IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN IMPROVED ALGORITHM FOR DIGITAL IMAGE AUTHENTICATION AND FORGERY LOCALIZATION

[1]REJITHA K R, [2]PRAMEEJA PRASIDHAN

[1]student

[1]Department of computer science St. Joseph's college (Autonomous) Irinjalakuda, Thrissur, Kerala,

[2]Department of computer science St. Joseph's college (Autonomous) Irinjalakuda, Thrissur, Kerala

Abstract— **This paper focuses on the digital image authentication and forgery localization using demosaicing artifacts. The aim is to make an algorithm allowing a bridge between the color filter array pattern and demosaicing algorithm estimation, and thus the statistical analysis of demosaicing artifacts in spatial domain to reinforce the authentication and localization performance. After analysing the evolution of demosaicing traces privately acquisition pipeline, a robust feature statistic characterizing demosaiced digital images is first developed on the thought of the noise residue of green channel. Such a feature statistic may be a smaller amount sensitive to the edges problem because only the graceful region of green channel is used within the event. Next, one normal mixture model is proposed to elucidate the probability distribution of feature statistics for both original and tampered images. Therefore, normality tests are often used to authenticate automatically digital images. The authentication performance are often further improved by human interpretation of supported graphic tools. Finally, a penalized expectation-maximization algorithm is used to localize forged areas in tampered images. Numerous comparative studies on four well-known datasets show that the developed algorithm yields better performance and robustness than existing forensics algorithms of the same kind.**

Keywords— ***Demosaicing traces, digital image authentication, forgery localization, normal mixture model, penalized expectation-maximization algorithm.***

I. INTRODUCTION

Digital image are a robust media of communication. People have doing image manipulation using cost free editing software's. Excellent example is photo shop, gimp etc. There are two sides of coins. Likewise every equipment have good and bad sides. Photoshop is used permanently and bad image manipulation. Tampering the image comes under bad manipulation.

Digital image forgeries are common nowadays as many picture editing soft wares are easily available. Also digital cameras and computers has become cheap and easily available to people, so visually identifying forgeries is difficult for humans. One cannot identify whether the image is original or

manipulated. Images are often manipulated by deleting a neighborhood of image or hiding some region within the image or by modifying the image to misrepresent the image information. Such

vulnerabilities decreases the credibility and authenticity of digital images. Generally speaking, these techniques are classified into two major categories: active (non-blind) approach and passive (blind) approach. With ``active", we mean that some pre-set authentic information (e.g., watermark, signature) embedded in digital images is required to seem at their truthfulness. Whereas, with ``passive", certain of intrinsic traces within the image acquisition or some specific traces left by forgeries are exploited to differentiate between tampered and natural images. As such, the passive approach doesn't believe any prior information, and hence having broader applications than the active approach. This paper addresses a passive algorithm for digital image authentication and forgery localization using demosaicing traces. During a camera acquisition pipeline, demosaicing (also mentioned as color filter array (CFA) interpolation) is an upstream operation for reconstructing a full color image from the sampled data overlaid with a CFA.

II. PROPOSED SYSTEM

The proposed system addresses an algorithm for digital image authentication and forgery localization using demosaicing artifacts. Normal mixture model is proposed to describe the probability distribution of both original and tampered images. A penalized expectation-maximization algorithm is used to localize forged areas in tampered images.

The proposed is a fool proof one and it is dependable. It will remove so many difficulties in establishing whether a digital image is forged one or not. It is less expensive and the outcome is received very quickly.

III. SYSTEM DESCRIPTION

The proposed system solves problems of existing system. The proposed system. This paper addresses a passive algorithm for digital image authentication and forgery localization using demosaicing traces. One normal mixture model is proposed to explain the probability distribution of feature statistics for both original and tampered images. Therefore, normality tests are often wont to authenticate automatically digital images. The authentication performance are often further improved by human interpretation of supported graphic tools. A penalized expectation-maximization algorithm is employed to localize forged areas in tampered images. Numerous comparative studies on four well-known datasets show that the developed algorithm yields better performance and robustness than existing forensics algorithms of an equivalent kind.

