

University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

Library Philosophy and Practice (e-journal)

Libraries at University of Nebraska-Lincoln

May 2021

A Bibliometric Analysis of Face Presentation Attacks based on Domain Adaptation

Smita C. Khairnar

Symbiosis International University and Pimpri Chinchwad College of Engineering, SPPU, Pune, India, chavansmita31@gmail.com


Shilpa Shailesh Gite Dr.

Symbiosis Institute of Technology (SIT), Symbiosis Centre for Applied Artificial Intelligence (SCAAI), Symbiosis International University, Lavale, Pune, India, shilpa.gite@sitpune.edu.in

Sudeep D. Thepade Dr.

Pimpri Chinchwad College of Engineering, SPPU, Pune, India, sudeepthepade@gmail.com

Follow this and additional works at: <https://digitalcommons.unl.edu/libphilprac>

 Part of the [Digital Communications and Networking Commons](#), and the [Library and Information Science Commons](#)

Khairnar, Smita C.; Gite, Shilpa Shailesh Dr.; and Thepade, Sudeep D. Dr., "A Bibliometric Analysis of Face Presentation Attacks based on Domain Adaptation" (2021). *Library Philosophy and Practice (e-journal)*. 5454.

<https://digitalcommons.unl.edu/libphilprac/5454>

A Bibliometric Analysis of Face Presentation Attacks based on Domain Adaptation

Smita Khairnar^a, Shilpa Gite^{b*}, Sudeep D Thepade^c

^aComputer Engineering, Symbiosis International University & Pimpri Chinchwad college of Engineering, SPPU, Pune, India, chavansmita31@gmail.com

^b Associate Professor, CS Department, Symbiosis Institute of Technology (SIT), Symbiosis Centre for Applied Artificial Intelligence (SCAAI), Symbiosis International University, Lavale, Pune, India, shilpa.gite@sitpune.edu.in

^cProfessor, Computer Engineering, Pimpri Chinchwad college of Engineering, SPPU, Pune, India, sudeepthepade@gmail.com

ABSTRACT

Background: This research aims to look into the work that has been done on Face Presentation attacks and detection with domain adaptation techniques from 2011 to 2021 utilizing bibliography methods.

Approaches: Diverse research articles on Face Presentation Attacks were retrieved using the two most popular databases Web of Science & Scopus. Research articles consider between 2011-2021. Some research results, such as documents by year, documents by source, documents by funding agencies, countries, etc are obtained using Web of Science and Scopus Analyzers. The analysis is performed using Vos Viewer version 1.6.16 and various parameters such as keywords, co-authorship, co-occurrences, citation analysis, and so on.

Results: We present findings for both the Web of Science and Scopus datasets in this paper. As a result of primary keywords as Face Presentation attacks and secondary keywords as domain adaptation-based Face anti-spoofing, the total no of documents is 117 and 151 respectively retrieved. The maximum number of documents are published in the year 2020, most of the research is carried out by China as it has maximum funding research agencies.

Conclusions: The purpose of using two databases for analysis in this study is to reduce the efforts of research scholars in analyzing the two most popular databases separately. Research documents are analyzed based on various parameters indicates that the research topic has a very good potential. The network study of various parameters shows that there is a lot of space for contribution in terms of domain adaptation, generalization, adversarial attacks, GAN, machine learning, and deep learning in future research.

Keywords: Face Presentation Attacks, Domain adaption, authentication systems, bibliometric analysis, face anti-spoofing.

I. INTRODUCTION

Biometrics has always performed better than traditional password-based authentication systems. Face, voice, fingerprint, palmprint, iris various biometrics standards are available. Facial-based biometric systems have been more popular due to their advantages over other biometric systems. According to a study by “Facial Recognition Business,” the global facial recognition market will generate USD 8.5 million by 2025, owing to a wide range of applications in various categories (Security-Law enforcement, health, banking, and retail, etc).

Face recognition systems are attracting more interest from academia and industry, according to a Thales-group survey. However, as a consequence of the increased attention, hackers are increasingly inspired to create biometric presentation attacks (PA), also known as spoofs, to be authenticated as the genuine consumer.

Due to the almost no-cost access to the human face, the spoof face can be as simple as a printed picture paper (i.e., print attack) and a digital image/video (i.e., replay attack) or as complex as a 3D Mask and facial cosmetic makeup. Those spoofs can be physically very similar to the real

user's live face if handled correctly. As a result, the development of robust face anti-spoofing algorithms is needed.

Categorization of face Presentation attacks is given as shown in figure 1. Majorly Face presentation attacks are broadly categorized as Impersonate attacks and obfuscation attacks.

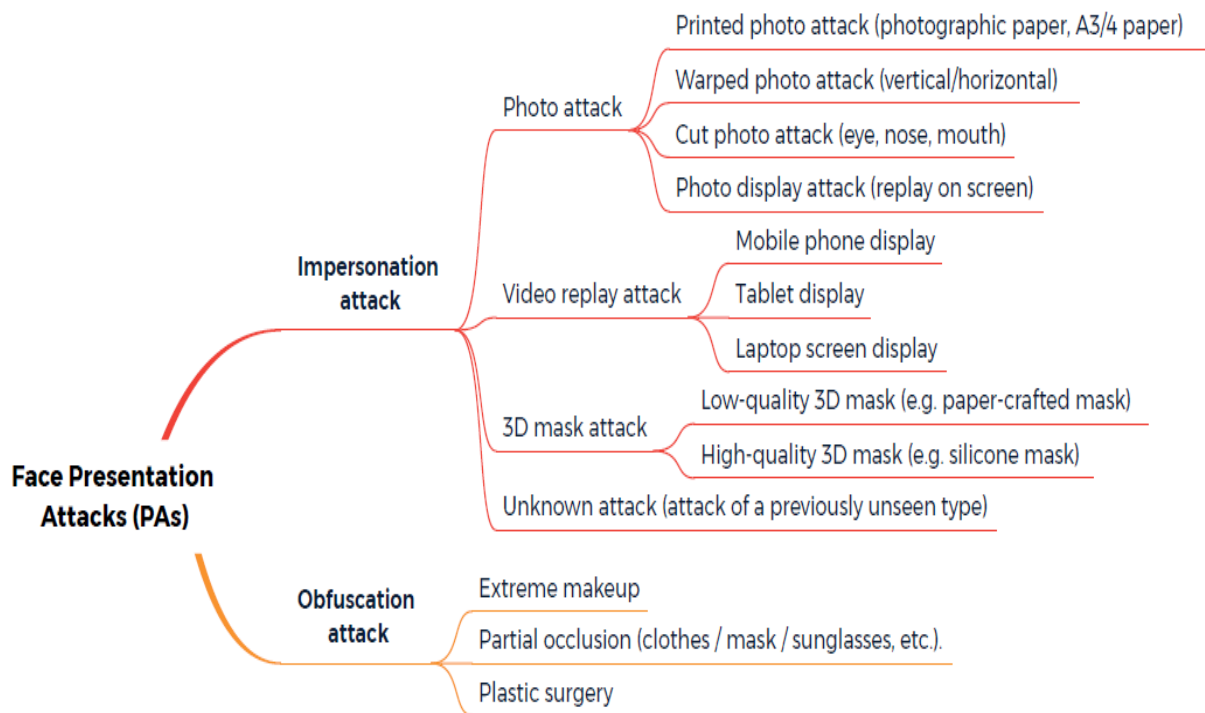


Fig. 1 Typology of Face Presentation Attacks (1)

Impersonation attacks are those in which the imposter makes use of a photo or video of the person whose authentication needs to be done. Where in obfuscation attacks the person doesn't want to get recognized by biometric systems. For example, a person with a criminal record at the airport doesn't want to get recognized in CCTV, so he may do extreme makeup or wear a different outfit or at an extreme case, he may do plastic surgery.

In literature Face presentation attack detection techniques are categorized on motion-based, Texture-based, geometric-based feature extraction methods. In some literature,

conventional feature extraction methods using FFT, LBP, LBP + Color spaces, HoG, LBP+ Gabor Wavelets are discussed.(1–3) proposed a technique that aims to solve the problem of face spoofing by extracting color texture features. The author tries to find out which color space amongst YCrCb, RGB, and HSV can well distinguish a face into true or fake classes by using color LBP features extracted from each channel.(4–6) To eliminate irrelevant components, the input image is transformed into guided scale space. Then Guided Scale Based Local Binary Pattern (GS-LBP) and Local Guided Binary Pattern (LGBP) descriptors are used to extract texture features which are then concatenated and classified using SVM.(7)(3) The method extracts the LBP features from YCrCb and Gray color space. Further, COALBPs (Co-occurrence of Adjacent Local Binary Patterns) are computed from Grayscale image. (8–10)These features are combined and passed to SVM for binary classification of input face images. From the literature, it is observed that all hand-crafted features show a limited generalization ability, as they are not powerful enough to capture all possible variations in acquisition conditions.

