10-12-2020

A Bibliometric Analysis of Face Anti Spoofing

Swapnil Ramesh Shinde
Symbiosis International University, Ramrao Adik Institute of Technology, swapnil.shinde.phd2019@sitpune.edu.in

Shraddha Phansalkar
Symbiosis International University, shraddhap@sitpune.edu.in

Sudeep D. Thepade
Pimpri Chinchwad College of Engineering,Pune, sudeepthepade@gmail.com

A Bibliometric Analysis of Face Anti Spoofing

Abstract

Face Recognition Systems are used widely in all areas as a medium of authentication, the ease of implementation and accuracy provides it with a broader scope. The face recognition systems are vulnerable to some extent and are attacked by performing different types of attacks using a variety of techniques. The term used to describe the measures taken to prevent these types of attacks is known as face anti spoofing. Research has been carried on since decades to design systems that are robust against these attacks. The focus of the work in this paper is to explore the area of face anti spoofing, research done in terms of quantitative analysis and its impact. The keyword analysis table indicates face recognition as a widely used keyword followed by biometrics and face anti spoofing as per the Scopus dataset search. The citation analysis indicates that texture based systems have contributed majorly for Face anti spoofing detection. The Bibliometric analysis done in this paper tends to provide some future research directions in the area of Face anti spoofing analyse the trends of research done.

Keywords: Biometrics, Bibliometric Analysis, Deep learning, Face anti-spoofing, Texture analysis

1. Introduction

Security aspects have evolved with time and many mechanisms have been developed, but yet the security factor remains an area of research. The primary goals of Security are confidentiality, Integrity and Availability, these are combined with Authentication and Access Control for advanced security. Any breach to the security goals leads to security threats and vulnerabilities which transform into attacks. The Different security threats are listed below:

1. Social Engineering
2. Phishing attacks
3. Ransom ware attack

4. SQL injection attack
5. Session Hijacking , Cracking

In the above attacks authentication is a primary concern either from the user end or the server end. If the user applies the standard authentication methods then the threats can be mitigated to greater extent. Authentication methods classification is shown below in Figure 1.

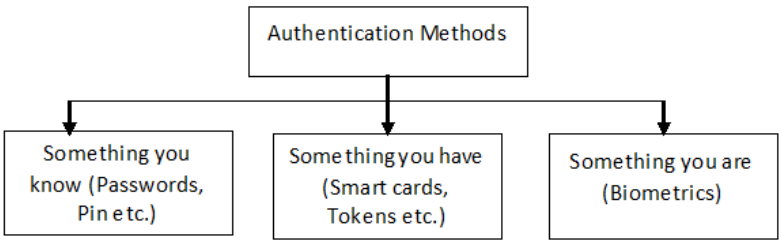

Figure 1. Authentication Methods Classification (Shinde and Thepade 2018)

The best and efficient means of imposing security is through authentication (Shinde and Thepade 2015), where authentication can be classified into many categories. The categorization of authentication is in terms of methods or ideas that are implemented to achieve authentication. Some of the key methods used are using physical instruments such as cards/chips, through known or set keys and through biometrics. Biometrics (Shinde and Thepade 2018) refers to two main categorizations viz. physical and behavioural. In Physical terms, human factors are used for authentication, face is a key factor that is widely used and readily applicable to devices. Face recognition systems (Kinnikar, Husain and Meena 2016) are used in different applications for achieving authentication, these systems can be broken by performing attacks. The attacks on face recognition systems are categorized into four main streams which are Photo Print attack, Replay attack, Masking and 3D mask attack (Edmunds & Caplier 2017).

Four main groups of the papers published in this research area consist of texture analysis, Image quality analysis, motion analysis and deep learning applied methods. The methods above are applicable to both 2D and 3D attacks, 2D systems are history and in today's world all the applications have built in 3D systems for face recognition. In terms of motion analysis the video replay attack datasets are analysed to design the anti-spoofing systems. Li et al. (2019) have proposed a system based on motion blur analysis, they have considered blur intensity variation and blur width in combination with CNN. The texture based methods that are widely used include LBP, LTP, ELTP and ELCTP. ELTCP is a novel texture descriptor proposed by Raghvendra and Kunte (2020) that performs well compared to other descriptor. In terms of image quality analysis different IQA methods have been developed, effective pixel similarity deviation (EPSD) model is one such methods that has been proposed by Yeh and Chang (2018) that performs extraction of 21 image features. Deep learning methods are evolving and hybrid learning models are being developed. Multi-channel CNN (George et al. 2019) based method proposed takes data from different channels and is specifically designed to detect 3D mask attacks. Some of the researchers have explored the use of hardware components for face anti spoofing, in one such paper (Chan et al. 2017) have collected images with flash and without flash using an external camera. They have explored texture based methods for evaluation of this dataset. Face anti spoofing research is also done by analysing the skin blood flow (Wang et al. 2017) using the texture features and colour distribution in local regions. Face anti spoofing research has also been done in terms of smartphones, where a new mobile based face spoofing dataset (Vaidehi and Vasuhi 2018) is generated and evaluated. Wasnik et al. (2016) have proposed a system for face anti spoofing making use of raw sensor data collected from the smartphones.

Along with above papers there is lot of research done in terms of devices used for face recognition and also in terms of depth information (Hamdan and Mokhtar 2018) termed as 3D information of the images for face anti spoofing.

