SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 4 | April 2020 - Peer Reviewed Journal

ANTI-FORENSICS: COUNTERING SENSOR NOISE CAMERA IDENTIFICATION

Nikhith Suvarna
Master of Computer Applications,Jain University,Bangalore, India

Article DOI: https://doi.org/10.36713/epra4271

ABSTRACT

In simple terms, Anti-Forensics can be told as the techniques used to counter forensic analysis done by forensic investigators. This paper mainly focuses on some of the most used anti-forensics techniques along with the challenges the forensics investigator faces. There are many tools and techniques available that when used properly can be highly effective against the forensic analysis techniques. Various tools assist you against various anti-forensics techniques like Elimination of evidence source, Data hiding, and Trail obfuscation. These techniques are used mainly to make the investigation consume more time and money. Sensor Noise Camera Identification is a way to link a photo with the camera the photo was taken from using a noise signature that is unique for every camera.

KEYWORDS: *Anti-Forensics (AF), Forensic Analysis, Anti-Forensic Techniques, Sensor Noise Camera Identification*

1. INTRODUCTION

Advanced technology has become the integral part of our life. To satisfy the need of the society, almost in each work, we use the technology and its applications. It has many real life applications such as internet of things [1, 2, 3, 4, 5, 6, 7, 8], SPP [9, 10, 11, 12, 13, 14, 15, 16], TP [17, 18, 19], PowerShell [20], uncertainty [21, 22, 23], cloud computing [24], artificial intelligence [25], internet Security [26], and so on. Information Communication Technology (ICT) is the mode by which user can use computers and internet to store, fetch, communicate and utilize the information. So all the organizations, industries and also every individual are using computer systems to preserve and share the information. The internet security plays a major role in all computer related applications. The internet security appears in many real-life applications, e.g., smart parking [27], home security, banking system, education sector, defense system, railway, and so on. In this manuscript we discuss about the protection of authentication which is a part of internet security.

Digital Forensics is gaining a lot of scope in the past few years mainly because Cybercrime is gradually increasing day by day. Digital Forensics is the process of collecting, preserving, analyzing and reporting the evidence found to the court without any tampering of the evidence and finally create a detailed report of the forensic analysis process and the evidence found. Anti-forensics techniques are used by Cybercriminals to be under the radar and make the forensic process more time consuming and costly. Anti-forensics, on the other hand, deals with the techniques used to cover the tracks or destroy digital data that can be submitted as evidence in the court of law. Some of the techniques used are Data Hiding, Artefact Wiping, Trail obfuscation. There are various digital forensics techniques [28].

- Data Recovery: As the name suggests in this technique the forensic investigators try to recover data from the confiscated storage medium if in any case the data in those mediums have been deleted by the attacker. Some of the tools that are used for data recovery are Stellar Data Recovery, PC-3000, SysTools Data Recovery [29] .
- File Carving: When the data on your storage medium is deleted the data cannot be viewed through the standard file explorer. This is when the concept of file carving comes in handy, it allows you to recover deleted files based on the content that was present in the before deletion. The used for file carving are Autopsy, Foremost [29].
- Header Analysis: This technique is used for email related crime investigations. Email Header contains some useful metadata that contains data like the IP address of the device from which the message was sent. This IP address can then be used to track

down the attacker. A tool like Email Tracker Pro can be used for this task [29].

- Known File Filtering: This technique is used when you have a large number of files and the investigator has to find specific files. This eliminates the need to go through all the files. Forensic Toolkit (FTK) is one such tool that can be used for this purpose [29].
- Network Sniffing: In this technique, the investigator will sniff the traffic that is being transmitted over the network, this is logged and analyzed. Wireshark and tcpdump are the popular tools used for network analysis [29].
- Sensor Noise Camera Identification: This technique uses subtle pixel anomalies caused by the camera hardware to identify a unique noise signature for every camera. Camera fingerprinting can be used to match a photo to a camera.

2. LITERATURE REVIEW

Sensor Noise Camera Identification also is known as Camera Fingerprinting this is a problem because it is also a technique for deanonymizing people and this can be done to a high degree of accuracy. Major tech companies and corporations already have this technology. There are many techniques used for countering Sensor Noise Camera Identification namely forgery. Camera fingerprinting is weak against forgery. [30] for example:- The attacker takes two images from two different cameras, after which the attacker can estimate the photo fingerprint and paste the same onto the second image by doing so the attacker makes the second image look like it's taken from the first camera. But this can be countered by making use of Digital X-ray [31] technique.

