

# Insights on Schemes towards Image Counterfeit Attacks & Their Effectiveness

Shashikala S, Lokesh N

**Abstract:** This paper reviews significant schemas pertaining to image forensics where the prime emphasis has been laid towards exploring the mechanisms which identify image counterfeit with higher accuracy. The study reviewed the prime contribution published in the last four years and also addressed the unsolved research problems which are needed to be objectified. The extraction of the research gap further extensively elaborated, which identify the gap needed to be filled up. The extensive review of literature also provides better insight into the design aspects associated with the conventional techniques which are defensive against counterfeit image attacks. The future direction of this investigational study aims to come up with a solution model which can address the accuracy and complexity problems which exist in the conventional system.

**Keywords:** Counterfeit Image attacks, Image Security, Manipulated region detection.

## I. INTRODUCTION

In the present, there is no doubt that we live in an era of an advanced digital camera in which we are in contact to a series of extraordinary digital images, which nowadays has become a useful and more convenient tool for sharing of information as well as communication [1]. The images are believed to offer more truthfulness about the event and incident than verbal communication. Images have their potential to deliver more information within less size of data and are more powerful when they get mixed with other forms of media such as text and speech. At present, the adoption of digital images is proliferating in the field of education, journalism, healthcare departments, social media, and various enterprises [2]. Hence, it significantly becomes a universal medium to provide impactful information to reach out needs of personal goals, business goals, as well as educational purposes [3]. However, as the usage of digital images increasing, the trustworthy factor of images decreasing day by day. It is due to because the images are nowadays readily available at various resources such as newspaper, magazines, and internet [4]. The internet is the primary source to capture or download an image from the publically accessible websites and social media platforms. With the existing robust image editing tools, peoples are performing manipulation, changing the content of an image without leaving any mark on the manipulated image [5]. Manipulating original image or creating a fake image is called counterfeit image attacks.

The digital images are a two-dimensional representation of a finite set of pixels. Therefore, it is not a big job to perform

**Revised Manuscript Received on January 05, 2020**

\* Correspondence Author

**Shashikala S\***, Assistant Professor, Department of Computer Science & Application, New Horizon College Kasturi Nagar, Bangalore, India, Email: shashikala.research@yahoo.com

**Lokesh N\*\***, Professor, Department of Computer Science & Engineering, Rajarajeshwari College of Engineering, Bangalore, India

counterfeiting attacks on digital images with the currently available image processing and editing tools. There exist various types of commonly known image attacks that are image cloning, image tampering, image splicing, etc. [6-8]. The image cloning refers to a process of post-processing followed with copying and pasting image content within the same image. Image tampering is an operation of content modification in the original digital image. The image splicing is another version of image tampering in which an attacker merges two pictures from the different source into a single surface image. Nowadays, various cases are arising associated with counterfeit image attacks in medical filed, news, social media platforms, and private firms [9-10]. The purpose is only to get attention, making fun, and misrepresents the situation, falsifying evidence, and making a negative image of an individual. This shows that a digital image counterfeit attack grows at a terrifying rate in different application areas, which has been negatively flagged to accept the authenticity of digital images. Therefore, to deal with image counterfeit attacks, the researchers have developed many image security techniques such as watermarking techniques, digital signature, active and passive authentication [11-12]. As the advancement in digital system and technology emerging day by day, the researchers have introduced forensic technology.

Currently, forensic technology is evolving as a flashpoint in the area of digital image security due to its potential of determining image authenticity and pattern of originality without depending on any embedded information and signature function [13-14]. However, there is still a requirement of efficient and robust technique. Because as the technology getting smart and advance the peoples are moving towards digitization where all the paper works are now uploaded mostly in the form of an image via the internet to secure database system. Therefore, the contribution of this manuscript is to provide a quick insight into the effectiveness of existing schemes towards Image Counterfeit Attacks. The rest part organized as follows: Section II presents the counterfeiting issues, Section III discusses the existing approaches for resisting image Counterfeit, Section IV presents review work. The next Section V demonstrates research trend. Section VI presents the research gap, and the conclusion of the presented survey work is given in Section VII.

## II. IMAGE COUNTERFEITING ISSUES

Different fraudulent access attempts are using various synthetic traits and gummy prints and printed iris, face on papers. The types of attacks [1] are classified as:-

- **Direct Attacks:** These attacks are done with artificial biometric samples, e.g., Sticky fingers and printed iris, etc., In this type of attacks, no exact knowledge regarding the system is wanted. Moreover, the

attack is carried out in the analog domain, outside the computerized restrictions of the system.

- **Indirect Attacks:** In this type of attacks the impostor needs to have some extra information about the internal operations of the system and, in some cases, physical access to some of the application mechanism is also required.

Different levels of attacks against a biometric system are

- Artificial biometric traits may be presented at the sensor.
- Illegal data may be submitted to the system.
- Some program may change the feature template.
- Matcher may be changed with that gives high scores.

