ANALYSIS ON SPLICING AND DEEPFAKES IN VISUAL FORGERY AND IMAGE FRAUD

Nikhat Fatima[1], Dr. Sameena Banu[2]

[1&2]Assistant professor, CSE Dep of Faculty of Engineering and Technology, Khaja Bandanawaz University.

ABSTRACT

Image forgery has become increasingly sophisticated, with deepfakes and GAN-generated images causing people to be more skeptical of visual evidence. This has a significant impact on politics, healthcare, terrorism, social media, and the legal system. As GANs and deepfake technologies evolve, the line between "real" and "fake" becomes blurrier, leading to new ethical, legal, and technical challenges. Society must balance the benefits of these technologies with the need for regulations and detection systems to combat their misuse. Splicing is the process of cutting and pasting parts of an image or video from one source to create an authentic composite, while deepfakes are synthetic media created using Generative Adversarial Networks (GANs) or Autoencoders. These forgeries generate new, realistic content, rather than copying and pasting it. Detecting these forgeries requires advanced deep learning models like CNNs, RNNs, LSTMs, and Transformers. Combating splicing and deepfakes is crucial in forensics, media verification, and financial fraud prevention. This paper reviews research work on visual media alteration to prevent frauds using deep learning methods, highlighting the importance of thorough knowledge of state-of-the-art approaches for detection.

Keywords: *Image Forgery, Deepfakes, CNN and GAN.*

1. INTRODUCTION

Image forgery, the process of altering or fabricating digital images to mislead or deceive viewers, has become a global issue due to the exponential growth of user-friendly image editing tools, advanced deep learning algorithms like Generative Adversarial Networks (GANs), and the rise of social media platforms. These forgeries have profound societal implications, affecting key sectors like politics, healthcare, media, law enforcement, and personal privacy. The ability to create, manipulate, and disseminate highly realistic fake images at scale poses significant risks to public trust, national security, and the credibility of information shared on social media. Fake images have become a powerful weapon for political manipulation, often used to shape public opinion, discredit opponents, or fuel propaganda. In elections, forged images are circulated on social media to mislead or sway voters. Infiltrated the healthcare sector, hackers and fraudsters use image manipulation techniques to alter diagnostic medical scans, such as CT scans, X-rays, and MRIs, leading to incorrect diagnoses and financial fraud. Terrorist organizations and extremist groups have embraced image forgery as a propaganda tool to spread their ideology and recruit supporters. Social media platforms like Instagram, Facebook, TikTok, and Reddit thrive on visual content, but they also serve as breeding grounds for fake images, memes with misinformation, and altered images used to push certain narratives.

The advent of advanced image-editing software in the 21st century has drastically affected the time, cost, and efforts required to tamper with images. Developing convincing, realistic fake images has become considerably easier than in the past due to the prevalence of user-friendly image editing softwares and advances in Deep Learning technologies like Generative Adversarial Networks (GAN). There is an urgent need for efficacious Forgery Detection techniques, which require standard datasets and custom datasets. This research work presents the development of a Multiple Image Splicing Dataset used to detect multiple image splicing forgery, which includes both authentic and multiple spliced images. The widespread use of smart devices, including cameras, image processing tools, and apps, has enabled the collection, storage, and processing of vast amounts of digital visual data. This has led to the widespread sharing of images and videos as information sources in various contexts. Digital technologies such as compression methods, fast networks, and user applications have enabled massive sharing of visual content, including web platforms like Instagram and forums like Reddit. Advanced image editing software, such as Adobe Photoshop and GIMP, and smartphone-based apps, are widely available to everyone. However, these factors have contributed to the spread of fake or forged images and videos, where semantic content is significantly altered. This can be done for malevolent purposes, such as political or commercial ones. As of 2022, major social network platforms are struggling to filter manipulated data to prevent fake content from going viral. Legal issues are also emerging regarding where to place responsibility for the potentially damaging fallout of fake content spreading. Humans are often easily fooled by forgeries, and in some cases, they are not able to detect any modifications undergone by visual content due to the change blindness cognitive effect. Therefore, carefully designed digital techniques are needed to detect forgery on still images. Image authentication, or image integrity verification, is the general problem of determining if an image has not been altered to modify its semantics. Image forgery detection is often referred to as image authentication or image integrity verification. This paper provides a comprehensive, performance-driven survey of selected forgery detection methods, with particular attention to deep learning (DL) techniques that have since come to the fore. It provides a broad overview of the considered application, a concise summary of the most commonly found types of forgery, and organization of the remainder of the paper while detailing the contributions of our present analysis.

