Digital authentication in digital images

Dr. Zulkharnain

CAIT, Jazan University

Abstract: *Nowadays it is necessary to post digital images online, for various reasons. These images are hijacked and used in social media. They are of concern because they are edited to suit the nefarious design of hackers. With upcoming generated Artificial intelligence, it has become difficult for common person to understand the fake make of it. These images are thus visually compelling deepfakes.With the use of integrated AI-based modules on dedicated hardware of the camera, this problem has become much more challenging. Similarly, image processors added in the cameras make the difficulty much more complicated. These devices hallucinate the images much more than the original. Hence, there is need of authentication mask creation, created as metadata with each of the image. When that is available, the hallucinated regions can be easily identified, for legal purposes. This paper provides an overview of the current literature.*

Keywords: **AI, deepfakes, Digital Image Forensics, GAN, Digital literacy, IPTC, XMP, EXIF**

1. INTRODUCTION

To check the validity of digital image, a technology called as Digital Image Forensics [1], has been initiated. There is mischief played using Generative Adversarial Networks [2], which create deepfakes. This is a machine-learning framework [3]. This technique generates new data with same statistics as the training set. For example, a series of new pictures can be created based on a real digital picture taken by a camera. It is similar to mimicry.

Using Digital image forensics we can detect fakes and check noise profiles, lens effects, compression pattern, lighting etc., We now presume that images secured from digital camera are no more authentic, because of the latest technologies used in the camera construction. Smart phone cameras use AI modules that hallucinate. The masking done can be thus recovered by metadata, by query.

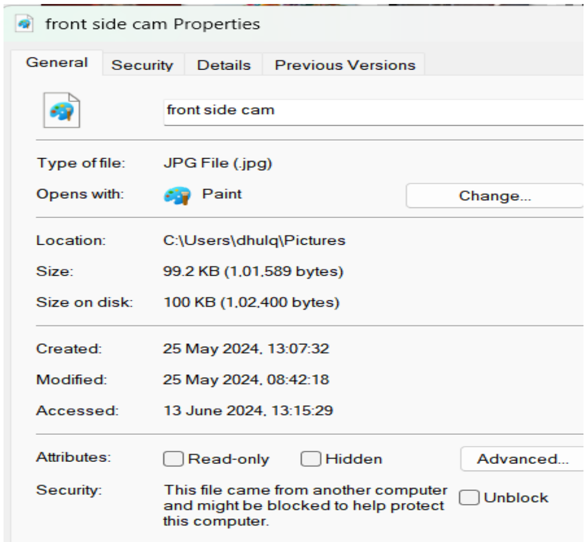
Thus Image Signal Processor [4] used in the camera does modify the image captured like demosaicing, noise removal, white balance, color space transformation, global and local tone mapping, exposure adjustment, sharpening, digital zoom, and final color space encoding. In addition algorithms are used to alter the colors and tones of the image. AI based Neural algorithms can play havoc on the image, thereby generating complete new image. The catch here that is useful in detecting fake, is the fact that generative methods fake in the form of a texture and enhance image details. Digital zooming for instance, is an Image processing technique that may also create a blurry image finally. AI can hallucinate into sharp visually plausible content. If such image is used as evidence can create wrongful result. Most of the latest cameras convert RAW images into Digital Negative. In smart phone camera burst of RAW images can be used to create a single clear photo. Such process creates better noise profiles and higher tonal range. Thus composite RAW image may also have hallucinated content in it.

Thus with image processing there may be question of authenticity. The purpose of this paper is to highlight that issue. A solution for that is to use authentication mask [5], which should be saved as metadata and should be displayed as additional information in the image. Pixel level Authentication [6] is one of the technique used for it. Fake pixels should be available for detection any time. This paper is a suggestive guide that needs further research and practical experimentation further, before commercialization.

2. Metadata:

EXIF stands for Exchangeable Image File Format [7]. It is the standard way of storing metadata in digital image files. It bears all technical information, how the image was created, including time and date, the camera and lens used and also the shooting settings. Similarly International Press Telecommunication Council and Extensible Metadata Platform can also form part of digital photo's data profile. IPTC metadata [8] describes the content of the image and rights associated with it. It also includes copyright status, caption information and keywords as well. XMP [9] is more modern and enables to add descriptive information to an image file. It is also flexible.

