Image Forgery Detection –Survey on Key Areas of Research Approaches and Challenges

Deepika Kamath[1*], G .P. Hegde[2]

[1]Computer Science & Engineering, Alva's Institute of Engg &Technology, Moodbidri, India(Orcid ID: https://orcid.org/0000-0009-1437-4525)
[2]Information Science &Engineering, SDM Institute of Technology, Ujire, Mangalore, India (Orcid ID: https://orcid.org/0000-0001-8328-0420)

Email address: deepika.k696@gmail.com, gphegde123@gmail.com,
**Corresponding Author: gphegde123@gmail.com*

Abstract— In the era of digital media and social networking, the proliferation of manipulated images has become a significant concern, leading to the spread of misinformation and fake news. Detecting these forged images is crucial for maintaining the integrity of digital content and ensuring trustworthiness in online communication. This review paper provides a comprehensive overview of image forgery detection techniques, covering traditional methods as well as recent advancements in deep learning approaches. The review begins by outlining the different types of image forgeries, including copy-move, splicing, and manipulation, and their implications in various contexts. Subsequently, this paper discusses on Traditional techniques for forgery detection, such as image processing algorithms and feature-based methods, are discussed, along with their limitations and challenges.

Keywords— Forensic, Forging, Tempering, Challenges, Detection, Approaches

1. Introduction

In today's digital age, the manipulation and fabrication of images have become prevalent, posing serious challenges to the authenticity and trustworthiness of visual content. With the widespread use of social media platforms and digital communication channels, forged images can be easily disseminated, leading to the spread of misinformation, fake news, and deception. Consequently, the detection of image forgeries has become a critical task in ensuring the integrity and reliability of digital content. Image forgery, also known as digital image manipulation or tampering, refers to the act of altering an image in a deceptive or misleading manner. This can involve various techniques, including but not limited to copy-move, splicing, retouching, and morphing, among others. The motivations behind image forgery can vary widely, ranging from malicious intent, such as spreading false information or defaming individuals, to more benign purposes, such as artistic expression or photo enhancement. Detecting image forgeries is a challenging task due to the increasing sophistication of manipulation techniques and the availability of powerful editing tools and software. Traditional methods for forgery detection often rely on manual inspection or rule-based algorithms, which are limited in their effectiveness and scalability. As a result, there is a growing need for automated and robust techniques capable of identifying forged images accurately and efficiently. In recent years, there has been significant research interest in developing advanced forgery detection techniques, leveraging machine learning and deep learning approaches. These techniques have shown promising results in detecting various types of image manipulations, including those that are difficult to detect with traditional methods. By learning from large datasets of both authentic and manipulated images, machine learning models can effectively discern patterns and anomalies indicative of forgery. This introduction sets the stage for the subsequent discussion in this paper, which will provide an in-depth review of the state-of-the-art techniques and methodologies for image forgery detection. By examining both traditional and modern approaches, we aim to elucidate the advancements, challenges, and future directions in this important field of research. Through a comprehensive understanding of image forgery detection, we can contribute to the development of more effective tools and strategies for combating digital manipulation and preserving the integrity of visual content in the digital age. Ryu et al. [1] employed locality-sensitive hashing (LSH) and rotationally invariant ZM features to detect rotated copy-move areas. Emam et al. [2] used the Polar Complex Exponential Transform (PCET) to extract features from circular image blocks and utilized Approximate Nearest Neighbor (ANN) for circular block matching, identifying potential copy-move regions. Unlike block-based methods, key point-based algorithms extract features from specific points of interest in the image and match these key points to detect suspicious pairs. Outstanding feature extraction algorithms for key point-based approaches include Speeded-Up Robust Feature (SURF) [3] and Scale Invariant Feature Transform (SIFT) [4], [5]. Pan and Lyu 6]

were among the first to use SIFT-based key point matching for copy-move forgery detection, showing strong robustness against geometric transformations. Shivakumar et al. [7] enhanced detection efficiency using SURF and KD-tree for key point matching. Pun et al. [8] combined key point-based and block-based methods by segmenting the image into non-overlapping, irregular blocks, extracting key point features from these blocks, and locating potential tampered areas through block matching. Wang et al. [9] addressed the challenge of extracting key points in homogeneous regions by removing the contrast threshold and increasing image resolution, introducing the bag-of-visual-words model to bridge the semantic gap in copy-move forgery detection. Generally, key point-based methods are more efficient and robust against geometric transformations compared to block-based methods but may struggle in homogeneous regions with few or no key points. Recently, deep CMFD frameworks have gained attention and shown promising results [10]–[11]. Unlike traditional methods, deep CMFD frameworks learn features adaptively from large datasets. Brani et al. [12] focused on source/target discrimination by leveraging interpolation artifacts and boundary forgery traces in the target area, using similarity masks from other detection algorithms. Figure 1 shows a sample image of both authentic image and fake image.