Proposed techniques for Face Anti Spoofing are classified as shown below in figure 2.

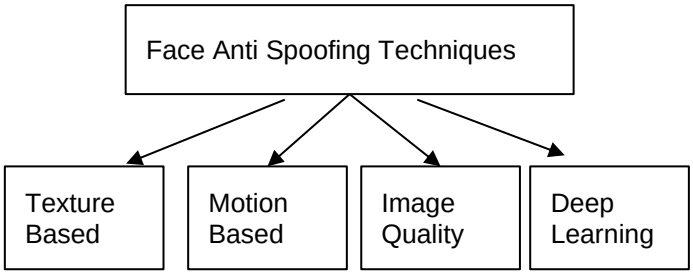

Figure 2. Face Anti Spoofing Techniques Classification

In this paper a Bibliometric analysis of the research done in the area of face anti spoofing is presented. The research discusses techniques designed for all the types of attacks mentioned above. The analysis is generated using the Scopus dataset that's one of the largest dataset available for researchers. The next sections of the paper are Data collection, Bibliometric analysis of Face anti spoofing in terms of quantitative aspects, deductions from analysis followed by scope of study and conclusion.

2. Data Collection

The publications in any research area are done under open access or paid access. These publications are available at different locations for access such as through IEEE Xplore, Scopus, Science Direct, Google Scholar, Research gate. The access to the publications is provided through some login mechanism either individual or institutional logins. The most popular database that has a large number of abstract and citations for peer-reviewed research is the Scopus dataset. This dataset has a collection of publications in all the domains such as engineering, computer science, mathematics, physics, social sciences, Medicine etc. In this paper we have explored the Scopus database from different aspects and listed its analysis.

Table 1. Search Result Count for Face Anti Spoofing Keyword

Sr No.	Name of Database	Search Results Count
1	Scopus Database	177
2	IEEE Xplore	113
3	Science Direct	35

The search was performed with face anti spoofing as the Core keyword and face liveness detection, face presentation attack as secondary key words. As shown in table 1 Scopus provides maximum results for the keyword that we focus on in this paper.

2.1 Search Results

The core keyword search presented a total 184 search results, wherein 178 articles published in English language, 5 Chinese and 1 Russian shown in table 2. The Scopus retrieves 184 results for the word face anti spoofing, earlier this was termed as face liveness detection. Number of papers with term face liveness detection is also quite

good with 110 documents with 39 patents.

Table 2. Publication Language

Sr. No.	Publication Language	Publication Count
1	English	178
2	Chinese	5
3	Russian	1
Total		184

The above count is for the documents available in the Scopus dataset, there are also a quite good number of secondary documents available along with patents for the core keyword search. Face Recognition keyword has also good count in keyword search, followed by anti spoofing keyword. In terms of patents, 38 patents are listed where majority patents are registered as US patents.

2.2 Document Type Analysis

The count of the documents is increasing considerably in this area from 2012, year 2019 reported the highest no of documents published which is 64 as per the analysis. In terms of types of documents that are published the conference paper and proceedings have a major share of 64% followed by publications of articles in journals and conference reviews. Some publications in terms of book chapter and review papers are also available. The pie chart for the type of documents is shown in figure 3 and its details reflected in table 3.

Table 3. Document Type Analysis

Sr. No.	Publication Type	Publication Count	Percentage
1	Conference Paper	115	64.60
2	Article	41	23.03
3	Review Paper	16	8.98
4	Book Chapter	5	2.79
5	Review	1	0.6
Total		178	100%

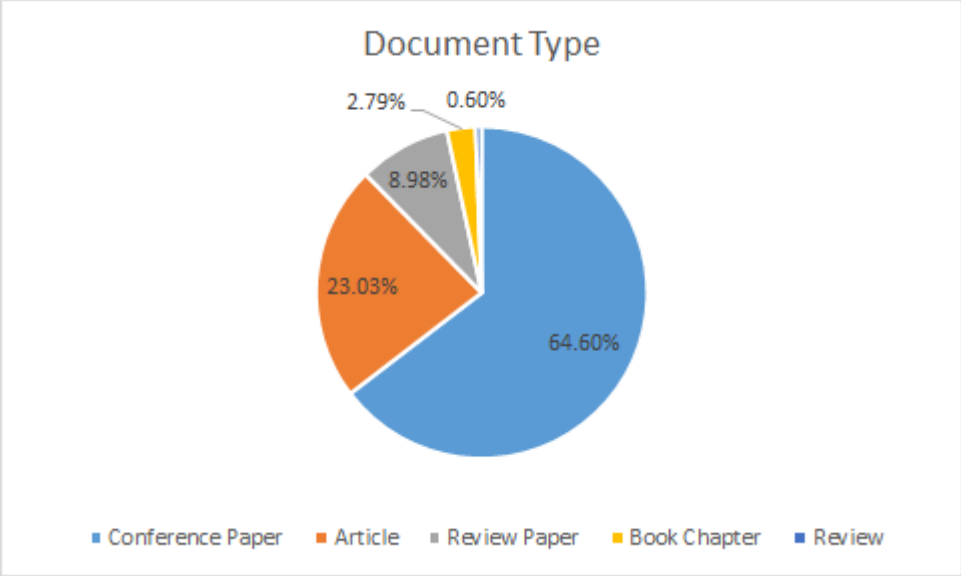

Figure 3. Pie Chart for Document Type Analysis

2.3 Trends of Publications

The publication consisting of face anti spoofing as keywords are published every year from 2012 to 2020. The count of publications show steady growth in the publications every year and the graph is rising every year. The year 2019 has recorded the highest number of publications in this domain. The table representing publication count obtained from Scopus dataset is shown in table 4 below and graph representing it is shown in figure 4.

