ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 11, November 2017

Security implementation for the Image Forgery Detection: A review

[1] Mr.Mahesh Enumula, [2] . Dr.D.N.Rao, [3] Dr.M.Suman,

Abstract:- **As we are living in the today's world where all type of advancements are becoming possible and at the same time the use of images have been increasing day by day in our lives by means of uploading and transferring. The manipulation of images also increasing simultaneously. The victims of Image forgery increasing on daily basis. In this paper, we are performing a review of this Image forgery types and methods to detect image forgery. There are two kinds of techniques for detecting image forgery: one is active method, and the other is passive method. The main types of Image forgeries are Image Splicing, Copy-Move forgery and image retouching. These techniques used mainly for making tempered photographs. As the Image forgery with sophisticated technology is growing it is very much necessary to develop tools for detection of original image and the region of forgery. We study on of the most powerful technique with a classifier based on Neural Networks. The proposed frame work involves key steps like image acquisition, future extraction and classification algorithm. This method also monitors parameters like accuracy, precision etc. The implementation of proposed method meets the future needs in image forensics and reduces the risk of digital images.**

Index Terms**: Image forgery, watermarking, neural network, classifier**

I. INTRODUCTION

Forgery in not new to us. If signatures are manipulated it is called signature forgery. If documents are manipulated it is called document forgery. Similarly if images are manipulated it is called image forgery. In general we call Image forgery as image morphing. Image forgery, it is manipulation of images by means of adding or removing some part of the image or altering the detail of the image. With the increasing usage of internet over computers and smartphones image forgery became very common thing which we cannot differentiate between original one and manipulated one. Social media has become part of the everyday life through which millions of images are being exchanged daily. A survey in September 2017 says that daily 100 billion photos are being uploaded through different social media platforms like facebook, instagram, twitter, whatsapp etc. So all those images are prone for the image forgery. These is a chance for everyone to become victims of image forgery. Image has become more and more simple and indiscoverable With the increasing applications of digital imaging, different types of software tools are introduced for processing images and photographs. Todays digital technology has begun to remove trust in our knowledge, as from the magazines, to fashion world and in scientific journals, political campaigns, courts and the photo that come in our e-mail. In all of these forged photographs are appearing with a more frequencies and sophistication. In the increase in the availability of multimedia data in digital form has come to a tremendous growth of tools to manipulate digital multimedia contents[1].

The process of creating fake image has been tremendously simple with the introduction of new and powerful computer graphics editing software which are freely available as Photoshop, GIMP, and Corel Paint Shop. Today, this powerful image processing software allow people to modify photos and images conveniently and unperceivably. Now days it creates a big challenge to authenticate images. Image forgery means manipulation of the digital image to conceal some meaningful or useful information from it. Sometimes it is difficult to identify the edited region from the original image. The detection of a forged image is driven by the need of authenticity and to maintain integrity of the image. The survey has been done on existing techniques for forged image and it highlights various copy–move detection and splicing detection methods based on their robustness and computational complexity [2]. With the development of Computer Network and Communication Technology, huge information and data need to exchange through communication channels and networks which are public. Safety of Data transmission becoming more and more important day by day with efficiency. The usage of internet becoming more day by day and it has become mandatory to upload everybody day including photographs. These personal images leading to cybercrimes and cyber bullying especially in case of women. They are becoming victims of these crimes [3].

However image forgery is simple and can be done by everyone. The common man who is not having proper

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 11, November 2017

computer literacy can do forgery. But for detecting forgery expert level knowledge is needed. It is somewhat easier to find weather image is forged or not but the challenging task is to detect exact region where forgery was being done. It requires complex mechanism for identifying and removing the region of forgery. In early years websites used to host images with less size and there were certain techniques for detecting the forgery. Nowadays the size of the images and quality of the images in terms of mega pixels increased due to the use of most sophisticated digital cameras. Through cloud storage every user are able to store and share without any hesitation. So it requires efficient algorithm to overcome all these complication to detect forgery and to give region of forgery with more accuracy and precision.

II.TYPES OF IMAGE FORGERY

A. Image Retouching:

Image Retouching generally can be used for enhancing the certain features of the image.