The biometric systems consist of an extensive database of biometric samples whose performance is quality assessed with a standard protocol of genuine and imposter traits. The performance is measured by the no. of misclassifications, i.e., genuine traits being classified as impostor trait and vice versa.

**A. Fingerprint Spoofing**

If there should be an occurrence of fingerprint spoofing attacks, the user can utilize his insight to make a sticky fingerprint through a dormant unique fingerprint. This dormant fingerprint is first featured by utilizing some scientific counterfeited strategies, and after that, a photo was captured. The two-phase procedure is commonly used to make the fake fingerprints. The primary (image template) stage is trailed by remaking the fingerprint from the original user's particulars template. The next stage is to make sticky fingerprint from the images, where the images were recreated to get characteristics of the fake fingerprint. Generally, more than 70% of the fingerprints are being acknowledged by the biometric frameworks [2-4].



**Fig.1 Fingerprint spoofing**

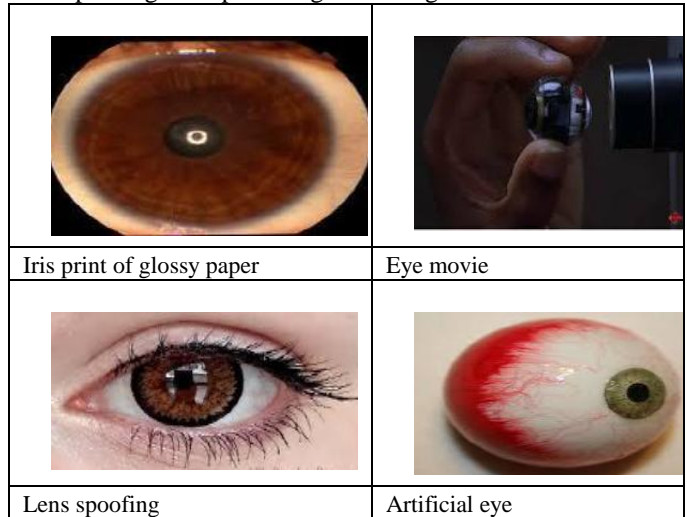
The fingerprint spoofing can be consensual or non-consensual type were the consensual type of fingerprints are created by fake traits with the joint effort of the fingerprints of the original user, and the non-consensual type of fingerprint spoofing utilizes fingerprint left over the surfaces, to make the fake fingerprints, and it does not require users. If there should arise an occurrence of consensual technique, the means to be pursued are:

- The user utilizes delicate material and puts stress on his finger to get the print of the finger as shape
- Gelatin, pliant plastic, dirt, wax, such throwing material is poured on the shape
- The fake fingerprint is shaped when the fluid gets solidified.

**B. Iris Spoofing**

The iris is that the space of the eye and place the hue circle, at times darker or blue, rings the dim pupil of the consideration. Iris recognition frameworks utilize modest, excellent cameras to catch a high contrast high-quality photo of the iris. In iris recognition, the framework use camera to require the input test and furthermore the software framework contrasts the outcome and the keep layouts. Iris biometry can have

particular qualities and alternatives to check the character of an individual. This technique takes 2 seconds and gives the data of the iris that are beginning mapped, recorded, and hang on for future confirmation. When the picture is caught, the iris' [5] versatile tissue which is referred as fibrous tissue coinciding that is examined, prepared into partner optical "unique finger impression," and converted into a digital form. The iris spoofing is possible in real ways one of the spoofing methods where the user uses eye printouts on the glossy paper, eye movie (placing the eye in front of the camera), Iris lens spoofing an artificial model of the eye and it has appeared front of the cameras during the task of detection. Some of the Iris spoofing examples are given in Figure.2.



**Fig. 2 Irish spoofing**

**C. Face Spoofing**

Face spoofing is a technique where anyone will capture the images of anyone without intimating them. Also, with the assistance of social networking websites, any pictures will be downloaded and that they will be used for spoofing in image attacks, which is shown in figure.3.



**Fig.3 Face spoofing**

Picture adjusting is portrayed as "including, changing, or erasing some significant highlights from an image which not indicating any conspicuous follow. There have been various systems used for producing an image. Considering the techniques used to make counterfeited images, computerized image counterfeit can be secluded into three essential orders: Copy-Move counterfeit, Image joining, and Image resampling [6-7].

**D. Copy-Move Counterfeit**

In copy-move counterfeit (or cloning), some piece of the image is reordered to another zone in the same picture to shroud some important data from exhibited in Figure 4. As the duplicated part began from a similar image, its fundamental properties, for example, noise, color, and surface, does not make the recognition procedure issues.