In some literature, deep learning-based feature extraction methods are discussed. (11–13) Convert face image into RGB, HSV & YCrCb color spaces. Feed RGB to 1st, HSV to 2nd & YCrCb to 3rd Deep FASD CNN stream. By using voting for all 3 streams, we give final results as REAL or FAKE(14–17) proposed CNN architecture called ResNet-18 is used in which outputs class probabilities based on Temporal, Color-based, and Patch-based features. These class probabilities are fed to SVM for detecting face spoofing. (17) first attempt to use NAS to solve the problem of Deep Face Recognition and customize the neural network structure for the recognition field through a reinforcement learning algorithm(18,19). Deep learning feature extraction methods have their limitations as they suffer from the problem of overfitting and suffer from poor generalization abilities.

A new approach of self-adaptation and generalization-based face anti-spoofing approach is an emerging research area. (20–22) has discussed an unsupervised domain adaptation with disentangled representation (DR-UDA) approach to improve the generalization capability of PAD into new scenarios. A self-domain adaptation system for the inference that takes advantage of unlabeled test domain data. A domain adaptor, in particular, is intended to adapt the model for the test domain.

II. DATA COLLECTION

Various prominent datasets are available for accessing research work done in the respective area for example Scopus, Web of Science, IEEE Explore, Science Direct, Google Scholar, Nature, PubMed, ResearchGate, Arxiv.org, etc. Out of which Scopus and Web of Science are well-known datasets. (23) has done bibliometric analysis using only Scopus dataset using search queries as face anti-spoofing or face presentation attacks or face liveness detection considering the year 2012 to 2021. The author got 177 search results using these keywords.

In literature, as discussed in section I, it is observed that more work is to be done on domain adaptation-based face anti-spoofing, it is an emerging research trend in this area. Hence in this paper, the Search query used is as face presentation attacks or domain adaptation based on Face Anti Spoofing for Web of Science & Scopus both datasets.

Search Query:

TITLE-ABS-KEY (face AND presentation AND attacks) OR domain AND adaptation AND based AND face AND anti AND spoofing
--

No of the research papers retrieved from Scopus & Web of Science are 151 & 117 respectively.

2. Search Results

A. Publication Trends

The articles with keywords face presentation attacks and Domain-based adaptation have been started from the year 2011. It has shown continuous improvement in the number of publications count in the same area. In the year 2020 majority of research is published. It indicates that this keyword has significant strength in research.

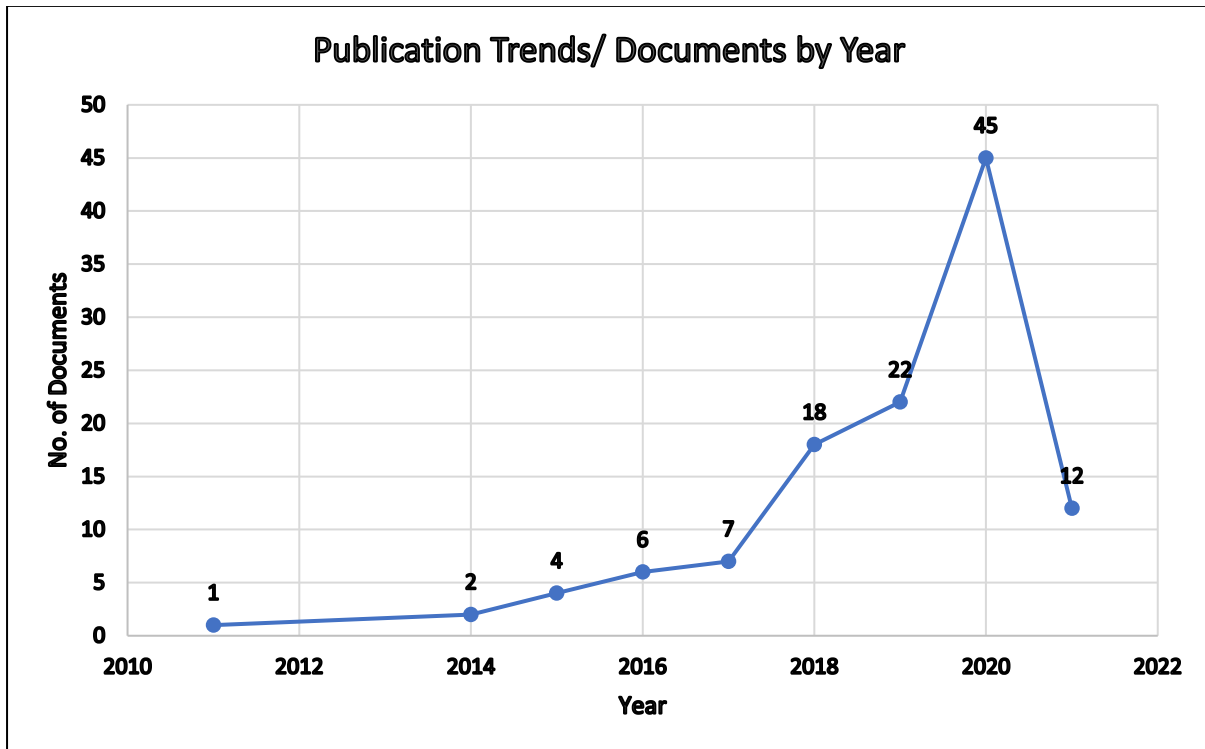


Fig. 1 Year-wise Publication trends (Web of Science accessed on 24-03-2021)

Table 1. Year-wise Publication Trends for Web of Science dataset accessed on 24-03-2021

Year	No. of Documents
2021	12
2020	45
2019	22
2018	18
2017	7
2016	6
2015	4
2014	2
2011	1

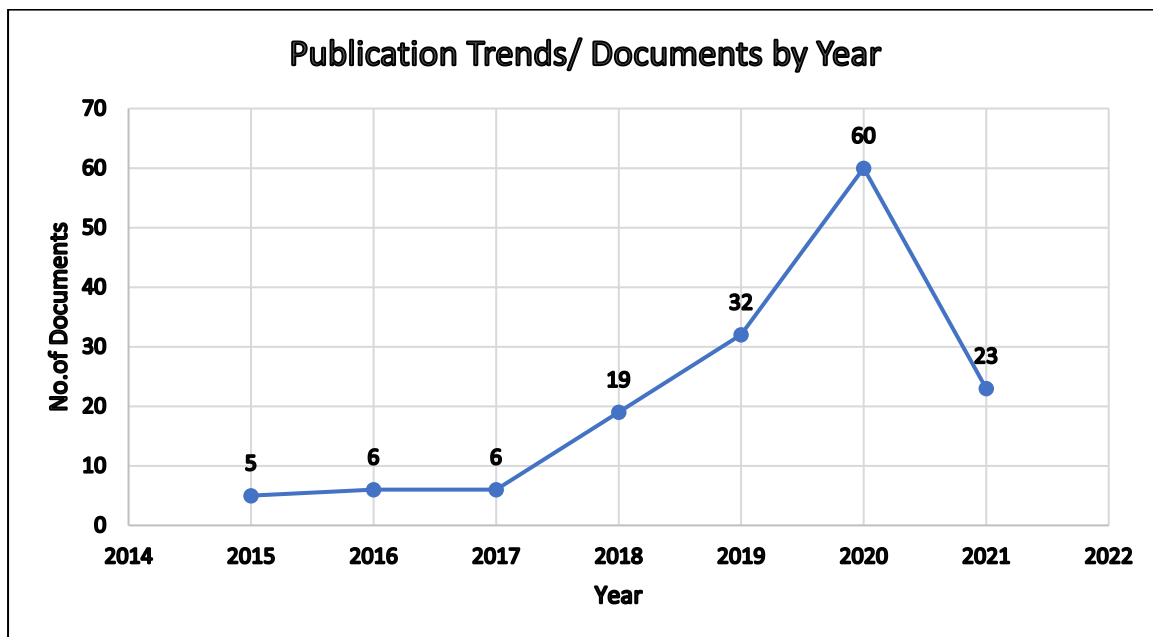


Fig. 2: Year-wise publication trends (Scopus accessed on 23-03-2021)

Table 2. Year-wise Publication Trends for Scopus dataset accessed on 23-03-2021

YEAR	No. of Documents
2021	23
2020	60
2019	32
2018	19
2017	6
2016	6
2015	5

B. Document Type Analysis

In the Year 2020 maximum number of documents are published in the area. Article type of documents has a maximum contribution of 90% in the published documents of web science database accessed in 24-03-2021. The distribution in documents by type has shown in Fig.3 in form of a pie chart. The Article type of documents has contributed 53.6 % followed by

Conference papers 36.4%, where review papers, Book chapters, books, conference review papers have contributed 5.3%, 2.6%,1.3%,0.7% respectively. It is represented by a pie chart as given in Fig. 4.