When one processes RAW file say in Photoshop [10], the edit details are saved in the sidecar of XMP file, leaving the original RAW file untouched! It is not possible to alter EXIF data recorded. To view the EXIF data in digital image file on a windows PC, we can right click on image file, select properties and click the details tab. Selecting File Info (or its equivalent) enables to look for EXIF data. Following is an example:



front side cam

Type of file: JPG File (.jpg)
Opens with: Paint

Location: C:\Users\dhulq\Pictures
Size: 99.2 KB (1,01,589 bytes)
Size on disk: 100 KB (1,02,400 bytes)

Created: 25 May 2024, 13:07:32
Modified: 25 May 2024, 08:42:18
Accessed: 13 June 2024, 13:15:29

Attributes: □ Read-only □ Hidden
Security: This file came from another computer and might be blocked to help protect this computer. □ Unblock

Fig.1EXIF data example

Before posting images online, some services may strip out embedded metadata for privacy reasons. During post processing and manipulation, such as compositing images EXIF data may be removed.

3. Authentication Process

The first step in authentication is creation of framework. There should be computation and propagation of a mask [11]. This should be carried over to different stages of signal processing. Artificial intelligence can be used in a black box fashion, using pre-trained modules [12]. This is useful if internal developed module cannot be changed. If control exists on AI module design and training, we can easily detect hallucinated pixels, and easily generate authentication mask.

Hybrid signal Mix Processing [13] is commonly used for authentication. Bayer Kernel is used in this such that one is for Blue, one for red and two for green. Thus hallucinated pixels need to be detected, then authentication masking need to be done. Figure 2. Shows the binary authentication process:

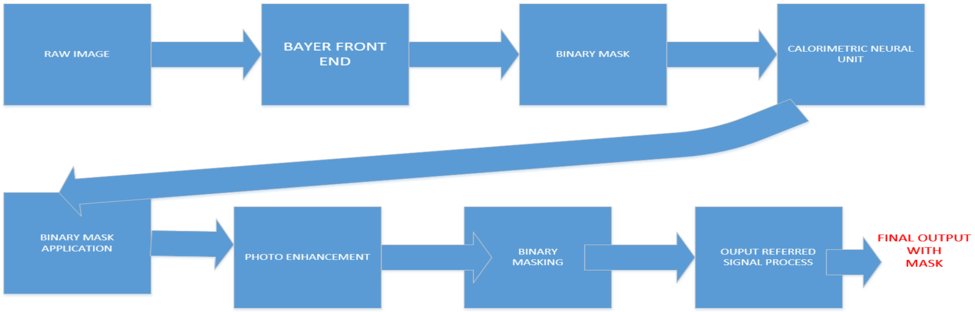


Fig.2 BINARY AUTHENTICATION

Camera Image signal processing is a hybrid process. There are 3 neural blocks and one signal processing block. The output of Bayer front end [14] is de-noised and de-mosaicked having 3 channel RAW-RGB image. The pixels are hallucinated as a magenta color in the mask. The Calorimetric Neural unit applies white balance and color space transforms. This is trained to use reconstruction losses. Thus mask is carried forward. The Photo Enhancement unit combines perpetual and generative losses. It hallucinates the structures in the image. The result is union of magenta and white. The final stage does sharpening and compression, and thus saved as Meta data.

For saving the metadata size, the binary mask can be down sampled and compressed. A 12 MP image requires about 4.5MB storage using JPEG compression. Binary mask for the same comes to about 225KB! The binary mask can also be down sampled to half the resolution making the storage equal to say 80KB! Using steganography, tampering with mask can be prevented.

4. CONCLUSION:

The main idea emphasized in this article, is that the image captured by any modern digital camera cannot be considered as completely original as the natural scene. This is because of many alterations that are possible in the image processing. Above all, use of Artificial Intelligence inbuilt in modern digital cameras have added more complexity in the authenticity of the image captured. Today's modern digital cameras use AI training using the perpetual and generative losses, thereby hallucinating the scene from the original. Thus there is no guarantee that the final output of the image is completely real in life. This is almost overseen in today's digital forensics.

Thus Emphasis is made to adopt some strategies in image signal processing inside the camera, so as to have validation possible, if authenticity is at question. The use of capture-time metadata in the output image solves the problem. Metadata as spatial mask can identify pixels modified by AI hallucination, making the authenticity process easier.