Sensor noise extracted from images can also be served as the camera fingerprint and this can be done using an approach suggested by Chang-Tsun Li [32, 33] were in he proposed the use of an SPN Enhancer which provides an increased rate of device identification.

So keeping that in mind we use a defense in depth approach by firstly using the method proposed and also chaining it with some of the operational mitigation which I suppose would be a solution for the problems mentioned above.

3. EXISTING SYSTEM

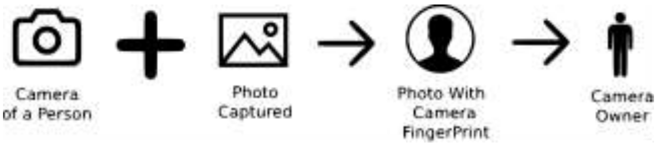


Figure 3.1: Camera Fingerprinting

What is Camera Fingerprinting?

Every camera is unique this is mainly due to something known as production tolerance. Each sensor produced for a smartphone is slightly different from one sensor to another it's these slight differences between the products is what causes the camera fingerprint [34].The noise signature is due to environmental heat and defectiveness on the Charge-coupled device itself which is a type of camera sensor [35]. To find the camera fingerprint each and every picture must be examined pixel by pixel for patterns. This technique works on each and every digital camera produced till date. Analog cameras are not safe either as these kinds of techniques exist for analog camera's too [34].

How does Camera Fingerprinting Work

Step 1: A photo is taken from a camera that belongs to an individual– The camera may be a digital camera or an analog camera that belongs to an individual from which the photo is captured.

Step 2: The photo captured will be generated in combination with a camera fingerprint that is unique for that camera – When the photo captured is generated it is combined with the camera fingerprint which is unique to that camera sensor.

Step 3: The photo-generated by this camera can be used to identify the owner of the camera by extracting and analyzing the camera fingerprint – As told earlier each camera sensor is unique and this can be used to identify the owner of the camera. Ex: If someone had to find who took a particular photo then they could extract the camera fingerprint from image and by inquiring the sensor manufacturer which camera was that sensor used in. Indirectly linking back to the camera owner.

Note:- Camera Fingerprint along with EXIF metadata can be used to identify an individual.

4. ANTI-FORENSICS

- Encryption: Encryption is the most commonly used Anti-Forensic technique [36] by attackers to make the data unreadable which can be used as evidence in the court of law. Some of the encryption algorithms are AES, 3DES, RSA, etc.
- Steganography: It is the process of hiding confidential data within various types of files such as Image, Video, Audio, etc. Some of the tools that can be used for this purpose are as follows StegHide, Crypture [36]
- Scrubbing Metadata/Timestamps: Changing or deleting on metadata and timestamps is another Anti-Forensic technique used. When an image is clicked via a camera the image will contain some data about the image itself such as "When the photo was

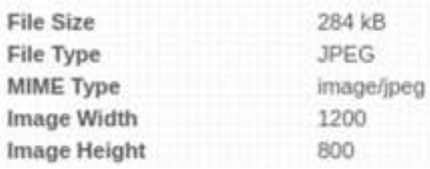
clicked", "GPS coordinates", "Name of the owner of the photo" etc. So deleting these data is necessary. Some tools used for this purpose are EXIF tool, JPEG & PNG Stripper [36].

- Wiping a Hard Drive: Wiping the hard drive multiple times and filling it with garbage values mostly with zeros. The wiping methods differ for both Solid State Drives and Mechanical Drives. There are different methods of wiping a hard drive but the most common methods are the Gutmann Method and Department of Defense 7 pass method [36].
- Analyzing the Quantification Matrix: For this method to work, a reference image is required in order to compare. Here the quantization matrix of both the images are counted and extracted. This is also known as quantification matrix, basically it is nothing but a set of values that are used for representing the image [37].
- Analyzing of Photo Response Non-Uniformity (PRNU): Photo Response Noise is an unique characteristic of every digital camera sensor. In this technique the PRNU pattern of the images that has to be analyzed is obtained and compared by using a correlation process. Both the images should be flat meaning the lighting condition for both the images should be the same. The photo acquired with the camera in question will have a value close to one and the photo acquired with the camera in question will have the value zero or even negative [37].
- Disable Logging: The system keeps logs of events that have occurred from the installation of software to system crash logs. Some of the tools used for this purpose are Auditpol and Winzapper [36].
- Adding Noise to Images: An image compression history can be used by a forensic investigator in order to determine whether the image has been modified, gain information on the camera from which the image was generated and also to know the regions that were forged [38].