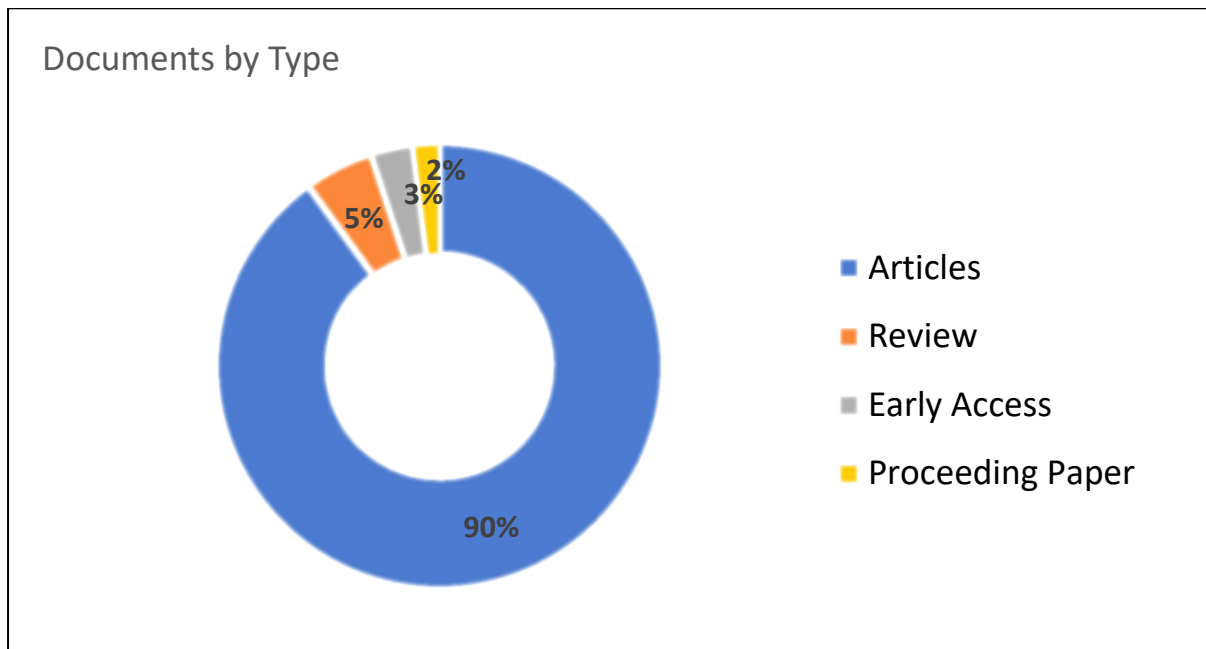


Fig. 3: Pie chart for Documents by type analysis (Web of Science accessed on 24-03-2021)

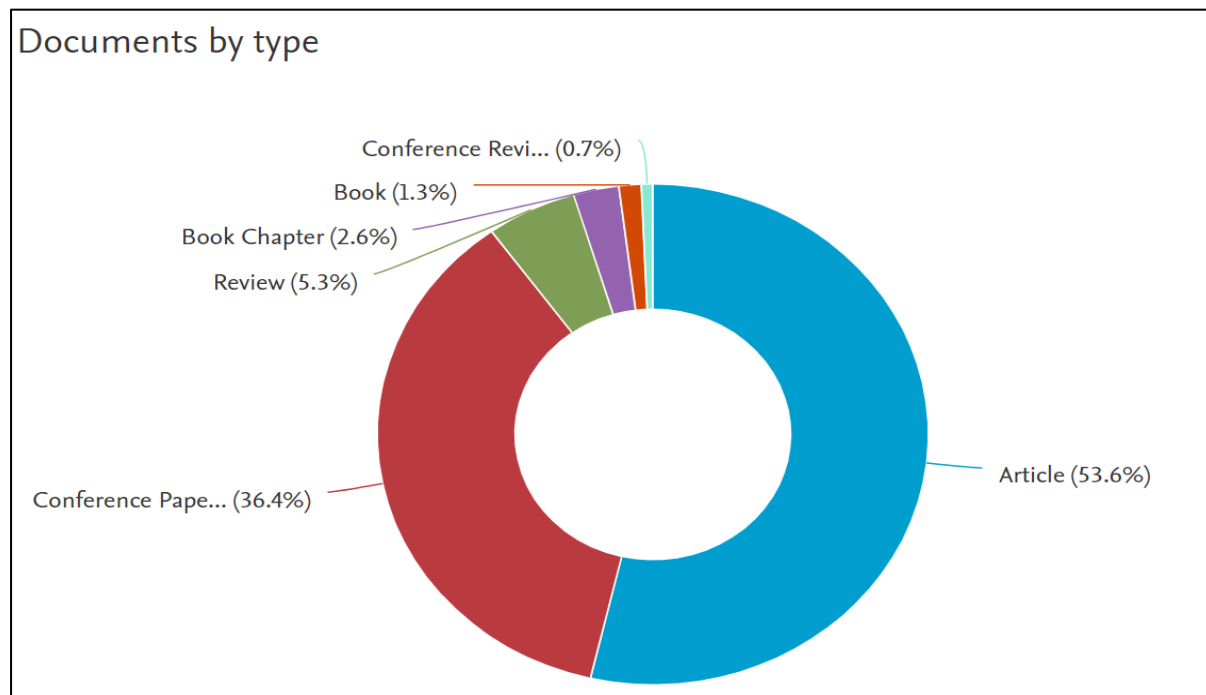


Fig. 4: Pie chart for Document type analysis (Scopus accessed on 23-03-2021)

III. BIBLIOMETRIC ANALYSIS

A. Documents by Subject Areas

It is observed that Documents published in Web of Science using keywords domain adaptation-based face anti-spoofing, face presentation attacks have contributed in various subject areas, the research is not only carried out in Computer Science & Engineering subject area but also Telecommunication, Optics, Image science photographic Technology, Instruments Instrumentation, Operation Research, as well as Mathematics and Science Technology. Figure 5 shows a pie chart for Document analysis by subject areas for Web of Science Documents.

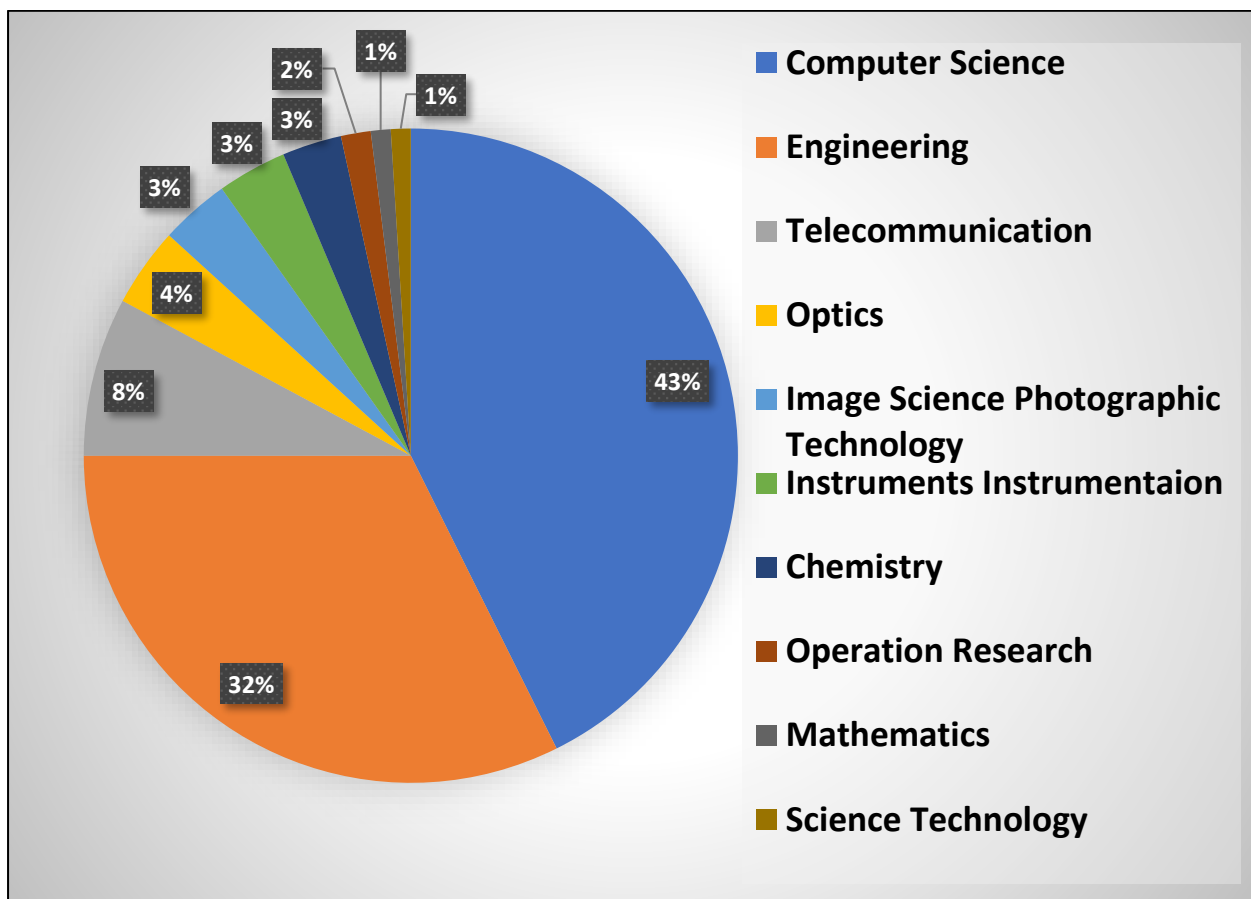


Fig. 5 Documents analysis based on Subject area (Web of Science access on 24-03-2021)

In the case of documents published in Scopus, Computer Science and Engineering Subject areas have contributed around 74.6% along with other subject areas as shown in figure 6 a pie chart for documents analysis by subject areas.

