Applied GIS

ISSN: 1832-5505
Vol-6 Issue-03 July 2018

Research study focusing on the use of watermarking for social media security.

Misses Rekha Kaps[1], Payal Mitkari[2] , Mayuri Ganjewar[3] ,

and Simran Khiani #4 from the Department of IT at the G.H. Raisoni College of Engineering and Management in Pune, India.

Abstract —

Everyone these days has at least one social media account. Every day, there are more and more people who join the world of social media. It causes people to illegally swap media files like photos. It's unlawful for some individuals to create fictitious profiles and then use those profiles to illegally post the images of other people. It is unacceptable for anybody to post illegal photos online. To solve this problem, we suggest developing a mechanism to identify original material owners. If someone steals your images for scientific purposes and posts them online without your knowledge or permission, you can easily track down your attacker..

Keywords — *Security, watermarking, and social media*

I. Introduction

Digital watermarking is a method of invisibly labeling data such as audio, video, or picture files that can tolerate background noise. It is often used to determine who has rights to utilize a certain signal. "Watermarking" refers to the practice of inserting digital data into an existing signal. Carrier signal authenticity and integrity may be confirmed or the signal's owners revealed with the use of digitalwatermarks. It is often used for authenticating banknotes and tracking out the sources of copyright violations. Source tracking is an example of a use case for digital watermarking. At each node in the network, a digital signal is modified by inserting a watermark. Watermarks allow the original distributor to be identified if a copy of the work is ever recovered from the wild. If the encoded information can be consistently recognized from the marked signal after being subjected to any number of transformations, then we say that the digital watermark is transformation-robust. JPEG compression, rotation, cropping, addictive noise, and quantization are all examples of picture degradations that are all too common. Time-based adjustments and MPEG compression are often included to this list for video footage. In order for a digital watermark to be undetectable, the watermarked material must be visually indistinguishable from the unwatermarked version.

II. LITERATURE SURVEY

First published in 2014, "A Survey of Digital Watermarking Techniques and its Applications" provides a comprehensive overview of the many watermarking methods now in use, with a particular emphasis on picture watermarking. Still, the effectiveness of watermarking is evaluated with regards to noise that will reduce the image's quality. The work has briefly discussed the technologies on watermarking their pros and cons, but the DCT, DWT, and DFT methods are still there to discuss in much more detail, as they can provide more security to the images, in the second paper "Digital watermarking techniques for Security application" in 2016.Due to space constraints, not enough technical details are covered in the 2014 paper "Different watermarking techniques and its Application: A review." This paper provides a review of some influential work in the area of digital watermarking technique and the main contribution to this field, including categories of digital watermarking.In 2012's "Social Network Content Management through Watermarking" article, researchers will detail how to implement a foolproof system for protecting users' anonymity while yet allowing them to share information freely. There still seems to be an issue with the suggested approach about who has 'owned' the item initially.

III. Existing System

Unlike newer systems, conventional methods cannot immediately reveal who submitted a photo with a watermark to a social networking platform. To do this, he or she will need to physically gather information and visit labs in an effort to figure out who submitted the photo in question.

Proposed System

Dual watermarking is used in the suggested system. Users should still utilize the reporting feature if they encounter issues that need human intervention, such as when someone snaps a photograph of another user without their permission, when the photo is objectionable, or when the user is abusing the service.

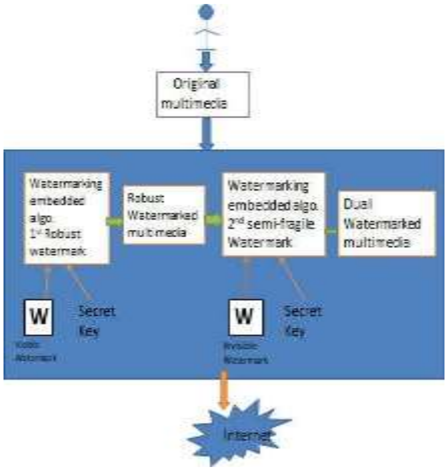
Original multimedia
Watermarking embedded algo 1st Robust watermark
Robust Watermarked multimedia
Watermarking embedded algo 2nd semi-fragile Watermark
Dual Watermarked multimedia
W
Secret Key
Visible Watermark
W
Secret Key
Invisible Watermark
Internet

Fig No.1: System Architecture

This can be considered as a kind of a signature that shows and reals the owner of the photo shared on social media. Our proposed system is used for copyright protection, content authentication, tamper detection.

Three main requirements are :

1. Transparency
2. Robustness
3. Capacity

Algorithm for watermark embedding

For each pixel in base, Watermark and watermarked image :

1. Set n least significant bits to zero for base image.
2. Shift right by 8-n bits for watermark.
3. Add values from base and watermark for the watermarked image.

Algorithm for Watermark Extraction

For each pixel in watermarked image and extracted image :

1. Shift left by 8 n bits for watermarked image.
2. Set to the shifted values of watermarked image for extracted image.

A. Objectives and Scope

Metadata may be used to verify the source and legitimacy of a media file. Date and time, smartphone model, storage location, filename, and file size are all examples of metadata. The production process varies from company to company. Most of the photos we see on social media are posted by individuals we know and care about. With this information, you can track down who illegally shared your photo or image. That's why we choose this metadata. For this reason, we recommend tracking out the original photographer.

IV. CONCLUSION

This system proposes that the original owner of the multimedia will be able to detect who had shared or uploaded his/her personal picture in social media without his permission, by usages of metadata embedded into images before uploaded on social media .

Conclusively, our proposed system can be able to better secure ownership and decrease unauthorized sharing of images.

REFERENCES

[1] ABS-CBN News (2016). NBI: Unauthorized 'sharing' of copyrighted materials is illegal. ABS- CBN News. Retrieved June 11, 2017, from http://news.abs-cbn.com/entertainment/07/05/16/nbi-unauthorizedsharing-of-copyrighted-materials-is-illegal.

[2] Eyed (2016). What are sensitive photos? Eyed Help Center.Retrieved April 22, 2016, from https://eyeem.zendesk.com/hc/enus/articles/202367021-What-are-sensitive-photos-.

[3] Oxford University Press (2017).Definition of social media in English.English Oxford Living Dictionaries.RetrievedApril 13, 2017, from https://en.oxforddictionaries.com/definition/social_ media.

[4] Statista (2016). Statistics and facts about Social Netw

[5] Heather Wood (2007). Invisible Digital Watermarking in the Spatial and DCT Domains for Color Images.Adams State College, Alamosa, Colorado.

[6] MazleenaSalleh, Subariah Ibrahim and Ismail FauziIsnin (2003). Image Encryption Algorithm based on Chaotic Mapping.JurnalTeknologi. 39(D), 1 – 12.

[7] NamitaChandrakar and JaspalBagga (2013). Performance Comparison of Digital Image Watermarking Techniques: A Survey. International Journal of Computer Applications Technology and Research. 2 (2), 126 – 130.

[8] TSR Watermark Image. (2016, April 1). Retrieved April 1

[9] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[10] Md. Selim Reza, Mohammed ShafiulAlam Khan, Md. GolamRbiulAlam, Serajul Islam (2012). An Approach of Digital Image Copyright Protection by Using Watermarking Technology.International Journal of Computer Science Issues, Vol. 9, Issue 2, pg 280 – 286.

[11] Hsiang-Cheh Huang, Wai-Chi Fang (2010). Metadata-based Image Watermarking for Copyright Protection. Simulation Modelling Practice and Theory, Vol. 18, Issue 4, pg 436-445.