BOOK CHAPTER | Do Not Touch

Digital Multimedia Tampering Detection for Forensics Analysis

Bernard Mainoo
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: mainoobernard12@gmail.com
Phone: +233549282439

ABSTRACT

In the virtual multimedia era, digital forensics is turning into a rising location of studies way to the huge quantity of picture and video documents generated. Ensuring the integrity of such media is of top-notch significance in lots of situations. This mission has end up extra complex, particularly with the development of symmetrical and asymmetrical community systems which make their authenticity tough. Consequently, it's far definitely vital to find out all feasible modes of manipulation through the improvement of latest forensics detector tools. For example, the symmetry and asymmetry inconsistencies associated with visible characteristic residences are capacity while carried out at a couple of scales and locations. We discover right here this subject matter and advocate a comprehensible smooth taxonomy and a deep assessment of the brand-new studies regarding multimedia forgery detection. Then, an in-intensity dialogue and destiny guidelines for similarly research are provided. This painting gives a possibility for researchers to apprehend the cutting-edge lively subject and to assist them broaden and examine their very own picture/video forensics approaches.

Keywords: Digital forensics, Multimedia tampering, Image/video processing, Watermarking, pattern recognition, Active/Passive Tampering Detection

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Bernard Mainoo (2022): Digital Multimedia Tampering Detection for Forensics Analysis SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 81-90 www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P14

1. INTRODUCTION

Multimedia forensics is one of the important research contents in the field of information security. It is mainly used in judicial forensics, criminal investigation and forensics, and is one of the key technologies in the fields of electronic evidence identification. Facebook, Twitter, YouTube and Instagram are the maximum famous on line web sites allowing humans to add

and proportion billions of pictures. Nowadays, social media web sites are gambling a greater crucial position in each day life. They assist customers to specific themselves, make new friendships and proportion their pastimes and thoughts with others.

The 8th annual report "social media withinside the Middle East: 2019 in review" (Radcliffe & Abuhmaid, 2019. 2020, in press.) states that social media is still the pinnacle information supply for Arab humans and it's far crucial for his or her lives. "More than seven out of ten Arabs use Facebook, and each day, 9 out of ten younger Arabs use as a minimum one social media channel" (http://www.mideastmedia.org/survey/2019/chapter/social-media/ (accessed on 4 April 2020). , 2019). Active social media customers in Saudi Arabia are developing rapidly. Over 38% of the Saudi populace are lively customers of social media. Nowadays, virtual multimedia forensics has turn out to be a rising studies subject. It has obtained sizeable interest aiming at figuring out the beginning and ability authenticity of virtual media.

For instance, photograph authenticity is crucial in lots of social areas, consisting of: withinside the scientific subject, physicians make crucial selections primarily based totally on virtual photos; in law-reinforcement organizations and in courtrooms, the trustworthiness of pics has a critical position in which they might be used as proof. In today's virtual age, the short improvement of effective and low-fee enhancing equipment facilitate the manipulation of virtual media consisting of including or eliminating components and items from photos and movies leaving very little signal of manipulation. Subsequently, this manipulated media will unfold fast and might have severe consequences, on each a countrywide and a worldwide scale. With the fast advances of excessive-decision virtual cameras and the supply of state-of-the-art editing software program, along with Adobe Photoshop, Pixar and Corel PaintShop, you can without difficulty adjust the content material of images without leaving any apparent perceptual signal of manipulation.

Figure 1. A photograph of an art project in 2014 in Germany that got shared on Facebook in 2020 to falsely claim that the people in this photo were coronavirus victims in China.

Unfortunately, they may be blurring the road among actual and faked multimedia content material. They also can result in rapid-developing troubles as lowering the trustworthiness on many actual programs. Tampering will become a fear for governments, public and personal organizations and for individuals' personal lives.

Hence, the sector is immersed in an extreme venture to deal with straight away the hassle of spreading fraudulent images and motion pictures. As an example, in January 2020, thousands of Facebook posts showed a fake photo (taken from an art project in 2014 in Germany) falsely claiming that the people in this picture were victims of coronaviruses in China (see Figure 1). A large number of rumors in the form of images and video clips circulating on the web regarding the virus COVID-19 makes the task of distinguishing between fake and true stories and news increasingly difficult. Therefore, the World Health Organization (WHO) decided to warn people with a list of twenty false stories about coronavirus.