5. PROPOSED SYSTEM

Since Sensor Noise Camera Identification uses unique noise signatures to identify every camera. So the most effective way to remove the noise signatures is by creating more noise.

Step 1: Remove any camera info that can be used to link back to you. Often when a image is clicked using a camera a data file is created this data contains information of the manufacturer of the camera, ISO setting, date and time when the image was captured etc. One way to remove this data is by using a tool such as EXIFtool, but alternatively you can open the image in photoshop and save it to web. When promted save in JPEG compression with the image quality being no greated that 60% this adds a lot of random noise which makes it hard to create noise signature [35] .



File Size	284 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	1200
Image Height	800

Figure 5.1: Remove Camera Information

Step 2: Cleaning your camera lens regularly with a smooth cloth removes dirt that will show up in every image you click and will never change. Thus making it very easy to identify you [35] .

Figure 5.2: Clean the Camera Lens

Step 3: So to avoid this from happening you will have to crop the image this makes the position of the static pixels to shift hence when compared it looks like noise [35].

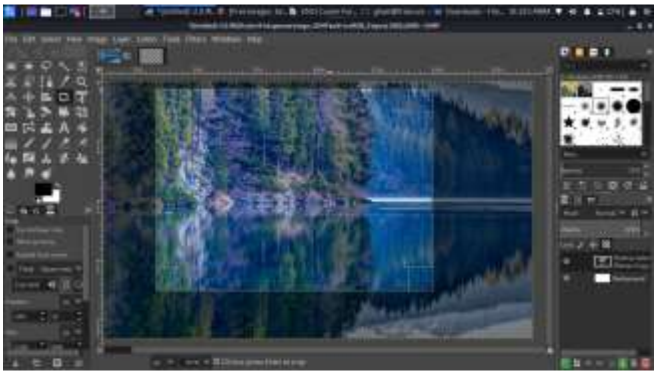


Figure 5.3: Crop the Image

Step 4: First open the image in an image editor like Gimp or Photoshop and resize the image [35] i.e. if the image is of

1366x768 pixels then resize it to 1600x900 pixels, now that the image is resized save it.

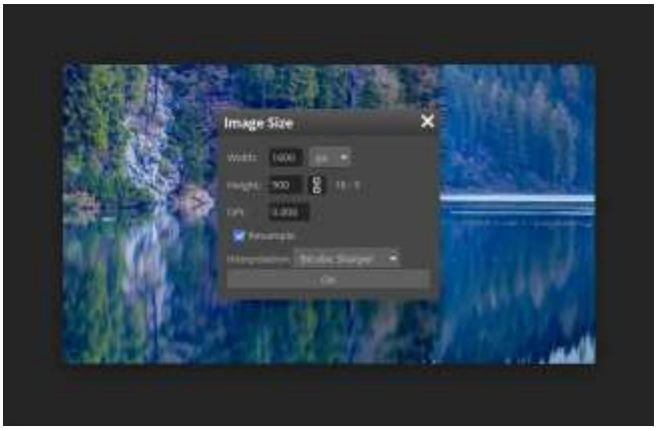


Image Size
Width: 1600 px
Height: 900 16 : 9
DPI: 3.000
☑ Resample
Interpolation: Bicubic Sharper
Ok

Figure 5.4: Resize the Image

Step 5:Crop the image and save the image using bi-cubic compression [35] .

