AUTOMATIC FORENSIC METHOD TO DETECT CHANGES IN DIGITAL PICTURES

Priti Swain
Student,
NCRD's Sterling Institute of Management Studies
Nerul, Navi Mumbai
pritiswain420@gmail.com

Anup Tiwari
Student,
NCRD's Sterling Institute of Management Studies
Nerul, Navi Mumbai
tiwarianup2000@gmail.com

Prof. Sagar Thakare
Assistant Professor (MCA),
NCRD's Sterling Institute of Management Studies,
Nerul, Navi Mumbai
sagthakare@gmail.com

ABSTRACT

We surely live in a time where we are bombarded with a staggering amount of visual imagery. Accepting digital photographs of government papers is becoming standard procedure. Image Authenticity is crucial in a variety of social situations. For example, the dependability of photos is crucial in they are utilised as evidence in courtrooms. Physicians use digital pictures to make key judgments in the medical industry Contracts, pictures, and other papers can now be exchanged fast thanks to modern technology. While we may have had faith in the purity of this imagery in the past, modern digital technology has begun to weaken that faith. Digital photos may now be easily modified and altered thanks to the introduction of low-cost, high-resolution digital cameras and sophisticated photo editing software. It is easy to alter the information conveyed by an image and generate forgeries that are indistinguishable from genuine images and documents with the naked eye. To identify copy-move forgeries, the proposed technique employs the Harris Interest Point detector in conjunction with SIFT descriptors. For matching, the KD-Tree is employed.

Keywords *– Copy-Move Forgery, CNN. IFSC, PRNU, FCN, BDIR, PFAXO.*

INTRODUCTION

A forged image can be created with access to a computer and a basic understanding of software such as Adobe Photoshop. Photographic image manipulation is not a new phenomenon. The practice of tampering with photographic photographs stretches back to the creation of permanent photographic images. One of the first perpetrators of photographic images. Alteration was Vladimir Ilyich Lenin. Egypt's state run newspaper, Al-Ahram, recently released a tampered photo(fig-1)of Egyptian President Hosni Mubarak walking with Israeli, US, Palestinian, and Jordanian Leaders during the most recent middle East Peace talks. The photo that was released, on the other hand, was a good example of tampering.

Fig.1. The photo(right) is a tampered with original (left)

The rise of digital forensics in recent years has aided in the restoration of some faith in the field of digital imaging. In the absence of watermarks or signatures put in the images, digital forensics deals with building solutions. In general, there are two types of digital picture forgery detection methods: 1- Active Digital Image Forensics and 2- Passive Digital Image Forensics, often known as Blind Digital Image Forensics.

Copy-move forgery is a sort of forgeryin which one component of a picture is copied and pasted into another part of the same image, as seen in fig-2. Because the duplicated section comes from the sae image, some components (colour and noise) will be compatible with the rest of the image and hence will not be detectable using methods that seek for statistical incompatibilities in various parts of the image because a copy-move forgery creates a link between the original.

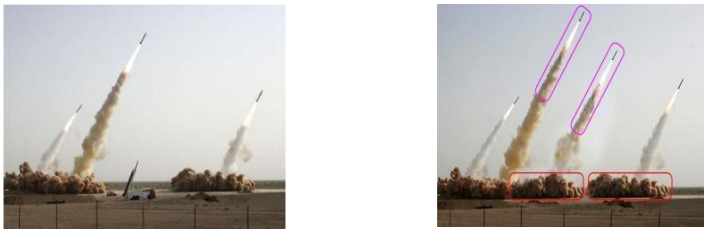

Fig.2.

An example of Copy-Move Forgery that appeared in press in July, 2008. The original image (on the left) shows 3 original images and a tapered image (on the right) shows Iranian missiles; two different sections (encircled in red and purple, respectively) replicate other image sections by applying a copy-moveattack.