2. IMAGE FORGERY DETECTION APPLICATIONS

Image forgery detection can be divided into active and passive methods, with active methods focusing on visual content protection and passive methods analyzing the image itself. Active methods are based on technologies like digital signatures and digital watermarking, which are cryptographic methods that authenticate the bit-stream. However, these methods are fragile and vulnerable to changes in the bit-stream, making them suitable for copyright protection but not for verifying image semantic content. To address these shortcomings, robust methods have been proposed, such as robust digital watermarking, which embeds security information in the content by controlled imperceptible modifications. This allows an attacker to alter the content of an image without changing the embedded watermark, while safely applying selected processing such as compression, allowing the consumer to detect the manipulation. Variants of these approaches exist, such as robust signatures and fragile watermarking, which sometimes combine but still inherit issues associated with metadata presence and fragility. Active methods have the advantage of conveying side information useful for detecting attempted forgery, but they require the watermark or signature to be computed on the unaltered version of the image, ideally at the acquisition level. This requires specific hardware and/or in-board post-processing software, and any entity interested in verifying the semantic content must be able to decode the authentication information, which means having access to the key of the creator and/or the watermark detector. A trusted third party could be set up to verify the image integrity, but scalability problems prevent this architecture from being feasible for everyday images shared on the Internet. Recently, commercial solutions based on the blockchain paradigm have appeared to remove the trusted third-party presence, but these techniques are not widespread for forgery detection. Passive methods, known as forensics, do not need additional data attached to the image and aim to tell whether an image is authentic by analyzing only the image itself. An attacker can apply one or a set of successive manipulations on the target image, either on the whole image or only on a tampered region, resulting in anti-forensics when used to disguise the original forgery.

3. CONVENTIONAL PASSIVE IMAGE FORGERY DETECTION METHODS

Image forgery detection is a critical field of research aimed at identifying manipulated images. Over the years, several passive detection methods have been proposed, with early approaches relying on traditional techniques from signal processing, statistics, physics, and geometry. These "classic" methods form the foundation for modern deep learning-based approaches and continue to offer certain advantages in specific scenarios.

For the purpose of misleading, deceiving, or changing the perception of the picture's legitimacy, deliberate manipulation of visual content is referred to as image forging. The complexity and difficulty of detecting forgeries have increased with the development of image manipulation tools and deep learning approaches. With their own unique characteristics, techniques, and outcomes, the four basic types of forgeries copy-move, splicing, inpainting, and DeepFakes are easily identifiable. These days, it's harder to spot an image forgery since modern techniques are so sophisticated. There are distinct methods and outcomes associated with the four main types of forgeries: copy-move, splicing, inpainting, and DeepFakes. Some forgeries, like copy-move and inpainting, alter content inside a single image, while others, like splicing and DeepFakes, use deep learning to create new content or include elements from other photographs. Worryingly, DeepFakes deploy complex AI models to create hyper-realistic media, which might be used for malicious purposes or in disinformation campaigns. When it comes to digital forensics and photo authentication, these forgeries are huge roadblocks. While older processes relied on human review, modern detection approaches use deep learning technologies like pattern recognition algorithms and convolutional neural networks (CNNs) to identify signs of fraud. Researchers are always developing more accurate models to distinguish between real and fake photographs, and detection technologies are advancing in tandem with image alteration techniques. In order to combat misinformation, protect privacy, and maintain faith in visual media, it is crucial to detect and mitigate these manipulations.

Traditional methods, which emerged in the pre-deep learning era, typically do not require large datasets for training. Instead, they rely on simpler machine learning models or handcrafted feature extraction techniques. These methods are computationally lightweight and can be deployed on low-power devices like smartphones and tablets.

1. Copy-Move Forgery

Copy-move forgery is a widely used method for picture manipulation. It entails duplicating a section of a picture and repositioning it inside the same image. This technique is often used to conceal or replicate items, therefore modifying the image's semantic value. An item may be obscured by replicating a visually like region, such as duplicating a segment of the sky to hide an undesirable element. An instance example is the duplication of a tower, when one tower is replicated to produce a second similar construction. Copy-move assaults are notably difficult to detect since the replicated area maintains identical colour, texture, and lighting to the original, complicating the identification of visual discrepancies.