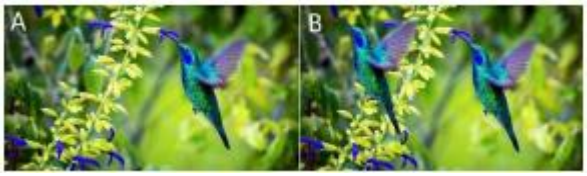

Figure 1. A-Actual mage and B-Forge Image

2. Key Areas of Research Approaches

Image forgery detection is a dynamic and multidisciplinary field that encompasses various techniques and approaches to identify and prevent the manipulation of digital images. Here are some key areas of research in image forgery detection approaches.

1.1 Passive (Blind) Techniques

i) **Pixel-Based Techniques**: Detect inconsistencies at the pixel level, such as double JPEG compression, color filter array (CFA) analysis, and pixel correlation. Error level Analysis is one of the key feature for this technique[13][14].

ii) **Statistical Methods**: Analyze the statistical properties of an image to identify anomalies, such as noise inconsistencies and statistical moment analysis.

iii) **Machine Learning and Deep Learning**: Utilize neural networks and deep learning models to detect forgeries based on training datasets of forged and authentic images.

1.2 Active Techniques

i) **Watermarking**: Embed a digital watermark into the image during creation, which can later be used to verify the image's authenticity.

ii) **Digital Signatures**: Generate a hash of the original image that can be compared to the hash of the suspected image to detect changes.

1.3 Color and Lighting Analysis

i) **Color Filter Array (CFA) Analysis**: Examines the color filter array pattern left by digital cameras. Inconsistencies in CFA patterns can indicate manipulation.

ii) **Illumination Inconsistencies**: Analyzes lighting conditions, shadows, and highlights to detect discrepancies between different parts of the image.

1.4 Edge and Contour Analysis

Edge and contour analysis play a crucial role in image forgery detection, as forgeries often introduce inconsistencies in the edges and contours of objects within the image. Here are some key references and methods related to edge and contour analysis in the context of image forgery detection:

1.5 Frequency Domain Analysis

i) **Discrete Cosine Transform (DCT)**: Transforms the image into the frequency domain. Inconsistencies in DCT coefficients can indicate compression artifacts or tampering [15].

ii) **Wavelet Transform**: Decomposes the image into different frequency components. Analyzing wavelet coefficients can help detect anomalies indicative of forgery [16].

1.6 Spatial Domain Analysis

i) **Pixel Correlation**: Examines the correlation between adjacent pixels. Inconsistencies in pixel correlation patterns can reveal tampered regions.

ii) **Noise Analysis**: Analyzes the noise pattern within the image. Differences in noise levels or distribution can indicate manipulation.

1.7 Statistical Features

i) **Histograms of Oriented Gradients (HOG)**: Captures the distribution of gradient orientations. Differences in HOG features can indicate forgery.

ii) **Statistical Moments**: Measures properties such as mean, variance, skewness, and kurtosis of pixel intensities. Anomalies in these statistical properties can suggest tampering.

1.8 Structural Similarity (SSIM)

SSIM Index: Measures the structural similarity between different parts of the image. Low SSIM values can indicate inconsistencies due to forgery.

1.9 Compression Artifacts

i) **Double JPEG Compression**: Detects artifacts from multiple rounds of JPEG compression, which can indicate tampering.

ii) **Quantization Tables**: Analyzes the quantization tables used in JPEG compression. Differences in tables across the image can suggest manipulation.

1.10 Machine Learning and Deep Learning Features

i) **Convolutional Neural Networks (CNNs)**: Automatically extract features from images and learn patterns indicative of forgery.

ii) **Support Vector Machines (SVM)**: Use extracted features to classify images as authentic or tampered based on learned patterns.

iii) **Feature Fusion**: Combines multiple types of features (e.g., texture, color, edge) to improve detection accuracy using machine learning models.

