Increasing the Throughput of Processors by Eliminating the Lobe’s Disorder” Majlesi Journal of Telecommunication Devices, 10(3), 119-123. https://doi.org/10.52547/mjtd.10.3.119
34. 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.
35. EtezadiFar. P., Talati. S., Hassani Ahangar. M.R., Molazade. M., “Investigation of Steganography Methods in Audio Standard Coders: LPC, CELP, MELP” Majlesi Journal of Telecommunication Devices, 12(1), in press, 2023.
36. Soltaninia, V., Talati, S., Hasani Ahangar, M., Samsami Khodadad, F., Baei, P. (2023). 'Security of UAV Relay Networks based on Covert Communication in the Presence of an