LITERATURE REVIEW

With advancements in the production of digital images, forgeries have a significant effect on people where DI is monitored before sending, impacting the digital image. DI has been used for successful decision-making systems in many regions. It requires forensic security, recognition and detection of crime patterns. Financial information, medical reports, journalism where applications are not guaranteed with confidentiality are the digital data use

on real-world applications. Cybercrime activities have been developed in multimedia systems for knowledge exchange with interactive multimedia content. In order to provide digital evidence for legal purposes, electronic forensics extracts knowledge from computers. Cyber forensics requires computer evidence construction processes for criminal investigation. Visual and multimedia sciences are facing a disruptive development in forensic sciences. To enhance the identification of affected portions in DI, many image forgery techniques were designed. The software were thoroughly developed with the aid of literature to analyse cyber forensic protection and multimedia data security.

Digital image segmentation.

Digital Image Denoising Techniques.

Machine Learning Based Denoising Methods.

Noise Removal In Image Denoising.

Filtering Methods.

Transform Based Image Denoising Methods.

Digital Image Forgery Detection.

Digital Image Forensic Security.

Security In Multimedia

RESEARCH GAP

Block matching algorithm was designed to address the time complexity by sequential block clustering. The noise introduced while sending the multimedia image was not detected. LSB replacement and matching are introduced to increase security level aspects. Forgery detection remained unsolved issue. Lossy Compression and Iterative Reconstruction (LCIR) with pseudo random permutation for encrypting the images produced quality image on receiving end through spatial correlation reducing the noise ratio. But, security was compromised though the compression ratio and quality of reconstructed image was improved.

PROBLEM DEFINITION

In implementing digital forensic solutions, the fundamental challenges are likely:

Improvement of technology: As the number of tambourinous photos and videos flood TVs, magazines and networks hide the truth, the numbers of networks and multimedia are increasing. With powerful image and video editing tools, images and videos that make digital forgery detection a difficult task can be easily manipulated.

In addition, forgery detection techniques present a number of challenges: reducing wrong positive rates, i.e. detecting authentic pictures as forged pictures; automating the system completely, localising the forging of any form of image (compressed or uncompressed), enhancing robustness and reliability, etc.

RESEARCH QUESTION

The aim of this work is to develop an automatic forensic method to detect changes in digital pictures. Until now, all picture forgings have not been detected universally.

-To detect key image manipulation, such as rotation re-sampling, rescaling, and rotating and rescaling factor estimations. The approach also seeks to improve the detection by de-noising of re-sampling (rotation/rescaling).

-R-CNN with Bayes Digital Image Rule is designed to achieve effective forensic security.

-Contrast improvement analysis and histogram equalisation for the detection of image improvement. Forensic analysis.

OBJECTIVE

Although improvements in images such as contrast and histogram evening are harmless, it can lead to the detection of another malicious and harmful forgery detection, as these improvements often take place in the process of imaging to hide artefacts created and to give a natural look to the changed images

.

RESEARCH METHODOLOGY

The flow process of proposed methodology is shown in Figure 3

Mask R-CNN is proposed for obtaining effective forensic security on digital multimedia image. Maximization of fast expectations Proof Identification Algorithm (MFEPIA) is used in the proposed mask R-CNN mechanism to calculate maximum probability and thus improve digital data security. Segmentation operations are applied to maximum probability

features to determine the number of variable components and parameters of mixture pixels. With the help of Bayes Digital Image Rule (BDIR), the proposed R-CNN mask mechanism increases forensic security legal proceedings for variable spatial components. It relates the odds of events to the probability calculation and preserves the legal process to improve the level of spatial resolution.

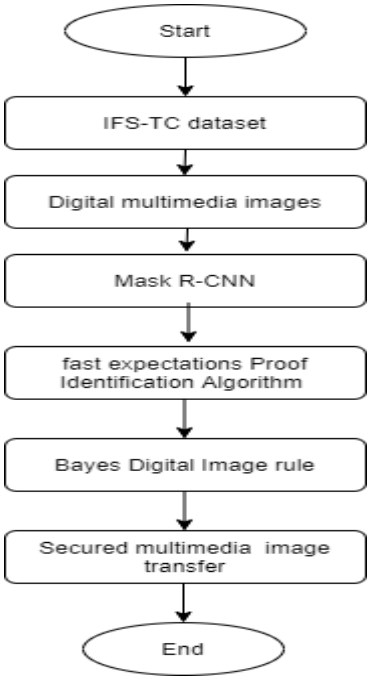

Fig.3.