Table 4. Yearly Publication Trends

Year	Publication Count	Year	Publication Count
2021	1	2016	17
2020	20	2015	6
2019	64	2014	5
2018	36	2013	2
2017	24	2012	3

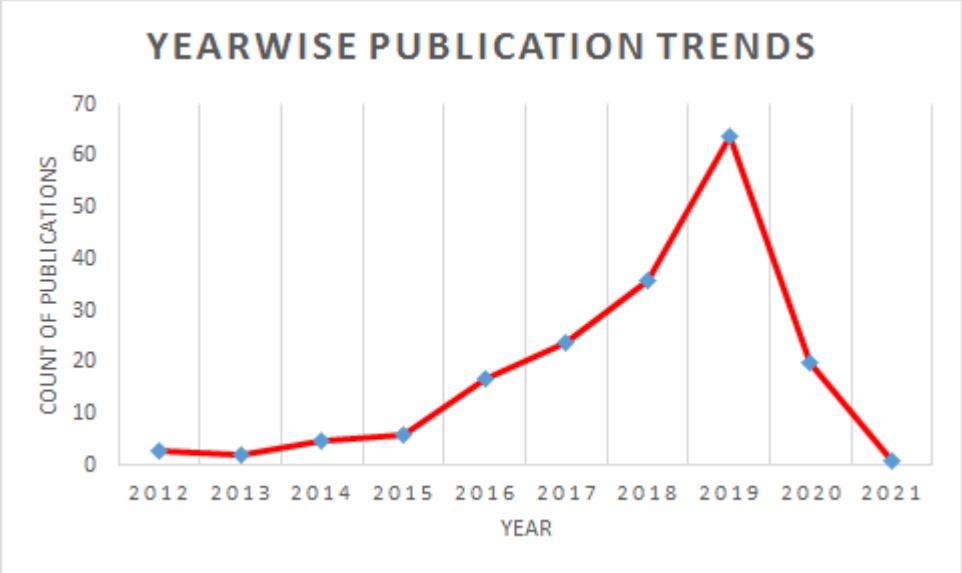

Figure 4. Year wise Analysis of Publications

The above section 2 describes the publication information in terms of total count of publications in Scopus database for face anti spoofing keyword, type of publications done, Yearly trends in the publications and lastly in terms of publishing language used in the document. The next section 3 describes the analysis of the publications for the core keyword considering different factors such as author affiliations , country wise publications, subject area wise publication’s etc. and many more.

3. Bibliometric Analysis: Face Anti Spoofing

Face Anti spoofing (Singh and Arora, 2017) is the term associated with developing systems that can prevent spoofing or falsification of face images of the individual that fool the authentication system and enable access to the system and resources associated with it. Many different techniques are developed to perform spoofing and these are referred to as spoofing attacks (Boulkenafet, Komulainen, and Hadid 2018). The work in this domain is done all over the globe and many researchers have contributed to the development of anti-spoofing techniques. This section focuses on the analysis of the work done in this research domain in respect to different aspects and regions.

Some of the aspects explored for analysis of the work published on face anti spoofing available in Scopus dataset are subject areas, geographical analysis, author statistics, affiliation analysis etc.

3.1 Subject Areas

The research on face anti spoofing is done in many domains where major share of research is by computer science researchers followed by the engineering stream researchers. It is interesting to note that mathematics experts too have worked on developing systems for face anti spoofing by writing statistical methods. There is very little work carried out in the area of management, material science, energy and biology. Figure 5 below represents the subject areas that have contributed in terms of searched keyword Face anti spoofing. 50% dominance is by researchers in the area of computer science, lot of research is carried out in this area at present.