1.1 Background to the Study

Nowadays, digital sources are increasingly used to make necessary decisions. The essential hassle is that it will become tough to hit upon manipulations for the reason that many present state-of-the-art enhancing software programs shape an extreme hazard to the safety. Hence, to deal with this hassle, it's miles important to plot new effective strategies that assist one to determine at the truthfulness of a given medium (picture or video). Consequently, virtual multimedia forensics and research has emerged as one of the maximum vital safety fields. Digital multimedia forensics combines technology, technique and programs that allows you to offer believe in one-of-a-kind media and to discover virtual evidences earlier than, whilst and after a cybernetic safety assault has occurred.

In particular, the lively virtual forensics (begins off evolved after the detection of incident and earlier than the incident closure) offers with the stay facts acquisition that allows you to make certain that applicable and admissible stay proof is available. The stay identification, acquisition, maintenance and reaction steps are crucial to make certain green facts collection. The stay facts collecting from networks reasons numerous problems like facts volume, facts interdependencies, and community throughput speed. One greater hard hassle is that of making sure the reliability of evidences that should be taken into consideration with excessive precedence in any judicial inquiry. The reliability offers basically with the development of the authenticity and veracity of the proof. These standards should now no longer be questionable withinside the courtroom docket that allows you to preserve the proof admissibility.

(a) Original image (b) tampered image

Figure 2. Example of digital tampering image.

Any virtual facts forgery withinside the gathered facts can also additionally result in incorrect research finishing and reason evidences to be discredited withinside the court of law. More typically, when you consider that new crime and crook profiling strategies are an increasing number of primarily based totally on mining the wealthy multimodal virtual facts, their fashions and profiling might be additionally erroneous if those assets are altered or fabricated.

Today's virtual forensics has come to be an rising studies discipline because of the massive quantity of generated multimedia files. Digital forensics has obtained tremendous attention, for each governmental and non-governmental businesses and departments, aiming at figuring out the beginning and potential authenticity of virtual media. An example of image tampering is depicted in Figure 2 where a Malaysian politician (Jeffrey Wong Su) is facing eviction from his party after faking snaps showing he was seen being knighted by the Queen of England in July 2010.

2. RELATED LITERATURE

Image (or video) tampering may be described because the motion of "including or disposing of vital capabilities from a picture (or video) without leaving any apparent strains of tampering" (Fridrich, A.J.; Soukal, B.D.; Lukáš, A.J.;, 6–8 August 2003). Generally, the maximum not unusual place carried out tampering operations are: (i) deleting (or hiding) a area withinside the picture, (ii) including a brand new item into the picture, and (iii) misrepresenting the picture statistics (e.g., resizing an item withinside the picture). Despite this hassle of virtual forensics that has attracted a good deal attention, however, maximum studies on this region nonetheless lacks rigorous and strong outcomes and discussions. In addition, numerous strategies have obvious boundaries and are tough to be optimally employed.

In the statistics age, with the improvement of numerous virtual with the popularization and fast improvement of media recording gadgets (along with voice recorders, virtual cameras, virtual video cameras, clever phones, etc.), the recording and garage of statistics now no longer is based totally on text, and virtual media statistics along with audio, photos and video has step by step come to be the mainstream statistics carrier. At the identical time, with the fast improvement of recent technology along with effective and easy-to- perform media enhancing gear, and social networks with statistics sharing functions, many media facts are associated with the source, integrity, authenticity and different safety. The hassle is turning into an increasing number of extreme.

The extended unfold of processed/edited/tampered media statistics thru social networks has an extreme effect on social safety, now no longer most effective disrupting people's day by day lives, however additionally severely threatening the harmonious and solid improvement of society. Active Tampering Detection: Active strategies, recognized additionally as facts hiding strategies, are derived from virtual watermarking discipline. Digital watermarking and signature gear make certain facts authenticity, like stopping the unlawful copying of photos from the Internet (Celik, Sharma, Saber, & Tekalp, 2002) (Meerwald & Uhl, 2001;) (Hartung & Kutter, 1999).

The method of watermarking is primarily based totally on inserting (embedding) a secondary fact (virtual watermark) into a picture or video. Although many lively strategies had been posted withinside the literature, they gift many troubles along with: (i) they may be impractical to embed virtual watermarks in all photos, and consequently, virtual watermarking is restricted in its potential to make certain authenticity. (ii) Not all gadgets embed a virtual watermark, and those do now no longer like the usage of gadgets containing an embedded watermark. (iii) In the case of a compressed picture, fragile watermarks may be without difficulty destroyed.

