Forensic Identification of the source of the morphed image: A case study on serious female disgrace.

Tilak Raj[1], Dr. Manish Malhotra[2]*, Rajat Choudhary[3]

1. Scientist 'B' (Physics), Central Forensic Science Laboratory, Bhopal
2. Corresponding author**:** Scientist 'B' (Physics), Central Forensic Science Laboratory, Bhopal*, *malhotraforensics@gmail.com*.
3. Scientist 'B' (Documents), Central Forensic Science Laboratory, Bhopal

To Cite this Article

Tilak Raj[1] |Dr.ManishMalhotra[2]| Rajat Choudhary[3],**"Forensic Identification of the source of the morphed image: A case study on serious female disgrace."** *Journal of Science and Technology, Vol.08, Issue 10, - Oct 2023, pp27-31*

Article Info

Received: 20-09-2023 Revised: 30-09-2023 Accepted: 10-10-2023 Published: 20-10-2023

Abstract:

The paradigm of the nature and means of functioning of crimes involving female humiliation has evolved as a result of advancements in digital image processing tools and techniques. Using digital image acquisition and transposition technology, altered images are produced that are closer to perfection. By employing various image enhancement techniques on suspected parts of the digital image and doing a pixel-by-pixel analysis of the observations obtained there by an expert in processing images, you can detect editing or morphing anomalies. In this case study, the authors provided an in-depth review of a morphing image and obtained proof that the image was taken from a website. Following website exploration, the source image was located using morphological criteria. The source image that was transformed and recognized contained the same quantization for the horizontal and vertical resolution, measured in DPI (dots per inch), and bit depth.

Keywords: *forensic, image, image manipulation, morphing.*

Introduction:

In today's digital age, advancements in technology have made image manipulation increasingly prevalent[1]. This raises concerns about the potential misuse of manipulated images for criminal activities such as disseminating false information, destroying evidence, or denying facts. This article explores the concept of image manipulation detection using forensic methodology, with a focus on the detection of morphed images. Image morphing is the process of combining or transforming parts of two images to create a new image that appears seamless and authentic. The ability to generate or transform images with minimal traces of manipulation using readily available image editing tools has made it difficult to identify manipulated images[2]. However, forensic experts have developed robust techniques to detect and analyze these manipulations, enabling the detection of even the most sophisticated morphed images[3]. To combat this situation, researchers have developed a set of digital forensic techniques over the last decade to authenticate digital media content[4]. Some of the commonly used techniques in image manipulation detection include analyzing metadata, examining pixel-level inconsistencies, and comparing visual similarities between images. One interesting challenge in image forensics is the detection of manipulated images and determining whether an image has been edited or not [5].

This article explores the various aspects of image manipulation detection and highlights the significance of this methodology in digital forensic investigation and analysis. Image morphing is the process of interjecting some parts between two images to create a new image that looks like a perfectly unified image of two input images[6]. The process of image morphing has several steps, viz., subdivision of initial and target images into geometrical shapes, creation of mapping between the shapes, i.e., one shape in the initial image must correspond to one shape in the target image, individually morphing of each shape, and combining all shapes into one image [7]. Due to recent advancements in the areas of image processing, image acquisition, and image transposition technology, the images created look like unedited real images. Usually, the online images posted on social media platforms by young girls and women are misused to create morphed images. The online criminals humiliate the females by various means, such as blackmailing or creating fake profiles for sex chat, pornographic content, nude pictures, etc., which ultimately damage our social lives and cause serious emotional trauma. It is utmost important to take every possible mandatory measure that protects us from being the victims of such offenses. Some of them are: use a strong login password; use two-factor authentication; enable security and privacy features; never share personal images with the public on social media platforms; use a watermark while sharing images; save all available evidence about the incident; seek the help of trusted friends and family; report the incident on a social media help center; register a complaint online at www.cybercrime.gov.in or offline at your nearest police station.

Brief of the case:

In this instance, the victim's husband reported the incident to the police after receiving a threat to post a modified pornographic image of his wife on social media from an unidentified sender. In response, the investigating authorities seized the mobile phone of the husband and forwarded the same to the Central Forensic Science Laboratory, Bhopal, after the completion of necessary procedures and fulfilling protocols for the extraction of relevant data as well as to determine the authenticity of the questioned pornographic images stated to be of the victim lady.