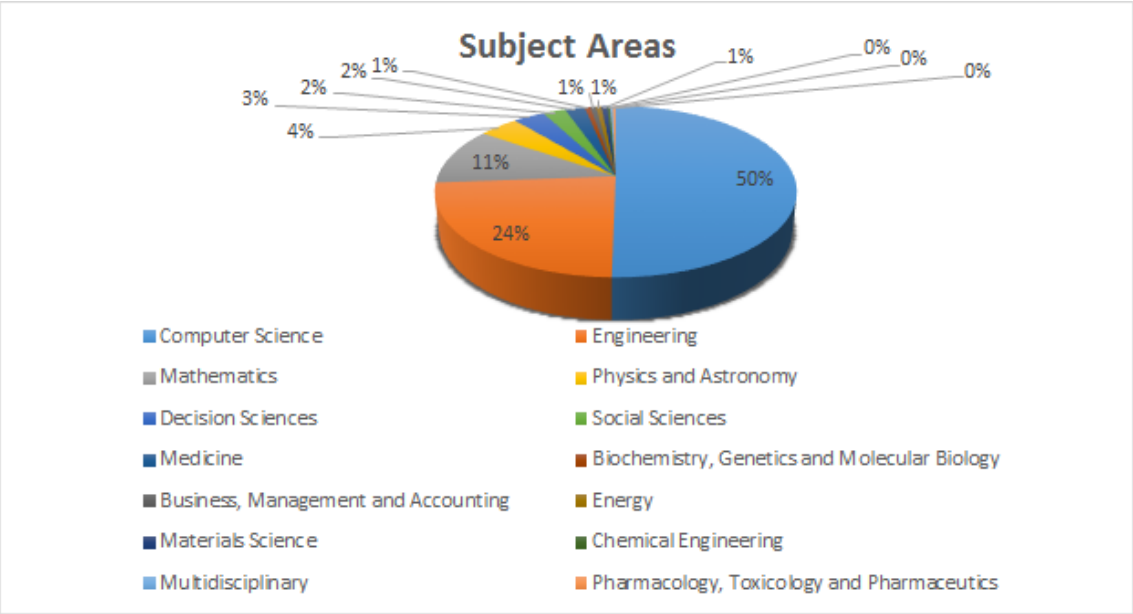

Figure 5. Analysis of document based on subject areas

The above graph clearly states that more than 74% of the work is published by the researchers in the subject area of computer science and engineering.

3.2 Geographical Analysis

This analysis is based on the research work done in different regions of the world and depicts the contribution of the researchers to this domain. In the figure 6 below top ten countries in terms of publications are shown where China leads with a share of 66 publications followed by Finland, Hong Kong and India.

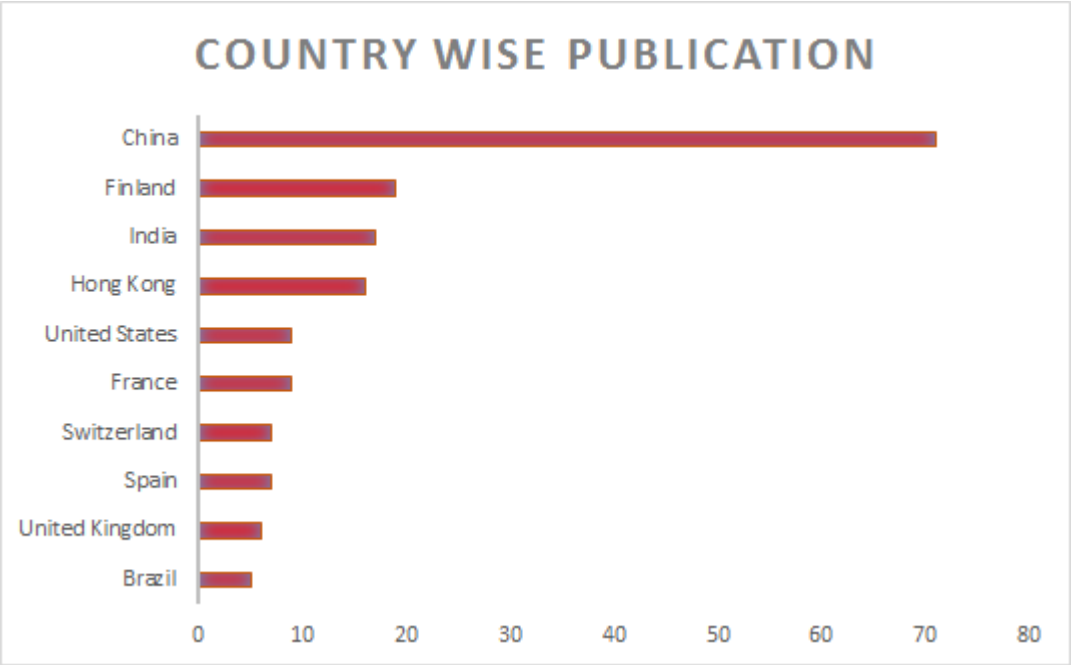

Figure 6.Top Ten Countries in publication on Face anti spoofing

The above graph depicts that Indian researchers have a scope and domain to work and contribute their research. The next section describes the publication count in terms of affiliations statistics and author statistics. The country based network map of researchers from different countries is generated and shown in below figure 7.

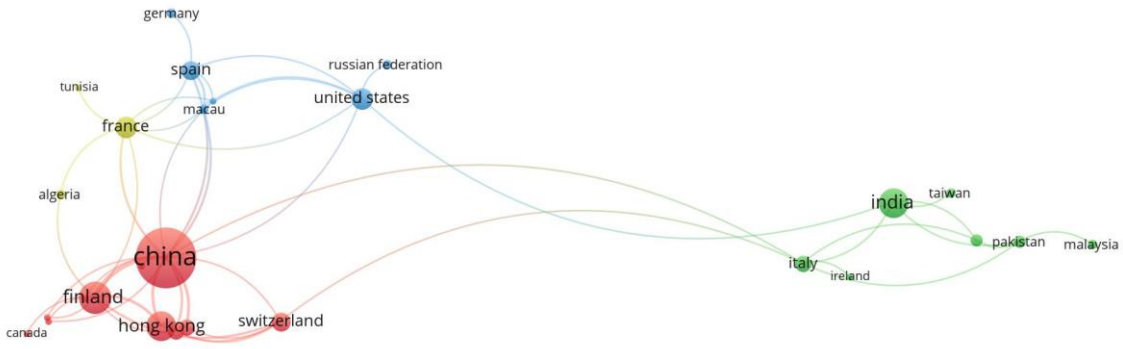

Figure 7. Network map based on Authorship for different countries

3.3 Affiliations Analysis

The affiliations analysis indicates the university/organizations that contribute to the research on Face anti spoofing. The graph for the affiliations is shown in figure 8 below. The analysis shows Oulun Yliopisto University, Finland tops the affiliations chart whereas out of top ten universities 6 universities are affiliated to China, 2 to Hong Kong and 1 is affiliated to Switzerland.