3. Challenging Task

CNN requires enormous amount of labelled training data. Computationally intensive and requires significant resources for training. It can be vulnerable to adversarial attacks. Recurrent Neural Networks (RNNs) and Long Short-Term Memory Networks (LSTMs) suffers from more complex to train compared to CNNs. May not be as effective for static image forgery detection compared to video analysis. In Generative Adversarial Networks (GANs) training is challenging and requires careful tuning.

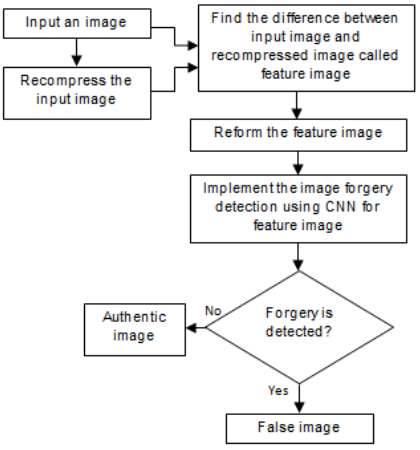

Figure 2. A-Actual mage and B-Forge Image

These techniques have risk of generating highly realistic forgeries that might fool the detection models [11]. Better detection of image forgery need higher resolution images sometimes it can make detection harder as the changes might be more subtle. During compression based forgery detection compression can mask forgery traces, making it are difficult to distinguish between natural artifacts and forgeries [26]. Natural noise and image distortions can complicate the detection process. Sometimes algorithms may incorrectly flag genuine images as forgeries or fail to detect actual forgeries. Algorithms trained on specific datasets may not perform well on unseen data or different types of forgeries [29]. The absence of comprehensive and standardized datasets may cause improper training and testing detection methods.

In traditional machine learning like SVM, Random Forest has generally less accurate compared to deep learning approaches. In this approach limited ability to handle high-dimensional data and complex forgeries [23]. Hybrid approaches more complex to implement and optimize. It requires more computational resources and training data. Handcrafted Feature-Based methods are limited in handling diverse and complex forgeries. It requires domain expertise to design effective features. Metadata and file structure analysis is limited by the availability and accuracy of metadata. It can be easily bypassed by sophisticated forgers who can manipulate metadata. State-of-the-art image forgery detection methods continue to evolve, with on-going research aimed at improving accuracy, robustness, and efficiency. Combining multiple techniques and leveraging advances in deep learning and artificial intelligence is a common trend to address the increasing sophistication of image forgeries. Figure 2 shows flow chart for error level analysis (ELA)[31] based image forgery detection method.

4. Performance Matrices for Comparison

i) **Accuracy**: Measures the overall correctness of the detection method.

ii) **Precision**: Indicates the quantity of true positive detections among all positive detections.

iii) **Recall (Sensitivity)**: Measures the proportion of true positive detections among all actual positives.

iv) **F1 Score**: Harmonic mean of precision and recall, providing a balanced measure.

v) **False Positive Rate**: Indicates the proportion of incorrect positive detections.

vi) **False Negative Rate**: Indicates the proportion of missed forgeries.

vii) **Robustness**: Ability to detect forgeries under various conditions and against adversarial attacks.

viii) **Computational Efficiency**: Resources and time required for training and detection.

5. Comparison Statistics, Datasets and Tools

Figure 3 shows the sample GUI of the Image Forgery System. GUI shows the original image and its Error Level Analysis image. While pressing the Test button it shows whether the image is Authentic or Forged. The Image Forgery Detection System GUI is designed to provide a seamless and intuitive experience for users seeking to verify the authenticity of images. Upon launching the application, users are greeted with a clean and organized interface that prominently features two main display areas. On the left side of the GUI, the original image selected by the user is showcased. This allows users to clearly see the image they are analyzing, ensuring they are working with the correct file. The right side of the GUI is dedicated to displaying the Error Level Analysis (ELA)[31] image. This technique works by saving the original image at a lower quality and then comparing it to the original to highlight discrepancies. These discrepancies can indicate areas that may have been digitally altered. The side-by-side display of the original and ELA images enables users to visually inspect and compare both images easily, identifying potential forgery signs at a glance.