The case exhibit (mobile phone) was examined for extraction of the data contained therein and to retrieve the relevant image files for further examination pertaining to authenticity.

As a result of the digital forensic examination of the mobile phone, two obscene photographs, prima facie appearing to be of the victim lady, were successfully retrieved.

Retrieval of obscene images:

The mobile phone (Make: Apple iPhone, Model: A1529) was forensically examined using the Universal Forensic Extraction Device (UFED) Touch 2, version 7.1. The WhatsApp chats between complainant and accused, extracted from the mobile device, were explored, and two obscene or pornographic images of the victim were retrieved (Figure 1).

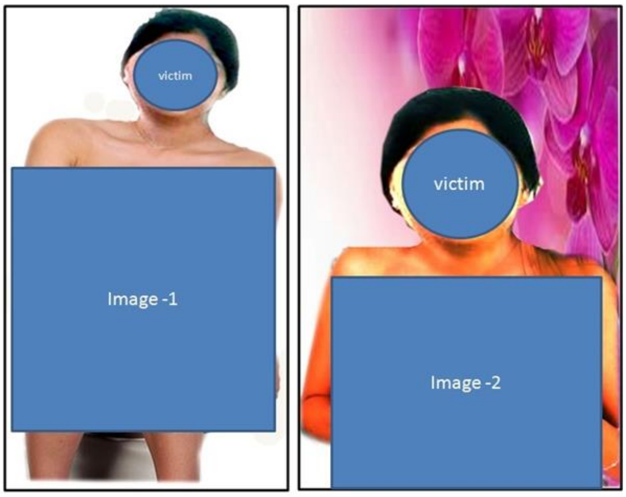

Figure 1: Images recovered from the complainant's mobile phone

Examination of retrieved images:

The suspected images were examined for their EXIF information first, and the images showed signs of editing in their respective EXIF information, showing that the images retrieved were manipulated using some image editing software (Adobe Photoshop being a high probability).

Further, software for image processing was used to look over the retrieved obscene images. The suspicious editing spots were identified and examined. In the modified sections, it was possible to see evidence of cropping and retouching as well as abrupt changes in the RGB value, hue, saturation, etc. (Figure2)

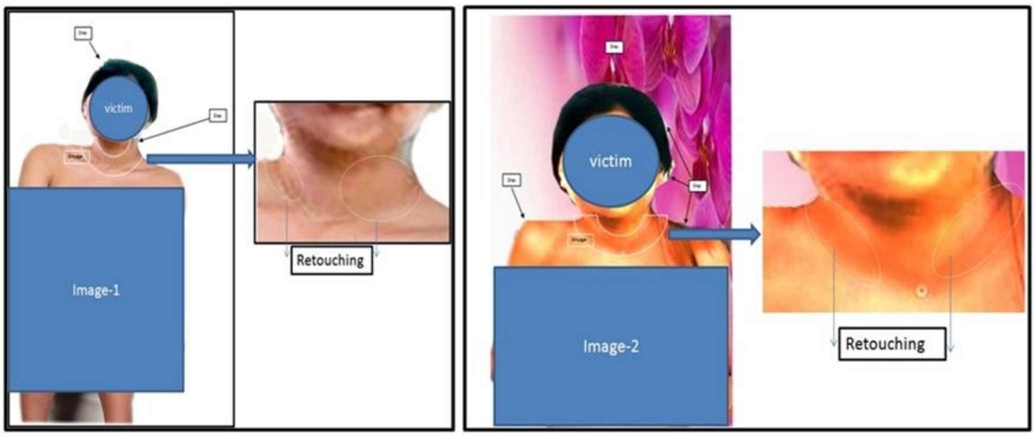

Figure 2: Signs of cropping and retouching

An overall analysis of the obscene images that were retrieved reveals that one of the photographs (Figure 3) has website inscriptions. When the inscriptions were looked up using the "Google search engine," a porn website was mentioned. Following a website exploration, two porn images were found that shared the same morphological characteristics as the recovered porn images. The in-depth comparison of the obtained photographs with the website's relevant images demonstrates that the pornographic images were utilized by the preparatory process to create morphed images of the victim lady.