Fig1: Block diagram of the proposed system

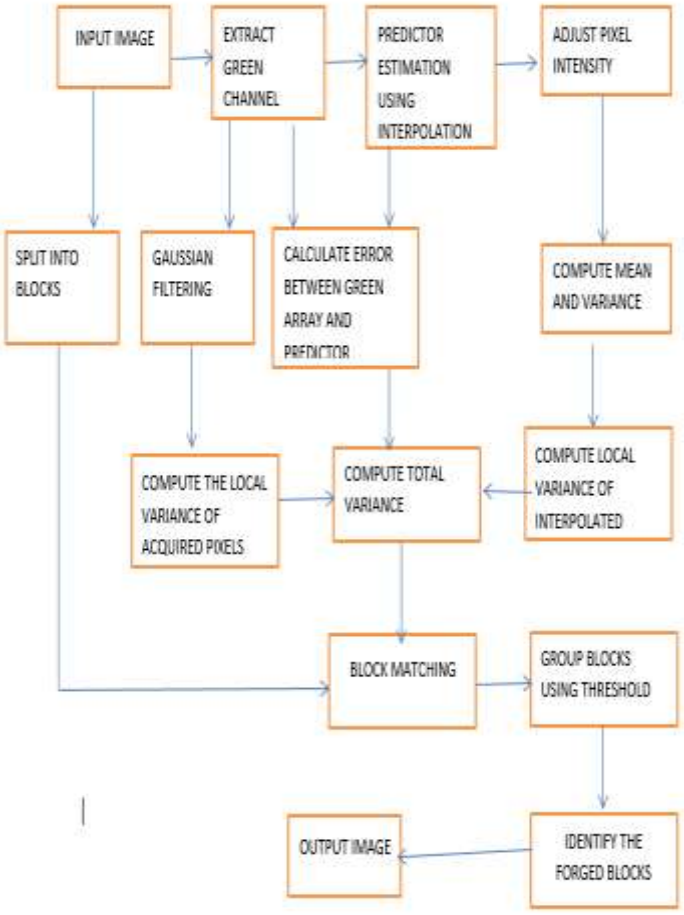
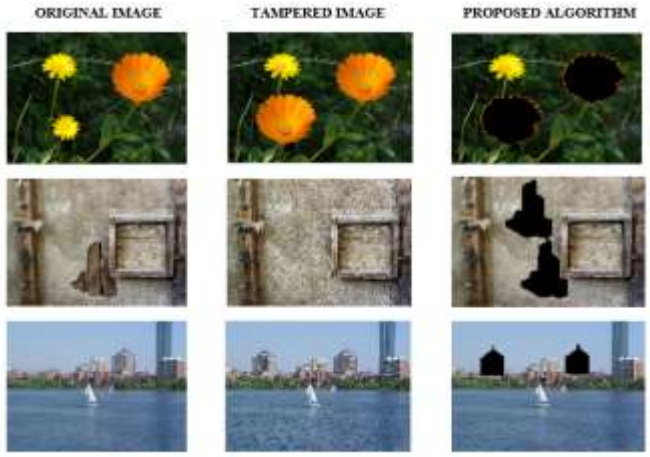


Fig2: Examples of forgery localization by the proposed algorithm



IV. SCOPE

Our proposed system thanks to enormous growth in e-governance throughout the general public & Private Sector and ecommerce activities Electronic Evidence have involved into a fundamental pillar of communication, processing and documentation. The govt agencies are opening up to introduce various governance policies electronically and periodical filings to manage and control the industries are done through electronic means. These various sorts of Electronic Evidence/ Digital Evidence are increasingly getting used within the judicial proceedings. At the stage of trial, Judges are often asked to rule on the admissibility of electronic evidence and it substantially impacts the result of civil law suit or conviction/acquittal of the accused. The Court still grapple with this new electronic frontier because the unique nature of evidence, also because the ease with which it are often fabricated or falsified, creates hurdle to admissibility not faced with the opposite evidences. This proposed system helps to extend the genuiness of the digital image and it'll solve the difficulties within the above said circumstance.