These features include image color, sharpness, brightness etc etc. Retouching is less harmful forgery technique when compared to the all other types at present. With the image retouching original image does not changes much, but it enhances or reduces certain feature of original image. This technique is popular among magazine photo editors. Even this technique is ethically wrong, while publishing a picture some features need to be enhanced. For this enhancement image retouching can be done.so this can be called as magazine publishing technique.

Fig.1. Example of Image Retouching

B. Image splicing or photomontage:

Image splicing technique is more dangerous than image retouching. Image splicing is simple process. This process can be carried out on two separate pictures involves copy and pasting different regions. In this method it requires simple tools like adobe photoshop for sticking two different images. With use of Microsoft paint also everyone can perform some basic level of image splicing. Image splicing or photomontage is composition of two or more images. This combination create a fake image. This image forgery technique become a tool for cyber bullying. From ordinary person to celebrity sometimes world leaders also becoming victims of cyber bullying. Fig. 2 below shows how to create forged Image; by copying a spliced portion from the source image into a target image, it is a composite picture of scenery which is forged image.

Fig.2. Example of Image splicing

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 11, November 2017

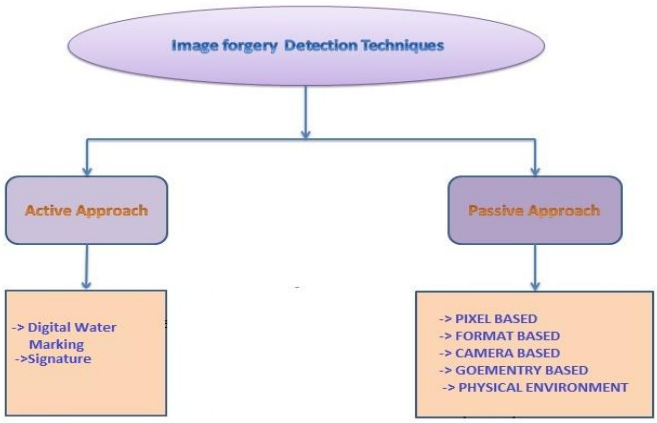
C. Copy-Move Attack:

The copy move forgery is popular among the all other technique. This technique is most complicated technique. It is widely used tampering technique. In this technique, in order to add or remove information part of the image has to copy and move or has to cut and move. In the Copy-Move manipulation technique a part of the image is copied and pasted into another part of same image itself. In the copy and move attack, the intention is to hide something in the original image. For hiding the information that particular part of the image has to be masked with the copied region. The example of Copy-Move type is as shown in below figure 3 below. The original image contains only one pigeon and its Copy-Moved version on the right has two pigeons. This type of forgery detection is very crucial in the field of defense and legal documents.

Fig.3. Example of Copy-Move attack

III.CLASSIFICATION OF IMAGE FORGERY TECHNIQUES

There are two kinds of techniques for image forgery detection. These approaches are vital in image forensics.one is active approach and the other is passive approach. Which again consist of many different methods, as shown in below chart.



A. Active Approach

In this active approach, the digital image requires some kind of pre-processing such as embedded signatures or digital water marking. These are generated at the time of creating the image. However, these approaches has got certain limitations. Digital watermarking and signature are two main active protection techniques, as something are embedded into images when they are obtained. We can detect the Image is tampered, if special information cannot be extracted from that obtained image. Watermarking is such a method of active tampering detection, as a security structure is embedded into the image, but most present imaging devices do not contain any watermarking or signature module and that are similar to the application of active protection[4]. This structure is used for integrity evaluation in the sense that if any discrepancy is found with the structure then the image is tampered and an inverse analysis over the structure is done to locate tampered. Regions of the image. In recent times, various schemes are proposed for providing security to the image, which is analogous to the concept of watermarking like, message authentication code, image hash, image checksum and image shielding as a counterpart to it[5].

Digital water marking can be used for the authentication of image or video content for the protection of copyrights. This technique frequently used in the broadcasting media.