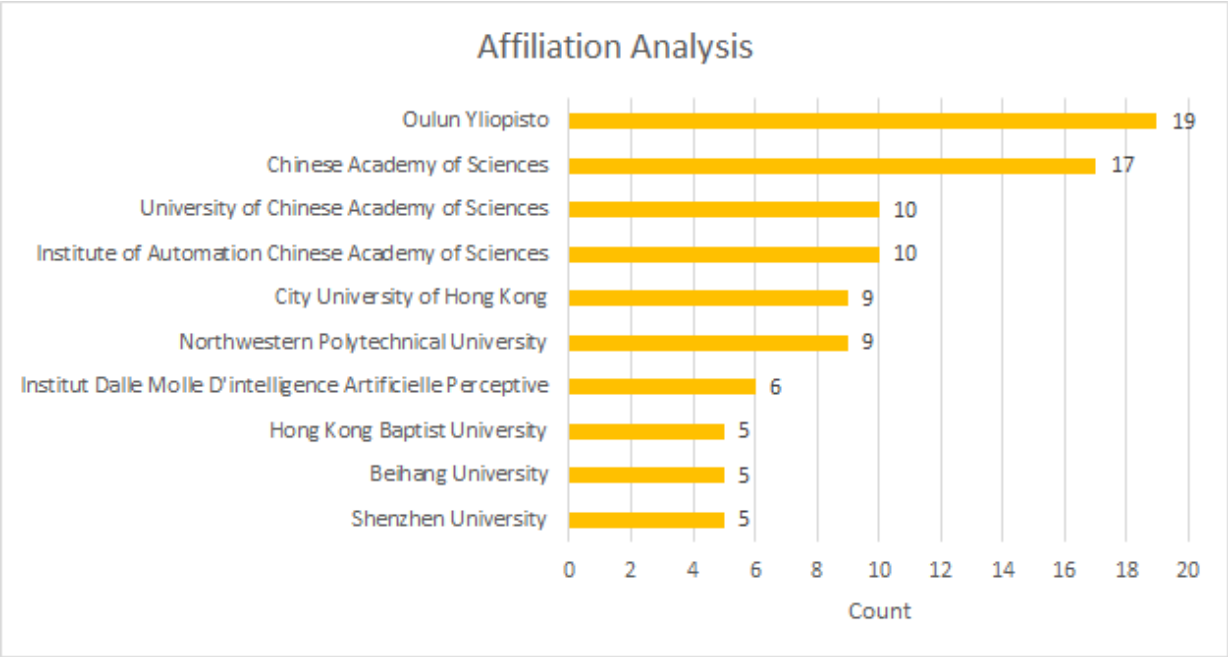

Figure 8. Affiliations for Face Anti Spoofing

The China Universities have worked a lot and have a good number of researchers working in face anti spoofing, there is lack of work from India affiliated university researchers. Here through this survey we try to contribute and review the scope and need for work to be done for face anti spoofing.

3.4 Keyword Analysis

This section presents analysis of different keywords, core keyword focussed is face anti spoofing and other keywords that are generated with it are secondary ones.

Secondary list of keywords include face recognition, anti-spoofing, biometrics and security. The table 5 below shows the frequency of keywords usage in the articles published in this domain.

Table 5. Keyword Frequency

Sr No.	Keyword	Count
1	Face Recognition	99
2	Anti- Spoofing	91
3	Biometrics	62
4	Face Anti-Spoofing	61

The keyword based network map is shown in figure 9, face recognition is at the centre of network map. It has connections to face anti spoofing, face recognition systems and many other keywords. Since the occurrence of face recognition, biometrics, and face anti spoofing is high they are concentrated at the centre.