Flow chart of Proposed work

OVERVIEW OF FORENSIC IMAGE DETECTION

Image enhancements like contrast improvements and histogram equalisation are often involved in many forgeries such as copy-paste, region duplication, etc. So, in digital pictures if there are traces of such enhancements, the image may be modified. This work is designed to detect these improvements in digital images. While this technique detects operations that alter the perceptive qualities of an image rather than more obviously malicious tampering, it remains forensically important that the manipulations are detected since these operations often participate in the majority of the forged images so as to make forged image look natural.

Our approach, named Mask R-CNN, extends R-CNN Faster [1] by an addition to the existing branch for clustering and bundle regression, in parallel with each region of interest, for

predicting segmentation mask (Figure 3.2). The mask branch is a small FCN used for each RoI, predicting a segmentation mask in a pixel-topixel manner. Mask R-CNN is simple to implement and train thanks to the Faster R-CNN framework, which facilitates a wide range of flexible architecture designs. In addition, the mask branch only adds a small computational overhead, enabling a quick system and rapid experimentation.

Mask R-CNN Architecture

The conceptually simple mask R-CNN is: Faster R-CNN is equipped with two outputs for the candidate object, a class label and an offset bounding box, to which we add an object mask in the third branch.

Let's begin by discussing Faster R-CNN architecture, which works in two stages to understand Mask R-CNN:

There are 2 phase in Mask-R-CNN.

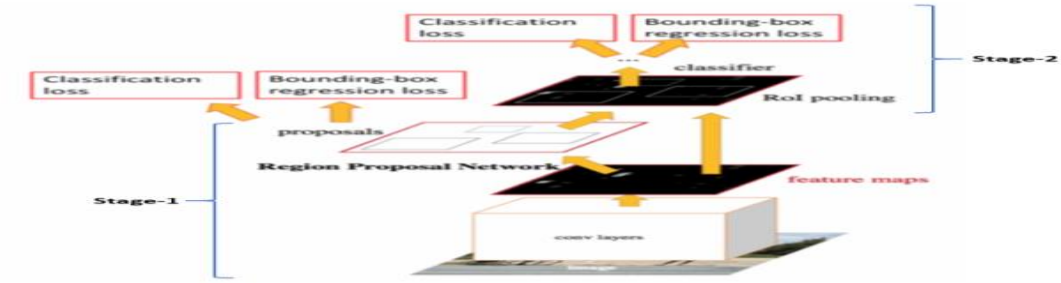

Fig.4.

Faster R-CNN architecture [1]

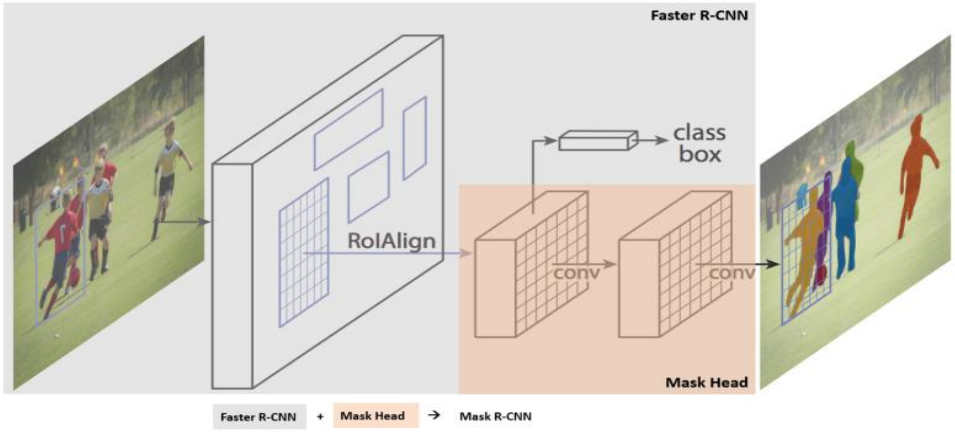

Fig.5.

