International Journal of Innovative and Emerging Research in Engineering
Volume 3, Special Issue 1, ICSTSD 2016

Efficient Approach for Image Anti-Forensic Methodology

Miss. N. D. Kadu
SGBAU, Amravati
India.
nehakadu93@gmail.com

Dr. R. V. Dharaskar
SGBAU, Amravati
India.
rvdharaskar@rediffmail.com

Dr. V. M. Thakare
SGBAU, Amravati
India.
vilthakare@yahoo.com

ABSTRACT

In digital Image Anti-Forensic techniques are used for photo response non-uniformity noise (PRNU), a unique fingerprint of imaging sensors, in various digital forensic applications such as source device identification, content integrity verification and authentication. The process of investigation make the analysis and reconstruction of attack scenarios difficult, challenging, or even impossible.To authenticate multimedia content analyze the interaction between a forger and a forensic investigator by examining the problem of authenticating digital videos. The electrical network frequency (ENF) signal is a time stamp that has been used by an emerging class of approaches for determining the creation time of digital audio and video recordings. At showing that having the tampering location known, image tampering can be modeled and dealt with as an erasure error. Anti-Forensic techniques are couple-decoupled PRNU (CD-PRNU) extraction, watermark bit-budget,deletion or addition detection, Concealment, and Mitigate Anti-forensic attacks.

Keywords:- couple-decoupled PRNU (CD-PRNU) extraction, watermark bit-budget ,deletion or addition detection, Concealment, and Mitigate Anti-forensic attacks.

I.INTRODUCTION

couple-decoupled PRNU (CD-PRNU) extraction this method prevent the interpolation noise from propagating into the physical components, thus improving the accuracy of device identification and image content integrity verification. watermark bit-budget method significantly outperforms recent techniques in terms of image quality for both watermarked and recovered image. The watermarked image quality gain is achieved through spending less bit-budget on watermark, while image recovery quality is considerably improved as a consequence of consistent performance of designed source and channel codes. deletion or addition detection this method to evaluate the performance of each of it proposed forensic and anti-forensic techniques, and identify the optimal actions of both the forger and forensic investigator. Concealment technique are forensic analysts and adversaries by providing an evolutionary perspective and a game-theoretical perspective as well as studying representative scenarios and the optimal forensic/anti-forensic strategies. to mitigate anti-forensic attacks and generate potential scenarios starting from traces that were targeted by these attacks. To exemplify the proposal, it provide a case study related to the investigation of an incident that exhibited anti-forensic attacks.

II. BACKGROUND

Is to demonstrate the capability of the proposed CD-PRNU in dealing with the color interpolation noise, so geometrical transformations will not be applied in order to prevent biased evaluation from happening.[1]. Their purpose is to formally generate the sequence of events, which describes the occurrence of the incident, using theoretical and scientifically proven methods, validate the correctness of the techniques used to process and analyze evidence, provide provable conclusive descriptions regarding the attackers activities, and reduce the complexity and automate the analysis of the incident.[2]. It analyze the interaction between a forger and a forensic investigator by examining the problem of authenticating digital videos. The problem of adding or deleting a sequence of frames from a digital video. An anti-forensic technique designed to fool video forensic techniques and develop a method for detecting the use of anti-forensics[3]. It examined the resilience of this time stamp against anti-forensics under adversarial environments. It investigated anti-forensic operations that can remove and alter the ENF signal present in a host audio signal. It developed a mathematical framework for ENF modification, which not only entails the effectiveness of ENF modification and challenges of antiforensics detection, but also motivates detection methods.[4].These scheme significantly outperforms recent techniques in terms of image quality for both watermarked and recovered image. The watermarked image quality gain is achieved through spending less bit-budget on watermark, while image recovery quality is considerably improved as a consequence of consistent performance of designed source and channel codes.[5].

This paper introduced efficient approach for image anti-forensic methodology **section I** Introduction. **Section II** discuss Background. **Section III** discuss Previous work done. **Section IV** discuss Existing methodology. **Section V** Analysis And Discussion **section VI** discuss Proposed methodology and possible result. **section VII** Conclude paper.

III.PREVIOUS WORK DONE

Chang-Tsun Li,et al[1]has worked on The last few years have seen the use of photo response non-uniformity noise (PRNU), a

unique fingerprint of imaging sensors, in various digital forensic applications such as source device identification, content integrity verification, and authentication.

Slim Rekhis,*et al* [2] has worked on To defeat the process of investigation and make the analysis and reconstruction of attack scenarios difficult, challenging, or even impossible, attackers aremotivated by conducting anti-forensic attacks.

Matthew C. Stamm,*et al* [3] has worked on analyze the interaction between a forger and a forensic investigator by examining the problem of authenticating digital videos.T he problem of adding or deleting a sequence of frames from a digital video. Wei-Hong Chuang, et al[4]has worked on paper explores possible antiforensic operations that can remove and alter the ENF signal while trying to preserve the host signal, and devises detection methods targeting these operations. Concealment techniques that can circumvent detection are also discussed and their corresponding trade-offs are examined.