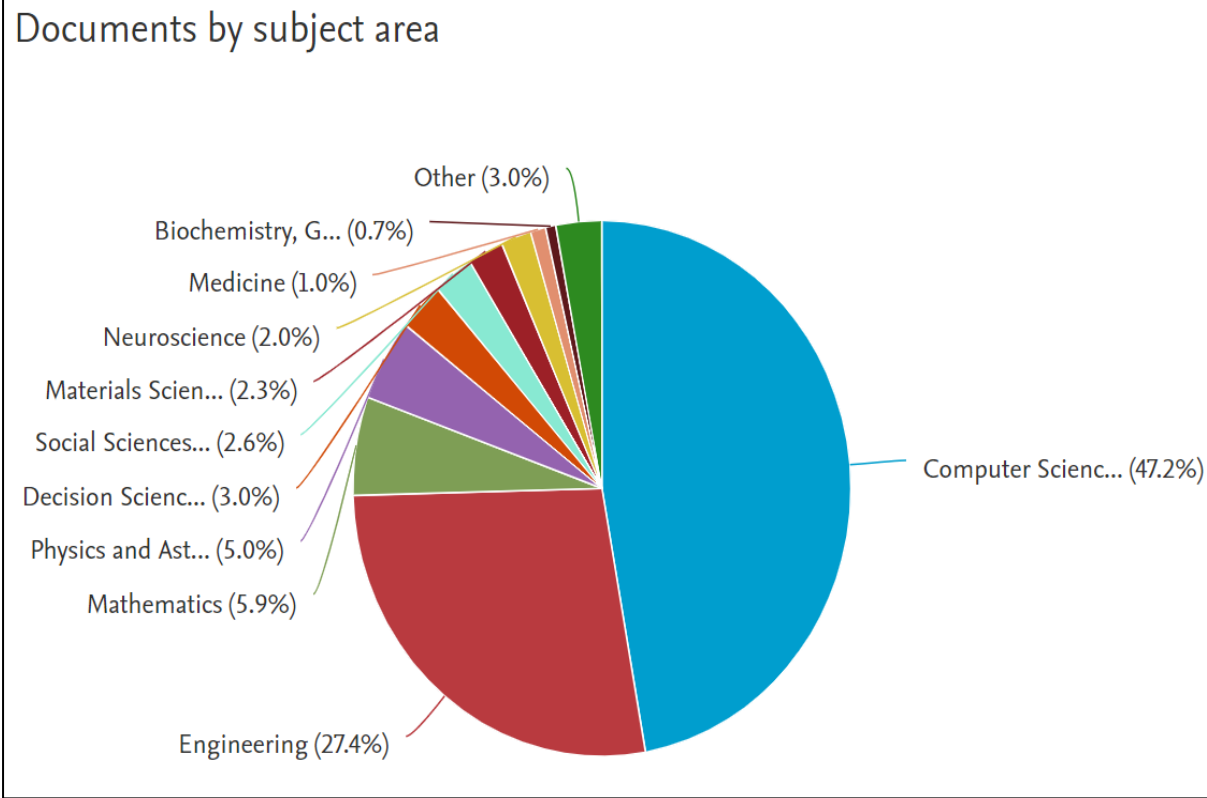


Fig. 6: Documents analysis by Subject Area (Scopus Access on 23-03-2021)

B. Geographical Analysis

The research using keywords Domain adaptation-based face anti-spoofing or face presentation attacks are keywords is done by various countries overall the globe. The top 10 countries that are contributing in the same research area are used for analysis.

Figure 7 and Figure 8 give the analysis of the number of documents published by Web of Science and Scopus Dataset. It is Observed that China is on the top number followed by India.

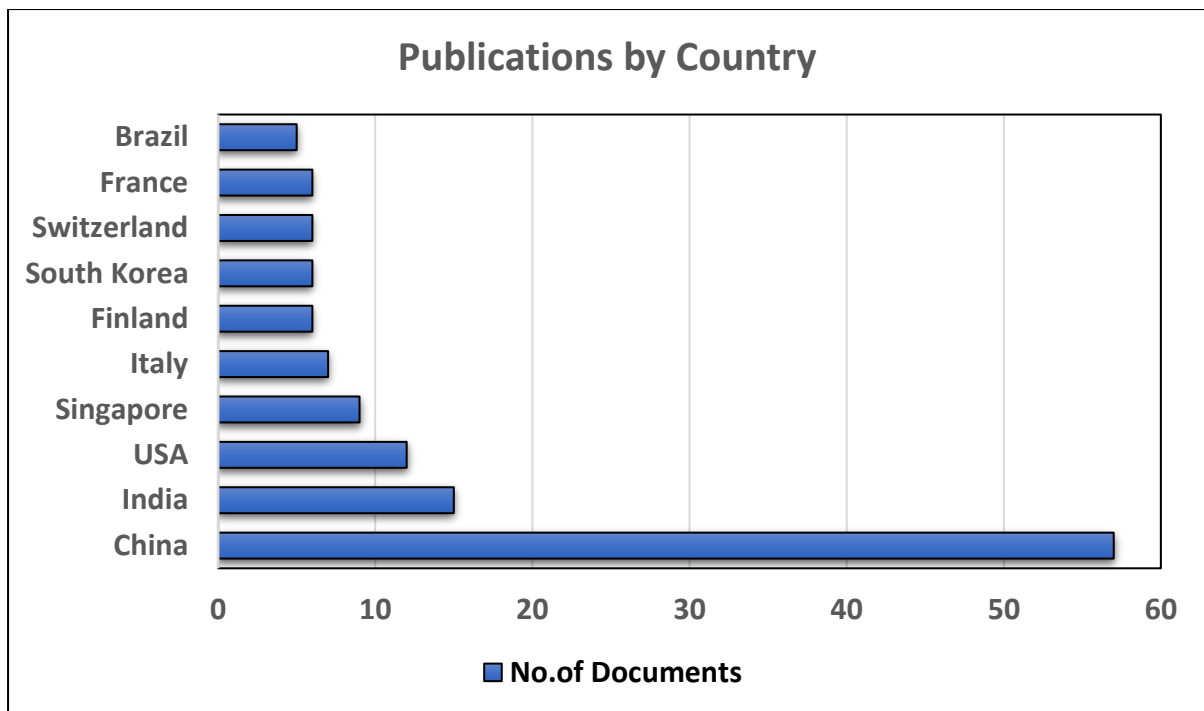


Fig. 7 Analysis of Publications by Country (Web of Science accessed on 24-03-2021)

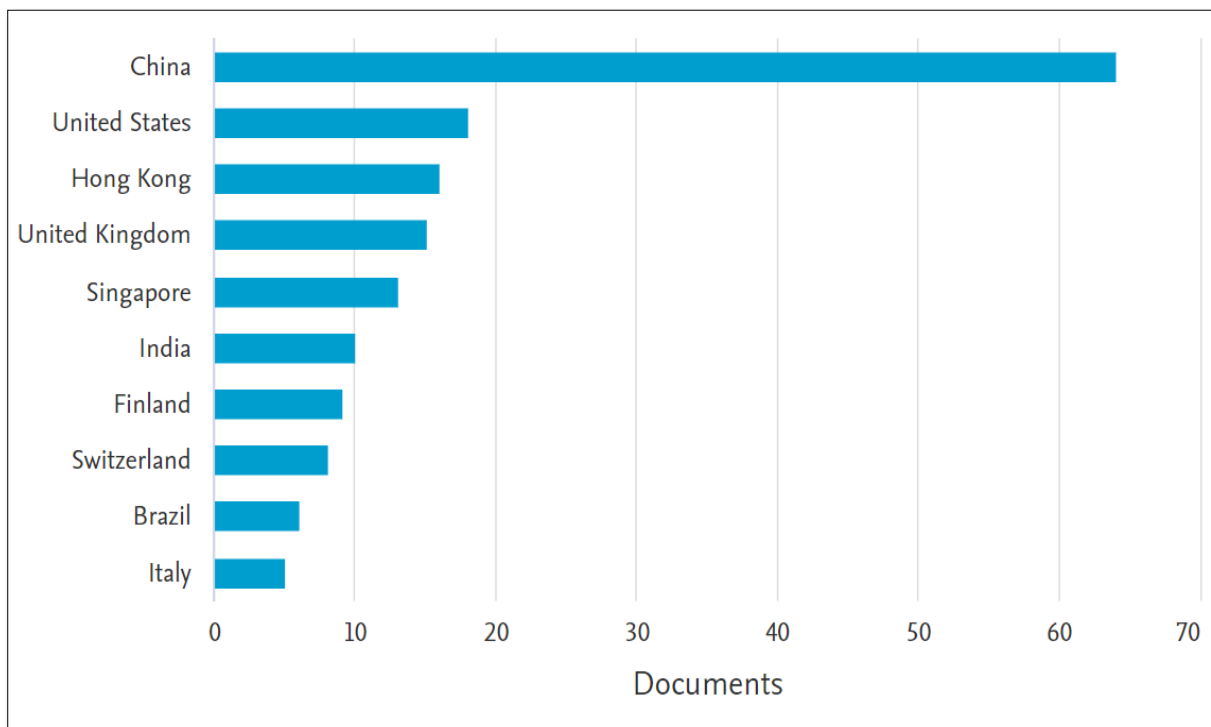


Fig. 8 Analysis of Publications by Country (Scopus accessed on 23-03-2021)

The next section shows the network map of the authors' relationship countrywide. As per citation, China is the country that has got more citations.