B. Passive Approach

Passive approach is most challenging detection technique in image forensics. There is no particular method to find a solution for all cases. But there are methods each can detect a forgery in its own way. The passive tampering detection deals with analyzing the raw image based on various statistics and semantics of image content to localize tampering of image. Neither construct is embedded in the image and nor associated with it for security, as like active approaches and hence this method is also known as raw image analysis. The localization of tampering is solely based on image feature statistics. Hence, algorithms and methods of detection and localization of image based on passive tampering vary depending upon the type of security construct used. Nevertheless, passive tampering detection typically aims for localization of tampering on raw image[5].This localization can be based on pixel, format, camera, geometry and physical environment. If take the example of format based image forgery detection technique it compares the format of the picture in one region with format of the picture with another region. If both are not matched that particular region will be shown under forged region.

IV. INTRODUCTION TO ARTIFICIAL NEURAL NETWORK

Artificial neural networks (ANNs) or connectionist systems are computing systems which are inspired by the biological neural networks that constitute animal brains. Such systems learn to progressively improve the performance. The Artificial Neural Networks performs the tasks by different observation. It does not require any specific programming. For detecting the forgeries in images, they might learn to identify images that contain different forgery images. Using the analytic results to identify forgery images. It is difficult to use artificial neural networks in the applications of a traditional computer. It is not possible to use algorithms with rule-based programming. An ANN is based on a collection of connected units called artificial neurons, which are analogous to axons in a biological brain. Each connection synapse between neurons can transmit a signal to another neuron. The receiving postsynaptic neuron can process the signals and then signal downstream neurons connected to it. Neurons may have state, generally represented by real numbers, typically between 0 and 1. Neurons and synapses may also have a weight that varies as learning proceeds, which can increase or decrease the strength of the signal that it sends downstream. Further, they may have a threshold such that only if the aggregate signal is below or above that level is the downstream signal sent. Typically, neurons are organized in layers. Different layers may perform different kinds of transformations on their inputs. Signals travel from the first input, to the last output layer, possibly after traversing the layers multiple times[6].
The main aim of the Neural networks in the image forgery detection are to give the image forgery regions with more accuracy and precision which requires huge lines of program if we perform with the conventional computer programming. It requires training with hundreds of images so a to detect the region of forgery. Neural networks can be used in various applications including computer vision, speech recognition, machine translation, social network filtering, playing board and video games, medical diagnosis and in many other domains.

V. CONCLUSION

In this paper, we studied that, due to the advancements in the field of digital image processing manipulation of digital images has become easy with the use of advanced software. Due to powerful computers, photo-editing software, high resolution capturing devices and huge Social networking the digital image forgery has become a threat. The detection of image forgery has categorized into two major groups as active and passive approaches. We studied different types of image forgeries as, Image Retouching, Image Splicing, and Copy-Move Attack. It is not only important to detect the location of the forgery and also important to reproduce the original image with a trusted mechanism. This paper introduced importance of Neural networks for the detection of image forgery. While detecting the forgery and producing the original image it is important to monitor the parameters like efficient, precision and accuracy. This can be achieved using Neural networks.

REFERENCES

[1]Varsha Sharma, Swati Jha , Dr. Rajendra Kumar Bharti, “Image Forgery and it’s Detection Technique: A Review” International Research Journal of Engineering and Technology (IRJET), March 2016.

[2] Sridevi M., Mala C., Sanyam S. (2012) Comparative Study of Image Forgery and Copy-Move Techniques. In: Wyld D., Zizka J., Nagamalai D. (eds) Advances in Computer Science, Engineering & Applications. Advances in Intelligent and Soft Computing, vol 166. Springer, Berlin, Heidelberg

[3] Mr.Enumula Mahesh and Prof.Dr.M.Suman “AN IMPLEMENTATION OF CYBER SECURITY FOR THE PROTECTION OF WOMEN” International Journal of Latest Trends in Engineering and Technology Vol.(7)Issue(4), pp.228-233.

[4]O. M., Al-Qershi and B. E. Khoo, “Passive detection of copy-move forgery in digital images: State-of-the-art,” Forensic Science International, vol. 231, no. 1, 2013, pp. 284– 295.

[5] Varsha Sharma, Swati Jha , Dr. Rajendra Kumar Bharti “ International Research Journal of Engineering and Technology (IRJET)” Volume: 03 Issue: 03 | Mar-2016

[6] Bhadeshia H. K. D. H. (1999). "Neural Networks in Materials Science" (PDF). ISIJ International. 39 (10): 966–979. doi:10.2355/isijinternational.39.966