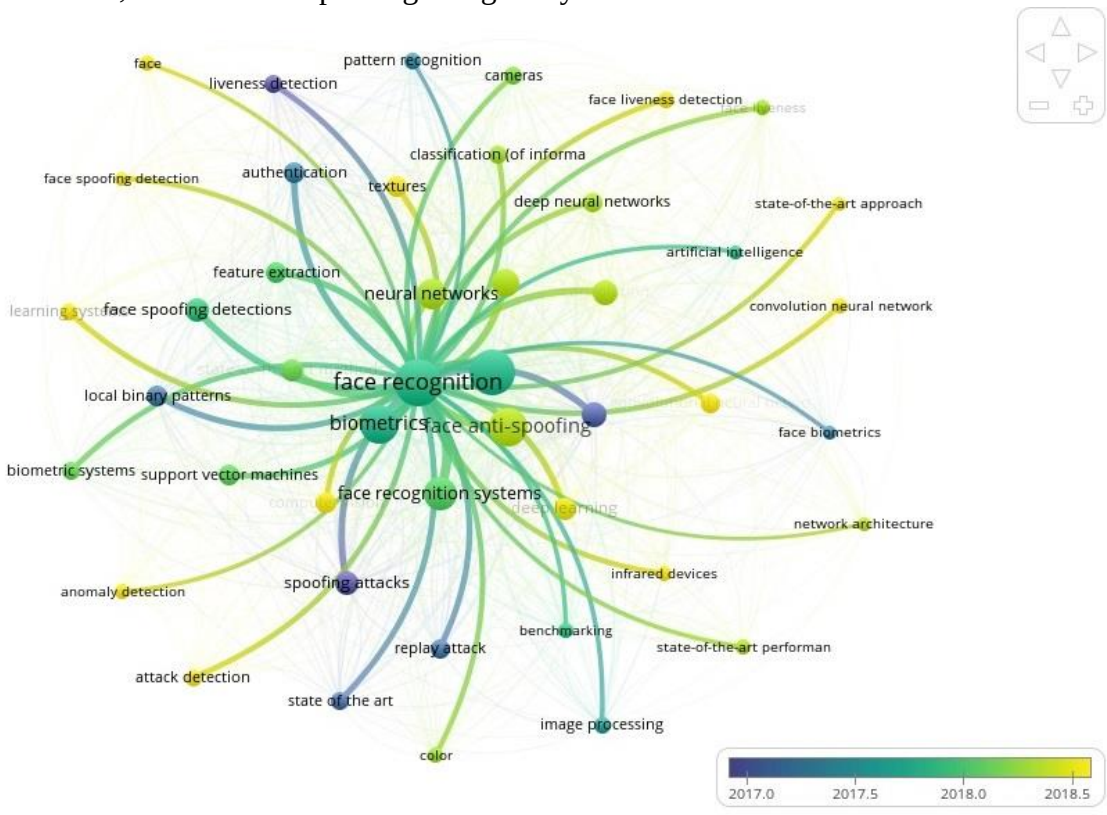

Figure 9. Network Map obtained using VOSViewer

Density map of keywords shown in figure 10, maximum density is concentrated on face recognition keyword as can be seen in figure with yellow patch.

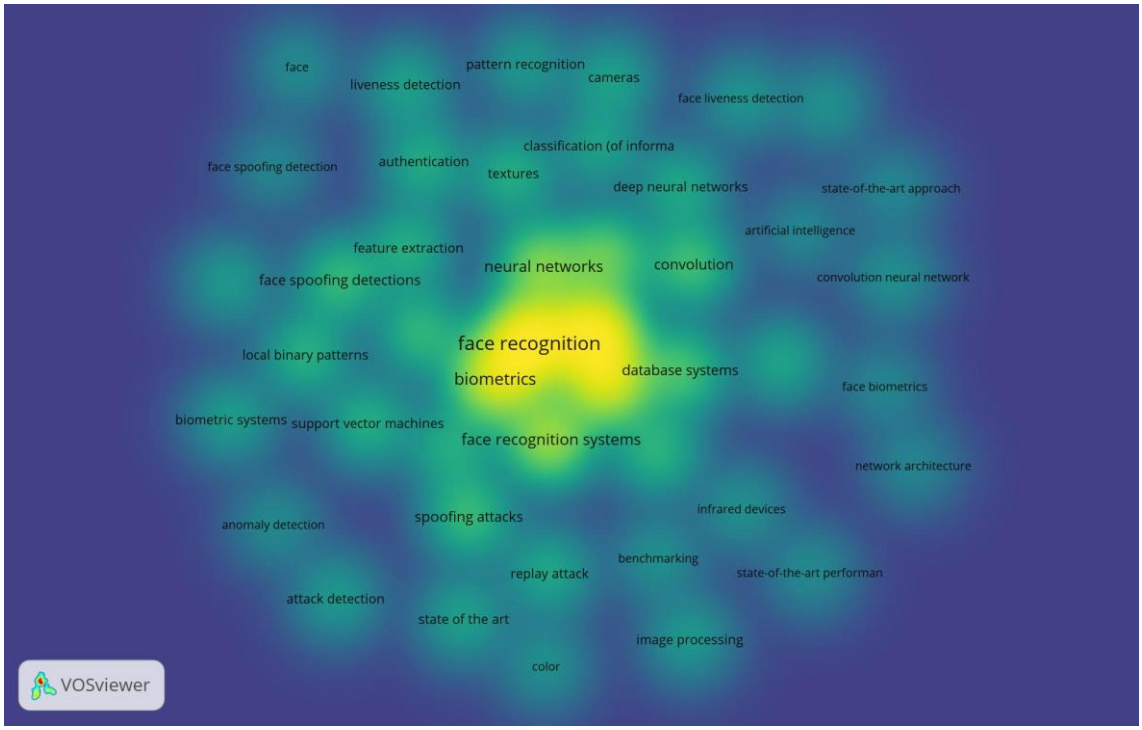

Figure 10. Density of Keywords obtained using VOSviewer

The network map obtained using VOSviewer () for the keywords and their density is shown in figure 9 and figure 10.

3.5 Source type Analysis

The Source analysis shows that maximum research has been published in Lecture Notes in Computer Science (LNCS) Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics.