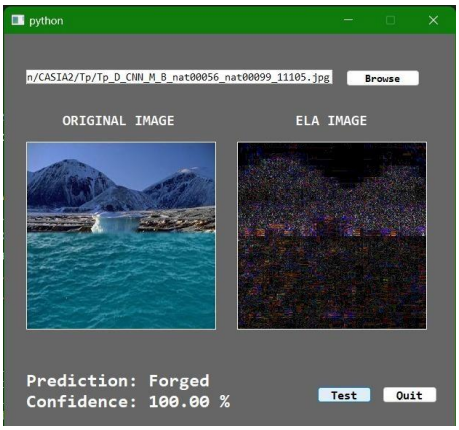

Figure 3. GUI of image forging technique

Table 1. State of art approaches-2

Methods	Precision	Recall	F1 Score
PM [17]	0.830	0.790	0.801
Iteration[18]	0.550	0.653	0.583
HFPM[19]	0.853	0.720	0.764
CMI[20]	0.798	0.885	0.803
SSG[9]	0.844	0.814	0.822
Buster Net[21]	0.330	0.420	0.336
DOA-GAN[11]	0.530	0.340	0.364
Serial Net[10]	0.412	0.392	0.369

Methods	Da1aset(s)	Evalua1ion metrics	Results
SURF, DCT[30]	Modified CASIA	FRR, TDR	1.5%, 95.42%
DCT[23]	CoMoFoD	FN,FP precision and re-precision=63.52% call	precision =63.52% call recall=97 .89
SURF and FAST[24]	MICC-F220 MICC-F2000 MICC-f8mult	TPR, FPR and execution time	97.4%, 8.6% and 9.2 sec
LBPRC and CR[25]	CMH and CoMo FoD_small _v2	TPR FPR	MICC-220(TPR =99.09% FPR=9.09)
CNN[26]	handmade, OXFORD and UCID	Error rate	2.32%, 2.43% and 42%
DCT, LBP and SVM[27]	CASIA and Columbia	Accuracy	97%
In.mom.[28]	CASIA	accuracy	99.5%, 87.5%
Branch-and-bound[29]	handmade	accuracy	99.5%

Table 2. State of art approaches-2

Table 1 and Table 2 illustrate state of art approaches in terms of accuracy and precision values. Recent methods in image forgery detection have significantly advanced, driven by deep learning, hybrid approaches, and improved feature-based techniques. These methods have become more sophisticated in detecting subtle and complex forgeries, but challenges such as robustness to adversarial attacks, computational efficiency, and the need for diverse datasets remain. Continued research and development in these areas are essential to keep pace with evolving forgery techniques. Most of the researchers used CASIA TIDEv2: It is a widely-used dataset for evaluating image tampering detection algorithms. Similarly copy-move forgery detection dataset (CoMoFoD) and IEEE Forensic Image Dataset also have been used by many authors during their research. Some of the tools have been used for image forgery detection like forensically**.** It is a suite of tools for image forensics. Amped Authenticate is another tool used in Professional software for image authentication. JPEGSnoop is recently added tool is a free tool for forensic analysis of JPEG files. It contains various types of image forgeries for research.

6. Conclusion and Future Scope

The on-going battle between image forgery techniques and detection methods is a dynamic and rapidly evolving field. To keep pace with advancing forgery methods, researchers must continue to innovate and refine detection techniques. This involves developing more sophisticated deep learning models, creating comprehensive datasets, and establishing standardized evaluation frameworks. Collaboration among researchers, law enforcement, and ethical oversight bodies is crucial to ensure that the advancements in image forgery detection are effectively and responsibly implemented. The ultimate goal is to create robust, reliable, and ethical detection systems that can safeguard the integrity of digital images in an increasingly digital world. This paper would help the research scholars to select different key areas of image forgery detection. Challenges are one of the most prominent considerable key points while solving the detection problems of image forgery.

Author Contributions

Author 1 involved for framing the state of art approaches and wrote the draft of the paper. Author 2 framed the key areas of research and challenges in image forgery detection.

Acknowledgements

First Author thanks the SDM Institute of Technology research center for providing required resources and given an opportunity to download reputed journal papers. This work was supported by Dr. G.P. Hegde, Professor and Head of information Science and Engineering research center. I thank for his encouragement and motivation to do this paper work.