Saeed Sarreshtedari, et al [5] has worked on showing that having the tampering location known, image tampering can be modeled and dealt with as an erasure error. Therefore, an appropriate design of channel code can protect the reference bits against tampering.

Concealment techniques that can circumvent detection are also discussed and their corresponding trade-offs are examined. The total watermark bit-budget is dedicated to three groups: 1) source encoder output bits; 2) channel code parity bits; and 3) check bits. A number of antiforensic operations have recently been designed to make digital forgeries undetectable by forensic techniques. An anti-forensic technique designed to fool video forensic techniques and develop a method for detecting the use of anti-forensics. Several methods were proposed by the literature to formally reconstruct the sequence of events executed during the incident using theoretical and scientifically proven methods. This new method can prevent the interpolation noise from propagating into the physical components, thus improving the accuracy of device identification and image content integrity verification.

IV. EXISTING METHODOGY

Digital image Anti-forensic techniques are couple-decoupled PRNU (CD-PRNU) extraction, watermark bit-budget,deletion or addition detection, Concealment, and Mitigate Anti-forensic attacks.

The last few years have seen the use of photo response non-uniformity noise (PRNU), a unique fingerprint of imaging sensors, in various digital forensic applications such as source device identification, content integrity verification, and authentication.[1]. An inference system is proposed to mitigate anti-forensic attacks and generate potential scenarios starting from traces that were targeted by these attacks. It provide a case study related to the investigation of an incident that exhibited anti-forensic attacks.[2].It begin by developing a theoretical model of the forensically detectable fingerprints that frame deletion or addition leaves behind, then use this model to improve upon the video frame deletion or addition detection technique. [3]. The electrical network frequency (ENF) signal is a time stamp that has been used by an emerging class of approaches for determining the creation time of digital audio and video recordings. However, in adversarial environments, anti-forensic operations may be conducted to manipulate ENF-based time stamps, and it is crucial to understand the resilience of ENF analysis against anti-forensics.[4]. The watermark bit-budget falls into three parts, check bits, source encoder output bits, and channel encoder parity bits. The original image is source coded using SPIHT compression algorithm. The source encoder output bit stream is channel coded using RS code of a required rate and over appropriate field. Since image tampering affects a burst of bits, the RS codes over large Galva fields are wise choices.[5].

DATASET:

For a system with a Pentium Core II 1.3G CPU and 3GB RAM, it takes 0.526 s to compute the similarity between the PRNUs of two images of 2048 × 1536 pixels and 0.567 s to calculate the similarity between a pair of CD-PRNUs of the same size. The amount of data processed during the extraction of PRNU and CD-PRNU is the same. Although extracting CDPRNU requires down-sampling and up-sampling, these two operations are trivial and only incur negligible increase of time complexity .8-bit gray scale Cameraman image of size 512 × 512 is watermarked using this proposed method . The watermarked image generated by 2-LSB version of this algorithm. The PSNR of watermarked image generated by 2-LSB version of our algorithm equals 44.15 dB, which is far beyond the HVS threshold of noticeable distortion. State-of-the-art tampering protection algorithms usually use three least significant bits for watermark insertion. This embedding approach degrades the PSNR of watermarked image down to 37.9 dB, which is not suitable for smooth areas.

V. ANALYSIS AND DISCUSSION

The PRNU noise patterns of the sub-images are then assembled to get the CD-PRNU. This new method can prevent the interpolation noise from propagating into the physical components, thus improving the accuracy of device identification and image content integrity verification.[1].These methods are not tailored to cope with anti-forensic attacks, as they assume that the collected evidence

is trusted, do not model anti-forensic actions, and do not characterize provable anti-forensic attacks based on the knowledge of attacks, security solutions, and forms of evidence expected to be generated. [2]. It propose an anti-forensic technique designed to fool

video forensic techniques and develop a method for detecting the use of anti-forensics.It introduce a new set of techniques for evaluating the performance of anti-forensic operations and develop a game theoretic framework for analyzing the interplay between a forensic investigator and a forger.[3]. Concealment techniques that can circumvent detection are also discussed and their corresponding trade-offs are examined. Based on the understanding of individual anti-forensic operations and countermeasures, this paper further characterizes the dynamic interplay between forensic analysts and adversaries by providing an evolutionary perspective and a game-theoretical perspective as well as studying representative scenarios and the optimal forensic/anti-forensic strategies.[4]. That proposed

scheme significantly outperforms recent techniques in terms of image quality for both watermarked and recovered image. The watermarked image quality gain is achieved through spending less bit-budget on watermark, while image recovery quality is considerably improved as a consequence of consistent performance of designed source and channel codes. [5].

Table 1: Comparison between different Image Anti-Forensic techniques.