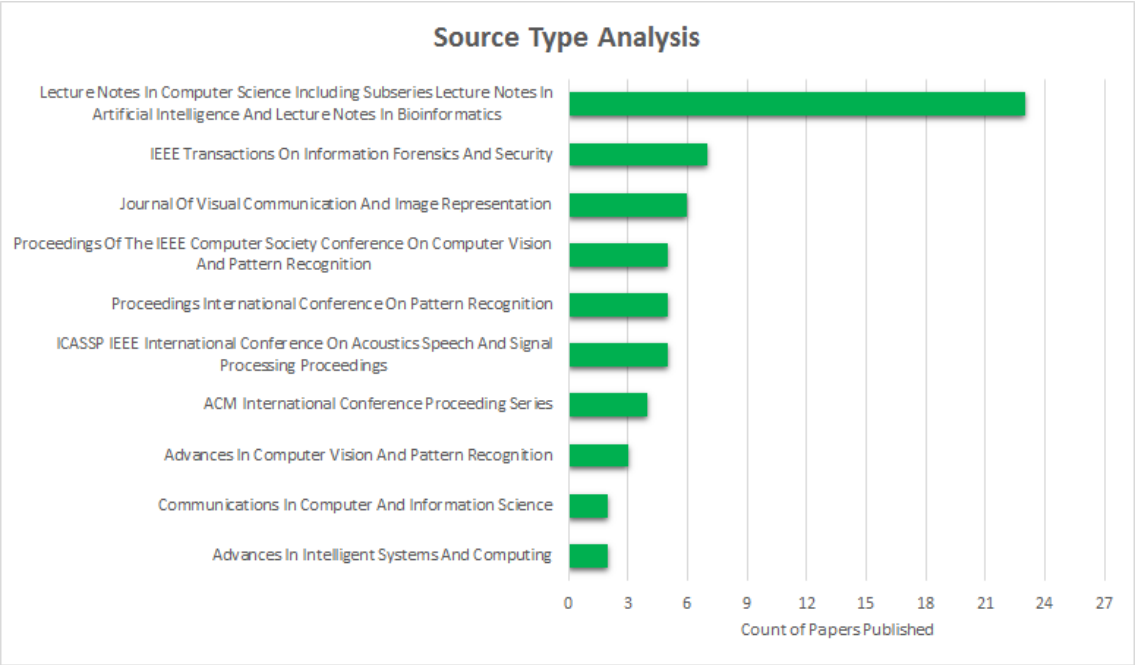

Figure 11. Source Type Analysis

The source statistics from figure 11 clearly indicates that Lecture Notes in Computer Science is the area where maximum publications are done followed by IEEE conference on CVPR and IEEE transactions on Information forensics and security. Maximum number of publications are done through conference proceedings through conferences on computer vision & pattern recognition and biometrics. This statistics paves a way for selection of sources for article publication on face anti spoofing.

3.6 Citation Analysis

The citation count year wise is shown in table 6 below. The total citation count of 172 publications is 2137 till date. The top ten papers in descending order of citation count is shown in the table 7 below, its represented year wise from 2012 to 2020. In table 7 the analysis states that among the top ten cited papers maximum papers are based on the texture features extracted, few papers on image quality assessment and there are few papers that have used CNN/deep learning approach.

Table 6. Citation count from 2012 to 2020

Year	<2016	2016	2017	2018	2019	2020	Total
Count	153	126	182	443	861	537	2319

Table 7. Citations Count for top ten publications in Face Anti Spoofing

Title of Paper	**<2016**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**
On the effectiveness of local binary patterns in face anti-spoofing	61	36	41	64	87	35	325
Face Spoofing Detection Using Colour Texture Analysis	0	1	15	36	68	35	155
Can face anti-spoofing countermeasures work in a real world scenario?	18	19	12	30	32	12	123
Face anti-spoofing based on color texture analysis	0	9	10	27	44	24	115
Face liveness detection using dynamic texture	13	10	13	30	22	11	100
Face anti-spoofing based on general image quality assessment	7	7	12	23	28	8	86
Integration of image quality and motion cues for face anti-spoofing: A neural network approach	0	2	5	21	39	10	78
Face anti-spoofing using patch and depth-based CNNs	0	0	0	10	40	25	76
Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision	0	0	0	1	46	25	74
Context based face anti-spoofing	7	7	8	13	27	8	71

The analysis of the citation count from 2012 to 2020 provides us with an important clue about the area / technique to focus on for starting the initial work and defining

objectives. The maximum citation count of 315 is obtained for paper on local binary pattern, this clearly provides an idea that local feature descriptors have been referenced continuously especially in terms of texture descriptors. This also deduces that many researchers have worked with LBP as their base and then designed its multiple variants to improve the systems. There are a good number of citations for systems with colour and texture combinations along with image quality assessment mechanisms.

4 Deductions from Bibliometric Analysis

This section describes the research outcomes obtained after the overall analysis done on the core keyword i.e. face anti spoofing. The outcomes will provide some research goals and objectives that can be explored further for implementation and designing of new systems. The aim of this paper is to develop insights that can strengthen research in this area and especially on face anti spoofing. As per the analysis done there are maximum publications in the English language by the authors from different regions, another analysis clearly states that maximum publications are done through conference paper and conference proceedings. There are a good number of papers published in journal papers too, the analysis reflects that there are only few review papers published in face anti spoofing. Writing a comprehensive review paper is one research direction that can be taken into consideration. A Key finding of the analysis is that , based on the citation analysis the top ten results indicate that texture based publications are cited mostly and scope of the researchers is on developing new texture descriptors and hybrid deep learning models.