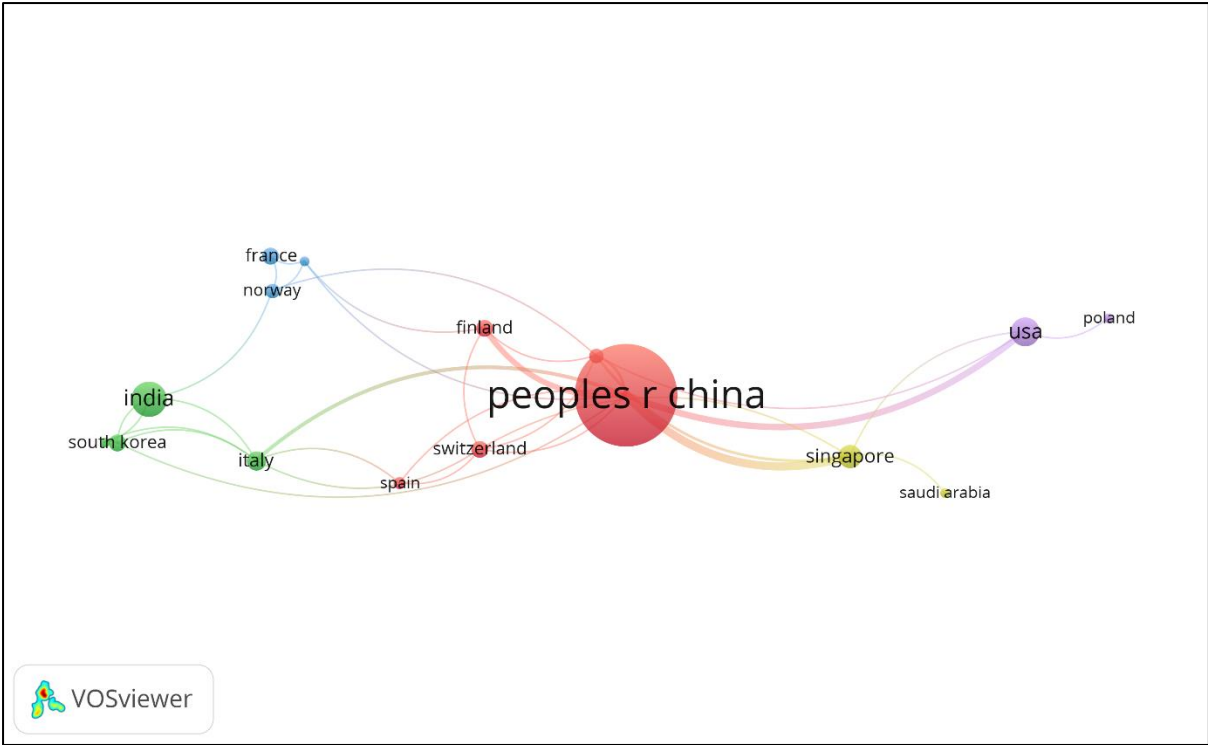


Fig. 9 Network Map for Authorship countrywide (Web of Science 24-03-2021)

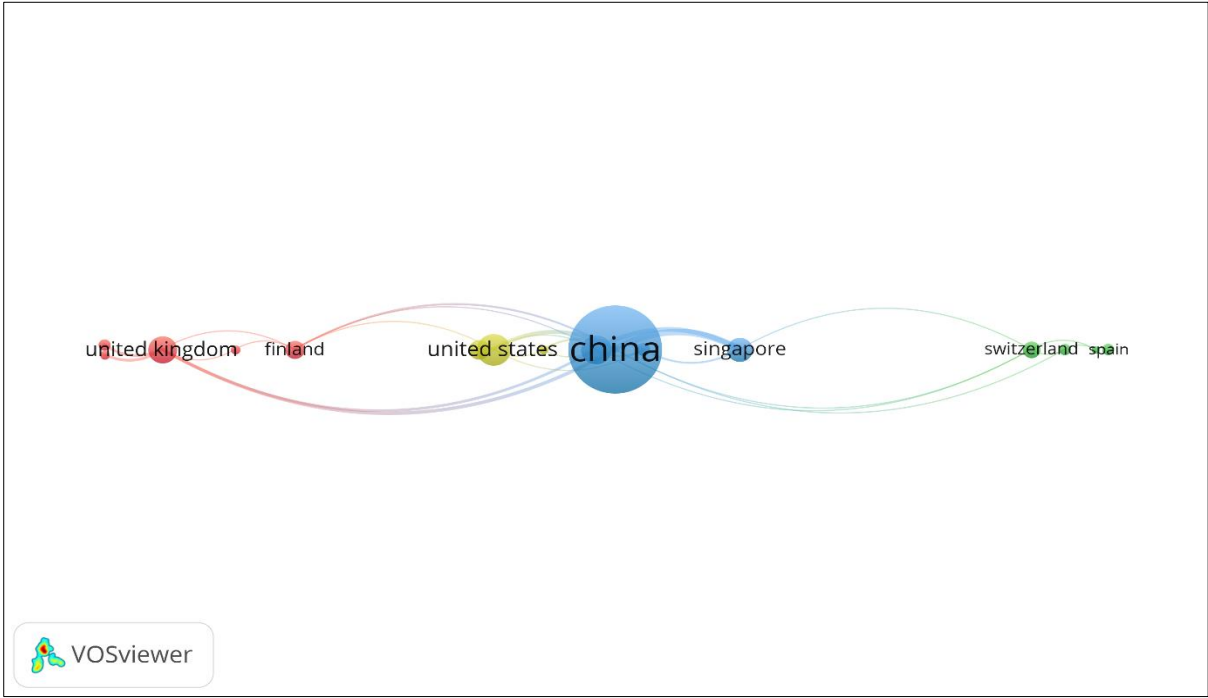


Fig.10 Network Map for Authorship countrywide for Scopus (accessed on 23-03-2021)

C. Document Analysis by Affiliations

Document analysis by affiliations shows organizations researching face presentation attacks or domain adaptation-based face anti-spoofing. The graph for document analysis by affiliations is

shown in figure 11 & fig 12 using the Web of Science and Scopus dataset. The top 10 universities contributing to the research, are considered for analysis. It is observed that most Chinese Universities and organizations are more active in this particular research domain.



Fig. 11 Document analysis by Affiliations (Web of Science accessed on 24-03-2021)

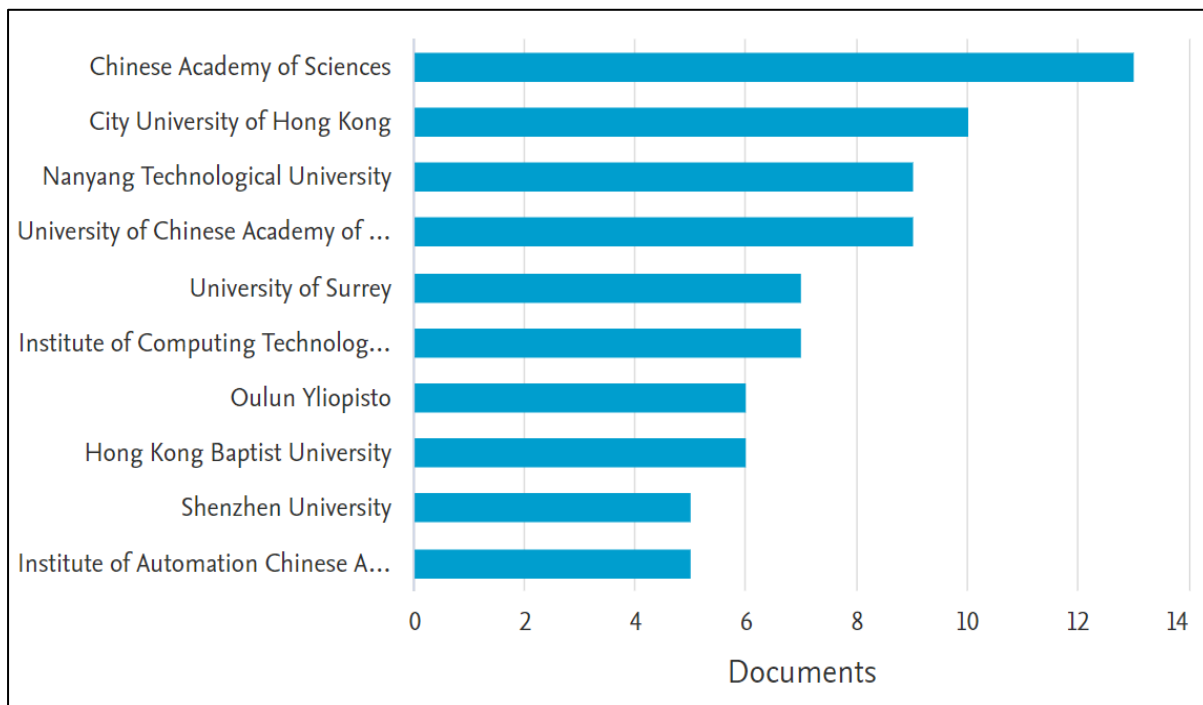


Fig. 12 Document analysis by Affiliations (Scopus accessed on 23-03-2021)

D. Keyword Analysis

In this section cluster of keywords is formed by occurrences in documents. The frequency of keywords such as feature extraction, deep learning, face anti-spoofing, Presentation attacks, adversarial examples, face liveness detection has been observed more in research documents from the Web of Science dataset. A graph of analysis of keywords of authors is shown in Fig. 13 using density-based visualization using Vos's viewer.