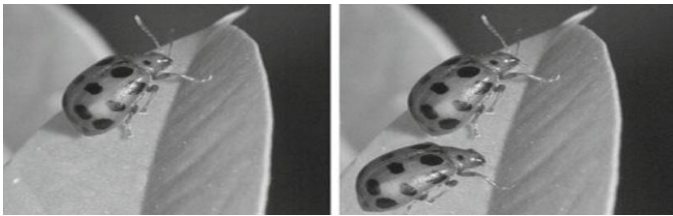


Fig.4 Copy-Move Counterfeit

**E. Image Counterfeit using joining**

Image joining uses reorder systems from at least one images to make another fake image. When grafting is performed accurately, the outskirts between the joined locales can outwardly be vague. Joining, be that as it may, bothers the high request Fourier measurements. These bits of knowledge can thusly be used as a piece of recognizing fake. Figure 5, exhibits an excellent example of image joining where the shark image and helicopter image are converted into one picture [8].



Fig.5 Image joining the attack

**F. Image Resampling**

In order to dumbfound a counterfeited image, some chosen districts need to experience geometric changes like the revolution, scaling, extending, slanting, flipping, etc. The interjection step assumes a significant job in the resampling procedure and presents non-irrelevant measurable changes. Resampling brings definite, specific correlations as the image and is used for recognition of false information through resampling. In Figure 6, the first image on the left and counterfeited image gotten by pivot and scaling it [10].



Fig. 6 Image Resampling Attack

**III. APPROACHES OF RESISTING COUNTERFEIT**

Computerized forensic is usually utilized in criminal/private laws examination. Scientific investigation if images on informal online organizations utilized for recognizing altered or counterfeited images. Image counterfeit recognition framework is required in numerous fields for securing copyright and forestalling counterfeit or modification of images. It is connected in territories, for example,

news-casting, logical distributions, computerized measurable science, media security, reconnaissance systems, and so on. Electronic picture counterfeit revelation strategies are requested in dynamic and dynamic methodology.

**A. Dynamic Methodologies**

A dynamic area technique which contains including picture focal points in order to delineate mechanized adjusting, i.e., name, date, signature, and so forth [1-12]. It requires an exceptional equipment execution to check the confirmation of the automated picture.

**B. Types of Active Approach**

There are two forms of active approaches which includes watermarking and computerized signatures.

- **Watermarking:** This is utilized for counterfeit image identification and needs to be installed at the period of making the image. Introducing a watermark in the image/video is proportionate to denoting a specific mechanized mark on the substance of pictures/chronicles. When the image/video is controlled, this watermark will be crushed with the end goal that the authenticator can see it to affirm the advancement of substance. The watermarking contains covering an engraving or a message in a photo remembering the ultimate objective to verify its copyright at the period of picture acquiring and to check the authenticity this message is isolated from the image and affirmed with the principal watermarks. If the image is not controlled, these watermarks will remain same else they will not organize the primary watermarks. Along these lines, this system relies upon the source data in advance. Some camera sources do not embed watermarks into the picture; subsequently, this method is not so useful, and more regularly that does not work splendidly with lossy compression. The active methodology offers low Computational cost, essential if information about a unique image is accessible [13].

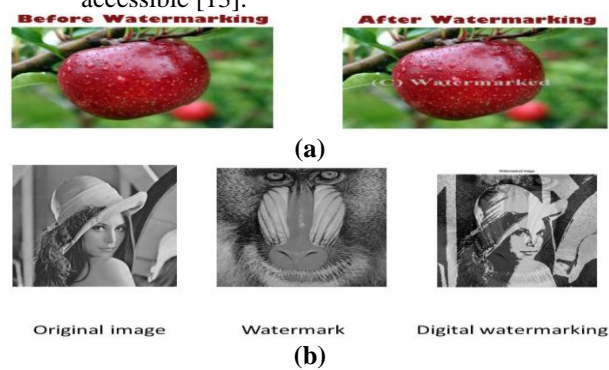
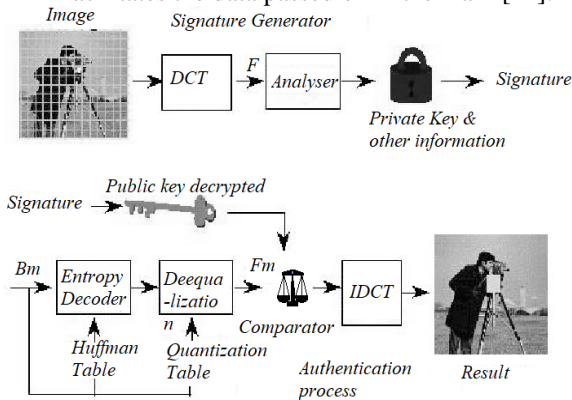


Fig. 7 Examples of watermarking

- **Computerized Signatures:** Modern mark is some cryptographic is a logical arrangement for displaying the validness of mechanized report. It makes a substance based automated mark which fuses the fundamental data of substance and the specific creator unmistakable confirmation. The mark is delivered by a producer specific private key with the end goal that it

cannot be made. Thus, the authenticator can check a picture/video by reviewing whether its substance facilitates the data passed on in the mark [14].