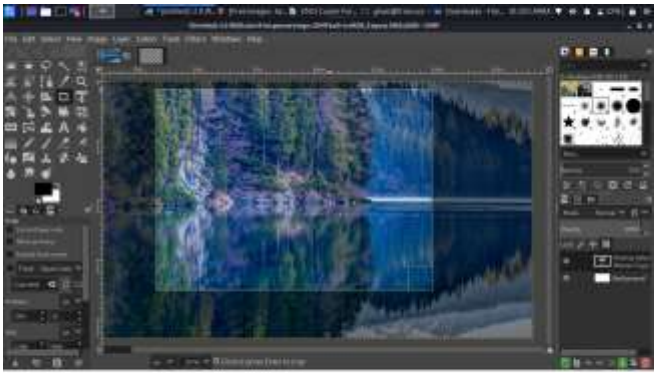
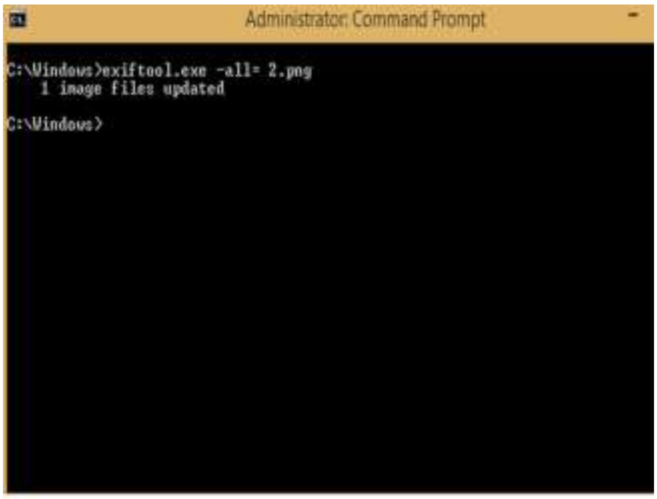


Figure 5.5: Crop using Bi-Cubic Compression

Step 6: Use the exiftool to remove any EXIF information. By using the command exiftool.exe –all= "filename.jpg" [35]



```
C:\Windows>exiftool.exe -all= 2.png
    1 image files updated

C:\Windows>
```

Figure 5.6: Erase EXIF Data using exiftool

Step 7: Next we blur and then deblur the image doing so will remove the camera fingerprint associated with the image [34].

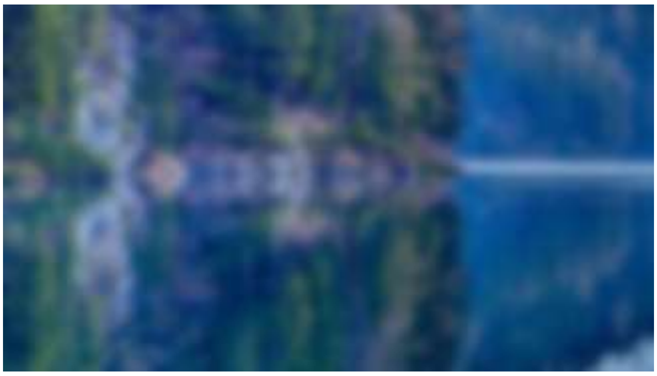


Figure 5.7: Original Image Blurred

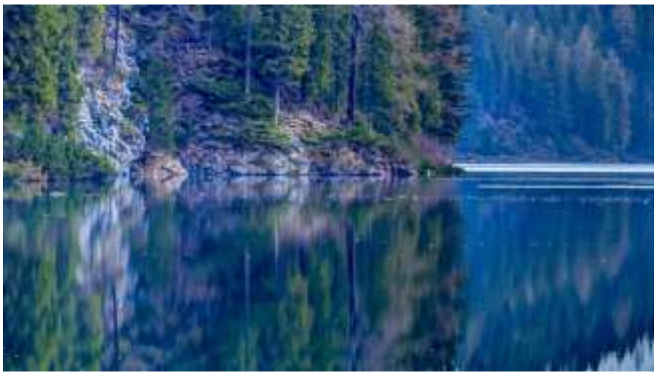
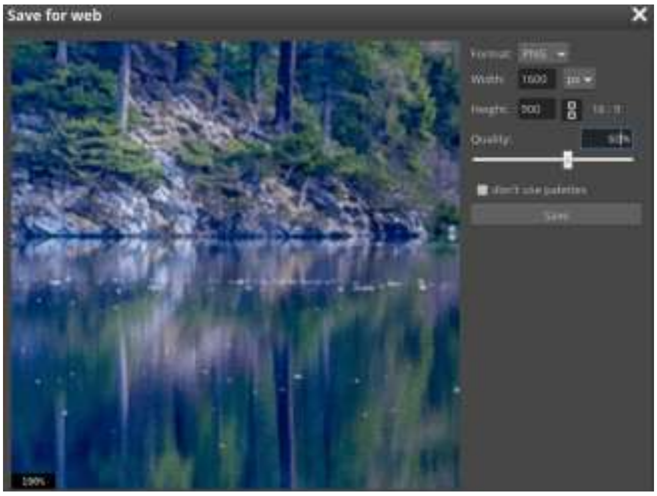