The Mask R-CNN framework [2]

Mask R-CNN is proposed for obtaining effective forensic security on digital multimedia image.

Maximization of fast expectations Proof Identification Algorithm (MFEPIA) is used in the proposed mask R-CNN mechanism to calculate maximum probability and thus improve digital data security. Segmentation operations are applied to maximum probability features to determine the number of variable components and parameters of mixture pixels. With the help of Bayes Digital Image Rule (BDIR), the proposed R-CNN mask mechanism increases forensic security legal proceedings for variable spatial components. It relates the odds of events to the probability calculation and preserves the legal process to improve the level of spatial resolution.

RESULTS

The proposed mask R-CNN mechanism is implemented using python. For conducting the experimental results, the proposed algorithm is applied using IEEE Information Forensics and Security Technical Committee (IFS-TC) launched a detection and localization forensics challenge. The dataset consists of fake and pristine images

R-CNN performance is compared with two methods already in place. The current approach compared is the non-uniformity Photo Response (PRNU) method as well as the preliminary Xbox One forensic analysis (PFAXO). The proposed mechanism is implemented using the following parameters for experimental purposes. For the following parameters the performance of the R-CNN is evaluated.

• Peak signal to noise ratio

• false positives

• legal forensic system process efficiency

• Computational Time.

LIMITATION

The methods proposed, namely the R-CNN mask mechanism with Bayes Digital Image Rule and Fast Expectation Maximisation Proof Identification algorithm, are designed to improve forensic safety of digital multimedia data.

However, only malware activities are minimised and criminal data are not extracted from digital secure multimedia data.

Without any of the fundamental operations such as turning, rescaling, contrasting and histogram equalisation the image falsifier could have forged the images. These are all motivations for the future development of improved forensic techniques. In recent years, video contents are also being manipulated to create video forgery. Consequently, the proposed falsification detection techniques can be extended to detect falsifications in videos.

CONCLUSION

The processing of images is described as the progress of the transition to different results of digital multimedia inputs. Multimedia data like documents, records, reports, pictures, videos, etc. Digital media data forensic security has been identified extensively as a promising paradigm to overcome cybercrime activities during the transmission of digital data. Digital fingerprint forensic accuracy creates a serious challenge in the field of digital forensic analysis. In order to frequently carry out fast data communication, the digital multimedia data shows a critical responsibility to achieve forensic security on digital multimedia data are proposed in the present study.

The R-CNN mask is initially used to achieve an effective forensic security on digital multimedia pictures. In order to assess maximum probability, the Fast Expectation Maximisation Proof Identification algorithm is developed here. It therefore improves digital data security. Afterwards, the process of image segmentation is applied to establish the changing components and mixing pixels as often as possible. In conclusion,

problem since a person's biometric data is undeniably connected to its owner, is non-transferable and unique for every individual.

Biometrics is not only a fascinating pattern recognition research problem but, if carefully used, could also be an enabling technology with the potential to make our society safer, reduce fraud and lead to user convenience by broadly providing functionalities like, positive identification,large scale identification and screening.

REFERENCES

[1] S. Ren, K. He, R. Girshick, and J. Sun. Faster R-CNN: Towards real-time object detection with region proposal networks. In NIPS, 2015.

[2] Kaiming He, Georgia Gkioxari, Piotr Dollár, Ross Girshick: "Mask R-CNN", 2017

[3] https://shodhganga.inflibnet.ac.in/handle/10603/224700.

[4] https://link.springer.com/article/10.1007/s11042-010-0620-1

[5] [http://arxiv.org/abs/1703.06870

[6] https://www.wikipedia.org/