2. Splicing Forgery

Splicing is an advanced method of picture editing that involves removing parts of one image and pasting them into another. Spliced areas don't come from inside the same image like copy-move fraud does; they come from outside the image. Photographers often use this method to make false stories about people by showing them in places or settings they didn't exist in. For example, splicing could involve putting together pictures of two famous people to make a meeting that never happened. When compared to copy-move, cutting makes it harder to mix the lighting, shadows, and colour tones of the different parts of the image so that the finished picture looks natural and smooth.

3. Inpainting Forgery

As a restoration-based editing technique, inpainting involves substituting visually plausible material for damaged or missing areas of an image. Even though inpainting is often used for legitimate image modification and restoration, it may also be utilised maliciously by attackers. Watermarks, logos, and other identifying features may be delicately removed from images using inpainting. The missing regions are either generated by algorithms like Generative Adversarial Networks (GANs) or filled with material from other parts of the image (similar to copy-move). Face reconstruction is a subfield of deep learning that makes use of inpainting to restore missing or obscured facial characteristics. Successful inpainting procedures have been developed by Nvidia, leading to high-quality face restorations. When using GANs to generate very realistic content, inpainting blends in seamlessly with the surrounding image, making it difficult to detect.

4. DeepFake Forgery

DeepFake frauds use deep learning models to make fake content that looks very much like the real thing. This makes them a very modern and advanced way to change pictures and videos. The word "DeepFake" draws attention to the way Generative Adversarial Networks (GANs), a type of deep learning, are used to automate editing tasks that used to be done by hand. Along with more common types of picture editing, DeepFakes often goes after video material.

The most well-known DeepFake way is swapping out someone's face for someone else's. To do this, we first use huge sets of face pictures to build a model that can figure out the "source" face's main features and feelings. Then, we put this model on top of the "target" face in the movie. You won't be able to tell it's not real film because the fake face might move to the music and look like it's feeling something. Although DeepFakes have been used in comedic and spoof situations, they could also be hacked to make fake films about famous people getting into trouble. While most DeepFakes are after movies, there are some that are after pictures as well. These changes are a type of editing, which is the process of putting together or changing out face features from different pictures. Since DeepFakes are now easier for non-experts to make with tools like FakeApp and faceswap-GAN, as well as open-source platforms, there are moral concerns about privacy, misrepresentation, and slander.

Table 1: Tools and technologies for forgery detection

Category	**Tools/Technology**	**Features**
Commercial Tools	Adobe Photoshop, Affinity Photo	Splicing, blending, object removal, color enhancement
Open Source Tools	GIMP, Darktable, RawTherapee	Free alternatives for splicing, color adjustments, object removal
Mobile Apps	FaceApp, Snapseed, PicsArt	Face swapping, retouching, filters, background removal
AI-Based Tools	DeepFaceLab, ThisPersonDoesNotExist	AI-based deepfakes, image synthesis, and GAN-generated faces

4. Computer-Generated Imagery (CGI) and Motion, and Face Synthesis Using GANs

The advent of advanced graphics processing technologies and deep learning techniques has revolutionized the creation of computer-generated images (CGI) and synthetic faces. These developments have profound implications for the entertainment industry, visual effects, gaming, and, more recently, the generation of realistic but fake images and videos that can be used for both creative and malicious purposes.

Computer-Generated Imagery (CGI) and Motion

Computer-Generated Imagery (CGI) refers to the creation of images, animations, and visual effects using computer software. This process involves the generation of 3D models, textures, lighting, and physics simulations to create scenes that are often indistinguishable from real-world images. The production of photorealistic CGI has been made significantly easier and more accessible due to advances in **graphics processing units (GPUs)**, **ray tracing**, and **real-time rendering engines**.

Technological Advances

- **Ray Tracing**: Ray tracing simulates the way light interacts with objects in a scene, including shadows, reflections, and refractions, creating highly realistic lighting effects. This technology, previously limited to high-end visual effects studios due to its computational demands, has become widely available due to modern GPUs. NVIDIA and AMD have introduced hardware-level support for ray tracing, enabling it to run in real time for video games and interactive media.