**Fig.8 Process of Signature Generator and Authentication**

An image and mark which are delivered is an encoded sort of the component codes or hashes of this image, and it is secured autonomously. When a user needs to check the received image, perform the on that mark and consider the hash characteristics or codes of the image to their relating esteems in the primary signature. If they organize, this image can be considered as "authentic."

- Limitations of Active Approach: With all significances, the active approaches exhibit some of the limitations:
- These systems require earlier information about the original image as they are not programmed to detect. They needed human help or uniquely prepared cameras.
- There exist many mechanized images over the cloud without a modernized signature or watermark. Hence, a dynamic methodology could not be utilized to discover the originality of the image.
- The computerized Signature mechanism requires additional bandwidth for transmission of signature.

**C. Passive Approach:** Inactive technique recognizes the replicated items in copied pictures without the need of novel watermark and depends upon pursues left on the image by different getting ready endeavors in the midst of picture control. The non-considered approaches choose a portion of the fake parts in the image. There are two systems for inactive approach, i.e., Picture source identification and recognition alteration. The source identification recognizes the contraption used for the verifying of the image. This indicates that an image is formed through an advanced camera or device. In this strategy, the region of impersonation in the picture cannot be settled. The next is recognition alteration, which perceives the intentional control of pictures for harmful purposes.

**D. Types of Passive Approach**

The passive approaches are of different types and are given below:

- A pixel-based approach which identifies the explicit anomalies placed in the level of the pixel.
- The next is a format-based approach which leverages the explicit correlations placed by the lossy compression mechanism.

- The camera-based approaches can identify the artifacts added due to the lens of the camera or by post-processing of chip.
- There exist physical or geometrical based approaches meant with light, object, and position of the camera.

The significance of the passive approach is that it overcomes the issues of passive approaches while it does not provide any proof of the counterfeit, and this approach is very complicated [10-14].

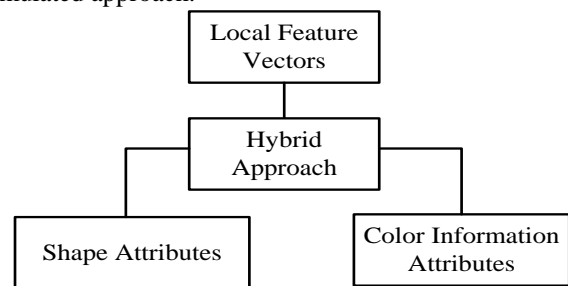
**IV. EXISTING APPROACHES**

This section introduces the most significant research studies evolved up to date with schemas, which are defensive against counterfeit image attacks. It also shows their effectiveness with respect to experimental outcomes. The study of Pun et al. [15] formulated a numerical design modeling which can effectively detect the copy-move counterfeit in the image. The following are the design characteristics of the formulated approach.

- It incorporates block-based and key-point based schemas for counterfeit image detection
- Applies adaptive segmentation and feature mapping.

The technique incorporates an over-segmentation schema which assesses different block representation and further extracts significant block features and other data. The study emphasized improving counterfeit detection accuracy, which is mostly addressed as a research problem. For this purpose, it introduces a robust computational model to extract the counterfeit region with the ease of computation. Finally, it applies a morphological operation on the objectified merged areas which assist in to produce the detected counterfeit regions on image. The study performed an extensive numerical analysis to validate this approach. The experimental outcome shows that irrespective of challenging factors the formulated system yields better detection accuracy in contrast with the state-of-the-art approaches.

A similar study of Ardizzone [16] also addressed the problem that arises due to Copy-move counterfeit and comes up with a novel hybrid strategy. The approach performs a comparative numerical execution in terms of triangles and does not consider the blocks. The following figure shows the triangle matching criteria and conditions associated with the formulated approach.



**Fig. 9 Hybrid approaches of [16]**

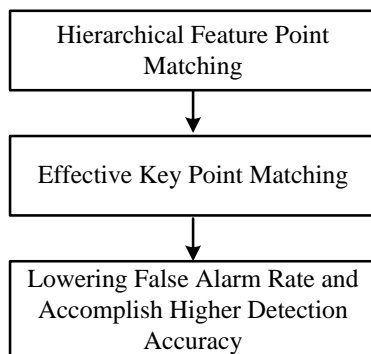
Figure 9 shows how the hybrid approach utilizes connected triangles and match their shapes in terms of three different prime factors. However, the authors claimed that this method is designed in a way where it is robust against any transformation criteria. The study also performed an extensive comparative analysis where the outcome of this approach further compared with the existing studies and even the



datasets made available for the academic research purpose.

Mayer and Stamm [17] also addressed the problem associated with copy-paste image counterfeit and introduces a novel methodology which considers prime chromatic attributes of intensities to identify the affected region of the image. The approach also identified the inconsistencies that exist into chromatic attribute features and assessed their presence through a hypothetical and statistical model. The detection paradigm is evaluated with respect to satisfying certain conditions and claimed that the method attains the optimal outcome. The experimental analysis shows that the formulated estimation towards localizing counterfeit region exhibit better detection accuracy. The experimental analysis also shows that the formulated approach minimizes the cost of computation with reduced estimation time and also balances the magnitude of new estimation errors.