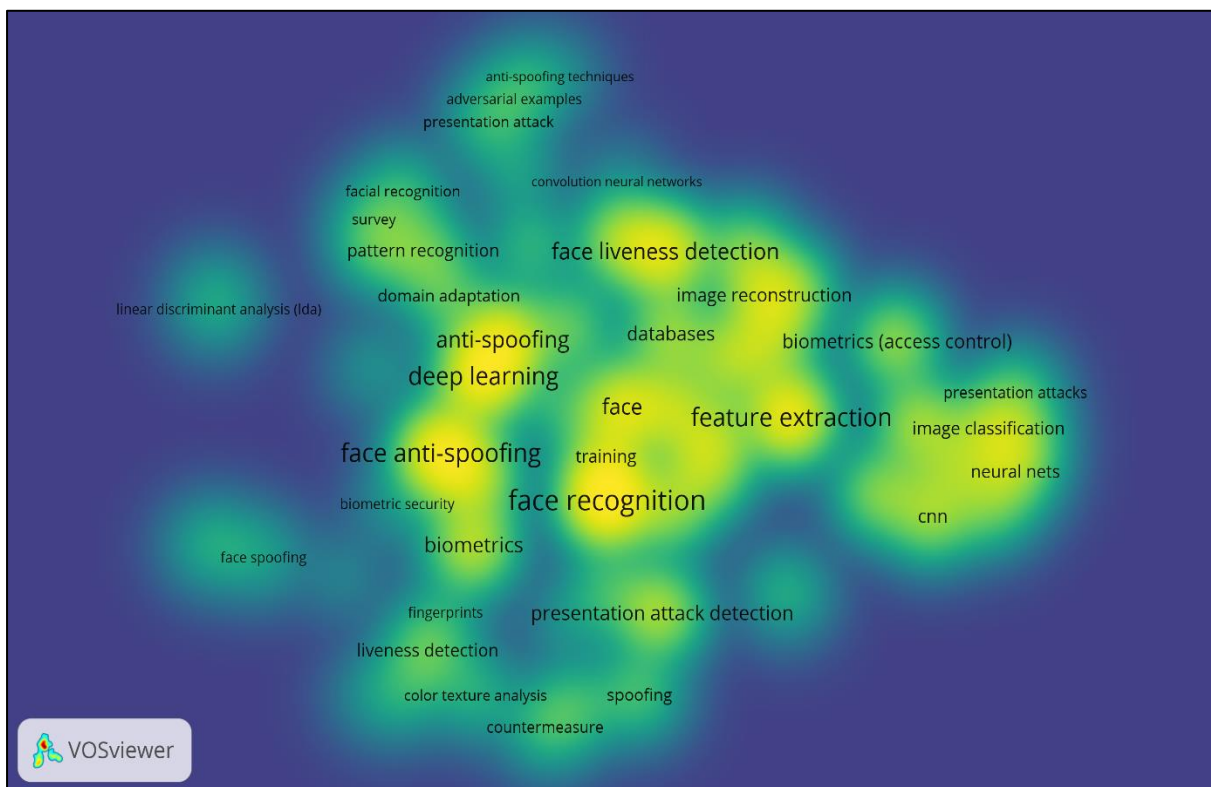


Fig.13 Keyword's analysis with authors keywords (Web of Science accessed on 24-03-2021)

Face Anti-spoofing, presentation attack detection, domain adaptation, face spoof detection, anomaly detection are the keywords used by most research documents in the Scopus dataset. Co- occurrences of author keywords using overlay visualization in Vos-viewer are as shown in figure 14.

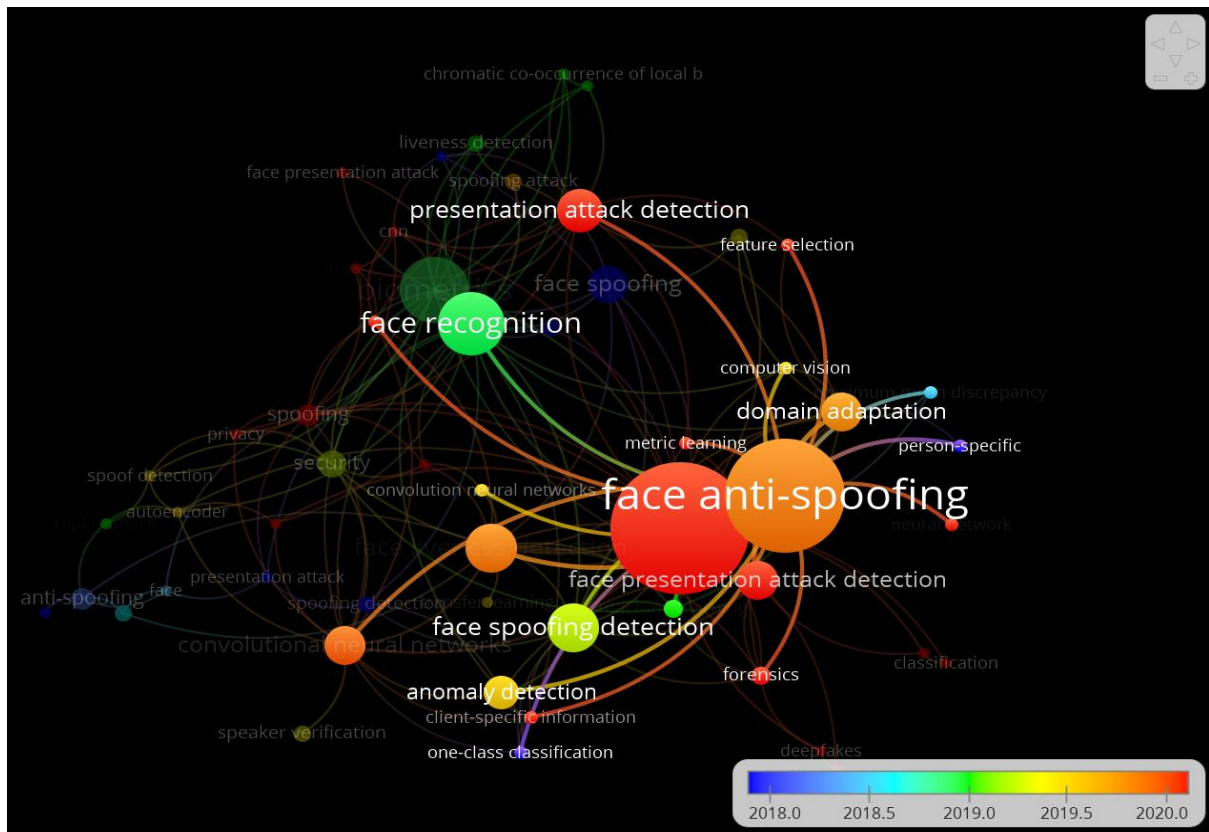


Fig. 14 Co-occurrence of authors keywords overlay visualization (Scopus Accessed on 23-03-2021)

E. Source Type Analysis

This section indicates that a maximum number of research articles i.e., 17 are published in IEEE Transactions on Information Forensics and Security followed by IEEE Access. Figure 15. Gives analysis of source types for Web of Science dataset. Where in Figure 16 gives the source type analysis for the Scopus database using overlay visualization using Vos’s viewer.

F. Analysis by Funding Agencies

It is observed that NSFC i.e., National Natural Science Foundation of China has maximum funds provided for research in this area. Another funding agency again from China, the National Key Research and Development Program of China.