- **Game Engines**: Platforms like **Unity** and **Unreal Engine** have democratized CGI production. Both engines offer robust tools for creating lifelike graphics, real-time physics, and motion capture integration. They are widely used in video game development, film production, architectural visualization, and virtual reality (VR) experiences. The fact that these engines are free or inexpensive to use means that more people, from hobbyists to professional creators, now have the tools to produce photorealistic images and videos.
- **AI-Assisted CGI**: Modern software incorporates machine learning (ML) and artificial intelligence (AI) to automate labor-intensive processes like motion capture, texture synthesis, and character rigging. For example, AI can automatically fill in gaps in motion-capture data or generate animations for characters, reducing production time and effort.

Potential Risks and Challenges

As CGI technology has become more accessible, the risk of malicious use has increased.

Misuse in Deception: The ability to produce photorealistic images indistinguishable from real-world photographs opens the door to creating false evidence or fake scenarios. Since the entire scene is built from scratch, there is no "source" image to reference, unlike splicing-based forgeries. This makes it difficult for traditional image forensics to detect manipulation, as there are no telltale signs of blending or misaligned textures.

Skill Requirements: While user-friendly software has made it easier to create realistic imagery, achieving truly lifelike CGI still requires a certain degree of skill. Mastery of lighting, physics, and texture design is essential to produce scenes that are visually indistinguishable from real-world photos. However, as AI-based automation tools continue to improve, this skill gap is rapidly shrinking.

Face Synthesis Using Generative Adversarial Networks (GANs)

The combination of computer-generated imagery (CGI) and Generative Adversarial Networks (GANs) has transformed the production of synthetic images and faces. CGI, powered by tools like Unreal Engine and Unity, creates entire 3D environments, while StyleGAN models can generate high-resolution human faces. These technologies are widely used in entertainment, advertising, and AI development but have also raised concerns about privacy, forgery, and the spread of disinformation.

CGI builds entire visual scenes from the ground up, making it challenging for forensic analysts to detect manipulation since no "original" image exists for comparison. GAN-generated faces are unique because they do not exist in the real world, making them particularly challenging to trace. Both technologies have clear creative benefits, but their potential misuse poses new challenges for digital forensics, content verification, and media trust.

With increasing accessibility to these tools, researchers and organizations must continue to develop robust methods for detecting synthetic content. As GANs evolve to produce more lifelike images and CGI engines become more accessible, it will be essential to create AI-based countermeasures that can identify and verify the authenticity of media content.

Face synthesis is one of the most impactful applications of **Generative Adversarial Networks (GANs)**, a type of deep learning model that generates new data samples from random noise. GANs have achieved extraordinary success in creating realistic human faces that never existed. Unlike CGI, which requires manual effort to design and render each feature, GANs automate the generation process, producing faces that look authentic with minimal human intervention.

5. Motivation

Rise of Image Forgeries: The advent of user-friendly editing tools (e.g., Photoshop, GIMP, Figma) and advances in GANs have made image forgeries more accessible, realistic, and difficult to detect. The rise of image forgeries is a direct consequence of the convergence of technological advancements, the democratization of editing tools, and the proliferation of image-sharing platforms. As visual content becomes a central medium for communication, forgeries have grown more frequent, sophisticated, and impactful. This section explores the key drivers, types, tools, and societal implications of image forgeries. Platforms like Instagram, Facebook, and TikTok are built around visual content, encouraging users to edit and enhance images for aesthetic appeal. Similarly, encrypted messaging apps like WhatsApp allow for easy and untraceable sharing of fake images.

- **Impact on Society:** Fake images have been used in political manipulation (like the Brazilian election), healthcare fraud (tampering with medical scans), and terrorist propaganda. Social networks struggle to filter such content, leading to misinformation and legal dilemmas.
- **Need for Detection Techniques:** Human perception alone is insufficient to detect subtle forgeries due to "change blindness." As a result, automated systems for image integrity verification and forgery detection are essential.

6. The Role of Deep Learning in Forgery Detection and Datasets

counter the rise of image forgeries, researchers have focused on deep learning-based detection methods. Advanced models, like Convolutional Neural Networks (CNNs) and attention-based models, are now widely used for forgery detection. With the rise of deep learning, modern approaches to image forgery detection have shifted from manual feature extraction to **automated feature learning**. **Convolutional Neural Networks (CNNs)** have been the most influential, offering state-of-the-art performance in classification, regression, and segmentation tasks.