V. CONCLUSION

We develop in this paper an improved algorithm for digital image authentication and forgery localization by jointly use the color filter array pattern identification, demosaicing algorithm
estimation, and the local statistical analysis of demosaicing artifacts in spatial domain. A new feature statistic less sensitive to the edges problem is thus built to characterize demosaiced images. By modelling such feature statistics by a single normal mixture model for both tampered and untampered images, four well-known normality tests (i.e., Anderson-Darling test, one-sample Kolmogorov-Smirnov test, Jarque-Bera test and Lilliefors test) are employed to automatically authenticate digital images. Numerical experiments on the four well-known datasets (i.e. Image Manipulation, MICC-F600, Realistic Tampering, and CUISDE) shows that the performance of automatic authentication is relatively low, but can be much more improved thanks to human interpretation of supported graphic tools(i.e., Q-Q plot diagram, probability distribution curves, and localization map). Regarding the forgery localization, we propose a penalized EM algorithm to automatically distinguish between

authentic and forged regions of a tampered image without any requirement on comparison thresholds as in most existing localization algorithm. Such a method is proved to be more effective and robuster by numerical examples.

REFERENCES

[1] J. A. Redi, W. Taktak, and J.-L. Dugelay, ``Digital image forensics:A booklet for beginners," *Multimedia Tools Appl.*, vol. 51, no. 1, pp. 133_162, Jan. 2011.
[2] A. Piva, ``An overview on image forensics," *ISRN Signal Process.*, vol. 2013, Nov. 2013, Art. no. 496701.
[3] M. A. Qureshi and M. Deriche, ``Abibliography of pixel-based blind image forgery detection techniques," *Signal Process., Image Commun.*, vol. 39, pp. 46_74, Nov. 2015.
[4] P. Korus, ``Digital image integrity_A survey of protection and veri_cation techniques," *Digit. Signal Process.*, vol. 71, pp. 1_26, Dec. 2017.
[5] S. Teerakanok and T. Uehara, ``Copy-move forgery detection: A state-of-the-art technical review and analysis," *IEEE Access*, vol. 7, pp. 40550_40568, 2019.
[6] H. Farid, ``Image forgery detection," *IEEE Signal Process. Mag.*, vol. 26, no. 2, pp. 16_25, Mar. 2009.
[7] X. Lin, J.-H. Li, S.-L. Wang, A.-W.-C. Liew, F. Cheng, and X.-S. Huang, ``Recent advances in passive digital image security forensics: A brief review," *Engineering*, vol. 4, pp. 29_39, Feb. 2018.
[8] M. Kirchner, ``Ef_cient estimation of CFA pattern con_guration in digital camera images," *Proc. SPIE*, vol. 7541, Jan. 2010, Art. no. 754111.
[9] C.-H. Choi, J.-H. Choi, and H.-K. Lee, ``CFA pattern identi_cation of digital cameras using intermediate value counting," in *Proc. 13th ACM Multimedia Workshop Multimedia Secur.*, 2011, pp. 21_26.
[10] J. Takamatsu, Y. Matsushita, T. Ogasawara, and K. Ikeuchi, ``Estimating demosaicing algorithms using image noise variance," in *Proc. IEEE Com- put. Soc. Conf. Comput. Vis. Pattern Recognit.*, Jun. 2010, pp. 279_286.
[11] J. J. Jeon, H. J. Shin, and I. K. Eom, ``Estimation of Bayer CFA pattern con_guration based on singular value decomposition," *EURASIP J. Image Video Process.*, vol. 47, p. 47, Dec. 2017.
[12] H. J. Shin, J. J. Jeon, and I. K. Eom, ``Color _lter array pattern identi_cation using variance of color difference image," *J. Electron. Imag.*, vol. 26, no. 4, 2017, Art. no. 043015.
[13] A. C. Popescu and H. Farid, ``Exposing digital forgeries in color _lter array interpolated images," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3948_3959, Oct. 2005.
[14] S. Bayram, H. T. Sencar, and N. Memon, ``Classi_cation of digital cameramodels based on demosaicing artifacts," *Digit. Invest.* vol. 5, nos. 1_2, pp. 49_59, 2008.
[15] A. C. Gallagher, ``Detection of linear and cubic interpolation in JPEG compressed images," in *Proc. 2nd Can. Conf. Comput. Robot Vis.*, May 2005, pp. 65_72.
[13] An Improved Algorithm for Digital Image Authentication and Forgery Localization Using Demosaicing Artifacts
NHAN LE AND FLORENT RETRAINT Laboratory of System Modeling and Dependability (LM2S), ICD, CNRS FRE 2019, Troyes University of Technology, 10004 Troyes, France Corresponding author: Nhan Le (nhan.le@utt.fr)

This work was supported by the National Research Agency (ANR) Project DEFACTO under Project ANR-16-DEFA-0002.