Figure 5.8: Original Image Deblurred

Step 8: Now click on Save for Web and reduce the quality of the image to at least 50 this should make the noise unrecognizable [35] [7]



Save for web

Format: PNG

Width: 1600 px

Height: 900 16 : 9

Quality: 50%

□ don't use palettes

Figure 5.9: Save for Web with Reduced Quality

6. Operational Mitigation against Sensor Noise Camera Identification

- Use a separate camera for different purposes. - Using a separate camera if you don't want any attributed linked back to you in the future then you have to use a separate camera.
  - Avoid using smartphones as a camera – As mention above already each sensor even if it is built for the same smartphone in the same production area each and every sensor is slightly different then each other which makes it unique for every smartphone.
  - Use CyanogenMod if you must use a smartphone camera. - If you are to use a smartphone camera then use the open-source firmware CyanogenMod as preference. One nice tool to use if you are using a smartphone is Obscura Camera available here. In [39] the authors have used a standard camera without a cellular or Wi-Fi connection. - Next use a standard camera that doesn't have any cellular or WiFi connection.
  - Leave no money trail between you and the camera you buy – Best way to buy a camera without linking it back to you is by making use of anonymizing services such as TOR, VPN and the payment should be done using a cryptocurrency such as Monero.
  - Don't do anything stupid! - Don't use your personal camera to click pictures that you want to post online. Use a separate camera as suggested above which is purchased using the recommended anonymizing service and payment method.
  - Use metadata and EXIF sanitization software. - Use software such as EXIFtool to clear the metadata from the captured images before posting it online.
  - Use the TOR browser to post the image anonymously. - If you care about your privacy online the use the TOR browser to post the photos online.
  - A film camera can be used as an alternative – You can use a film camera instead of a smartphone or also a digital camera – If you are one of those people who are extremely paranoid then you can use a film camera to capture the photos and scan them with multiple scanners at multiple scanning centres.
  - Wait before posting – Finally wait for a few days before posting the image online as this will make it difficult for anyone to link it back to you.
  - Don't Cross Contaminate Aliases or your real identity by using your personal camera to post images online.

7. Result

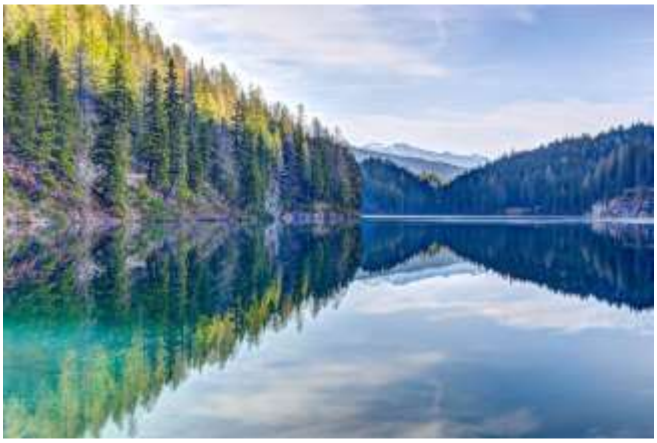


Figure 7.1: Original Image

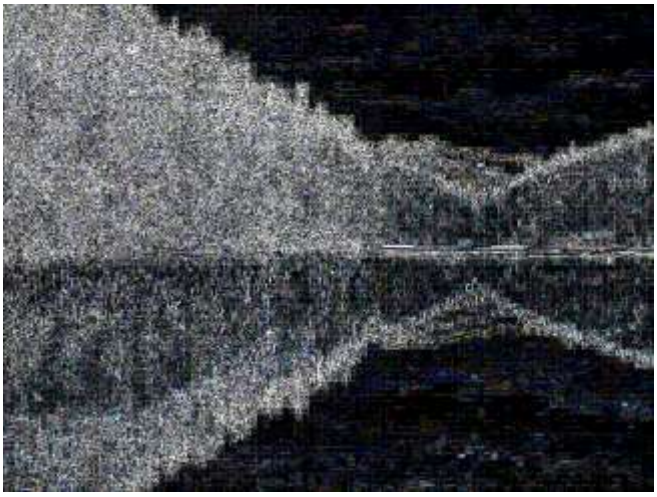


Figure 7.3: Noise Analysis after the use of Proposed Method

8. CONCLUSION

This paper proposes a new anti-forensic technique to counter sensor noise camera identification where in which we make use of image manipulation techniques such as Image resizing, Cropping, Removing Exit Metadata, Image Blurring and Deblurring to scrub the camera fingerprint from the photo-generated. In addition to this we also discuss some operational controls that can be used along with the proposed methodology in order to achieve defence in depth approach.