On the alternative hand, there are tens of thousands and thousands of virtual photos and motion pictures at the net without a virtual signature or watermark, and consequently it isn't realistic to undertake lively strategies to study the authentication of unmarked virtual photos. Passive Tampering Detection: Passive strategies paintings with none previous statistics at the real facts. They can hit upon manipulation via way of means of exploiting the content material-primarily based totally capabilities of photos and motion pictures (i.e., the statistical visible statistics). Verifying the integrity of virtual media and detecting strains of tampering with out the usage of any pre–embedded statistics has established to be powerful for virtual forensics (just like the case of scene crime analysis). The integrity may be proven passively that allows you to pick out strains like cloning, sampling, re-sampling, and inconsistencies in lighting. To carry out passive tampering detection, numerous standards should be taken into consideration that allows you to expand sturdy multimedia forensic gear along with pixel-primarily based totally, physically-primarily based totally, camera-primarily based totally, format-primarily based totally, and geometric-primarily based totally gear (Farid, 2009).

Fig 3: How to Stop fake News
Source; https://repository.ifla.org/handle/123456789/167

3. RESEARCH GAPS/FINDINGS

Despite the reality that a few research was proposed to address copy-pass tampering detection and that they have got mentioned promising outcomes, lots of them do now no longer gain excessive overall performance. We summarize on this segment the principal drawbacks of numerous associated strategies.

As photograph tampering detection is a difficult hassle, the computational time is incredibly excessive for block-primarily based totally strategies, given that each one pixel or extracted functions should be tested in keeping with block. Sometimes, huge-scaling distortion is undetectable. In contrast, the characteristic-primarily based totally strategies, have much less computational complexity.

Thus, fixing the trade-off speed–accuracy is now a hard hassle.

- Determining the best and optimal feature extraction algorithm is not easy and final results are highly dependent on the used technique, which may be a key factor-primarily based totally or block-primarily based totally technique.
- In many cases, the existing methods in the literature fail to hit upon especially small reproduction regions (resulting from copy-pass operation), and consequently the accuracy could be very low.
- Some strategies fail to discover more than one duplicated region.
- In general, key factor-primarily based totally strategies cannot cope with the smoothing tampering.
- Sometimes, block-primarily based totally strategies are greater correct than key factor-primarily based totally ones in figuring out the shapes of duplicated regions.
- Both the important thing factor functions and block-primarily based totally matching have problems in correctly detecting the smoothed form region.
- It is just too tough that simply one unmarried photograph tampering detection technique or set of rules can display totally solid images. Thus, related to numerous methodologies and capabilities is noticeably recommended.
- Some tampering detectors can be misled through counter-intrusive procedures created through counterfeiting.

To cope with the above obstacles, researchers made a whole lot of attempts to keep away from the weak spot of every technique on my own and to take gain in their electricity together (Chihaoui, Bourouis, & Hamrouni, 17-19 March, 2014) Most of the newly advanced thoughts attention on combining each key factor-primarily based totally functions and block-primarily based totally matching strategies into the equal hybrid framework. For instance, a passive detection with a hybrid technique is proposed in (Ardizzone, Bruno, & Mazzola, 2015), primarily based totally on key factors functions evaluation for triangle shapes instead of fashionable blocks. In this case, items are characterized through a linked triangle. Detector strategies like SIFT and Harris are implemented for nearby key factors functions extraction.

Combining numerous detectors primarily based totally on fusion policies is a promising method and permits using complementary homes to cope with a difficult hassle like multimedia tampering detection. Conventional fusion strategies can fail to absolutely address this challenge, considering that they regularly do now no longer recall a few homes just like the spatio dependence (neighboring pixels) and the intrinsic homes of the photograph. These homes may be taken into consideration as essential clues and evidences for virtual forensics. Another promising painting handling this issue thru a decision-making technique method turned into posted in (Ferreira, et al., 2016).

Indeed, authors tested the drawbacks of conventional fusing strategies through growing a powerful behavior information area representation (BKS) for copy-pass modelling and detection. Recently, a hybrid technique turned into advanced that exploits nearby visible functions (Soni, Das, & Thounaojam, 2019) to enhance block-primarily based totally copy-pass tampering detection.