The field of passive image forgery detection has evolved from simple statistical methods to sophisticated deep learning techniques. Traditional methods remain useful for lightweight, on-device detection, while deep learning models dominate in performance, particularly in complex scenarios like DeepFake detection. Future research will likely focus on **generalizable, explainable, and hybrid models** that combine the strengths of traditional and deep learning methods.

- CNNs for Feature Extraction: CNNs automatically learn and extract local features, such as edges, textures, and lighting inconsistencies, that reveal signs of tampering.
- Autoencoders: Autoencoders reconstruct images from compressed latent representations. Discrepancies between the input and output images may highlight forgery areas.
- Deep Learning Pipelines: Hybrid models combine CNNs with RNNs, attention mechanisms, or Transformers to achieve better spatial and temporal analysis.
- GANs for Detection: Although GANs create forgeries, they can also be used for detection. By training "forgery detectors" against GAN-generated forgeries, detection models become more robust.

Deep learning models for forgery detection rely heavily on benchmark datasets for training, testing, and validation. These datasets cover **copy-move**, **splicing**, and **DeepFake** detection tasks.

CASIA1 is among the first datasets used for splicing and copy-move detection. The fabricated photos are produced by altering components of the source photographs. This dataset is appropriate for preliminary research on picture forgery detection owing to its modest size and simple changes.

CASIA2 is a more comprehensive iteration of CASIA1. The tampering procedure involves border post-processing, hence complicating the detection of forgeries. The photographs exhibit diverse sizes and formats (JPEG, BMP, TIFF), complicating machine learning algorithms. CASIA2 is extensively used to evaluate methods for detecting copy-move and splicing forgeries.

DVMM This collection is smaller than CASIA however distinctive in its use of uncompressed greyscale photos. The reduced resolution (128x128) and monochromatic characteristics make it suitable for evaluating deep learning models under limited situations, especially inside greyscale settings.

MICC-F220 This dataset was specifically designed for the detection of copy-move forgeries. The forgeries include manipulations like as rotation, scaling, and noise augmentation. This makes it advantageous for training models that are resilient to forgeries generated by transformations.

MICC-F600 enhances MICC-F220 by including numerous copy-move areas inside a single picture. The altered areas are also modified by rotation and scale. This dataset is essential for training algorithms that generalise to intricate and large-scale copy-move frauds.

MICC-F2000 MICC-F2000, the most extensive of the MICC datasets, provides high-resolution pictures, making it suitable for models requiring forgery detection in huge, high-quality photos. Enhanced resolution and increased dataset quantity enable improved model generalisation.

The SATs-130 dataset is modest in size and comprises photos sourced from 10 original photographs. Copy-move forgeries include JPEG compression at many levels, making them beneficial for the development of models capable of addressing lossy compression artefacts.

The CMFD dataset focusses on segments of pictures where copy-move forgeries have been executed. The authors furthermore provide a software tool for the creation of supplementary forgeries. This dataset facilitates the evaluation of models for region-based copy-move forgery detection.

CoMoFoD is among the most extensive datasets for detecting copy-move forgeries. It contributes considerable complexity via post-processing techniques like as compression, noise reduction, blurring, and adjustments to brightness and contrast. Models trained on CoMoFoD demonstrate superior generalisation in practical environments.

DFDC is a leading dataset for DeepFake detection, including films of different quality and featuring 66 individuals from various ethnic backgrounds. It serves as a crucial standard for training algorithms that identify facial modification.

FaceForensics++ is an augmentation of the original FaceForensics dataset. It comprises DeepFakes produced by four sophisticated techniques: DeepFakes, Face2Face, FaceSwap, and NeuralTexture. The extensive size and diverse ways of fake production render it essential for training resilient DeepFake detection models.

The datasets mentioned are crucial for creating effective forgery detection systems. Each dataset confronts distinct obstacles in copy-move, splicing, and DeepFake forgeries, offering a range of picture formats, resolutions, and attack methodologies.