The study of Li and Zhou [18] also explored the potential aspects of key-point based copy-move counterfeit detection mechanisms and also exploited their robustness against various conditions such as in the presence of large-scale geometric transformations. It further encountered that this kind of approaches has limitations to deal with copy-move counterfeit which involve smoother regions. To address this limitation, the study challenged it and introduced a fast and cost-effective scheme which is designed based on hierarchical feature point matching. The design of this formulated approach (as shown in Figure.10) involves valid key-point matching over smooth regions by balancing and lowering the contrast threshold.



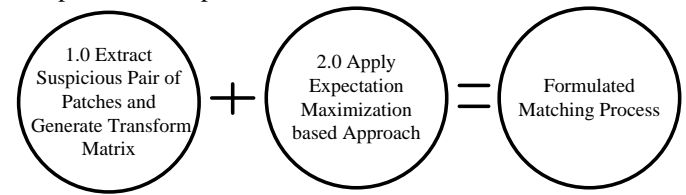
**Fig.10 Approach formulated in the study of [18]**

The approach is also further improvised with an idea of dominant information and scale information handling. The numerical outcome clearly shows that this approach attains superior performance as compared to existing mechanisms to detect the affected region in the image. It also shows that the approach attains superior performance in some of the challenging operational cases.

Another approach of Bappy et al. [19] also formulates a design architecture pertaining to investigate and identify the manipulated region in an image as manipulated regions are not visually apparent often. The manuscript also proposes a robust high-confidence image manipulation architecture and with the advanced and improvised approach of contrast identification. The extensive simulation results show that it is well capable of identifying the manipulation with higher precision factor when three different types of diverse datasets are considered.

Likewise, the approach considered in the study of [20], the study of Li et al. [20] also utilized key-point extraction to determine effective copy-move regions in an image. The

following figure.11 shows the matching process intermediate computational steps.



**Fig.11 Formulated matching approach of [20]**

The algorithm is designed in a way where it effectively refines the matrix composition and confirms the localization of copy-move counterfeit. The numerical interpretation and simulation outcome shows that the formulated algorithm exhibit accuracy and complexity performance, which is quite superior as compared to state-of-art schemas.

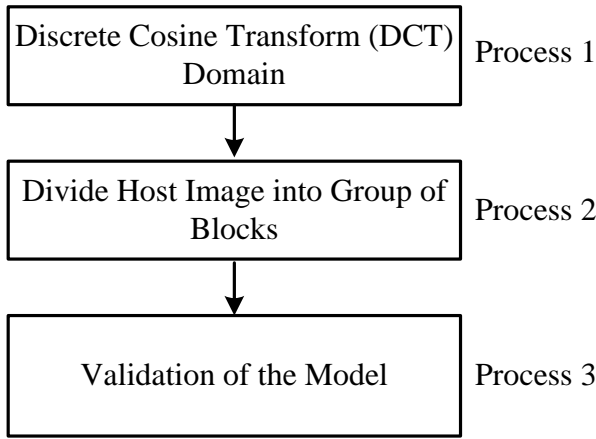
Chen et al. [21], and Cozzolino et al. [22] also focused on this problem with two different novel approaches and formulated reliable and simplified solution models.

In the manuscript of Chen et al. [23], a novel approach, namely FrZMs, is designed and discussed from an experimental and theoretical viewpoint. It has considered fractional quaternion attributes with signal processing. The algorithm execution targeted to speed up the image counterfeit attack detection and localization. The performance of the system has been evaluated considering quaternion signal analysis and robust color image copy-move counterfeit detection procedure. The experimentation has been performed considering two different sets of data, i.e., (FAU and GRIP data set). The outcome shows that FrQZM-based algorithm outperforms the conventional techniques, especially when some extraordinary operational cases are concerned.

The study of Li et al. [24] also introduces a mechanism which can easily and carefully detect the tampered region in an image matrix. In order to perform better localization of image counterfeit, the study focuses on important issues that have not been extensively considered in the majority of the studies. Finally, it proposes a mechanism to improve the performance of counterfeit localization. In the formulated approach, the study initially attempts to improve the

performance aspects of the existing statistical feature-based detector and also further improvised the design structure of copy-move counterfeit detector. The simplified strategy utilizes very less computational resources during runtime, and the experimental outcome shows that it is superior than most existing mechanisms were tried to attain best f1-score in IEEE IFS-TC Image Forensics Challenge.

In the study of Kwon et al. [25], another robust counterfeit detection methodology got evolved up to maintain the privacy preservation of JPEG compressed images. The approach is exclusively watermark based, and its prime target is to prevent the violation of JPEG image content privacy. The implantation of the formulated system targets to identify tampered regions of JPEG with 100% accuracy level. The following figure.13 shows the major steps adopted into this research methodology.