The keywords analysis done for face anti spoofing indicate there is increasing work done in the area of deep learning by designing new CNN models in combination with depth information. Depth information of face images in terms of 3D images and

motion analysis in videos serves important cue in face anti spoofing detection. The analysis clearly indicates that lecture notes on computer science is the source for maximum publications which is followed by domain specific conferences on computer vision and pattern recognition and Biometrics. The IEEE transactions on Information forensics and security which is a high impact factor journal has a good number of works published with some other journals from Elsevier and Scopus on biometrics. The citation analysis opens three main paths for the work that can be done in this area, developing a hybrid system of colour and texture combination, design of new image quality assessment methods and lastly building deep learning models with hybrid structures.

5 Scope of Existing Study

The scope of the study and analysis for Face anti spoofing is restricted to only Scopus dataset, other datasets have not been considered such as IEEE Xplore, Google scholar etc. The language of publications has been restricted to English only, researchers can explore the other datasets and can come up with refined and improved analysis for face anti spoofing.

6 Conclusion

The survey of the bibliography on face anti spoofing indicates that maximum work is contributed by China and satisfactory contribution by India too. The publication source for these publications is majorly LNCS and also conferences and journals related to computer science. The conferences related to domain areas such as computer vision and pattern recognition and biometrics security have good work published by different authors. IEEE and Scopus journals are also among the major sources for face anti spoofing work. The keyword analysis indicates that face anti

spoofing is the majorly used keyword followed by face recognition, biometrics and anti spoofing. The major subject area contributing to this domain is computer science and engineering but very few contributions done in terms of review papers. The keyword analysis shows that deep learning is a less utilized key word and area that can be explored. In terms of research region wise, Indian researchers have a good opportunity to explore this domain and contribute massively.

The citation count from the table clearly indicates that texture and color based pacers have been cited highly and the research community focuses on designing or redefining the texture descriptor techniques. Design of new texture descriptor, improved and improvised method for image quality assessment and Design of hybrid deep learning model are the three key mechanisms that can be targeted in face anti spoofing. The in depth Bibliometric analysis clarifies the research direction and provides an important insight on the future research work in this domain.

7 References

Boulkenafet, Z., Komulainen, J., & Hadid, A. (2018). On the generalization of color texture-based face anti-spoofing. Image and Vision Computing, 77, 1-9.

Chan, P. P., Liu, W., Chen, D., Yeung, D. S., Zhang, F., Wang, X., & Hsu, C. C. (2017). Face liveness detection using a flash against 2D spoofing attack. IEEE Transactions on Information Forensics and Security, 13(2), 521-534.

Edmunds, T., & Caplier, A. (2017). Face spoofing detection based on colour distortions. IET Biometrics, 7(1), 27-38.

George, A., Mostaani, Z., Geissenbuhler, D., Nikisins, O., Anjos, A., & Marcel, S. (2019). Biometric face presentation attack detection with multi-channel convolutional neural network. IEEE Transactions on Information Forensics and Security, 15, 42-55.

Hamdan, B., & Mokhtar, K. (2018). The detection of spoofing by 3D mask in a 2D identity recognition system. Egyptian Informatics Journal, 19(2), 75-82.

Kinnikar, A., Husain, M., & Meena, S. M. (2016, August). Face recognition using Gabor filter and convolutional neural network. In Proceedings of the International Conference on Informatics and Analytics (pp. 1-4).

Li, L., Xia, Z., Hadid, A., Jiang, X., Zhang, H., & Feng, X. (2019). Replayed video attack detection based on motion blur analysis. IEEE Transactions on Information Forensics and Security, 14(9), 2246-2261.

Raghavendra, R. J., & Kunte, R. S. (2020). Extended Local Ternary Co-relation Pattern: A novel feature descriptor for face Anti-spoofing. Journal of Information Security and Applications, 52, 102482.

Shinde, S. R., & Thepade, S. (2018, August). Gender Classification from Face Images Using LBG Vector Quantization with Data Mining Algorithms. In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA) (pp. 1-5). IEEE.

Shinde, S. R., & Thepade, S. D. (2015, December). Gender classification with KNN by extraction of Haar wavelet features from canny shape fingerprints. In 2015 International Conference on Information Processing (ICIP) (pp. 702-707). IEEE.

Singh, M., & Arora, A. S. (2017). A robust anti-spoofing technique for face liveness detection with morphological operations. Optik, 139, 347-354.

Vanitha, A., Vaidehi, V., & Vasuhi, S. (2018, September). Liveliness Detection in Real Time Videos using Color based Chromatic Moment Feature. In 2018 International Conference on Recent Trends in Advance Computing (ICRTAC) (pp. 162-167). IEEE.

Wang, S. Y., Yang, S. H., Chen, Y. P., & Huang, J. W. (2017). Face liveness detection based on skin blood flow analysis. Symmetry, 9(12), 305.

Wasnik, P., Raja, K. B., Raghavendra, R., & Busch, C. (2016, November). Presentation attack detection in face biometric systems using raw sensor data from smartphones. In 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS) (pp. 104-111). IEEE.

Yeh, C. H., & Chang, H. H. (2018, March). Face liveness detection based on perceptual image quality assessment features with multi-scale analysis. In 2018 IEEE Winter Conference on Applications of Computer Vision (WACV) (pp. 49-56). IEEE.