References

[1]. S.-J. Ryu, M. Kirchner, M.-J. Lee, and H.-K. Lee, “Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments,” IEEE Trans. Inf. Foren. Secur., vol. 8, no. 8, pp. 1355–1370, 2013.

[2]. M. Emam, Q. Han, and X. Niu, “PCET based copy-move forgery detection in images under geometric transforms,” Multimedia Tools Appl., vol. 75, no. 18, pp. 11 513–11 527, 2016.

[3]. V. T. Manu and B. M. Mehtre, “Detection of Copy-Move Forgery in Images Using Segmentation and SURF,” in Adv. Neural Inf. Process. Syst., pp. 645–654, 2016

[4]. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A SIFT-based forensic method for copy–move attack detection and transformation recovery,” IEEE Trans. Inf. Foren. Secur., vol. 6, no. 3, pp. 1099–1110, 2011.

[5]. Y. Li and J. Zhou, “Fast and effective image copy-move forgery detection via hierarchical feature point matching,” IEEE Trans. Inf. Forensic. Security., vol. 14, no. 5, pp. 1307–1322, 2019.

[6]. X. Pan and S. Lyu, “Region duplication detection using image feature matching,” IEEE Trans. Inf. Foren. Secur., vol. 5, no. 4, pp. 857–867, 2010.

[7]. B. Shivakumar and S. S. Baboo, “Detection of region duplication forgery in digital images using surf,” International Journal of Computer Science Issues (IJCSI), vol. 8, no. 4, p. 199, 2011.

[8]. C.-M. Pun, X.-C. Yuan, and X.-L. Bi, “Image forgery detection using adaptive over segmentation and feature point matching,” IEEE Trans. Inf. Foren. Secur., vol. 10, no. 8, pp. 1705–1716, 2015.

[9]. C. Wang, Z. Huang, S. Qi, Y. Yu, G. Shen, and Y. Zhang, “Shrinking the semantic gap: Spatial pooling of local moment invariants for copy move forgery detection,” IEEE Trans. Inf. Foren. Secur., vol. 18, pp. 1064–1079, 2023.

[10]. B. Chen, W. Tan, G. Coatrieux, Y. Zheng, and Y. Q. Shi, “A serial image copy-move forgery localization scheme with source/target distinguish ment,” IEEE Trans. Multimedia, vol. 23, pp. 3506–3517, 2021.

[11]. A. Islam, C. Long, A. Basharat, and A. Hoogs, “DOA-GAN: Dual-order attentive generative adversarial network for image copy-move forgery detection and localization,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2020, pp. 4675–4684.

[12]. M. Barni, Q.-T. Phan, and B. Tondi, “Copy move source-target disam biguation through multi-branch CNNs,” IEEE Trans. Inf. Foren. Secur., vol. 16, pp. 1825–1840, 2021.

[13]. Ansari Mohd, Dilshad Satya, Prakash. Ghrera and Vipin. Tyagi, "Pixel-based image forgery detection: A review", *IETE journal of education*, vol. 55, no. 1, pp. 41-46, 2014.

[14]. P.-P. Niu, C. Wang, W. Chen, H. Yang, and X. Wang, “Fast and effective key point-based image copy-move forgery detection using complex valued moment invariants,” J. Vis. Communication. Image Representation., vol. 77, p. 103068, 2021

[15]. J. Zhong, Y. Gan, and S. Xie, “Radon odd radial harmonic Fourier moments in detecting cloned forgery image,” Chaos, Solitons Fractals., vol. 89, pp. 115–129, 2016.

[16]. Zear, A. K. Singh, and P. Kumar, ‘‘A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine,’’ Multimedia Tools Appl, vol. 77, no. 4, pp. 4863–4882, Feb. 2018

[17]. D. Cozzolino, G. Poggi, and L. Verdoliva, “Efficient dense-field copy–move forgery detection,” IEEE Trans. Inf. Foren. Secur., vol. 10, no. 11, pp. 2284–2297, 2015

[18]. M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, “Iterative copymove forgery detection based on a new interest point detector,” IEEE Trans. Inf. Foren. Secur., vol. 11, no. 11, pp. 2499–2512, 2016

[19]. Y. Li and J. Zhou, “Fast and effective image copy-move forgery detection via hierarchical feature point matching,” IEEE Trans. Inf. Forensics. Security. vol. 14, no. 5, pp. 1307–1322, 2019.