**Fig.12 Formulated approach in [25]**

The experimental outcome shows that the formulated approach attains better accuracy and also exhibit the negligible visual difference between the original and watermark image.

The study of Cristin et al. [26] introduces a new counterfeit detection mechanism where they have incorporated a supervised learning approach. It utilizes the strength factors of vector neural network and fruit fly optimization. The feature extraction is performed using Gabor filter + wavelet + texture operator, and further, it is concatenated with the present input.

The performance evaluation and the validation of the proposed approach have been performed by comparing its outcome with the existing approaches. The outcome of the simulation shows that it attains the accuracy of 0.9523 along with a sensitivity factor of 0.94 and specificity of 0.9583, which are found superior as compared to the baseline techniques.

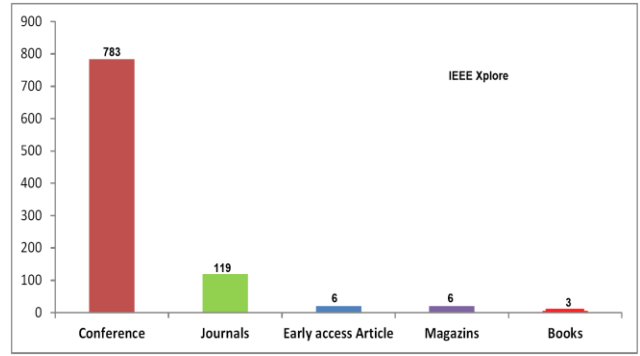
In the study of Guo et al. [27], an effective tamper region detection technique has been introduced from both design and numerical analysis viewpoint. The procedure two consecutive steps of execution, i.e., histogram-based fake colorized image detection along with encoding based image analysis. The comparative analysis further demonstrated the effectiveness of the formulated system which is quite superior as compared to the exiting colorization approaches

**V. RESEARCH TRENDS**

A research publication plays a crucial act to access the information with a collection of the vast library associated with the research subject for the development of technological innovation and concepts. Therefore, this section intended to demonstrate research patters towards digital image counterfeit attacks. The datasets are collected from the many standard publications like IEEE Xplore, Springer, Wiley, and Elsevier (Shown in table 1-to4). The followings are the graphical representation of the research trend carried a different form of publications. The statistics are carried out using the user desired keyword, i.e., image forgery detection.

**Table 1. Shows statistics of the research form IEEE Publication**

Conference	Journals	Early access article	Magazines	Books
783	119	6	6	3

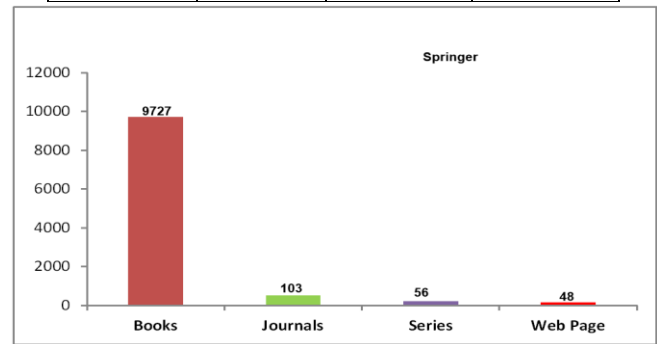


**Fig.13 Statistics of research form IEEE Publication**

The figure.13 graphical representation of research pattern form IEEE Explore digital library subjected to digital image counterfeit detection.

**Table 2. Shows statistics of the research form the Springer**

Books	Journals	Series	Webpage
9727	103	56	48

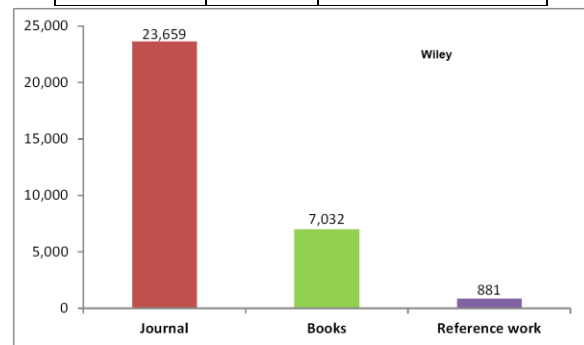


**Fig.14 Statistics of research form Springer Publication**

The above figure.14 demonstrates the graphical representation of the research pattern form Springer Publication subjected to digital image counterfeit attack detection.

**Table 3. Demonstrates the statistics of the research form the Wiley publication**

Journal	Books	Reference Work
23659	7032	881

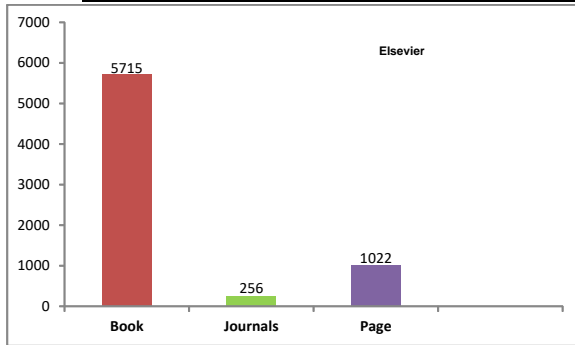


**Fig. 15 Statistics of research form Wiley Publication**

The above figure.15 demonstrates the graphical representation of Statistics carried out from Wiley Publication.