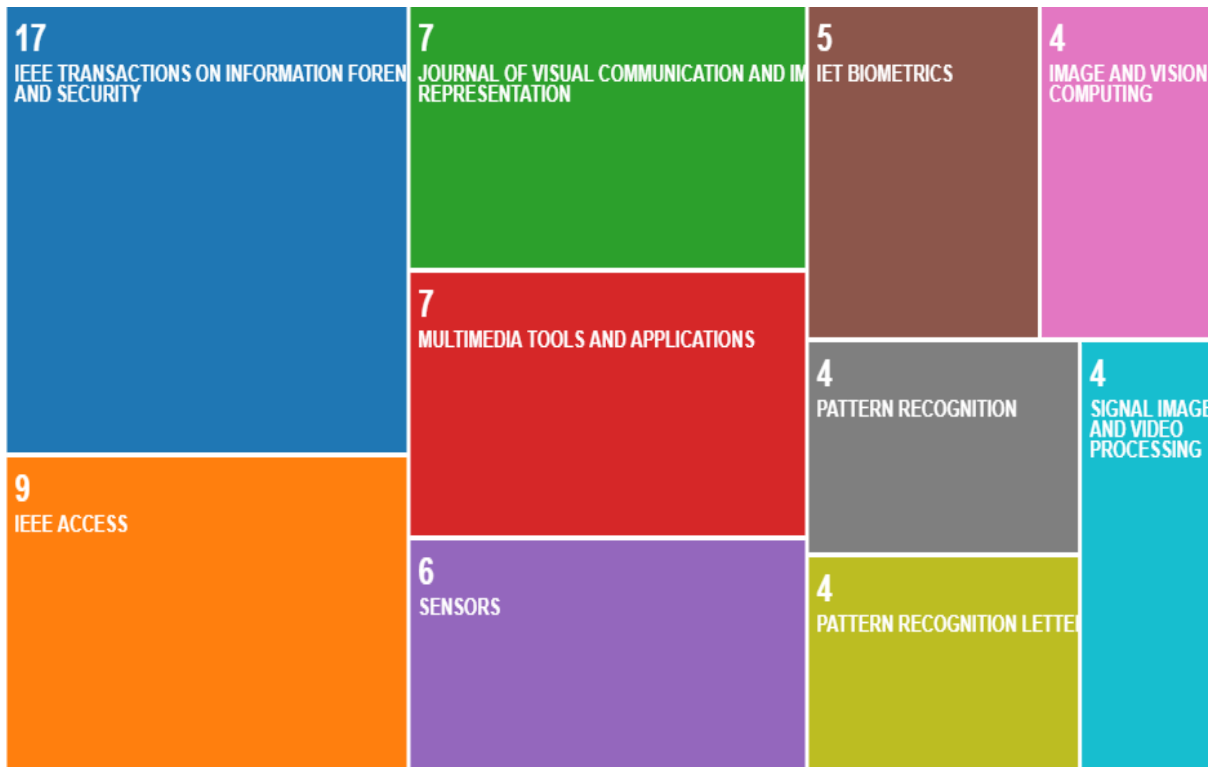


Fig. 15. Source type analysis (web of Science accessed on 24-03-2021)

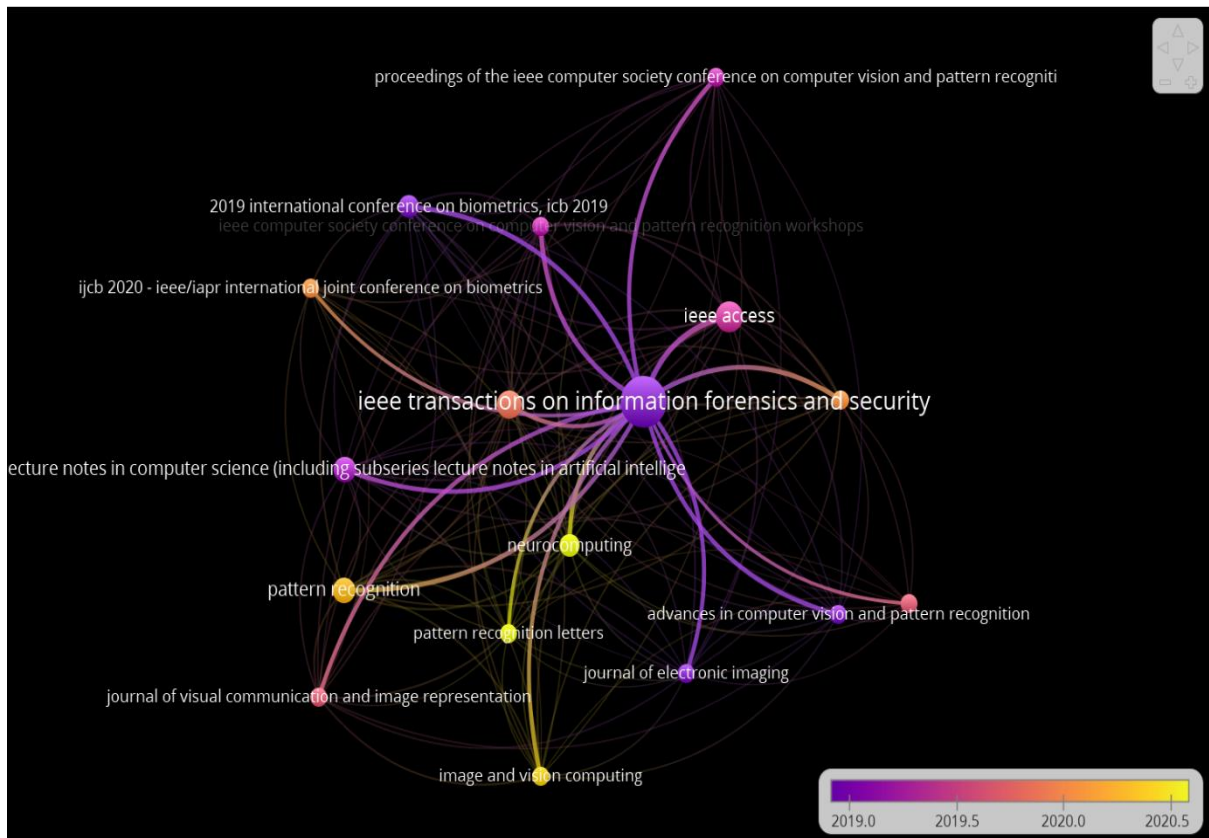


Fig. 16. Source type analysis in overlay visualization using Vos viewer (Scopus accessed on 23-03-2021)

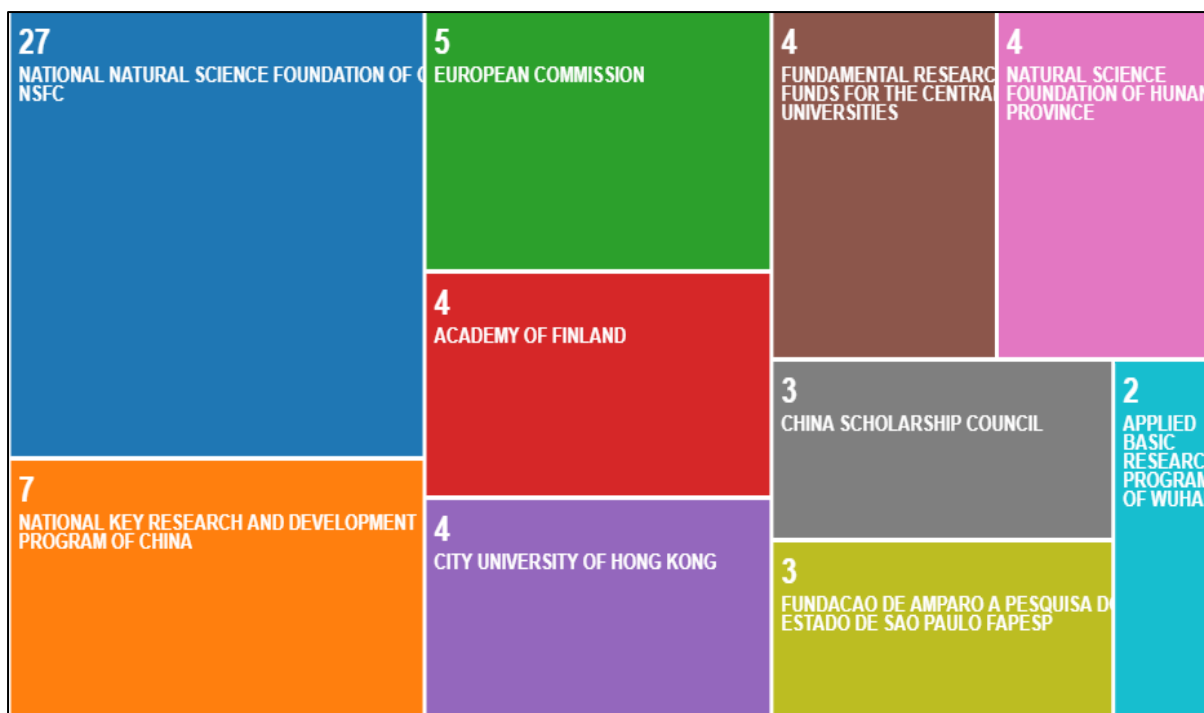


Fig. 17 Analysis by Funding Agencies (Web of Science accessed on 24-03-2021)