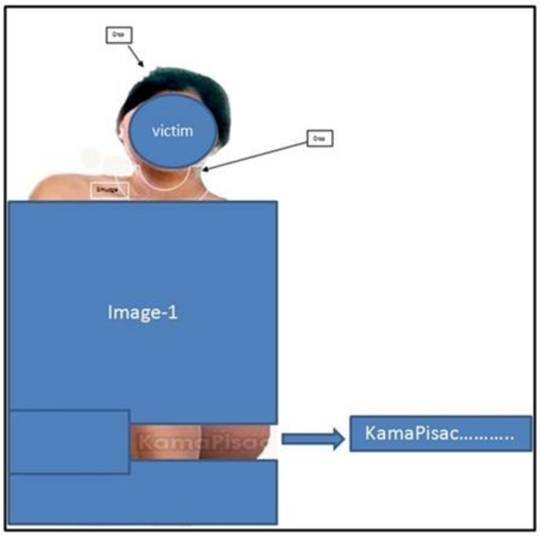

Figure 3: Inscriptions of a Website

Conclusion and discussions:

Cybercriminals take advantage of data posted on social media platforms to commit different types of cybercrimes. Almost every individual, whether from an urban or rural area, uses different types of social media platforms to communicate, share videos, images, or even official or personal documents. It is the need of the hour to make the common user aware of the secure use of such social media platforms. The Government of India initiated various programs like CCPWC, Cyber Surksha Pakhwara, etc. to make the common public aware of cyber crimes. It is also not enough for digital forensic examiners to just confine themselves to the queries of investigating agencies. They must examine the exhibits as a whole and gather every possible clue, which helps investigating agencies link crime scene, victim, and suspect. As in digital crimes, the same technology is used to commit the crime as well as for its detection. It is like a rematch between cybercriminals and forensic experts. It is necessary to update knowledge.

The forensic methodology for detecting image manipulation offers a comprehensive and intelligent approach to uncovering even the most sophisticated manipulations. By combining image file analysis, mobile forensic artifact analysis, and intelligent analysis techniques, forensic experts can accurately identify and analyze manipulated images. This methodology plays a crucial role in digital forensic investigation, supporting legal proceedings, and ensuring the integrity of digital evidence. As technology continues to advance, it is essential to stay vigilant and develop innovative techniques to combat image manipulation effectively.

We can all work together to create a safer digital world by sharing information, expertise, and research in order to shield people from the negative impacts of picture alteration. The suggested methodology is a useful resource for forensic professionals, law enforcement officials, and academics who are looking for the truth and pursuing justice. In a variety of sectors, including journalism, personal security, and criminal investigations, it is essential to be able to recognize and analyze manipulated photographs. With the suggested approach, experts can improve their abilities and methods to unearth the truth underlying faked images, thus ensuring a just and fair society. Additionally, ongoing research and information sharing among professionals might result in the creation of more sophisticated tools and techniques to successfully counteract picture manipulation.

References:

1. Zakharova, V. A., Chernov, I. V., Nazarenko, T. I., Pavlov, P. V., Lyubchenko, V. S., & Kulikova, A. A. (2020). Social health and environmental behavior of students in the digital age. Cypriot Journal of Educational Sciences, 15(5), 1288-1294.
2. AlShariah, N. M., Khader, A., & Saudagar, J. (2019). Detecting fake images on social media using machine learning. International Journal of Advanced Computer Science and Applications, 10(12), 170-176.
3. Chandra Sekhar, P. N. R. L., & Shankar, T. N. (2019). Splicing localization based on noise level inconsistencies in residuals of color channel differences. IJRTE, 8(3), 764-769.
4. Stamm, M. C., Chu, X., & Liu, K. R. (2013, November). Forensically determining the order of signal processing operations. In 2013 IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 162-167). IEEE.
5. Kronander, J. (2015). Physically Based Rendering of Synthetic Objects in Real Environments (Vol. 1717). Linköping University Electronic Press.
6. Akhtar, Z. (2023). Deepfakes Generation and Detection: A Short Survey. Journal of Imaging, 9(1), 18.
7. Dong, B., Zeng, F., & Pan, B. (2019). A simple and practical single-camera stereo-digital image correlation using a color camera and X-cube prism. Sensors, 19(21), 4726.