5. REFERENCES

1. V. I and S. S, "Fine – Grained Forgery Localization in Images Using CNN - SVM Approach," 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), Chennai, India, 2024, pp. 1-5, doi: 10.1109/ADICS58448.2024.10533553. keywords: {Support vector machines; Location awareness; Image segmentation;

2. M. Zhang, C. Guo, Y. Zhang, H. Liu and W. Li, "GCCD: A Generative Cross-domain Change Detection Network," in IEEE Transactions on Geoscience and Remote Sensing, doi: 10.1109/TGRS.2024.3413542.

3. M. Unnisa and V. Ganesan, "An Improved XGBoost Classifier for Micro Expression Recognition using Hybrid Optimization Algorithm," 2024 International Conference on

Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 2024, pp. 1-6, doi: 10.1109/IC3IoT60841.2024.10550313

4. Y. Zhong et al., "Unsupervised Fusion of Misaligned PAT and MRI Images via Mutually Reinforcing Cross-Modality Image Generation and Registration," in IEEE Transactions on Medical Imaging, vol. 43, no. 5, pp. 1702-1714, May 2024, doi: 10.1109/TMI.2023.3347511.

5. R. A.C, M. B, P. Muralapur and V. H, "Implementation of Face Feature Algorithms for Authentication of a Person (IFFAP)," 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India, 2024, pp. 1-8, doi: 10.1109/ICDCECE60827.2024.10548337

6. N. Liu and R. Xu, "Image Robust Watermarking Based on Improved Invariant Feature Matrix and Chaotic Map," 2023 IEEE 17th International Conference on Anti-counterfeiting, Security, and Identification (ASID), Xiamen, China, 2023, pp. 50-56, doi: 10.1109/ASID60355.2023.10426435.

7. M. Ölvecký and M. Host'ovecký, "Digital image forensics using EXIF data of digital evidence," 2021 19th International Conference on Emerging eLearning Technologies and Applications (ICETA), Košice, Slovakia, 2021, pp. 282-286.

8. C. Liu and Z. Wei, "Multi-feature Method: An Integrated Content Based Image Retrieval System," 2011 2nd International Symposium on Intelligence Information Processing and Trusted Computing, Wuhan, China, 2011, pp. 43-46.

9. J. G. Park, S. Liu and J. H. Hong, "XMP: A Cross-Attention Multi-Scale Performer for File Fragment Classification," ICASSP 2024 - 2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Seoul, Korea, Republic of, 2024, pp. 4505-4509, doi: 10.1109/ICASSP48485.2024.10447626.

10. M. Maddel, M. Kakarla, S. D, G. R. K, S. Amol Ubale and M. Kumar A S, "Novel Approaches in Machine Learning for Enhanced Facial Recognition Systems," 2024 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2024, pp. 49-56, doi: 10.1109/ICICT60155.2024.10544442.

11. M. Li, J. Xu, T. J. Cui and L. Li, "Microwave Reconstruction of 3D Human Facial Landmarks Using a Programmable Metasurface," in IEEE Antennas and Wireless Propagation Letters, doi: 10.1109/LAWP.2024.3403686.

12. A. Farhad and J. -Y. Pyun, "AI-ERA: Artificial Intelligence-Empowered Resource Allocation for LoRa-Enabled IoT Applications," in IEEE Transactions on Industrial Informatics, vol. 19, no. 12, pp. 11640-11652, Dec. 2023, doi: 10.1109/TII.2023.3248074.

13. H. Wu, S. He, G. Ren, R. Yang, Y. Zhao and L. Wu, "Instantaneous Hybrid Signal Separation Based on CANDECOMP/PARAFAC Decomposition with Accelerated Proximal Gradient Method," 2022 6th International Conference on Imaging, Signal Processing and Communications (ICISPC), Kumamoto, Japan, 2022, pp. 89-93, doi: 10.1109/ICISPC57208.2022.00024. keywords: {Gradient methods;Analytical models;Tensors;Signal processing algorithms;Imaging;Blind source separation;Signal resolution;instantaneous hybrid model;blind signal Separation;Candecomp/parafac decomposition},

14. L. Zhiyong, Y. Weihua and D. Xiance, "The Analog Front End of Ultra-High Resolution CCD Design Based on AD9920A," 2015 8th International Conference on Intelligent Computation Technology and Automation (ICICTA), Nanchang, China, 2015, pp. 921-924, doi: 10.1109/ICICTA.2015.234.