Digital Image Anti-Forensic techniques	**Advantages**	**Disadvantages**
couple-decoupled PRNU (CD-PRNU) extraction	**1**. Source device identification, content integrity verification, and authentication. 2. The color variation between neighboring pixels is greater, thus the interpolation noise is also more significant.	1. The credibility of digital multimedia when used as evidence in legal and security domains will be constantly challenged and has to be scientifically proved. 2. It is of no doubt that unwatermarked multimedia will keep on being produced
Watermark bit-budget	1.Digital imaging has been rapidly developing in last two decades, and digital multimedia products are utilized in countless applications nowadays. 2. Showing that having the tampering location known, image tampering can be modeled and dealt with as an erasure error. 3. An appropriate design of channel code can protect the reference bits against tampering.	1. The watermark waste problem by offering schemes in which the content information is derived from several blocks. **2.** Provide almost error free restoration at the expense of very limited TTR or a very low quality of the watermarked image 3. Constant fidelity algorithms offer constant quality of reconstruction for tampering up to a certain limit at the expense of failing to restore tampered area beyond that limit.
deletion or addition detection	**1** To remove contrast enhancement fingerprints and to artificially synthesize color filter array artifacts used for camera identification or forgery detection.	1. The forensic investigator's probability of false alarm constraint is increased, the strength with which the forger should apply anti-forensics is decreased.
Concealment Mitigate	1. the feasibility of digital forgeries, reliable use of multimedia data requires forensic authentication mechanisms that can identify data origin and detect content tampering. 2. Anti-forensics so as to discover the weaknesses of current forensic methods and improve the robustness of forensic technology.	1. Attacker would perform some anti-forensic operations to confuse the current forensic methods.

VI.PROPOSED METHODOLOGY:

The signal will inevitably be distorted when passing through each process and these distortions result in slight differences between the scene and the camera captured image.

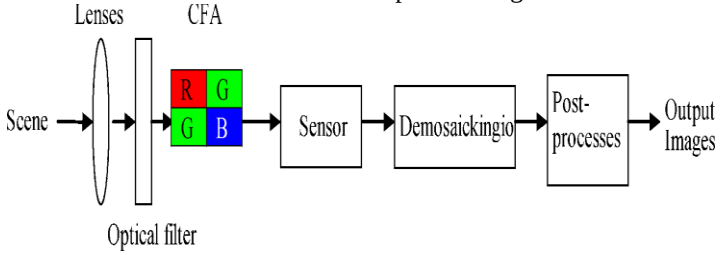

Fig1. Image acquisition process of a digital camera

The PRNU can be contaminated by various types of noise introduced at different stages of the image acquisition process. Fig. 1 demonstrates the image acquisition process . A color photo is represented in three color components (i.e., *R*, *G*, and *B*). For most digital cameras, during the image acquisition process, the lenses let through the the PRNU can be contaminated by various types of noise introduced at different stages of the image acquisition process. Fig. 1 demonstrates the image acquisition process. A color photo is represented in three color components (i.e., *R*, *G*, and *B*). For most digital cameras, during the image acquisition process, the lenses let through the a color interpolation function generates the electronic signals of the other two color components for every pixel according to the color intensities of the neighboring pixels. This color

interpolation process is commonly known asdemosaicking. The signals then undergo additional signal processing such as white balance, gamma correction, and image enhancement. These signals are stored in the camera's memory in a customized format, primarily the JPEG format.

OUTCOME AND POSSIBLE RESULTS

A couple-decoupled PRNU (CD-PRNU) extraction method, which first decomposes each color channel results is based on the detection of inconsistencies between secure and attack-prone evidence, with respect to the content of the library of attacks, the form and properties of evidence expected to be generated by the deployed security solutions, forms of evidence expected to be generated to evaluate the performance of each of proposed forensic , anti-forensic techniques and identify the optimal actions of both the forger and forensic investigator.

VII. COCLUSION

CD-PRNU extraction method, which can prevent the CFA interpolation error from diffusing from the artificial color channels into the physical channels, improving the accuracy of the fingerprint. In these methods are not tailored to cope with anti-forensic attacks, as they assume that the collected evidence is trusted, do not model anti-forensic actions, and do not characterize provable anti-forensic attacks based on the knowledge of attacks, security solutions, and forms of evidence expected to be generated to evaluate the performance of each of proposed forensic and anti-forensic techniques, and identify the optimal actions of both the forger and forensic investigator .

FUTURE SCOPE

Future work will address the formal digital investigation of anti-forensic attacks on multimedia content, and the extension of the inference system to address anti-forensic attacks on the algorithms of evidence generation used by observers. It could address the investigation of online anti-forensics taking into consideration the definition of reactive measures to capture evidence related to these attacks, and the development of a formal model of analysis of this evidence.

REFERENCES

[1] Chang-Tsun Li and Yue Li, "Color-Decoupled Photo Response Non-Uniformity for Digital Image Forensics," IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 22, NO. 2 , FEBRUARY 2012.

[2] Slim Rekhis and Noureddine Boudriga, "A System for Formal Digital Forensic Investigation Aware of Anti-Forensic Attacks," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[3] Matthew C. Stamm, W. Sabrina Lin, and K. J. Ray Liu, "Temporal Forensics and Anti-Forensics for Motion Compensated Video" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 4, AUGUST 2012.

[4] Wei-Hong Chuang, Ravi Garg and Min Wu, ," Anti-Forensics and Countermeasures of Electrical Network Frequency Analysis ,"IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 12,DECEMBER 2013.

[5] Saeed Sarreshtedari, and Mohammad Ali Akhaee, "A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 24, NO. 7, JULY 2015.