4. CONCLUSION, RECOMMENDATION FOR POLICY AND PRACTICES AND DIRECTION FOR FUTURE WORKS

In summary, numerous strategies and research in literature were advanced to cope with the difficult hassle of virtual multimedia tampering detection and lots of them have mentioned promising outcomes, many of those techniques are commonly much less powerful, specifically while handling homogeneous regions and while we need to preserve robustness to rotation, scaling, blurring, noisy images, and compression with loss. It is likewise essential to mention that in spite of the significance of the web issue, now no longer all of the proposed video counterfeit detection strategiespaintings successfully in an internet way and lots of them have obstacles while coping with a huge range of video sequences (massive facts). In addition, it's far essential that in addition studies research for the temporal courting assets among frames so that it will boom the spatio-temporal forgery detection.

This goal might be completed if one considers the fulfillment of superior and present-day strategies derived from pc vision, facts mining and gadget getting to know fields. For example, statistical getting to know techniques permit the green modelling of huge-scale of records after which they might be an awesome opportunity for each photograph and video tampering detection. Regarding the complexity of extracting numerous functions from the video, this problem may be tackled through adopting characteristic choice procedures. It is really well worth noting that for virtual tampering detection, offering greater records may want to enhance the anticipated outcomes. Indeed, precise items are prominent and characterized on the premise in their traits (form, color, texture). Then, thinking about the reality that a few traits are greater applicable than others which can be called “informative descriptors”, it will likely be greater realistic to apply simplest those informative descriptors rather than making use of all viable descriptors.

The traits may be simplest noise, therefore now no longer powerful to explain correctly the favored items. Selecting simplest the maximum applicable spatio-temporal functions is especially essential and performs a number one function in enhancing the accuracy of manipulation detection algorithms and reducing the computational time. Addressing those troubles will absolutely assist gain excessive overall performance in phrases of real-time tampering detection. In addition, exploring those challenges could open the door to greater powerful contributions.

5. IMPLICATIONS FOR ONLINE SAFETY AND CYBERCRIME PROSECUTION/PREVENTION IN AFRICA

As only about 20% of States have the basic legal framework in place, the situation in Africa regarding legislation on cybercrime and electronic evidence is not satisfactory. On the positive side, it is encouraging that reforms are under underway in many States, even though in some cases, draft laws have been under discussion for several years with little progress.

A number of (draft) laws contain provisions that create risks to the freedom of expression and other fundamental rights, in particular where offences are vaguely defined and conditions and safeguards are weak or missing. Examples are the criminalization of the "creation of sites with a view to disseminating ideas and programmes contrary to public order or morality", "broadcasting information to mislead security forces", "publication of false information" and similar. This not only affects the rights of individuals and restricts media freedoms but also undermines trust and hinders international and public/private cooperation.

Procedural law powers are not always precisely defined and safeguards may be lacking. For example, a law allows for orders to compel the production of content data without court order, or a police officer can carry out searches or seizures of computers without court order. This may be contrary to rule of law requirements, namely, that investigative powers that interfere with the rights of individuals must be prescribed precisely, be subject to guarantees against abuse, be necessary and proportionate and must allow for effective remedies.

On the other hand, data protection regulations are increasingly being adopted in African States, often in conjunction with laws on cybercrime. This creates additional safeguards to the rights of individuals. Mauritius, Morocco and Senegal are not only Parties or have been invited to accede to the Budapest Convention on Cybercrime, but have also requested accession to the Data Protection Convention 108 of the Council of Europe.16 The African Union Convention on Cyber Security and Personal Data Protection of 2014 also contains an important chapter on the protection of personal data.

Joining an international treaty such as the Budapest Convention on Cybercrime not only provides a legal framework for international cooperation but instills confidence and trust that such cooperation has a solid foundation in domestic law. This also applies to cooperation between criminal justice authorities and private sector service providers. Mauritius was one of the first countries of Africa to adopt comprehensive legislation on cybercrime in 2003, and in 2014 was the first African State to become a Party to the Budapest Convention on Cybercrime. South Africa signed this treaty in 2001 and the additional Protocol on Xenophobia and Racism in 2008 but has not yet ratified these instruments. Morocco and Senegal have been invited to accede and it is expected that both will become Parties in the course of 2016.

These countries participate in the Cybercrime Convention Committee17 and are priority countries for capacity building. Several other African countries have expressed their political commitment to join and implement this Convention. Limited capacities of law enforcement, prosecutors and the judiciary is the main impediment to an effective criminal justice response to cybercrime and other offences involving electronic evidence not only in Africa but in most countries around the world.18 The adoption of legislation by African States needs to be accompanied by capacity building programmes.
The Council of Europe – often jointly with the European Union – is providing support to those African countries that have requested accession to the Budapest Convention, including in the training of criminal justice authorities.