9. ACKNOWLEDGMENT

I would like to express my profound gratitude to my guide Dr. Hitesh Mohapatra, for their patient, encouragement and valuable assessments of this research work. I appreciate his willingness to generously contribute time.

BIBLIOGRAPHY

[1] H. Mohapatra, "HCR using neural network," 2009.

[2] H. Mohapatra and A. Rath, "Detection and avoidance of water loss through municipality taps in india by using smart tap and ict," IET Wireless Sensor Systems, vol. 9, no. 6, pp. 447-457, 2019.

[3] H. Mohapatra and A. Rath, "Fault tolerance in WSN through PE-LEACH protocol," IET Wireless Sensor Systems, vol. 9, no. 6, pp. 358-365, 2019.

[4] H. Mohapatra, S. Debnath and A. Rath, "Energy management in wireless sensor network through EB-LEACH," International Journal of Research and Analytical Reviews (IJRAR), pp. 56-61, 2019.

[5] V. Nirgude, H. Mahapatra and S. Shivarkar, "Face recognition system using principal component analysis & linear discriminant analysis method simultaneously with 3d morphable model and neural network BPNN method," Global Journal of Advanced Engineering Technologies and Sciences, vol. 4, p. 1, 2017.

[6] M. Panda, P. Pradhan, H. Mohapatra and N. Barpanda, "Fault tolerant routing in heterogeneous environment," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 8, pp. 1009-1013, 2019.

[7] H. Mohapatra and A. Rath, "Fault-tolerant mechanism for wireless sensor network," IET Wireless Sensor Systems, vol. 10, no. 1, pp. 23-30, 2020.

[8] D. Swain, G. Ramkrishna, H. Mahapatra, P. Patra and P. Dhandrao, "A novel sorting technique to sort elements in ascending order," International Journal of Engineering and Advanced Technology, vol. 3, pp. 212-126, 2013.

[9] S. Broumi, A. Dey, M. Talea, A. Bakali, F. Smarandache, D. Nagarajan, M. Lathamaheswari and R. Kumar, "Shortest path problem using Bellman algorithm under neutrosophic environment," Complex & Intelligent Systems, vol. 5, pp. 409--416, 2019.

[10] R. Kumar, S. Edalatpanah, S. Jha, S. Broumi, R. Singh and A. Dey, "A multi objective programming approach to solve integer valued neutrosophic shortest path problems," Neutrosophic Sets and Systems, vol. 24, pp. 134-149, 2019.

[11] R. Kumar, A. Dey, F. Smarandache and S. Broumi, "A study of neutrosophic shortest path problem," in Neutrosophic Graph Theory and Algorithms, F. Smarandache and S. Broumi, Eds., IGI-Global, 2019, pp. 144-175.

[12] R. Kumar, S. Edalatpanah, S. Jha and R. Singh, "A novel approach to solve gaussian valued neutrosophic shortest path problems," International Journal of Engineering and Advanced Technology, vol. 8, pp. 347-353, 2019.

[13] R. Kumar, S. Edalatpanah, S. Jha, S. Gayen and R. Singh, "Shortest path problems using fuzzy weighted arc length," International Journal of Innovative Technology and Exploring Engineering, vol. 8, pp. 724-731, 2019.

[14] R. Kumar, S. Edaltpanah, S. Jha, S. Broumi and A. Dey, "Neutrosophic shortest path problem," Neutrosophic Sets and Systems, vol. 23, pp. 5-15, 2018.

[15] R. Kumar, S. Jha and R. Singh, "A different approach for solving the shortest path problem under mixed fuzzy environment," International Journal of fuzzy system Applications, vol. 9, no. 2, pp. 132-161, 2020.

[16] R. Kumar, S. Jha and R. Singh, "Shortest path problem in network with type-2 triangular fuzzy arc length," Journal of Applied Research on Industrial Engineering, vol. 4, pp. 1-7, 2017.

[17] R. Kumar, S. Edalatpanah, S. Jha and R. Singh, "A Pythagorean fuzzy approach to the transportation problem," Complex and Intelligent System, vol. 5, pp. 255-263, 2019.