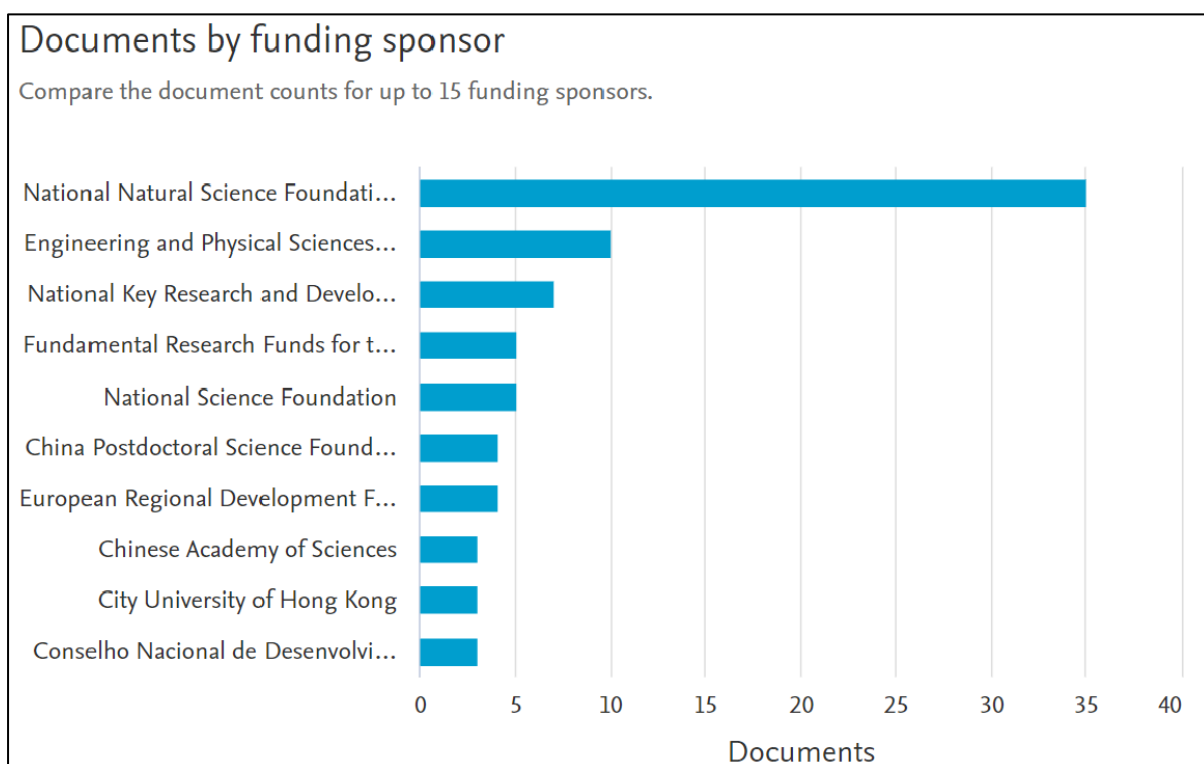


Fig. 18 Analysis by Funding Agencies (Scopus accessed on 23-03-2021)

G. Citation Analysis

For Web of Science out of 117 documents, 79 documents are cited at least once. Fig. 19 gives citation analysis using Vos viewer.

IV. CONCLUSION

Bibliometric analysis of face presentation attacks based on domain adaptation is carried out by using the most popular databases Scopus and Web of Science. The database is considered from the year 2011 to 2021-time span. For Search operations AND, OR are used along with keywords face presentation attacks, domain adaptation for face anti-spoofing. Total 151, and 117 documents are retrieved as a result of keyword search.

Different parameters are considered for analysis purposes. From Keyword analysis, it is been observed that the maximum used keywords by documents are facing anti-spoofing, face spoof detection, domain adaptation. The document-by-year analysis has been shown that the maximum o. of documents is published in the year 2020 followed by 2019. Maximum research documents published are of article type. The maximum research has been contributed by China and India. Most of the research is funded by research organizations or universities in China. The Subject area analysis has indicated that Computer Science and Engineering has the contribution of 75%. Where 17 documents have been published by Source Journal IEEE Transactions on Information Forensics and Security, 9 documents are published by IEEE Access.

The Network Analysis is done using Vos Viewer 1.6.16 version software. Some other parameters are used for analysis such as co-authorship, co-occurrences of keywords by documents. Network analysis with different parameters indicates that major contribution towards this topic has done in the year 2019 and 2020. It could be commented that Domain adaptation-based face anti-spoofing, Face presentation attacks has a great scope and potential for research in the future.

REFERENCES

1. Ming Z, Visani M, Luqman MM, Burie JC. A survey on anti-spoofing methods for face recognition with RGB cameras of generic consumer devices. arXiv. 2020;
2. Boulkenafet Z, Komulainen J, Hadid A. FACE ANTI-SPOOFING BASED ON COLOR TEXTURE ANALYSIS. 2015 IEEE Int Conf Image Process. 2015;2636–40.
3. Song L, Ma H. Face liveliness detection based on texture and color features. 2019 IEEE 4th Int Conf Cloud Comput Big Data Anal ICCCBDA 2019. 2019;418–22.
4. Peng F, Qin L, Long M. Face presentation attack detection using guided scale texture. *Multimed Tools Appl.* 2018;77(7):8883–909.
5. Peng F, Qin L, Long M. Face presentation attack detection based on chromatic co-occurrence of local binary pattern and ensemble learning. *J Vis Commun Image Represent [Internet].* 2020;66:102746. Available from: <https://doi.org/10.1016/j.jvcir.2019.102746>
6. Khurshid A, Tamayo SC, Fernandes E, Gadelha MR, Teofilo M. A Robust and Real-Time Face Anti-spoofing Method Based on Texture Feature Analysis. *Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics).* 2019;11786 LNCS(September):484–96.
7. He J, Luo J. Face Spoofing Detection Based on Combining Different Color Space Models. 2019 IEEE 4th Int Conf Image, Vis Comput ICIVC 2019. 2019;523–8.
8. Jagdale PA, Thepade SD. Face Liveness Detection using Feature Fusion Using Block Truncation Code Technique. *Int J Recent Innov Trends Comput Commun.* 2019;7(8):19–22.

9. Thepade SD, Dindorkar MR, Chaudhari PR, Bangar RB, Bang S V. The Comprehensive Review of Face Anti-Spoofing Techniques. *Int J Adv Sci Technol* [Internet]. 2020;29(5):8196–205. Available from: <http://sersc.org/journals/index.php/IJAST/article/view/18468>
10. Thepade SD, Bang S V, Chaudhari PR, Dindorkar MR. Improved Face Spoof Detection using GLCM with Stride and Color Space Variations using Machine Learning Algorithm. 2020;29(3):10247–61.
11. Larbi K, Ouarda W, Drira H, Ben Amor B, Ben Amar C. DeepColorFASD: Face Anti Spoofing Solution Using a Multi Channeled Color Spaces CNN. *Proc - 2018 IEEE Int Conf Syst Man, Cybern SMC 2018*. 2019;4011–6.
12. Jenkins J, Roy K, Shelton J. Using deep learning techniques and genetic-based feature extraction for presentation attack mitigation. *Array*. 2020;7(April):100029.
13. Koshy R, Mahmood A. Enhanced deep learning architectures for face liveness detection for static and video sequences. *Entropy*. 2020;22(10):1–27.
14. Almeida WR, Andaló FA, Padilha R, Bertocco G, Dias W, da Torres RS, et al. Detecting face presentation attacks in mobile devices with a patch-based CNN and a sensor-aware loss function. *PLoS One*. 2020;15(9 september):1–24.
15. Chen FM, Wen C, Xie K, Wen FQ, Sheng GQ, Tang XG. Face liveness detection: Fusing colour texture feature and deep feature. *IET Biometrics*. 2019;8(6):369–77.
16. Tang Y, Wang X, Jia X, Shen L. Fusing multiple deep features for face anti-spoofing [Internet]. Vol. 10996 LNCS, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer International Publishing; 2018. 321–330 p. Available from:

http://dx.doi.org/10.1007/978-3-319-97909-0_35

17. Zhu N. Neural Architecture Search for Deep Face Recognition. arXiv. 2019;
18. Swapnil Shinde, Dr. Sudeep Thepade SP, Shao R, Lan X, Li J, Yuen PC, Volpi R, et al. Generalizing to unseen domains via adversarial data augmentation. arXiv [Internet]. 2020;11217 LNCS(NeurIPS):297–315. Available from: http://dx.doi.org/10.1007/978-3-319-97909-0_35
19. Cai R, Li H, Wang S, Chen C, Kot AC. DRL-FAS: A novel framework based on deep reinforcement learning for face anti-spoofing. arXiv. 2020;16:937–51.
20. Ada S, Wang J, Zhang J, Bian Y, Cai Y, Wang C, et al. Self-Domain Adaptation for Face Anti-Spoofing. 2021;(January).
21. Wang G, Han H, Shan S, Chen X. Unsupervised Adversarial Domain Adaptation for Cross-Domain Face Presentation Attack Detection. IEEE Trans Inf Forensics Secur. 2021;16(XX):56–69.
22. Qin Y, Zhang W, Shi J, Wang Z, Yan L. One-class adaptation face anti-spoofing with loss function search. Neurocomputing [Internet]. 2020;417:384–95. Available from: <https://doi.org/10.1016/j.neucom.2020.08.068>
23. Swapnil Shinde, Dr. Sudeep Thepade SP. Bibliometric analysis of Face Anti Spoofing. Libr Philos Pract. 2020;2020.