6. CONCLUSIONS

The current state of legislation on cybercrime and electronic evidence in Africa is not satisfactory. By April 2016, only 20% of countries seemed to have the minimum legislation in place. On the positive side, some African countries represent examples of good practice, the African Union Convention on Cyber Security and Personal Data Protection of 2014 should help create a political momentum for stronger legislation and the Budapest Convention on Cybercrime may serve as a guideline for comprehensive legislation that reconciles the need for an effective criminal justice response with the need to meet human rights and rule of law requirements. Accession to this treaty will facilitate cooperation between African countries and criminal justice authorities of countries in other regions of the world.

Efforts currently underway in a number of African countries to reform domestic legislation should be supported and carried through. Over-criminalization – in particular with regard to content andspeech – should be avoided, and conditions and safeguards limiting law enforcement powers should be established. The enactment of data protection legislation should be encouraged. The adoption of legislation should go hand in hand with the improvement of criminal justice capacities, ranging from the establishment of specialized units for cybercrime investigations and computer forensics, to the strengthening law enforcement and judicial training, interagency cooperation, financial investigations, child protection, public/private cooperation and international cooperation. The challenge may seem immense, but as indicated at the outset: governments cannot remain passive; they have the obligation to protect society and the right of individuals and to create the conditions for realizing the human development potential of information technology.

REFERENCES

1. Radcliffe, D.; Abuhmaid, H. Social Media in the Middle East: 2019. 2020, https://www.techradar.com/news/twitter-announces-expansion-to-mena-video-contentwith- over-16-partnerships (accessed on 4 April 2020).
2. Available online: https://www.statista.com/statistics/315405/snapchat-user-region-distribution/ (accessed on 4 April 2020).
3. Available online: http://www.mideastmedia.org/survey/2019/chapter/social-media/ (accessed on 4 April 2020).
4. Available online: https://www.thinkwithgoogle.com/intl/en-145/getting-know-youtubes-biggest-middleeastern- audience-millennials/ (accessed on 4 April 2020).
5. Fridrich, A.J.; Soukal, B.D.; Lukáš, A.J. Detection of copy-move forgery in digital images. In Proceedings of the Digital Forensic Research Workshop, Cleveland, OH, USA, 6–8 August 2003.
6. Celik, M.U.; Sharma, G.; Saber, E.; Tekalp, A.M. Hierarchical watermarking for secure image authentication with localization. IEEE Trans. Image Process. 2002, 11, 585–595. [CrossRef] [PubMed]
7. Meerwald, P.; Uhl, A. Survey of wavelet-domain watermarking algorithms. In Security and Watermarking of Multimedia Contents III; International Society for Optics and Photonics: Bellingham, WA, USA, 2001; pp. 505– 516.
8. Hartung, F.; Kutter, M. Multimedia watermarking techniques. Proc. IEEE 1999, 87, 1079–1107. [CrossRef]
9. Farid, H. Image forgery detection. IEEE Signal Process. Mag. 2009, 26, 16–25. [CrossRef]
10. Chihaoui, T.; Bourouis, S.; Hamrouni, K. Copy-move image forgery detection based on SIFT descriptors and SVD-matching. In Proceedings of the 2014 1st International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Sousse, Tunisia, 17–19 March 2014; pp. 125–129.
11. Ardizzone, E.; Bruno, A.; Mazzola, G. Copy-Move Forgery Detection by Matching Triangles of Keypoints. IEEE Trans. Inf. Forensics Secur. 2015, 10, 2084–2094. [CrossRef]
12. Ferreira, A.; Felipussi, S.C.; Alfaro, C.; Fonseca, P.; Vargas-Munoz, J.E.; dos Santos, J.A.; Rocha, A. Behavior Knowledge Space-Based Fusion for Copy-Move Forgery Detection. IEEE Trans. Image Process. 2016, 25, 4729–4742. [CrossRef]
13. Soni, B.; Das, P.K.; Thounaojam, D.M. Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features. J. Inf. Secur. Appl. 2019, 45, 44–51. [CrossRef]
14. For analysis of the state of the protection of freedom of expression on the Internet in European countries see page 47 ff of http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680646af8
15. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
16. http://www.coe.int/en/web/cybercrime/tcy
17. http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e6
18. See the GLACY and GLACY+ projects on Global Action on Cybercrime. http://www.coe.int/en/web/cybercrime/capacity-building-programmes