[18] J. Pratihar, R. Kumar, A. Dey and S. Broumi, "Transportation problem in neutrosophic environment," in Neutrosophic Graph Theory and Algorithms, F. Smarandache and S. Broumi, Eds., IGI-Global, 2019, pp. 176-208.

[19] J. Pratihar, S. E. R. Kumar and A. Dey, "Modified Vogel's Approximation Method algorithm for transportation problem under uncertain environment," Complex & Intelligent Systems (Communicated).

[20] H. Mohapatra, S. Panda, A. Rath, S. Edalatpanah and R. Kumar, "A tutorial on powershell pipeline and its loopholes," International Journal of Emerging Trends in Engineering Research, vol. 8, no. 4, 2020.

[21] S. Gayen, F. Smarandache, S. Jha and R. Kumar, "Interval-valued neutrosophic subgroup based on interval-valued triple t-norm," in Neutrosophic Sets in Decision Analysis and Operations Research, M. Abdel-Basset and F. Smarandache, Eds., IGI-Global, 2019, p. 300.

[22] S. Gayen, F. Smarandache, S. Jha, M. Singh, S. Broumi and R. Kumar, "Introduction to plithogenic subgroup," in Neutrosophic Graph Theory and Algoritm, F. Smarandache and S. Broumi, Eds., IGI-Global, 2020, pp. 209-233.

[23] S. Gayen, S. Jha, M. Singh and R. Kumar, "On a generalized notion of anti-fuzzy subgroup and some characterizations," International Journal of Engineering and Advanced Technology, vol. 8, pp. 385-390, 2019.

[24] X. Xu, "From cloud computing to cloud manufacturing," Robotics and Computer-Integrated Manufacturing, vol. 28, pp. 75-86, 2012.

[25] M. Haenlein and A. Kaplan, "A brief history of artificial intelligence: on the past, present, and future of artificial intelligence," California Management Review, vol. 61, pp. 5-14, 2019.

[26] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. Parizi and G. Srivastava, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," Internet of Things, pp. 100-111, 2019.

[27] H. Mohapatra and A. K. Rath, "An IoT based Efficient Multi-Objective Real-Time Smart Parking System," IET Wireless Sensor Systems, 2020.

[28] K. H. a. S. Gruičić, "Anti-computer forensics," in 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2017.

[29] "ObscuraCam: Secure Smart Camera," Guardian Project, [Online]. Available: https://guardianproject.info/apps/obscuracam/.

[30] M. &. F. J. &. C. M. Goljan, "Sensor Noise Camera Identification: Countering Counter-Forensics," in SPIE - The International Society for Optical Engineering, San Jose, 2010.

[31] M. &. F. J. &. L. J. &. G. M. Chen, "Imaging Sensor Noise as Digital X-Ray for Revealing Forgeries," in International Workshop on Information Hiding, Saint Malo, France, 2007.

[32] C.-T. Li, "Source Camera Identification Using Enhanced Sensor Pattern Noise," in IEEE Transactions on Information Forensics and Security, 2010.

[33] C.-T. Li, "Source camera linking using enhanced sensor pattern noise extracted from images," in 3rd International Conference on Imaging for Crime Detection and Prevention, London, UK, 2009.

[34] "Computer Forensics: Anti-Forensic Tools & Techniques," Infosecinstitute, 2019. [Online]. Available: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/anti-forensic-tools-techniques/.

[35] C. Chen, "Researchers show that your smartphone’s camera fingerprint allows anyone to track videos and pictures back to you," privateinternetaccess, 2016. [Online]. Available: https://www.privateinternetaccess.com/blog/smartphones-camera-fingerprint-allows-anyone-track-videos-pictures-back/.

[36] "Computer Forensics: Forensic Tools & Techniques," Infosecinstitute, 2019. [Online]. Available: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/forensic-techniques-part-1/.

[37] m1k3y, "Avoiding Camera Noise Signatures," Instructables, 2010. [Online]. Available: https://www.instructables.com/id/Avoiding-Camera-Noise-Signatures/.

[38] S. K. T. W. S. L. a. K. J. R. L. M. C. Stamm, "Anti-forensics of JPEG compression," in IEEE International Conference on Acoustics, Speech and Signal Processing, Dallas, US, 2010.

[39] M. Á. Mendoza, "Forensic analysis techniques for digital imaging," We Live Security, 2017. [Online]. Available: https://www.welivesecurity.com/2017/01/13/forensic-analysis-techniques-digital-imaging/.