[20]. P.-P. Niu, C. Wang, W. Chen, H. Yang, and X. Wang, “Fast and effective keypoint-based image copy-move forgery detection using complexvalued moment invariants,” J. Vis. Commun. Image Represen., vol. 77, p. 103068, 2021

[21]. Y. Wu, W. Abd-Almageed, and P. Natarajan, “BusterNet: Detecting copy-move image forgery with source/target localization,” in Proc. Eur. Conf. Comput. Vis.,vol. 11210, pp. 170–186, 2018

[22]. Ustubıoglu, V. Nabıyev, G. Ulutas, and M. Ulutas, “Image forgery detection using colour moments”, in 2015 38th International Conference on Telecommunications and Signal Processing (TSP). IEEE, pp. 540–544, 2015.

[23]. X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, “Image copy-move forgery detection based on surf,” in 2010 International Conference on Multimedia Information Networking and Security. IEEE, 2010, pp. 889–892.

[24]. B. Soni, P. K. Das, and D. M. Thounaojam, “Improved block-based technique using surf and fast key points matching for copy-move attack detection,” in 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN). IEEE, pp. 197–202, 2018.

[25]. T. Zhu, J. Zheng, Y. Lai, and Y. Liu, “Image blind detection based on lbp residue classes and color regions,” PloS one, vol. 14, no. 8, 2019.

[26]. J. Ouyang, Y. Liu, and M. Liao, “Copy-move forgery detection based on deep learning,” in 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISPBMEI). IEEE, pp. 1–5, 2017.

[27]. A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on dct and local binary pattern," in 2013 IEEE Global Conference on Signal and Information Processing. IEEE, pp. 253–256, 2013.
[28]. C. S. Prakash, A. Kumar, S. Maheshkar, and V. Maheshkar, "An integrated method of copy-move and splicing for image forgery detection," Multimedia Tools and Applications, vol. 77, no. 20, pp. 26 939–26 963, 2018.
[29]. J. Van Beusekom, F. Shafait, and T. M. Breuel, "Text-line examination for document forgery detection," International Journal on Document Analysis and Recognition (IJDAR), vol. 16, no. 2, pp. 189–207, 2013.
[30]. Y. Zheng, Y. Cao, and C.-H. Chang, "A puf-based data-device hash for tampered image detection and source camera identification," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 620– 634, 2019.
[31]. Azhan, N. A. N., Ikuesan, R. A., Razak, S. A., & Kebande, V. R., " Error Level Analysis Technique for Identifying JPEG Block Unique Signature for Digital Forensic Analysis", Electronics, issue 11, vol-9, pp. 1468, 2022.
[32]. Alberry, H. A., Hegazy, A. A., & Salama, G. I, "A fast SIFT based method for copy move forgery detection. Future Computing and Informatics Journal", issue 3, vol 2, pp 159-165, 2018.

Author-1 Earned her B.E in Computer Science and Engineering from MIT ,Manipal in 2004. M.Tech in Computer Science and Engineering from SDM, Dharwad in 2016. She is currently working as a Sr. Assistant Professor in Department of Computer Science and Engineering in Alva's Institute of Engineering and Technology since 2021. She has 15 years of teaching experience. Her main research work focuses on image tamper detection using new approaches. She has published more than 10 review papers of project guided to undergraduate students in reputed international journals. She has been a coordinator of cyber security finishing school-2024 organized by CYSECK (Cyber Security Karnataka ,Govt) and conducted 35 days cyber security training for selected 35 BE final year students .

Author-2 He has obtained BE from Karnataka University Dharwad in 1994. He has completed MTech in Computer Science & Engineering from VTU, Belagavi during 2009. He has obtained PhD degree in Computer Science & Engineering from VT University, Belagavi during 2018. He is currently working as Professor in Department of Information Science & Engineering, SDM Institute of Technology, Ujire. Mangalore, India. He is a life member of ISTE since from 1996. He has published more than 36 research articles in various reputed International Journals and conferences including IEEE and it's also available online. His main research work focuses on Image Processing, Data Mining, Internet of Things, He has 15 years of teaching experience and 10 years of research experience.