Table 2: forgery methods and datasets

Copy-Move Datasets:	CASIA, MICC, CMFD, CoMoFoD
Splicing Datasets:	CASIA, DS0-1, Korus, DVMM
DeepFake Datasets:	DFDC, FaceForensics++, Celeb-DF

Models trained on multiple datasets exhibit better generalization in real-world conditions. For copy-move and splicing, datasets like CoMoFoD and Korus offer realistic and large-scale benchmarks. For DeepFake detection, datasets like DFDC, Celeb-DF, and FaceForensics++ are vital due to their size, diversity, and visual quality.

CONCLUSION

The proliferation of picture forgeries is a significant issue for contemporary culture. Progress in artificial intelligence, intuitive tools, and superior technologies have facilitated forgeries to an unprecedented degree. The proliferation of altered photographs presents difficulties in politics, security, healthcare, and social media. Although deep learning models provide promise for effective forgery detection, the struggle continues. Researchers, governments, and social media platforms must persist in advancing and enhancing detection technologies to safeguard the integrity of visual material. The proliferation of picture forgeries is driven by the amalgamation of AI technology, social media, and accessible editing tools. These forgeries have extensive repercussions, including political influence, medical fraud, and cybersecurity threats. As GANs and deepfakes advance in complexity, the distinction between authentic and fabricated images is more difficult to discern.

Advanced deep learning models, including as CNNs, Transformers, and autoencoders, are at the forefront of combating forgeries; yet, the struggle persists. In the future, more comprehensive, multi-modal strategies that include metadata analysis, picture content analysis, and blockchain verification systems may be necessary to effectively address this danger.

REFERENCES

1. Andreas Rössler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies, and Matthias Nießner. Faceforensics++: Learning to detect manipulated facial images
2. Birajdar GK, Mankar VH (2013) Digital image forgery detec
3. tion using passive techniques: a survey. Digit Investig 10(3):226–245.
4. Elaskily M, Elnemr H, Sedik A, Dessouky M, El Banby G, Elaskily O, Khalaf AAM, Aslan H, Faragallah O, El-Samie FA (2020) A novel deep learning framework for copy-move forgery detection in images. Multimed Tools Appl 79.
5. Kadam, K.; Ahirrao, D.; Kotecha, D.; Sahu, S. Detection and Localization of Multiple Image Splicing Using MobileNet V1. *arXiv* **2021**, arXiv:2108.09674.
6. Nath, S.; Naskar, R. Automated image splicing detection using deep CNN-learned features and ANN-based classifier. *Signal Image Video Process.* **2021**, *15*, 1601–1608.
7. Ouyang J, Liu Y, Liao M (2017) Copy-move forgery detection based on deep learning. In: 2017 10th international congress on image and signal processing, BioMedical engineering and informatics (CISP-BMEI), pp 1–5.
8. Rao, Y.; Ni, J. A deep learning approach to detection of splicing and copy-move forgeries in images. In Proceedings of the 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, United Arab Emirates, 4–7 December 2016; pp. 1–6.
9. Schetinger M, Chang S (1996) A robust content based digital signature for image authentication. In: Proceedings of 3rd IEEE international conference on image processing, vol 3. IEEE, pp 227–230
10. Tralic D, Zupancic I, Grgic S, Grgic M (2013) Comofod — new database for copy-move forgery detection. In: Proceedings ELMAR-2013, pp 49–54
11. Prasadu Peddi, & Dr. Akash Saxena. (2016). STUDYING DATA MINING TOOLS AND TECHNIQUES FOR PREDICTING STUDENT PERFORMANCE. International Journal Of Advance Research And Innovative Ideas In Education, 2(2), 1959-1967.
12. Various. Columbia image splicing detection evaluation dataset - list of photographers, 2004. https://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/photographers.htm. Accessed 16 Mar 2022
13. Wu Y, Abd-Almageed W, Natarajan P (2018) Busternet: detecting copy-move image forgery with source/target localization. In: Proceedings of the European conference on computer vision (ECCV), pp 168–184.
14. Weihong Wang and Hany Farid. Exposing digital forgeries in video by detecting double mpeg compression. In Proceedings of the 8th workshop on Multimedia and security, pages 37–47. ACM, 2006.
15. Warif NBA, Wahab AWA, dris MYI, Ramli R, Salleh R, Shamshirband S, Choo K-KR (2016) Copy-move forgery detection: Survey, challenges and future directions. J Netw Comput Appl 75:259–278.