**Table 4. Demonstrates the statistics of the research form the Elsevier publication**

Book	Journals	Page
5715	256	1022

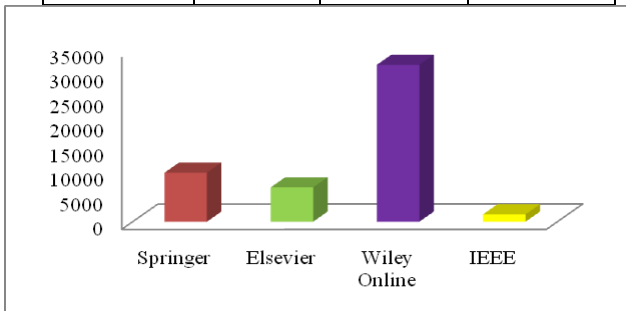


**Fig.16 Statistics of research form Elsevier Publication**

The above figure.16 demonstrates the graphical representation of Statistics carried out from Elsevier Publication. The table 5 shows the datasets are collected from the many standard publications that belongs to Springer, Elsevier, Wiley Online and IEEE publications.

**Table 5. Demonstrates the statistics of the research form different research publication**

Springer	Elsevier	Wiley Online	IEEE
10000	7000	32000	1500



**Fig.17 Statistics of research form different research publications**

The above figure.17 shows the comparative analysis of different research publication where it can be seen that Wiley has published more research paper in the domain of image security and counterfeit attack detection.

## VI. OPEN RESEARCH ISSUES

This section extracts the gap, and there exists an evolution of research track pertaining to image counterfeit attacks. The extensive analysis of existing research works carried out in the prior sections clearly shows that most of the existing studies do not work properly when a noisy image is considered for counterfeit detection. However, a few more significant limitations of the existing system are shown as follows:

- In most of the existing studies, it is observed that computational mechanisms lack efficiency as it consumes much more resource during execution and runtime.
- Few of the existing approaches detect only false-positive results.
- It is also found that most of the existing approaches are specific to image format, whether it fails to

achieve better-tampered region localization when the image format get altered.

- Few existing approaches do not work effectively in the case of blurred images and also consume more time where accuracy is also found lesser.
- Most of the significant techniques also lack efficiency in terms of scaling and local bending factors.
- Few techniques cannot identify manipulated regions which have a rotation of above 10 degrees and scaling.

Along with all these limitations, there exist a set of loop-holes in the existing paradigms which are needed to be addressed. The extensive analysis, as highlighted above, clearly shows that the majority of the techniques also do not accomplish better performance with poor image quality and also not much robust with geometrical operations. It also found that in most of the cases, computation of Zernike movement coefficients invites unnecessary cost of computation and also generate overhead to the system.

Most of the approaches also exhibit slow execution and even result in more false-positive cases, which make this research evolution challenging at a certain stage. Thereby the study formulates its problem in a way where it aims to develop a robust pattern recognition paradigm which can overcome the image altering problem to a greater extent. Also, it aims to design a probabilistic graphical model of pattern recognition to extract counterfeit regions with lesser computational complexity and even with a higher degree of accuracy level, which is less likely addressed in the existing system.

## VII. CONCLUSION

This manuscript mainly presents a comprehensive insight into the effectiveness of existing approaches towards counterfeit image attacks. In the last decades, many techniques for image counterfeit attacks detection have been proposed. However, it has analyzed that image integrity, and identification of tampering areas on images have become daunting research problem without having prior knowledge of original image content. In order to solve this problem, some more techniques were recently presented to detect counterfeit attacks on the image.

But such techniques require more computational time and are not efficient to deal with different types of counterfeit attacks. In this paper, various existing approaches for image attack detection is discussed and reviewed. Based on a review of existing techniques, a significant research gap is concluded for the future research direction.

## REFERENCES



1. Stocchetti, Matteo. "Images and Power in the Digital Age: The political role of digital visuality", Accada Working Papers, 2014
2. "The Power of Picture, "https://digitalmarketingmagazine.co.uk/digital-marketing-content/the-power-of-a-picture/4779, Retrieved on 03-07-2019
3. Örtegren, Hans. "The scope of digital image media in art education." Computers & Education 59.2 (2012): 793-805.
4. Charpe, Jayshri, and Antara Bhattacharya."Revealing image forgery through image manipulation detection." 2015 Global Conference on Communication Technologies (GCCT).IEEE, 2015.
5. Sharma, Deepika, and PawaneshAbrol. "Digital image tampering-A threat to security

management." International Journal of Advanced Research in Computer and Communication Engineering 2.10 (2013): 4120-4123.

