Article Review: Journal of Cyber Security

Deep Learning Based Image Forgery Detection Methods by Liang Xiu-jian and Sun He

By: Sarah Vakos

Old Dominion University

Dr. Leigh Armistead CYSE 201S 23181

Deep Learning Based Image Forgery Detection Methods by Liang Xiu-jian and Sun He

The topic of this article relates to a few of the social science principles including determinism, ethical neutrality and objectivity. The first principle of social science is determinism, and it is defined as the reason why someone acts or conducts themselves as, is because of and or affected by previous events. Let's go back to the article, "Deep Learning Based Image Forgery Detection Methods" by Liang Xiu-jian and Sun He, why would someone want to alter the content of a digital image? Some reason as to why an individual would change an image might be to make someone look bad, to make a joke out of the digital image, to mislead or persuade viewers. The hidden dangers of image security follow, which will undoubtedly bring negative effects to all aspects of society, resulting in a serious crisis of trust (Xiu-jian & He, 2022).

The second principle of social science that I will go over is, ethical neutrality. Ethical neutrality is defined as what scientists do while conducting research and that is to stick to ethical standards. Ethical neutrality protects the individual's rights that are being studied on and to analytically and accurately study problems. Should the use of digital image editing be illegal or not available to all users on the internet? Should digital image editing only be available to educational and governmental organizations? These tampered images have posed a serious threat to personal privacy, social order, and national security. Therefore, detecting and locating tampered areas in images has important practical significance, and has become an important research topic in the field of multimedia information security. (Xiu-jian & He, 2022). By improving the recognition of image authenticity and finding the outlines of digital image tampering will secure digital images and the individuals, if any, in the images from being photoshopped into another image, for example.

The third principle of social science that I will go over is, objectivity. Objectivity is defined as, researchers studying issues in a non-bias manner. By not assuming anything when first observing something and being open-minded to other possibilities is the correct way of having objectivity. In the article, “Deep Learning Based Image Forgery Detection Methods” by Liang Xiu-jian and Sun He, a question to consider is, how do you find the original image that an individual got their hands on to copy a part of and use for the creation of another digital image? Is their technology out their available today that can detect the part of an edited image that was stolen from a copyrighted image? The forensic technology of digital image tampering mainly judges whether the content of the image is real after the image is generated from the imaging device, whether the image has been tampered with, and what kind of device is it generated from (Xiu-jian & He, 2022). By using the latest image forensics technology out today can help identify if an image has been altered or not.

Research methods used in this article are field research by applying deep learning methods to the field of image forensics. The research method used two different tasks which are the tampering method detection and location of tampered area. They found that the conventional computer vision field has three big differences; the recognition target is different, the statistical features are different, and post-processing effects are different. Researchers can then output the content after locating the tampered area in the way of bounding box and or in the form of binary mask.

Victim precipitation is a concept from class that might be the source of image editing in the sense of, if an individual posts a picture of him/herself on their social media platform, then are they giving others the opportunity to copy or edit the picture to then make him/her look bad and posting it back on the same social media platform for the individual to see and be

humiliated? By giving others on social media information about yourself, whether it be a picture or a post containing what you are currently doing or are interested in then you are giving hackers motivation and inspiration to go off of.

The person copying and or editing the picture of another to then make them look bad and post it back on a social media platform for more to see can be called a Machiavellian. A Machiavellian is someone who looks at others maybe on social media as items to be controlled in pursuit of his/her goals through premeditated deception. The same person might also have narcissism as a characteristic along with Machiavellian because they are self-centered and only care about themselves. Humiliating others on social media by editing images of them, they show lack of empathy for others, they are considered selfish because they don't care about others along with their feelings and how they are being used on social media for a laugh.

Victim blaming is another concept linked with victim precipitation. If we take my example in the previous paragraph of victim precipitation, those who laugh or share the content of what someone edited to make an individual look bad from the picture they posted, then those who fall for the edited image and continue to show their friends are all involved in victim blaming. Those who report the content are not victim blaming but trying to help the individual who is being made fun of by taking the post down permanently.

Groups of people or marginalized groups who might be vulnerable to image editing are those who can't get on social media platforms because they don't have internet access might be the homeless or those living in poverty. Senior citizens are another group of people that are vulnerable to image editing, unfortunately, since they wouldn't have a clue if a picture of them might be trending on the internet, unless someone told them.

In order to reduce image editing and those who pride on their work to make fun of others, we all need to be aware of what we are posting and who can see it. In other words, be aware of who you are friends with on social media and if your account is public or not. Before posting a picture of anything or anyone make sure the privacy is set in order to limit the amount of people seeing the content. Do not add anyone that you do not know because it is not safe. Before posting a picture of someone other than yourself make sure you have permission to because of how easy image editing is these days.

References

Xiu-jian, L., & He, S. (2022). Deep Learning Based Image Forgery Detection Methods. *Journal of Cyber Security*, *4*(2), 119–133. https://doi.org/10.32604/jcs.2022.032915