6. Jwaid, MohanadFadhil, and Trupti N. Baraskar. "Study and analysis of copy-move & splicing image forgery detection techniques." 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.
7. Hakimi, Fahime, Mahdi Hariri, and FarhadGharehBaghi. "Image splicing forgery detection using local binary pattern and discrete wavelet transform." 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEL).IEEE, 2015.
8. Mishra, Minati, and M. C. Adhikary. "Detection of clones in digital images." arXiv preprint arXiv:1407.6879 (2014).
9. Mushtaq, Saba& Mir, Ajaz, "Novel method for image splicing detection.Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2014.
10. Zampoglou, Markos, Symeon Papadopoulos, and YiannisKompatsiaris. "Detecting image splicing in the wild (web)." 2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW).IEEE, 2015.
11. Murty, M. Sreerama, D. Veeraiah, and A. SrinivasRao. "Digital signature and watermark methods for image authentication using cryptography analysis." Signal & Image Processing: An International Journal (SIPIJ) 2.2 (2011): 170-179.
12. David, Derroll, and B. Divya. "Image Authentication Techniques and Advances Survey." CompuSoft 4.4 (2015): 1597.
13. Wan, X., He, J., Liu, G., Huang, N., Zhu, X., Zhao, B., & Mai, Y. (2015). Survey of Digital Forensics Technologies and Tools for Android based Intelligent Devices. International Journal of Digital Crime and Forensics (IJDCF), 7(1), 1-25.
14. Bhattacharya, Sharbani. "Survey on Digital Watermarking–A Digital Forensics & Security Application." International Journal4, no. 11 (2014).
15. C. Pun, X. Yuan and X. Bi, "Image Counterfeit Detection Using Adaptive Oversegmentation and Feature Point Matching," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1705-1716, Aug. 2015.
16. E. Ardizzone, A. Bruno and G. Mazzola, "Copy–Move Counterfeit Detection by Matching Triangles of Keypoints," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2084-2094, Oct. 2015
17. O. Mayer and M. C. Stamm, "Accurate and Efficient Image Counterfeit Detection Using Lateral Chromatic Aberration," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1762-1777, July 2018.
18. Y. Li and J. Zhou, "Fast and Effective Image Copy-Move Counterfeit Detection via Hierarchical Feature Point Matching," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 1307-1322, May 2019.
19. J. H. Bappy, C. Simons, L. Nataraj, B. S. Manjunath and A. K. Roy-Chowdhury, "Hybrid LSTM and Encoder–Decoder Architecture for Detection of Image Forgeries," in IEEE Transactions on Image Processing, vol. 28, no. 7, pp. 3286-3300, July 2019.
20. J. Li, X. Li, B. Yang and X. Sun, "Segmentation-Based Image Copy-Move Counterfeit Detection Scheme," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 507-518, March 2015.
21. C. Chen, J. Ni, Z. Shen and Y. Q. Shi, "Blind Forensics of Successive Geometric Transformations in Digital Images Using Spectral Method: Theory and Applications," in IEEE Transactions on Image Processing, vol. 26, no. 6, pp. 2811-2824, June 2017.
22. D. Cozzolino, G. Poggi and L. Verdoliva, "Efficient Dense-Field Copy–Move Counterfeit Detection," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2284-2297, Nov. 2015.
23. B. Chen, M. Yu, Q. Su, H. J. Shim and Y. Shi, "Fractional Quaternion Zernike Moments for Robust Color Image Copy-Move Counterfeit Detection," in IEEE Access, vol. 6, pp. 56637-56646, 2018.
24. H. Li, W. Luo, X. Qiu and J. Huang, "Image Counterfeit Localization via Integrating Tampering Possibility Maps," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1240-1252, May 2017.
25. O. Kwon, S. Choi and B. Lee, "A Watermark-Based Scheme for Authenticating JPEG Image Integrity," in IEEE Access, vol. 6, pp. 46194-46205, 2018.  
doi: 10.1109/ACCESS.2018.2866153
26. R. Cristin, J. P. Ananth and V. Cyril Raj, "Illumination-based texture descriptor and fruitfly support vector neural network for image

- counterfeit detection in face images," in IET Image Processing, vol. 12, no. 8, pp. 1439-1449, 8 2018.
27. Y. Guo, X. Cao, W. Zhang and R. Wang, "Fake Colorized Image Detection," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 1932-1944, Aug. 2018.

### AUTHOR'S PROFILE

	<p><b>Shashikala S</b>, Assistant Professor, Department of Computer Science &amp; Application in New Horizon College, Kasturinagar, Bangalore, India. Currently she is pursuing her PhD from VTU, Belagavi, Karnataka, India. She has done her B.E and M.Tech in computer science from. She has around 6 years of teaching experience.</p>
	<p><b>Dr. Lokesh N S</b>, Associate Professor, Department of Computer Science and Engineering at Rajarajeshwari College of Engineering. He has around 10 years of experience.</p>